VORLESUNGSSKRIPT
LINEARE ALGEBRA

WINTERSEMESTER 2023

Roland Herzog[*]

2023-12-10

---

[*] Interdisciplinary Center for Scientific Computing, Heidelberg University, 69120 Heidelberg, Germany (roland.herzog@iwr.uni-heidelberg.de, `https://scoop.iwr.uni-heidelberg.de/team/rherzog`).

Dieses Skript orientiert sich an früheren Vorlesungen von Jan Johannes und Alexander Schmidt (Universität Heidelberg).

Änderungen gegenüber bereits veröffentlichten Versionen werden in dieser Farbe gekennzeichnet.

Material für 27–29 Vorlesungen (Lineare Algebra I).

Kommentare und Korrekturen bitte an roland.herzog@iwr.uni-heidelberg.de.

Inhaltsverzeichnis

Kapitel 1 Mathematische Grundlagen

Die **Algebra** (von arabisch الجبر, *al-ǧabr*, „das Zusammenfügen gebrochener Teile“, englisch: algebra) hat ihren Ursprung in der Beschreibung von Lösungsverfahren linearer und quadratischer Gleichungen. Heute versteht den Begriff Algebra deutlich weiter, es geht jedoch immer um Strukturen, Abbildungen zwischen Strukturen und die in ihnen geltenden „Rechen“regeln. Speziell die **lineare Algebra** (englisch: linear algebra) befasst sich mit „linearen Strukturen“, das sind vor allem Vektorräume, Abbildungen zwischen Vektorräumen und lineare Gleichungssysteme.

Wie andere Wissenschaften auch hat die Mathematik eine eigene Sprache, die man erlernen muss, um die Gegenstände dieser Wissenschaft zu verstehen und sich sachgerecht ausdrücken und argumentieren zu können. Das Herz der Mathematik bilden Beweise. Jede Aussage, jeder Lehrsatz muss bewiesen werden, d. h., durch logische Verknüpfungen aus den verwendeten Grundaxiomen und bereits bewiesenen Aussagen hergeleitet werden.

Eine streng formale, axiomatische Einführung der Logik und logischer Schlussweisen ist im Rahmen dieser Lehrveranstaltung leider nicht möglich. Diese kann später bei Interesse in weiterführenden Veranstaltungen zur Logik nachgeholt werden. Wir beschränken uns hier auf eine „naive“ (nicht-axiomatische) Einführung in die Logik.

§ 1 Aussagenlogik

Literatur: Deiser, 2022b, Kapitel 1.1, Magnus u. a., 2023, Kapitel 1–14

Definition 1.1 (Aussage, Wahrheitswert)**.**

Eine **Aussage** (englisch: statement) ist ein Satz (einer Sprache), dem eindeutig entweder der **Wahrheitswert wahr** (kurz: W oder $\top$, englisch: true, T) oder der **Wahrheitswert falsch** (kurz: F oder $\perp$, englisch: false, F) zugeordnet werden kann.

Der Satz kann dabei der gewöhnlichen Sprache oder der mathematischen Sprache entstammen. Wir bezeichnen Aussagen in der Regel mit Großbuchstaben wie A, B usw.

Beispiel 1.2 (Aussagen und Nicht-Aussagen)**.**

(*i*) A: 9 ist durch 3 teilbar.
Dieses ist eine wahre Aussage.

(ii) B: Am 17.10.2023 ist London die Hauptstadt von Frankreich.
Dieses ist eine falsche Aussage.

(iii) C: München ist 781 km von Hamburg entfernt.
Dieses ist keine Aussage, da der Satz zuviel Interpretationsspielraum lässt. Was ist mit „München" und „Hamburg" gemeint? Mit welcher Toleranz ist die Entfernungsangabe zu verstehen?

(iv) D: Das Team des VfL Wolfsburg ist ~~wird~~ in der Saison 2023/24 deutscher Meister in der Frauen-Fußball-Bundesliga.
Dieses ist eine Aussage, deren Wahrheitswert wir im Moment aber nicht kennen.

(v) E: Es gibt unendlich viele Primzahlzwillinge.
Dieses ist eine ebenfalls Aussage, deren Wahrheitswert wir zur Zeit nicht kennen.[1]

Ein grundlegendes Prinzip in der Mathematik ist es, aus bekannten Objekten durch Verknüpfung neue Objekte zu schaffen. In der Logik heißen diese Verknüpfungen **Junktoren** (englisch: logical operators, junction, lateinisch: iungere: verbinden, verknüpfen). Ein Junktor erschafft also aus einer oder aus mehreren Aussagen eine neue Aussage. Der Wahrheitswert der neuen Aussage ergibt sich aus den Wahrheitswerten der miteinander verknüpften Aussagen. Wir definieren einen Junktor über seine **Wahrheitswerttabelle** (auch: **Wahrheitstafel**, englisch: truth table).

Definition 1.3 (Junktoren)**.**

Im Folgenden seien A und B Aussagen. Wir definieren folgende wichtige ein- und zweistellige Junktoren.

