Mathematik für 1nf0rmatiker:innen

Tobias Prisching

Fassung vom 25. September 2021

Inhaltsverzeichnis

Vorwort

Hier wird das Vorwort stehen.

Symbole

Symbol	Bedeutung	Beispiel
w, $\top$	logisches wahr (Tautologie)	-
f, $\perp$	logisches falsch (Antilogie)	-
$\neg$	logische Negation	$\neg A$
$\wedge$	logische Konjunktion (Und/AND)	$A \wedge B$
$\vee$	logische Disjunktion (Oder/OR)	ToBe $\vee$ $\neg$ToBe
$\tilde{\wedge}$	logisches Nicht-Und (NAND)	$A\tilde{\wedge}B$
$\tilde{\vee}$	logisches Nicht-Oder (NOR)	$A\tilde{\vee}B$
$\veebar$	logisches exklusives Oder (XOR)	$A \veebar B$
$\Rightarrow$	logische Implikation	$A \Rightarrow B$
$\Leftrightarrow$	logische Äquivalenz	$A \Leftrightarrow B$

Tabelle 0.1: Logik Symbole

Symbol	Bedeutung	Beispiel
$\in$	ist Element von	$x \in M$
$\notin$	ist nicht Element von	$y \notin M$
$\subseteq$	ist Teilmenge von	$N \subseteq M$
$\subset, \subsetneq, \subsetneqq$	ist echte Teilmenge von	$N \subset M$
$\nsubseteq$	ist nicht Teilmenge von	$N \nsubseteq M$
$\supseteq$	ist Obermenge von	$M \supseteq N$
$\supset, \supsetneq, \supsetneqq$	ist echte Obermenge von	$M \supset N$
$\nsupseteq$	ist nicht Obermenge von	$M \nsupseteq N$
$\mathcal{P}$	Potenzmenge	$\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$
$\cap$	Durchschnitt	$M \cap N$
$\cup$	Vereinigung	$M \cup N$
$\setminus$	Differenz	$M \setminus N$
$\overline{M}$, M^{C}	Komplement	$M^{\mathrm{C}} = \overline{M}$

Tabelle 0.2: Mengen Symbole

Logik

1 Grundlagen der Logik

Definition 1.0.1 (Aussage)**.** Unter einer **Aussage** verstehen wir einen Satz der natürlichen Sprache, welchem entweder der Wahrheitswert wahr (w, $\top$) oder falsch (f, $\bot$) zugeordnet werden kann.

Definition 1.0.2 (Logische Operatoren)**.** Mithilfe von **logischen Operatoren** (auch **Verknüpfungen**) können aus vorhandenen Aussagen neue Aussagen gebildet werden. Seien A und B Aussagen, so definieren wir folgende logische Operatoren:

Negation
(Nicht/NOT)

A	$\neg A$
f	w
w	f

Konjunktion
(Und/AND)

A	B	$A \wedge B$
f	f	f
f	w	f
w	f	f
w	w	w

Disjunktion
(Oder/OR)

A	B	$A \vee B$
f	f	f
f	w	w
w	f	w
w	w	w

Implikation

A	B	$A \Rightarrow B$
f	f	w
f	w	w
w	f	f
w	w	w

Aufbauend auf diesen Operatoren lassen sich neue Verknüpfungen definieren, wie beispielsweise das Nicht-Und/-Oder, das exklusive Oder und die Äquivalenz:

Nicht-Und
(NAND)

A	B	$A\tilde{\wedge}B$
f	f	w
f	w	w
w	f	w
w	w	f

Nicht-Oder
(NOR)

A	B	$A\tilde{\vee}B$
f	f	w
f	w	f
w	f	f
w	w	f

Exklusive Oder
(XOR)

A	B	$A \veebar B$
f	f	f
f	w	w
w	f	w
w	w	f

Äquivalenz

A	B	$A \Leftrightarrow B$
f	f	w
f	w	f
w	f	f
w	w	w

Definition 1.0.3 (Atomare Aussage)**.** Unter einer **atomaren Aussage** verstehen wir eine Aussage welche keine logischen Verknüpfungen enthält.

Definition 1.0.4 (Tautologie)**.** Unter einer **Tautologie** verstehen wir eine Aussage welche immer *wahr* ist.[1]

Definition 1.0.5 (Antilogie, Kontradiktion)**.** Unter einer **Antilogie** (auch **Kontradiktion**) verstehen wir eine Aussage welche immer *falsch* ist.[2]

[1] Beispiel: Die Aussage $A \vee \neg A$ ist immer wahr da immer entweder A oder $\neg A$ wahr ist

[2] Beispiel: Die Aussage $A \wedge \neg A$ ist immer falsch da A und $\neg A$ nie gleichzeitig wahr sind

2 Beweistechniken

Definition 2.0.1 (Mathematische Aussage)**.** Unter einer **mathematischen Aussage** (auch **Satz** genannt) verstehen wir im Normalfall ein Konstrukt der Form $v \Rightarrow f$, bestehend aus einer Voraussetzung v und einer Folgerung f, welche beide ebenfalls wiederum Aussagen (auch mathematische Aussagen) sein können.

Definition 2.0.2 (Mathematischer Beweis)**.** Unter einem **mathematischen Beweis** (meist auch nur **Beweis**) verstehen wir den Nachweis dass der zu einem mathematischen Satz korrespondierende logische Ausdruck immer wahr ist, d.h. eine Tautologie ist.

