Mathematik für 1nf0rmatiker:innen

Tobias Prisching

Fassung vom 9. Oktober 2021

Inhaltsverzeichnis

Vorwort

Hier wird das Vorwort stehen.

Symbole

Symbol	Bedeutung	Beispiel
w, $\top$	logisches wahr (Tautologie)	-
f, $\bot$	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)	$A \tilde{\vee} B$
$\veebar$, $\dot{\vee}$	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	$N \subset M$
$\not\subseteq$	ist nicht Teilmenge von	$N \not\subseteq M$
$\supseteq$	ist Obermenge von	$M \supseteq N$
$\supset, \supsetneq, \supsetneqq$	ist echte Obermenge von	$M \supset N$
$\not\supseteq$	ist nicht Obermenge von	$M \not\supseteq N$
$\mathcal{P}$	Potenzmenge	$\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$
$\cap$	Durchschnitt	$M \cap N$
$\cup$	Vereinigung	$M \cup N$
$\setminus$	Differenz	$M \setminus N$
$\overline{M}, M^{\mathrm{C}}$	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: $\mathbb{N} = \{x | x \text{ ist eine natürliche Zahl}\}$
- 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]:

[9] nach Giuseppe Peano (1858-1932)

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:

$$\forall n \in \mathbb{N} : n' \in \mathbb{N}$$

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

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:

$$\forall M : (0 \in M \land (n \in M) \Rightarrow (n' \in M)) \Rightarrow \mathbb{N} \subseteq M$$

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** $\mathbb{Z}$:

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

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 stellen 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:

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

  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:

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

  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 $\mathbb{R}$

Definition 4.2.1 (Reelle Zahlen, irrationale Zahl)**.** Basierend auf der Menge der rationalen Zahlen definieren wir die Menge der **reellen Zahlen**, welche zusätzlich die Menge der irrationalen Zahlen enthält. Unter einer **irrationalen Zahl** verstehen wir eine Zahl x welche sich *nicht* als Bruch $\frac{z}{n}$ (mit $z \in \mathbb{Z}$, $n \in \mathbb{N}^*$) aufschreiben lässt.[14] Wir notieren die Menge der reellen Zahlen als $\mathbb{R}$, die der irrationalen Zahlen als $\mathbb{R} \setminus \mathbb{Q}$.[15]

[14] Prominente Beispiele: π, e, $\sqrt{2}$

[15] Es folgt: Eine reelle Zahl ist entweder rational oder irrational

Die Mächtigkeit von $\mathbb{R}$

Definition 4.2.2 (überabzählbar unendlich)**.** Nachdem die Menge der reellen Zahlen auf der Menge der rationalen Zahlen aufbaut scheint es zunächst logisch, dass diese ebenfalls unendlich groß ist und abzählbar unendlich ist. Dem ist allerdings nicht so, und wir werden nun sehen, dass die unendliche Kardinalität von $\mathbb{R}$ größer ist als die von $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$.

Beweis. Nehmen wir zunächst an, $\mathbb{R}$ sei abzählbar unendlich. Dann könnte man eine bijektive Abbildung $f_R : \mathbb{N} \to \mathbb{R}$ folgendermaßen konstruieren, wobei die reellen Zahlen mit unendlich vielen Nachkommastellen aufgeschrieben werden[16]:

- $0 \to 0.00000...$
- $1 \to 1.29456...$
- $2 \to 2.71828...$
- $3 \to 3.14159...$
- ...

Dabei gibt es keine besondere Reihenfolge, welche natürliche Zahl auf welche reelle Zahl abgebildet wird. Nun konstruieren wir die folgende reelle Zahl $r \in \mathbb{R}$, welche vor dem Komma (der Einfachheit halber) schlicht eine 0 stehen hat. Dann...

- ...setzen wir die *erste* Nachkommastelle auf die *erste* Nachkommastelle von $f_R(0)$, addieren zu dieser Ziffer 1 und bilden falls notwendig den Modulo 10. Wir erhalten 0.1. Weiters...
- ...setzen wir die *zweite* Nachkommastelle auf die *zweite* Nachkommastelle von $f_R(1)$, addieren zu dieser Ziffer 1 und bilden falls notwendig den Modulo 10. Wir erhalten 0.10. Weiters...
- ...setzen wir die *dritte* Nachkommastelle auf die *dritte* Nachkommastelle von $f_R(2)$, addieren zu dieser Ziffer 1 und bilden falls notwendig den Modulo 10. Wir erhalten 0.109. Weiters...
- ...setzen wir die *vierte* Nachkommastelle auf die *vierte* Nachkommastelle von $f_R(3)$, addieren zu dieser Ziffer 1 und bilden falls notwendig den Modulo 10. Wir erhalten 0.1096. Weiters...
- ...

Wir erhalten am Ende eine reelle Zahl $r \in \mathbb{R}$, welche kein Urbild[17] hat:

- Das Urbild kann nicht 0 sein, da sich $f_R(0)$ und r in der *ersten* Nachkommastelle unterscheiden.
- Das Urbild kann nicht 1 sein, da sich $f_R(1)$ und r in der *zweiten* Nachkommastelle unterscheiden.
- Das Urbild kann nicht 2 sein, da sich $f_R(2)$ und r in der *dritten* Nachkommastelle unterscheiden.
- Das Urbild kann nicht 3 sein, da sich $f_R(3)$ und r in der *vierten* Nachkommastelle unterscheiden.
- ...