(i) **Negation** (**Verneinung**, englisch: negation) $\neg$

Die Operation $\neg A$ (sprich: „nicht A") heißt **Negation**. $\neg A$ ist wahr, wenn A falsch ist, und falsch, wenn A wahr ist.

A	$\neg A$
W	F
F	W

(ii) **Konjunktion**[2] (**Und-Verknüpfung**, englisch: conjunction) $\wedge$

Die Aussage $A \wedge B$ (sprich: „A und B") ist dann wahr, wenn A und B beide wahr sind, ansonsten falsch.

A	B	$A \wedge B$
W	W	W
W	F	F
F	W	F
F	F	F

---

[1] siehe Primzahlzwillingsvermutung

[2] lateinisch: coniungere: verbinden

(*iii*) **Disjunktion**[3] (**Oder-Verknüpfung**, englisch: disjunction) $\vee$

Die Aussage $A \vee B$ (sprich: „A oder B“) ist wahr, wenn mindestens eine der Aussagen A und B wahr ist, ansonsten falsch. Das „Oder“ ist also in einem nicht-ausschließenden Sinne gemeint.

A	B	$A \vee B$
W	W	W
W	F	W
F	W	W
F	F	F

(*iv*) **Implikation**[4] (**Konditional**[5], **Wenn-Dann-Verknüpfung**, englisch: implication) $\longrightarrow$

Die Aussage $A \longrightarrow B$ ist über die nebenstehende Wahrheitswerttabelle definiert. Man benennt die Aussage auch als „A ist **hinreichend** für B“ (englisch: „A is sufficient for B“), „B ist **notwendig** für A“ (englisch: „B is necessary for A“), „A impliziert B“ (englisch: „A implies B“) oder „Wenn A, dann B“ (englisch: „If A, then B“). In einer Implikation $A \longrightarrow B$ nennt man A auch das **Antezedens** (englisch: antecedent, lateinisch: antecedens: das Vorausgehende) und B das **Konsequens** (englisch: consequent, lateinisch: consequentis: folgerichtig).

A	B	$A \longrightarrow B$
W	W	W
W	F	F
F	W	W
F	F	W

Die Implikation behauptet keinerlei kausalen oder sonstigen inhaltlichen Zusammenhang zwischen den Aussagen A und B. Man spricht auch von **materialer Implikation** (englisch: material implication). Die häufig anzutreffende Sprechweise „Wenn A, dann B“ ist daher problematisch, weil wir diese intuitiv als Kausalität oder zeitliche Nähe interpretieren.

(*v*) **Äquivalenz**[6] (**Bikonditional**, **Genau-Dann-Wenn-Verkn.**, englisch: equivalence) $\longleftrightarrow$

Die Aussage $A \leftrightarrow B$ ist wahr, wenn entweder A und B beide wahr oder beide falsch sind, ansonsten falsch. Man benennt die Aussage auch als „A ist **notwendig und hinreichend** für B“ (englisch: „A is necessary and sufficient for B“), „A ist äquivalent zu B“ (englisch: „A is equivalent to B“), „A genau dann, wenn B“ oder „A dann und nur dann, wenn B“ (englisch: „A if and only if B“, „A iff B“).

A	B	$A \leftrightarrow B$
W	W	W
W	F	F
F	W	F
F	F	W

Auch hier gilt, dass die Äquivalenz nichts über einen eventuellen kausalen oder sonstigen inhaltlichen Zusammenhang zwischen den Aussagen A und B aussagt. Man spricht auch von **materialer Äquivalenz** (englisch: material equivalence).

Quizfrage 1.1: Wieviele verschiedene einstellige Junktoren gibt es? Wieviele zweistellige?

Quizfrage 1.2: Können Sie alle zweistelligen Junktoren aus den oben genannten, also aus $\neg$ sowie $\wedge$, $\vee$, $\longrightarrow$ und $\leftrightarrow$, zusammensetzen? Reicht evtl. sogar eine Teilmenge davon aus?

Beispiel 1.4 (Symbolisierung von Sätzen der Umgangssprache[7]).
Die Symbolisierung von Sätzen der Umgangssprache in logische Aussagen ist nicht immer ganz einfach. Es folgen einige Beispiele jeweils mit einer oder mehreren gleichwertigen Symbolisierungen.

---

[3] lateinisch: disiungere: trennen, unterscheiden

[4] lateinisch: implicare: verwickeln

[5] lateinisch: conditio: Bedingung

[6] lateinisch: aequivalens: gleichwertig

[7] angelehnt an Beispiele aus Magnus u. a., 2023, Kapitel 5, genutzt unter der Lizenz CC-BY 4.0

(*i*) Zum Burger servieren wir Pommes oder Salat.
Das „oder“ ist hier im ausschließenden Sinne gemeint.

P: Zum Burger servieren wir Pommes.
S: Zum Burger servieren wir Salat.

- $(P \vee S) \wedge (\neg(P \wedge S))$
- $(P \wedge (\neg S)) \vee (S \wedge (\neg P))$

(*ii*) Obwohl Barbara energisch ist, ist sie nicht sportlich.

