Lineare Algebra (Vogel)

Robin Heinemann

November 18, 2016

Contents

1 Einleitung

Übungsblätter/Lösungen: jew. Donnerstag / folgender Donnerstag Abgabe Donnerstag 9:30 50% der Übungsblätter

1.1 Plenarübung

Aufgeteilt

1.2 Moodle

Passwort: vektorraumhomomorphismus

1.3 Klausur

24.02.2017

2 Grundlagen

2.1 Naive Aussagenlogik

naive Logik: wir vewenden die sprachliche Vorstellung ($\neq$ mathematische Logik: eigne Vorlesung) Eine Aussage ist ein festehender Satz, dem genau einer der Wahrheitswerte "wahr" oder "falsch" zugeordnet werden kann. Aus einfachen Aussagen kann man durch logische Verknüpfungen kompliziertere Aussagen bilden. Angabe der Wahrheitswertes der zusammengesetzten Aussage erfolgt duch Wahrheitstafeln (liefern den Wahrheitswert der zusammengesetzten Aussage, aus dem Wahrheitswert der einzelnen Aussagen). Im folgenden seien A und B Aussagen.

- Negation (NICHT-Verknüpfung)
  - Symbol: $\$\neg$
  - Wahrheitstafel:

A	$\neg A$
w	f
f	w

  - Beispiel: A: 7 ist eine Primzahl (w) $\neg A$: 7 ist keine Primzahl (f)
- Konjunktion (UND-Verknüpfung)
  - Symbol $\wedge$
  - Wahrheitstafel:

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

- Disjunktion (ODER-Verknüpfung)
  - Symbol: $\vee$
  - Wahrheitstafel:

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

  - exklusives oder: $(A \vee B) \wedge (\neg(A \wedge B))$
- Beispiel A: 7 ist eine Primzahl (w), B: 5 ist gerade (f)
  - $A \wedge B$ 7 ist eine Primzahl und 5 ist gerade (f)
  - $A \vee B$ 7 ist eine Primzahl oder 5 ist gerade (w)
- Implikation (WENN-DANN-Verknüpfung)
  - Symbol: $\Rightarrow$
  - Wahrheitstafel:

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

  - Sprechweise: A impliziert B, aus A folgt B, A ist eine hinreichende Bedingung für B (ist $A \Rightarrow B$ wahr, dann folgt aus A wahr, B ist wahr), B ist eine notwendige Bedingung für A (ist $A \Rightarrow B$ wahr, dann kann A nur dann wahr sein, wenn Aussage B wahr ist)
  - Beispiel Es seinen $m, n \in \mathbb{N}$
    * A: m ist gerade
    * B: mn ist gerade
    * Dann gilt $\forall\, m, n \in \mathbb{N}$ $A \Rightarrow B$ wahr
      Fallunterscheidung:
      · m gerade, n gerade, dann ist A wahr, B wahr, d.h. $A \Rightarrow B$ wahr
      · m gerade, n ungerade, dann ist A wahr, B wahr, d.h. $A \Rightarrow B$ wahr
      · m ungerade, n gerade, dann ist A falsch, B wahr, d.h. $A \Rightarrow B$ wahr
      · m ungerade, n ungerade, dann ist A falsch, B falsh, d.h. $A \Rightarrow B$ wahr
- Äquivalenz (GENAU-DANN-WENN-Verknüpfung)
  - Symbol $\Leftrightarrow$

– Wahrheitstafel:

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

– Sprechweise: A gilt genau dann, wenn B gilt, A ist hinreichend und notwendig für B
Die Aussagen $A \Leftrightarrow B$ und $(A \Rightarrow B) \wedge (B \Rightarrow A)$ sind gleichbedeutend:

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
w	w	w	w	w	w
w	f	f	f	w	f
f	w	f	w	f	f
f	w	f	w	f	f
f	f	w	w	w	w

– Beispiel: Es sei n eine ganze Zahl
$A: \ n-2>1$
$B: \ n>3$
$\forall\, n \in \mathbb{N}$ gilt $A \Leftrightarrow B$ $C: \ n>0$
$D: \ n^2>0$
Für $n=-1$ ist die Äquivalenz $C \Leftrightarrow$ falsch (C falsch, D wahr)
Für alle ganzen Zahlen n gilt zumindest die Implikation $C \Rightarrow D$

2.2 Beweis

Mathematische Sätze, Bemerkungen, Folgerungen, etc. sind meistens in Form wahrer Implikationen formuliert

2.2.1 beweisen

Begründen warum diese Implikation wahr ist

2.2.2 Beweismethoden for diese Implikation $A \Rightarrow B$

- direkter Beweis ($A \Rightarrow B$)
- Beweis durch Kontraposition ($\neq B \Rightarrow \neg A$)
- Widerspruchbeweis ($\neg(A \wedge \neg B)$)

Diese sind äquivalent zueinander

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	$\neg(A \wedge \neg B)$
w	w	f	f	w	w	w
w	f	f	w	f	f	f
f	w	w	f	w	w	w
f	f	w	w	w	w	w

Beispiel m, n natürliche Zahlen

$$A: \ m^2 < n^2$$

$$B: \ m < n$$

Wir wollen zeigen, dass $A \Rightarrow B$ für alle natürlichen Zahlen m, n wahr ist

- direkter Beweis:

$$A: \ m^2 < n^2 \Rightarrow 0 < n^2 - m^2 \Rightarrow 0 < (n-m)\underbrace{(n+m)}_{>0} \Rightarrow 0 < n - m \Rightarrow m < n$$

- Beweis durch Kontraposition:

$$\neg B: \ m \geq n \Rightarrow m^2 \geq nm \wedge mn \geq n^2 \Rightarrow m^2 \geq n^2 \Rightarrow \neg A$$

- Beweis durch Widerspruch:

  $A \wedge \neg B \Rightarrow m^2 < n^2 \wedge n \leq m \Rightarrow m^2 < n^2 \wedge mn \leq m^2 \wedge n^2 \leq mn \Rightarrow mn \leq m^2 < n^2 \leq mn$

  Wiederspruch

2.3 Existenz- und Allquantor

2.3.1 Existenzquantor

$A(x) Aussage, die von Variable x abhängt
$\exists x: \ A(x)$ ist gleichbedeutend mit "Es existiert ein x, für das $A(x)$ wahr ist" (hierbei ist "existiert ein x" im Sinne von "existiert mindestens ein x" zu verstehen)
Beispiel:

$$\exists n \in \mathbb{N}: \ n > 5 \quad \text{(w)}$$

$\exists! x: \ A(x)$ ist gleichbedeutend mit "Es existiert genau ein x, für dass $A(x)$ wahr ist"

2.3.2 Allquantor

$\forall\, x: \ A(x)$ ist gleichbedeutend mit "Für alle x ist A(x) wahr" Beispiel:

$$\forall\, n \in \mathbb{N}: 4n \text{ ist gerade}$$

2.3.3 Negation von Existenz- und Allquantor

$$\neg(\exists x: \ A(x)) \Leftrightarrow \forall\, x: \ \neg A(x)$$
$$\neg(\forall\, x: \ A(x)) \Leftrightarrow \exists x: \ \neg A(x)$$

2.3.4 Spezielle Beweistechniken für Existenz und Allaussagen

- Angabe eines Beispiel, um zu zeigen, dass deine Existenzaussage wahr ist.
  Beispiel:

  $$\exists n \in \mathbb{N}: \ n > 5\text{ist wahr, denn für } n = 7 \text{ ist die Aussage } n > 5 \text{ wahr}$$

- Angabe eines Gegenbeispiel, um zu zeigen, dass eine Allausage falsch ist.
  Beispiel:

  $$\forall\, n \in \mathbb{N}: \ n \leq 5\text{ist flasch, dann für } n = 7 \text{ ist die Aussage } n \leq 5 \text{ falsch}$$

2.4 Naive Mengenlehre

Mengenbegriff nach Cantor:
Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten userer Anschauung oder useres Denkens (die Elemente genannt werden) zu einem Ganzen

2.4.1 Schreibweise

- $x \in M$, falls x ein Element von M ist
- $x \notin M$, falls x kein Element von M ist
- $M = N$, falls M und N die gleichen Elemente besitzen, $M \subseteq N \wedge N \subseteq M$

2.4.2 Angabe von Mengen

- Reihenfolge ist unrelevant (\${1,2,3}={1,3,2})
- Elemente sind wohlunterschieden $\{1, 2, 2\} = \{1, 2\}$
- Auflisten der Elemente $M = \{a, b, c, \ldots\}$
- Beschreibung der Elemente durch Eigenschaften: $M = \{x \mid E(x)\}$
  (Elemente x, für die E(x) wahr)
  - Beispiel:
    $$\{2, 4, 6, 8\} = \{x \mid x \in \mathbb{N}, x \text{ gerade}, 1 < x < 10\}$$

2.4.3 leere Menge

Die leere Menge $\emptyset$ enthält keine Elemente

Beispiel

$$\{x \mid x \in \mathbb{N}, x < -5\} = \emptyset$$

2.4.4 Zahlenbereiche

Menge der natürlichen Zahlen:

$$\mathbb{N} := \{1, 2, 3, \ldots\}$$

Menge der natürlichen Zahlen mit Null:

$$\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$$

Menge der Ganzen Zahlen:

$$\mathbb{Z} := \{0, 1, -1, 2, -2\}$$

Menge der rationalen Zahlen:

$$\mathbb{Q} := \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$$

Menge der reellen Zahlen: $\mathbb{R}$

2.4.5 Teilmenge

A, B seien Mengen.
A heißt Teilmenge von B $(A \subseteq B) \overset{\text{Def.}}{\iff} \forall\, x \in A : x \in B$ A heißt echte Teilmenge von B $(A \subset B) \overset{\text{Def.}}{\iff} A \subseteq B \wedge A \neq B$

Anmerkung Offenbar gilt für Mengen A, B:

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

$\emptyset$ ist Teilmenge jeder Menge

Beipspiel

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$$

2.4.6 Durschnitt

$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

Beispiel

$$A = \{2, 3, 5, 7\}, B = \{3, 4, 6, 7\}, A \cap B = \{3, 7\}$$

2.4.7 Vereinigung

$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

Beispiel

$$A = \{2, 3, 5, 7\}, B = \{3, 4, 6, 7\}, A \cup B = \{2, 3, 4, 5, 6, 7\}$$

2.4.8 Differenz

$$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$$

Im Fall $B \subseteq A$ nennt man $A \setminus B$ auch das Komplement von B in A und schreibt $\rfloor_A(B) = A \setminus B$

Beispiel

$$A = \{2, 3, 5, 7\}, B = \{3, 4, 6, 7\}, A \setminus B = \{2, 5\}$$

2.4.9 Bemerkung zu Vereinigung und Durschnitt

A, B seien zwei Mengen. Dann gilt

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

Beweis

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

"$\subseteq$" Sei $x \in A \cap (B \cup C)$. Dann ist $x \in A \wedge x \in B \cup C$

- 1. Fall: $x \in A \wedge x \in B$

$$\Rightarrow x \in A \cap B \Rightarrow x \in (A \cap B) \cup (A \cap C)$$

- 2. Fall $x \in A \wedge x \in C$

$$\Rightarrow x \in A \cap C \Rightarrow x \in (A \cap B) \cup (A \cap C)$$

Damit ist "$\subseteq$" gezeigt. "$\supseteq$" Sei $x∈ (A∩ B) ∪ (A∩ C)

$\Rightarrow x \in A \cap B \vee x \in A \cap C \Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Rightarrow x \in A \wedge (x \in B \vee x \in C) \Rightarrow x \in A \wedge x \in B \cup C =$

Damit ist "$\supseteq$" gezeigt.