Definition 2.0.3 (Axiom)**.** Unter einem **Axiom** verstehen wir eine Aussage welche *unbewiesen* als wahr angenommen wird. [3]

[3] Axiome dienen uns als Grundbausteine für Beweise usw. die wir allerdings selbst nicht beweisen können und daher als wahr annehmen *müssen*

Definition 2.0.4 (Axiomensystem)**.** Unter einem **Axiomensystem** verstehen wir eine Ansammlung von Axiomen welche folgende Eigenschaften erfüllt:

- So wenig und einfache Axiome wie möglich welche genügen um eine Theorie vollständig zu beschreiben
- Die Axiome des Axiomensystems sind voneinader unabhängig
- Die Axiome des Axiomensystems müssen für sich selbst und untereinander widerspruchsfrei sein

2.1 Arten von Beweisen

Definition 2.1.1 (Direkter Beweis)**.** Beim **direkten Beweis** nehmen wir an, dass die Voraussetzung v wahr ist und wir versuchen, durch Vereinigung von wahren Implikationen zur Aussage "f ist wahr"zu kommen.

$$((v \Rightarrow v_1) \wedge (v_1 \Rightarrow v_2) \wedge ...(v_n \Rightarrow f)) \Rightarrow (v \Rightarrow f)$$

Definition 2.1.2 (Beweis durch Kontradiktion)**.** Beim **Beweis durch Kontradiktion** nehmen wir an, dass die Folgerung f falsch ist und versuchen dann zu dem Schluss zu kommen, dass dies nur der Fall sein kann wenn die Voraussetzung v falsch ist. [4]

[4] Dies entspricht einem direkten Beweis mit Voraussetzung $\neg f$ und Folgerung $\neg v$

$$(v \Rightarrow f) \Leftrightarrow (\neg f \Rightarrow \neg v)$$

Definition 2.1.3 (Indirekter Beweis)**.** Beim **indirekten Beweis** (auch **Beweis durch Widerspruch**) nehmen wir an, dass die Voraussetzung v wahr, aber dier Folgerung f falsch ist. Nun versuchen wir zu zeigen, dass es sich dabei um einen (logischen) Widerspruch handelt, wodurch der einzige Fall in dem $v \Rightarrow f$ falsch ist ausgeschlossen werden kann und die (logische) Aussage zur Tautologie wird.

Definition 2.1.4 (Vollständige Induktion)**.** Bei der **vollständigen Induktion**

Mengen und Relationen

3 Mengenlehre

3.1 Mengen

Definition 3.1.1 (Menge)**.** Unter einer **Menge** verstehen wir eine beliebige Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen. [5]

[5] Definiton nach Georg Cantor (1845-1918)

Eigenschaften und Regeln

- Mengen enthalten Objekte (= Elemente einer Menge) **ohne** einer vorgegebenen Reihenfolge
- Mengen selbst sind Objekte und können folglich in Mengen enthalten sein
- Explizite Notation: $M = \{0, 1, \pi, \{i\}\}$
- Implizite Notation: $\mathbb{N} = \{x|x$ ist eine natürliche Zahl$\}$
- Objekt x ist Element der Menge M: $x \in M$
- Ein Objekt innerhalb einer Menge gefasst ist ungleich dem Objekt selbst: $\{0\} \neq 0$
- $M = N \Leftrightarrow M$ und N enthalten die gleichen Elemente
- Leere Menge: $\emptyset = \{\}$

3.2 Teilmenge und Obermenge

Definition 3.2.1 (Teilmenge)**.** Unter einer **Teilmenge** der Menge M verstehen wir eine Menge N von der jedes Element in M enthalten ist: $N \subseteq M$.

Ist N keine Teilmenge von M (d.h., N enthält mindestens ein Objekt x sodass gilt $x \in N$ und $x \notin M$), so schreiben wir: $N \not\subseteq M$

Definition 3.2.2 (Echte Teilmenge)**.** Unter einer **echten Teilmenge** der Menge M verstehen wir eine Menge N von der jedes Element in M enthalten ist *und* $N \neq M$ *gilt*: $N \subset M$ (auch $N \subsetneq M$ oder $N \subsetneqq M$).

Definition 3.2.3 (Obermenge)**.** Analog zur Teilmenge verstehen wir bei der **Obermenge** von N eine Menge M die jedes Element von N enthält: $M \supseteq N$

Definition 3.2.4 (Echte Obermenge)**.** Analog zur echten Teilmenge verstehen wir bei der **echten Obermenge** von N eine Menge M die jedes Element von N enthält *und* $N \neq M$ *gilt*: $M \supset N$ (auch $M \supsetneq N$ oder $M \supsetneqq N$)

Eigenschaften und Regeln

- Die leere Menge ist Teilmenge jeder Menge: $\emptyset \subseteq M$
- Die Gleichheit von Mengen lässt sich über Teilmengen ausdrücken: Gilt $N \subseteq M$ und $M \subseteq N$, so folgt $M = N$
- Ist N eine (echte) Teilmenge von M ($N \subseteq M$ bzw. $N \subsetneq M$), so ist M (echte) Obermenge von N ($M \supseteq N$ bzw. $M \supsetneq N$)

3.3 Potenzmenge

Definition 3.3.1 (Potenzmenge)**.** Unter der **Potenzmenge** $\mathcal{P}(M)$ einer Menge M verstehen wir eine Menge welche alle möglichen Teilmengen von M enthält. [6] Es gilt: $M \in \mathcal{P}(M)$

[6] Für $M = \{0, 1\}$ ist die Potenzmenge $\mathcal{P}(M) = \{\emptyset, \{0\}, \{1\}, M\}$

3.4 Operationen mit Mengen

Definition 3.4.1 (Durschnitt, Vereinigung, Differenz)**.** Seien M und N Mengen. Wir definieren folgende Operationen:

- **Durchschnitt**: Alle Elemente die in M *und* N enthalten sind:
$$M \cap N = \{x|x \in M \wedge x \in N\}$$
- **Vereinigung**: Alle Elemente die in M *oder* N enthalten sind:
$$M \cup N = \{x|x \in M \vee x \in N\}$$
- **Differenz**: Alle Elemente die in M aber nicht in N enthalten sind:
$$M \setminus N = \{x|x \in M \wedge x \notin N\}$$
- **Komplement**: Ist $N \subseteq M$, so ist $M \setminus N$ das Komplement von N in M: $\overline{N}^M$ Ist bekannt innerhalb welcher Menge das Komplement gebildet wird kann auch $\overline{N}$ oder N^C geschrieben werden.