E: Barbara ist energisch.
S: Barbara ist sportlich.

- $E \wedge (\neg S)$

(*iii*) Du wirst keine Suppe bekommen, aber dafür den Salat.

S_1: Du wirst Suppe bekommen.
S_2: Du wirst Salat bekommen.

- $(\neg S_1) \wedge S_2$

(*iv*) Du wirst Dich erkälten, es sei denn, Du trägst eine Jacke.

J: Du trägst eine Jacke.
E: Du wirst Dich erkälten.

- $(\neg J) \longrightarrow E$
- $J \vee E$

An den Beispielen sieht man, dass unter der formalen Symbolisierung Nuancen der Sprache zugunsten der Präzision verloren gehen.

Lemma 1.5 (Umschreibung von $\longrightarrow$ und $\longleftrightarrow$)**.**
Es seien A und B Aussagen.

(*i*) Die Aussagen

- $A \longrightarrow B$
- $(\neg A) \vee B$
- $(\neg B) \longrightarrow (\neg A)$

haben dieselben Wahrheitstafeln.

(*ii*) Die Aussagen

- $A \longleftrightarrow B$
- $(A \longrightarrow B) \wedge (B \longrightarrow A)$

haben dieselben Wahrheitstafeln.

Beweis. Wir stellen die Wahrheitstafeln für die drei Aussagen in Aussage (*i*) auf:

A	B	$A \to B$	$(\neg A) \vee B$	$\neg B$	$\neg A$	$(\neg B) \to (\neg A)$
W	W	W	W	F	F	W
W	F	F	F	W	F	F
F	W	W	W	F	W	W
F	F	W	W	W	W	W

Der Beweis der Aussage (ii) ist Teil von Hausaufgabe 1.3. □

Da die Verknüpfung von Aussagen stets wieder auf Aussagen führt, können wir durch wiederholte Verknüpfung komplexe Aussagen aufbauen, wie etwa $(A \to D) \to ((B \vee C) \to (D \wedge C))$. Zur Vereinfachung der Notation vereinbaren wir folgende Bindungsregeln:

$$\neg \text{ bindet stärker als } \wedge \text{ bindet stärker als } \vee \text{ bindet stärker als } \to \text{ bindet stärker als } \leftrightarrow . \tag{1.1}$$

Diese Regeln erlauben uns, auf Klammern zu verzichten. Beispielsweise ist

$$\begin{aligned} (\neg A) \wedge B \quad &\text{dasselbe wie} \quad \neg A \wedge B \\ \text{und} \quad (\neg(A \wedge B)) \to (B \vee \neg B) \quad &\text{dasselbe wie} \quad \neg(A \wedge B) \to B \vee \neg B. \end{aligned}$$

Es gilt jedoch, dass Klammern zur Verdeutlichung nicht schaden können. Statt $(\cdot)$ können auch $[\cdot]$ oder $\{\cdot\}$ verwendet werden.

Wir berechnen jetzt die Wahrheitstafeln einiger zusammengesetzter Aussagen.

Beispiel 1.6 (Wahrheitstafeln zusammengesetzter Aussagen)**.**

(i) $\neg(\neg A \wedge \neg B)$

A	B	$\neg A$	$\neg B$	$\neg A \wedge \neg B$	$\neg(\neg A \wedge \neg B)$
W	W	F	F	F	W
W	F	F	W	F	W
F	W	W	F	F	W
F	F	W	W	W	F

Diese Wahrheitstafel ist offenbar dieselbe wie die von $A \vee B$.

(ii) $A \vee B \to B \wedge C$

A	B	C	$A \vee B$	$B \wedge C$	$A \vee B \to B \wedge C$
W	W	W	W	W	W
W	W	F	W	F	F
W	F	W	W	F	F
W	F	F	W	F	F
F	W	W	W	W	W
F	W	F	W	F	F
F	F	W	F	F	W
F	F	F	F	F	W

(iii) $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

A	B	$\neg(A \wedge B)$	$\neg A \vee \neg B$	$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
W	W	F	F	W
W	F	W	W	W
F	W	W	W	W
F	F	W	W	W

Die letzte Aussage $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$ hat also immer den Wahrheitswert W, unabhängig von den Wahrheitswerten der Aussagen A und B. Eine solche Aussage nennt man **Tautologie**[8] (englisch: tautology) oder **logisches Gesetz**. Tautologien spielen eine entscheidende Rollen in mathematischen Beweisen, siehe § 3.

Definition 1.7 (logische Implikation, logische Äquivalenz)**.**

Es seien A und B Aussagen.

(i) Die Aussage B heißt eine **logische Implikation** (englisch: logical implication) der Aussage A, wenn $A \to B$ eine Tautologie ist. A heißt dann **Prämisse** (englisch: premise), und B heißt **Konklusion** (englisch: conclusion). Wir schreiben: $A \Rightarrow B$ und sagen: „A impliziert B“ oder „B folgt aus A“.

