Theorie
Diskrete Mathematik
Bern University of Applied Sciences

Martin Schmidli

30. März 2014

Inhaltsverzeichnis

Kapitel 1

Grundlagen

1.1 Quadratische Ergänzung

Wir nutzen die Quadratische Ergänzung, um eine quadratischen Gleichung in die Binomform umzuformen.

Zuerst bringen wir die Gleichung in die Normalform

$$x^2 + px + q$$

Die quadratische Ergänzung ist definiert durch

$$(\frac{p}{2})^2$$

Kapitel 2

Logik (Boolesche Algebra)

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

2.1 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 ¬a die Negation von a*

Beispiel 1. *a: Xaver isst gerne Kuchen ¬a: Xaver isst nicht gerne Kuchen*

2.2 Konjunktion

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

$$a \wedge b \tag{2.1}$$

Beispiel 2. *Morgen ist Sonntag und ich werde ausschlafen*

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

$$a \wedge \neg a = falsch \tag{2.2}$$

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

$$a \wedge 1 = a \tag{2.3}$$

$$a \wedge 0 = 0 \tag{2.4}$$

Weiter finden wir Gesetze

Kommutativgesetz (Vertauschungsgesetz)

$$a \wedge b = b \wedge a \tag{2.5}$$

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)

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c \tag{2.6}$$

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

$$a \wedge a = a \tag{2.7}$$

2.3 Disjunktion

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

$$a \vee b \tag{2.8}$$

und definieren

a	b	a ∨ b
0	0	0
0	1	1
1	0	1
1	1	1

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

$$a \vee 1 = 1 \tag{2.9}$$

$$a \vee 0 = a \tag{2.10}$$

$$a \vee \neg a = 1 \tag{2.11}$$

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

Es gelten die Gesetze

Kommutativgesetz

$$a \vee b = b \vee a \tag{2.12}$$

Assoziativgesetz

$$a \vee (b \vee c) = (a \vee b) \vee c \tag{2.13}$$

Idempotenzgesetz

$$a \vee a = a \tag{2.14}$$

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

$$a(b + c) = ab + ac \tag{2.15}$$

was in der Logik zu

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \tag{2.16}$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \tag{2.17}$$

dem Distributivgesetz (Verteilungsgesetz) führt. Der folgende Beweis zeigt, dass die Gleichung 2.16 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

$$a \wedge (a \vee b) = a \tag{2.18}$$

$$a \vee (a \wedge b) = a \tag{2.19}$$

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

$$\neg(a \wedge b) = \neg a \vee \neg b \tag{2.20}$$

$$\neg(a \vee b) = \neg a \wedge \neg b \tag{2.21}$$

Wir verwenden die Gesetze, um die Aussagen zu vereinfachen.

Beispiel 3. *Folgende Beispiele zeigen, wie sich Aussagen mittels den oben genannten Gesetzen vereinfachen lassen.*

1. $[a \wedge (b \vee a)] \vee \neg a$
   $= a \vee \neg a$
   $= 1$

2. $[\neg(a \wedge b) \vee \neg b] \wedge a$
   $= (\neg a \vee \neg b \vee \neg b) \wedge a$
   $= (\neg a \vee \neg b) \wedge a$
   $= (\neg a \wedge a) \vee (\neg b \wedge a)$
   $= 0 \vee (\neg b \wedge a)$
   $= \neg b \wedge a$

3. $(a \wedge b) \vee \neg b$
   $= (a \vee \neg b) \wedge (b \vee \neg b)$
   $= (a \vee \neg b) \wedge 1$
   $= (a \vee \neg b)$

4. $b \wedge [(a \wedge b) \vee (\neg a \wedge b)]$
   $= b \wedge [b \wedge (a \vee \neg a)]$
   $= b \wedge (b \wedge 1)$
   $= b \wedge b = b$

2.4 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. Gemäss Ïndischer Beweis":

$$\begin{aligned} c^2 &= 4\frac{ab}{2} + (a-b)^2 \\ c^2 &= 2ab + a^2 - 2ab + b^2 \\ c^2 &= a^2 + b^2 \end{aligned} \tag{2.22}$$

□

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 böder "wenn a so böder äus a folgt b (a impliziert b)"verknüpfen, so schreiben wir dafür

$$a \to b \tag{2.23}$$

und definieren

a	b	a → b
0	0	1
0	1	1
1	0	0
1	1	1

Wir finden sofort, das äus a folgt b"

$$a \to b = \neg a \vee b \tag{2.24}$$

ein etwas anschaulichers Beispiel:

Ich habe einen Sohn	Ich bin Vater	Aussage Wahrheitswert
0	0	1
0	1	1
1	0	0
1	1	1

Beispiel 4. *Vereinfache*

1. $(a \to b) \to b$
$= (\neg a \vee b) \to b = \neg(\neg a \vee b) \vee b$
$= (a \wedge \neg b) \vee b = (a \vee b) \wedge (\neg b \vee b)$
$= (a \vee b) \wedge 1 = (a \vee b)$

2. $b \to (a \to b)$
$= b \to (\neg a \vee b) = \neg b \vee (\neg a \vee b)$
$= \neg b \vee b \vee \neg a = 1 \vee \neg a = 1$

3. $[(a \vee c) \wedge (c \to a)] \vee (a \wedge \neg b) \vee (a \wedge c) \vee [\neg a \wedge (b \to c)]$
$= [(a \vee c) \wedge (\neg c \vee a)] \vee (a \wedge \neg b) \vee (a \wedge c) \vee [\neg a \wedge (\neg b \vee c)]$
$= [(a \vee c) \wedge (\neg c \vee a)] \vee [a \wedge (\neg v \vee c)] \vee [\neg a \wedge (\neg b \vee c)]$
$= [a \vee (c \wedge \neg c)] \vee [(\neg b \vee c) \wedge (a \vee \neg a)]$
$= [a \vee 0] \vee [(\neg b \vee c) \wedge 1]$
$= a \vee (\neg v \vee c) = a \vee \neg b \vee c$
$(= a \vee (b \to c))$

Ein mathematischer Satz besteht aus Voraussetzung a, Behauptung b und Beweis. Der Satz wird als $a \to b$ formuliert.
Der direkte Beweis ist eine Folge von Implikationen

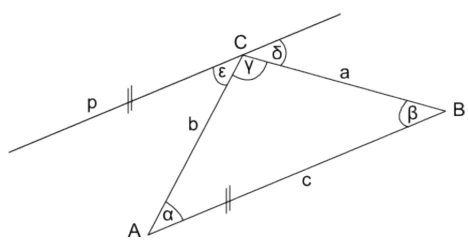
$$a \to x_1 \to x_2 \to x_3 \to ... \to b \tag{2.25}$$

Beispiel 5. *Vereinfache*

1. *Voraussetzung: Ein Dreieck ABC mit Innenwinkel* α, β, γ
Behauptung: Die Innenwinkelsumme ist 180°, *d.h.*

$$\alpha + \beta + \gamma = 180° \tag{2.26}$$

Beweis. Wir beweisen mit einer Zeichnung:



Wähle $p \parallel c$ durch C. Dann ist $\epsilon + \delta + \gamma = 180°$. Es ist $\alpha_1 = \alpha_2$: Stufenwinkel an Parallelen und $\alpha_1 = \alpha_3$: Wechselwinkel an Parallelen, eine weitere Voraussetzung.
Also ist $\alpha = \epsilon$ und $\beta = \delta$ und somit

$$\alpha + \beta + \gamma = 180° \tag{2.27}$$

□

2. *Voraussetzung: Es ist mit* $n \in \mathbb{N}, a \in \mathbb{R}$

$$a^n := a \cdot a \cdot ... \cdot a \text{ (n Faktoren)}$$

die Potenz definiert. Behauptung:

$$a^m \cdot a^n = a^{m+n} \tag{2.28}$$

Beweis. Wir zeigen auf, dass m Faktoren mit n Faktoren multipliziert werden. Durch die grundlegenden Rechengesetze können wir die Klammern wegfallen lassen

$$\begin{gathered} a^m \cdot a^n \\ = (a \cdot a \cdot a \cdot ... \cdot a)(a \cdot a \cdot ... \cdot a) \\ = a \cdot a \cdot a \cdot a \cdot ... \cdot a \text{ (m+n Faktoren)} \\ = a^{m+n} = a^m \cdot a^n \end{gathered} \tag{2.29}$$

□

3. *Voraussetzung:* $x, y \in \mathbb{R}$
   Behauptung:

$$x^y = y^x \to x = y \tag{2.30}$$

Die Behauptung ist falsch. Wollen wir zeigen, dass ein Satz falsch ist, so genügt ein einziges Beispiel, dass wir Gegenbeispiel nennen, um die Behauptung zu widerlegen.
Gegenbeispiel: Für 3 ist das Gegenbeispiel $x = 2, y = 4$*, denn* $2^4 = 4^2 = 16$*, aber* $x \neq y$*.*

2.4.1 Umkehrung, Kontraposition

Definition 4. *Hat eine Aussage die Form*

$$a \to b \tag{2.31}$$

so heisst

$$b \to a \tag{2.32}$$

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

$$\begin{gathered} \neg b \to \neg a = \neg(\neg b) \vee \neg a \\ = b \vee \neg a = \neg a \vee b = a \to b \end{gathered} \tag{2.33}$$

Definition 5. *Wir nennen*

$$\neg b \to \neg a \tag{2.34}$$

die <u>*Kontraposition*</u> *von*

$$a \to b \tag{2.35}$$

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 5. *Der direkte Beweis*

$$\begin{aligned} n^2 &= 2p \wedge p \in \mathbb{N} \\ \to n &= \sqrt{2} \cdot \sqrt{p} \end{aligned} \tag{2.36}$$

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

Also beweisen wir die Kontraposition:

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

Beweis 6.

$$\begin{aligned} n &= 2p + 1 \quad \wedge p \in \mathbb{N}_0 \\ \to n^2 &= (2p+1)^2 \\ n^2 &= 4p^2 + 4p + 1 \\ n^2 &= 2(2p^2 + 2p) + 1 \end{aligned} \tag{2.37}$$

Also ist n^2 *eine ungerade Zahl.* □

2.5 Aequivalenz

Wenn zwei Aussagen gleichwertig (aequivalent) sind, wenn also

$$(a \to b) \wedge (b \to a) \tag{2.38}$$

so schreiben wir dafür

$$a \iff b \tag{2.39}$$

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

$$\begin{aligned} a \iff b &= (a \to b) \wedge (b \to a) \\ &= (\neg a \vee b) \wedge (\neg b \vee a) \\ &= (\neg a \wedge b) \vee (\neg a \wedge a) \vee (b \wedge \neg b) \vee (a \wedge b) \\ &= (a \wedge b) \vee (\neg a \wedge \neg b) \end{aligned} \tag{2.40}$$

Ausserdem ist

$$a \iff b = \neg(a \veebar b) \tag{2.41}$$

also

$$\begin{aligned} a \veebar b &= [(a \wedge b) \vee (\neg a \wedge \neg b)] \\ &= \neg(a \wedge b) \wedge \neg(\neg a \wedge \neg b) \\ &= (\neg a \vee \neg b) \wedge (a \vee b) \end{aligned} \tag{2.42}$$

Beispiel 6. *Vereinfache*

1. $(\neg a \vee \neg b) \wedge (a \vee b)$
   $= a \veebar b$ *nach obriger Herleitung*

2. $(a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c)$
   $= a \wedge [(\neg b \wedge \neg c) \vee (b \wedge c)]$
   $= a \wedge (b \iff c)$

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

"dann und nur dannöder "genau dann"

im Englischen

ïf and only iföder ïff"

Beispiel 7. *Folgende Beispiele zeigen solche Sätze*

1. *Zwei Dreiecke ABC und $A_1B_1C_1$ sind genau dann ähnlich, wenn zwei Winkel gleich sind.*

2. *Sind a, b reelle Zahlen, so ist das Produkt dann und nur dann 0, wenn a oder b Null ist.*

   Voraussetzung: $a, b \in \mathbb{R}$

Satz: $(a \cdot b = 0) \iff (a = 0 \vee b = 0)$

Anwendung:

$$\begin{aligned} a^2 - 7x + 12 &= 0 \quad (x \in \mathbb{R}) \\ (x-3)(x-4) &= 0 \\ \to x - 3 = 0 \quad &\vee \quad x - 4 = 0 \\ x_1 = 3 \quad & \quad x_2 = 4 \end{aligned} \tag{2.43}$$

Wie zeigen wir, dass zwei Terme gleich sind?

Behauptung:

$$\sin 2\alpha = 2 \sin\alpha \cos\alpha \tag{2.44}$$

Wir wählen die linke Seite und formen diese so lange um, bis die rechte Seite entsteht (oder umgekehrt).
Es ist falsch

$$\sin 2\alpha = 2 \sin\alpha \cos\alpha \tag{2.45}$$

so lange umzuformen, bis eine Identität wie z.B. $1 = 1$ entsteht!

Beispiel 8. *Richtig ist*

$$\begin{aligned} \sin 2\alpha &= \sin\alpha + \alpha \\ \textit{denn} \quad \sin\alpha + \beta &= \sin\alpha\cos\beta + \sin\beta\cos\alpha \\ \sin\alpha + \alpha &= \sin\alpha\cos\alpha + \sin\alpha\cos\alpha \\ &= 2\sin\alpha\cos\alpha \end{aligned} \tag{2.46}$$

□

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.

Beispiel 9. *Wir versuchen, dieses Konzept anzuwenden:*

Voraussetzung:

$$\tan\delta = \frac{\sin\delta}{\cos\delta} \quad \textit{und} \quad \cot\delta = \frac{1}{\tan\delta} \tag{2.47}$$

Behauptung:

$$\tan\delta + \cot\delta = \frac{2}{\sin 2\delta} \tag{2.48}$$

Beweis:

1.

$$\tan\delta + \frac{1}{\tan\delta} = \frac{\sin\delta}{\cos\delta} + \frac{\cos\delta}{\sin\delta}$$
$$= \frac{\sin^2\delta + \cos^2\delta}{\sin\delta\cdot\cos\delta} = \frac{1}{\sin\delta\cdot\cos\delta} \tag{2.49}$$

2.

$$\frac{2}{\sin 2\delta} = \frac{2}{2\sin\delta\cdot\cos\delta} = \frac{1}{\sin\delta\cdot\cos\delta} \tag{2.50}$$

□

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

Beispiel 10. *1. Behauptung:*

$$[\neg(a\vee b)\wedge a] \iff [\neg(a\vee b)\wedge b] \tag{2.51}$$

Beweis:

(a)

$$\begin{aligned} \neg(a\vee b)\wedge a &= \neg a\wedge\neg b\wedge a \\ = \neg a\wedge a\wedge\neg b &= 0\wedge\neg b = 0 \end{aligned} \tag{2.52}$$

(b)

$$\begin{aligned} \neg(a\vee b)\wedge b &= \neg a\wedge\neg b\wedge b \\ = \neg a\wedge b\wedge\neg b &= \neg a\wedge b = 0 \end{aligned} \tag{2.53}$$

Beide Terme sind aequivalent □

2. Behauptung:

$$a\rightarrow(b\wedge c) = (a\rightarrow b)\wedge(a\rightarrow c) \tag{2.54}$$

Beweis:

$$\begin{aligned} \neg a\vee(b\wedge c) &= (\neg a\vee b)\wedge(\neg a\vee c) \\ &= (a\rightarrow b)\wedge(a\rightarrow c) \end{aligned} \tag{2.55}$$

2.6 Logische Schlüsse

Wir gehen aus von verschiedenen Prämissen wie

$$\begin{array}{ll} \text{Prämisse 1} & p_1 = a\wedge b \\ \text{Prämisse 2} & p_2 = \neg a \\ \text{Prämisse 3} & p_3 = a\wedge\neg b \end{array} \tag{2.56}$$

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
$$(p_1 \wedge p_2 \wedge ... \wedge p_n) \rightarrow k = 1 \tag{2.57}$$
eine Tautologie sein. Im Beispiel ist also
$$[(a \wedge b) \wedge \neg a \wedge (a \wedge \neg b)] \rightarrow (a \vee b) \tag{2.58}$$
so lange umgeformt werden, bis erkenntlich ist, ob eine Tautologie vorliegt oder nicht.

$$\begin{aligned} & [(a \wedge b) \wedge \neg a \wedge (a \wedge \neg b)] \rightarrow (a \vee b) \\ = \quad & (a \wedge b \wedge \neg a \wedge a \wedge \neg b) \rightarrow (a \vee b) \\ = \quad & 0 \rightarrow (a \vee b) \\ = \quad & \neg 0 \vee (a \vee b) = 1 \vee (a \vee b) = 1 \end{aligned} \tag{2.59}$$

und damit liegt ein logischer Schluss vor.