Definition 3.4.2 (Unendlicher Durchschnitt, Unendliche Vereinigung)**.** Sei I eine unendliche Menge von Indizes, sodass es für jedes $i \in I$ eine Menge M_i gibt. Wir definieren folgende Operationen:

- **Unendlicher Durchschnitt**: Alle Elemente die in jeder Menge M_i enthalten sind:
$$\bigcup_{i \in I} M_i = \{x|x \in M_i \forall i \in I\}$$
- **Unendliche Vereinigung**: Alle Elemente die in mindestens einer Menge M_i enthalten sind:
$$\bigcup_{i \in I} M_i = \{x|\exists i \in I|x \in M_i\}$$

Ist I endlich (betrachten wir im folgenden Beispiel den konkreten Fall $I = \{1, ..., n\}$), so handelt es sich um den Durschnitt/die Vereinigung einer endlichen Anzahl von Mengen, welche gleich unserer bisherigen Definition dieser Operationen ist:

$$\bigcup_{i \in I} M_i = M_1 \cup ... \cup M_n = \bigcup_{i=1}^{n} M_i$$

(Analog für Durchschnitt)

Definition 3.4.3 (Kartesische Produkt)**.** Unter dem **kartesischen Produkt** zweier Mengen M und N verstehen wir eine Menge alle *geordneter Paare*[7] (m, n) mit $m \in M$ und $n \in N$:
$$M \times N = \{(m, n)|m \in M, n \in N\}$$

[7] Die Reihenfolge der Elemente des Paars spielt (im Gegensatz zu wie es bei Mengen der Fall ist) eine Rolle: $(0, 1) \neq (1, 0)$
Aber: $\{0, 1\} = \{1, 0\}$
$\rightarrow$ Paare sind keine Mengen

Eigenschaften und Regeln

- Die Differenzmenge einer Menge M mit der leeren Menge ist die Menge selbst: $M \setminus \emptyset = M$
- Kommutativgesetze:
$$M \cup N = N \cup M$$
$$M \cap N = N \cap M$$
- Assoziativgesetze:
$$(M \cup N) \cup O = M \cup (N \cup O)$$
$$(M \cap N) \cap O = M \cap (N \cap O)$$

- Distributivgesetze:

$$M \cap (N \cup O) = (M \cap N) \cup (M \cap O)$$

$$M \cup (N \cap O) = (M \cup N) \cap (M \cup O)$$

- Rechenregeln der Komplementbildung:
  - $\overline{\overline{M}} = M$
  - $M \subseteq N \Rightarrow \overline{N} \subseteq \overline{M}$
  - $M \setminus N = M \cap \overline{N}$
  - $\overline{M \cup N} = \overline{M} \cap \overline{N}$
  - $\overline{M \cap N} = \overline{M} \cup \overline{N}$
- Im Allgemeinen gilt $M \times N = N \times M$ **nicht**
- $M \times \emptyset = \emptyset$

3.5 Mächtigkeit

Definition 3.5.1 (Mächtigkeit, Kardinalität, Kardinalzahl)**.** Unter der **Mächtigkeit** (auch **Kardinalität**) einer Menge M verstehen wir die Anzahl der in M enthaltenen Elemente (die **Kardinalzahl**), welche als $|M|$ notiert wird.

Definition 3.5.2 (gleichmächtig)**.** Gilt $|M| = |N|$, so nennen wir die beiden Mengen M und N **gleichmächtig** (wir sagen auch, sie haben die gleiche Kardinalität). Des Weiteren halten wir fest, dass zwei Mengen M und N genau dann gleichmächtig sind, wenn es eine bijektive Abbildung[8] $f : M \to N$ zwischen diesen Mengen gibt.

[8] Siehe Kapitel 6

4 Spezielle Mengen

4.1 Natürliche ($\mathbb{N}$), Ganze ($\mathbb{Z}$) und Rationale ($\mathbb{Q}$) Zahlen

Definition 4.1.1 (Natürliche Zahlen)**.** Wir definieren die Menge $\mathbb{N}$ der **natürlichen Zahlen** mithilfe des folgenden Axiomensystems, bekannt als die *Peano-Axiome*[9]:

1. Die Zahl 0 ist eine natürliche Zahl:
$$0 \in \mathbb{N}$$
2. Sei n eine natürliche Zahl, so hat n genau einen Nachfolger n'[10] welcher ebenfalls eine natürliche Zahl ist:
$$\forall n \in \mathbb{N} : n' \in \mathbb{N}$$
3. Sei n eine natürliche Zahl, so hat n genau einen Nachfolger n' ungleich 0:
$$\forall n \in \mathbb{N} : n' \neq 0$$
4. Seien n und m natürliche Zahlen und n' und m' ihre respektiven Nachfolger, so gilt dass falls n' und m' gleich sind auch n und m gleich sind:
$$\forall n, m \in \mathbb{N} : n' = m' \Rightarrow n = m$$
5. Sei M eine Menge. Enthält M die Zahl 0 und für jede in M enthaltene Zahl n auch ihren Nachfolger n', so ist die Menge der natürlichen Zahlen eine Teilmenge von M:
$$\forall M : (0 \in M \land (n \in M) \Rightarrow (n' \in M)) \Rightarrow \mathbb{N} \subseteq M$$

[9] nach Giuseppe Peano (1858-1932)

[10] Unter dem Nachfolger n' einer Zahl n verstehen wir im Kontext dieser Definition $n + 1$