(ii) Die Aussagen A und B heißen **logisch äquivalent (zueinander)** (englisch: logically equivalent), wenn $A \leftrightarrow B$ eine Tautologie ist. Wir schreiben: $A \Leftrightarrow B$ und sagen: „A ist äquivalent zu B“ oder „A und B sind (zueinander) äquivalent“.

Beachte: Die logische Implikation und die logische Äquivalenz sind *Aussagen über Aussagen.* Sie sind von den Junktoren „Implikation“ (Konditional) und „Äquivalenz“ (Bikonditional) zu unterscheiden!

Wir vereinbaren, dass $\Rightarrow$ und $\Leftrightarrow$ noch schwächer binden als die Junktoren in (1.1).

Beispiel 1.8 (logische Implikationen und Äquivalenzen)**.**

(i) Die Aussage $(A \to B) \wedge A$ impliziert die Aussage B, kurz: $(A \to B) \wedge A \Rightarrow B$, denn $(A \to B) \wedge A \to B$ ist eine Tautologie:

A	B	$A \to B$	$(A \to B) \wedge A$	$(A \to B) \wedge A \to B$
W	W	W	W	W
W	F	F	F	W
F	W	W	F	W
F	F	W	F	W

(ii) Die Aussagen $\neg(A \wedge B)$ und $\neg A \vee \neg B$ sind logisch äquivalent, kurz: $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$, denn $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$ ist eine Tautologie, wie in Beispiel 1.6 gerade schon gezeigt wurde.

---

[8] altgriechisch: *ταυτο*: dasselbe

Satz 1.9 (logische Implikationen und Äquivalenzen)**.**
Es seien A, B und C Aussagen. Es gelten die folgenden Implikationen und Äquivalenzen.

$\neg(\neg A) \Leftrightarrow A$ doppelte Verneinung[9] (1.2)

$A \Rightarrow \top$ „Aus Beliebigem folgt Wahres.“[10] (1.3a)
$\bot \Rightarrow A$ „Aus Falschem folgt Beliebiges.“[11] (1.3b)

$A \wedge A \Leftrightarrow A$ **Idempotenz**[12] (1.4a)
$A \vee A \Leftrightarrow A$ **Idempotenz** (1.4b)

$A \wedge \top \Leftrightarrow A$ **Neutralität**[13] (1.5a)
$A \vee \bot \Leftrightarrow A$ **Neutralität** (1.5b)

$A \wedge \bot \Leftrightarrow \bot$ **Absorption**[14] (1.6a)
$A \vee \top \Leftrightarrow \top$ **Absorption** (1.6b)

$A \wedge \neg A \Leftrightarrow \bot$ **Komplementarität**[15] (1.7a)
$A \vee \neg A \Leftrightarrow \top$ **Komplementarität**[16] (1.7b)

$A \wedge B \Leftrightarrow B \wedge A$ **Kommutativität von $\wedge$**[17] (1.8a)
$A \vee B \Leftrightarrow B \vee A$ **Kommutativität von $\vee$** (1.8b)

$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$ **Assoziativität von $\vee$**[18] (1.9a)
$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$ **Assoziativität von $\wedge$** (1.9b)

$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ **De Morgansches Gesetz**[19] (1.10a)
$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ **De Morgansches Gesetz** (1.10b)

$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ **Distributivität**[20] (1.11a)
$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ **Distributivität** (1.11b)

Beweis. Der Beweis erfolgt durch Aufstellen der Wahrheitstafeln und wird hier nicht ausgeführt. □

Ende der Vorlesung 1

---

[9] lateinisch: duplex negatio affirmat
[10] lateinisch: verum ex quolibet
[11] lateinisch: ex falso quodlibet
[12] englisch: idempotence
[13] englisch: neutrality
[14] englisch: absorption
[15] englisch: complementarity
[16] Gesetz vom ausgeschlossenen Dritten, lateinisch: tertium non datur
[17] englisch: commutativity, lateinisch: commutare: tauschen, vertauschen
[18] englisch: associativity, lateinisch: associare: verbinden, beigesellen
[19] englisch: De Morgan’s law
[20] englisch: distributivity, lateinisch: distribuere: verteilen, aufteilen

§ 2 PRÄDIKATENLOGIK

Literatur: Magnus u. a., 2023, Kapitel 22–39

Die Aussagenlogik reicht für die Bedürfnisse der Mathematik nicht aus. Beispielsweise lässt sich die Aussage „Wenn n eine gerade ganze Zahl ist, dann ist auch n^2 eine gerade ganze Zahl.“ innerhalb der Aussagenlogik nicht wie erforderlich symbolisieren. Die Schwierigkeit ist, dass wir in der Aussagenlogik keine Aussagen mit Variablen zur Verfügung haben. Wir benötigen dazu die **Prädikatenlogik**[21], eine Erweiterung der Aussagenlogik. In der Prädikatenlogik ist es möglich, eine Aussage von dem Gegenstand, über den sie gemacht wird, zu trennen. Neben den schon bekannten Junktoren verwendet die Prädikatenlogik

- **Aussageformen** (englisch: statement) oder **Prädikate** (englisch: predicate), das sind sprachliche Gebilde mit Variablen (Leerstellen), die nach Einsetzen der Variablen in Aussagen übergehen.

