Diskrete Mathematik

Simon Krenger
Christian Meyer
Marco Füllemann

January 10, 2012

Chapter 1

Logik (Boolesche Algebra)

Nach George Bool, 1815 bis 1864, Cork (Irland)

1.1 Aussagen

Wir betrachten Aussagen (Sätze), die entweder wahr (1) oder falsch (0) sind.

Heute ist Freitag → wahr

Morgen schneit es in Bern → falsch

Schauen Sie einmal! → keine Aussage

Aussagen bezeichnen wir mit a, b, c, d, ...

Definition 1. *Ist a eine Aussage, somit heisst* $\neg a$ *die Negation von a*

1.2 Konjunktion

Wir verbinden zwei Aussagen a, b mit Hilfe von "und" zu einer einzigen Aussage

$$a \wedge b \tag{1.1}$$

Die Wahrheitstabelle von a ∧ b sind abhängig von denjenigen von a als auch von b. Dies stellen wir in einer Wahrheitswerttabelle dar. Wir finden sofort die Regeln

$$a \wedge \neg a = falsch \tag{1.2}$$

Definition 2. *Eine Aussage, die immer falsch ist, heisst Kontradiktion.*

$$a \wedge 1 = a \tag{1.3}$$

$$a \wedge 0 = 0 \tag{1.4}$$

Weiter finden wir Gesetze

Kommutativgesetz (Vertauschungsgesetz)

$$a \wedge b = b \wedge a \tag{1.5}$$

Beweis 1. *Wir beweisen mit einer Wahrheitswerttabelle*

a	b	$a \wedge b$	$b \wedge a$
0	*0*	*0*	*0*
0	*1*	*0*	*0*
1	*0*	*0*	*0*
1	*1*	*1*	*1*

Assoziativgesetz (Verbindungsgesetz)

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c \tag{1.6}$$

Beweis 2. *Wir beweisen mit einer Wahrheitswerttabelle*

a	b	c	$a \wedge (b \wedge c)$	$(a \wedge b) \wedge c$
0	*0*	*0*	*0*	*0*
0	*0*	*1*	*0*	*0*
0	*1*	*0*	*0*	*0*
0	*1*	*1*	*0*	*0*
1	*0*	*0*	*0*	*0*
1	*0*	*1*	*0*	*0*
1	*1*	*0*	*0*	*0*
1	*1*	*1*	*1*	*1*

Idempotenzgesetz

$$a \wedge a = a \tag{1.7}$$

1.3 Disjunktion

Zwei Aussagen a, b werden mit der Disjunktion "oder" zu einer neuen Aussage verbunden. Dafür schreiben wir:

$$a \vee b \tag{1.8}$$

und definieren

a	b	a $\vee$ b
0	0	0
0	1	1
1	0	1
1	1	1

Nicht verwechseln mit "entweder oder" (XOR)! Wir finden die Regeln

$$a \vee 1 = 1 \tag{1.9}$$

$$a \vee 0 = a \tag{1.10}$$

$$a \vee \neg a = 1 \tag{1.11}$$

Definition 3. *Eine Aussage, die stets wahr ist, heisst Tautologie.*

Es gelten die Gesetze

Kommutativgesetz

$$a \vee b = b \vee a \tag{1.12}$$

Assoziativgesetz

$$a \vee (b \vee c) = (a \vee b) \vee c \tag{1.13}$$

Idempotenzgesetz

$$a \vee a = a \tag{1.14}$$

In der Algebra in $\mathbb{R}$ gilt

$$a(b + c) = ab + ac \tag{1.15}$$

was in der Logik zu

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \tag{1.16}$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \tag{1.17}$$

dem Distributivgesetz (Verteilungsgesetz) führt. Der folgende Beweis zeigt, dass die Gleichung 1.16 gilt.

Beweis 3. *Wir beweisen mit einer Wahrheitswerttabelle*

a	b	c	$b \vee c$	$a \wedge (b \vee c)$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Das zweite Distributivgesetz kann analog dazu bewiesen werden.

In der Logik gibt es zu jedem Gesetz ein duales Gesetz. Dies entsteht durch wechseln von $\vee$ zu $\wedge$ und umgekehrt. Weiter finden wir

Absorbtionsgesetz

$$a \wedge (a \vee b) = a \tag{1.18}$$

$$a \vee (a \wedge b) = a \tag{1.19}$$

Beweis 4. *Wir beweisen mit einer Wahrheitswerttabelle*

a	b	$a \vee b$	$a \wedge (a \vee b)$
0	*0*	*0*	*0*
0	*1*	*1*	*0*
1	*0*	*1*	*1*
1	*1*	*1*	*1*

Gesetz von de Morgan

$$\neg(a \wedge b) = \neg a \vee \neg b \tag{1.20}$$

$$\neg(a \vee b) = \neg a \wedge \neg b \tag{1.21}$$

Wir verwenden die Gesetze, um die Aussagen zu vereinfachen.

1.4 Implikation

Mathematische Lehrsätze haben die Form "Wenn ein Dreieck rechtwinklig ist mit Hypothenuse c und Katheten a, b, dann ist $c^2 = a^2 + b^2$"
Sie bestehen also aus Voraussetzung(en):

Das Dreieck ist rechtwinklig

und Behauptung

Es ist $a^2 + b^2 = c^2$

und einem Beweis

Beweis 5. *Gemäss "Indischer Beweis":*

$$\begin{aligned} c^2 &= 4\frac{ab}{2} + (a-b)^2 \\ c^2 &= 2ab + a^2 - 2ab + b^2 \\ c^2 &= a^2 + b^2 \end{aligned} \tag{1.22}$$

Im obrigen Beispiel haben wir einen direkten Beweis geführt. Von der Voraussetzung durch Rechnung zur Behauptung.
Wenn wir zwei Aussagen a, b mit "wenn a, dann b" oder "wenn a so b" oder "aus a folgt b (a impliziert b)" verknüpfen, so schreiben wir dafür

$$a \to b \tag{1.23}$$

und definieren

a	b	a $\to$ b
0	0	1
0	1	1
1	0	0
1	1	1

Wir finden sofort, das "aus a folgt b"

$$a \to b = \neg a \vee b \tag{1.24}$$

Wollen wir zeigen, dass ein Satz falsch ist, so genügt ein einziges Beispiel, dass wir Gegenbeispiel nennen, um die Behauptung zu widerlegen.

1.4.1 Umkehrung, Kontraposition

Definition 4. *Hat eine Aussage die Form*

$$a \to b \tag{1.25}$$

so heisst

$$b \to a \tag{1.26}$$

die Umkehrung.

Ist eine Aussage, ein Satz wahr, so muss die Umkehrung nicht wahr sein, wie zum Beispiel:

"Wenn ich Geburtstag habe, so esse ich einen Kuchen"

"Wenn ein Mensch glücklich ist, so trinkt er Sinalco"

Wir finden aber, dass

$$\begin{aligned} \neg b \to \neg a &= \neg(\neg b) \vee \neg a \\ = b \vee \neg a &= \neg a \vee b = a \to b \end{aligned} \tag{1.27}$$

Definition 5. *Wir nennen*

$$\neg b \to \neg a \tag{1.28}$$

die Kontraposition von

$$a \to b \tag{1.29}$$

Wir haben gezeigt, dass $\neg b \to \neg a = a \to b$ ist, was bedeutet, dass bei einem wahren Satz auch dessen Kontraposition wahr ist.

Satz: "Wenn es heute Freitag ist, so gehe ich ein Bier trinken."

Kontraposition: "Wenn ich nicht ein Bier trinken gehe, so ist heute Freitag"

Manchmal ist der direkte Beweis eines Satzes zu schwierig oder nicht möglich, dann beweisen wir die Kontraposition.

Satz: Ist $n \in \mathbb{N}$ und n^2 eine gerade Zahl, so ist n auch eine gerade Zahl.

Beweis 6. *Der direkte Beweis*

$$\begin{aligned} n^2 &= 2p \wedge p \in \mathbb{N} \\ \rightarrow n &= \sqrt{2} \cdot \sqrt{p} \end{aligned} \tag{1.30}$$

gelingt nicht. Grund dafür ist, dass eine irrationale Zahl ($\sqrt{2}$) per Definition ein nichtperiodischer, nichtendlicher Dezimalbruch ist.