In der Logik schreiben wir Prämissen und Konklusion untereinander wie zum Beispiel
$$\frac{a \rightarrow b \qquad a \wedge b \rightarrow c \qquad c}{a} \tag{2.60}$$

Beispiel 11. *Handelt es sich hierbei um einen logischen Schluss?*

$$\begin{aligned} & [(a \rightarrow b) \wedge \{(a \wedge b) \rightarrow c\} \wedge c] \rightarrow a \\ = \quad & [(\neg a \vee b) \wedge \{\neg(a \wedge b) \vee c\} \wedge c] \rightarrow a \\ = \quad & \neg[(\neg a \vee b) \wedge (\neg a \vee \neg b \vee c) \wedge c] \vee a \\ = \quad & \neg[(\neg a \vee b) \wedge c] \vee a \\ = \quad & \neg[(\neg a \wedge c) \vee (b \wedge c)] \vee a \\ = \quad & [\neg(\neg a \wedge c) \wedge \neg(b \wedge c)] \vee a \\ = \quad & [(a \vee \neg c) \wedge (\neg b \vee \neg c)] \vee a \\ = \quad & (a \vee \neg c \vee a) \wedge (a \vee \neg b \vee \neg c) \\ = \quad & (\neg c \vee a) \wedge (\neg b \vee \neg c \vee a) \\ = \quad & (\neg c \vee a) \wedge \neg b \end{aligned} \tag{2.61}$$

Also kein logischer Schluss □

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

1. modus ponens (Abtrennungsregel)
$$\frac{a \rightarrow b \qquad a}{b} \tag{2.62}$$

ist ein logischer Schluss, denn

$$\begin{aligned}
& [(a \to b) \wedge a] \to b \\
= \; & [(\neg a \vee b) \wedge a] \to b \\
= \; & (a \wedge b) \to b \\
= \; & \neg(a \wedge b) \vee b \\
= \; & \neg a \vee \neg b \vee b = \neg a \vee 1 = 1
\end{aligned} \tag{2.63}$$

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

Beispiel 12. *Beispielsweise Kosinussatz:*
$a \to b$*: In einem Dreieck ABC gilt* $c^2 = a^2 + b^2 - 2ab \cdot \cos\gamma$
a*:* $a = 10, b = 7, \gamma = 70$
dann tritt b *ein, d.h.* c *kann nun berechnet werden.*

2. modus tollens (Aufhebende Schlussweise)

$$\frac{a \to b \qquad \neg b}{\neg a} \tag{2.64}$$

ist ein logischer Schluss, denn

$$\begin{aligned}
& [(a \to b) \wedge \neg b] \to \neg a \\
= \; & [(\neg a \vee b) \wedge \neg b] \to \neg a \\
= \; & [(b \wedge \neg b) \vee (\neg a \wedge \neg b)] \to \neg a \\
= \; & (\neg a \wedge \neg b) \to \neg a \\
= \; & \neg(\neg a \wedge \neg b) \vee \neg a \\
= \; & a \vee b \vee \neg a = 1 \vee b = 1
\end{aligned} \tag{2.65}$$

3. reductio ad absurdum (zurückführen auf einen Widerspruch)

$$\frac{a \to (b \wedge \neg b)}{\neg a} \tag{2.66}$$

ist ein logischer Schluss, denn

$$\begin{aligned}
& [a \to (b \wedge \neg b)] \to \neg a \\
= \; & [a \to 0] \to \neg a \\
= \; & [\neg a \vee 0] \to \neg a \\
= \; & \neg a \to \neg a = a \vee \neg a = 1
\end{aligned} \tag{2.67}$$

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.

Beispiel 13. *1. Satz: Ës gibt unendlich viele Primzahlen"*
Beweis mit Gegenannahme (Euklid, ca. 300 v.Chr., Alexandria):

Ës gibt nur endlich viele Primzahlen"

$$p_1 < p_2 < p_3 < ... < p_{n-1} < p_n \tag{2.68}$$

wobei p_n die Grösste sei.
Nun bilden wir eine neue Zahl

$$z = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1 \tag{2.69}$$

die sicher keine der Zahlen $p_1, p_2, p_3, ..., p_n$ als Primfaktoren besitzt.
Nun ist z entweder

(a) eine Primzahl, dann ist dies ein Widerspruch

(b) keine Primzahl und damit in Primfaktoren zerlegbar. Es muss also neben $p_1, p_2, ..., p_n$ einen weiteren Primfaktor geben, dies ist ein Widerspruch

zur Gegenannahme.
Also ist die Gegenannahme falsch und damit die ursprüngliche Behauptung wahr. □

2. *Behauptung: $\sqrt{2}$ ist irrational*
Beweis mit Gegenannahme:

$\sqrt{2}$ ist rational

also ist $\sqrt{2} = \frac{p}{q} \wedge p, q \in \mathbb{N}$ und vollständig gekürzt. Somit

$$\begin{aligned} 2 &= \frac{p^2}{q^2} \\ p^2 &= 2q^2 \end{aligned} \tag{2.70}$$

Also ist p^2 eine gerade Zahl und damit auch p (Beweis siehe 2.37). Somit ist $p = 2x \wedge p \in \mathbb{N}$, was eingesetzt in 2.70 zu

$$(2x)^2 = 2q^2 \tag{2.71}$$

führt. Weiter ist

$$\begin{aligned} 4x^2 &= 2q^2 \\ 2x^2 &= q^2 \end{aligned} \tag{2.72}$$

Also ist q^2 gerade und damit auch q. Somit ist

$$q = 2y \wedge y \in \mathbb{N} \tag{2.73}$$

WIr haben also gefunden

$$\sqrt{2} = \frac{p}{q} = \frac{2x}{2y} \tag{2.74}$$

und damit erhalten wir einen Widerspruch zu "vollständig gekürzt". Somit ist die Gegenannahme falsch und damit die Behauptung richtig.

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

Ist

$$\frac{a \wedge \neg b \quad a \rightarrow b}{a \vee b} \tag{2.75}$$

ein logischer Schluss?

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

$$[(a \wedge \neg b) \wedge (a \rightarrow b)] \rightarrow (a \vee b) = 0 \tag{2.76}$$

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

$$x \rightarrow y = 0$$

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:

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

(2.77)

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

Beispiel 14. *1. Ist*

$$\frac{a \wedge \neg d \quad \neg a \vee c \quad (b \wedge \neg c) \rightarrow a}{a \vee c \vee d} \tag{2.78}$$

ein logischer Schluss?

<u>Gegenannahme:</u>

$$\{(a \wedge \neg d) \wedge (\neg a \vee c) \wedge [(b \wedge \neg c) \rightarrow a]\} \rightarrow (b \vee c \vee d) = 0 \tag{2.79}$$

also

	$a \wedge \neg d$	$\neg a \vee c$	$(b \wedge \neg c) \to a$	$\to$	$b \vee c \vee d$
1)	*1*	$\underline{1}$	*1*		*0*
2)					$b = 0, c = 0, d = 0$
3)	$a = 1$				
4)		$\underline{0 \vee 0 = 0}$			

(2.80)

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

2. *Wir untersuchen, ob*

$$\frac{a \to \neg b \quad \neg c \to d \quad c \to a \quad e \to b}{b \to (d \vee c)} \tag{2.81}$$

ein logischer Schluss ist. Gegenannahme:

$$[(a \to \neg b) \wedge (\neg c \to d) \wedge (c \to a) \wedge (e \to b)] \to [b \to (d \vee e)] = 0 \tag{2.82}$$

also

	$a \to \neg b$	$\neg c \to d$	$c \to a$	$e \to b$	$\to$	$b \to (d \vee e)$
1)	*1*	$\underline{1}$	*1*	*1*		*0*
2)						$1 \to 0$, $b = 1$, $d \vee e = 0$, $d = e = 0$
3)	$a = 0$		$c = 0$			
4)		$\underline{1 \to 0 \neq 1}$				

(2.83)

Also liegt ein logischer Schluss vor.

2.7 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.

Beispiel 15. *Prädikatenlogik*

$M = \{x \quad | \quad x \quad \textit{ist ein Hund}\}$
$B(x) : x \; \textit{bellt}$

und es ist $x \in M : \forall x(B(x))$

Wählen wir

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

so können wir formulieren

$$s \in M : \forall s(q(s)) \tag{2.84}$$

was natürlich falsch ist. Korrekt ist

$$\neg \forall s(q(s)) \quad \text{oder auch} \quad \not\forall s(q(s)) \tag{2.85}$$

geschrieben. Dieses "nicht alleïst gleichbedeutend mit

Ës gibt (mindestens) ein(e)"

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

$$\exists s(\neg q(s)) \tag{2.86}$$

Wir haben also

$$\neg \forall x(P(x)) = \exists x(\neg P(x)) \tag{2.87}$$

Betrachten wir

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

und

$$k \in K : \exists k(s(k)) \tag{2.88}$$

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

$$\neg \exists k(s(k)) \quad \text{oder} \quad \nexists k(s(k)) \tag{2.89}$$

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

$$\neg \exists k(s(k)) = \forall k(\neg s(k)) \tag{2.90}$$

Auch in der Mathematik werden die Quantoren verwendet wie zum Beispiel

1.
$$a, b \in \mathbb{R} : \forall a \forall b (ab = ba) \tag{2.91}$$

oder auch
$$a, b \in \mathbb{R} : \forall a, b (ab = ba) \tag{2.92}$$

2.
$$a \in \mathbb{R} \backslash \{0\}, x \in \mathbb{R} : \forall a \exists x (ax = 1) \tag{2.93}$$

Wir nennen $x = a^{-1}$ das zu a inverse Element.

2.7.1 Zwei Prädikate

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

> Älle Informatik-Studierenden besitzen ein iPhone"

wählen wir

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

und schreiben
$$s \in S : \forall s (i(s) \to p(s)) \tag{2.94}$$

ist die Aussage falsch, weil nicht alle Informatik-Studierenden ein iPhone besitzen, so schreiben wir
$$\neg \forall s (i(s) \to p(s)) \tag{2.95}$$

was gleichbedeutend ist mit

$$\exists s (\neg [i(s) \to p(s)]) \tag{2.96}$$

Dies kann mit Hilfe der Gesetze der Logik umgeformt werden zu

$$\begin{aligned} & \exists s (\neg [\neg i(s) \vee p(s)]) \\ = \quad & \exists s (i(s) \wedge \neg p(s)) \end{aligned} \tag{2.97}$$

Wir sehen also, dass der Existenzquantor eine Verbindung der Prädikate mit ünd"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

$$g \in G : \exists g(j(g) \wedge f(g)) \tag{2.98}$$

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

$$\begin{aligned} \neg\exists g(j(g) \wedge f(g)) &= \forall g(\neg[j(g) \wedge f(g)]) \\ &= \forall g(\neg j(g) \vee \neg f(g)) \\ &= \forall g(j(g) \rightarrow [\neg f(g)]) \end{aligned} \tag{2.99}$$

Wir beachten also, dass

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

Bei

> Ës 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

$$m \in M : \exists m(T(m) \wedge K(m)) \tag{2.100}$$

und die Negation

$$\begin{aligned} & \neg\exists m(T(m) \wedge K(m)) \\ = \; & \forall m(\neg(T(m) \wedge K(m))) \\ = \; & \forall m(\neg T(m) \vee \neg K(m)) \\ = \; & \forall m(T(m) \rightarrow \neg K(m)) \quad \text{oder} \quad \forall m(K(m) \rightarrow \neg T(m)) \end{aligned} \tag{2.101}$$

2.7.2 Zweiwertige Prädikate

Sei

$M = \{x \quad | \quad x \quad$ 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

$$\begin{aligned} K(x,y) &\neq K(y,x) \\ L(x,y) &\neq L(y,x) \end{aligned} \tag{2.102}$$

so bedeutet

$$x, y \in M : \forall x \exists y (K(x,y)) \tag{2.103}$$

dass alle Leute die Person y kennen. Und

$$x, y \in M : \exists x \forall y (K(y,x)) \tag{2.104}$$

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

Kapitel 3

Mengen

3.1 Mächtigkeit

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

3.1.1 Aufzählung

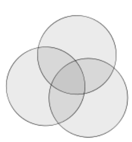
$A = \{-3, a, \diamond, \sqrt{3}, x\}$
$B = \{2, 2, 3, 4, 5\}$ ist nicht möglich: Jedes Element genau einmal, also ist $B = \{2, 3, 4, 5\}$
$C = \{10, 14, 18, 22, ...\}$
$\mathbb{N} = \{1, 2, 3, 4, ...\}$ heisst Menge der natürlichen Zahlen.
$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ heisst Menge der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

3.1.2 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.
$\mathbb{R} = \{x | x \quad$ ist als Dezimalbruch darstellbar ist die Menge der reellen Zahlen.

3.1.3 Euler-Venn-Diagramm

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



algebraische Zahl: Lösung einer (Polynom-) Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 n^1 + a_0 \tag{3.1}$$

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 $|A|$.*

Beispiel 16. *Wir untersuchen die Mächtigkeit der Menge A:*

$A = \{2, 7, 12, ..., 122\}$
$\rightarrow |A| = 24$

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

Definition 7. *Die Mächtigkeit von $\mathbb{N}$ ist $\aleph_0$ (Äleph-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.

Beispiel 17. *Wir versuchen herauszufinden, ob folgende zwei Mengen (A und B gleichmächtig sind:*

$$A = \{4, 7, 10, ..., 94\}$$
$$B = \{6, 10, 14, ..., 82\}$$

Mit einer Funktion f

4	*7*	*10*	*...*	*94*
6	*10*	*14*	*...*	*82*

muss $f(a) = \frac{4}{3}(a-1)+2$ sein. So wird $f(94) = \frac{4}{3}(93)+2 = 4 \cdot 31+2 = 126 \neq 82$ und somit ist $|A| > |B|$.