  Beispiele:

  $$\begin{aligned} A(x) &: x \text{ wohnt in Aachen.} \\ Z(x) &: x \text{ ist eine gerade ganze Zahl.} \\ G(x, y) &: x \text{ ist mindestens so groß wie } y. \end{aligned}$$

  Die Anzahl der Variablen einer Aussageform heißt deren **Stelligkeit** (englisch: arity).

- **Quantoren** (englisch: quantifier), und zwar

  $\forall$ für alle (**Allquantor**, englisch: universal quantifier),
  $\exists$ es existiert (mindestens) ein (**Existenzquantor**, englisch: existential quantifier),
  $\exists!$ es existiert genau ein (**Eindeutigkeitsquantor**, englisch: uniqueness quantifier).

Zu jedem Quantor geben wir den **Grundbereich** (auch: **Individuenbereich**, **Diskursuniversum**, **Domäne**, englisch: universe of discourse, domain of discourse) an. In der Regel nimmt man an, dass der Grundbereich nicht leer ist, um gewisse Komplikationen auszuschließen. Der Grundbereich ist wichtig und beeinflusst den Wahrheitswert einer quantorisierten Aussage:

$\forall x \in \mathbb{N} \; (x \geqslant 0)$	„Alle natürlichen Zahlen sind nichtnegativ.“	(wahre Aussage)
$\forall x \in \mathbb{R} \; (x \geqslant 0)$	„Alle reellen Zahlen sind nichtnegativ.“	(falsche Aussage)

Beispiel 2.1 (Symbolisierung von Sätzen der Umgangssprache mit Quantoren).
Wir betrachten die Aussageformen

$$\begin{aligned} E(x) &: x \text{ hat 100 000 oder mehr Einwohner} \\ S(x) &: x \text{ ist eine Stadt} \end{aligned}$$

mit dem Grundbereich $O :=$ „Menge aller Orte in Deutschland“. Dann können wir die folgenden Aussagen wie angegeben symbolisieren:

Es gibt mindestens eine Stadt in Deutschland, die 100 000 oder mehr Einwohner hat.
$\exists x \in O \; (E(x) \land S(x))$

---

[21] genauer: Prädikatenlogik erster Stufe, englisch: first order logic

Es gibt genau einen Ort in Deutschland, der 100 000 oder mehr Einwohner hat, aber keine Stadt ist.
$\exists! x \in O \; (E(x) \wedge \neg S(x))$

Alle Städte in Deutschland haben 100 000 oder mehr Einwohner.
$\forall x \in O \; (S(x) \to E(x))$

Keine Stadt in Deutschland hat 100 000 oder mehr Einwohner.
$\neg\exists x \in O \; (E(x) \wedge S(x))$

Man sagt, dass die Variable einer Aussageform durch ihren Quantor **gebunden** (englisch: bound variable) wird. Auf den Namen der Variablen kommt es dabei übrigens nicht an, es sind also $\exists x \; (E(x) \wedge S(x))$ und $\exists y \; (E(y) \wedge S(y))$ äquivalente Aussagen.

Besonders mehrstellige Aussageformen spielen in vielen mathematischen Aussagen eine große Rolle. Die Reihenfolge verschiedener Quantoren ist dabei wichtig! Unterscheide zum Beispiel (siehe Lehrveranstaltung *Analysis*)

Die Funktion $f\colon (a,b) \to \mathbb{R}$ ist stetig:

$$\forall x \in (a,b) \; \forall \varepsilon > 0 \; \exists \delta > 0 \; \forall y \in (a,b) \; \underbrace{\bigl(|x-y| < \delta \to |f(x)-f(y)| < \varepsilon\bigr)}_{\text{vierstellige Aussageform}}.$$

Die Funktion $f\colon (a,b) \to \mathbb{R}$ ist gleichmäßig stetig:

$$\forall \varepsilon > 0 \; \exists \delta > 0 \; \forall x \in (a,b) \; \forall y \in (a,b) \; \bigl(|x-y| < \delta \to |f(x)-f(y)| < \varepsilon\bigr).$$

Für Aussagen mit Quantoren gelten folgende Regeln (ohne Beweis).