2.4.10 Bemerkung zu Äquivalenz von Mengen

Seien A, B Mengen, dann sind äquivalent:

1. $A \cup B = B$
2. $A \subseteq B$

Beweis Wir zeigen 1) $\Rightarrow$ 2) und 2) $\Rightarrow$ 1.

1) $\Rightarrow$ 2) : Es gelte $A \cup B = B$, zu zeigen ist $A \subseteq B$Sei $x \in A \Rightarrow x \in A \wedge x \in B \Rightarrow x \in A \cup B = B$

2) $\Rightarrow$ 1) : Es gelte $A \subseteq B$, zu zeigen ist $A \cup B = B$

"$\subseteq$": Sei $x \in A \cup B \Rightarrow x \in A \vee x \in B \overset{A \subseteq B}{\Longrightarrow} x \in B$ "$\supseteq$": $B \subseteq A \cup B$ klar

2.4.11 Kartesisches Produkt

Seien A, B Mengen

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

heipt das kartesische Produkt von A und B. Hierbei ist $(a, b) = (a', b') \overset{\text{Def}}{\Longleftrightarrow} a = a' \wedge b = b'$
a = a' $\wedge$ b = b'$

Beispiel

- $$\{1, 2\} \times \{1, 3, 4\} = \{(1, 1), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4)\}$$
- $$\mathbb{R} \times \mathbb{R} = \{(x, y) | midx, y \in \mathbb{R}\} = \mathbb{R}^2$$

2.4.12 Potenzmenge

A sei eine Menge

$$\mathcal{P}(A) := \{M \mid M \subseteq A\}$$

heißt die Potenzmenge von A

Beispiel

$$\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\{1, 2, 3, 4\}\}$$

2.4.13 Kardinalität

M sei eine Menge. Wir setzen

$$|M| := \begin{cases} n & \text{falls } M \text{ eine endliche Menge ist und } n \text{ Elemente enthält} \\ \infty & \text{falls } M \text{ nicht endlich ist} \end{cases}$$

$|M|$ heißt Kardinalität von A

Beispiel

- $|\{7, 11, 16\}| = 3$
- $|\mathbb{N}| = \infty$

2.4.14 Bemerkung zu natürlichen Zahlen

Für die natürlichen Zahlen gilt das Induktionsaxiom Ist $M \subseteq N$ eine Teilmenge, für die gilt:

$$1 \in M \wedge \forall\, n \in M : n \in M \Rightarrow n+1 \in M$$

dann ist $M = \mathbb{N}$

2.4.15 Prinzip der vollständigen Induktion

Für jedes $n \in \mathbb{N}$ sei eine Aussage $A(n)$ gegeben. Die Aussagen $A(N)$ gelten für alle $n \in \mathbb{N}$, wenn man folgendes zeigen kann:

- (IA) $A(1)$ ist wahr
- (IS) Für jedes $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$

Der Schritt (IA) heißt Induktionsanfang, die Implikation $A(n) \Rightarrow A(n+1)$ heißt Induktionsschritt

Beweis Setze $M := \{n \in \mathbb{N} \mid A(n) \text{ ist wahr}\}$ Wegen (IA) ist $1 \in M$, wegen (IS) gilt: $n \in M \Rightarrow n+1 \in M$
Nach Induktionsaxiom folgt $M = \mathbb{N}$, das heißt $A(n)$ ist wahr für alle $n \in \mathbb{N}$

Beispiel Für $n \in \mathbb{N}$ sei $A(n)$ die Aussage: $1 + \ldots + n = \frac{n(n+1)}{2}$ Wir zeigen: $A(n)$ ist wahr für alle $n \in \mathbb{N}$, und zwar durch vollständige Induktion

- (IA) $A(1)$ ist wahr, denn $1 = \frac{1(1+1)}{2}$
- (IS) zu zeigen: $A(n) \Rightarrow A(n+1)$
  Es gelte $A(n)$, das heißt $1 + \ldots + n = \frac{n(n+1)}{2}$ ist wahr

  $\Rightarrow 1+\ldots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}\square$

2.5 Relationen

2.5.1 Definiton

Eine Relation auf M ist eine Teilmenge $R \subseteq M \times M$ Wir schreiben $a \sim b \overset{\text{Def}}{\Longleftrightarrow} (a,b) \in R$ ("a steht in Relation zu b")

- anschaulich: eine Relation auf M stellt eine "Beziehung" zwischen den Elementen von M her.
- Für $a, b \in M$ gilt entweder $a \sim b$ oder $a \not\sim b$, denn: entweder ist $(a,b) \in R$ oder $(a,b) \notin R$

Anmerkung Aufgrund der obigen Notation spricht man in der Regel von Relation "$\sim$" auf M als von der Relation $R \subseteq M \times M$

Beispiel \$M = {1,2,3}. Durch $R = \{(1,1),(1,2),(3,3) \subseteq M \times M\}$ ist eine Relation auf M gegeben. Es gilt dann: $1 \sim 1, 1 \sim 2, 3 \sim 3$ (aber zum Beispiel: $1 \not\sim 3, 2 \not\sim 1, 2 \not\sim 2$)

2.5.2 Eigenschaften von Relationen

M Menge, $\sim$ Relation auf M
$\sim$ heißt:

- reflexiv $\overset{\text{Def}}{\iff}$ für alle $a \in M$ gilt $a \sim a$
- symmetrisch $\overset{\text{Def}}{\iff}$ für alle $a, b \in M$ gilt: $a \sim b \Rightarrow b \sim a$
- antisymmetrisch $\overset{\text{Def}}{\iff}$ für alle $a, b \in M$ gilt: $a \sim b \wedge b \sim a \Rightarrow a = b$
- transitiv $\overset{\text{Def}}{\iff}$ für alle $a, b, c \in M$ gilt: $a \sim b \wedge b \sim v \Rightarrow a \sim c$
- total $\overset{\text{Def}}{\iff}$ für alle $a, b \in M$ gilt: $a \sim b \vee b \sim a$

Beispiel Sei M die Menge der Studierenden in der LA1-Vorlesung

1. Für $a, b \in M$ sei $a \sim b \overset{\text{Def}}{\iff} a$ hat den selben Vornamen wie b
   $\sim$ reflexiv, symmetrisch, nicht antisymmetrisch, transitiv, nicht total
2. Für $a, b \in M$ sei $a \sim b \overset{\text{Def}}{\iff}$ Martrikelnummer von a ist kleiner gleich als die Martrikelnummer von b
   $\sim$ ist reflexiv, nicht symmetrisch, antisymmetrisch, transitiv, total
3. Für $a, b \in M$ sei $a \sim b \overset{\text{Def}}{\iff} a$ sitzt auf dem Platz recht von b
   $\sim$ ist nicht reflexiv, nicht symmetrisch, nicht antisymmetrisch, nicht transitiv, nicht total

2.5.3 Halbordnung / Totalordung

$\sim$ heißt

- Halbordnung auf $M \overset{\text{Def}}{\iff}$ $\sim$ ist reflexiv, antisymmetrisch und transitiv
- Totalordung auf $M \overset{\text{Def}}{\iff}$ $\sim$ ist eine Halbordnung und $\sim$ ist total

In diesen Fällen sagt man auch: Das Tupel $(M, \sim)$ ist eine halbgeordnete, beziehungsweise totalgeordnete Menge.

Beispiel

1. $\leq$ auf $\mathbb{N}$ ist eine Totalordung
2. Sei $M = \mathcal{P}(\{1,2,3\})$. $\subseteq$ ist auf M eine Halbordung, aber keine Totalordung (es ist zum Beispiel weder $\{1\} \subseteq \{3\}$ noch $\{3\} \subseteq \{\}$)

Anmerkung Wegen der Analogie zur $\leq$ auf $\mathbb{N}$ bezeichnen wir Halbordnungen in der Regel mit $\leq$

2.5.4 Größtes / kleinstes Element

$(M, \leq)$ halbgeordnete Menge, $a \in M$
a heißt ein

- größtes Element von $M \overset{\text{Def}}{\iff}$ Für alle $x \in M$ gilt $x \leq a$
- kleinstes Element von $M \overset{\text{Def}}{\iff}$ Für alle $x \in M$ gilt $a \leq x$

Bemerkung $(M, \leq)$ halbgeordnete Menge
Dann gilt: Existiert in M ein größtes (beziehungsweise kleinstes) Element, so ist dieses eindeutig bestimmt

Beweis Es seien $a, b \in M$ größte Elemente von M
$\Rightarrow x \leq a$ für alle $x \in M$, also auch $b \leq a$
Außerdem: $x \leq b$ für alle $x \in M$, also auch $a \leq b$
$\overset{\text{Antisymmetrie}}{\Longrightarrow} a = b$
Analog für kleinstes Element

Anmerkung Dies sagt nichts darüber aus, ob ein größtes (beziehungsweise kleinstes) Element in M überhaupt existiert.