Es gibt verschiedene Formulierungen der Peano-Axiome denen man begegnet. Eine Weitere wäre beispielsweise:

1. $1 \in \mathbb{N}$
2. Sei $n \in \mathbb{N}$, so hat n genau einen Nachfolger n' mit $n' \neq 1$ und $n' \in \mathbb{N}$
3. Seien $n, m \in \mathbb{N}$ voneinander verschiedene natürliche Zahlen, so sind ihre Nachfolger n' bzw. m' ebenfalls voneinander verschieden ($n \neq m \Rightarrow n' \neq m'$)
4. Sei $M \subseteq \mathbb{N}$. Erfüllt M die beiden Eigenschaften
   - $1 \in M$
   - Sei $n \in M$, so ist der Nachfolger n' von n ebenfalls in M ($n \in M \Rightarrow n' \in M$)

   so gilt: $M = \mathbb{N}$

Wir sehen, dass diese Version der Axiome die Zahl 0 nicht zu den natürlichen Zahlen zählt. In weiterer Folge werden wir jedoch die Zahl 0 zu $\mathbb{N}$ hinzunehmen.[11]

[11] Falls doch einmal notwendig werden wir $\mathbb{N}^*$ für $\mathbb{N} \setminus \{0\}$ verwenden.

Definition 4.1.2 (Ganze Zahlen)**.** Basierend auf der Menge der natürlichen Zahlen definieren wir die Menge der **ganzen Zahlen** $\mathbb{Z}$:

$$\mathbb{Z} = \{z | z \in \mathbb{N} \lor -z \in \mathbb{N}\}$$

Definition 4.1.3 (Rationale Zahlen)**.** Basierend auf der Menge der natürlichen Zahlen und der ganzen Zahlen definieren wir die Menge der **rationalen Zahlen** $\mathbb{R}$:

$$\mathbb{R} = \{r | r = \frac{z}{n}, z \in \mathbb{Z}, n \in \mathbb{N}^*\}$$

Die Mächtigkeit von $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$

Definition 4.1.4 (abzählbar unendlich)**.** Intuitiv stelle wir fest dass es *unendlich* viele natürliche Zahlen gibt, da es für jede beliebige natürliche Zahl n einen Nachfolger $n+1$ gibt welcher ebenfalls eine natürliche Zahl ist und ebenfalls einen Nachfolger hat usw. Folglich hat die Menge $\mathbb{N}$ keine endliche Kardinalität, daher definieren wir $|\mathbb{N}| = \aleph_0$ (gesprochen: Aleph Null) und sagen, dass $\mathbb{N}$ **abzählbar unendlich** ist.

Nun zeigen wir, basierend auf den Definition 3.5.2 und 4.1.4, dass auch die Mengen $\mathbb{Z}$ und $\mathbb{Q}$ abzählbar unendlich sind. Dazu suchen wir uns bijektive Abbildungen[12] $f_Z : \mathbb{N} \to \mathbb{Z}$ und $f_Q : \mathbb{N} \to \mathbb{Q}$ um zu zeigen dass $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ gleichmächtig sind:

[12] Siehe Kapitel 6

- $f_Z : \mathbb{N} \to \mathbb{Z}$: Eine solche Funktion wäre z.B.: $f_Z(0) = 0$, $f_Z(1) = 1$, $f_Z(2) = -1$, bei der wir 0 auf 0, die ungeraden Elemente von $\mathbb{N}$ auf die positiven Elemente von $\mathbb{Z}$, und alle weiteren geraden Elemente aus $\mathbb{N}$ (größer 0 natürlich) auf die negativen Elemente von $\mathbb{Z}$ abbilden. Es folgt: $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$

- $f_Q : \mathbb{N} \to \mathbb{Q}$: Wir beginnen damit, Brüche systematisch in folgendem Schema aufzuschreiben und nacheinander über die eingezeichneten Diagonalen abzuzählen, wobei ungekürzte Brüche wie $\frac{2}{2}$ übersprungen werden:

$$\begin{array}{cccccccc}
\frac{1}{1} & \rightarrow & \frac{1}{2} & & \frac{1}{3} & \rightarrow & \frac{1}{4} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \frac{2}{4} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \\
\frac{3}{1} & & \frac{3}{2} & & \frac{3}{3} & & \frac{3}{4} & \cdots \\
\vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

Wir erhalten dadurch folgende Abbildung:

$$\begin{array}{ccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \dots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
1 & \frac{1}{2} & 2 & 3 & \frac{1}{3} & \frac{1}{4} & \frac{2}{3} & \frac{3}{2} & \dots
\end{array}$$

Des Weiteren bilden wir 0 auf 0 ab und fügen für jedes Bild zusätzlich dessen negatives Gegenstück hinzu, ähnlich wie bei der Funkition f_Z:

$$\begin{array}{cccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \dots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
0 & 1 & -1 & \frac{1}{2} & -\frac{1}{2} & 2 & -2 & 3 & -3 & \frac{1}{3} & -\frac{1}{3} & \dots
\end{array}$$

Durch diese Vorschrift[13] erhalten wir die bijektive Abbildung f_Q, aus welcher folgt: $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$

[13] Bekannt als *Cantors erstes Diagonalargument*

4.2 Reelle Zahlen $\mathbb{R}$

Kommt später... $\mathfrak{c}$

Definition 4.2.1 (Reelle Zahlen)**.**

Definition 4.2.2 (überabzählbar unendlich)**.** $\mathfrak{c}$

4.3 Komplexe Zahlen $\mathbb{C}$

Kommt später...