Folglich kann es keine bijektive Abbildung $f_R : \mathbb{N} \to \mathbb{R}$ geben.[18] □

Wir sehen also, dass $|\mathbb{R}| > |\mathbb{N}|$ gelten muss. Wir nennen $\mathbb{R}$ **überabzählbar unendlich** und definieren $|\mathbb{R}| = \mathfrak{c}$ (gesprochen: Kontinuum).

[16] um bspw. π oder e korrekt zu notieren

[17] Siehe Kapitel 6

[18] Bekannt als *Cantors zweites Diagonalargument*

4.3 Komplexe Zahlen $\mathbb{C}$

Definition 4.3.1 (imaginäre Einheit)**.** Unter der **imaginären Einheit** verstehen wir die Zahl i und definieren diese als $i^2 = -1$.

Definition 4.3.2 (Komplexe Zahlen)**.** Basierend auf der Menge der reellen Zahlen und der imaginären Einheit definieren wir die Menge der **komplexen Zahlen** als

$$\mathbb{C} = \{c | c = a + b \cdot i \text{ mit } a, b \in \mathbb{R}\}$$

Definition 4.3.3 (Realteil, Imaginärteil)**.** Sei $c \in \mathbb{C}$, also $c = a + b \cdot i$ mit $a, b \in \mathbb{R}$. Dann definieren wir den **Realteil** $\Re(c)$ der komplexen Zahl c als $\Re(c) = a$ und den **Imaginärteil** $\Im(c) = b$[19]

[19] i gehört *nicht* zum Imaginärteil: $\Im(c) = b \neq b \cdot i$

Definition 4.3.4 ((komplexe) Konjugation)**.** Sei $c \in \mathbb{C}$, also $c = a + b \cdot i$ mit $a, b \in \mathbb{R}$. Dann definieren wir die **(komplexe) Konjugation** von c als $\overline{c} = a - b \cdot i$

Definition 4.3.5 (Betrag einer komplexen Zahl)**.** Sei $c \in \mathbb{C}$, also $c = a + b \cdot i$ mit $a, b \in \mathbb{R}$. Dann definieren wir den **Betrag (der komplexen Zahl)** c als $|c| = |a+b\cdot i| = \sqrt{a^2 + b^2}$

Satz 4.3.1. Sei $c \in \mathbb{C}$. Dann gilt:

$$|c|^2 = c \cdot \overline{c}$$

Beweis. Wir benutzen $c = a + b \cdot i$ und $\overline{c} = a - b \cdot i$ um $c \cdot \overline{c}$ umzuschreiben: $c \cdot \overline{c} = (a + b \cdot i) \cdot (a - b \cdot i)$. Mithilfe der binomischen Formel[20] erhalten wir:

[20] Verweis erforderlich.

$$c \cdot \overline{c} = a^2 - a \cdot b \cdot i + a \cdot b \cdot i - b^2 \cdot i^2 = a^2 - b^2 \cdot i^2$$

Mithilfe der Definition der imaginären Einheit erhalten wir

$$c \cdot \overline{c} = a^2 - b^2 \cdot i^2 = a^2 - b^2 \cdot (\sqrt{-1})^2 = a^2 - b^2 \cdot (-1) = a^2 + b^2$$

Setzen wir nun in $|c|^2$ ein:

$$|c|^2 = |a + b \cdot i|^2 = (\sqrt{a^2 + b^2})^2 = a^2 + b^2$$

Wir sehen, dass die beiden Seiten gleich sind. □

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.[21]

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

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.

Um auszudrücken dass beispielsweise die Elemente 0 und 1 die Relation $<$ erfüllen können wir eine der folgenden Schreibweisen verwenden: $R_<(0,1)$[22] oder $(0,1) \in R_<$ oder schlicht $0 < 1$.

[22] 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**[23] verstehen wir eine Relation R auf einer Menge M welche folgende Eigenschaften erfüllt:

[23] 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 "⇐": 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 "⇒" 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 $z_1 - z_1$[24] 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 $(z_2 \mod n) = (z_3 \mod n)$[25], 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.

□

[24] Nein, kein Tippfehler

[25] 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**[26] verstehen wir eine Relation R auf einer Menge M welche folgende Eigenschaften erfüllt:

[26] 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 $m \in M$.[27]

[27] 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 $f(m) = n$.

Definition 6.0.8 (Nullstelle)**.** Sei $f : M \to N, m \mapsto f(m)$ eine Funktion wobei $0 \in N$. Unter einer **Nullstelle** m_0 verstehen wir ein Element $m_0 \in M$ sodass $f(m_0) = 0$.

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.[28]

[28] 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**[29]) Gruppe.

[29] 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: [30]

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

  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: $g_1 * g_1^{-1} = e$ □

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

- 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 $(G, *)$[31], wenn folgende Eigenschaften erfüllt sind:

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

- Für jedes in U enthaltene Element ist auch dessen inverses Element in U:[32]

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

[32] 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:

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

Definition 7.1.4 (Halbgruppe)**.** Unter einer **Halbgruppe** verstehen wir eine Menge G auf welcher eine Operation $* : G \times G \to G$ definiert ist. Dabei muss die folgende Eigenschaft erfüllt sein:

- 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.

Eine Halbgruppe muss also kein neutrales Element, noch für jedes Element von G ein inverses Element beinhalten.[33]

[33] bspw. ist schon $(\emptyset, +)$ eine Halbgruppe, da G auch leer sein kann

Definition 7.1.5 (Monoid)**.** Unter einem **Monoid** verstehen wir eine Halbgruppe $(G, *)$ welche zusätzlich die folgende Eigenschaft erfüllt:

- 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.