Beispiel

1. In $(\mathbb{N}, \leq)$ ist 1 das kleinste Element, ein größtes Element gibt es nicht
2. $(\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\}, \subseteq)$ ist eine halbgeordnete Menge ohne kleinstes beziehungsweise größtes Element

2.5.5 maximales / minimales Element

$(M, \leq)$ halbgeordnete Menge, $a \in M$
a heißt ein

- maximales Element von $M \overset{\text{Def}}{\iff}$ für alle $x \in M$ gilt: $a \leq x \Rightarrow a = x$
- minmales Element von $M \overset{\text{Def}}{\iff}$ für alle $x \in M$ gilt: $x \leq a \Rightarrow a = x$

Beispiel In $(\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\},\subseteq)$ sind $\{1,2\},\{1,3\},\{2,3\}$ maximale Elemente und $\{1\},\{2\},\{3\}$ sind minimale Elemente.

Bemerkung $(M,\leq)$ halbgeordnete Menge, $a \in M$
Dann gilt: Ist a ein größtes (beziehungsweise kleinstes) Element von M, dann ist a ein maximales (beziehungsweise minimales) Element von M.

Beweis Sei a ein größtes Element von M.
zu zeigen ist: Für alle $x \in M$ gilt $a \leq x \Rightarrow a = x$ Sei $x \in M$ mit $a \leq x$. Da a größtes Element von M ist, gilt auch $x \leq a$
$\overset{\text{Antisymmetrie}}{\Longleftrightarrow} a = x$
Analog für kleinstes Element.

2.5.6 Äquivalenzrelation

M Menge, $\sim$ auf M
$\sim$ heißt Äquivalenzrelation $\overset{\text{Def}}{\Longleftrightarrow}$ $\sim$ ist reflexiv, symmetrisch und transitiv. In dem Fll sagen wir für $a \sim b$ auch a ist äquivalent zu b. Für $a \in M$ heißt $[a] := \{b \in M \mid b \sim a\}$ heißt die Äquivalentklasse von a. Elemente aus $[a]$ nennt man Vertreter oder Repräsentanten von a

Beispiel M Menge aller Bürgerinnen und Bürger Deutschlands.
Wir definieren für $a, b \in M$ $a \sim b \overset{\text{Def}}{\Longleftrightarrow} a$ und b sind im selben Jahr geboren.
$\sim$ ist ein Äquivalenzrelation.
Jerôme Boateng wurde 1988 geboren.
[Jerôme Boateng] $= \{b \in M \mid b$ ist im selben Jahr geboren wie Jerôme Boateng$\} = \{b \in M \mid b$ wurde 1988 geboren$\}$ Weitere Vertreter von [Jerôme Boateng] sind zum Beispiel Mesut Özil, Mats Hummels. Es ist [Jerôme Boateng] = [Mesut Özil] = [Mats Hummels].
Man sieht in diesem Beispiel: Die Menge M zerfällt komplett in verschiedene Äquivalentzklassen:

- Jeder Bürger / jede Bürgerinn Detuschalnds ist in genau einer Äquivalenzklasse enthalten
- Jede zwei Äquivalentklasse sind entweder gleich oder disjunkt (haben leeren Durchschnitt)

Bemerkung M Menge, $\sim$ Äquivalenzrelation auf M
Dann gilt:

1. Jedes Element von M liegt in genau einer Äquivalenzklasse
2. Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt

Man sagt auch: Die Äquivalenzklassen bezüglich "$\sim$" bilden eine **Partition** von M.

Beweis

1. Sei $a \in M$
   zu zeigen: Es gibt genau eine Äquivalenzklassen, in der a liegt
   a) Es gibt eine Äquivalenzklasse, in der a liegt, denn $a∈ [a], denn $a \sim a$
   b) Ist $a∈[b] und a∈[c], dann ist [b]=[c] (d.h. a liegt in höchstens einer Äquivalenzklasse)
   denn: Seien $b, c \in M$ mit $a \in [b]$ und $a \in [c] \Rightarrow a \sim b$ und $a \sim c \xRightarrow{\text{Symmetrie}}$ $b \sim a$ und $a \sim c \xRightarrow{\text{Transitivität}} b \sim c$ Behautptung $[b] = [c]$ denn: "$\subseteq$" Sei $x \in [b] \Rightarrow x \sim b \xRightarrow{Transitivitt}{}^{b\sim c} x \sim c \Rightarrow x \in [c]$ denn: "$\supseteq$" Sei $x \in [c] \Rightarrow x \sim c \xRightarrow{Transitivitt}{}^{c\sim b} x \sim b \Rightarrow x \in [b]$
2. Sind $b, c \in M$ mit $[b] \cap [c] \neq \emptyset$, dann existiert ein $a∈ [b]∩ [c], und es folgt wie in 2.:
   $[b] = [c]$ Für $b, c \in M$ gilt also entweder $[b] \cap [c] = \emptyset$ oder $[b] = [c]$ □

Faktormenge M Menge, $\sim$ Äquivalenzrelation auf M $M/\sim := \{[a] | a \in M\}$ (Menge der Äquivalenzklassen) heißt die Faktormenge (Quotientenmenge) von M nach $\sim$

Beispiel

$$M = \{1, 2, 3, -1, -2, -3\}$$

Für $a, b, c \in M$ setzen wir $a \sim b \xLeftrightarrow{\text{Def.}} |x| = |b|$ Das ist eine Äquivalenzrelation auf M Es ist $[1] = \{1, -1\}, [2] = \{2, -2\}, [3] = \{3, -3\}$ Somit: $M/sim := \{[1], [2], [3]\} = \{\{1, -1\}, \{2, -2\}, \{3, -3\}\}$

Anmerkung Der Übergang zur Äquivalenzklassen soll (für eine jeweils gegebene Relation) irrelevante Informationen abstreifen.

2.6 Abbildungen

naive Definition:
Eine Abbildung f von M nach N ist eine Vorschrift, die jedem $n \in M$ genau ein Element aus N zuordnet, dieses wird mit $f(n)$ bezeichnet. **Notation**:

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

Zwei Abbildungen $f, g : M \to N$ sind gleich, wenn gilt $\forall\, n \in M : f(n) = g(n)$ M heißt die Definitionsmenge von f, N heißt die Zielmenge von f

2.6.1 Definition

Eine Abbildung f von M nach N ist ein Tupel (M, N, G_f), wobei G_f eine Teilmenge von $M \times N$ mit der Eigenschaft ist, dass für jedes Element $m \in M$ genau ein Element $n \in N$ mit $(m, n) \in G_f$ existiert. (für dieses Element n schreiben wir auch $f(m)$). G_f heißt der Graph von f.

2.6.2 Beispiel

1. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
2. $f : \mathbb{R} \to \mathbb{R}^2, x \mapsto (x, x + 1)$
3. M Menge, $id_M : M \to M, m \mapsto m$ heißt Identität (identische Abbildung) auf M
4. I,M Mengen: Eine über I indizierte Familie von Elementen von M ist eine Abbildung:
   $m : I \to M, i \mapsto m(i) =: m_i$. Wir schreiben für die Familie auch kurz $(m_i)_{i \in I}$. I heißt Indexmenge der Familie.
5. Spezialfall von 4.: $I = \mathbb{N}, M = \mathbb{R}$: $((m_i)_{i \in \mathbb{N}})$ nennt man auch Folge reeler Zahlen.

2.6.3 Anmerkung über den Begriff der Familie

Über den Begriff der Familie lassen sich diverse Konstruktionen aus der naiven Mengenlehre verallgemeinern. Ist $(M_i)_{i \in I}$ eine Familie von Mengen, dann ist:

$$\cup_{i \in I} M_i := \{x \mid \exists i \in I : x \in M_i\}$$

$$\cap_{i \in I} M_i := \{x \mid \forall\, i \in I : x \in M_i\}$$

$$\prod_{i \in I} M_i := \{(x_i)_{i \in I} \mid \forall\, i \in I : x_i \in M\}$$

2.6.4 Bild

m, N Mengen, $f : M \to n$ Abbildung.
Sind $m \in M, n \in N$ mit $n = f(m)$ dann nennen wir n ein **Bild** von m unter f und wir nennen m ein **Urbild** von n unter f.

Anmerkung In obiger Situation ist das Bild von m unter f eindeutig bestimmt (nach der Definition einer Abbildung) Urbilder sind im allgemeinen nicht eindeutig bestimmt, und im Allgemeinen besitzt nicht jedes Element aus N ein Urbild.

Beispiel $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, dann ist $4 = f(2) = f(-2)$, das heißt 2 und -2 sind Urbilder von 4, das Element -5 hat kein Urbild unter f, denn es existiert kein $x \in \mathbb{R}$ mit $x^2 = -5$

Definition M, N Mengen, $f : M \to N$ Abbildung, $A \subseteq M, B \subseteq N$
$f(A) := \{f(a) \mid a \in A\} \subseteq N$ heißt das Bild von A unter f.
$f^-1(B) := \{m \in M \mid f(m) \in B\} \subseteq M$ heißt das Urbild von B unter f

Beispiel

$$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$$
$$f(\{1, 2, 3\}) = \{1, 4, 9\}$$
$$f^-1(\{4, -5\}) = \{2, -2\}$$
$$f^-1(\{4\}) = \{2, -2\}$$
$$f^-1(\{-5\}) = \emptyset$$
$$f(\mathbb{R}) = x^2 \mid x \in \mathbb{R} = \{x \in \mathbb{R} \mid x \geq 0\} =: \mathbb{R}_{\geq 0}$$

2.6.5 Restriktion

M, N Mengen, $f : M \to N$ Abbildung, $A \subseteq M$

$$f \mid_A : A \to N, m \mapsto f(m)$$

heißt die Restriktion von f auf A. Ist $B \subseteq N$ mit $f(A) \subseteq B$, dann setzen wir

$$f \mid_A^B : A \to B, m \mapsto f(m)$$

Ist $f(M) \subseteq B$ dann setzen wir:

$$f \mid^B := f \mid_M^B, M \to B, m \mapsto f(m)$$

2.6.6 Komposition

L, M, N Mengen, $f : L \to M, g : M \to N$ Abbildung

$$g \circ f : L \to N, x \mapsto (g \circ f)(x) := g(f(x))$$

heißt die Komposition (Hintereinanderausführung) von f und g

Beispiel

$$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2, g : \mathbb{R} \to \mathbb{R} : x \mapsto x + 1$$
$$\Rightarrow g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto g(f(x)) = g(x^2) = x^2 + 1$$

Assoziativität L, M, N, P Mengen, $f : L \to M, g : M \to N, h : n \to p$
Dann gilt

$$h \circ (g \circ f) = (h \circ g) \circ f$$

das heißt die Verknüpfung von Abbildungen ist assoziativ.