5 Relationen

5.1 Grundlegendes

Definition 5.1.1 ((2-stellige) Relation)**.** Seien M und N Mengen und R eine Teilmenge des kartesischen Produkt der beiden ($R \subseteq M \times N$). Nun verstehen wir unter R eine **Relation** auf $M \times N$. Für den Spezialfall $M = N$ heißt R Relation auf M.[14]

Dabei gilt es vor allem zu beachten, dass eine Relation für ein Paar von Werten (= ein Element des kartesischen Produkts) nur entweder zutreffen kann oder nicht - entweder es gibt eine Relation zwischen den Werten oder nicht. Wir können eine Relation also als eine Aussagevorschrift über das Verhältnis zwischen diesen Werten betrachten.

[14] Der Punkt dabei ist, dass die Teilmenge R beliebig definiert werden kann um verschiedenste Relationen bilden zu können.

Um auszudrücken dass beispielsweise die Elemente 0 und 1 die Relation $<$ erfüllen können wir eine der folgenden Schreibweisen verwenden: $R_<(0,1)$[15] oder $(0,1) \in R_<$ oder schlicht $0 < 1$.

[15] Es kann auch nur $R(0,1)$ geschrieben werden, vorausgesetzt die Bezeichnung R ist eindeutig

Definition 5.1.2 (n-stellige Relation)**.** Basierend auf der vorangehenden Definition von 2-stelligen Relationen definieren wir diese nun für n Stellen: Seien M_1, ..., M_n Mengen und $R \subseteq M_1 \times ... \times M_n$ dann heißt R **n-stellige Relation** auf $M_1 \times ... \times M_n$.

5.2 Äquivalenzrelationen

Definition 5.2.1 (Äquivalenzrelation)**.** Unter einer **Äquivalenzrelation**[16] verstehen wir eine Relation R auf einer Menge M welche folgende Eigenschaften erfüllt:

[16] wie bspw. $R_=$

- **Reflexivität**: Für alle Elemente m aus M gilt, dass diese mit sich selbst in Relation stehen:
$$\forall m \in M : R(m,m)$$
- **Symmetrie**: Für alle Paare von Elementen (m_1, m_2) aus $M \times M$ gilt, dass falls m_1 und m_2 in Relation stehen ($R(m_1, m_2)$) auch m_2 und m_1 in Relation stehen ($R(m_2, m_1)$):
$$\forall m_1, m_2 \in M : R(m_1, m_2) \Leftrightarrow R(m_2, m_1)$$
- **Transitivität**: Für alle Elemente m_1, m_2 und m_3 aus M gilt, dass falls m_1 und m_2 in Relation stehen ($R(m_1, m_2)$) und m_2 und m_3 in Relation stehen ($R(m_2, m_3)$) auch m_1 und m_3 in Relation stehen ($R(m_1, m_3)$):
$$\forall m_1, m_2, m_3 \in M : (R(m_1, m_2) \wedge R(m_2, m_3)) \Rightarrow R(m_1, m_3)$$

5.2.1 Äquivalenzklassen

Definition 5.2.2 (Äquivalenzklasse)**.** Sei R eine Äquivalenzrelation auf einer Menge M und $m \in M$. Nun verstehen wir unter einer **Äquivalenzklasse** $[m]$ eine Menge von Elementen welche zu m in Relation stehen (auch, *die zu m äquivalent sind*):
$$[m] = \{n \in M | R(n, m)\}$$

5.2.2 Einschub: Teilbarkeit

Definition 5.2.3 (teilbar, Quotient)**.** Es seien $z_1, z_2 \in \mathbb{Z}$ mit $z_2 \neq 0$. Wir sagen dass z_1 durch z_2 **teilbar** ist (geschrieben $z_2 | z_1$, "z_2 teilt z_1") wenn ein **Quotient** $q \in \mathbb{Z}$ existiert sodass $z_1 = z_2 \cdot q$ gilt.

Definition 5.2.4 (kongruent modulo n)**.** Es seien $z_1, z_2 \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Die beiden Elemente z_1, z_2 nennen wir **kongruent modulo** n wenn $z_1 - z_2$ durch n ohne Rest teilbar ist, geschrieben $z_1 \equiv z_2 \mod n$.

Satz 5.2.1. Seien $z_1, z_2 \in \mathbb{Z}$. Die beiden Elemente z_1, z_2 sind genau dann kongruent modulo n mit $n \in \mathbb{N}^*$ (also $z_1 \equiv z_2 \mod n$) wenn z_1 und z_2 nach der Division mit n beide den gleichen Rest haben (also $z_1 \mod n = z_2 \mod n$).

Beweis. Wir wollen zeigen:

$$z_1 \equiv z_2 \mod n \Leftrightarrow z_1 \mod n = z_2 \mod n$$

Zeigen wir zunächst "$\Leftarrow$": Dazu schreiben wir z_1 und z_2 um: $z_1 = q_1 \cdot n + r$ und $z_2 = q_2 \cdot n + r$ mit den Quotienten q_1, q_2 und dem Rest r (aus $z_1 \mod n = z_2 \mod n$ folgt dass beide den gleichen Rest r haben müssen). Folglich lautet die Differenz $z_1 - z_2$ der beiden Elemente: $z_1 - z_2 = q_1 \cdot n + r - (q_2 \cdot n + r) = q_1 \cdot n - q_2 \cdot n = (q_1 - q_2) \cdot n$. Diese Differenz ist durch n teilbar, also folgt $z_1 \equiv z_2 \mod n$.