Also beweisen wir die Kontraposition:

Kontraposition: "Ist $n \in \mathbb{N}$ und n ungerade, so ist auch n^2 ungerade"

Beweis 7.

$$\begin{aligned} n &= 2p+1 \quad \wedge p \in \mathbb{N}_0 \\ \rightarrow n^2 &= (2p+1)^2 \\ n^2 &= 4p^2+4p+1 \\ n^2 &= 2(2p^2+2p)+1 \end{aligned} \tag{1.31}$$

Also ist n^2 eine ungerade Zahl. □

1.5 Aequivalenz

Wenn zwei Aussagen gleichwertig (aequivalent) sind, wenn also

$$(a \rightarrow b) \wedge (b \rightarrow a) \tag{1.32}$$

so schreiben wir dafür

$$a \iff b \tag{1.33}$$

und finden die Wahrheitswerte

a	b	a $\iff$ b
0	0	1
0	1	0
1	0	0
1	1	1

Wir finden die Umformung

$$\begin{aligned} a \iff b &= (a \rightarrow b) \wedge (b \rightarrow a) \\ &= (\neg a \vee b) \wedge (\neg b \vee a) \\ &= (\neg a \wedge b) \vee (\neg a \wedge a) \vee (b \wedge \neg b) \vee (a \wedge b) \\ &= (a \wedge b) \vee (\neg a \wedge \neg b) \end{aligned} \tag{1.34}$$

Ausserdem ist

$$a \iff b = \neg(a \veebar b) \tag{1.35}$$

also

$$\begin{aligned} a \veebar b &= [(a \wedge b) \vee (\neg a \wedge \neg b)] \\ &= \neg(a \wedge b) \wedge \neg(\neg a \wedge \neg b) \\ &= (\neg a \vee \neg b) \wedge (a \vee b) \end{aligned} \tag{1.36}$$

Wenn wir in der Mathematik einen Satz finden, dessen Umkehrung auch wahr ist, so wählen wir die Formulierung mit

"dann und nur dann" oder "genau dann"

im Englischen

"if and only if" oder "iff"

Manchmal gelingt es nicht, die linke Seite in die rechte Seite umzuformen. Dann verwenden wir die Eigenschaft

"Wenn $l = x$ und $r = x$, so ist $l = r$

Wir formen also die linke Seite zuerst einmal um und dann unabhängig davon die rechte Seite und hoffen, dass wir beide Male das gleiche Resultat (x) erhalten.

Genau gleich behandeln wir Behauptungen der Logik wenn es um die Aequivalenz zweier Aussagen geht.

1.6 Logische Schlüsse

Wir gehen aus von verschiedenen Prämissen wie

$$\begin{aligned} &\text{Prämisse 1} \quad && p_1 = a \wedge b \\ &\text{Prämisse 2} && p_2 = \neg a \\ &\text{Prämisse 3} && p_3 = a \wedge \neg b \end{aligned} \tag{1.37}$$

und ziehen daraus eine Konklusion $k : a \vee b$. Nun fragen wir uns, ob die Konklusion bei diesen Prämissen richtig ist. Ist dies der Fall, so sprechen wir von einem logischen Schluss (wenn also das die richtige Konklusion ist).

Es muss also

$$(p_1 \wedge p_2 \wedge ... \wedge p_n) \rightarrow k = 1 \tag{1.38}$$

eine Tautologie sein. Im Beispiel ist also

$$[(a \wedge b) \wedge \neg a \wedge (a \wedge \neg b)] \rightarrow (a \vee b) \tag{1.39}$$

so lange umgeformt werden, bis erkenntlich ist, ob eine Tautologie vorliegt oder nicht.

$$\begin{aligned} & [(a \wedge b) \wedge \neg a \wedge (a \wedge \neg b)] \rightarrow (a \vee b) \\ = \;& (a \wedge b \wedge \neg a \wedge a \wedge \neg b) \rightarrow (a \vee b) \\ = \;& 0 \rightarrow (a \vee b) \\ = \;& \neg 0 \vee (a \vee b) = 1 \vee (a \vee b) = 1 \end{aligned} \tag{1.40}$$

und damit liegt ein logischer Schluss vor.

In der Logik schreiben wir Prämissen und Konklusion untereinander wie zum Beispiel

$$\frac{a \to b \qquad a \wedge b \to c \qquad c}{a} \tag{1.41}$$

Verschiedene bekannte logische Schlüsse besitzen einen Namen, wie zum Beispiel die Folgdenden:

1. modus ponens (Abtrennungsregel)

   $$\frac{a \to b \qquad a}{b} \tag{1.42}$$

   ist ein logischer Schluss, denn

   $$\begin{aligned} & [(a \to b) \wedge a] \to b \\ = \; & [(\neg a \vee b) \wedge a] \to b \\ = \; & (a \wedge b) \to b \\ = \; & \neg(a \wedge b) \vee b \\ = \; & \neg a \vee \neg b \vee b = \neg a \vee 1 = 1 \end{aligned} \tag{1.43}$$

   Es ist die Art und Weise, wie wir einen mathematischen Satz $a \to b$ anwenden.

2. modus tollens (Aufhebende Schlussweise)

   $$\frac{a \to b \qquad \neg b}{\neg a} \tag{1.44}$$

   ist ein logischer Schluss, denn

   $$\begin{aligned} & [(a \to b) \wedge \neg b] \to \neg a \\ = \; & [(\neg a \vee b) \wedge \neg b] \to \neg a \\ = \; & [(b \wedge \neg b) \vee (\neg a \wedge \neg b)] \to \neg a \\ = \; & (\neg a \wedge \neg b) \to \neg a \\ = \; & \neg(\neg a \wedge \neg b) \vee \neg a \\ = \; & a \vee b \vee \neg a = 1 \vee b = 1 \end{aligned} \tag{1.45}$$

3. reductio ad absurdum (zurückführen auf einen Widerspruch)

   $$\frac{a \to (b \wedge \neg b)}{\neg a} \tag{1.46}$$

   ist ein logischer Schluss, denn

   $$\begin{aligned} & [a \to (b \wedge \neg b)] \to \neg a \\ = \; & [a \to 0] \to \neg a \\ = \; & [\neg a \vee 0] \to \neg a \\ = \; & \neg a \to \neg a = a \vee \neg a = 1 \end{aligned} \tag{1.47}$$

Dieser logische Schluss führt uns zum Beweis mit Gegenannahme.

Wollen wir beweisen, dass ein Satz s wahr ist und gelingt uns dies nicht mit einem direkten Beweis oder mit einem Beweis mit Kontraposition, so wählen wir die Gegenannahme:

$\neg s$ ist wahr

und zeigen, dass dies zu einem Widerspruch führt wie $\neg b \wedge b$ oder $1 = 2$ oder ähnlich.

Dann sagt uns die "reductio ad absurdum", dass meine Gegenannahme falsch ist und damit die Aussage s wahr ist.

Einen Beweis mit Gegenannahme nennen wir auch einen indirekten Beweis. Dieses Beweisverfahren können wir auch für logische Schlüsse anwenden.

Ist

$$\frac{a \wedge \neg b \quad a \to b}{a \vee b} \tag{1.48}$$

ein logischer Schluss?

Gegenannahme: Es ist liegt kein logischer Schluss vor und damit ist

$$[(a \wedge \neg b) \wedge (a \to b)] \to (a \vee b) = 0 \tag{1.49}$$

Nun zeigen wir, dass die Gegenannahme zu einem Widerspruch führt. Wir haben die Aussage

$$x \to y = 0$$

Also muss $x = 1$ und $y = 0$ sein.

Es ist $x = p_1 \wedge p_2 \wedge ... \wedge p_n$ (Alle Prämissen und damit muss auch

$$p_1 = p_2 = ... = p_n = 1$$

sein. Um den Widerspruch zu sehen, machen wir eine Tabelle:

	$a \wedge \neg b$	$a \to b$	$\to$	$a \vee b$
1)	$\underline{1}$	1		0
2)				$a = 0, b = 0$
3)	$\underline{0 \wedge 1 = 0}$			

(1.50)

Bei den unterstrichenen Werten haben wir einen Widerspruch hergeführt. Die Gegenannahme ist falsch, also liegt ein logischer Schluss vor.

1.7 Prädikatenlogik

Einige Aussagen wie

- Informatiker(innen) besitzen einen Laptop
- Katzen schnurren
- Hunde bellen
- $a \cdot b = b \cdot a$

verlangen eine Präzisierung wie

- Nicht alle Informatiker(innen) besitzen einen Laptop
- Einige Katzen schnurren
- Alle Hunde bellen
- Für alle $a, b \in \mathbb{R}$ ist $a \cdot b = b \cdot a$

WIr brauchen also ein Prädikat (Aussage) über Grössen aus einer bestimmten Menge und einen Quantor. Wir nennen $\forall$ den Allquantor. Damit bedeutet

$x \in M : \forall x(P(x))$
(Für alle x gilt $P(x)$")

dass alle Elemente der Menge M das Prädikat P besitzen.