Im Gegensatz zur Gruppe muss ein Monoid also nicht für jedes enthaltene Element ein inverses Element beinhalten.[34]

[34] bspw. ist $(\mathbb{N}, +)$ ein Monoid mit neutralem Element 0

Definition 7.1.6 (zyklische Gruppe, erzeugendes Element)**.** Es sei $(G, *)$ eine Gruppe, wobei G endlich ist, d.h. $|G| < \aleph_0$. Es sei $n = |G|$ die Anzahl der endlich vielen Elemente in G. Wir nennen $(G, *)$ nun eine **zyklische Gruppe** falls es ein $g \in G$ gibt, sodass $G = \{g, g^2, g^3, ..., g^n\}$, wobei

$$g^i = \underbrace{g * g * ... * g}_{i\text{-mal}}$$

und g als **erzeugendes Element** von G bezeichnet wird.

Satz 7.1.2. Es sei $(G, *)$ eine zyklische Gruppe wobei $n = |G|$. Dann gilt:

$$g^n = e$$

wobei e das neutrale Element von $(G, *)$ ist.

Beweis. Angenommen es gilt $g^m = e$ für ein $m < n$. Dann wäre $g^m * g = e * g = g$. Dadurch würden allerdings nicht mehr alle Elemente aus G getroffen werden, g wäre folglich nicht erzeugendes Element von G. □

Permutationsgruppen

Definition 7.1.7 (Permutation, Zyklus)**.** Sei $n \in \mathbb{N}^*$ und M die Menge $\{1, ..., n\}$. Unter einer **Permutation** verstehen wir schlicht eine bestimmte Anordnung der Elemente aus M, wobei es sich dabei um eine bijektive Abbildung handelt, bei der die Zahlen $1, ..., n$ auf eine andere Anordnung abgebildet werden.

Beispiel: Sei $n = 5$, so können wir beispielsweise Permutationen so anschreiben, dass wir in eine Zeile die "originalen" Elemente anschreiben und darunter eine Anordnung dieser:

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$$

Zur Vereinfachung schreiben wir einfach die Abfolge auf, welche Elemente bei wiederholter Anwendung einer Permutation durchlaufen, wobei das letzte Element wieder auf das erste abgebildet wird. Beispielsweise wird in p_1 1 auf 4 abgebildet, die 4 auf die 5, 5 auf 2, 2 auf 3 und 3 wieder zurück auf 1. Eine solche Abfolge bezeichnen wir als **Zyklus**. Ein Zyklus ist dabei immer eine Permutation, eine Permutation kann aber aus mehreren Zyklen bestehen. Gibt es mehrere Zyklen innerhalb einer Permutation, so schreiben wir diese separat hintereinander auf, wobei diese durch den "$\circ$" Operator verknüpft werden. Für unser Beispiel:

$$p_1 = \begin{pmatrix} 1 & 4 & 5 & 2 & 3 \end{pmatrix} \qquad p_2 = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 5 & 4 \end{pmatrix}$$

Satz 7.1.3. Anhand des Beispiels aus Definition 7.1.7 sehen wir: Es kann *mehrere* Schreibweisen für die gleiche Permutation geben: $\begin{pmatrix}1 & 2\end{pmatrix}$ ist das gleiche wie $\begin{pmatrix}2 & 1\end{pmatrix}$

Satz 7.1.4. Die Operation "$\circ$" auf Permutationen ist *nicht* kommutativ.

Beweis. Wir beweisen diesen Satz indirekt. Es seien $p_1 = \begin{pmatrix}1 & 2\end{pmatrix}$ und $p_2 = \begin{pmatrix}2 & 3\end{pmatrix}$ aus S_3. Nun nehmen wir an dass $p_1 \circ p_2 = p_2 \circ p_1$. Wir berechnen beide Seiten der Gleichung:

$$p_1 \circ p_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3 & 2\end{pmatrix}$$

$$p_2 \circ p_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$$

Wir haben ein Gegenbeispiel für unsere Annahme gefunden, folglich ist $p_1 \circ p_2 \neq p_2 \circ p_1$ und die Operation "$\circ$" ist *nicht* kommutativ. □

Definition 7.1.8 (Transposition)**.** Unter einer **Transposition** verstehen wir einen Zyklus mit genau 2 Elementen: $t = \begin{pmatrix}t_1 & t_2\end{pmatrix}$

Satz 7.1.5. Ein Zyklus $z = \begin{pmatrix}z_1 & ... & z_m\end{pmatrix}$ lässt sich immer als eine Hintereinanderausführung von Transpositionen $t_1 \circ ... \circ t_{m-1}$ mit $t_i = \begin{pmatrix}p_i & p_{i+1}\end{pmatrix}$aufschreiben.

Definition 7.1.9 (Permutationsgruppe)**.** Sei $n \in \mathbb{N}^*$ und M die Menge $\{1, ..., n\}$. Wir definieren nun die Menge S_n der sogenannten **Permutationsgruppe**, wobei S_n alle möglichen Permutationen von M beinhaltet, also ist S_n genau genommen eine Menge von (bijektiven) Abbildungen.[35]

[35] Wir werden später sehen dass $|S_n| = n!$ gilt, wobei $n! = 1 \cdot ... \cdot n$ definiert ist

Satz 7.1.6. Sei $n \in \mathbb{N}^*$ und S_n die Menge aller Permutationen für n Elemente aus $M = \{1, ..., n\}$. Dann ist die Permutationsgruppe $(S_n, \circ)$ eine Gruppe.

Beweis.