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

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\} \tag{3.2}$$

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 <u>abzählbar-unendlich</u> viele Elemente.*

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

$$\begin{array}{ccccccccccc}
\frac{1}{1}\ (1) & \rightarrow & \frac{1}{2}\ (2) & & \frac{1}{3}\ (5) & \rightarrow & \frac{1}{4}\ (6) & & \frac{1}{5}\ (11) & \rightarrow & \\
& \swarrow & & \nearrow & & \swarrow & & \nearrow & & & \\
\frac{2}{1}\ (3) & & \frac{2}{2}\ (\cdot) & & \frac{2}{3}\ (7) & & \frac{2}{4}\ (\cdot) & & \frac{2}{5} & & \dots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & & & & \\
\frac{3}{1}\ (4) & & \frac{3}{2}\ (8) & & \frac{3}{3}\ (\cdot) & & \frac{3}{4} & & \frac{3}{5} & & \dots \\
& \swarrow & & \nearrow & & & & & & & \\
\frac{4}{1}\ (9) & & \frac{4}{2}\ (\cdot) & & \frac{4}{3} & & \frac{4}{4} & & \frac{4}{5} & & \dots \\
\downarrow & \nearrow & & & & & & & & & \\
\frac{5}{1}\ (10) & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \frac{5}{5} & & \dots \\
& & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

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 <u>überabzählbar-unendlich</u> und ihre <u>Mächtigkeit ist $\aleph_1$</u>.*

3.2 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)

Beispiel 18. *Folgende Beispiele zeigen den Beweis mittels vollständiger Induktion*

1. *Behauptung:* $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$
   Beweis mit vollständiger Induktion:

   (a) *Behauptung ist für $n = 1$ richtig, denn*

$$\frac{n(n+1)(2n+1)}{6} \quad \textit{wird} \quad \frac{1 \cdot (1+1)(2+1)}{6} = 1 \tag{3.3}$$

   und

$$1^2 = 1 \tag{3.4}$$

   (b) *Voraussetzung:* $s_n = 1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$
   Behauptung: $s_{n+1} = 1^2 + 2^2 + 3^2 + ... + n^2 + (n+1)^2$
   damit

$$\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} = \frac{(n+1)(n+2)(2n+3)}{6} \tag{3.5}$$

   Beweis 7.

$$\begin{aligned} s_{n+1} &= 1^2 + 2^2 + 3^2 + ... + (n+1)^2 \\ &= s_n + (n+1)^2 \\ &= \frac{1}{6} n(n+1)(2n+1) + (n+1)^2 \\ &= \frac{1}{6}(n^2+n)(2n+1) + n^2 + 2n + 1 \\ &= \frac{1}{6}(2n^3 + n^2 + 2n^2 + n) + n^2 + 2n + 1 \\ &= \frac{1}{6}(2n^3 + 3n^2 + n + 6n^2 + 12n + 6) \\ &= \frac{1}{6}(2n^3 + 9n^2 + 13n + 6) \end{aligned} \tag{3.6}$$

und

$$\begin{aligned}\frac{(n+1)(n+2)(2n+3)}{6} &= \frac{1}{6}(n^2+3n+2)(2n+3)\\ &= \frac{1}{6}(2n^3+6n^2+3n^2+4n+9n+6)\\ &= \frac{1}{6}(2n^3+9n^2+13n+6) \qquad (3.7)\end{aligned}$$

(c) *Nach (1a) gilt die Behauptung für $n = 1$ und nach (1b) gilt sie für $n + 1$, falls sie für n gilt.*
Also gilt sie für $n = 2$ und nach (1b) für $n + 1$, ist 3 usw. Also gilt die Behauptung für alle $n \in \mathbb{N}$. □

2. *Wir betrachten die Summe der ungeraden Zahlen bis n:*

$$\begin{aligned}1+3 &= 4\\ 1+3+5 &= 9\\ 1+3+5+7 &= 16\\ 1+3+5+7+...+21 &= 11^2 = 121\\ 1+3+5+...+n & \qquad (3.8)\end{aligned}$$

Wir finden sofort die Formel

$$(\frac{(n-1)}{2}+1)^2 \qquad (3.9)$$

3. *<u>Behauptung</u>: Ist $n \in \mathbb{N}$, so ist $n^3 + 2n$ durch 3 teilbar.*
Da alle Zahlen $n \in \mathbb{N}$ sind, wählen wir den <u>Beweis mit vollständiger Induktion:</u>

(a) *Ist $n = 1$, so ist*

$$n^3 + 2n = 1^3 + 2 \cdot 1 = 3 \qquad (3.10)$$

und

$$3 \mod 3 = 0 \qquad (3.11)$$

(b) *<u>Voraussetzung</u>: $n^3 + 2n$ ist durch 3 teilbar.*
<u>Behauptung</u>: $(n + 1)^3 + 2(n + 1)$ ist durch 3 teilbar.
<u>Beweis</u>:

$$\begin{aligned}(n+1)^3+2(n+1) &= (n+1)[(n+1)^2+2]\\ &= (n+1)(n^2+2n+3)\\ &= (n+1)[n(n+2)+3]\\ &= (n+1)n(n+2)+3(n+1)\\ &= n(n+1)(n+2)+3(n+1) \qquad (3.12)\end{aligned}$$

Da $n \in \mathbb{N}$, sind n, $n+1$, $n+2$ drei aufeinanderfolgende Zahlen, also ist eine davon durch 3 teilbar. Auch $3(n+1)$ ist durch 3 teilbar, also lässt sich $n(n+1)(n+2)$ in der Form

$$3xy + 3(n+1) = 3(xy + (n+1) \quad ; \quad x, y \in \mathbb{N} \tag{3.13}$$

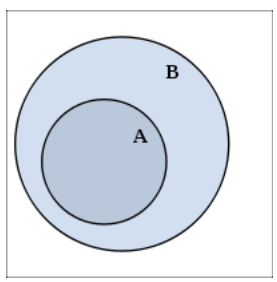
schreiben. Somit ist $(n+1)^3 + 2(n+1)$ durch 3 teilbar.

(c) *Nach (3a) gilt die Behauptung für $n = 1$ und nach (3b) 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

3.3 Teilmengen



Definition 11. *A ist eine Teilmenge von B*

$$A \subset B \iff \forall x (x \in A \to x \in B) \tag{3.14}$$

Beispiel 19. *Wir betrachten die folgenden Mengen:*

$$\begin{aligned} A &= \{a \quad | \quad 10 \leq a \leq 20 \land a \in \mathbb{N}\} \\ B &= \{b \quad | \quad 10 \leq b \leq 50 \land b \in \mathbb{N}\} \end{aligned}$$

also ist $A \subset B$.

$$C = \{9, 10, 11, ..., 31\}$$

also ist $A \subset C$ aber $C \not\subset B$.

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* <u>*Potenzmenge* $\mathcal{P}(A)$</u>

$|\mathcal{P}| = 2^n$

Beispiel 20. *Beispiele zu den Teilmengen:*

1.

$$M = \{a, b\} \rightarrow \mathcal{P}(M))\{\emptyset, \{a\}, \{b\}, \{a, b\}\} \tag{3.15}$$

das heisst

$$\begin{gathered} \{a\} \in \mathcal{P}(M) \ \textit{ist richtig,} \\ \textit{aber } a \in \mathcal{P}(M) \ \textit{ist falsch.} \end{gathered}$$

2. Wir untersuchen, welche Aussagen richtig sind:

$$\begin{array}{cc} \mathbb{N} \subset \mathbb{Q} & \textit{Richtig} \\ \{\mathbb{N}\} \subset \mathbb{Q} & \textit{Falsch} \\ \{\mathbb{N}\} \in \mathbb{Q} & \textit{Falsch} \\ \mathbb{N} \in \mathbb{Q} & \textit{Falsch} \end{array}$$

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 <u>Pascalsche Dreieck</u> (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:

$$
\begin{aligned}
(a+b)^4 &= 1 \quad +4 \quad +6 \quad +4 \quad +1 \\
\text{und weiter} \quad &= 1a^4 \quad +4a^3 \quad +6a^2 \quad +4a^1 \quad +1a^0 \\
&= 1a^4b^0 + 4a^3b^1 + 6a^2b^2 + 4a^1b^3 + 1a^0b^4 \\
&= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4
\end{aligned} \tag{3.16}
$$

Beispiel 21. *Damit können wir auch höhere Binome ausrechnen:*

$$
\begin{aligned}
(2^x - y)^5 &= 1(2x)^5 + 5(2x)^4(-y) + 10(2x)^3(-y)^2 \\
&\quad +10(2x)^2(-y)^3 + 5(2x)^1(-y)^4 + 1(-y)^5
\end{aligned} \tag{3.17}
$$

$$
= 32x^5 - 80x^4y + 80x^3y^2 - 40x^2y^3 + 10xy^4 - y^5 \tag{3.18}
$$

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.*

Beispiel 22.

$$
\binom{4}{2} = 6, \binom{70}{1} = 70, \binom{21}{20} = 21, \binom{10}{0} = 1 = \binom{10}{10} \tag{3.19}
$$

Es ist also

$$
(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{k}a^{n-k}b^k + ... + \binom{n}{k}b^n \tag{3.20}
$$

was wir den binomischen Lehrsatz nennen.

3.3.1 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.

Beispiel 23. *Beispiele mit Intervallen*

1. $$[5;11] = \{x \quad | \quad x \in \mathbb{R} \wedge a \leq x \leq b\} \tag{3.21}$$

2. *Aber:*
$$\{5, 6, 7, 8, 9, 10, 11\} \neq [5;11] \tag{3.22}$$
Achtung: Gilt für reelle Zahlen!

3. *Definitionsmenge von* $f(x) = \log(x-3)$ *ist* $D_f =]3;\infty[$

4. *Ist* $G = \mathbb{R}$, *so ist die Lösungsmenge von*

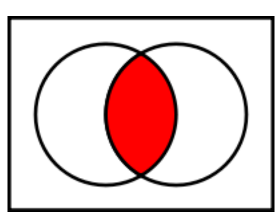
   (a) $x^2 < 49$
   das Intervall $]-7;7[$

   (b) $|x| < 10$
   das Intervall $[-10;10]$

   (c)
$$\begin{aligned} \frac{4}{x^2-1} &> \frac{1}{5} \\ \frac{4}{x^2-1} - \frac{1}{5} &> 0 \\ \frac{20-(x^2-1)}{5(x^2-1)} &> 0 \\ \frac{21-x^2}{5x^2-5} &> 0 \end{aligned} \tag{3.23}$$
   also
$$\begin{aligned} (21-x^2 > 0 \wedge 5x^2-5 > 0) \quad &\vee \quad (21x^2 < 0 \wedge 5x^2-5 < 0) \\ (x^2 < 21 \wedge x^2 > 1) \quad &\vee \quad (x^2 > 21 \wedge x^2 < 1) \end{aligned} \tag{3.24}$$
   und so $L =]-\sqrt{21};-1[\quad \cup \quad]1;\sqrt{21}[$

3.4 Operationen mit Mengen

3.4.1 Schnittmenge



$A \cap B$

Definition 15.

$$A \cap B := \{x \quad | \quad x \in A \wedge x \in B\} \tag{3.25}$$

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

Beispiel 24.

$$\begin{aligned} A &= \{a \quad | \quad -10 \leq a \leq 9 \wedge a \in \mathbb{Z}\} \\ B &= \{b \quad | \quad -2 < b \leq 24 \wedge b \in \mathbb{Z}\} \\ \rightarrow A \cap B &= \{-1, 0, 1, 2, 3, ..., 8\} \end{aligned} \tag{3.26}$$

Wir finden sofort:

$$A \cap \emptyset = \emptyset \tag{3.27}$$

$$A \cap A = A \tag{3.28}$$

$$A \cap B = B \cap A \tag{3.29}$$

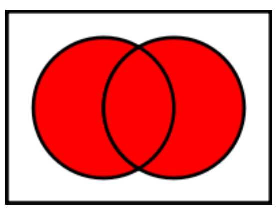
$$(A \cap B) \cap C = A \cap (B \cap C) \tag{3.30}$$

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

Beispiel 25.

$$[4; 10] \cap [100; 150] = \emptyset \tag{3.31}$$

3.4.2 Vereinigungsmenge



$A \cup B$

Definition 17.

$$A \cup B := \{x \quad | \quad x \in A \vee x \in B\} \tag{3.32}$$

heisst *Vereinigungsmenge* *(Verein) von A und B.*

Beispiel 26.

$$\begin{aligned} A &= \{2; 4; 6; ...; 120\} \\ B &= \{1; 3; 5; ...; 119\} \\ \rightarrow A \cup B &= \{1; 2; 3; 4; ...; 120\} \end{aligned} \tag{3.33}$$

Wir finden sofort:

$$A \cup \emptyset = A \tag{3.34}$$

$$A \cup A = A \tag{3.35}$$

$$A \cup B = B \cup A \tag{3.36}$$

$$(A \cup B) \cup C = A \cup (B \cup C) \tag{3.37}$$

und die Distributivgesetze

$$\begin{aligned} \forall A, B, C \quad &: \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ \forall A, B, C \quad &: \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{aligned} \tag{3.38}$$

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

Beweis mit Hilfe der Definitionen

Beweis 8.

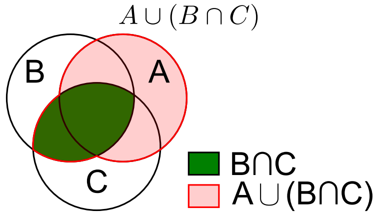
$$\begin{aligned} A \cap (B \cup C) &= \{x \quad | \quad x \in A \wedge x \in (B \cup C)\} \\ &= \{x \quad | \quad x \in A \wedge (x \in B \vee x \in C)\} \\ &= \{x \quad | \quad (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\} \\ &= \{x \quad | \quad x \in A \wedge x \in B\} \cup \{x \quad | \quad x \in A \wedge x \in C\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned} \tag{3.39}$$

□

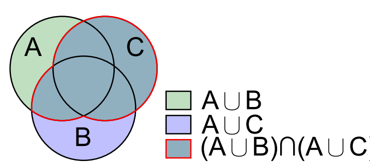
Beweis mit 2 Diagrammen

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

$A \cup (B \cap C)$



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



und die Absorbtionsgesetze

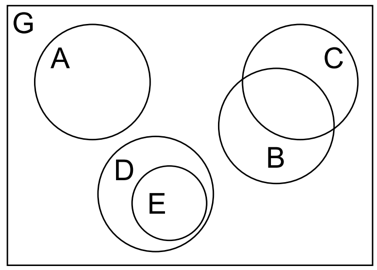
$$\forall a, b : A \cap (B \cup A) = A \tag{3.40}$$

$$\forall a, b : A \cup (B \cap A) = A \tag{3.41}$$

Beweis analog.

3.4.3 Komplement

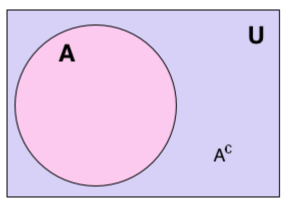
Im Folgenden sind die von uns betrachteten Mengen A, B, C... Teilmengen der Grundmenge G.