Wählen wir

$M = \{s \quad | \quad s \quad \text{ist Student(in)}\}$
$q(s) : s$ ist in der Klasse I1q

so können wir formulieren

$$s \in M : \forall s(q(s)) \tag{1.51}$$

was natürlich falsch ist. Korrekt ist

$$\neg\forall s(q(s)) \quad \text{oder auch} \quad \not\forall s(q(s)) \tag{1.52}$$

geschrieben. Dieses "nicht alle" ist gleichbedeutend mit

"Es gibt (mindestens) ein(e)"

was wir mit dem Existenzquantor $\exists$ so schreiben:

$$\exists s(\neg q(s)) \tag{1.53}$$

Wir haben also

$$\neg\forall x(P(x)) = \exists x(\neg P(x)) \tag{1.54}$$

Betrachten wir

$K = \{k \quad | \quad k \quad \text{Ist eine Katze}\}$
$s(k) : k$ schnurrt

und

$$k \in K : \exists k(s(k)) \tag{1.55}$$

was "es gibt mindestens eine Katze, die schnurrt" bedeutet. Verneinen wir die Aussage

$$\neg\exists k(s(k)) \quad \text{oder} \quad \nexists k(s(k)) \tag{1.56}$$

so bedeutet dies: "Es gibt keine Katze, die schnurrt.", was gleichbedeutend ist mit "Alle Katzen schnurren nicht", also

$$\neg\exists k(s(k)) = \forall k(\neg s(k)) \tag{1.57}$$

Auch in der Mathematik werden die Quantoren verwendet wie zum Beispiel

1.
$$a, b \in \mathbb{R} : \forall a \forall b(ab = ba) \tag{1.58}$$
oder auch
$$a, b \in \mathbb{R} : \forall a, b(ab = ba) \tag{1.59}$$

2.
$$a \in \mathbb{R}\backslash\{0\}, x \in \mathbb{R} : \forall a \exists x(ax = 1) \tag{1.60}$$
Wir nennen $x = a^{-1}$ das zu a inverse Element.

1.7.1 Zwei Prädikate

Oft ist es einfacher, wenn eine Aussage mit Hilfe von zwei Prädikaten formuliert wird. Für

"Alle Informatik-Studierenden besitzen ein iPhone"

wählen wir

$s = \{s \quad | \quad s \quad \text{ist Student(in)}\}$
$i(s) : s$ studiert Informatik
$p(s) : s$ besitzt ein iPhone

und schreiben

$$s \in S : \forall s(i(s) \to p(s)) \tag{1.61}$$

ist die Aussage falsch, weil nicht alle Informatik-Studierenden ein iPhone besitzen, so schreiben wir

$$\neg\forall s(i(s) \to p(s)) \tag{1.62}$$

was gleichbedeutend ist mit

$$\exists s(\neg[i(s) \to p(s)]) \tag{1.63}$$

Dies kann mit Hilfe der Gesetze der Logik umgeformt werden zu

$$\begin{aligned} & \exists s(\neg[\neg i(s) \vee p(s)]) \\ = \quad & \exists s(i(s) \wedge \neg p(s)) \end{aligned} \tag{1.64}$$

Wir sehen also, dass der Existenzquantor eine Verbindung der Prädikate mit "und" verlangt. Wollen wir "Grosskatzen jagen und fressen Fleisch" formulieren, so wählen wir

$G = \{g \quad | \quad g \quad$ ist eine Grosskatze $\}$
$j(g) : g$ jagt
$f(g) : f$ frisst Fleisch

und erhalten

$$g \in G : \exists g(j(g) \wedge f(g)) \tag{1.65}$$

weil wir nicht genau wissen, ob es vegetarische Grosskatzen gibt. Negation ergibt

$$\begin{aligned} \neg\exists g(j(g) \wedge f(g)) \quad &= \quad \forall g(\neg[j(g) \wedge f(g)]) \\ &= \quad \forall g(\neg j(g) \vee \neg f(g)) \\ &= \quad \forall g(j(g) \rightarrow [\neg f(g)]) \end{aligned} \tag{1.66}$$

Wir beachten also, dass

1. $\forall$ verlangt Implikation ($\rightarrow$)
2. $\exists$ verlangt Konjunktion ($\wedge$)

Bei

"Es gibt Leute, die bein Torten-Essen gerne einen Kaffee dazu trinken"

schreiben wir

$M = \{m \quad | \quad m \quad$ ist ein Mensch $\}$
$T(m) : m$ isst ein Stück Torte
$K(m) : m$ trinkt Kaffee

$$m \in M : \exists m(T(m) \wedge K(m)) \tag{1.67}$$

und die Negation

$$\begin{aligned} & \neg\exists m(T(m) \wedge K(m)) \\ = \quad & \forall m(\neg(T(m) \wedge K(m))) \\ = \quad & \forall m(\neg T(m) \vee \neg K(m)) \\ = \quad & \forall m(T(m) \rightarrow \neg K(m)) \quad \text{oder} \quad \forall m(K(m) \rightarrow \neg T(m)) \end{aligned} \tag{1.68}$$

1.7.2 Zweiwertige Prädikate

Sei

$$M = \{x \quad | \quad x \quad \text{ist ein Mensch}\}$$

so lassen sich für $x, y \in M$ z.B. die zweistelligen Prädikate

$L(x, y) : x$ liebt y
$K(x, y) : x$ kennt y
$S(x, y) : x$ streitet mit y

formulieren. Beachte, dass

$$\begin{aligned} K(x,y) &\neq K(y,x) \\ L(x,y) &\neq L(y,x) \end{aligned} \tag{1.69}$$

so bedeutet

$$x, y \in M : \forall x \exists y (K(x, y)) \tag{1.70}$$

dass alle Leute die Person y kennen. Und

$$x, y \in M : \exists x \forall y (K(y, x)) \tag{1.71}$$

bedeutet "Es gibt einen Menschen x, der allen y bekannt ist".

Chapter 2

Mengen

2.1 Mächtigkeit

Die Mengenlehre geht zurück auf Georg Cantor, 1845 bis 1918, in Halle. Heute definieren wir eine Menge, in dem wir ihre Element angeben.

2.1.1 Aufzählung

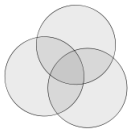
$A = \{-3, a, \diamond, \sqrt{3}, x\}$
$B = \{2, 2, 3, 4, 5\}$ ist nicht möglich: Jedes Element genau einmal, also ist $B = \{2, 3, 4, 5\}$
$C = \{10, 14, 18, 22, ...\}$
$\mathbb{N} = \{1, 2, 3, 4, ...\}$ heisst Menge der natürlichen Zahlen.
$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ heisst Menge der ganzen Zahlen.

2.1.2 Charakterisierung

$M = \{m | m \in \mathbb{N} \wedge 8 < m < 21\}$
$N = \{x | x \in 2^{2-n} \wedge n \in \mathbb{N}\}$ also ist $N = \{2, 1, \frac{1}{2}, \frac{1}{4}, ...\}$
$A = \{x | x \in \mathbb{R} \wedge x^2 = -1\}$, A hat keine Elemente, die leere Menge $\emptyset$.
$\mathbb{Q} = \{x | x = \frac{a}{b} \wedge a, b \in \mathbb{Z} \wedge b \notin 0\}$ ist die Menge der rationalen Zahlen.
$\mathbb{R} = \{x | x$ ist als Dezimalbruch darstellbar ist die Menge der reellen Zahlen.

2.1.3 Euler-Venn-Diagramm

Nach Leonard Euler, Riehen b. Basel, Petersburg, Berlin, 1707 bis 1783.



algebraische Zahl: Lösung einer (Polynom-) Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 n^1 + a_0 \tag{2.1}$$

mit rationalen Koeffizienten $a_i \in \mathbb{Q}$ $(i = 0, 1, ...n)$

transzendente Zahl: Nicht-algebraisch, aber irrational. Nach L. Euler: "quod algebrae vires transcendit" (lat. "Was die Kraft der Algebra übersteigt")
π, e sind transzendente Zahlen.

Definition 6. *Wir nennen die Anzahl der Elemente einer Menge A die Mächtigkeit $|A|$.*

In $\mathbb{N} = \{1, 2, 3, ...\}$ hat es unendlich viele Elemente.

Definition 7. *Die Mächtigkeit von $\mathbb{N}$ ist $\aleph_0$ ("Aleph-null").*

Welches ist nun die Mächtigkeit von $G = \{2, 4, 6, ...\}$?

Definition 8. *Zwei Mengen A und B sind gleichmächtig $|A| = |B|$, wenn jedem Element von A genau eines von B zugeordnet werden kann und umgekehrt.*

Es muss also eine Funktion von A nach B existieren, wie umkehrbar ist.