- Neutrales Element: Für alle Permutationen $p \in S_n$ gilt, dass $e = ()$ (die "leere" Permutation bei der jedes Element auf sich selbst abgebildet wird) als neutrales Element dient:
$$p \circ e = e \circ p = p$$
- Inverses Element: Für jede Permutation $p \in S_n$ gibt es eine Permutation p^{-1} welche die Elemente in ihre ursprüngliche Reihenfolge permutiert. Dies erscheint plausibel da S_n jede mögliche Permutation enthält und es nur endlich viele Permutationen für ein endliches M gibt.
- Assoziativ: Es seien p_1, p_2, p_3 Permutationen aus S_n. Des Weiteren sei $m \in M$. Wir wollen zeigen, dass die Anwendung von $(p_1 \circ p_2) \circ p_3$ auf m das gleiche Ergebnis liefert wie $p_1 \circ (p_2 \circ p_3)$:
$$((p_1 \circ p_2) \circ p_3)(m) = (p_1 \circ (p_2 \circ p_3))(m)$$

□

7.2 Ringe

Definition 7.2.1 (Ring, distributiv)**.** 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, Einselement)**.** Es sei $(R, \oplus, \odot)$ ein Ring. Erfüllt $(R, \oplus, \odot)$ nun zusätzlich die Eigenschaft

- Neutrales Element (bezüglich $\odot$): Es existiert ein $e \in R$ sodass $e \odot r = r \odot e = r$ für alle $r \in R$ gilt. Dieses Element e nennen wir neutrales Element (bezüglich $\odot$) in R oder auch **Einselement**.

so nennen wir $(R, \oplus, \odot)$ einen **unitären Ring** (oder auch **Ring mit Eins**).

Definition 7.2.4 (Unterring, Teilring)**.** Es sei $(R, \oplus, \odot)$ ein Ring und $U \subseteq R$, so ist $(U, \oplus, \odot)$ ein **Unterring** (auch **Teilring**) von $(R, \oplus, \odot)$[36], wenn folgende Eigenschaften erfüllt sind:

- $(U, \oplus)$ ist eine Untergruppe von $(R, \oplus)$
- Die Verknüpfung zweier Elemente durch $\odot$ aus U ist ebenfalls in U:

$$\forall r_1, r_2 \in R : (r_1, r_2 \in U) \Rightarrow (r_1 \odot r_2 \in U)$$

[36] bspw. ist $(\mathbb{Q}, +, \cdot)$ ein Unterring von $(\mathbb{R}, +, \cdot)$

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 die 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 $z_1 \cdot z_2$).[37]

[37] Dabei ist es rechnerisch egal, wann der Modulo gebildet wird: $[344 \cdot 6 - 48 \cdot 2]_7 = [1968]_7 = [1]_7$ ist das gleiche wie $[1 \cdot 6 - 6 \cdot 2]_7 = [6-12]_7 = [6-5]_7 = [1]_7$

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:

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

7.3 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"[38] 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.

[38] "1" statt 1 da es um "die Idee hinter 1 als neutrales Element" und nicht speziell um $1 \in \mathbb{N}$ geht. Siehe auch Definition 7.2.3

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

Anders lässt sich ein Körper als ein kommutativer Ring mit Eins $(K, \oplus, \odot)$ der *ungleich* dem Nullring $(\emptyset, \oplus, \odot)$ ist definieren, für welchen zusätzlich gilt, dass K jedes $k \in K$ mit $k \neq 0$ ein inverses Element bezüglich der Operation "$\odot$" enthält.

Definition 7.3.2 (endlicher Körper,Galoiskörper)**.** Unter einem **endlichen Körper** (auch **Galoiskörper**[39]) verstehen wir einen Körper $(K, \oplus, \odot)$ für den gilt, dass die Menge K endlich ist, d.h. sie enthält endlich viele Elemente. Für ihre Kardinalität gilt: $|K| < |\mathbb{N}| = \aleph_0$

[39] benannt nach Evariste Galois (1811-1832)

Satz 7.3.1. Sei $\mathbb{Z}/n\mathbb{Z}$ ein Restklassenring mit $n \in \mathbb{N}^*$. Nun gilt: Genau dann wenn n eine Primzahl[40] ist, ist $\mathbb{Z}/n\mathbb{Z}$ ein endlicher Körper.

[40] Verweis erforderlich

7.4 Homomorphismen

Definition 7.4.1 ((Gruppen-)Homomorphismus, verknüpfungsverträglich)**.** Es seien $(G, *)$ und $(H, *)$ Gruppen und $\varphi : G \to H$ eine Abbildung, wobei für alle $g_1, g_2 \in G$ gilt:

$$\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$$

dann nennen wir φ einen **(Gruppen-)Homomorphismus**. Die Besonderheit eines Homomorphismus ist, dass dieser **verknüpfungsverträglich** ist, d.h. die Eigenschaften von Operationen bleiben erhalten.[41]

[41] Dies ist nützlich, da man so zum Rechnen in eine andere Struktur wechseln kann, wobei das Ergebnis davon nicht beeinflusst wird

Satz 7.4.1. Es sei $\varphi : G \to H$ ein Gruppen-Homomorphismus. Es gilt:

- Das neutrale Element aus G wird immer auf das neutrale Element aus H abgebildet:

  $$\varphi(e_G) = e_H$$

  Beweis.

  $$\begin{aligned} e_H &= \varphi(e_G) * \varphi(e_G)^{-1} = \\ &= \varphi(e_G * e_G) * \varphi(e_G)^{-1} = \\ &= (\varphi(e_G) * \varphi(e_G)) * \varphi(e_G)^{-1} = \\ &= \varphi(e_G) * (\varphi(e_G) * \varphi(e_G)^{-1}) = \\ &= \varphi(e_G) * e_H = \\ &= \varphi(e_G) \end{aligned}$$

  □

- Der Homomorphismus bewahrt die Eigenschaft der inversen Elemente:

  $$\varphi(g^{-1}) = \varphi(g)^{-1} \text{ für alle } g \in G$$

Definition 7.4.2 ((Ring-)Homomorphismus)**.** Es seien $(R, \oplus, \odot)$ und $(S, \oplus, \odot)$ Ringe und $\varphi : R \to S$ eine Abbildung, wobei für alle $r_1, r_2 \in R$ gilt:

$$\varphi(r_1 \oplus r_2) = \varphi(r_1) \oplus \varphi(r_2)$$

$$\varphi(r_1 \odot r_2) = \varphi(r_1) \odot \varphi(r_2)$$

dann nennen wir φ einen **(Ring-)Homomorphismus**.