Definition 18.

$$\overline{A} := \{x \quad | \quad x \notin A\} \tag{3.42}$$

heisst Komplementärmenge (Komplement) der Menge A



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

Dann sehen wir, dass

$$A \cap \overline{A} = \emptyset \tag{3.43}$$

und

$$A \cup \overline{A} = G \tag{3.44}$$

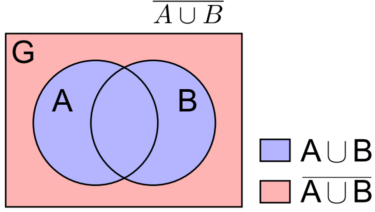
Weiter gelten die Gesetze von De Morgan:

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{3.45}$$

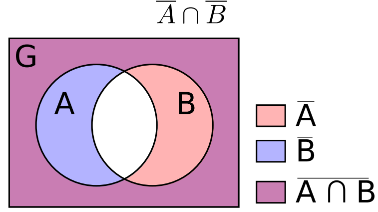
$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{3.46}$$

Beweis 10. *Wir beweisen mit zwei Diagrammen:*

$\overline{A \cup B}$



$\overline{A} \cap \overline{B}$



Beispiel 27. *Vereinfache:*

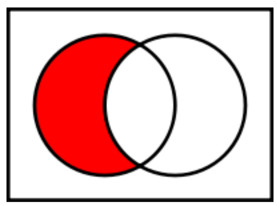
1.

$$(A \cap \overline{\overline{A} \cup B}) \cup B = (A \cap \overline{A} \cap \overline{B}) \cup B \tag{3.47}$$
$$= (\emptyset \cap \overline{B}) \cup B$$
$$= \emptyset \cup B = B$$

2.

$$[\overline{A \cap B} \cup (\overline{A} \cap \overline{B})] \cap \overline{A} = [\overline{A} \cup \overline{B} \cup (\overline{A} \cap \overline{B})] \cap \overline{A} \tag{3.48}$$
$$= (\overline{A} \cup \overline{B}) \cap \overline{A} = \overline{A}$$

3.4.4 Differenz



Definition 19.

$$A \setminus B = \{x \quad | \quad x \in A \wedge x \notin B\} \tag{3.49}$$

heisst Differenz der Mengen A und B.

Beispiel 28. *Ein paar Beispiele zur Differenz:*

1.

$$\begin{aligned} A &= \{a \quad | \quad 11 \leq a < 30 \wedge a \in \mathbb{N}\} \\ B &= \{b \quad | \quad 25 < b \leq 40 \wedge b \in \mathbb{N}\} \\ &\rightarrow \quad A \setminus B = \{11, 12, ..., 25\} \\ &und \quad B \setminus A = \{30, 31, ..., 40\} \end{aligned} \tag{3.50}$$

also

$$A \setminus B \neq B \setminus A \tag{3.51}$$

2. $A \setminus A = \emptyset$

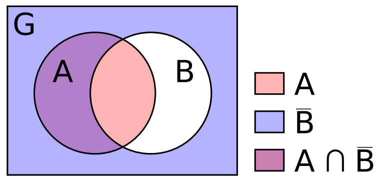
3. $A \setminus \emptyset = A$

4. *A und B disjunkt, dann ist*

$$A \setminus B = A$$
$$B \setminus A = B$$

Wir finden

$$A \setminus B = A \cap \overline{B} \tag{3.52}$$



Beispiel 29. *Mit dieser Vereinfachung können wir nun versuchen, Gesetze zu finden:*

1. *Ist* $\forall A, B, C : A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$*?*
   Nein, denn

   (a)

   $$\begin{aligned} A \cup (B \setminus C) &= A \cup (B \cap \overline{C}) \\ &= (A \cup B) \cap (A \cup \overline{C}) \end{aligned} \tag{3.53}$$

   und

   (b)

   $$\begin{aligned} (A \cup B) \setminus (A \cup C) &= (A \cup B) \cap (\overline{A \cup C}) \\ &= (A \cup B) \cap \overline{A} \cap \overline{C} \end{aligned} \tag{3.54}$$

   In der Algebra ist $a(b-c) = ab - ac$ *und auch* $\frac{a}{b-c} \neq \frac{a}{b} - \frac{a}{c}$*, aber* $\frac{(b-c)}{a} = \frac{b}{a} - \frac{c}{a}$.

2. *Ist also eventuell*

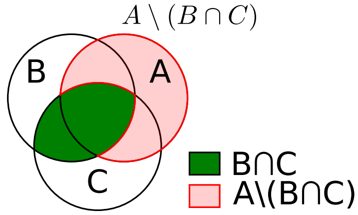
   $$\forall A, B, C : A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C) \tag{3.55}$$

   oder

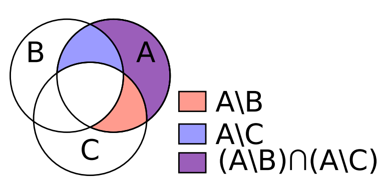
   $$\forall A, B, C : (B \cap C) \setminus A = (B \setminus A) \cap (C \setminus A)? \tag{3.56}$$

   (a) Versuch des Beweises mit zwei Diagrammen:

   $A \setminus (B \cap C)$

   $(A \setminus B) \cap (A \setminus C)$

   also

   $$A \setminus (B \cap C) \neq (A \setminus B) \cap (A \setminus C) \tag{3.57}$$

(b) *Versuchen wir es mit dem zweiten Teil der Vermutung:*

$$(B \cap C) \setminus A = B \cap C \cap \overline{A} \tag{3.58}$$

und

$$\begin{aligned} (B \setminus A) \cap (C \setminus A) &= B \cap \overline{A} \cap C \cap \overline{A} \\ &= B \cap C \cap \overline{A} \cap \overline{A} \\ &= B \cap C \cap \overline{A} \end{aligned} \tag{3.59}$$

Also

$$B \cap (C \setminus A) = (B \setminus A) \cap (C \setminus A) \tag{3.60}$$

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

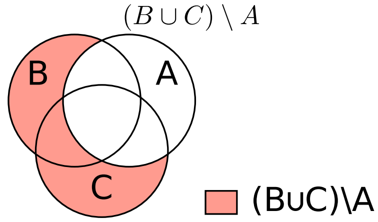
3. *Ist die Differenz rechtsdistributiv bezüglich der Vereinigung?*

   Ist also

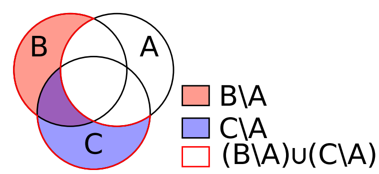
$$\forall A, B, C : (B \cup C) \setminus A = (B \setminus A) \cup (C \setminus A)? \tag{3.61}$$

   Ja, denn

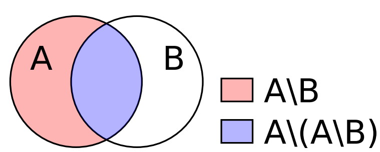
$(B \cup C) \setminus A$



$(B \setminus A) \cup (C \setminus A)$



4. *Vereinfache:* $A \setminus (A \setminus B)$



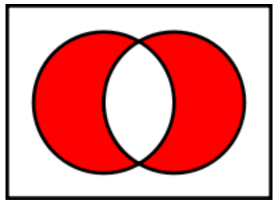
   also

$$A \setminus (A \setminus B) = A \cap B \tag{3.62}$$

5. *Vereinfache:* $A \cup \overline{A \setminus B}$

$$\begin{aligned} A \cup \overline{A \setminus B} &= A \cup \overline{A \cap \overline{B}} \\ &= A \cup \overline{A} \cup \overline{\overline{B}} \\ &= A \cup \overline{A} \cup B \\ &= G \cup B = G \end{aligned} \tag{3.63}$$

3.4.5 Symetrische Differenz



Definition 20.

$$A \Delta B := (A \setminus B) \cup (B \setminus A) \tag{3.64}$$

heisst die <u>*symetrische Differenz*</u> *der Mengen A und B.*

Beispiel 30. *Vereinfache $(A \cup B) \cap (\overline{B} \cup \overline{A})$:*

$$\begin{aligned}
(A \cup B) \cap (\overline{B} \cup \overline{A}) &= (A \cap \overline{A}) \cup (A \cap \overline{B}) \cup (B \cap \overline{A}) \cup (B \cap \overline{B}) \qquad (3.65)\\
&= \emptyset \cup (A \cap \overline{B}) \cup (B \cap \overline{A}) \cup \emptyset \\
&= (A \cap \overline{B}) \cup (B \cap \overline{A}) \\
&= (A \setminus B) \cup (B \setminus A) \\
&= A \Delta B
\end{aligned}$$

3.5 Kartesisches Produkt

Nach René Decartes, 1596 bis 1650, Erfinder des (kartesischen) Koordinatensystems, lebte in Frankreich, Holland und Sweden, sein Axiom war 'Cognito, ergo sum" (Ich zweife (denke) also bin ich).

Definition 21.

$$A \times B := \{(x/y) \quad | \quad x \in A \wedge y \in B\} \tag{3.66}$$

heisst <u>*kartesisches Produkt*</u> *der Mengen A und B.*

Beispiel 31. *Wir bilden das kartesische Produkt zweier Mengen:*
$A = \{4, 7, 8\}$ und $B = 3, 7$

$$A \times B = \{(4/3), (4/7), (7/3), (7/7), (8/3), (8/7)\} \tag{3.67}$$

und

$$B \times A = \{(3/4), (3/7), (3/8), (7/4), (7/7), (7/8)\} \tag{3.68}$$

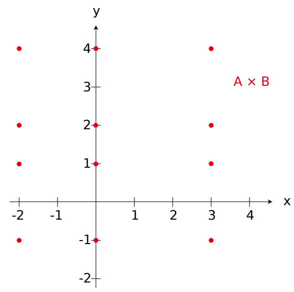
Es ist also

$$A \times B \neq B \times A \tag{3.69}$$

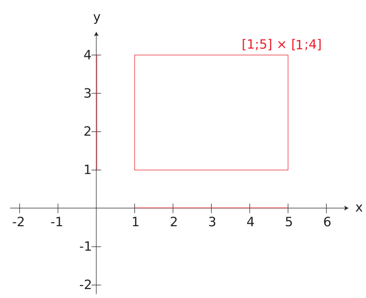
Wir sagen auch, dass $A \times B$ die Menge der geordneten Paare ist. Sind $A, B \in \mathbb{R}$, so können wir $A \times B$ im <u>kartesischen Koordinatensystem</u> darstellen.

Beispiel 32. $A, B \in \mathbb{R}$.

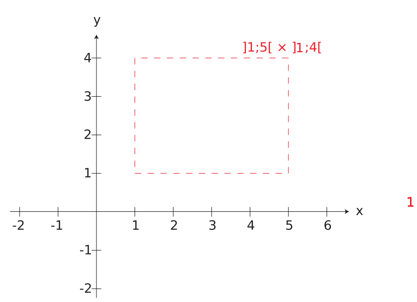
1. $A = \{-2, 0, 3\}$, $B = \{-1, 1, 2, 4\}$



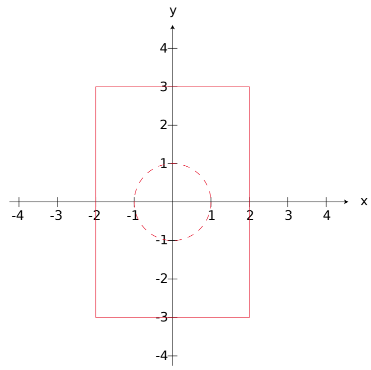
2. $[1; 5] \times [1; 4]$
   $[1; 5]$ *erster Wert (1) X Koordinate von* P_1*, zweiter Wert (5) X Koordinate von* P_2
   $[1; 4]$ *erster Wert (1) Y Koordinate von* P_1*, zweiter Wert (4) Y Koordinate von* P_2



3. $]1; 5[\times]1; 4[$



4. $([-2; 2] \times [-3; 3]) \setminus \{(x/y) \quad | \quad x^2 + y^2 \leq 1 \wedge x, y \in \mathbb{R}\}$
   Es ist $x^2 + y^2 = 1$ *die <u>Gleichung eines Kreises</u> mit Radius 1 und Mittelpunkt im Ursprung.*



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

$$A^n := A \times A \times A \times ... \times A \quad \text{(n Faktoren)} \tag{3.70}$$

Beispiel 33. *Wir zeigen die Potenz an weiteren Beispielen:*

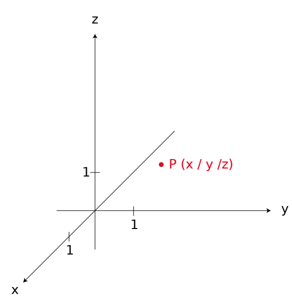
1. $A = \{1, 2, 3\}$

$$\begin{aligned} \to A^3 &= A^2 \times A \quad (3.71) \\ &= \{(1/1), (1/2), ..., (3/2), (3/3)\} \times A \\ &= \{((1/1), 1), ((1/1), 2), ...\} \end{aligned}$$

wofür wir

$$A^3 = \{(1/1/1), (1/1/2), ...\} \tag{3.72}$$

schreiben. Die Elemente von A^3 heissen (Zahlen-)Tripel.

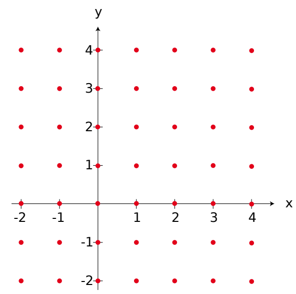


2. $M = \{m_1, m_2, m_3\}$

$$\to M^4 = \{(m_1/m_1/m_1/m_1), (m_1/m_1/m_1/m_2), ..., (m_3/m_3/m_3/m_3)\} \tag{3.73}$$

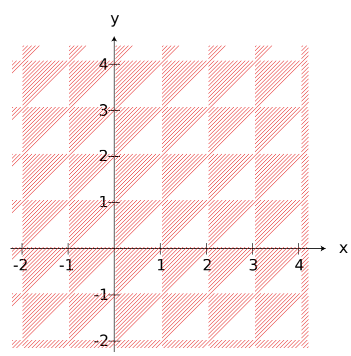
Die Elemente von M^4 heissen Quadrupel. Fahren wir so fort, so erhalten wir Quintupel, Sextupel, ..., n-Tupel ($n \in \mathbb{N}$).

3. *Zeichnen wir $\mathbb{Z}^2$ im Koordinatensystem*



so erhalten wir das ganzzahlige Gitter (Zahlengitter).

4. $R^2 = x/y|x \in R \wedge y \in R$
   ist die Menger aller reelen Zahlenpaare.
   Zeichnen wir $\mathbb{R}^2$,



so erhalten wir den zweidimensionalen Raum.

5. $R^3 = x/y/z|x \in R \wedge y \in R \wedge z \in R$
   Ist der dreidimensionale Raum, die Menge aller reelen Zahlentripel.