Gehen wir nun zurück zu $G = \{2, 4, 6, 8, ...\}$,

$\mathbb{N}$	1	2	3	4	...
$\mathbb{G}$	2	4	6	8	...

Mit $f(n) = 2n$ haben wir eine umkehrbare, eindeutige Funktion gefunden. Also ist $|G| = \aleph_0$
Betrachten wir nun

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\} \tag{2.2}$$

und versuchen eine Zuweisung mit $\mathbb{N}$ zu bilden.

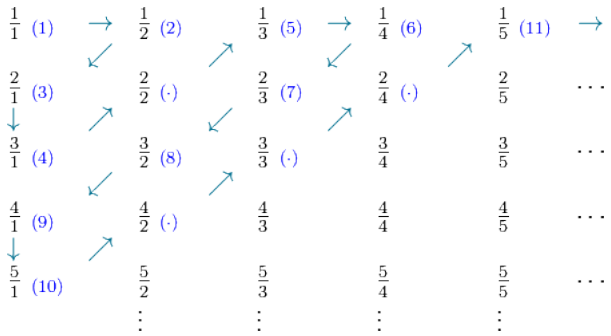
$\mathbb{N}$	1	2	3	4	5
$\mathbb{Z}$	0	1	-1	2	-2

und finden $|\mathbb{Z}| = \aleph_0$ mit

$$f(x) = \begin{cases} \frac{x}{2} & \text{wenn } x \text{ gerade, } x \in \mathbb{N} \\ \frac{-x-1}{2} & \text{wenn } x \text{ ungerade, } x \in \mathbb{N} \end{cases}$$

Definition 9. *Eine Menge A mit $|A| = \aleph_0$ besitzt abzählbar-unendlich viele Elemente.*

Wie ist es nun mit $\mathbb{Q}$ und der Mächtigkeit? Wir versuchen das Cantorsche Diagonalverfahren.



Zusätzlich definieren wir als erstes Element in der Menge die Zahl 0. Kommt eine Zahl zum

- ersten Mal vor, so zählen wir diese
- zweiten Mal vor, so wählen wir diese negativ.
- dritten, vierten Mal vor, so überspringen wir diese

Die 0 kommt an den Anfang. Also ist $|\mathbb{Q}| = \aleph_0$.

Betrachten wir nun $\mathbb{R}$:

Wir versuchen zu ordnen: $0.1, 0.01, 0.001, ...$

Es gelingt nicht, eine Funktion von $\mathbb{N}$ nach $\mathbb{R}$ zu finden.

Definition 10. *Die Menge $\mathbb{R}$ ist überabzählbar-unendlich und ihre Mächtigkeit ist $\aleph_1$.*

2.2 Vollständige Induktion

Nach Giuseppe Peano, Turin, 1858 bis 1932
Peano hat gezeigt, dass die natürlichen Zahlen auf den Axiomen

Axiom 1. *Es gibt eine kleinste Zahl*

Axiom 2. *Jede Zahl besitzt einen Nachfolger*

Axiom 3. *Gilt eine Aussage für n und auch für $n+1$, so gilt sie für alle $n \in \mathbb{N}$, falls sie für $n = 1$ gilt.*

beruhen (Peano-Axiome genannt).

Axiom (3) führt uns zum Beweis mit vollständiger Induktion. Dieser Beweis besteht aus drei Teilen.

1. Induktionsverankerung (Induktionsanfang)
   Die Behauptung stimmt für $n = 1$

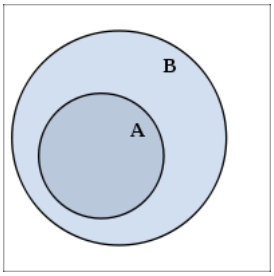
2. Induktionsschritt
   Unter der Voraussetzung, dass die Behauptung für n gilt, ist zu zeigen, dass sie auch für $n+1$ gilt.

3. Induktionsvererbung (Induktionsschluss)
   Nach (1) gilt die Behauptung für $n = 1$ und nach (2) gilt sie für $n+1$, wenn sie für n gilt. Somit gilt die Behauptung für $n = 2$ usw. Also gilt sie für $n \in \mathbb{N}$.

Mit der vollständigen Induktion haben wir die letzte der vier wichtigsten Beweisverfahren in der Mathematik definiert. Im Folgenden nochmals die Beweisverfahren:

- Direkter Beweis
- Indirekter Beweis (Beweis mit Gegenannahme)
- Beweis mit Kontraposition
- Beweis mit vollständiger Induktion

2.3 Teilmengen



Definition 11. *A ist eine Teilmenge von B*

$$A \subset B \iff \forall x(x \in A \to x \in B) \tag{2.3}$$

Wie viele Teilmengen besitzt A, wenn $|A| = n$?

1. $n = 1$: $A = \{x\}$
   Teilmengen: $\{x\}, \emptyset$
   (Die leere Menge $\emptyset$ ist Teilmenge jeder Menge)

2. $n = 2$: $A = \{x, y\}$
   Teilmengen: $\emptyset, \{x\}, \{y\}, \{x, y\}$

3. $n = 3$: $A = \{x, y, z\}$
   Teilmengen: $\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{y, z\}, \{x, z\}, \{x, y, z\}$

Ist $|A| = n$, so gibt es 2^n Teilmengen, denn für jedes Element von A gibt es zwei Möglichkeiten, zur Teilmenge zu gehören oder nicht.

Definition 12. *Die Menge aller Teilmengen einer Menge A heisst Potenzmenge $\mathcal{P}(A)$*

Nun untersuchen wir, wieviele Teilmengen mit genau k Elementen eine Menge $|A| = n$ besitzt, wenn $0 \leq k \leq n$ ist.

	k=					
n=	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

Wir erhalten das Pascalsche Dreieck (Blaise Pascal, 1623 bis 1662, Paris).

$$
\begin{array}{lccccccccc}
n=0: & & & & & 1 & & & & \\
n=1: & & & & 1 & & 1 & & & \\
n=2: & & & 1 & & 2 & & 1 & & \\
n=3: & & 1 & & 3 & & 3 & & 1 & \\
n=4: & 1 & & 4 & & 6 & & 4 & & 1
\end{array}
$$

Das 3. Element in der 5. Zeile gibt uns also die Anzahl der Teilmengen mit genau 3 Elementen einer Menge A mit $|A| = 5$ an: das sind 10.
Um das Binom $(a+b)^4$ zu berechnen, wählen wir die vierte Zeile und finden dort die Koeffizienten:

$$
\begin{aligned}
(a+b)^4 &= 1 \quad +4 \quad +6 \quad +4 \quad +1 \\
\text{und weiter} \quad &= 1a^4 \quad +4a^3 \quad +6a^2 \quad +4a^1 \quad +1a^0 \\
&= 1a^4b^0 + 4a^3b^1 + 6a^2b^2 + 4a^1b^3 + 1a^0b^4 \\
&= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4
\end{aligned} \tag{2.4}
$$

Definition 13. *Die Zahlen im Pascalschen Dreieck werden Binominalkoeffizienten genannt. Wir schreiben $\binom{n}{k}$ ("n tief k") für das k-te Element in der n-ten Zeile.*

Es ist also

$$
(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{k}a^{n-k}b^k + ... + \binom{n}{k}b^n \tag{2.5}
$$

was wir den binomischen Lehrsatz nennen.

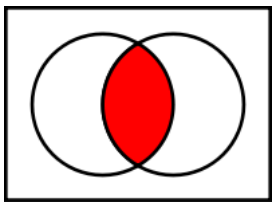
2.3.1 Intervalle

Definition 14. *Wir nennen*

- $[a;b] := \{x \quad | \quad x \in \mathbb{R} \wedge a \leq x \leq b\}$
  ein abgeschlossenes Intervall.
- $]a;b[= (a;b) := \{x \quad | \quad x \in \mathbb{R} \wedge a < x < b\}$
  ein offenes Intervall.
- $[a;b[:= \{x \quad | \quad x \in \mathbb{R} \wedge a \leq x < b\}$
  ein halboffenes (abgeschloffenes) Intervall.

2.4 Operationen mit Mengen

2.4.1 Schnittmenge



$A \cap B$

Definition 15.

$$A \cap B := \{x \quad | \quad x \in A \wedge x \in B\} \tag{2.6}$$

heisst Schnittmenge (Durchschnittsmenge, Schnitt) von A und B.