Satz 2.2 (logische Implikationen und Äquivalenzen von Aussagen mit Quantoren)**.**
Es seien A, B einstellige Aussageformen mit gemeinsamem Grundbereich und C eine zweistellige Aussageform. Es gelten die folgenden Implikationen und Äquivalenzen.[22]

$$\neg(\forall x \; A(x)) \quad \Leftrightarrow \quad \exists x \; (\neg A(x)) \qquad \text{Negation des Allquantors} \tag{2.1a}$$

$$\neg(\exists x \; A(x)) \quad \Leftrightarrow \quad \forall x \; (\neg A(x)) \qquad \text{Negation des Existenzquantors} \tag{2.1b}$$

$$\forall x \; \forall y \; C(x,y) \quad \Leftrightarrow \quad \forall y \; \forall x \; C(x,y) \qquad \textbf{Kommutativität gleicher Quantoren} \tag{2.2a}$$

$$\exists x \; \exists y \; C(x,y) \quad \Leftrightarrow \quad \exists y \; \exists x \; C(x,y) \qquad \textbf{Kommutativität gleicher Quantoren} \tag{2.3a}$$

$$\forall x \; (A(x) \wedge B(x)) \quad \Leftrightarrow \quad \forall x \; A(x) \wedge \forall x \; B(x) \qquad \textbf{Distributivität} \tag{2.4a}$$

$$\exists x \; (A(x) \vee B(x)) \quad \Leftrightarrow \quad \exists x \; A(x) \vee \exists x \; B(x) \qquad \textbf{Distributivität} \tag{2.4b}$$

$$(\forall x \; A(x)) \vee (\forall x \; B(x)) \quad \Rightarrow \quad \forall x \; (A(x) \vee B(x)) \tag{2.5a}$$

$$\exists x \; (A(x) \wedge B(x)) \quad \Rightarrow \quad (\exists x \; A(x)) \wedge (\exists x \; B(x)) \tag{2.5b}$$

---

[22] Aus Gründen der Lesbarkeit lassen wir die Angabe des Grundbereichs bei den Quantoren hier weg.

$$\forall x\ (A(x) \to B(x)) \quad \Rightarrow \quad (\forall x\ A(x)) \to (\forall x\ B(x)) \tag{2.6a}$$

$$\exists x\ (A(x) \to B(x)) \quad \Leftrightarrow \quad (\forall x\ A(x)) \to (\exists x\ B(x)) \tag{2.6b}$$

Auf https://de.wikipedia.org/wiki/Prädikatenlogik#Quantoren finden sich schöne Veranschaulichungen wahrer Aussagen mit zweistelligen Aussageformen und verschiedenen Quantoren.

§ 3 BEWEISMUSTER

Literatur: Deiser, 2022b, Kapitel 1.1, Magnus u. a., 2023, Kapitel 15–21

In einem Beweis versuchen wir in der Regel, für gegebene Aussagen A, B die Implikation $A \Rightarrow B$ nachzuweisen. Das heißt, wir müssen nachweisen, dass $A \to B$ eine Tautologie ist. Meistens besteht die Prämisse A selbst aus einer Konjunktion (Und-Verknüpfung) mehrerer einzelner Prämissen. Nicht alle Prämissen werden in der Formulierung eines mathematischen Satzes explizit genannt. Beispielsweise wird man die als wahr geltenden Grundannahmen (Axiome) über die reellen Zahlen nicht jedes Mal explizit erwähnen.

Ein Beweis wird oft in viele kleine Schritte zerlegt. Das Aufstellen einer Wahrheitswerttabelle ist nicht zielführend. Vielmehr werden wir Schlussregeln anwenden, die auf Tautologien beruhen. Solche Tautologien haben wir in Satz 1.9 und Satz 2.2 bereits aufgeführt. Dazu kommen die weiteren Tautologien

$$(A \to B) \wedge A \quad \Rightarrow \quad B \qquad \textbf{modus ponendo ponens}, \tag{3.1a}$$

$$(A \to B) \wedge \neg B \quad \Rightarrow \quad \neg A \qquad \textbf{modus tollendo tollens}, \tag{3.1b}$$

$$(A \to \neg B) \wedge A \quad \Rightarrow \quad \neg B \qquad \textbf{modus ponendo tollens}^{23}, \tag{3.1c}$$

$$(\neg A \to B) \wedge \neg A \quad \Rightarrow \quad B \qquad \textbf{modus tollendo ponens}^{24}, \tag{3.1d}$$

$$(A \to B) \wedge (B \to C) \quad \Rightarrow \quad (A \to C) \qquad \textbf{Kettenschluss} \text{ (englisch: chain inference).} \tag{3.2}$$

Quizfrage 3.1: Können Sie einfache Beispiele in Alltagssprache für die Argumentation gemäß der vier Argumentationsmuster in (3.1a)–(3.1d) angeben?

Folgende Beweismuster für Implikationen $A \Rightarrow B$ werden häufig verwendet:

(1) Beim **direkten Beweis** (englisch: direct proof) wird $A \Rightarrow B$, typischerweise unter Verwendung von Axiomen und bereits bewiesenen Sätzen, direkt mit Hilfe von Schlussregeln hergeleitet.

(2) Beim **indirekten Beweis** oder **Beweis durch Kontraposition** (englisch: indirect proof, proof by contrapositive) nutzen wir die Äquivalenz $(A \to B) \Leftrightarrow (\neg B \to \neg A)$ aus. Wir führen also einen direkten Beweis für $\neg B \Rightarrow \neg A$.