Beweis Für $x \in List$

$$(h \circ (g \circ f)) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x) \square$$

2.6.7 Eigenschaften von Abbildungen

M, N Mengen, $f : M \to N$ Abbildung

Injektivität f heißt injektiv:

$$\overset{\text{Def}}{\iff} \forall\, m_1, m_2 \in M : f(m_1) = f(m_2) \Rightarrow m_1 = m_2 \Leftrightarrow \forall\, m_1, m_2 \in M : m_1 \neq m_2 \Rightarrow f(m_1) \neq f(m_2)$$

Surjektivität f heißt sujektiv:

$$\overset{\text{Def}}{\iff} \forall\, n \in M : \exists m \in M : f(m) = n \Leftrightarrow f(M) = N$$

Bijektivität f heißt bijektiv: $\overset{\text{Def}}{\iff}$ f ist injektiv und surjektiv

Beispiel

1. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist:
   - nicht injektiv, denn $f(2) = f(-2)$, aber $2 \neq -2$
   - nicht surjektiv, denn es existier kein $m \in \mathbb{R}$ mit $f(m) = -1$
   - nicht bijektiv
2. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto x^2$ ist:
   - injektiv, denn für $m_1, m_2 \in \mathbb{R}_{\geq 0}$ gilt: $f(m_1) = f(m_2) \Rightarrow m_1^2 = m_2^2 \overset{m_1, m_2 > 0}{\Longrightarrow} m_1 = m_2$
   - nicht surjektiv, denn es existier kein $m \in \mathbb{R}_{\geq 0}$ mit $f(m) = -1$
   - nicht bijektiv
3. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist:
   - injektiv, denn für $m_1, m_2 \in \mathbb{R}_{\geq 0}$ gilt: $f(m_1) = f(m_2) \Rightarrow m_1^2 = m_2^2 \overset{m_1, m_2 > 0}{\Longrightarrow} m_1 = m_2$
   - surjektiv, denn für $m \in \mathbb{R}_{\geq 0}$ ist $f(\sqrt{m}) = (\sqrt{m})^2 = m$
   - bijektiv

Bemerkung 4.12 M, N Mengen, $f : M \to N, g : n \to M$ mit $g \circ f = id_M$ Dann ist f injektiv und g surjektiv.

Beweis

1. f ist injektiv, denn:
   Seien $m_1, m_2 \in M$ mit $f(m_1) = f(m_2) \Rightarrow g(f(m_1)) = g(f(m_2)) \Rightarrow (g \circ f)(m_1) = (g \circ f)(m_2) \Rightarrow id_m(m_1) = id_M(m_2) \Rightarrow m_1 = m_2$

2. g ist surjektiv, denn:
   Sei $m \in M$ Dann ist $m = id_M(m) = (g \circ f)(m) = g(f(m))$

Bemerkung Sei $f : M \to N$, N, M Mengen Dann sind äquivalent:

1. f ist bijektiv
2. Zu jedem $n \in N$ gibt es genau ein $m \in M$ mit $f(m) = n$
3. Es gibt genau eine Abbildung $g : N \to M$ mit $g \circ f = id_M$ und $f \circ g = id_N$

In diesem Fall bezeichnen wir die Abbildung $g : N \to M$ aus 3. mit f^{-1} und nennen f^{-1} die Umkehrabbildung von f. Sie ist gegeben durch

$$f^{-1} : N \to M, n \mapsto \text{ Das eindeutig bestimmte Element } m \in M \text{ mit } f(m) = n$$

Beweis Statt 1. $\Leftrightarrow$ 2. und 2. $\Leftrightarrow$ 3. zeigen 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 1.

- 1. $\Rightarrow$ 2. Sei f bijektiv
  zz: Ist $n \in N$, dann existiert genau ein $m \in M$ mit $f(m) = n$
  - Existenz folg aus Surjektivität von f
  - Eindeutigkeit: Seien $m_1,m_2 \in M$ mit $f(m_1) = n, f(m_2) = n \Rightarrow f(m_1) = f(m_2) \xrightarrow{finjektiv} m_1 = m_2$

- 2. $\Rightarrow$ 3. Zu jedem $n \in M$ existiere genau ein $m \in M$ mit $f(m) = n$
  zz: Ex existert genau eine Abbildung $g : N \to M$ mit $f \circ f = id_M$ und $f \circ g = id_N$
  - Existenz: Wir definieren $g : N \to M, n \mapsto$ das nach 2. eindeutigbestimmte Element $m \in M$ mit
    Dann gilt für $m \in M$:
    $$(g \circ f)(m) = f(f(m)) = m, \; textdasheit \; g \circ f = id_M$$
    und für $n \in N$ ist $(f \circ g)(n) = f(g(n)) = n$ also $f \circ g = id_N$
  - Eindeutigkeit: Es seinen $g_1, g_2 : N \to M$ mit $g_i \circ f = id_M, f \circ g_i = id_N$ für $i = 1, 2$
    $$\Rightarrow g_1 = g_1 \circ id_N = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = id_M \circ g_2 = g_2$$

- 3. $\Rightarrow$ 1. Wegen 3. existier $g : N \to M$ mit $g \circ f = id_M, f \circ g = id_N$
  $$\xrightarrow{[[Bemerkung 4.12]]} f \text{ injektiv }, f \text{ surjektiv } \Rightarrow f \text{ bijektiv} \Rightarrow \text{ 1.}$$

Anmerkung

- Bitte stets aufpassen, ob mit f^{-1} die Unmkerhabbildung (falls existent) oder das Bilden der Urbildmenge gemeint ist.
- Im Beweis von 3. $\Rightarrow$ 1. haben wir die Eindeutigkeit von g garnicht verwendet, das heißt wir haben sogar gezeigt:
  f bijektiv $\Leftrightarrow$ 3.' Es existiert eine Abbildung $g : N \to M$ mit $f \circ g = id_N$ und $f \circ f = id_M$ Soch eine Abbildung g ist in diesem Fall automatisch bestimmt.

Beispiel Im Beispiel vorher haben wir gesehen $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist bijektiv. Die Umkehrabbildung ist gegeben durch $f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto \sqrt{x}$

Bemerkung M, N Mengen, $f : M \to N$ Dann gilt:

1. f injektiv $\Leftrightarrow$ Es existiert $g : N \to M$ mit $g \circ f = id_M$
   Beweis:
   - "$\Leftarrow$" folgt aus 2.6.7
   - "$\Rightarrow$" Sei f injektiv. Sein x ein beliebiges Element aus M Wir definieren

     $$g : N \to M, n \mapsto \begin{cases} x & n \notin f(M) \\ \text{das eindeutig bestimmte Element } m \in M \text{ mit } f(m) = n & n \in f(M) \end{cases}$$

     Für alle $m \in M$ ist dann $(g \circ f)(m) = g(f(m)) = m$ das geißt $g \circ f = id_M$
2. f surjektiv $\Leftrightarrow$ Es existiert $g : N \to M$ mit $f \circ g = id_N$
   Beweis:
   - "$\Leftarrow$" folgt aus 2.6.7
   - "$\Rightarrow$" Sei f surjektiv. Für jedes Element $n \in N$ wählen wir ein Element $\tilde{n} \in f^{-1}(\{n\}) \neq \emptyset$ und sehen $g : N \to M, n \mapsto \tilde{n}$. Dann ist $(f \circ g)(n) = f(g(n)) = n$ für alle $n \in N$ und das heißt $f \circ g = id_N$ $\square$

Anmerkung Das wir stets einen Auswahlprozess wie im Beweis von 2. "$\Rightarrow$" vornehmen können ist ein Axiom der Mengenlehre (erkennen wir als gültig an, ist jedoch nicht beweisbar), das **Auswahlaxiom**:
Ist I eine Indexmenge und $(A_i)_{i \in I}$ eine Familie von nichtleeren Mengen, dann gibt es eine Abbildung $\gamma : I \to \bigcup_{i \in I} A_i$ mit $\gamma(i) \in A_i$ für alle $i \in I$ (im obigen Beweis ist $I = N, A_n = f^{-1}(\{n\})$ für $n \in N$)

Bemerkung 4.16 L, M, N Mengen, $f : L \to M, g : M \to N$
Dann gilt: g, f beide injektiv (beziehungsweise surjektiv oder bijektiv) $\Rightarrow g \circ f$ injektiv (beziehungsweise sujektiv oder bijektiv)

Definition 4.17

Bemerkung 4.19 M, N endliche Mengen mit $|M| = |N|, f : M \to N$ Dann sind äquivalent:

1. f ist injektiv
2. f ist surjektiv
3. f ist bijektiv

Beweis

- 1. $\Rightarrow$ 2. Sei f injektiv $\Rightarrow |f(M)| = |M| = |N|$ wegen $f(M) \subseteq N$ folgt $f(M) = N$ $\Rightarrow$ f surjektiv
- 2. $\Rightarrow$ 3. Sei f sujektiv, das heißt $f(M) = N$
  Annahme: f ist nicht bijektiv $\Rightarrow$ f nicht injektiv $\Rightarrow \exists m_1, m_2 \in M : m_1 \neq m_2 \wedge f(M_1) = f(m_2) \Rightarrow |f(M)| < |M| = |N|$ Wiederspruch zu $f(M) = N$
- 3. $\Rightarrow$ 1. trivial

3 Gruppen, Ringe, Körper

3.1 Gruppe

3.1.1 Verknüpfung

M Menge, Eine Verknüpfung (inverse Verknüpfung) auf M ist ein Abbildung

$$* : M \times M \to M$$

Anstelle von $*(a, b)$ schreiben wir $a * b$

Beispiel

- $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a, b) \mapsto a + b$
- $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a, b) \mapsto a \cdot b$

sind Verknüpfungen

3.1.2 Monoid

Ein Monoid ist ein Tupel $(M, *)$, bestehend aus einer Menge M und einer Verküpfung $* : M \times M \to M$, welche folgende Bedingungen genügt:

- (M1) Die Verküpfung ist assoziativ, das heißt

$$\forall\, a, b, c \in M : (a * b) * c = a * (b * c)$$

- (M2) Ex existiert ein neutrales Element e in M, das heißt

$$\exists e \in M : \forall\, a \in M e * a = a = a * e$$

Beispiel

- $(\mathbb{N}_0, +), (\mathbb{Z}, +)$ sind Monoide (neutrales Element: 0)
- $(\mathbb{N}, +)$ ist kein Monoid (ex existiert kein neutrales Element)
- $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot)$ sind Monoide (neutrales Element: 1)

Bemerkung $(M, *)$ Monoid. Dann gibt es in M genau ein neutrales Element.