   So erhalten wir Quadrupel, Quintupel, Sextupel ... n- Tupel, wenn wir die Elemente von $A^4, B^5, C^6, \ldots, M^n$ *bezeichnen wollen.*

6. *Die Grundmenge eines Gleichungssystems mit zwei Variablen ist* $\mathbb{R}^2$

   (a) $(x/y) \in \mathbb{R}^2$:

   $$\left| \begin{array}{rcl} 2x + y & = & 8 \\ x - 3y & = & 1 \end{array} \right|$$

   Mit dem Gauss-Algorithmus (Additionsmethode) finden wir

$$\left| \begin{array}{rcl} 6x+3y & = & 24 \\ x-3y & = & 1 \end{array} \right|$$

Darauf folgt

$$\begin{aligned} \rightarrow 7x &= 25 \\ x &= \frac{25}{7} \end{aligned} \tag{3.74}$$

Eingesetzt in 6a:

$$\begin{aligned} \frac{25}{7} - 3y &= 1 \\ 25 - 21y &= 7 \\ 18 &= 21y \\ y &= \frac{18}{21} = \frac{6}{7} \end{aligned} \tag{3.75}$$

und so ist $(\frac{25}{7}/\frac{6}{7})$ *die Lösung. Das ist auch* $\in$ *von* $\mathbb{R}^2$*, womit die Lösung in der Grundmenge liegt.*

(b) *Gegeben ist folgendes Gleichungssystem:*

$$\left| \begin{array}{rcl} \frac{3}{x}+\frac{2}{y} & = & 1 \\ \frac{4}{x}-\frac{1}{y} & = & 2 \end{array} \right|$$

Die Grundmenge ist $\mathbb{R}^2$*, so ist die Definitionsmenge* $D = \mathbb{R}^2 \setminus \{(x/y)|x = 0 \vee y = 0\}$. *Mit "(1) + 2(2)ërhalten wir*

$$\begin{aligned} \frac{11}{x} &= 5 \\ x &= \frac{11}{5} \end{aligned} \tag{3.76}$$

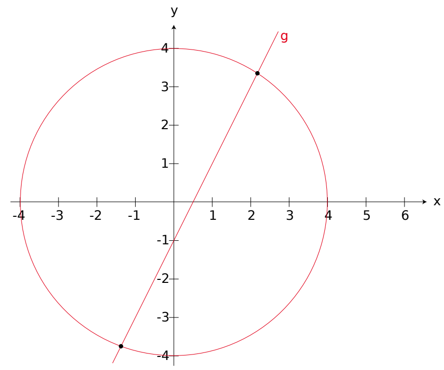
Mit "4(1) - 3(2)"wird

$$\begin{aligned} \frac{11}{y} &= -2 \\ y &= -\frac{11}{2} \end{aligned} \tag{3.77}$$

und so ist $L = \{(\frac{11}{5}/-\frac{11}{2})\}$

(c) *Gegeben ist folgendes Gleichungssystem:*

$$\left| \begin{array}{rcl} x^2+y^2 & = & 16 \\ 2x-y & = & 1 \end{array} \right|$$



Definition 23. *wir nennen*
$x^2 + y^2 = r^2$
Die Koordinatengleichung des Kreises
mit Zentrum im Urpsrung und Radius r.

Weiter ist $2x - y = 1$ die Gleichung einer Geraden meistens explizit als y = 2x-1 geschrieben.
Wir berechnen also die Schnittpunkte einer Geraden mit einem Kreis.

Mit 6c wird $y = 2x - 1$, was eingesetzt in 6c zu

$$x^2 + (2x - 1)^2 = 16 \tag{3.78}$$

führt. Also

$$\begin{aligned} x^2 + 4x^2 - 4x + 1 &= 16 \\ 5x^2 - 4x - 15 &= 0 \\ x_{1,2} &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{4 \pm \sqrt{16 - 4 \cdot 5 \cdot (-15)}}{10} \\ &= \frac{4 \pm \sqrt{316}}{10} = \frac{4 \pm \sqrt{4 \cdot 79}}{10} \\ &= \frac{4 \pm 2\sqrt{79}}{10} = \frac{2 \pm \sqrt{79}}{5} \end{aligned} \tag{3.79}$$

Mit $x_1 = \frac{2+\sqrt{79}}{5}$ wird $y_1 = \frac{4+2\sqrt{79}}{5} - 1$:

$$y_1 = \frac{4 + 2\sqrt{79} - 5}{5} = \frac{2\sqrt{79} - 1}{5} \tag{3.80}$$

und mit $x_2 = \frac{2-\sqrt{79}}{5}$ wird $y_2 = \frac{2-2\sqrt{79}-5}{5} = \frac{-2\sqrt{79}-3}{5}$.
Also sind die Schnittpunkte

$$S_1(\frac{2 + \sqrt{79}}{5} / \frac{2\sqrt{79} - 1}{5}) \tag{3.81}$$

und

$$S_2(\frac{2-\sqrt{79}}{5}/\frac{-2\sqrt{79}-3}{5}) \tag{3.82}$$

7. *Die Menge $M = x/y|x^2 + y^2 \leq 9 \wedge x, y \in R$ ist also*
   BILD
   eine Kreisscheibe
   dh. alle Punkte im Kreis resp. innerhalb des Radius 3.

Kapitel 4

Relationen

4.1 Darstellung von Relationen

Wir betrachten eine Menge von Geschwistern

M = {Alex, Barbara, Claudia}

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

ïst die Schwester von"

und finden

Älex ist die Schwester von Barbaraïst falsch
"Barbara ist die Schwester von Alexïst richtig

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

$$(B, A), (B, C), (C, B), (C, A) \tag{4.1}$$

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 MxM*

Anstelle von $(x/y) \in R$ könne wir auch xRy schreiben

Beispiel 34. $\mathbb{N}$ *mit der Relation "a teil b"
wofür wir*

$$a, b \in \mathbb{N} : aRb \iff a|b \tag{4.2}$$

schreiben. Dann ist

$$R = \{(2, 4), (2, 6), (4, 8), (7, 14), (9, 27), ...\} \tag{4.3}$$

Beachte, dass die Relation als deutscher Satz gleich heisst wie die Menge!

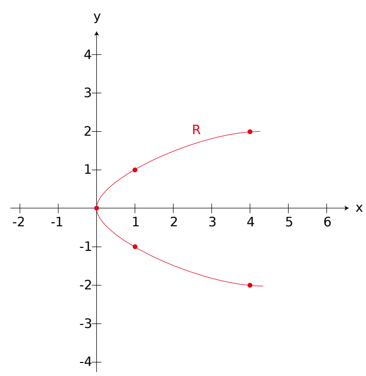
Relationen können wir im kartesischen Koordinatensystem darstellen.

$$\text{Ist} x, y \in \mathbb{R} : xRy \iff x = y^2 \tag{4.4}$$

so finden wir einige Paare:

$$R = \{(0/0), (4/2), (4/-2), (1/1), (1/-1), ...\} \tag{4.5}$$

und damit



Das ist <u>nicht</u> der Graph einer Funktion, da wir für einen x-Wert mehrere y-Werte erhalten.

Beispiel 35. *Wir suchen die Relationen*

1. $M = \{2, 5, 7, 10\}$

$$a, b \in M : aRb \iff b = 2a \tag{4.6}$$

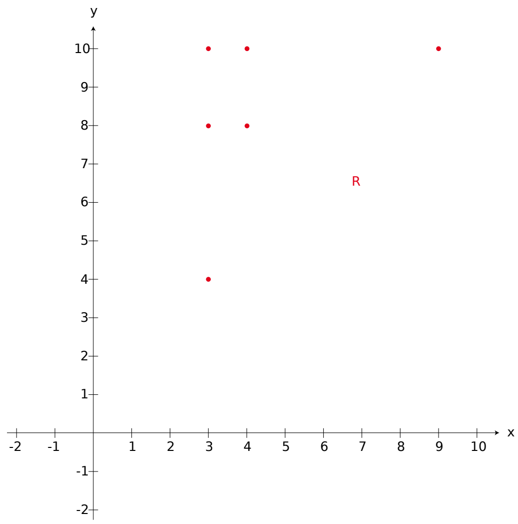
   $\rightarrow R = \{(5/10)\}$

2. $M = \{3, 4, 8, 10\}$

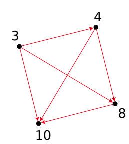
$$a, b \in M : aRb \iff a < b \tag{4.7}$$

   Also $\rightarrow R = \{(3/4), (3/8), (3/10), (4/8), (4/10), (8/10)\}$

Im Koordinatensystem

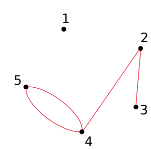


Eine andere Möglichkeit ist die Darstellung mit einem Graphen.



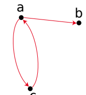
Definition 25. *Ein* <u>*Graph*</u> *ist ein Paar, bestehend aus einer Menge E von* <u>*Eckpunkten*</u> *(Ecken, engl. vertices) und einer Menge K von* <u>*Kanten*</u> *(engl. edges).*

Also zum Beispiel



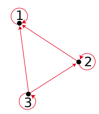
In unserem Beispiel, ist:
$E = \{1, 2, 3, 4, 5\}$
$K = \{(2/3), (2/4), (4/5), (5/4)\}$

Bei einer Relation, ist es wesentlich, ob aRb oder bRa oder beides zutrifft. Dann verwenden wir einen <u>gerichteten Graphen</u>.



In unserem Beispiel, ist:
$aRb \wedge aRc \wedge cRa$

Beispiel 36. *Zeichne den Graphen der Relation, wenn*
$M = \{1, 2, 3\}$
und $a, b \in M : aRb \iff a \geq b$



Wir erhalten die folgenden Relationen:
$R = \{(1/1), (2/1), (2/2), (3/1), (3/2), (3/3)\}$

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

Im Normalfall, wird von der linken Spalte aus begonnen zu lesen.

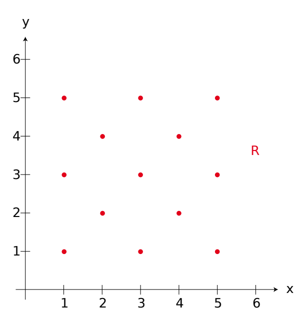
Damit finden wir die Adjazenzmatrix

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \tag{4.8}$$

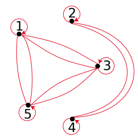
Beispiel 37. *Bestimme einige Elemente der Relation R, wenn*
$M = \{1, 2, 3, 4, 5\}$ *und*

$$a, b \in M : aRb \iff a - b \text{ ist gerade} \tag{4.9}$$

Zeichne dann R im Koordinatensystem, Zeichne den Graphen und suche die Adjazenzmatrix.
$\rightarrow R = \{..., (2/2), ..., (3/1), ..., (5/3), ...\}$ *Koordinatensystem:*



Graph:



Adjazenzmatrix:

	1	*2*	*3*	*4*	*5*
1	*1*	*0*	*1*	*0*	*1*
2	*0*	*1*	*0*	*1*	*0*
3	*1*	*0*	*1*	*0*	*1*
4	*0*	*1*	*0*	*1*	*0*
5	*1*	*0*	*1*	*0*	*1*

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

4.2 Eigenschaften

Wir betrachten die Menge M mit der realtion $R \subset MxM = R \subset M^2$

Definition 26. *Eine Relation heisst reflexiv, wenn*

$$a \in M : \forall a(aRa) \tag{4.10}$$

Beispiel 38.

$$a, b \in R : aRb \iff a \leq b \tag{4.11}$$

ist reflexiv, denn $\forall a(a \leq a)$ *ist eine wahre Aussage.*

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

Definition 27. *Eine Relation heisst symetrisch, wenn*

$$a, b \in M : \forall a, b(aRb \rightarrow bRa) \tag{4.12}$$

Beispiel 39. $G = \{g \quad | \quad g \text{ ist eine Gerade in } R^2\}$

$$a, b \in M : aRb \iff a \perp b \tag{4.13}$$

R ist eine symetrische Relation, denn

$$aRb \rightarrow a \perp b \rightarrow b \perp a \rightarrow bRa \tag{4.14}$$

Definition 28. *Eine Relation heisst antisymetrisch, wenn*

$$a, b \in M : \forall a, b[(aRb) \wedge (bRa) \rightarrow (a = b)] \tag{4.15}$$

Beispiel 40.
1. $a \geq b$ *in* $\mathbb{R}$ *ist antisymetrisch, denn* $(a \geq b \wedge b \geq a) \rightarrow (a = b)$
2. $(A \subset B \wedge B \subset A) \rightarrow (A = B)$

Definition 29. *Eine Relation heisst transitiv, wenn*

$$a, b, c \in M : \forall a, b, c[(aRb \wedge bRc) \rightarrow (aRc)] \tag{4.16}$$

Beispiel 41.

$$a, b, c \in R : aRb \iff a = b \tag{4.17}$$

R ist transiv, denn

$$(aRb \wedge bRc) \rightarrow (a = b \wedge b = c) = (a = c) \rightarrow (aRc) \tag{4.18}$$

Beispiel 42. *Welche Eigenschaften besitzen die Relationen?*

1. $a, b \in R : aRb \rightarrow a \geq b$
   Um mit der Relation arbeiten zu können, brauchen wir eine rechenfähige Definition:
   $a \geq b \iff a - b \in R_0^+$

   reflexiv:
   $\forall a(a \geq a)$, *denn* $a \geq a$ *bedeutet* $a - a = 0$
   und $0 \in R_0^+$, *also ist die Relation reflexiv.*

   symmetrisch:
   Das würde bedeuten, $\forall a, b(a \geq b \wedge b \geq a)$, *was nicht stimmen kann, ist doch bspw.* $2 \geq 5 \neq 5 \geq 2$.

   antisymmetrisch:

$$\begin{aligned} \forall a, b(aRb \wedge bRa) \rightarrow a \geq b \wedge b \geq a \\ a - b \in R_0^+ \wedge b - a \in R_0^+ \\ a - b \in R_0^+ \wedge (-1)(a - b) \in R_0^+ \\ a - b = 0 \\ a = b \end{aligned}$$

   Also ist R antisymmetrisch.

   transitiv:

$$\begin{aligned} \forall a, b, c(aRb \wedge bRc) \\ \rightarrow a \geq b \wedge b \geq c \\ \rightarrow a - b \in R_0^+ \wedge b - c \in R_0^+ \end{aligned}$$

   Die Summe zweier Zahlen ist positiv

$$\begin{aligned} \rightarrow (a - b) + (b - c) \in R_0^+ \\ \rightarrow a - c \in R_0^+ \\ \rightarrow aRc \end{aligned}$$

   R ist transitiv

2. $M = \{a,b,c\}$ *und*
   $R = \{(a/b),(b/a),(a/c),(c/a),(a/a),(c/c)\}$

   reflexiv:
   Ist R refelxiv?

   Nei, denn $(b/b) \notin R$

<u>*symmetrisch:*</u>
Ist R symmetrisch?

Ja, denn $(a/b) \in R$ *ist auch* $(b/a) \in R$
und auch $(a) \in R$ *ist auch* $(c/a) \in R$

<u>*antisymmetrisch:*</u>
Ist R antisymmentrisch?

Kann nicht beantwortet werden.

<u>*transitiv:*</u>
Ist R transitiv?

$$\begin{aligned}
((a/b) \in R \wedge (b/a) \in R) &\to (a/a) \in R \\
((a/c) \in R \wedge (c/a) \in R) &\to (a/a) \in R \\
((a/c) \in R \wedge (c/c) \in R) &\to (a/c) \in R \\
&\textit{aber} \\
((c/b) \in R \wedge (a/b) \in R) &\to (c/b) \notin R
\end{aligned}$$

ist nicht erfüllt.
R ist nicht transitiv.