Nun zeigen wir den "$\Rightarrow$" Teil: Schreiben wir z_1 und z_2 erneut um: $z_1 = q_1 \cdot n + r_1$ und $z_2 = q_2 \cdot n + r_2$ mit den Quotienten q_1, q_2 und den Resten r_1, r_2 (aus $z_1 \equiv z_2 \mod n$ ist nicht direkt ersichtlich dass beide den gleichen Rest haben müssen). Des Weiteren wissen wir dass die Differenz $z_1 - z_2$ ein Vielfaches von n ist: $z_1 - z_2 = q \cdot n$. Wir können die Differenz aber auch so schreiben: $z_1 - z_2 = q_1 \cdot n + r_1 - q_2 \cdot n + r_2 = (q_1 - q_2) \cdot n + (r_1 - r_2)(= q \cdot n)$. Da $(q_1 - q_2) \cdot n$ offensichtlich ein Vielfaches von n ist, muss auch $(r_1 - r_2)$ ein Vielfaches von n sein: $r_1 - r_2 = q_r \cdot n$. Durch Umformen erhalten wir: $r_1 = q_r \cdot n + r_2$. Da aber $r_1 < n$ sein muss (und der Rest r_2 positiv sein muss), muss $q_r = 0$ gelten, woraus folgt: $r_1 = 0 \cdot n + r_2 = r_2$. Da wir die Reste durch Anwendung von Modulo erhalten, folgt: $z_1 \mod n = z_2 \mod n$. □

Satz 5.2.2. Die Relation $\equiv$ ist eine Äquivalenzrelation.

Beweis.

- Reflexivität: $z_1 \equiv z_1 \mod n$ ist offensichtlich wahr (ob $z_1 - z_1$ oder $z_1 - z_1$[17] durch n teilbar ist macht keinen Unterschied)
- Symmetrie: Aus $z_1 \equiv z_2 \mod n$ folgt $z_2 \equiv z_1 \mod n$, da dadurch schlichtweg das Vorzeichen der Differenz der Elemente (und folglich auch des Quotienten) umgedreht wird, der Rest aber unverändert bleibt.
- Transitivität: Dass wenn $z_1 \equiv z_2 \mod n$ und $z_2 \equiv z_3 \mod n$ wahr sind auch $z_1 \equiv z_3 \mod n$ wahr ist, lässt sich dank Satz 5.2.1 einfach zeigen: z_1 und z_2 haben offensichtlich nach der Division mit n den gleichen Rest ($z_1 \mod n = z_2 \mod n$), gleiches gilt auch für z_2 und z_3. Wenn $(z_1 \mod n) = (z_2 \mod n)$ und $(z_2 \mod n) = (z_3 \mod n)$[18], dann muss auch $(z_1 \mod n) = (z_3 \mod n)$ gelten, woraus (dank Satz 5.2.1) folgt, dass $z_1 \equiv z_3 \mod n$ wahr ist.

□

[17] Nein, kein Tippfehler

[18] Klammern gesetzt um "=" als Äquivalenzrelation hervorzuheben

5.2.3 Restklassen

Definition 5.2.5 (Restklasse). Sei $n \in \mathbb{N}^*$ und $m \in \mathbb{N}$ mit $m < n$. Nun bilden jene Elemente welche zu m kongruent modulo n sind eine Äquivalenzklasse $[m]_n$ (auch nur $[m]$ wenn der Modulo im Kontext klar ist), eine sogenannte **Restklasse**:

$$[m]_n = \{z \in \mathbb{Z} | z \equiv m \mod n\}$$

Eine Restklasse enthält dabei alle Elemente welche nach der Division mit n den gleichen Rest $m < n$ hinterlassen. Für eine Restklasse kann es verschiedene Bezeichnungen geben: Die Restklasse $[m]_n$ ist gleich der Restklasse $[m + n]_n$, genauso $[m + 2 \cdot n]_n$, $[m + 3 \cdot n]_n$, usw.

5.3 Ordnungsrelationen

Definition 5.3.1 (partielle Ordnungsrelation). Unter einer **partiellen Ordnungsrelation**[19] verstehen wir eine Relation R auf einer Menge M welche folgende Eigenschaften erfüllt:

[19] wie bspw. $R_\leq$

- Reflexivität (Siehe 5.2.1)
- Transitivität (Siehe 5.2.1)
- **Anti-Symmetrie**: Für alle Paare von Elementen (m_1, m_2) aus $M \times M$ gilt, dass falls m_1 und m_2 und auch m_2 und m_1 in Relation stehen ($R(m_1, m_2)$ und $R(m_2, m_1)$), m_1 und m_2 gleich sein müssen:

$$\forall m_1, m_2 \in M : (R(m_1, m_2) \wedge R(m_2, m_1)) \Rightarrow m_1 = m_2$$

Definition 5.3.2 (totale Ordnungsrelation)**.** Unter einer **totalen Ordnungsrelation** verstehen wir eine Relation R auf einer Menge M welche neben den Eigenschaften der partiellen Ordnungsrelation auch die folgende Eigenschaft erfüllt:

- **Totalität**: Für alle Paare von Elementen m_1, m_2 mit $m_1 \in M$ und $m_2 \in M$ gilt, dass entweder m_1 und m_2 in Relation stehen oder aber m_2 und m_1:

$$\forall m_1, m_2 \in M : R(m_1, m_2) \vee R(m_2, m_1)$$

Funktionale Abhängigkeiten

6 Abbildungen

Definition 6.0.1 (Abbildung, Funktion)**.** Nehmen wir zwei Mengen M und N. Unter einer **Abbildung** (auch, *und viel häufiger*, **Funktion** genannt)

$$f : M \to N, m \mapsto f(m)$$

verstehen wir nun die Zuordnung *genau eines* Elements $n \in N$ zu jedem Element $m \in M$.[20]

[20] In diesem Kontext: "$\to$" für Mengen "$\mapsto$" für Elemente

Definition 6.0.2 (Definitionsmenge)**.** Sei $f : M \to N, m \mapsto f(m)$ eine Abbildung, dann nennen wir $D(f) = M$ **Definitionsmenge** von f.

Definition 6.0.3 (Argument)**.** Sei $f : M \to N, m \mapsto f(m)$ eine Abbildung, dann nennen wir $m \in M$ das Argument von f.