Beweis

- Existenz: Es existert ein neutrales Element: folgt aus Definition eines Monoids
- Eindeutigkeit: Seien $e, \tilde{e} \in M$ neutrale Element

$$\Rightarrow e = e * \tilde{e} = \tilde{e}$$

3.1.3 Inverses

$(M, *)$ Monoid mit neutralem Element e, $a \in M$ Ein Element $b \in M$ heit Inverses zu $a \overset{\text{Def}}{\iff} a * b = e = b * a$

Beispiel

- In $(\mathbb{Z}, +)$ ist -2 ein Inverses zu 2 denn $2 + (-2) = 0 = (-2) + 2$
- In $(\mathbb{N}_0, +)$ existiert kein Inverses zu 2, denn es existiert kein $n \in \mathbb{N}_0$ mit $n + n = 0 = n + 2$
- In $(\mathbb{Z}, \cdot)$ existiert kein Inverses zu 2, denn es existiert kein $n \in \mathbb{Z}$ mit $2 \cdot n = 1 = n \cdot 2$

Bemerkung $(M, *)$ Monid, $a \in M$ Dann gilt: besitzt a ein Inverses, dann ist dieses eindeutig bestimmt.

Beweis Seinen $b, \tilde{b}$ Inversen zu a, sein $e \in M$ das neutrale Element

$$\Rightarrow b = e * b = (\tilde{b} * a) * b = \tilde{b} * (a * b) = \tilde{b}$$

3.1.4 Gruppe

Eine Gruppe ist ein Tupel $(G, *)$, bestehen aus einer Menge G und einer Verknüpfung $* : G \times G \to G$, sodass gilt:

- (G1) $(G, *)$ ist ein Monoid
- (G2) Jedes Element aus G besitzt ein Inverses

In diesem Fall schreiben wir a' für das nach 3.1.3 eindeutig bestimmte Inverse eines Elements $a \in G$

Beispiel

- $(\mathbb{Z}, +)$ ist eine Gruppe, denn $(\mathbb{Z}, +)$ ist ein Monoid und für $a \in \mathbb{Z}$ ist $-a$ das inverse Element: $a + (-a) = 0 = (-a) + a$
- $(\mathbb{Z}, \cdot)$ ist keine Gruppe, denn das Element $2 \in \mathbb{Z}$ hat kein Inverses (vergleiche 3.1.3).
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine Gruppe denn es ist ein Monoid mit neutralem Element 1 und für jedes Element $a \in \mathbb{Q} \setminus \{0\}$ existiert ein $b \in \mathbb{Q} \setminus \{0\}$ mit $a \cdot b = 1 = b \cdot a$, nämlich $b = \frac{1}{a}$

Bemerkung 5.11 $(G, *)$ Gruppe mit neutralem Element $e, a, b, c \in G$. Dann gilt

1. (Kürzungsregel)
$$a * b = a * c \Rightarrow b = c$$
$$a * c = b * c \Rightarrow a = b$$
2. $a * b = e \Rightarrow b = a'$
3. $(a')' = a$
4. (Regel von Hemd und Jacke) $(a * b)' = b' * a'$

Beweis

1. Sei $a*b = a*c \Rightarrow a'*(a*b) = a'*(a*c) \Rightarrow (a'*a)*b = (a'*a)*c \Rightarrow e*b = e*c \Rightarrow b = c$
2. aus 1. $a * b = c = a * a' \Rightarrow b = a'$
3. Es ist $a * a' = e = a' * a$, das heißt a ist Inverses zu $a' \Rightarrow (a')' = a$
4. Es ist $(a * b) * (b' * a') = a * (b * b') * a' = a * a' = e \Rightarrow b' * a' \overset{2.}{\Rightarrow} (a * b)'$

3.1.5 Abelsche Gruppe

$(M, *)$ Monoid / Gruppe heißt kommutativ (abelsch)

$$\overset{\text{Def}}{\iff} \forall\, a, b \in M : a * b = b * a$$

Beispiel Alle bisher betrachteten Beispiele von Monoiden beziehungsweise Gruppen sind abelsch

Bemerkung 5.14 M Menge, Wir setzten $S(M) := \{f : M \to M | f \text{ bijektiv}\}$ Dann ist $(S(M), \circ)$ eine Gruppen, die **symmetrische** Gruppe auf M

Beweis

1. "$\hat{}$" ist wohl definiert, das heißt für $f, g \in S(M)$ ist $f \circ g \in S(M)$ folgt aus 2.6.7
2. "$\hat{}$" ist assoziativ $f \circ (g \circ h) = (f \circ g) \circ h \, \forall \, f, g \in S(M)$ nach `4.9`
3. id_M ist neutral: $id_M \in S(M)$ und $id_M \circ f = f = f \circ id_M \, \forall \, f \in S(M)$
4. Existenz von Inversen: $f \in S(M) \Rightarrow f$ bijektiv $\Rightarrow$ Es existiert Umkehrabbildung $f^{-1} \in S(M)$ zu f für diese gilt: $f \circ f^{-1} = id_M = f^{-1} \circ f$ das heißt f^{-1} ist immer zu f bezüglich "$\hat{}$"

3.1.6 Permutationen

$n \in \mathbb{N}$

$$S_n := S(\{1, \ldots, n\}) = \{\pi\{1, \ldots, n\} \to \{1, \ldots, n\} \mid \pi \text{ ist bijektiv}\}$$

$(S_n, \circ)$ heißt die symmetrische Gruppe auf n Ziffern, Elemente aus S_n heißen Permutationen. Wir schreiben Permutationen $\pi \in S_n$ in der Form:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix} \tag{1}$$

Beispiel In S_3 ist

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

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

das heißt $(S_3, \circ)$ ist nicht abelsch.

3.1.7 Restklassen

Motivation Im täglichen Leben verwendet man zur Bestimmung von Uhrzeiten das Rechnen "modulo 24", zum Beispiel 22Uhr + 7h = 5Uhr. Wir wollen dies mathematisch präzisieren und verallgemeinern

Bemerkung 5.17 $n \in \mathbb{N}$. Dann ist durch

$$a \sim b \overset{\text{Def}}{\iff} \exists \, q \in \mathbb{Z} : a - b = qn$$

eine Äquivalenzrelatioin auf $\mathbb{Z}$ gegeben. Anstelle von $a \sim b$ schreiben wir auch $a \equiv b(\mod n)$ ("n ist kongruent b modulo n") Die Äquivalenzklasse von $a \in \mathbb{Z}$ ist durch

$$\bar{a} := \{b \in \mathbb{Z} \mid b \equiv a(\mod n)\} = a + n\mathbb{Z} := \{a + nq \mid q \in \mathbb{Z}\}$$

gegeben und heißt die Restklasse von a modulo n. Die Menge aller Restklassen modulo n wird $\frac{\mathbb{Z}}{n\mathbb{Z}}$ bezeichnet ("$\mathbb{Z}$ modulo $n\mathbb{Z}$") Es ist:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

und die Restklassen $\bar{0}, \ldots, \overline{n-1}$ sind paarweise verschieden

Beweis

1. "$\equiv$" ist eine Äquivalenzrelation, denn:
   - "$\equiv$" ist reflexiv: Fpr $a \in \mathbb{Z}$ ist $a \equiv a(\mod n)$ denn $a - a = 0 = 0n$
   - "$\equiv$" ist symmetrisch: Seien $a, b \in \mathbb{Z}$ mit $a \equiv b(\mod n) \exists q \in \mathbb{Z} : a - b = qn$ $\Rightarrow b - a = (-q)n \Rightarrow b \equiv a(\mod n)$
   - "$\equiv$" ist transitiv: Seien $a, b, c \in \mathbb{Z}$ mit $a \equiv b(\mod n), b \equiv c(\mod n)$
     - $\Rightarrow \exists q_1, q_2 \in \mathbb{Z}$ mit $a - b = q_1 n, b - c = q_2 n$
     - $\Rightarrow a - c = (a - b) + (b - c) = q_1 n + q_2 n = (q_1 + 1_2)n \Rightarrow a \equiv c(\mod n)$
2. Die Äquivalenzklasse von $n \in \mathbb{Z}$ ist gegeben durch

$$\begin{aligned} &\{b \in \mathbb{Z} \mid b = a(\mod n)\} \\ &= \{b \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : b - a = qn\} \\ &= \{b \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : b = a + qn\} \\ &= a + n\mathbb{Z} \end{aligned}$$

3. $$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

   denn:
   - Ist $a \in \mathbb{Z}$ beliebig, dann liefert Division mit Rest durch n:
     Es gibt $q, r \in \mathbb{Z}$ mit $a = qn + r, 0 \leq r < n$

     $$\Rightarrow a - r = qn \Rightarrow q \equiv r(\mod n) \Rightarrow \bar{a} = \bar{r}$$

     Das heißt: Jede Restklasse ist von der Form $\bar{r}$ mit $r \in \{0, \ldots, n-1\}$
   - Die Restklassen $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ sind paarweise verschieden denn:
     Seien $a, b \in \{0, \ldots, n-1\}$ mit $\bar{a} = \bar{b} \Rightarrow a \equiv b(\mod n) \Rightarrow \exists q \in \mathbb{Z} : a - b = qn \Rightarrow |a - b| = |q|n$.
     - Wäre $q \neq 0$, dann $|q| \geq 1$ wegen $q \in \mathbb{Z} \Rightarrow |a - b| \geq n$ **Wiederspruch** zu $a, b \in \{0, \ldots, n-1\}$
       Also: $q = 0$ das heißt $a = b$