Definition 30. *Eine Relation heisst* <u>*Ordnungsrelation*</u>*, wenn R reflexiv, antisymetrisch und transitiv ist.*

Beispiel 43. *Im Folgenden Beispiele für Ordnungsrelationen*

1. $a \geq b$ *in* $\mathbb{R}$*, siehe Beispiel 42*

2. *"A befiehlt B' ist eine Ordnungsrelation in einer Firma.*

3. *Lexikographische Ordnung*
   Aarau $\prec$ *Aare*
   $(a/b) \prec (c/d) \leftrightarrow (a < c \vee (a = c \wedge b < d))$

4. *Teilerrelation in N*

$$a, b \in N, m \in N$$
$$a/b \leftrightarrow \exists m(b = ma)$$

5. $a, b \in \mathbb{N} : aRb \iff (a|b)$
   Wir definieren
$$x \in \mathbb{N} : a|b \iff \exists x(b = ax) \tag{4.19}$$

Sagen also, dass b ein Vielfaches von a ist.
reflexiv: $\forall a(a|a)$*, denn* $a = 1 \cdot a$*, also ist* $x = 1$ *in* $\exists x(a = ax)$ *zu wählen.*
antisymmetrisch:

$$\begin{aligned} \forall a, b(a|b \quad &\wedge \quad b|a) \\ \rightarrow \exists x, y(b = ax \quad &\wedge \quad a = by) \end{aligned} \tag{4.20}$$

$$\begin{aligned} \rightarrow a &= (ax) \cdot y \\ a &= (xy) \cdot a \\ \rightarrow xy &= 1 \\ \rightarrow x = 1 \quad &\wedge \quad y = 1 \quad \textit{(weil } \mathbb{N}\textit{)} \\ \rightarrow b &= 1 \cdot a \\ \rightarrow b &= a \end{aligned} \tag{4.21}$$

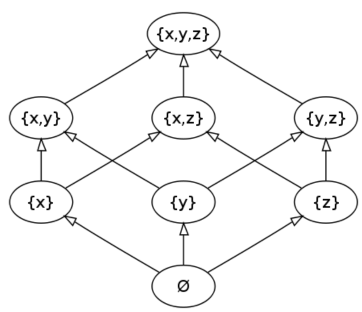
also ist R antisymmetrisch in $\mathbb{N}$*).*
transitiv:

$$\begin{aligned} \forall a, b, c(a|b \quad &\wedge \quad b|c) \\ \rightarrow \exists x, y(b = ax \quad &\wedge \quad c = by) \\ \rightarrow c = (x \cdot y) \cdot a \quad &\wedge \quad xy \in \mathbb{N} \\ \rightarrow a \quad &| \quad c \end{aligned} \tag{4.22}$$

c ist damit ein Vielfaches von a, daraus folgt dass a die Zahl c teilt.

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

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.*

Beispiel 44. *Wir untersuchen, ob es sich um eine Aequivalenzrelation handelt.*

1. $x, y \in \mathbb{R} : xRy \iff x = y$

2. $x, y \in Z : xRy \leftrightarrow x = y$ *ist durch 3 teilbar*
   Wir wählen die Definition:

$$xRy \leftrightarrow (x - y) mod 3 = 0$$

relfexiv

$$\forall x(xRx)$$
$$\rightarrow (x - x) mod 3 = 0 mod 3 = 0$$

Also ist R reflexiv *symmetrisch*

$$\forall x, y(xRy)$$
$$\rightarrow (x - y) mod 3 = 0$$
$$(-1)(x - y)$$
$$(y - x) mod 3 = 0$$
$$\rightarrow yRx$$

Also ist R symmetrisch. *transitiv*

$$\forall x, y, z(xRy \wedge yRz)$$
$$\rightarrow (x - y) mod 3 = 0 \wedge$$
$$(y - z) mod 3 = 0$$
$$\rightarrow [(x - y + (y - z)] mod 3 = 0$$
$$\rightarrow (x - z) mod 3 = 0$$
$$\rightarrow xRz$$

Also ist die Relation transitiv.
R ist eine Aequivalenzrelation und wir können die *Aequivalenzklassen*

todo
BILD

$$K_a = \{x | xRa \wedge x \in M\}$$

des Elementes $a \in M$ *bilden.*

Im Beispiel finden wir also 3 Aequivalenzklassen:

$$\begin{aligned} K_1 &= \{..., -2, 1, 4, 7, ...\} \\ K_2 &= \{..., -1, 2, 5, 8, ...\} \\ K_3 &= \{..., -3, 0, 3, 6, 9, ...\} \end{aligned}$$

Die Klassen sind paarweise disjunkt und bilden eine Partition *der Menge Z.*

todo
Bild

Definition 32. *Wir nennen eine Gruppe vonMengen eine* Partition *der Menge M, wenn*

$$A_1 \cup A_2 \cup A_3 \ldots \cup A_n = M$$
$$A_i \cap A_k = \emptyset (i \neq k)$$

Bei einer Aequivalenzrelation, haben wir die freie Wahl des Repräsentanten *einer Klasse.*
Dies nutzen wir z.Bsp. beim addieren in Q aus. (Bruchrechnen).

Wenn wir

$$\frac{2}{3} + \frac{4}{5} \tag{4.23}$$

rechnen, so rechnen wir

$$\frac{10}{15} + \frac{12}{15} \tag{4.24}$$

wählen also einerseits ein anderes Element in der Klasse $K_{\frac{2}{3}}$ *und andererseits eine anderes Element in der Klasse* $K_{\frac{4}{5}}$

todo
Bild
Relation:

$$\frac{a}{b} R \frac{c}{d} \iff ad = bc \tag{4.25}$$

3. *Auch Vektoren sind Arquivalenzklassen, nähmlich die Klasse der* gleichlangen, gleich- gerichtetetn Pfeile.

   $a, b \in E^3$ *sind Pfeile im dreidimensionalen euklidischen Raum.*

   $$aRb \iff \text{ä und b haben gleiche Länge und gleiche Richtung"}$$

   ist eine Aequivalenzrelation.

4.3 Kongruenz

Wir untersuchen die Operation

$$a \mod m \tag{4.26}$$

für $a \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{1\}$. Dabei heisst m der <u>Modul</u>.

Beispiel 45.

$34 \mod 4 = 4$, *weil* $34 : 5 = 6$ *mit Rest 4*

$77 \mod 11 = 0$

$-13 \mod 4 = 3$, *weil* $-13 = (-4) \cdot 4 + 3$ *ist*

Definition 33. *Wir können also*

$$a \mod m = r \iff \exists x(a = mx + r) \tag{4.27}$$

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

Wir überlegen, ob

$$(a + b) \mod m = a \mod m + b \mod m \tag{4.28}$$

ist.

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

$$(a + b) \mod m = 39 \mod 4 = 3 \tag{4.29}$$

und

$$\begin{aligned} a \mod m &= 21 \mod 4 = 1 \\ b \mod m &= 18 \mod 4 = 2 \end{aligned} \tag{4.30}$$

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

$$\begin{aligned} (a + b) \mod m &= 52 \mod 6 \\ a \mod m &= 35 \mod 6 = 5 \\ b \mod m &= 17 \mod 6 = 5 \end{aligned} \tag{4.31}$$

Es ist also

$$\begin{aligned} (a + b) \mod m &= (a \mod m + b \mod m) \mod m \\ (ab) \mod m &= (a \mod m \cdot b \mod m) \mod m \end{aligned} \tag{4.32}$$

wie wir mit obriger Definition zeigen können.

Beispiel 46. *Wie ist die Uhrzeit in 31h?*

$$31 mod 24 = 7$$

also 7h später als jetzt.

Beispiel 47. *Welcher Wochentag ist in 1000 Tagen?*

$$1000 mod 7 = 6$$

Heute ist Freitag, das heisst in 1000 Tagen ist Donnerstag (+6 Tage).

Beispiel 48. *Welches ist die letzte Ziffer von* 3^{25}*?*

$$\begin{aligned} 3^{25} \mod 10 &= (3^2)^{12} \cdot 3 \mod 10 \\ &= ((3^2)^{12} \mod 10 \cdot 3 \mod 10) \mod 10 \\ &= ((9^{12} \mod 10) \cdot 3 \mod 10) \mod 10 \end{aligned} \tag{4.33}$$

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

$$\begin{aligned} & ((-1)^{12} \mod 10 \cdot 3 \mod 10) \mod 10 \\ = & (1 \mod 10 \cdot 3 \mod 10) \mod 10 \\ = & (1 \cdot 3) \mod 10 = 3 \end{aligned} \tag{4.34}$$

Beispiel 49. *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

$$[\frac{Jahre}{4}] = \text{floor(Jahre / 4)} \tag{4.35}$$

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

4.3.1 Die Kongruenzrelation $a \equiv b \pmod m$

$$a \equiv b(modm) \leftrightarrow (amodm = bmodm)$$

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

ä kongruent b modulo n"

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

$$\exists x(a = mx + r) \land \exists y(b = my + r) \tag{4.36}$$

mit $0 \leq r < m$ gilt.

Weiter ist dann

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

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

$$a, b \in \mathbb{Z}, m \in \mathbb{N} \setminus \{1\} : a \equiv b(\mod m) \iff m|a - b \tag{4.37}$$

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

$$\begin{aligned} 32 &\equiv 17(\mod 5) && (4.38)\\ 44 &\equiv 9(\mod 5) && (4.39)\\ -4 &\equiv 11(\mod 5) && (4.40)\\ -8 &\equiv -13(\mod 5) && (4.41) \end{aligned}$$

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

$$a \equiv a(\mod m) \to m|a-a \to m|0 \tag{4.42}$$

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

$$\begin{aligned} a \equiv b(\mod m) &\to m|a-b \\ &\to m|(-1)(a-b) \to m|b-a \to b \equiv a(\mod m) \end{aligned} \tag{4.43}$$

<u>transitiv</u>, denn

$$\begin{aligned} & a \equiv b(\mod m) \wedge b \equiv c(\mod m) \\ \to\ & m|a-b \wedge m|b-c \\ \to\ & m|(a-b)+(b-c) \\ \to\ & m|a-c \\ \to\ & a \equiv c(\mod m) \end{aligned} \tag{4.44}$$

Somit ist $a \equiv b(\mod m)$ eine Aequivalenzrelation.
Bei $a \equiv b(mod5)$ erhalten wir die folgenden Aequivalenzklassen:

todo
Bild

4.4 Restklassen

Definition 34. *Die durch $a \equiv b(\mod m)$ entstehenden Aequivalenzklassen heissen <u>Restklassen</u>. Also alle die den selben Rest ergeben.*

Ist der Modul $m = 5$, so sind

$$\begin{aligned} \overline{0} &= \{..., -10, -5, 0, 5, 10, ...\} \\ \overline{1} &= \{..., -9, -4, 1, 6, 11, ...\} \\ \overline{2} &= \{..., -8, -3, 2, 7, 12, ...\} \\ \overline{3} &= \{..., -7, -2, 3, 8, 13, ...\} \\ \overline{4} &= \{..., -6, -1, 4, 9, 14, ...\} \end{aligned} \tag{4.45}$$

die Restklassen. Ausgesprochen 0 quer, 1 quer...

Definition 35. *Wir nennen*

$$\mathbb{Z}_5 := \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} \tag{4.46}$$

ein vollständiges Restsystem.

Nun rechnen wir mit diesen Restklassen und überlegen dass

$$\overline{4} + \overline{3} \tag{4.47}$$

bedeutet, dass $a \in \overline{4}$, $b \in \overline{3}$ beliebig gewählt werden darf und diejenige Klasse gesucht ist, die $a + b$ enthält.

Beispiel 50. $\overline{4} + \overline{3} = 7 \mod 5 = \overline{2}$

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)

Nun untersuchen wir, welche Gesetze in einer algebraischen Struktur erfüllt sind.

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

Assoziativgesetz:
(A) $\forall a, b, c \in Z_5(a + (b + c) = (a + b) + c))$
Beweis: a,b,c sind Restklassen und damit Mengen von ganzen Zahlen. Da für die Addition in Z das Assoziativgesetz gilt, muss es auch für Z_5 gelten.

Neutrales Element:
Es gibt eine Zahl n, so dass $\forall a \in Z_5(a + n = n + a = 0)$
ist. Diese Zahl nennen wir das neutrale Element.
In Z_5 ist n = 0, da a+0 = 0+a = 0

Inverses Element:
Zu jedem $a \in Z_5$ existiert ein $\overline{a} \in Z_5$, so dass $a + \overline{a} = \overline{a} + a = n$ (neutrales Element) ist. Die Zahl $\overline{a}$ heisst das $a(additiv-)\underline{inverseElement}$
1 und 4, denn 1+4 = 0 (inZ_5)

Also gelten für die Addition in Z_5 die gleichen Gesetze wie für die Addition in Z.

$x + 3inZ$
so addieren wir -3 auf beiden Seiten
$x + 3 - 3 = 1 - 3$
$x = -2$
da -3 zu 3 invers ist.

Beispiel 51.

$$\begin{aligned} x^2 + 3x + 2 &= 0 \\ (x+2)(x+1) = 0 & \\ x+2=0 &\vee \quad x+1=0 \\ x_1 = 3 & \qquad x_2 = 4 \end{aligned} \tag{4.48}$$

Definition 36. *Ist in einer Menge M eine Operation * so definiert, dass*

$$\forall a, b : a * b \in M \tag{4.49}$$

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

Beispiel 52. *Wir untersuchen:*

1. *$< \mathbb{N}; + >$ ist eine algebraische Struktur*
2. *$< \mathbb{R}; \cdot >$ ist eine algebraische Struktur*
3. *$< \mathbb{Z}; / >$ ist keine algebraische Struktur*
4. *$< V^3; + >$ ist eine algebraische Struktur*
5. *$< V^3; \cdot >$ ist keine algebraische Struktur,*
   denn $\vec{a} \cdot \vec{b}$ ist ein Skalar (eine reelle Zahl).
6. *$< \mathbb{Z}_5; + >$ ist 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

$$a \in \mathbb{Z}_5 : \forall a(a + 0 = 0 + a = a) \tag{4.50}$$

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 37. *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).*

Beispiel 53. *Wir untersuchen, ob folgende algebraische Strukturen abelsche Gruppen sind*

1. *$< \mathbb{Z}; \cdot >$ ist keine abelsche Gruppe*

2. *$< \mathbb{Z} \setminus \{0\}; \cdot >$ ist eine abelsche Gruppe*

3. *$< \mathbb{Q}; \cdot >$ ist keine abelsche Gruppe, da zu 0 kein inverses Element existiert*

4. *$< \mathbb{R}; + >$ ist eine abelsche Gruppe*

Nun betrachten wir $< \mathbb{Z};\ \{0\}, * >$

$*$	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)

Es ist (A) Assoziative und (K) Kommutativ erfüllt und 1 ist neutral.
Zu 1 ist 1 invers, denn 1*1 = 1
Zu 2 ist 3 invers, denn 2*3 = 1
Zu 3 ist 2 invers, denn 3*2 = 1
Zu 4 ist 1 invers, denn 4*4 = 1
Also ist $< \mathbb{Z};\ \{0\}, * >$ eine abelsche Gruppe.

Nun können wir Z_5 rechnen und Gleichungen lösen.