Wir finden sofort:

$$A \cap \emptyset = \emptyset \tag{2.7}$$

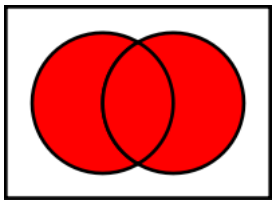
$$A \cap A = A \tag{2.8}$$

$$A \cap B = B \cap A \tag{2.9}$$

$$(A \cap B) \cap C = A \cap (B \cap C) \tag{2.10}$$

Definition 16. *Ist $A \cap B$ die leere Menge ($A \cap B = \emptyset$), so heissen A und B disjunkt.*

2.4.2 Vereinigungsmenge



$A \cup B$

Definition 17.

$$A \cup B := \{x \quad | \quad x \in A \vee x \in B\} \tag{2.11}$$

heisst Vereinigungsmenge (Verein) von A und B.

Wir finden sofort:

$$A \cup \emptyset = A \tag{2.12}$$

$$A \cup A = A \tag{2.13}$$

$$A \cup B = B \cup A \tag{2.14}$$

$$(A \cup B) \cup C = A \cup (B \cup C) \tag{2.15}$$

und die Distributivgesetze

$$\begin{aligned} \forall A, B, C \quad &: \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ \forall A, B, C \quad &: \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{aligned} \tag{2.16}$$

Der Beweis kan entweder mit Hilfe der Definitionen oder mit 2 Diagrammen geführt werden.

Beweis mit Hilfe der Definitionen

Beweis 8.

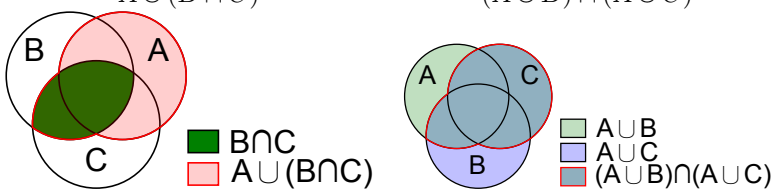
$$\begin{aligned} A \cap (B \cup C) &= \{x \quad | \quad x \in A \wedge x \in (B \cup C)\} \\ &= \{x \quad | \quad x \in A \wedge (x \in B \vee x \in C)\} \\ &= \{x \quad | \quad (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\} \\ &= \{x \quad | \quad x \in A \wedge x \in B\} \cup \{x \quad | \quad x \in A \wedge x \in C\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned} \tag{2.17}$$

□

Beweis mit 2 Diagrammen

Beweis 9. *Wir zeichnen zwei Diagramme, eines für die linke Seite und eines für die rechte Seite der Behauptung (mit Index).*

$A \cup (B \cap C)$ $\qquad$ $(A \cup B) \cap (A \cup C)$



und die Absorbtionsgesetze

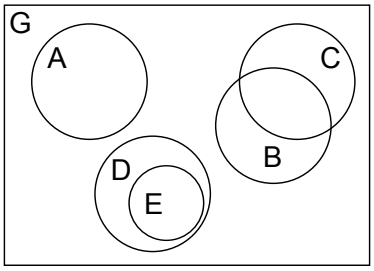
$$\forall a, b : A \cap (B \cup A) = A \tag{2.18}$$

$$\forall a, b : A \cup (B \cap A) = A \tag{2.19}$$

Beweis analog.

2.4.3 Komplement

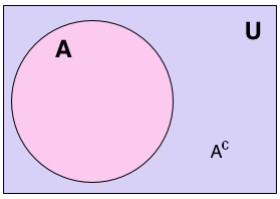
Im Folgenden sind die von uns betrachteten Mengen $A, B, C...$ Teilmengen der Grundmenge G.



Definition 18.

$$\overline{A} := \{x \quad | \quad x \notin A\} \tag{2.20}$$

heisst Komplementärmenge (Komplement) der Menge A



$\overline{A}$ entspricht in diesem Bild A^c in der Grundmenge U.

Dann sehen wir, dass

$$A \cap \overline{A} = \emptyset \tag{2.21}$$

und

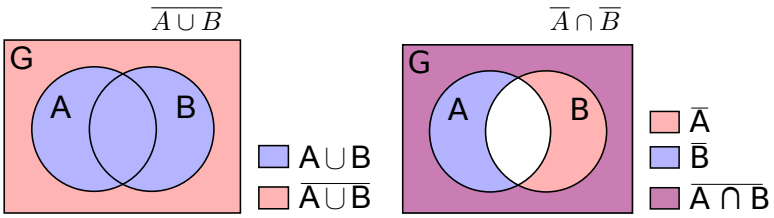
$$A \cup \overline{A} = G \tag{2.22}$$

Weiter gelten die Gesetze von De Morgan:

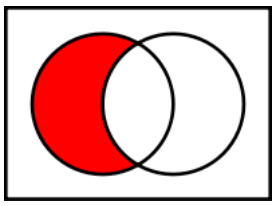
$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{2.23}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{2.24}$$

Beweis 10. *Wir beweisen mit zwei Diagrammen:*



2.4.4 Differenz



Definition 19.

$$A \setminus B = \{x \quad | \quad x \in A \wedge x \notin B\} \tag{2.25}$$

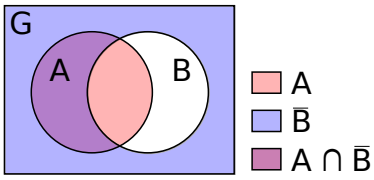
heisst Differenz der Mengen A und B.

Wir finden

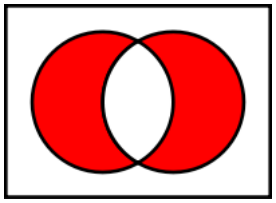
$$A \setminus B = A \cap \overline{B} \tag{2.26}$$

$$B \cap (C \setminus A) = (B \setminus A) \cap (C \setminus A) \tag{2.27}$$

Wir sagen, dass die Differenz rechtsdistributiv bezüglich des Schnittes ist. Sie ist aber nicht linksdistributiv des Schnittes.



2.4.5 Symetrische Differenz



Definition 20.

$$A \Delta B := (A \setminus B) \cup (B \setminus A) \tag{2.28}$$

heisst die symetrische Differenz der Mengen A und B.

2.5 Kartesisches Produkt

Nach René Decartes, 1596 bis 1650, Paris, Stockholm

Definition 21.

$$A \times B := \{(x/y) \quad | \quad x \in A \wedge y \in B\} \tag{2.29}$$

heisst kartesisches Produkt der Mengen A und B.

Es ist also

$$A \times B \neq B \times A \tag{2.30}$$

Wir sagen auch, dass $A \times B$ die Menge der geordneten Paare ist. Sind $A, B \in \mathbb{R}$, so können wir $A \times B$ im kartesischen Koordinatensystem darstellen.

Definition 22. *Für $n \in \mathbb{N}$ ist*

$$A^n := A \times A \times A \times ... \times A \quad \textit{(n Faktoren)} \tag{2.31}$$

Definition 23. *Für $n \in \mathbb{N}$ ist*

$$A^n := A \times A \times A \times ... \times A \quad \textit{(n Faktoren)} \tag{2.32}$$

Chapter 3

Relationen

3.1 Darstellung

Ausgehend von einer Menge

M = {Alex, Barbara, Claudia} von Geschwistern

suchen wir Beziehungen zwischen den Elementen. Wie z.B.

"ist die Schwester von"

und finden

"Alex ist die Schwester von Barbara" ist falsch
"Barbara ist die Schwester von Alex" ist richtig

etc.
So erhalten wir Paare, welche die Relation (Beziehung) erfüllen:

$$(B, A), (B, C), (C, B), (C, A) \tag{3.1}$$

Fassen wir diese Paare in einer Menge zusammen, so erhalten wir eine Teilmenge von M^2 (das kartesische Produkt).