Beispiel $n = 3 : a \equiv b(\mod 3) \Leftrightarrow \exists q \in \mathbb{Z} : a - b = 3q$
zum Beispiel: $11 \equiv 5(\mod 3)$, denn $11 - 5 = 6 = 2 \cdot 3$
zum Beispiel: $7 \not\equiv 2(\mod 3)$, denn $7 - 2 = 5$ und es gibt kein $q \in \mathbb{Z}$ mit $5 = 3q$

$$\bar{0} = \{a \in \mathbb{Z} \mid a \equiv 0(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a = 3q\} = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$\bar{1} = \{a \in \mathbb{Z} \mid a \equiv 1(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a-1 = 3q\} = 1+3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

$$\bar{2} = \{a \in \mathbb{Z} \mid a \equiv 2(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a-2 = 3q\} = 2+3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

$$\bar{3} = \{a \in \mathbb{Z} \mid a \equiv 3(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a-3 = 3q\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a = 3(q+1)\}3\mathbb{Z} = \bar{0}$$

$$\bar{4} = \bar{1}, \bar{5} = \bar{2}, \overline{-1} = \bar{2}$$

Bemerkung 5.18 $n \in \mathbb{N}$ wir definieren eine Verküpfung (Addition) auf $\frac{\mathbb{Z}}{n\mathbb{Z}}$ wie folgt:
Für $\bar{a}, \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ setzen wir $\bar{a} + \bar{b} = \overline{a + b}$ Dann gilt $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ ist eine abelsche Gruppe

Beweis

1. Die Verknüpfung ist wohldefiniert:
   Problem: Die Addition verweendet Vertreter von Restklassen. Es ist zum Beispiel in $\frac{\mathbb{Z}}{n\mathbb{Z}}$: $\bar{3} + \bar{4} = \overline{3 + 4} = \bar{7} = \bar{2}$, aber man könnte auch Rechnen: $\bar{3} + \bar{4} = \bar{8} + \bar{9} = \overline{8 + 9} = \overline{17} = \bar{2}$
   Wir müssen nachweisen, dass die Wahl der Vertreter keinen Einfluss auf das Ergebnis hat, das heißt die Verknüfung ist "vertreter unahbhängig":
   Seien $a_1, a_2, b_1, b_2 \in \mathbb{Z}, \overline{a_1} = \overline{a_2}, \overline{b_1} = \overline{b_2}$

   $$\Rightarrow a_1 \equiv a_2(\mod n), b_1 \equiv b_2(\mod n) \tag{4}$$
   $$\Rightarrow \exists q_1, q_2 \in \mathbb{Z} : a_1 - a_2 = q_1 n, b_1 - b_2 = q_2 nn, b_1 - b_2 = q_2 n \tag{5}$$
   $$\Rightarrow (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = q_1 n + q_2 n = (q_1 + q_2)n \tag{6}$$
   $$\Rightarrow a_1 + b_1 \equiv a_2 + b_2(\mod n) \tag{7}$$
   $$\Rightarrow \overline{a_1 + b_1} = \overline{a_2 + b_2} \tag{8}$$

2. $(\frac{\mathbb{Z}}{n\mathbb{Z}})$ ist eine abelsche Gruppe:
   - Assoziativgesetz: Für alle $a, b, c \in \mathbb{Z}$ ist

     $$(\bar{a} + \bar{b}) + \bar{c} = \overline{a + b} + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + \overline{b + c} = \bar{a} + (\bar{b} + \bar{c})$$

   - $\bar{0}$ ist neutrales Element, denn $\forall\, a \in \mathbb{Z} : \bar{0} + \bar{a} = \overline{0 + a} = \bar{a} = \bar{a} + \bar{0}$
   - Für $a \in \mathbb{Z}$ inst $\overline{-a}$ das inverse Element zu $\bar{a}$, denn $\bar{a} + \overline{-a} = \overline{a + (-a)} = \bar{0} = \overline{-a} + \bar{a}$
   - Kommutativgesetz: $\forall\, a, b \in \mathbb{Z} : \bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a}$

Beispiel Wir tragen die Ergebnisse der Verknüpfung "+" in einer Verknüpfungstafel zusamme: n = 3

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

n = 4

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

3.1.8 Gruppenhomomorphismus

$(G,+),(H,\circledast),\varphi: G \to H$ Abbildung
φ heißt ein Gruppenhomomorphismus $\overset{\text{Def}}{\iff} \forall\, a,b,c \in G : \varphi(a * b) = \varphi(a) \circledast \varphi(b)$
φ heißt ein Gruppenisomorphismus $\overset{\text{Def}}{\iff}$ φ ist bijektiver Gruppenhomomorphismus

Beispiel

1. $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto 2a$ ist Gruppenhomomorphismus von $(\mathbb{Z},+)$ nach $(\mathbb{Z},+)$ denn:

   $$\varphi(a+b) = 2(a+b) = 2a + 2b = \varphi(a) + \varphi(b) \,\forall\, a,b \in \mathbb{Z}$$

   φ ist aber kein Gruppenisomorphismus, denn φ ist nicht surjektiv $(1 \notin \varphi = \varphi\mathbb{Z})$

2. $n \in \mathbb{N}$. Dann gilt $\varphi : \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}, a \mapsto \bar{a}$ ist ein Gruppenhomomorphismus von $(\mathbb{Z},+)$ nach $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$, denn

   $$\forall\, a,b \in \mathbb{Z} : \varphi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \varphi(a) + \varphi(b)$$

   φ ist kein Gruppenisomorphismus, denn φ ist nicht injektiv $(\varphi(0) = \bar{0} = \bar{n} = \varphi(n)$, aber $0 \neq n)$

3. $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto a+1$ ist kein Gruppenhomomorphismus von $(\mathbb{Z},+)$ nach $(\mathbb{Z},+)$, denn

   $$\varphi(2+6) = \varphi(8) = 9, \text{ aber } \varphi(2) + \varphi(6) = 3 + 7 = 10$$

4. $\exp : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto \exp x = e^x$ ist ein Gruppenisomorphismus von $(\mathbb{R},+)$ nach $(\mathbb{R}_{\geq 0},\cdot)$, denn:

   - $$\exp(a+b) = \exp(a)\exp(b) \,\forall\, a,b \in \mathbb{R}$$
   - *exp* ist bijektiv (vgl. Ana1 - Vorlesung)

Bemerkung 5.23 $(G, *), (H, \circledast)$ Gruppen mit neutralen Elementen e_G beziehungsweise $e_H, \varphi : G \to H$ Gruppenhomomorphismus. Dann gilt

1. $\varphi(e_G) = e_H$
2. $\forall\, a \in G : \varphi(a') = \varphi(a)'$ (Hierbei ist $'$ das Inverse)
3. Ist φ Gruppenisomorphismus, dann gilt $\varphi^{-1} : H \to G$ ebenfalls Gruppenisomorphismus

$(G, *), (H, \circledast)$ heißen isomorph $\overset{\text{Def}}{\iff}$ Ex existert ein Gruppenisomorphismus $\phi : G \to H$ Wir schreiben dann $(G, *) \cong (H, \circledast)$

Beweis

1. Es $e_H \circledast \varphi(e_G) = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \circledast (e_G) \Rightarrow e_H = \varphi(e_G)$
2. Sei $a \in G$ Dann ist $e_H = \varphi(e_G) = \varphi(a * a') = \varphi(a) \circledast (a') \Rightarrow \varphi(a') = \varphi(a)'$
3. φ^{-1} ist bijektiv, noch zu zeigen: φ^{-1} ist ein Gruppehomomorphismus, das heißt

$$\varphi^{-1}(c \circledast d) = \varphi^{-1}(c) * \varphi^{-1}(d)\, \forall\, c, d \in H$$

Seien $c, d \in H$ Weil φ bijektiv: $\exists a, b \in G : \varphi(a) = c, \varphi(b) = d$

$$\Rightarrow \varphi^{-1}(c \circledast d) = \varphi^{-1}(\varphi(a) * \varphi(b)) = \varphi^{-1}(\varphi(a * b)) = a * b = \varphi^{-1}(c) * \varphi^{-1}(d) \square$$

3.2 Ring

Ein Ring ist ein Tupel $(R, +, \cdot)$, bestehend aus einer Menge R und 2 Verknüpfungen:

- $+ : R \times R \to R, (a, b) \mapsto a + b$ genannt Addition
- $\cdot : R \times R \to R, (a, b) \mapsto a \cdot b$ genannt Multiplikation

welche den folgenden Bedingungen genügen

- (R1) $(R, +)$ ist eine abelsche Gruppe
- (R2) $(R, \cdot)$ ist ein Monoid
- (R3) Es gelten die Distributivgeseze, das heisßt

$$\forall\, a, b, c \in R : a \cdot (a + b) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$$

Ein Ring heißt **kommutativ** $\overset{\text{Def}}{\iff}$ die Multiplikation ist kommutativ, das heißt $\forall\, a, b \in R : a \cdot b = b \cdot a$

3.2.1 Anmerkung

- ohne Klammerung gilt die Konvention "$\cdot$" vor "$+$", "$\cdot$" wird häufig weggelassen
- das neutrale Element bezüglich "$+$" bezeichnen wri mit 0_R (Nullelement), das neutrale Element bezüglich "$\cdot$" mit 1_R (Einselement). Das zu $a \in R$ bezüglich "$+$" inverse Element bezeichnen wir mit $-a$, für $a + (-b)$ schreben wir $a - b$. Existiert zu $a \in R$ ein Inverses bezüglich "$\cdot$", so bezeichnen wir diesses mit a^{-1}
- Wir schreiben häufig verkürzend "R Ring" statt "$(R, +, \cdot)$ Ring"
- In der Literatur wird gelegentlich die Forderung der Existenz eines neutralen Elements bezüglich "$\cdot$" weggelassen, "unser" Ringbegriff entspricht dort dem Begriff "Ring mit Eins"

3.2.2 Beispiel

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring
2. Nullring $(\{0\}, +, \cdot)$ mit $0 + 0 = 0, 0 \cdot 0 = 0$ ist ein kummutativer Ring
   (hier ist Nullelement = Einselement = 0). Wir bezeichnen den Nullring kurz mit 0.