Definition 7.4.3 (Kernel, Kern, Image, Bild)**.** Es sei $\varphi : A \to B$ ein (Gruppen- oder Ring-)Homomorphismus. So nennen wir

- $\text{Ker}(\varphi) = \{a \in A | \varphi(a) = 0\}$ den **Kern** (engl. **Kernel**) von φ[42]
- $\text{Im}(\varphi) = \{b \in B | \exists a \in A : \varphi(a) = b\}$ das **Bild** (engl. **Image**) von φ[43]

[42] "Ker" ist die Abkürzung von "Kernel"

[43] "Im" ist die Abkürzung von "Image"

Definition 7.4.4 (Isomorphismus)**.** Es sei $\varphi : A \to B$ ein *bijektiver* (Gruppen- oder Ring-)Homomorphismus. Dann nennen wir φ einen **Isomorphismus**.

Beispiel für einen Ring-Homomorphismus

Satz 7.4.2. Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, z \to z \mod n$ ist ein Ring-Homomorphismus.

Beweis. Es seien $z_1 = q_1 \cdot n + r_1$ und $z_2 = q_2 \cdot n + r_2$ ganze Zahlen. Dann gilt:

$$\begin{aligned}\varphi(z_1 + z_2) &= \varphi(q_1 \cdot n + r_1 + q_2 \cdot n + r_2) = \\ &= \varphi((q_1 + q_2) \cdot n + (r_1 + r_2)) = \\ &= r_1 + r_2 = \\ &= \varphi(q_1 \cdot n + r_1) + \varphi(q_2 \cdot n + r_2) = \varphi(z_1) + \varphi(z_2)\end{aligned}$$

$$\begin{aligned}\varphi(z_1 \cdot z_2) &= \varphi((q_1 \cdot n + r_1) \cdot (q_2 \cdot n + r_2)) = \\ &= \varphi(q_1 \cdot q_2 \cdot n \cdot n + q_1 \cdot r_2 \cdot n + q_2 \cdot r_1 \cdot n + r_1 \cdot r_2) = \\ &= \varphi((q_1 \cdot q_2 \cdot n + q_1 \cdot r_2 + q_2 \cdot r_1) \cdot n + (r_1 \cdot r_2)) = \\ &= (r_1 \cdot r_2) \mod n = \\ &= [r_1 \cdot r_2] = \\ &= [(r_1 \mod n) \cdot (r_2 \mod n)] = \\ &= \varphi(q_1 \cdot n + r_1) \cdot \varphi(q_2 \cdot n + r_2) = \varphi(z_1) \cdot \varphi(z_2)\end{aligned}$$

□

8 Polynome

8.1 Allgemein

Definition 8.1.1 (Polynom, Polynomfunktion)**.** Sei $(R, +, \cdot)$ ein Ring und seien $a_0, ..., a_n \in R$. So nennen wir die Abbildung

$$f : R \to R, x \mapsto a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n$$

eine **Polynomfunktion** über R und den Term $a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n$ ein **Polynom** über R.

Definition 8.1.2 (Grad eines Polynoms)**.** Sei $(R, +, \cdot)$ ein Ring und $p = a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n$ mit $a_0, ..., a_n \in R$ ein Polynom über R mit dem Argument $x \in R$. Unter dem **Grad des Polynoms** grad(p) verstehen wir das größte i für das gilt dass $a_i \neq 0$. Ist also $a_n \neq 0$, so ist das Polynom vom Grad n.

Definition 8.1.3 (Polynomring)**.** Sei $(R, +, \cdot)$ ein Ring, so bezeichnen wir die Menge aller Polynome über R mit einem variablen $x \in X$ als $R[X]$. Des Weiteren seien $p_1, p_2 \in R[X]$, so definieren wir die Operationen $+$ und $\cdot$ als

- $p_1 + p_2 = (p_1 + p_2)(x) = p_1(x) + p_2(x)$
- $p_1 \cdot p_2 = (p_1 \cdot p_2)(x) = p_1(x) \cdot p_2(x)$

für alle $x \in X$. Wir nennen dann den Ring $(R[X], +, \cdot)$ einen **Polynomring** über R.

8.2 Polynomdivision

Definition 8.2.1 (Polynomdivision)**.** Sei $(K, +, \cdot)$ ein Körper und $K[X]$ ein Polynomring über K. Des Weiteren seien $p_1, p_2 \in K[X]$ mit $p_2 \neq 0$, so verstehen wir unter der **Polynomdivision** von p_1 durch p_2 das Aufsuchen von $q, r \in K[X]$ sodass $p_1 = q \cdot p_2 + r$ mit grad$(r) <$ grad(p_2).