Definition 24. *Eine Relation R in einer Menge M ist eine Teilmenge von $M^2 : R \subset M^2$*

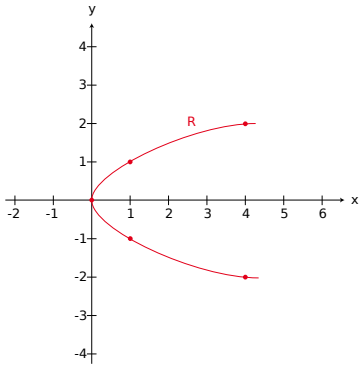
Relationen können wir im kartesischen Koordinatensystem darstellen.

$$\text{Ist} x, y \in \mathbb{R} : xRy \iff x = y^2 \tag{3.2}$$

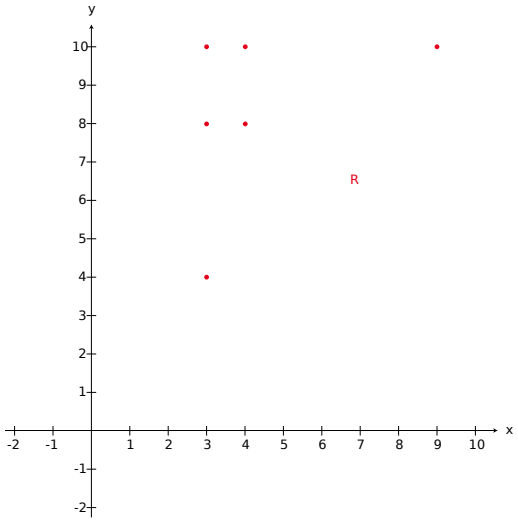
so finden wir einige Paare:

$$R = \{(0/0), (4/2), (4/-2), (1/1), (1/-1), ...\} \tag{3.3}$$

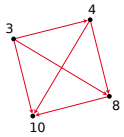
und damit



Das ist nicht der Graph einer Funktion, da wir für einen x-Wert mehrere y-Werte erhalten. Im Koordinatensystem

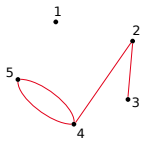


Eine andere Möglichkeit ist die Darstellung mit einem Graphen.

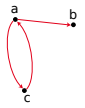


Definition 25. *Ein Graph ist ein Paar, bestehend aus einer Menge E von Eckpunkten (Ecken, engl. vertices) und einer Menge K von Kanten (engl. edges).*

Also zum Beispiel



Bei den Relationen müssen wir im Graphen angeben, ob a mit b oder b mit a in Relation steht. So erhalten wir einen gerichteten Graphen.



Der Graph enthält Schlingen.
Wir können auch eine Tabelle mit Wahrheitswerten wählen, um eine Relation darzustellen. Für obige Relation erhalten wir

	1	2	3
1	1	0	0
2	1	1	0
3	1	1	1

Damit finden wir die Adjazenzmatrix

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \tag{3.4}$$

3.2 Eigenschaften

Definition 26. *Eine Relation $R \subset M^2$ heisst reflexiv, wenn*

$$a \in M : \forall a(aRa) \tag{3.5}$$

Bei einer reflexiven Relation besitzt im Graphen jede Ecke eine Schlinge.

Definition 27. *Eine Relation $R \subset M^2$ heisst symetrisch, wenn*

$$a, b \in M : \forall a, b(aRb \rightarrow bRa) \tag{3.6}$$

Definition 28. *Eine Relation $R \subset M^2$ heisst antisymetrisch, wenn*

$$a, b \in M : \forall a, b[(aRb) \wedge (bRa) \rightarrow (a = b)] \tag{3.7}$$

Definition 29. *Eine Relation $R \subset M^2$ heisst transitiv, wenn*

$$a, b, c \in M : \forall a, b, c[(aRb \wedge bRc) \rightarrow (aRc)] \tag{3.8}$$

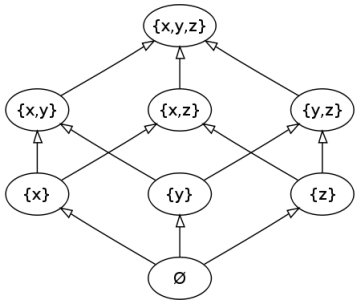
Definition 30. *Eine Relation R aus $M \times M$ heisst Ordnungsrelation, wenn R reflexiv, antisymetrisch und transitiv ist.*

Ordnungsrelationen in endlichen Mengen können in einem Hasse-Diagramm (Helmut Hasse, 1898–1979) dargestellt werden.

Nehmen wir $M = \{2, 3, 4, 5, 12, 13, 25\}$ und die Relation $a|b$:

TODO

Die Relation $A \subset B$ in $\mathcal{P}(A)$, wenn $M = \{x, y, z\}$



Definition 31. *Eine Relation R aus $M \times M$ heisst Aequivalenzrelation, wenn sie reflexiv, symetrisch und transitiv ist.*

3.3 Restklassen

Wir untersuchen die Operation

$$a \mod m \tag{3.9}$$

für $a \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{1\}$. Dabei heisst m der Modul. Wir können also

$$a \mod m = r \iff \exists x(a = mx + r) \tag{3.10}$$

mit $a \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{1\}$, $0 \leq r < m$, $x \in \mathbb{Z}$ schreiben.
Wir überlegen, ob

$$(a + b) \mod m = a \mod m + b \mod m \tag{3.11}$$

ist. Ist $a = 21, b = 18, m = 4$, so ist

$$(a + b) \mod m = 39 \mod 4 = 3 \tag{3.12}$$

und

$$\begin{aligned} a \mod m &= 21 \mod 4 = 1 \\ b \mod m &= 18 \mod 4 = 2 \end{aligned} \tag{3.13}$$

aber mit $a = 35$, $b = 17$, $m = 6$ wird

$$\begin{aligned} (a + b) \mod m &= 52 \mod 6 \\ a \mod m &= 35 \mod 6 = 5 \\ b \mod m &= 17 \mod 6 = 5 \end{aligned} \tag{3.14}$$

Es ist also

$$\begin{aligned} (a + b) \mod m &= (a \mod m + b \mod m) \mod m \\ (ab) \mod m &= (a \mod m \cdot b \mod m) \mod m \end{aligned} \tag{3.15}$$

wie wir mit obriger Definition zeigen können.

Beispiel 1. *Welches ist die letzte Ziffer von* 3^{25}*?*

$$\begin{aligned} 3^{25} \mod 10 &= (3^2)^{12} \cdot 3 \mod 10 \\ &= ((3^2)^{12} \mod 10 \cdot 3 \mod 10) \mod 10 \\ &= ((9^{12} \mod 10) \cdot 3 \mod 10) \mod 10 \end{aligned} \tag{3.16}$$

Da $-1 \mod 10$ *auch* 9 *ist, erhalten wir*

$$\begin{aligned} & ((-1)^{12} \mod 10 \cdot 3 \mod 10) \mod 10 \\ = \; & (1 \mod 10 \cdot 3 \mod 10) \mod 10 \\ = \; & (1 \cdot 3) \mod 10 = 3 \end{aligned} \tag{3.17}$$

Beispiel 2. *An welchem Wochentag war der 10. Januar 1986?*
Wir gehen davon aus, dass

1. Januar 1900 war ein Montag

und berechnen die Anzahl Tage bis zum gesuchten Tag. Es ist $365 \mod 7 = 1$*, also wird pro Jahr (ohne Schaltjahr) alles um einen Wochentag verschoben. Für die Monate finden wir eine Verschiebung gemäss folgender Tabelle:*

Monat	*Verschiebung*
Januar	*0 Tage*
Februar	*3 Tagen*
März	*3 Tagen*
April	*6 Tagen*
Mai	*1 Tag*
Juni	*4 Tage*
Juli	*6 Tage*
August	*2 Tage*
September	*5 Tage*
Oktober	*0 Tage*
November	*3 Tage*
Dezember	*5 Tage*

Im Februar haben wir eine Verschiebung von 3 Tagen, da $31 \mod 7 = 3$ *und der Januar eben 31 Tage hat. Der Mai hat eine Verschiebung von 1 Tag, da der April 30 Tage hat und* $30 \mod 7 = 2$ *ist und* $6 + 2 = 8$*, aber* $8 \mod 7 = 1$*.*

Betrachten wir die Schaltjahre, so müssen wir

$$[\frac{Jahre}{4}] = \text{floor(Jahre / 4)} \tag{3.18}$$

berechnen. $[x]$ heisst Gauss'sche Klammer.
So finden wir für den 10. Januar 1986

Jahr:	$86 \mod 7 = 2$
Schaltjahre:	$[\frac{86}{4}] = 21 \mod 7 = 0$
Monat:	Januar = 0
Tag:	$10 \mod 7 = 3$
Summe:	5

1 ist Montag, 2 ist Dienstag usw. Also war der 10. Januar 1989 an einem Samstag. Für den 2. Dezember 2011 finden wir

Jahr:	$111 \mod 7 = 6$
Schaltjahre:	$[\frac{111}{4}] = 27$ und $27 \mod 7 = 6$
Monat:	Dezember = 5 (gemäss Tabelle)
Tag:	2
Summe:	19 und $19 \mod 7 = 5$, also Freitag

3.3.1 Die Relation $a \equiv b \ (\mod m)$

Für ganze Zahlen a, b und $n \in \mathbb{N} \setminus \{1\}$ untersuchen wir, wann a und b bei Division durch m denselben Rest besitzen. Dann sagen wir

"a kongruent b modulo n"