3.2.3 Bemerkung 6.3

R Ring. Dann gilt:

1. $0_R \cdot a = 0_R = a \cdot 0_R \forall\, a \in R$
2. $a \cdot (-a) = -ab = (-a) \cdot b \forall\, a, b \in R$
3. Ist $R \neq 0$, dann ist $1_R \neq 0_R$

Beweis

1. $0_R + 0_R \cdot a = 0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot \xrightarrow{\text{"kürzen s. [[Bemerkung 5.11]]"}} 0_R = 0_R \cdot a$, $a \cdot 0_R = 0_R$ analog
2. $0_R = 0_R \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b \Rightarrow$ [[Bemerkung 5.11]] $- ab = (-a) \cdot b$, $a \cdot (-b)0 - ab$ analog
3. Beweis durch Kontraposition: Sei $1_R = 0_R$

   $$\Rightarrow \forall\, a \in R : a = a \cdot 1_R = a \cdot 0_R = 0_R$$

   das heißt $R = 0$ $\square$

3.2.4 Bemerkung 6.4

$n \in \mathbb{N}$ Für $\bar{a}, \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ setzen wir $\bar{a} + \bar{b} := \overline{a+b}, \bar{a} \cdot \bar{b} := \overline{ab}$, dann ist $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ ein kommutativer Ring.

Wenn wir ab jetzt vom Ring $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sprechen, dann meinen wir $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ mit den obigen Verknüpfungen

Beweis

1. Multiplikaiton ist wohldefiniert (das heißt "vertreterunabhängig", vergleiche 3.1.7)
   Sei $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $\overline{a_1} = \overline{a_2}, \overline{b_2} = \overline{b_2}$

$$\Rightarrow a_1 \equiv a_2 (\mod n), b_1 \equiv b_2 (\mod n) \tag{9}$$
$$\Rightarrow \exists q_1, q_2 \in \mathbb{Z} : a_1 - a_2 = q_1 n, b_1 - b_2 = q_2 n \tag{10}$$
$$\Rightarrow a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2) = a_q q_2 n + b_2 q_1 n = (a_1 q_2 + b_2 q_1) n \tag{11}$$
$$\Rightarrow a_1 b_1 \equiv a_2 b_2 (\mod n) \tag{12}$$
$$\Rightarrow \overline{a_1 b_1} = \overline{a_2 b_2} \tag{13}$$

2. Multiplikation ist assoziativ, Für $a, b, c \in \mathbb{Z}$ ist

$$\bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot \overline{a \cdot c} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$

3. Existenz eines Enselements: $\forall\, a \in \mathbb{Z} : \bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a} = \bar{a} \cdot \bar{1}$

4. Multiplikation ist kommutativ:

$$\forall\, a, b \in \mathbb{Z} : \bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}$$

5. $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ ist abelsche Gruppe nach 3.1.7

6. Distributivgesetz:

$$\begin{aligned} \bar{a} \cdot (\bar{b} + \bar{c}) &= \bar{a} \cdot \overline{b + c} && (14)\\ &= \overline{a \cdot (b + c)} && (15)\\ &= \overline{a \cdot b + a \cdot c} && (16)\\ &= \overline{a \cdot b} + \overline{a \cdot c} \qquad = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} && (17) \end{aligned}$$

   $(\bar{a} + \bar{b}) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$ folgt wegen Kommutativität der Multiplikation

Beispiel 6.5 Verknüpfungstafeln für $\frac{\mathbb{Z}}{n\mathbb{Z}}$ n = 3:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

n = 4:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

In $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist $\bar{2} \cdot \bar{2} = \bar{0}$, aber $\bar{2} \neq \bar{0}$.

3.2.5 Integritätsbereich

ist ein kommuativer Ring $(R, +, \cdot)$ mit $R \neq 0$, in dem gilt:

$$\forall\, a, b \in R : a \cdot b = 0_R \Rightarrow a = 0_R \vee b = 0_R$$

beziehungsweise äquivalent dazu:

$$a \neq 0_R \wedge b \neq 0_R \Rightarrow a \cdot b \neq 0_R$$

Beispiel 6.7

- $\frac{\mathbb{Z}}{3\mathbb{Z}}$ ist ein Integritätsbereich, $\frac{\mathbb{Z}}{4\mathbb{Z}}$ ist kein Integritätsbereich, denn $\bar{2} \cdot \bar{2} = \bar{0}$, aber $\bar{2} \neq \bar{0}$

Bemerkung 6.8 $n \in \mathbb{N}$ Dann sind äquivalent

1. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist ein Integritätsbereich
2. n ist eine Primzahl

Beweis $1 \Rightarrow 2$ zeigen wir durch Kontraposition, das heißt \$≠\$2 $\Rightarrow \neq 1$
Sei $n \in \mathbb{N}$ keine Primzahl. Falls $n = 1$ dann ist $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}\}$ (Nullring), das heißt $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist kein Integritätsbereich. Seim im Folgenden $n > 1$ und keine Primzahl.

$$\Rightarrow \exists a, b \in \mathbb{N} : 1 \ < a, b < n \wedge n = a \cdot b \tag{18}$$

$$\Rightarrow \bar{0} = \bar{n} = \overline{ab} = \bar{a} \cdot \bar{b} \tag{19}$$

und es ist $bara, \bar{b} \neq \bar{0} \Rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ kein Integrationsbereich.
$2 \Rightarrow 1$: Sein n eine Primzahl $\Rightarrow n > 1$, insbesondere $\frac{\mathbb{Z}}{n\mathbb{Z}} \neq 0$. Seien $\bar{a}, \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ mit $\bar{a} \cdot \bar{b} = \bar{0}$

$$\Rightarrow \exists q \in \mathbb{Z} : ab = qn$$

Da n Primzahl, kommt n n der Primfaktorzerlengung von ab als Primfaktor vor
$\Rightarrow n$ kommt in der Primfaktorzerlegung von a oder b als Primfaktor vor

$$\Rightarrow n \mid a \vee n \mid b \Rightarrow \bar{a} = \bar{0} \vee \bar{b} = \bar{0}$$

3.3 Körper

Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$, in dem gilt $K \neq 0$ und jedes Element $a \in K, a \neq 0$ besitzt ein Inverses in K bezüglich "$\cdot$", das heißt: $\exists b \in K : a \cdot b = 1_K$. Wir setzen $K^* := K \setminus \{0\}$

3.3.1 Beispiel

1. $(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot)$ sind Körper (mit den üblichen $+, \cdot$)
2. $\frac{\mathbb{Z}}{3\mathbb{Z}}$ ist ein Körper (betrachte Verknüpfungstafel)
3. $\frac{\mathbb{Z}}{4\mathbb{Z}}$ ist ein kein Körper: Das Element $\bar{2}$ besitzt kein Inverses bezüglich "$\cdot$"

3.3.2 Bemerkung 6.11

K Körper, Dann gilt:

1. $0_K \neq 1_K$
2. K ist ein Integritätsbereich
3. $(K^*, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_K

Beweis

1. folgt aus 3.2.3
2. $K \neq 0$ nach Definition. Seien $a, b \in K$ mit $ab = 0_K$. Falls $a \neq 0_K$ dann

$$b = 1_K \cdot b = (a^{-1}a) \cdot b = a^{-a}(ab) = a^{-1} \cdot 0_K = 0_K$$

Insebesondere gilt: $a = 0 \vee b = 0$

3. $K^* \times K^* \to K^*$ ist wohldefiniert nach 2 (aus $a, b \in K^*$ folgt $ab \in K^*$)
   Da $(K, \cdot)$ abelscher Monoid mit neutralem Element 1_K ist auch $(K^*, \cdot)$ abelscher Monid mit neutralem Element 1_K. Nach 3.3 besitzt jedes Element $a \in K^*$ ein Inverses $b \in K$ mit $ab = 1_K$ Wegen $0_K \neq 1_K$ ist $b \neq 0_K$ (sonst $ab = a \cdot 0_K = 0_K \neq 1_K$), das heißt $b \in K^*$ □

3.3.3 Bemerkung 6.12

R Integritätsbereich, der nur endlich viele Elemente hat. Dann ist R ein Körper.

Beweis R Integritätsbereich $\Rightarrow R \neq 0$
Noch zu zeigen: $a \in R \setminus \{0_R\} \Rightarrow \exists b \in R : ab = 1_R$ Sei $a \in R \setminus \{0_R\}$. Wir betrachten die Abbildung $\varphi_a : R \to R, x \mapsto ax$

1. Behauptung: φ_a ist injektiv, denn:

   Seien $x, y \in R$ mit

   $$\varphi_a(x) = \varphi_a(y) \Rightarrow ax = ay \Rightarrow ax + (-(ay)) = 0_R \tag{20}$$

   Mit [[Bemerkung 6.3]] folgt:

   $$\Rightarrow ax + a(-a) = -R \Rightarrow a(x - y) = 0_R \tag{21}$$

   Aus R Integrationsbereich und $a \neq 0$ folgt:

   $$x - y = 0 \Rightarrow x = y \tag{22}$$

2. Da R endlich ist und φ_a inejktiv ist, ist φ_a nach 2.6.7 surjektiv

   $$\Rightarrow \exists b \in R : \varphi_a(b) = 1_R \Rightarrow ab = 1_R$$

3.3.4 Folgerung 6.13

$n \in \mathbb{N}$ Dann sind äquivalent

1. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist ein Körper
2. n ist eine Primzahl

Beweis $1 \Rightarrow 2$ durch Kontraposition: $\neq 2 \Rightarrow 1$
Sei n keine Primzahl $\Rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ kein Integritätsbereich $\Rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ kein Körper
$2 \Rightarrow 1$ Sei n eine Primzahl $\Rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ Integritätsbereich, der nur endlich viele Elemente hat $\Rightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ Körper

Notation p Primzahl. Man nennt $\mathbb{F}_P := \frac{\mathbb{Z}}{p\mathbb{Z}}$ auch den endlichen Körper mit p Elemente

3.3.5 Definition 6.14

R Ring

$$\operatorname{char}(R) := \begin{cases} 0 & \sum_{k=1}^{n} 1_R \neq 0 \, \forall \, n \in \mathbb{N} \\ \min\{n \in \mathbb{N} \mid \sum_{k=1}^{n} 1_R = 0_R\} & \text{sonst} \end{cases}$$

heißt die Charakteristik von R

Beispiel 1.