Beispiel: Sei $p_1 = 6 \cdot x^2 + 2 \cdot x + 8$ und $p_2 = 2 \cdot x + 8$. Die Polynomdivision $p_1 : p_2$

$$\begin{array}{rl} (6 \cdot x^2 & +2 \cdot x + 8) : (2 \cdot x + 8) = 3 \cdot x - 11 \\ -(6 \cdot x^2 & +24 \cdot x) \\ \hline 0 \cdot x^2 & -22 \cdot x + 8 \\ & -(-22 \cdot x - 88) \\ \hline & 0 \cdot x + 96 \end{array}$$

Gibt uns den Quotienten $q = 3 \cdot x - 11$ und den Rest $r = 96$.

Definition 8.2.2 (Wurzel einer Polynomfunktion)**.** Sei $(K, \oplus, \odot)$ ein Körper und $f : K \to K$ eine Polynomfunktion über K. Unter einer **Wurzel**[44] k_0 **der Polynomfunktion** f verstehen wir eine Nullstelle von f: $f(k_0) = 0$

[44] Nicht zu verwechseln mit der Wurzel beim Wurzelziehen, bspw. der Wurzel aus 2: $\sqrt{2}$

Definition 8.2.3 (Linearfaktor)**.** Sei $(K, \oplus, \odot)$ ein Körper und $f : K \to K$ eine Polynomfunktion über K. Wir nennen das Polynom von f einen **Linearfaktor** wenn dieses von der Form $x + a_0$ mit $a_0 \in K$.

Satz 8.2.1. Sei $f : \mathbb{R} \to \mathbb{R}$ eine Polynomfunktion über $\mathbb{R}$. Hat f nun die Wurzel (Nullstelle) x_0 (also $f(x_0) = 0$), so lässt sich das Polynom von f ohne Rest durch den Linearfaktor $(x - x_0)$ dividieren, d.h. es gibt ein Polynom $q \in K[\mathbb{R}]$ sodass für alle $x \in \mathbb{R}$ gilt:

$$f(x) = q(x) \cdot (x - x_0) + r(x) \text{ mit } r(x) = 0 \to f(x) = q(x) \cdot (x - x_0)$$

Wir sagen, wir haben die Nullstelle x_0 (oder auch den Linearfaktor $x - x_0$) **abgespalten**[45].

[45] Es gibt Polynome über $\mathbb{R}$ bei denen dies nicht möglich ist, bspw. $x^2 + 1$ (da diese keine Wurzel $x_0 \in \mathbb{R}$ besitzen)

Beweis. Wir wollen zeigen, dass wenn x_0 Wurzel der Polynomfunktion f ist, das Polynom von f sich in ein Polynom bestehend aus dem Linearfaktor $(x - x_0)$, multipliziert mit einem weiteren unbekannten Polynom q (dem Quotienten der Polynomdivision), aufspalten lässt mit Rest 0:

$$f(x) = q(x) \cdot (x - x_0)$$

Wir wissen, dass der Grad des Polynoms $(x - x_0)$ gleich 1 ist (da kein $a_i \cdot x^i$ mit $i > 1$ und $a_i \neq 0$ vorkommt) und folglich der Grad von dem "Rest-Polynom" r kleiner 1 sein muss, folglich ist $\text{grad}(r) = 0$ und das Polynom r lässt sich durch eine Konstante r_0 beschreiben. Es folgt also:

$$f(x) = q(x) \cdot (x - x_0) + r_0$$

Außerdem wissen wir: $f(x_0) = 0$, also $f(x_0) = q(x_0) \cdot (x - x_0) + r_0 = q(x_0) \cdot 0 + r_0 = r_0$, woraus folgt: $r_0 = 0$ □

Definition 8.2.4 (Leitkoeffizient, normiertes Polynom)**.** Sei $(K, \oplus, \odot)$ ein Körper und $p \in K[X]$ ein Polynom über K mit $p = a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n$ und $a_0, ..., a_n \in K$. Wir nennen p ein **normiertes Polynom** wenn der sogenannte **Leitkoeffizient** a_n (der Koeffizient von x^n wobei $\text{grad}(p) = n$) gleich dem Einselement ist.

Definition 8.2.5 ((ir)reduzibles Polynom)**.** Sei $(K, \oplus, \odot)$ ein Körper und $p \in K[X]$ ein Polynom über K. Wir nennen p ein **irreduzibles Polynom** wenn es *kein* Polynom $q \in K[X]$ mit $0 < \text{grad}(q) < \text{grad}(p)$ gibt, sodass p durch q ohne Rest geteilt werden kann. Anders formuliert gibt es *keine* Polynome $p_1, p_2 \in K[X]$ sodass $p = p_1 \cdot p_2$. Ansonsten nennen wir p ein **reduzibles Polynom**.

Satz 8.2.2. Sei $(K, \oplus, \odot)$ ein Körper und $p \in K[X]$ ein normiertes Polynom über K. Es gilt für *jedes beliebige* p:

- p lässt sich *eindeutig* als Produkt von normierten irreduziblen Polynomen aufschreiben
- Sei $p = p_1 \cdot ... \cdot p_m$, so gilt: $\text{grad}(p) = \text{grad}(p_1) + ... + \text{grad}(p_m)$

8.3 Der Körper $(\mathbb{C}, +, \cdot)$

Definition 8.3.1 (algebraisch abgeschlossen)**.** Sei $(K, +, \cdot)$ ein Körper. Wir nennen diesen Körper **algebraisch abgeschlossen** wenn jede beliebige Polynomfunktion $f : K \to K$ über K mindestens eine Wurzel $x_0 \in K$ besitzt.

Satz 8.3.1 (Fundamentalsatz der Algebra)**.** Der Körper $(\mathbb{C}, +, \cdot)$ ist algebraisch abgeschlossen.