Somit gibt es $x, y \in \mathbb{Z}$, so dass

$$a = mx + r \wedge b = my + r \tag{3.19}$$

mit $0 \leq r < m$ gilt. Weiter ist dann

$$\begin{aligned} a - b &= mx + r - (my + r) \\ a - b &= mx - my \\ a - b &= m(x - y) \end{aligned} \tag{3.20}$$

also ist $a-b$ ein Vielfaches von m, was das Gleiche bedeutet wie "m teilt $a-b$". Wir haben also die Relation

$$a, b \in \mathbb{Z}, m \in \mathbb{N} \setminus \{1\} : a \equiv b(\mod m) \iff a | a - b \tag{3.21}$$

Ist z.B. $m = 5$, so ist

$$32 \equiv 17(\mod 5) \tag{3.22}$$
$$44 \equiv 9(\mod 5) \tag{3.23}$$
$$-4 \equiv 11(\mod 5) \tag{3.24}$$
$$-8 \equiv -13(\mod 5) \tag{3.25}$$

Die Relation ist <u>reflexiv</u>, denn

$$a \equiv a(\mod m) \to m | a - a \to m | 0 \tag{3.26}$$

was für alle $m \in \mathbb{N} \setminus \{1\}$ wahr ist.
<u>symmetrische</u>, denn

$$\begin{aligned} a \equiv b(\mod m) &\to m | a - b \\ &\to m | (-1)(a - b) \to m | b - a \to b \equiv a(\mod m) \end{aligned} \tag{3.27}$$

<u>transitiv</u>, denn

$$\begin{aligned} & a \equiv b(\mod m) \wedge b \equiv c(\mod m) \\ \to \quad & m | a - b \wedge m | b - c \\ \to \quad & m | (a - b) + (b - c) \\ \to \quad & m | a - c \\ \to \quad & a \equiv c(\mod m) \end{aligned} \tag{3.28}$$

Somit ist $a \equiv b(\mod m)$ eine Aequivalenzrelation. Ist z.B. $m = 5$ der Modul, so sind die Aequivalenzklassen

TODO

Definition 32. *Die durch $a \equiv b(\mod m)$ entstehenden Aequivalenzklassen heissen Restklassen.*

Ist der Modul $m = 5$, so sind

$$\begin{aligned} \overline{0} &= \{..., -10, -5, 0, 5, 10, ...\} \\ \overline{1} &= \{..., -9, -4, 1, 6, 11, ...\} \\ \overline{2} &= \{..., -8, -3, 2, 7, 12, ...\} \\ \overline{3} &= \{..., -7, -2, 3, 8, 13, ...\} \\ \overline{4} &= \{..., -6, -1, 4, 9, 14, ...\} \end{aligned} \tag{3.29}$$

die Restklassen.

Definition 33. *Wir nennen*

$$\mathbb{Z}_5 := \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} \tag{3.30}$$

ein vollständiges Restsystem.

Nun rechnen wir mit diesen Restklassen und überlegen dass

$$\overline{4} + \overline{3} \tag{3.31}$$

bedeutet, dass $a \in \overline{4}$, $b \in \overline{3}$ beliebig gewählt werden darf und diejenige Klasse gesucht ist, die $a + b$ enthält. Alle möglichen Additionen stellen wir ein einer Verknüpfungstabelle dar (Der Strich ist weggelassen).

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(Linke Seite zuerst)

Dann erstellen wir die Verknüpfungstafel für die Multiplikation in $\mathbb{Z}_5 \setminus \{0\}$

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(Linke Seite zuerst)

Definition 34. *Ist in einer Menge M eine Operation * so definiert, dass*

$$\forall a, b : a * b \in M \tag{3.32}$$

so heisst $< M; * >$ eine algebraische Struktur.

Nun untersuchen wir, welche Gesetze in einer algebraischen Struktur erfüllt sind. Es ist $< M; * >$ eine algebraische Struktur

Kommutativgesetz: $a, b \in M : \forall a, b(a * b = b * a)$
Assoziativgesetz: $a, b, c \in M : \forall a, b, c[(a * b) * c = a * (b * c)]$
Neutrales Element: $a, e \in M : \forall a \exists e(a * e = e * a = a)$
Inverses Element: $a, a^{-1} \in M : \forall a \exists a^{-1}(a * a^{-1} = a^{-1} * a = e)$

Wenn wir nun $< \mathbb{Z}_5; + >$ untersuchen, so sehen wir, dass

1. Das Kommutativgesetz erfüllt ist, weil die Tabelle symmetrisch bezüglich der Hauptdiagonalen (links oben nach rechts unten) ist.

2. Das Assoziativgesetz erfüllt ist, weil die Klassen stellvertretend für ganze Zahlen stehen und die Addition von ganzen Zahlen assoziativ ist.

3. 0 das neutrale Element ist, weil

$$a \in \mathbb{Z}_5 : \forall a(a + 0 = 0 + a = a) \tag{3.33}$$

4. Zu jedem $a \in \mathbb{Z}_5$ ein inverses Element existiert, denn

   4 ist zu 1 invers, denn $1 + 4 = 4 + 1 = 0$
   1 ist zu 4 invers, denn $4 + 1 = 1 + 4 = 0$
   2 ist zu 3 invers, denn $3 + 2 = 2 + 3 = 0$
   3 ist zu 2 invers, denn $2 + 3 = 3 + 2 = 0$
   0 ist zu 0 invers, denn $0 + 0 = 0 + 0 = 0$

Untersuchen wir $< \mathbb{Z}_5 \setminus \{0\}; \cdot >$, so gelten (K) und (A). Weiter ist 1 das neutrale Element und

3 ist zu 2 invers, da $2 \cdot 3 = 1$
2 ist zu 3 invers, ...
4 ist zu 4 invers, da $4 \cdot 4 = 1$
1 ist zu 1 inver, da $1 \cdot 1 = 1$

Definition 35. *Gelten in einer algebraischen Struktur $< M; * >$ das Assoziativgesetz, das Kommutativgesetz und existieren ein neutrales Element und existiert zu jedem $a \in M$ ein inverses Element, so heisst $< M; * >$ eine abelsche Gruppe (Niels Henrik Abel, 1802 bis 1829, Oslo).*

Wie wir gesehen haben, genügen diese vier Eigenschaften, um Gleichungen zu lösen. Wollen wir

$$x^2 + 2x + 2 = 0 \quad \text{in} \quad \mathbb{Z}_5 \tag{3.34}$$

lösen, so können wir nicht in Faktoren zerlegen. Wir wählen deshalb andere Repräsentanten.

$$x^2 + 2x + 7 = 0 \quad \text{weil} \quad \overline{2} = \{..., -3; 2; 7; 12, ...\} \tag{3.35}$$

geht immer noch nicht, daher

$$x^2 + 7x + 12 = 0 \tag{3.36}$$

und damit

$$\begin{aligned} \rightarrow (x+3)(x+7) &= 0 \\ x+3=0 \quad &\vee \quad x+4=0 \\ x_1 = 2 \quad &\vee \quad x_2 = 1 \end{aligned} \tag{3.37}$$

Betrachten wir nun $\mathbb{Z}_8$ mit Addition und Multiplikation

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\cdot$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Wir finden

> $< \mathbb{Z}_8; + >$ ist eine abelsche Gruppe
> $< \mathbb{Z}_8 \setminus \{0\}; \cdot >$ ist keine abelsche Gruppe, da zu 2, 4 und 6 kein inverses Element existiert,

Ausserdem ist

$$a \cdot b = 0 \rightarrow (a = 0 \vee b = 0) \tag{3.38}$$

für $a, b \in \mathbb{Z}_8$ erfüllt, aber ausserdem gilt noch

$$ab = 0 \rightarrow (a = 2 \wedge b = 4) \tag{3.39}$$

$$ab = 0 \rightarrow (a = 4 \wedge b = 6) \tag{3.40}$$

usw. Wir sagen, dass $\mathbb{Z}_8$ Nullteiler besitzt (Zahlen, die Null ergeben, wenn man sie multipliziert). Lösen wir Gleichungen in $\mathbb{Z}_8$ wie

$$\begin{aligned} 2(x+5) &= 6x+2 \\ 2x+2 &= 6x+2 \\ 2x &= 6x \\ 4x &= 0 \rightarrow x = 0 \end{aligned} \tag{3.41}$$