(3) Beim **Widerspruchsbeweis** (englisch: proof by contradiction, lateinisch: reductio ad adsurdum: Zurückführung auf das Sinnlose) nutzen wir die Äquivalenz $(A \to B) \Leftrightarrow (A \wedge \neg B) \to \bot$ aus. Dazu nehmen wir die Aussage A als wahr und die Aussage B als falsch an und zeigen, dass dann $\bot$ folgt.

---

[23] Der modus ponendo tollens wird häufig als $\neg(A \wedge B) \wedge A \;\Rightarrow\; \neg B$ geschrieben.

[24] Der modus tollendo ponens wird häufig als $(A \vee B) \wedge \neg A \;\Rightarrow\; B$ geschrieben.

(4) Beim **Beweis durch Fallunterscheidung** (englisch: proof by distinction of cases) nutzen wir die Äquivalenz $(A \wedge C \longrightarrow B) \wedge (A \wedge \neg C \longrightarrow B) \Leftrightarrow A \longrightarrow B$. Dabei ist C irgendeine weitere Aussage. Wir nehmen also zunächst die Aussagen A und C als wahr an und zeigen, dass dann auch die Aussage B wahr ist. Anschließend nehmen wir die Aussage A weiterhin als wahr aber die Aussage C als falsch an und zeigen, dass dann wiederum die Aussage B wahr ist.

Beispiel 3.1 (verschiedene Beweismuster)**.**

(1) **direkter Beweis**

Behauptung: Für natürliche Zahlen m, n gelte $m^2 < n^2$, dann gilt auch $m < n$.

Wir symbolisieren die zugehörigen Aussagen über zweistellige Aussageformen:

$$\begin{aligned} A(m,n) &: m^2 < n^2 \\ B(m,n) &: m < n \end{aligned}$$

und verwenden als Grundbereich für beide Variablen in beiden Aussageformen die Menge $\mathbb{N} := \{1, 2, 3, \dots\}$ der natürlichen Zahlen. Wir wollen zeigen:

$$\forall m \in \mathbb{N}\ \forall n \in \mathbb{N}\ \big(A(m,n) \Rightarrow B(m,n)\big).$$

Es seien dazu $m, n \in \mathbb{N}$.

$$\begin{aligned} & m^2 < n^2 && \text{nach Definition von } A \\ \Rightarrow\quad & 0 < n^2 - m^2 && \text{nach Subtraktion von } m^2 \\ \Rightarrow\quad & 0 < (n-m)(n+m) && \text{nach Rechenregeln in } \mathbb{N} \\ \Rightarrow\quad & 0 < n - m && \text{da } n+m > 0 \text{ und nach Regeln von } < \text{ in } \mathbb{N} \\ \Rightarrow\quad & m < n && \text{nach Rechenregeln in } \mathbb{N}. \end{aligned}$$

Ab sofort werden wir solche Beweise als Fließtext schreiben, etwa wie folgt: „Es seien $m, n \in \mathbb{N}$ und $m^2 < n^2$. Dann gilt auch $0 < n^2 - m^2 = (n-m)(n+m)$. Die Division durch die positive Zahl $n + m$ ergibt $0 < n - m$, also auch $m < n$, was zu zeigen war.“

Die konkrete Benennung der verwendeten Aussageformen A und B war für den Beweis auch nicht wesentlich, sodass wir im Folgenden darauf verzichten können.

(2) **Beweis durch Kontraposition**

Behauptung: Für natürliche Zahlen $n \in \mathbb{N}$ gilt: Wenn $4^n - 1$ eine Primzahl ist, dann ist notwendig n ungerade.

Kontraposition der Behauptung: Für natürliche Zahlen $n \in \mathbb{N}$ gilt: Wenn n gerade ist, dann ist $4^n - 1$ keine Primzahl.

Beweis: Es sei $n \in \mathbb{N}$ gerade, also gilt $n = 2k$ für eine Zahl $k \in \mathbb{N}$. Damit ist $4^n - 1 = 4^{2k} - 1 = (4^k - 1)(4^k + 1)$. Beide Faktoren sind > 1, d. h., $4^n - 1$ ist keine Primzahl.

(3) **Widerspruchsbeweis**[25]

Behauptung: Für alle reellen Zahlen $x \in \mathbb{R}$ gilt $\sin x + \cos x \neq \frac{3}{2}$.

Beweis: Wir nehmen an, es gäbe eine Zahl $x_0 \in \mathbb{R}$ mit der Eigenschaft $\sin x + \cos x = \frac{3}{2}$. Durch Quadrieren folgt dann $(\sin x_0)^2 + (\cos x_0)^2 + 2\,(\sin x_0)(\cos x_0) = \frac{9}{4}$. Wegen $(\sin x)^2 + (\cos x)^2 = 1$

---

[25] Dieses Beispiel ist Thiele, 1979 entnommen.

und $2\,(\sin x)(\cos x) = \sin(2\,x)$ für alle $x \in \mathbb{R}$ (insbesondere auch für x_0) folgt also $\sin(2\,x_0) = \frac{5}{4} > 1$. Jedoch nimmt die sin-Funktion nur Werte zwischen -1 und 1 an.