Satz 8.3.2. Sei $f : \mathbb{C} \to \mathbb{C}$ eine beliebige Polynomfunktion über $\mathbb{C}$ mit Grad n. Aus Satz 8.3.1 folgt nun, dass jede solche Funktion f mindestens eine Nullstelle $x_0 \in \mathbb{C}$ besitzt, welche sich laut Satz 8.2.1 vom Polynom von f ohne Rest abspalten lässt. Dabei erhalten wir als Quotienten ein neues Polynom f', wobei gilt: $f = f' \cdot (x - x_0)$. Dies lässt sich immer weiter fortsetzen, bis f ausschließlich in n Linearfaktoren (und einen zusätzlichen Faktor $a \in \mathbb{C}$) aufgespalten wurde:

$$f = a \cdot (x - x_0) \cdot ... \cdot (x - x_{n-1})$$

Satz 8.3.3. Aus Satz 8.3.2 folgt, dass ein Polynom (über $\mathbb{C}$) maximal n Nullstellen haben kann (wobei sich Nullstellen wiederholen dürfen)

9 Vektorräume

Definition 9.0.1 ((reeller/komplexer)Vektorraum, Vektor)**.** Sei $(K, +, \cdot)$ ein Körper. Ein sogenannter **Vektorraum** V mit Skalaren[46] aus K besteht dann aus einer kommutativen Gruppe $(V, +)$ und einer zusätzlichen Operation, der **skalaren Multiplikation**, welche die Multiplikation "$\cdot$" aus $(K, +, \cdot)$ erweitert: $\cdot : K \times V \to V, (k, v) \mapsto k \cdot v$, wobei für alle $v_1, v_2 \in V$, $k_1, k_2 \in K$ gilt:

- Assoziativ: $k_1 \cdot (k_2 \cdot v_1) = (k_1 \cdot k_2) \cdot v_1$
- Neutrales Element: $1 \cdot v_1 = v_1$
- Distributiv 1: $k_1 \cdot (v_1 + v_2) = k_1 \cdot v_1 + k_1 \cdot v_2$
- Distributiv 2: $(k_1 + k_2) \cdot v_1 = k_1 \cdot v_1 + k_2 \cdot v_1$

Die Elemente von V nennen wir **Vektoren**. Für $K = \mathbb{R}$ reden wir von einem **reellen Vektorraum** (Vektorraum über $\mathbb{R}$, $V(\mathbb{R})$, $\mathbb{R}$-Vektorraum), bei $K = \mathbb{C}$ von einem **komplexen Vektorraum**.

[46] Mathematische Objekte welche sich allein durch einen einzigen Wert beschreiben lassen, bspw. 0, 1, π, etc.

Definition 9.0.2 (Teilraum, Untervektorraum, Unterraum)**.** Sei V ein Vektorraum über einen Körper $(K, +, \cdot)$ und $U \subseteq V$ mit $U \neq \emptyset$. Bildet U mit den gleichen Verknüpfungen aus V ebenfalls einen Vektorraum über K, so nennen wir U einen **Untervektorraum** (auch **Teilraum** oder nur **Unterraum**).

Definition 9.0.3 (Linearkombination)**.** Sei V ein Vektorraum über einen Körper $(K, +, \cdot)$, $k_1, ..., k_m \in K$ beliebig und $v_1, ..., v_m \in V$ beliebig. Dann nennen wir

$$k_1 \cdot v_1 + ... + k_m \cdot v_m$$

eine **Linearkombination** von $v_1, ..., v_m$.

Definition 9.0.4 (Lineare Hülle)**.** Sei V ein Vektorraum über einen Körper $(K, +, \cdot)$. Des Weiteren seien $v_1, ..., v_m \in V$ beliebig. Wir bezeichnen dann

$$\text{span}(v_1, ..., v_m) = \{k_1 \cdot v_1 + ... + k_m \cdot v_m | k_1, ..., k_m \in K \text{beliebig}\}$$

als die **lineare Hülle** von $v_1, ..., v_m$. Diese Menge enthält alle möglichen Linearkombinationen von $v_1, ..., v_m$ und bildet immer einen Untervektorraum von V.

Definition 9.0.5 (Lineare Abbildung)**.** Es seien V, W Vektorräume über einen Körper $(K, +, \cdot)$. Wir bezeichnen eine Abbildung $f : V \to W$ als **lineare Abbildung**, wenn für alle $v_1, v_2 \in V$ und alle $k \in K$ gilt:

- $f(v_1 + v_2) = f(v_1) + f(v_2)$
- $f(k \cdot v_1) = k \cdot f(v_1)$

Definition 9.0.6 (Verketten von linearen Abbildungen)**.** Es seien f_1, f_2 lineare Abbildungen. Beim **Verketten der beiden linearen Abbildungen** f_1 und f_2 erhalten wir ebenfalls wieder eine lineare Abbildung und bezeichnen diese Verkettung als $f_1 \circ f_2$, wobei *zuerst* f_2 und *danach* f_1 ausgeführt wird: $f_1(f_2(x))$.

Satz 9.0.1. Es seien f_1, f_2 bijektive lineare Abbildungen. Dann ist auch $f_1 \circ f_2$ eine bijektive lineare Abbildung.