Beispiel 54. *1.*

$$\begin{aligned}
(3x+2) &= 4 + x \wedge inZ_5 \\
3x+1 &= 4+x \\
2x+1 &= 4| + 4^* \\
2x &= 3| * 3^{**} \\
3(2x) &= 3*3 \\
x &= 9 = 4
\end{aligned}$$

*) *da 4 zu 1 additiv invers ist*
**) *da 3 zu 2 additiv invers ist*

2.

$$\begin{aligned}
x^2+3x+2 &= 0 \wedge Z_5 \\
(x+1)(x+3) &= 0 \\
x+1 \vee x+2 &= 0 \\
x_1 = 4 & \qquad x_2 = 3
\end{aligned}$$

3.

$$x^2+2x+2 = 0 \wedge Z_5$$

In R

$$\begin{aligned}
x^2+2x+2 &= 0 \\
x^2+2x &= -2 \\
\textit{quadratisch ergänzen} & \\
x^2+2x+1 &= -2+1 \\
x^2+2+1 &= -1 \\
(x+1)^2 &= -1 \\
x \in R & \\
\to L = \{\} &
\end{aligned}$$

In Z_5

$$\begin{aligned} x^2+2x+2 &= 0|-2 \\ x^2+2x &= 3 \\ x^2+2x+1 &= 4 \\ (x+1)^2 &= 4 \\ x+1 &= 2 \vee x+1=3 \\ x_1=1 & \quad x_2=2 \end{aligned}$$

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

$$a \cdot b = 0 \to (a = 0 \vee b = 0) \tag{4.51}$$

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

$$ab = 0 \to (a = 2 \wedge b = 4) \tag{4.52}$$

$$ab = 0 \to (a = 4 \wedge b = 6) \tag{4.53}$$

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

$$\begin{aligned} 2(x+5) &= 6x+2 \\ 2x+2 &= 6x+2 \\ 2x &= 6x \\ 4x &= 0 && (4.54) \\ \to x &= 0 && (4.55) \end{aligned}$$

So müssen wir die Nullteiler berücksichtigen und finden zusätzliche Lösungen

$$x_2 = 2, x_3 = 4, x_4 = 6$$
$$L = \{0, 2, 4, 6\}$$

$$
\begin{aligned}
x(x+3) &= 0 \\
\text{mit} & \\
x = 0 \vee x+3 = 0 \rightarrow x_1 = 0, x_2 = 5 & \\
\text{oder } x = 4 \wedge x+3 &= 4 \rightarrow x \notin Z_8 \\
\text{oder } x = 2 \wedge x+3 &= 4 \rightarrow x \notin Z_8 \\
\text{oder } x = 4 \wedge x+3 &= 2 \rightarrow x \notin Z_8 \\
\text{oder } x = 4 \wedge x+3 &= 6 \rightarrow x \notin Z_8 \\
\text{oder } x = 6 \wedge x+3 &= 4 \rightarrow x \notin Z_8 \\
\text{daher ist die Lösungsmenge} & \\
L = \{0, 5\} &
\end{aligned}
$$

Wir überprüfen alle Konstellationen bei denen das Endergebnis 0 sein kann. Zuerst schauen wir uns die Gleichung an und sehen, wenn x= 0 oder x= 5 das Ergebnis 0 ergibt. (5+3 = 8 = 0).
Anschliessend setzen wir für x die Nullteiler ein, möglicherweise ergibt sich so eine weitere Lösung. In diesem fall nicht.

Beispiel 55. *Wir lösen*

1.

$$x^2 + 2x + 5 = 0 \quad in \quad \mathbb{Z}_8 \tag{4.56}$$

Wählen wir andere Repräsentanten (5 -8 = -3)

$$
\begin{aligned}
x^2 + 2x - 3 &= 0 \\
(x+3)(x-1) &= 0
\end{aligned} \tag{4.57}
$$

So müssen wir alle Fälle

$$
\begin{aligned}
x+3 = 0 &\quad \wedge \quad x-1 = 0 \\
x+3 = 2 &\quad \wedge \quad x-1 = 4 \\
x+3 = 4 &\quad \wedge \quad x-1 = 2 \\
x+3 = 4 &\quad \wedge \quad x-1 = 4
\end{aligned} \tag{4.58}
$$

etc. untersuchen. Wir formen deshalb so um, dass ein <u>*Binom*</u> *entsteht. In* $\mathbb{R}$*:*

$$
\begin{aligned}
x^2 + 6x - 2 &= 0 \\
x^2 + 6x &= 2 \\
x^2 + 6x + 9 &= 2 + 9
\end{aligned} \tag{4.59}
$$

Wir nennen "+9"die <u>*quadratische Ergänzung*</u>*. So erhalten wir*

$$
\begin{aligned}
(x+3)^2 &= 11 \\
x+3 &= \pm\sqrt{11} \\
x_1 &= \sqrt{11} - 3 \\
x_2 &= -\sqrt{11} - 3
\end{aligned} \tag{4.60}
$$

In $\mathbb{Z}_8$:

$$\begin{aligned} x^2+2x+5 &= 0 \\ x^2+2x &= 3 \\ x^2+2x+1 &= 3+1 \\ (x+1)^2 &= 4 \\ x+1=2 \quad &\vee \quad x+1=6 \\ x_1 = 1 \quad & \quad\; x_2 = 5 \end{aligned} \tag{4.61}$$

2.

$$\begin{aligned} x^2+6x+7 &= 0 \quad in \quad \mathbb{Z}_8 \\ x^2+6x+9 &= 1 \\ (x+3)^2 &= 2 \to L = \emptyset \end{aligned} \tag{4.62}$$

Wollen wir

$$x^2+5x+4=0 \quad \text{in} \quad \mathbb{Z}_{10} \tag{4.63}$$

lösen, so finden wir keine quadratische Ergänzung zu

$$x^2+5x \tag{4.64}$$

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

$$(x+4)(x+1)=0 \tag{4.65}$$

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

$$2\cdot 5 = 4\cdot 5 = 6\cdot 5 = 8\cdot 5 = 0 \tag{4.66}$$

Zuerst aber

$$\begin{aligned} x+4=0 \quad &\vee \quad x+1=0 \\ x_1=6 \quad & \quad\; x_2=9 \end{aligned} \tag{4.67}$$

und dann

$$\begin{aligned} x+4=2 \quad &\wedge \quad x+1=5 \\ x=8 \quad &\wedge \quad x=4 \quad \text{(Kontradiktion)} \end{aligned} \tag{4.68}$$

oder

$$\begin{aligned} x+4=5 \quad &\wedge \quad x+1=2 \\ x=1 \quad &\wedge \quad x=1 \to x_3=1 \end{aligned} \tag{4.69}$$

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.

$$x+4=8 \wedge x+1=5 \tag{4.70}$$

finden wir $x_4=4$. Somit ist $L=\{1,4,6,9\}$ die Lösungsmenge.

Beispiel 56.

$$x^2 + 9x + 2 = 0 \quad in \quad \mathbb{Z}_{12} \tag{4.71}$$

Wahl eines anderen Repräsentanten:

$$\begin{aligned} x^2 + 9x + 14 &= 0 \\ (x+7)(x+2) &= 0 \\ x+7=0 &\vee \quad x+2=0 \\ x_1 = 5 & \qquad x_2 = 10 \end{aligned} \tag{4.72}$$

Dann fragen wir uns, was sind die Nullteiler? In $\mathbb{Z}_{12}$

ist $2 \cdot 6 = 4 \cdot 6 = 6 \cdot 6 = 8 \cdot 6 = 10 \cdot 6 = 0$
und $3 \cdot 4 = 6 \cdot 4 = 9 \cdot 4 = 0$
und $3 \cdot 8 = 9 \cdot 8 = 0$

Die Differenz der Lösungen muss 5 sein, also kommt nur

$9 \cdot 4 = 3 \cdot 8 = 0$

in Frage. Mit

$x + 7 = 9 \wedge x + 2 = 4$

wird $x_3 = 2$ *und wenn*

$x + 7 = 8 \wedge x + 2 = 3$

wird $x_4 = 1$*. Also ist* $L = \{1, 2, 5, 10\}$.

4.5 Inverse Restklassen

Die Gleichung

$$ax = 1 \quad in \quad \mathbb{Z}_m \tag{4.73}$$

lässt sich auch als

$$ax \equiv (\mod m) \tag{4.74}$$

schreiben. Also haben ax *und* 1 *bei der Division durch* m *den gleichen Rest* r*. Somit*

$$\exists v, w \in \mathbb{Z}(ax \equiv vm + r \wedge 1 = wm + r) \tag{4.75}$$

also

$$\begin{aligned} ax - 1 &= vm + r - (wm + r) \\ ax - 1 &= vm - wm \\ ax - 1 &= (v - w)m \end{aligned} \tag{4.76}$$

Schreiben wir y *für* $v - w$*, so ist also*

$$\begin{aligned} ax - 1 &= ym \\ ax - ym &= 1 \end{aligned} \tag{4.77}$$

Wir müssen also <u>eine</u> Gleichung mit <u>zwei Unbekannten</u> x, y so lösen, dass x, y ganze Zahlen werden.

Definition 38. *Gleichungen der Form*

$$ax + by = c \tag{4.78}$$

mit $a, b, c, x, y \in \mathbb{Z}$ heissen <u>diophantische Gleichungen</u>. (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 <u>euklidischen Algorithmus</u>. Suchen wir $ggT(4004, 588)$, so teilen wir so lange, bis der Rest 0 wird.

$$\begin{aligned} 4004 &= 6 \cdot 588 + 476 && (4.79)\\ 588 &= 1 \cdot 476 + 112 && (4.80)\\ 476 &= 4 \cdot 112 + 28 && (4.81)\\ 112 &= 4 \cdot 28 + 0 && (4.82) \end{aligned}$$

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

$$4004x + 588y = 28 \tag{4.83}$$

lösen. Denn es ist

$$476 = 4 \cdot 112 + 28 \tag{4.84}$$

also

$$28 = 476 - 4 \cdot 112 \tag{4.85}$$

Weiter ist

$$588 = 1 \cdot 476 + 112 \tag{4.86}$$

also

$$112 = 558 - 1 \cdot 476 \tag{4.87}$$

was zu

$$28 = 476 - 4(588 - 1 \cdot 476) = 5 \cdot 476 - 4 \cdot 588 \tag{4.88}$$

führt. Und schliesslich ist

$$4004 = 6 \cdot 588 + 476 \tag{4.89}$$

also ist

$$476 = 4004 - 6 \cdot 588 \tag{4.90}$$

was eingesetzt zu

$$28 = 5(4004 - 6 \cdot 588) - 4 \cdot 588 = 5 \cdot 4004 - 34 \cdot 588 \tag{4.91}$$

führt. Somit hat die diophantische Gleichung

$$4004x + 588y = 28 \tag{4.92}$$

die Lösung

$$x = 5, y = -34 \tag{4.93}$$

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

$$ax + by = c \tag{4.94}$$

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.

Beispiel 57. *Wir untersuchen, ob folgende Gleichungen lösbar sind:*

1. $5x + 9y = 12$ *ist lösbar, denn* $ggT(5,9) = 1$ *und 12 ist ein Vielfaches von* 1.
2. $15x + 10y = 12$ *ist nicht lösbar, denn* $ggT(12,10) = 5$ *und* 12 *ist kein Vielfaches von* 5.

Wir wollen ja die Gleichung

$$ax = 1 \quad \text{in} \quad \mathbb{Z}_m \tag{4.95}$$

lösen. Dies führt bekanntlich zu

$$ax + my = 1 \tag{4.96}$$

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

$$7x = 1 \quad \text{in} \quad \mathbb{Z}_{19} \tag{4.97}$$

zu lösen, müssen wir also

$$7x + 19y = 1 \quad \text{in} \quad \mathbb{Z}_{19} \tag{4.98}$$

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

$$\begin{aligned} 19 &= 2 \cdot 7 + 5 && (4.99) \\ 7 &= 1 \cdot 5 + 2 && (4.100) \\ 5 &= 2 \cdot 2 + 1 && (4.101) \end{aligned}$$

Damit wird

$$1 = 5 - 2 \cdot 2 \tag{4.102}$$

und mit 4.100 ist

$$2 = 7 - 1 \cdot 5 \tag{4.103}$$

was eingesetzt in 4.102 zu

$$1 = 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 \tag{4.104}$$

führt. Mit 4.99 wird

$$5 = 19 - 2 \cdot 7 \tag{4.105}$$

was wir in 4.104 einsetzen:

$$1 = 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 = 3 \cdot 19 - 8 \cdot 7 \tag{4.106}$$

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

$$-8 + 19 = 11 \tag{4.107}$$

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

4.6 Satz von Euler-Fermat

4.6.1 Satz von 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 39. *Satz von Fermat: Ist p eine Primzahl und der $ggT(a,p) = 1$, so ist*

$$a^{p-1} \equiv 1(\mod p) \tag{4.108}$$

$$x^n + y^n = z^n \wedge x, y, z \in N \wedge n > 2$$

Ergibt keine mögliche Lösung. Bewiesen 1994 von Andrew Wiles. Auch grosser Fermat genannt.

Beweis 11. *Vorbereitung: Wir wählen*

$$\mathbb{Z}_5 := \{0, 1, 2, 3, 4\} \tag{4.109}$$

und berechnen

$$a \cdot k(\mod 5) \quad \textit{für} \quad k \in \mathbb{Z}_5 \tag{4.110}$$

$$a * 1, a * 2, a * 3, a * 4 in Z_5 \tag{4.111}$$

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*

$$a \cdot 1, a \cdot 2, a \cdot 3, ..., a \cdot (p-1) \tag{4.112}$$

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

$$\begin{aligned} (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot ... \cdot (a(p-1)) &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1) \\ &= (p-1)! \\ a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1) \\ a^{p-1} &= 1 \qquad (4.113) \end{aligned}$$

Beispiel 58. *Wir nutzen diese Eigenschaft aus:*

1. $23^{109} (\mod 37)$
   Es ist $a^{36} = 1(\mod 37)$ *nach dem Satz von Fermat*
   Nun ist $109 = 3 * 36 + 1$*, also*

$$\begin{aligned} 23^{109} \mod 37 &= 23^{3*36+1} \mod 37 \\ &= 23^{3*36} * 23 \mod 37 \\ &= (23^{36})^3 * 23 \mod 37 \\ &= (23^{36} \mod 37)^3 * 23 mod 27 \\ &= 1^3 * 23 \mod 37 \\ &= 23 \end{aligned}$$

2. $9x = 1 \quad in \quad \mathbb{Z}_{11}$
   Mit dem Satz von Fermat ist $a^{10} \equiv 1(\mod 11)$*. Also multiplizieren wir mit* 9^9

$$9^9(9x) \equiv 9^9(\mod 11) \tag{4.114}$$
$$9^{10}x \equiv 9^9(\mod 11) \tag{4.115}$$
$$x \equiv 9^9(\mod 11) \tag{4.116}$$

und $9^9 \mod 11$

$$\begin{aligned} &\equiv (9^2)^4 * 9 \mod 11 \\ &\equiv (81^4) * 9 \mod 11 \\ &\equiv (81 \mod 11)^4 * (9 \mod 11) \\ &\equiv (4)^4 * (9 \mod 11) \\ &\equiv 4^2 * 4^2 * 9 \mod 11 \\ &\equiv (16 \mod 11) * (16 \mod 11) * (9 \mod 11) \\ &\equiv (25 \mod 11) * 9 \mod 11 \\ &\equiv 3 * 9 \mod 11 = 27 \mod 11 \\ &\equiv 5 \end{aligned}$$

Also ist $9x = 1$ *in* $Z_{11} \rightarrow x = 5$

Betrachten wir nun Potenzen in Z_m (m ist keine Primzahl)

$Z_4\{0\}$

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

$Z_8\{0\}$

a	a^2	a^3	a^4	a^5	a^6	a^7
2	4	0	0	0	0	0
3	3	1	3	1	3	1
4	0	0	0	0	0	0
5	1	5	1	5	1	5
6	4	0	0	0	0	0
7	1	7	1	7	1	7

2,4,6 sind die Nullteiler

Wann ist $a^x = 1$?
Die Antwort hat Euler gefunden.