1. $\operatorname{char}(\mathbb{Z}) = \operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = 0$
2. $\operatorname{char}(\frac{\mathbb{Z}}{n\mathbb{Z}}) = n$, denn $\sum_{k=1}^{n} \bar{1} = \bar{n} = \bar{0}$ und $\sum_{k=1}^{m} \bar{1} = \bar{m} \neq \bar{0}$ für $m \in \{1, \ldots, n-1\}$

Bemerkung 1. R Integritätsbereich. Dann ist $\operatorname{char}(R) = 0$ oder $\operatorname{char}(R)$ ist eine Primzahl

Beweis. Beweis durch Widerspruch. Annahme: $\operatorname{char}(R) \neq 0$ und $\operatorname{char}(R)$ ist keine Primzahl.
Da R Integritätsbereich ist ist $1_R \neq 0_R$ also $\operatorname{char}(R) \neq 1$

$$\begin{aligned} &\Rightarrow \exists a, b \in \mathbb{N}, 1 < a, b < \operatorname{char}(R) : \operatorname{char}(R) = ab \\ &\Rightarrow 0_R = \sum_{k=1}^{\operatorname{char}(R)} 1_R = \sum_{k=1}^{a} 1_R \cdot \sum_{k=1}^{b} 1_R \\ &\xRightarrow{R \text{ Integritätsbereich}} \sum_{k=1}^{a} 1_R = 0_R \vee \sum_{k=1}^{b} = 0_R \\ &\Rightarrow \operatorname{char}(R) \leq a \vee \operatorname{char}(R) \leq b \lightning \text{ zu } a, b < \operatorname{char}(R) \end{aligned}$$ □

Bemerkung 2. K Körper, dann ist $\operatorname{char}(K) = 0$ oder $\operatorname{char}(K)$ ist Primzahl.

Beweis. Folgt aus 1 und 3.3.2 □

Beispiel 2. p Primzahl, dann ist $\operatorname{char}(\mathbb{F}_|) = p$

4 Polynome

Definition 1 7.1 Polynome**.** K Körper, ein Polynom in der Varablen t über K ist ein Ausdruch der Form

$$f = \sum_{k=0}^{n} a_k t^k$$

mit $n \in \mathbb{N}_0$ (das heißt insbesondere nur endliche Summanden), $a_0, \ldots, a_n \in K$ (fehlende $a = 0$, ebenso setzen wir $a_{k>n} = 0$). Die a_k heißen die Koeffizienten von f

$$\deg(f) := \begin{cases} -\infty & f = 0 \\ \max\{k \in \mathbb{N}_0 \mid a_k \neq 0\} & f \neq 0 \end{cases}$$

heißt Grad von f. für $f \neq 0$ heißt $l(f) := a_{\deg(f)}$ heißt der Leitkoeffizient von f, $l(0) := 0$. f heißt normiert $\overset{\text{Def}}{\iff} l(f) = 1$ Hierbei sind zei Polynome $f = \sum_{k=0}^{n} a_k t^k, g = \sum_{k=0}^{m} b_m t^k$ gleich $(f = g) \overset{\text{Def}}{\iff} \deg(f) = \deg(g) =: r$ und $a_r = b_r, \ldots, a_1 = b_1, a_0 = b_0$

Bemerkung 3. Man kann das auch präzise macchen (Algebra 1, WS15/16, Blatt 5, Aufgabe 3)

Beispiel 3 7.2.

1. $f = \frac{3}{4}x^2 - 7x + \frac{1}{2} \in \mathbb{Q}[x] \Rightarrow \deg(f) = 2, l(f) = \frac{3}{4}, f$ ist nicht normiert
2. $f = x^5 - \frac{1}{3}x + \frac{2}{5} \in \mathbb{Q}[x] \Rightarrow \deg(f) = 5, l(f) = 1, f$ ist normiert

Bemerkung 4 7.3. K Körper, $f, g \in K[t], f = \sum_{k=0}^{n} a_k t^k, g = \sum_{k=0}^{m} b_k t^k$. Wir setzen $r := \max\{m, n\}$ und definieren

$$f + g = (a_r + b_r)t^r + \ldots + (a_1 + b_1)t + (a_0 + b_0)$$
$$f \cdot g = c_{n+m}t^{n+m} + \ldots + c_1 t + c_0, c_k := \sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} a_i b_j$$

Mittels der Verknüpfung $+, \cdot$ wir die Menge aller Polynome über K in der Variablen $t (=: K[t])$ zu einem kommutativen Ring, dem Polynomring über K in der Variablen t

Beweis. Man rechnet die Ringaxiome nach □

Bemerkung 5 7.4. K Körper, $f, g \in K[t]$, Dann gilt:

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(fg) = \deg(f) + \deg(g)$

(Hierbei setzt man Formel für $n \in \mathbb{N}_0 : -\infty < n, n + (-\infty) = -\infty = (-\infty) + n, (-\infty) + -(\infty) = -\infty$)

Beweis. Falls $f = 0$ oder $g = 0$, dann sind 1. und 2. klar. Im Folgenden seien $f, g \neq 0$, etwa $f = \sum_{k=0}^{n} a_k t^k, g = \sum_{k=0}^{m} b_k t^k$ mit $a_n, b_m \neq 0$ (insbesondere $\deg(f) = n, \deg(g) = m$)

1. Wir setzen $k := \max\{m, n\}$

   $\Rightarrow f + g = (a_k + b_k)t^k + \ldots + (a_1 + b_1)t + (a_0 + b_0)$
   $\Rightarrow \deg(f + g) \leq k$ (beachte: Ex könnte $a_k + b_k = 0$ sein)

2. Es sei $fg = a_n b_m t^{n+m} + \ldots + a_0 b_0$ und es ist $a_n b_m \neq 0$ da K als Körper ein Integritätsbereich ist $\Rightarrow \deg(fg) = n + m$

□

Folgerung 1 7.5. K Körper, dann ist $K[t]$ ein Integritätsbereich

Beweis. $K[t] \neq 0$ klar (zum Beispiel $t \in \approx$) Seien $f, g \in K[t], f, g \neq 0 \Rightarrow \deg(f), \deg(g) \geq 0 \Rightarrow \deg(fg) = \deg(f) + \deg(g) \geq 0 \Rightarrow fg \neq 0$ □

Bemerkung 6. $K[t]$ ist kein Körper: Das Polynom $t \in K[t]$ besitzt kein Inverses bezüglich "$\cdot$", denn:
Wäre $f \in K[t]$ invers zu t, dann wäre $ft = 0 \Rightarrow \deg(1) = 0 \deg(ft) = \deg(f) + \deg(t) = \deg(f) + 1 \Rightarrow \deg(f) = -1 \lightning$

Satz 1 7.6 Polynomdivision**.** *K Körper, $f, g \in K[t], g \neq 0$*
Dann existieren eindeutig bestimmte Polynome $q, r \in K[t]$, mit $f = qg + r$ und $\deg(r) < \deg(g)$

Beispiel 4 7.7. $f = 3t^3 + 5t + 1, g = t^2 + 1 \in \mathbb{Q}[t]$

$$(3t^3 + 5t + 1) : (t^2 + 1) = 3t$$

Also $3t^3 + 5t + 1 = 3^t(t^2 + 1) + 2t + 1, q = 3t, r = 2t + 1$

Beweis. 1. Existenz:
Falls $f = 0$, setzen wir $q := 0, r := 0$ fertig.
Im Folgenden sei $f \neq 0$, das Polynom g sei fixiert. Wir zeigen die Existenz von q, r per Induktion nach $\deg(f) \in \mathbb{N}_0$

- Induktionsanfang: (etwas unkonventionell, geht aber auch): $\deg(f) \in \{0, \ldots, \deg(g) - 1\}$ (das heißt $\deg(f) < \deg(g)$)
  Setze $q := 0, r := g$, dann ist $f = qg + r, \deg(r) = \deg(f) < \deg(g)$.
- Induktionsschritt: Es sei $\deg(f) \geq \deg(g)$ und die Behauptung sei für alle Polynome aus $K[t]$ von Grad $< \deg(f)$ schon gezeigt.
  Wir sezen $n := \deg(f), m := \deg(g)$ und schreiben:

$$f = l(f)t^n + \text{ Terme kleineren Grades}$$

$$g = l(g)t^m + \text{ Terme kleineren Grades}$$

Es ist $f - \frac{l(f)}{l(g)} t^{n-m} g =$

$$l(f)t^n + \text{ Terme kleineren Grades} - \underbrace{\frac{l(f)}{l(g)} t^{n-m} l(g) t^m}_{l(f)t^n} + \text{ Terme kleineren Grades}$$

$$\Rightarrow \deg(f - \frac{l(f)}{l(g)} t^{n-m}) < n$$

Nach Induktionsannahme gilt: Es existert $q_1, r_1 \in K[t]$ mit

$$f - \frac{l(f)}{l(g)} t^{n-m} g = q_1 g + r_1, \text{ mit } \deg r_1 < \deg(g)$$

$$\to f = (q_1 + \frac{l(f)}{l(g)} t^{n-1})g + r_1$$

Setze $q := q_1 + \frac{l(f)}{l(g)} t^{n-m}, r := r_1$, dann ist $f = qg + r$ und $\deg(r) < \deg(g)$

2. Eindeutigkeit: Seien $q_1, q_2, r_1, r_2 \in K[T]$ mit $f = q_1 g + r_1 + q_2 g + r_2$ und $\deg(r_1) < \deg(g), \deg(r_2) < \deg(g)$

$$\Rightarrow (q_1 - q_2)g = r_2 - r_1$$
$$\Rightarrow \deg(g_1 - q_2) + \deg(g) = \deg(r_1 - r_2)$$

Falls $q_1 \neq q_2$, dann sind beide Seiten der Gleichung in $\mathbb{N}_0$ und es wäre

$$\deg(g) \leq \deg(r_2 - r_1)$$

Nach 5 ist $\deg(r_2 - r_1) \leq \max\{\deg(r_2), \deg(-r_1)\} < \deg(g)$↯ Also $q_1 = q_2$, somit $r_2 - r_1 = \underbrace{q_1 - q_2}_{=0} g = 0$, also $r_1 = r_2$

□