Definition 6.0.4 (Bildmenge)**.** Sei $f : M \to N, m \mapsto f(m)$ eine Abbildung, dann nennen wir

$$f(M) = \{n \in N | \exists m \in M : n = f(m)\}$$

Definition 6.0.5 (Bild, Urbild)**.** Sei $f : M \to N, m \mapsto f(m)$ eine Abbildung, $m \in M$, $n \in N$ und $n = f(m)$. Dann nennen wir n das **Bild** von m und m das **Urbild** von n. Weiters sei $O \subseteq M$ und $P \subseteq N$. Dann heißt die Menge der Bilder von $o \in O$ **Bild von** O und die Menge der Urbilder von $p \in P$ **Urbild von** P:

Definition 6.0.6 (Injektiv, Surjektiv, Bijektiv)**.** Sei $f : M \to N, m \mapsto f(m)$ eine Abbildung. So nennen wir f

- **Injektiv**: Für jedes Paar $m_1, m_2 \in M$ gilt, dass wenn die Bilder von m_1 und m_2 gleich sind, auch m_1 und m_2 gleich sind:

$$\forall m_1, m_2 \in M : (f(m_1) = f(m_2)) \Rightarrow m_1 = m_2$$

- **Surjektiv**: Für jedes $n \in N$ gibt es ein $m \in M$ sodass $f(m) = n$:

$$\forall n \in N : \exists m \in M : f(m) = n$$

- **Bijektiv**: Wenn f injektiv und surjektiv ist

Definition 6.0.7 (Umkehrabbildung)**.** Sei $f : M \to N, m \mapsto f(m)$ eine bijektive Abbildung. Nun definieren wir die sogenannte **Umkehrabbildung**

$$f^{-1} : N \to M, n \mapsto m$$

mit $f^{-1}(n) = m$ wenn $f(m) = n$.

Algebra

7 Algebraische Strukturen

Definition 7.0.1 (Operation)**.** Unter einer **Operation** verstehen wir eine Abbildung vom kartesischen Produkt einer zugrundeliegenden Menge mit sich selbst in eben diese Menge. Einfacher formuliert handelt es sich dabei um eine Verknüpfung von Elementen.[21]

[21] Addition und Multiplikation sind zwei Beispiele für Operationen

Definition 7.0.2 (Algebraische Struktur)**.** Unter einer **algebraischen Struktur** verstehen wir eine Menge auf welcher eine oder mehrere Operation(en) definiert ist/sind.

7.1 Gruppen

Definition 7.1.1 (Gruppe, neutrales Element, inverses Element, assoziativ)**.** Unter einer **Gruppe** $(G, *)$ verstehen wir eine Menge G auf welcher eine Operation (Abbildung) $* : G \times G \to G$ definiert ist. Dabei müssen folgende Eigenschaften erfüllt sein:

- **Neutrales Element**: Es existiert ein $e \in G$ sodass $e * g = g * e = g$ für alle $g \in G$ gilt. Dieses Element e nennen wir neutrales Element in G.
- **Inverses Element**: Für jedes $g \in G$ existiert genau ein eindeutiges Element $g^{-1} \in G$ sodass $g * g^{-1} = g^{-1} * g = e$ gilt. Jedes solche Element g^{-1} nennen wir das inverse Element zu g.
- **Assoziativ**: Es seien $g_1, g_2, g_3 \in G$ beliebig. Gilt für jedes solches Triplett dass $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$, so nennen wir G assoziativ.

Definition 7.1.2 (kommutativ, kommutative Gruppe, abelsche Gruppe)**.** Es sei $(G, *)$ eine Gruppe. Erfüllt $(G, *)$ nun zusätzlich die Eigenschaft

- **Kommutativ**: Für alle $g_1, g_2 \in G$ gilt, dass $g_1 * g_2 = g_2 * g_1$

so nennen wir $(G, *)$ eine **kommutative** (oder auch **abelsche**[22]) Gruppe.

[22] benannt nach Niels Henrik Abel (1802-1829)

Satz 7.1.1. Es sei $(G, *)$ eine Gruppe, so gilt für alle $g_1, g_2 \in G$:

- Das inverse Element von $(g_1 * g_2)$ lässt sich folgendermaßen umschreiben: [23]

$$(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$$

[23] Wichtig: $(g_1 * g_2)^{-1} = g_1^{-1} * g_2^{-1}$ gilt nur in abelschen Gruppen

Beweis. Wir wollen folgendes zeigen: $(g_1 * g_2) * (g_2^{-1} * g_1^{-1}) = e$. Dazu wenden wir das Assoziativgesetz an: $(g_1 * g_2) * (g_2^{-1} * g_1^{-1}) = g_1 * (g_2 * g_2^{-1}) * g_1^{-1}$. Nun können wir die Eigenschaft des inversen Elements anwenden: $g_2 * g_2^{-1} = e$ $\Rightarrow g_1 * (g_2 * g_2^{-1}) * g_1^{-1} = g_1 * e * g_1^{-1}$. Aufgrund der Eigenschaft des neutralen Elements wissen wir: $g_1 * e = g_1$, woraus folgt: $g_1 * e * g_1^{-1} = g_1 * g_1^{-1}$. Wir wenden erneut die Eigenschaft des inversen Elements an: $g_1 * g_1^{-1} = e$ □

- Das inverse Element eines Elements $g \in G$ ist eindeutig.