Definition 40. *Ist $m \in \mathbb{N}$, so heisst*

$$\phi(m) := |\{a|ggT(a,m) = 1 \land 1 \leq a < m\}| \tag{4.117}$$

die Euler-Phi-Funktion von m.

Wir suchen also die Anzahl der zu m teilerfremden Zahlen (1 eingeschlossen)

Beispiel 59.

$$\phi(6) = |\{1,5\}| = 2$$
$$\phi(8) = |\{1,3,5,7\}| = 4$$
$$\phi(10) = |\{1,3,7,9\}| = 4$$

Ist p prim, so ist $\phi(p) = p - 1$

4.6.2 Satz von Euler Fermat

$$a^{\phi(m)} \equiv 1(\mod m) \land ggT(a,m) = 1 \land a, m \in N$$

Suchen wir die inverse Restklasse

$$ax \equiv 1(\mod m)$$

So können wir neu das Problem auch mit dem Satz von Euler-Fermat lösen.
Sind a und m teilerfremd, so ist:

$$a^{\phi(m)} * x = 1 * x = x$$

also wird aus

$$\begin{aligned}
ax &\equiv 1(\mod m)\\
a^{p(m)} * x &\equiv a^{p(m)-1}(\mod m)\\
x &\equiv a^{p(m)-1}(\mod m)
\end{aligned}$$

Beispiel 60. *1.*

$$\begin{aligned}
8x &\equiv 1(\mod 25)\\
ggT(8,25) = 1 \textit{ und } \phi(25) &= 20\\
\textit{also } 8^{20} &= 1(\mod 25)
\end{aligned}$$

und so mutliplizieren wir die Gleichung mit 8^{19}

$$\begin{aligned}
8^{19} * 8x &\equiv 8^{19}(\mod 25)\\
x &\equiv 8^{19}(\mod 25)
\end{aligned}$$

also

$$\begin{aligned}
x &\equiv ((8)^2)^9 * 8(\mod 25)\\
&\equiv (64(\mod 25))^9 * 8(\mod 25)\\
&\equiv (14)^9 * 8(\mod 25)\\
&\equiv (14^2)^4 * 14 * 8(\mod 25)\\
&\equiv (14^2(\mod 25))^4 * 14 * 8(\mod 25)\\
&\equiv (-4))^4 * 12(\mod 25)|196 = -4\\
&\equiv 256(\mod 25) * 12(\mod 25)\\
&\equiv 6 * 12(\mod 25)\\
&\equiv 72(\mod 25)\\
&\equiv 22
\end{aligned}$$

also

$$8x \equiv 1(\mod 25) \rightarrow x = 22$$

2.

$$\begin{aligned}
8^{18} &\mod 21\\
ggT(8,21) = 1 \textit{ und } \phi(21) &= 12\\
\textit{also } 8^{12} &\equiv 1(\mod 21)
\end{aligned}$$

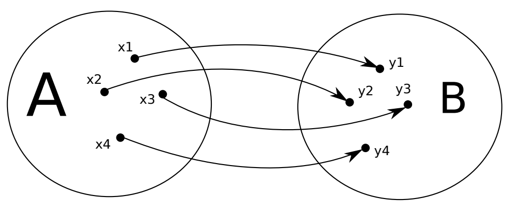
somit

$$
\begin{aligned}
8^{18} \mod (21) &\equiv 8^{12} * 8^{6} (\mod 21) \\
&\equiv 8^{12} (\mod 21) * 8^{6} (\mod 21) \\
&\equiv 8^{6} (\mod 21) \\
&\equiv (8^{2})^{3} (\mod 21) \\
&\equiv (64 \mod 21) 3 \\
&\equiv 1 \mod 21 \\
&\equiv 1
\end{aligned}
$$

Kapitel 5

Funktionen

5.1 Definitions- und Bildmenge



Definition 41. *Eine Funktion f besteht aus einer Definitionsmenge A, einer Bildmenge B und einer Vorschrift, die* <u>*jedem*</u> *$x \in A$* <u>*genau ein*</u> *$y \in B$ zuordnet.*

Ist f der Name einer Funktion, so schreiben wir

D_f für die Definitionsmenge

und

$y = f(x)$ heisst der <u>Funktionswert</u> oder das <u>Bild</u> von $x \in D_f$

Umgekehrt heisst x das <u>Urbild</u> von $y \in B$. Die Funktion beschreiben wir mit

$f : A \mapsto B$ mit $y = f(x)$

oder mit

$y = f(x)$, wobei $D_f = A$

Beispiel 61. *Beispiele von Funktionen:*

1.
$$f : \mathbb{R} \setminus \{1\} \mapsto \mathbb{R} \quad mit \quad f(x) = \frac{3}{x-1} \tag{5.1}$$

2.
$$g(x) = ln(x-3) \quad mit \quad D_g =]3; 8[\tag{5.2}$$

Kapitel 6

Kurzreferenz

6.1 Definitionen

6.1.1 natürliche Zahlen

$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$
$\mathbb{N}^0 = \{0, 1, 2, 3, 4, 5, \dots\}$

6.1.2 ganze Zahlen

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, 4, \dots\}$
$\mathbb{Z}^- = \{\dots, -3, -2, -1\}$
$\mathbb{Z}_0^- = \{\dots, -3, -2, -1, 0\}$
$\mathbb{Z}^+ = \{\mathbb{N}\}$

6.1.3 rationale Zahlen

$Q = \{x | x = \frac{p}{q} \wedge p, q \in Z \wedge p \neq 0\}$
Wenn sich eine Zahl als gemeiner Bruch schreiben lässt, Nenner und Zähler Elemente der Menge Z und p ungleich 0 ist, so handelt es sich um eine rationale Zahl. Die Zahl muss abbrechen oder periodisch sein.
Ist $0.75 \in Q$?
Ja den $0.75 = \frac{3}{4}$

Ist $0,101001000100001... \in Q$
Nein, weil es nicht abricht ud nicht periodisch ist.

Ist $0,142857 \in Q$
Ja denn $0,142857 = \frac{1}{7}$

6.1.4 irrationale Zahlen

Eine irrationale Zahl ist eine nicht periodischer und eine nicht abbrechender Dezimalbruch. Bsp. Pi

6.1.5 reele Zahlen

Die Reelen Zahlen lassen sich in zwei Gruppen aufteilen, die transzendenten und die algebraischen.

6.1.6 Kardionalität

Kardinalität = Mächtigkeit

6.1.7 Primzahlen

```
 3  5  7 11 13 17 19 23
29 31 37 41 43 47 53 59
61 67 71 73 79 83 89 97
```

6.2 Gesetze der boolschen Algebra

6.2.1 Kommutativgesetz (Vertauschungsgesetz)

$$a \wedge b = b \wedge a$$
$$a \vee b = b \vee a$$

6.2.2 Assoziativgesetz (Verbindungsgesetz)

$$a \wedge (b \wedge c) = (a \vee b) \vee c$$
$$a \vee (b \vee c) = (a \vee b) \vee c$$

6.2.3 Distributivgesetz (Verteilungsgesetz)

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

6.2.4 Absorptionsgesetz

$$a \wedge (a \vee b) = a$$
$$a \vee (a \wedge b) = a$$

6.2.5 Gesetz von De Morgan

$$\neg(a \wedge b) = \neg a \vee \neg b$$
$$\neg(a \vee b) = \neg a \wedge \neg b$$

6.2.6 Implikation

$$a \to b = \neg a \vee b$$

Umkehrung

$$a \to b = b \to a$$

Kontraposition

$$a \to b = \neg b \to \neg a$$

6.2.7 Aequivalenz

$$a \iff b = (a \to b) \wedge (b \to a)$$
$$a \iff b = \neg(a \underline{\vee} b)$$
$$\neg(a \underline{\vee} b) = (\neg a \vee \neg b) \wedge (a \vee b)$$

6.2.8 Prädikatenlogik

$$\neg\forall x(P(x)) = \exists x(\neg P(x))$$
$$\forall x(\neg P(x)) = \neg\exists x(P(x))$$

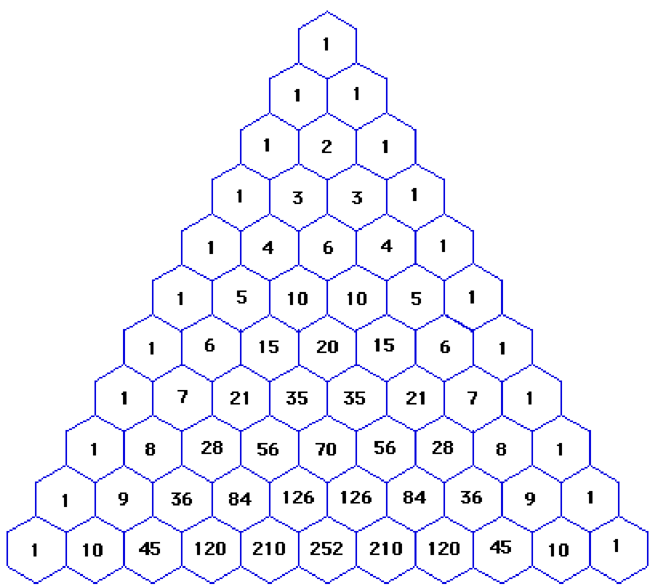
$$\neg\forall x(P(x) \to P(x))$$

was gleichbedeutend ist mit

$$\exists x(\neg[P(x) \to P(x)])$$

6.3 Mengen

6.3.1 Pascalsches Dreieck



6.3.2 Vollständige Induktion

Besteht aus 3 Teilen:

1. Induktionsverankerung (Induktionsanfang)
   Die Behauptung stimmt für n = 1
   Dieser Schritt wird in 2 Punkte unterteilt:
   - Behauptung
   - Beweis
2. Induktionsschritt
   Unter der Voraussetzung, dass die Behauptung für n gilt, ist zu zeigen, dass sie auch für n + 1 gilt.
   Dieser Schritt wird in 3 Punkte unterteilt:
   - Vorraussetzung
   - Behauptung
   - Beweis
3. Induktionsvererbung (Induktionsschluss)
   Nach (1) gilt die Behauptung für n = 1 und nach (2) gilt sie fü n + 1, falls sie fü n gilt.
   Also gilt sie für n = 2 und nach (2) für n+1, ist 3 usw. Also gilt die Behauptung für alle $n \in N$.

6.3.3 Teilmengen

$$A \subset B \iff \forall x (x \in A \rightarrow x \in B)$$

$|A|$ = n
Mächtigkeit der Potenzmenge $|P(A)| = 2^n$

6.3.4 Schnittmenge

$$\begin{aligned} A \cap B := \{x \quad | \quad x \in A \wedge x \in B\} \\ A \cap \emptyset = \emptyset \\ A \cap A = A \\ A \cap B = B \cap A \\ (A \cap B) \cap C = A \cap (B \cap C) \end{aligned}$$

6.3.5 Vereinigungsmenge

$$
\begin{aligned}
A \cup B := \{x \quad | \quad x \in A \vee x \in B\} \\
A \cup \emptyset = A \\
A \cup A = A \\
A \cup B = B \cup A \\
(A \cup B) \cup C = A \cup (B \cup C) \\
A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\
A \cup (B \cap C) = (A \cup B) \cap (A \cup C)
\end{aligned}
$$

6.3.6 Komplement

$$
\begin{aligned}
A \cap \overline{A} = \emptyset \\
A \cup \overline{A} = G \\
\overline{A \cap B} = \overline{A} \cup \overline{B} \\
\overline{A \cup B} = \overline{A} \cap \overline{B}
\end{aligned}
$$

6.3.7 Differenz

$$
\begin{aligned}
A \setminus B = A \cap \overline{B} \\
A \setminus B \neq B \setminus A \\
A \setminus B \neq B \setminus A \\
A \setminus A = \emptyset \\
A \setminus \emptyset = A
\end{aligned}
$$

A und B disjunkt, dann ist

$$
\begin{aligned}
A \setminus B = A \\
B \setminus A = B
\end{aligned}
$$

Beachten Sie

$$
\begin{aligned}
A \setminus (B \cap C) \neq (A \setminus B) \cap (A \setminus C) \\
A \cup (B \setminus C) \neq (A \cup B) \setminus (A \cup C)
\end{aligned}
$$

Aber

$$
\begin{aligned}
(B \cap C) \setminus A &= (B \setminus A) \cap (C \setminus A) \\
B \cap (C \setminus A) &= (B \setminus A) \cap (C \setminus A) \\
(B \cup C) \setminus A &= (B \setminus A) \cup (C \setminus A)
\end{aligned}
$$

6.3.8 Symetrische Differenz

$$
\begin{gathered}
A \Delta B = (A \setminus B) \cup (B \setminus A) \\
A \Delta B = (A \cup B) \cap (\overline{B} \cup \overline{A})
\end{gathered}
$$

6.3.9 Kartesisches Produkt

$[a; b] \times [c; d]$
$[a; b]$ erster Wert (a) X Koordinate von P_1, zweiter Wert (b) X Koordinate von P_2
$[c; d]$ erster Wert (c) Y Koordinate von P_1, zweiter Wert () Y Koordinate von P_2

Distributivität

$$
\begin{aligned}
(A \cup B) \times C &= (A \times C) \cup (B \times C) \\
(A \cap B) \times C &= (A \times C) \cap (B \times C) \\
(A \setminus B) \times C &= (A \times C) \setminus (B \times C) \\
A \times (B \cup C) &= (A \times B) \cup (A \times C) \\
A \times (B \cap C) &= (A \times B) \cap (A \times C) \\
A \times (B \setminus C) &= (A \times B) \setminus (A \times C)
\end{aligned}
$$

6.4 Relationen

6.4.1 Eigenschaften

reflexiv

$$a \in M : \forall a (aRa) \tag{6.1}$$

symmetrisch

$$a, b \in M : \forall a, b (aRb \rightarrow bRa) \tag{6.2}$$

antisymmetrisch

$$a, b \in M : \forall a, b [(aRb) \wedge (bRa) \rightarrow (a = b)] \tag{6.3}$$

transitiv

$$a, b, c \in M : \forall a, b, c [(aRb \wedge bRc) \rightarrow (aRc)] \tag{6.4}$$

Eine Aequivelenzklasse besitzt die Eigenschaften:

- reflexiv
- symmetrisch
- transitiv

6.4.2 Teilt

Es bedeuted $a|b$, dass a das b teilt.
Bsp. 5|30,4|28,−3|27
also
$a|b \leftrightarrow b = na$

6.4.3 Datumsbestimmung

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

6.4.4 Kongruenz

6.4.5 Kongruenzrelation

$$a \equiv b(mod m) \leftrightarrow (a mod m = b mod m)$$

6.4.6 Restklassen

$$K_a = \{x|xRa \wedge x \in M\}$$
$$a \cdot b = 0 \rightarrow (a = 0 \vee b = 0) \tag{6.5}$$

6.4.7 Inverse Restklasse

Phi Funktion

Anzahl teilerfremde Elemente in m

$$\phi(m)$$

Diophantische Gleichung

$$ax = 1 in Z_m$$
$$ax + bm = c$$

Satz von Euler Fermat

$$ax \equiv 1(mod m)$$
$$a^{\phi(m)}a^{\phi(m)} * x = 1 * x = x$$