Definition 9.0.7 (Kern/Kernel und Bild/Image einer linearen Abbildung)**.** Es seien V, W Vektorräume und $f : V \to W$ eine lineare Abbildung. So nennen wir analog zu Definition 7.4.3

- $\text{Ker}(f) = \{v \in V | f(v) = 0\}$ den **Kern** (engl. **Kernel**) von f
- $\text{Im}(f) = \{w \in W | \exists v \in V : f(v) = w\}$ das **Bild** (engl. **Image**) von f

9.1 Lineare (Un)Abhängigkeit, Basis & Dimension

Definition 9.1.1 (Lineare (Un)Abhängigkeit eines Vektors)**.** Es seien $v_1, ..., v_n$ n Vektoren eines Vektorraums V über einen Körper $(K, +, \cdot)$. Gibt es nun $k_1, ..., k_{n-1} \in K$ sodass

$$v_n = k_1 \cdot v_1 + ... + k_{n-1} \cdot v_{n-1}$$

wobei mindestens ein $k_i \neq 0$, so nennen wir v_n **linear abhängig** von $v_1, ..., v_{n-1}$. Das heißt, dass die Aussagen

$$v_n \text{ lässt sich als Linearkombination von } v_1, ..., v_{n-1} \text{ aufschreiben}$$

und

$$v_n \in \text{span}(\{v_1, ..., v_{n-1}\})$$

und

$$v_n \text{ist linear abhängig von } v_1, ..., v_{n-1}$$

äquivalent sind.[47] Falls es *keine* solchen $k_1, ..., k_{n-1} \in K$ mit mindestens einem $k_i \neq 0$ gibt, so nennen wir v_n **linear unabhängig** von $v_1, ..., v_{n-1}$.

[47] v_n muss natürlich nicht unbedingt der "letzte" Vektor sein, sondern schlicht ein beliebiger Vektor aus unserer Menge

Definition 9.1.2 (Lineare (Un)Abhängigkeit einer Menge von Vektoren)**.** Es seien $v_1, ..., v_n$ n Vektoren eines Vektorraums V über einen Körper $(K, +, \cdot)$. Wir nennen die Menge $\{v_1, ..., v_n\}$ **linear unabhängig**, wenn für jede Linearkombination dieser Vektoren gilt:

$$k_1 \cdot v_1 + ... + k_n \cdot v_n = 0 \Rightarrow k_1 = ... = k_n = 0$$

Die Menge $\{v_1, ..., v_n\}$ heißt **linear abhängig** wenn sie nicht linear unabhängig ist.

Satz 9.1.1. Es seien $v_1, ..., v_n$ n Vektoren eines Vektorraums V über einen Körper $(K, +, \cdot)$. Es gilt: Die Menge $\{v_1, ..., v_n\}$ ist dann linear abhängig, wenn ein Vektor $v_i \in \{v_1, ..., v_n\}$ linear abhängig ist von den restlichen Vektoren $\{v_1, ..., v_n\} \setminus \{v_i\}$.

Satz 9.1.2. Es seien $v_1, ..., v_n$ n Vektoren eines Vektorraums V über einen Körper $(K, +, \cdot)$. Des Weiteren sei v_i ein beliebiger Vektor aus $\{v_1, ..., v_n\}$. Es gilt:

$$v_i \in \text{span}(\{v_1, ..., v_n\} \setminus \{v_i\}) \Rightarrow \text{span}(\{v_1, ..., v_n\}) = \text{span}(\{v_1, ..., v_n\} \setminus \{v_i\})$$

Definition 9.1.3 (Basis)**.** Sei V ein Vektorraum. Eine Teilmenge W von V, welche die Eigenschaften

- $\text{span}(W) = V$[48]
- Die Menge W ist linear unabhängig

erfüllt, nennen wir **Basis** von V.

[48] Wir sagen: "*B erzeugt V*"

Definition 9.1.4 (Dimension)**.** Sei V ein Vektorraum und $W = \{w_1, ..., w_n\}$ eine (endliche) Basis von V. Dann sagen wir dass n ($n = |W|$) die **Dimension** von V ist: $\dim(V) = n$. Der *Nullraum* $\{0\}$ hat Dimension 0.

Satz 9.1.3. Sei V ein Vektorraum mit $\dim(V) = n$. Dann hat jede (endliche) Basis von V n Elemente.

Satz 9.1.4. Sei V ein Vektorraum mit $\dim(V) = n$. Es ist nicht möglich eine linear unabhängige Menge von $n + 1$ (oder mehr) Vektoren $v_i \in V$ zu finden.

Satz 9.1.5. Sei V ein Vektorraum und $W \subseteq V$ ein Untervektorraum. Folgende Aussagen sind dann äquivalent:[49]

- W ist eine Basis von V
- W ist eine maximale linear unabhängige Teilmenge von V (gibt es eine linear unabhängigeTeilmenge $X \subseteq V$ und gilt $W \subseteq X$, so folgt: $W = X$)
- W ist eine *minimale Spannmenge* von V (gibt es eine Teilmenge $X \subseteq V$ sodass $\text{span}(X) = V$ und gilt $X \subseteq W$, so folgt: $W = X$)

[49] Natürlich folgt aus $W \subseteq V$ *nicht* dass W eine Basis von V ist, es gilt lediglich, dass entweder alle oder keine der Aussagen wahr sind

Satz 9.1.6. Seien V, W Vektorräume und $f : V \to W$ eine lineare Abbildung. Es gilt:

- f ist genau dann injektiv wenn $\text{Ker}(f) = \{0\}$
- $\text{Ker}(f)$ ist ein Untervektorraum von V, $\text{Im}(f)$ ein Untervektorraum von W.
- $\dim(V) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f))$
- Ist f ein Isomorphismus, so ist die Umkehrabbildung $f^{-1} : W \to V$ auch eine lineare Abbildung
- $\dim(V) = \dim(W) \Leftrightarrow f$ ist ein Isomorphismus