Beweis. Nehmen wir an, es gibt zwei inverse Elemente g^{-1} und $\hat{g}$ zu $g \in G$. Wir wollen zeigen, dass diese beiden inverse Elemente gleich sind: $g^{-1} = \hat{g}$. Wir wissen, dass wir ein Element mit dem neutralen Element erweitern können: $g^{-1} = g^{-1} * e$. Des Weiteren erhalten wir das neutrale Element durch Verknüpfung: $g^{-1} * e = g^{-1} * (g * \hat{g})$. Nun wenden wir das Assoziativgesetz an und erneut die Eigenschaften des inversen und des neutralen Elements: $g^{-1} * (g * \hat{g}) = (g^{-1} * g) * \hat{g} = e * \hat{g} = \hat{g}$ □

Definition 7.1.3 (Untergruppe)**.** Es sei $(G, *)$ eine Gruppe und $U \subseteq G$, so ist $(U, *)$ eine **Untergruppe** von G[24], wenn folgende Eigenschaften erfüllt sind:

[24] bspw. ist $(\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{R}, +)$

- Für jedes in U enthaltene Element ist auch dessen inverses Element in U:[25]

$$\forall g \in G : (g \in U) \Rightarrow (g^{-1} \in U)$$

[25] Achtung: Der Allquantor $\forall$ besagt *nicht* dass jedes Element von G auch in U ist!

- Die Verknüpfung zweier Elemente aus U ist ebenfalls in U:

$$\forall g_1, g_2 \in G : (g_1, g_2 \in U) \Rightarrow (g_1 * g_2 \in U)$$

7.1.1 Permutationsgruppen

7.1.2 Restklassen als Gruppen

7.2 Ringe

Definition 7.2.1 (Ring)**.** Unter einem **Ring** $(R, \oplus, \odot)$ verstehen wir eine Menge auf welcher zwei Operation $\oplus$ und $\odot$ definiert sind. Dabei müssen folgende Eigenschaften erfüllt sein:

- **Kommutative Gruppe**: $(R, \oplus)$ ist eine kommutative Gruppe
- **Assoziativ**: Es seien $r_1, r_2, r_3 \in R$ beliebig. Gilt für jedes solche Triplett dass $r_1 \odot (r_2 \odot r_3) = (r_1 \odot r_2) \odot r_3$, so nennen wir R assoziativ (bezüglich $\odot$).
- **Distributiv**: Es seien $r_1, r_2, r_3 \in R$ beliebig. Gilt für jedes solche Triplett dass
  - $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
  - $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

  so nennen wir R distributiv.

Definition 7.2.2 (kommutativer Ring)**.** Es sei $(R, \oplus, \odot)$ ein Ring. Erfüllt $(R, \oplus, \odot)$ nun zusätzlich die Eigenschaft

- **Kommutativ (bezüglich $\odot$)**: Für alle $r_1, r_2 \in R$ gilt, dass $r_1 \odot r_2 = r_2 \odot r_1$

so nennen wir $(R, \oplus, \odot)$ einen **kommutativen Ring**.

Definition 7.2.3 (Ring mit Eins, unitärer Ring)**.** Kommt später...

Definition 7.2.4 (Unterring)**.** Kommt später...

7.2.1 Restklassenringe

Definition 7.2.5 (Restklassenring)**.** Sei $n \in \mathbb{N}^*$. Die Menge aller Restklassen [0], ..., $[n-1]$ bezeichnen wir als $\mathbb{Z}/n\mathbb{Z}$, welche die Struktur eines Rings hat und wir deshalb als **Restklassenring** bezeichnet. Wir definieren die folgenden Verknüpfungen auf $\mathbb{Z}/n\mathbb{Z}$, wobei $[z_1]_n$, $[z_2]_n$ Restklassen aus $\mathbb{Z}/n\mathbb{Z}$ sind:

- $[z_1]_n \oplus [z_2]_n = [z_1 + z_2]_n$
- $[z_1]_n \odot [z_2]_n = [z_1 \cdot z_2]_n$

Was wenn $z_1 + z_2$ bzw. $z_1 \cdot z_2$ größer n? Erinnern wir uns an Definition von Restklassen: Die Restklassen $[m]_n$, $[m + n]_n$, usw. sind gleich, d.h. $[z_1 + z_2]_n$ ist die gleiche Restklasse wie $[(z_1 + z_2) \mod n]_n$ (analog für $z_1 \cdot z_2$).

Aufgrund der Bedeutung von Restklassenringen in der Informatik werden wir in Zukunft auch schlichtweg nur Reste und nicht die gesamte Restklasse anschreiben (also z_1 statt $[z_1]_n$, wobei n immer klar aus dem Kontext erkennbar bleiben sollte). Da es in diesem Fall wichtig ist, dass das Ergebnis *immer* kleiner n sein muss, definieren wir diese Operationen für diese Schreibweise neu: Seien z_1, z_2 Reste:

- $z_1 \oplus z_2 = (z_1 + z_2) \mod n$
- $z_2 \odot z_2 = (z_1 \cdot z_2) \mod n$

7.2.2 Polynomringe

7.3 Körper

Definition 7.3.1 (Körper)**.** Unter einem **Körper** $(K, \oplus, \odot)$ verstehen wir eine Menge K auf welcher zwei Operation $\oplus$ und $\odot$ definiert sind. Dabei müssen folgende Eigenschaften erfüllt sein:

- **Kommutativer Ring**: $(K, \oplus, \odot)$ ist ein kommutativer Ring

- **″1″-Element**: Es existiert ein Element ″1″[26] in K sodass $1 \odot k = k \odot 1 = k$ für jedes $k \in K$ mit $k \neq 0$
- **Inverses Element (bezüglich $\odot$)**: Für jedes Element $k \in K$ mit $k \neq 0$ existiert genau ein eindeutiges Element $k^{-1} \in K$ sodass $k^{-1} \odot k = 1$ gilt.

Daraus folgt dass $(K \setminus \{0\}, \odot)$ eine abelsche Gruppe mit neutralem Element 1 ist.

[26] ″1″ statt 1 da es um ″die Idee hinter 1 als neutrales Element″ und nicht um $1 \in \mathbb{N}$ geht. Dies wird später bspw. bei der Identitätsmatrix verständlicher.