So müssen wir die Nullteiler berücksichtigen und finden

$x_2 = 2, x_3 = 4, x_4 = 6$

Wollen wir

$$x^2 + 5x + 4 = 0 \quad \text{in} \quad \mathbb{Z}_{10} \tag{3.42}$$

lösen, so finden wir keine quadratische Ergänzung zu

$$x^2 + 5x \tag{3.43}$$

da 2^{-1} in $\mathbb{Z}_{10}$ nicht existiert. Also zerlegen wir in Faktoren

$$(x + 4)(x + 1) = 0 \tag{3.44}$$

und betrachten die Fälle (in $\mathbb{Z}_{10}$)

$$2 \cdot 5 = 4 \cdot 5 = 6 \cdot 5 = 8 \cdot 5 = 0 \tag{3.45}$$

Zuerst aber

$$\begin{aligned} x + 4 = 0 \quad &\vee \quad x + 1 = 0 \\ x_1 = 6 \quad &\qquad x_2 = 9 \end{aligned} \tag{3.46}$$

und dann

$$\begin{aligned} x + 4 = 2 \quad &\wedge \quad x + 1 = 5 \\ x = 8 \quad &\wedge \quad x = 4 \quad \text{(Kontradiktion)} \end{aligned} \tag{3.47}$$

oder

$$\begin{aligned} x + 4 = 5 \quad &\wedge \quad x + 1 = 2 \\ x = 1 \quad &\wedge \quad x = 1 \to x_3 = 1 \end{aligned} \tag{3.48}$$

Um nicht alle Fälle durchrechnen zu müssen, überlegen wir, dass $x+4$ und $x+1$ um 3 unterscheiden. Also müssen wir nur noch $8 \cdot 5 = 0$ betrachten.

$$x + 4 = 8 \wedge x + 1 = 5 \tag{3.49}$$

finden wir $x_4 = 4$. Somit ist $L = \{1, 4, 6, 9\}$ die Lösungsmenge. Wir müssen also eine Gleichung mit zwei Unbekannten x, y so lösen, dass x, y ganze Zahlen werden.

Definition 36. *Gleichungen der Form*

$$ax + by = c \tag{3.50}$$

mit $a, b, c, x, y \in \mathbb{Z}$ heissen diophantische Gleichungen. (Diophant von Alexandria, um 250 n. Chr.)

Das Lösen diophantischer Gleichungen ist eng verwandt mit dem Suchen des ggT von a und b. Dann verwenden wir den euklidischen Algorithmus. Suchen wir $ggT(4004, 588)$, so teilen wir so lange, bis der Rest 0 wird.

$$\begin{aligned} 4004 &= 6 \cdot 588 + 476 && (3.51)\\ 588 &= 1 \cdot 476 + 112 && (3.52)\\ 476 &= 4 \cdot 112 + 28 && (3.53)\\ 112 &= 4 \cdot 28 + 0 && (3.54) \end{aligned}$$

Der Letzte von 0 verschiedene Rest ist der ggT. Also ist $ggT(4004, 588) = 28$. Nun können wir auch die diophantische Gleichung

$$4004x + 588y = 28 \tag{3.55}$$

lösen. Denn es ist

$$476 = 4 \cdot 112 + 28 \tag{3.56}$$

also

$$28 = 476 - 4 \cdot 112 \tag{3.57}$$

Weiter ist

$$588 = 1 \cdot 476 + 112 \tag{3.58}$$

also

$$112 = 558 - 1 \cdot 476 \tag{3.59}$$

was zu

$$28 = 476 - 4(588 - 1 \cdot 476) = 5 \cdot 476 - 4 \cdot 588 \tag{3.60}$$

führt. Und schliesslich ist

$$4004 = 6 \cdot 588 + 476 \tag{3.61}$$

also ist

$$476 = 4004 - 6 \cdot 588 \tag{3.62}$$

was eingesetzt zu

$$28 = 5(4004 - 6 \cdot 588) - 4 \cdot 588 = 5 \cdot 4004 - 34 \cdot 588 \tag{3.63}$$

führt. Somit hat die diophantische Gleichung

$$4004x + 588y = 28 \tag{3.64}$$

die Lösung

$$x = 5, y = -34 \tag{3.65}$$

Dieses Verfahren (euklidischer Algorithmus + rückwärts) nennen wir den erweiterten Euklidischen Algorithmus. Damit haben wir gezeigt, dass die diophantische Gleichung

$$ax + by = c \tag{3.66}$$

lösbar ist, wenn $c = ggT(a, b)$. Da jede Gleichung mit $k \neq 0$ multipliziert werden kann, darf c auch ein Vielfaches des ggT sein. Wir wollen ja die Gleichung

$$ax = 1 \quad \text{in} \quad \mathbb{Z}_m \tag{3.67}$$

lösen. Dies führt bekanntlich zu

$$ax + my = 1 \tag{3.68}$$

Nun wissen wir, dass diese Gleichung nur lösbar ist, wenn $ggT(a, m) = 1$. Um

$$7x = 1 \quad \text{in} \quad \mathbb{Z}_{19} \tag{3.69}$$

zu lösen, müssen wir also

$$7x + 19y = 1 \quad \text{in} \quad \mathbb{Z}_{19} \tag{3.70}$$

lösen. Da $ggT(19, 7) = 1$, ist also die diophantische Gleichung lösbar. Mit den erweiterten Algorithmus finden wir

$$19 = 2 \cdot 7 + 5 \tag{3.71}$$
$$7 = 1 \cdot 5 + 2 \tag{3.72}$$
$$5 = 2 \cdot 2 + 1 \tag{3.73}$$

Damit wird

$$1 = 5 - 2 \cdot 2 \tag{3.74}$$

und mit 3.72 ist

$$2 = 7 - 1 \cdot 5 \tag{3.75}$$

was eingesetzt in 3.74 zu

$$1 = 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 \tag{3.76}$$

führt. Mit 3.71 wird

$$5 = 19 - 2 \cdot 7 \tag{3.77}$$

was wir in 3.76 einsetzen:

$$1 = 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 = 3 \cdot 19 - 8 \cdot 7 \tag{3.78}$$

Somit ist $x = -8$ in $\mathbb{Z}_{19}$ und die kleinste positive Zahl ist

$$-8 + 19 = 11 \tag{3.79}$$

also hat $7x = 1$ in $\mathbb{Z}_{19}$ die Lösung $x = 11$.

3.4 Satz von Euler-Fermat

(Pierre du Fermat, 1607 bis 1655, Orleans, Toulouse)
Wir betrachten $a^2, a^3, ..., a^{m-1}$ in $\mathbb{Z}_m$

$\mathbb{Z}_3 \setminus \{0\}$:

a	a^2
1	1
2	1

$\mathbb{Z}_4 \setminus \{0\}$:

a	a^2	a^3
1	1	1
2	0	0
3	1	3

$\mathbb{Z}_5 \setminus \{0,1\}$:

a	a^2	a^3	a^4
2	4	3	1
3	4	2	1
4	1	4	1

$\mathbb{Z}_6 \setminus \{0,1\}$:

a	a^2	a^3	a^4	a^5
2	4	2	4	2
3	3	3	3	3
4	4	4	4	4
5	1	5	1	5

$\mathbb{Z}_7 \setminus \{0,1\}$:

a	a^2	a^3	a^4	a^5	a^6
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Wir sehen, dass $a^{p-1} = 1$, wenn p eine Primzahl ist.

Definition 37. *Satz von Fermat: Ist p eine Primzahl und a kein Vielfaches von p, so ist*

$$a^{p-1} \equiv 1(\mod m) \tag{3.80}$$

Beweis 11. *Vorbereitung: Wir wählen*

$$\mathbb{Z}_5 := \{0, 1, 2, 3, 4\} \tag{3.81}$$

und berechnen

$$a \cdot k(\mod 5) \quad \textit{für} \quad k \in \mathbb{Z}_5 \tag{3.82}$$

Ist $a = 3$, so wird

$a \cdot 0 = 0$
$a \cdot 1 = a = 3$
$a \cdot 2 = 1$
$a \cdot 3 = 4$
$a \cdot 4 = 2$

Also erhalten wir alle $x \in \mathbb{Z}_5$ in neuer Reihenfolge. Allgemein gilt also

$$a \cdot 1, a \cdot 2, a \cdot 3, ..., a \cdot (p-1) \tag{3.83}$$

gibt lauter verschiedene Werte für a aus $\mathbb{Z}_p$. Also ist

$$\begin{aligned} (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot ... \cdot (a(p-1)) &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1) \\ &= (p-1)! \\ a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1) \\ a^{p-1} &= 1 \end{aligned} \tag{3.84}$$

Wie ist es nun in $\mathbb{Z}_m$, wenn m keine Primzahl ist? Dann brauchen wir die Euler-Phi-Funktion: Wir zählen, wie viele Zahlen es gibt, die kleiner als m und zu m teilerfremd sind sind.

Definition 38. *Ist $m \in \mathbb{N}$, so heisst*

$$\phi(m) := |\{a | ggT(a, m) = 1 \wedge a < m\}| \tag{3.85}$$

die Euler-Phi-Funktion von m.