Weitere klassische Aussagen, die typischerweise mit Widerspruchsbeweisen gezeigt werden, sind „Es gibt unendlich viele Primzahlen“ und „$\sqrt{2}$ ist keine rationale Zahl“.

(4) **Beweis durch Fallunterscheidung**

Behauptung: Für jede ganze Zahl $n \in \mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ gilt: $n^2 + n$ ist gerade.

Beweis: Es sei $n \in \mathbb{Z}$. Wir unterscheiden zwei Fälle:

Fall 1: n ist ungerade.

In diesem Fall gilt also $n = 2\,k + 1$ für ein $k \in \mathbb{Z}$. Dann ist

$$n^2 + n = (2\,k + 1)^2 + 2\,k + 1 = 4\,k^2 + 4\,k + 1 + 2\,k + 1 = 4\,k^2 + 6\,k + 2,$$

also eine gerade Zahl.

Fall 2: n ist gerade.

In diesem Fall gilt also $n = 2\,k$ für ein $k \in \mathbb{Z}$. Dann ist

$$n^2 + n = (2\,k)^2 + 2\,k = 4\,k^2 + 2\,k,$$

also wiederum eine gerade Zahl.

Das Ende eines Beweises wird oft mit der Abkürzung **q.e.d.** (lateinisch: quod erat demonstrandum: was zu zeigen war, englisch: what was to be proved) oder mit dem Symbol □ markiert.

Andere Sätze sind nicht als Implikation formuliert, sondern in Form mehrerer äquivalenter Aussagen $A_1 \Leftrightarrow A_2 \Leftrightarrow \cdots \Leftrightarrow A_n$. In diesem Fall verwenden wir häufig einen

(5) **Beweis durch Ringschluss** (englisch: closed chain inference). Bei diesem zeigen wir nacheinander die Implikationen $A_1 \Rightarrow A_2$, $A_2 \Rightarrow A_3$ usw. bis $A_{n-1} \Rightarrow A_n$ und $A_n \Rightarrow A_1$, was dann wiederum die gewünschten Äquivalenzen zur Folge hat. Das erfordert n Beweisschritte. Wir können sogar allgemeiner solange verschiedene Implikationen $A_i \Rightarrow A_j$ zeigen, bis wir mittels Kettenschluss von jeder der beteiligten Aussagen zu jeder anderen Aussage gelangen können. Die Anzahl der zu zeigenden Implikationen beträgt aber mindestens n.

Quizfrage 3.2: Wieviele Implikationen wären zu zeigen, wenn man die Äquivalenz der Aussagen A_i und A_j für $i, j = 1, \dots, n$ mit $i \neq j$ paarweise zeigen würde?

Schließlich betrachten wir noch den

(6) **Beweis durch vollständige Induktion** (englisch: proof by induction), der dann verwendet werden kann, wenn wir die Wahrheit einer Aussageform $A(n)$ für alle ganzen Zahlen $n \in \mathbb{Z}$ ab einem gewissen Startindex $n_0 \in \mathbb{Z}$ zeigen wollen, also für $n \geqslant n_0$. In diesem Fall zeigen wir am **Induktionsanfang** (englisch: base case) die Wahrheit der Aussage $A(n_0)$. Oft wird der Induktionsanfang bei $n_0 = 0$ oder $n_0 = 1$ gesetzt.

Im **Induktionsschritt** (englisch: induction step) wird $A(n) \Rightarrow A(n + 1)$ gezeigt. Dabei heißt $A(n)$ die **Induktionsannahme** (englisch: induction hypothesis). Bei Bedarf kann sogar auf alle vorgehenden Aussagen $A(n_0), \dots, A(n)$ zurückgegriffen werden, also $A(n_0) \wedge \cdots \wedge A(n) \Rightarrow A(n + n_0)$ gezeigt werden.

Ein schönes Beispiel für einen fehlerhaft ausgeführten Induktionsbeweis ist das Pferde-Paradoxon, bei dem „bewiesen" wird, dass alle Pferde dieselbe Farbe haben.

Beispiel 3.2 (vollständige Induktion).
Behauptung: Die Summe der ersten n natürlichen Zahlen ist gleich $\frac{1}{2}n\,(n+1)$.

$$A(n) : \sum_{j=1}^{n} j = \frac{1}{2}n\,(n+1).$$

Induktionsanfang bei $n_0 = 1$: $A(1)$ lautet: $\sum_{j=1}^{1} j = \frac{1}{2} \cdot 1 \cdot 2$, was eine wahre Aussage ist. Wir zeigen nun im Induktionsschritt, dass $A(n)$ auch $A(n+1)$ impliziert:

$$\begin{aligned}
\sum_{j=1}^{n+1} j &= n+1+\sum_{j=1}^{n} j && \text{wegen der Assoziativität der Addition}\\
&= n+1+\frac{1}{2}n\,(n+1) && \text{nach Induktionsannahme, dass } A(n) \text{ wahr ist}\\
&= (n+1)\left[1+\frac{1}{2}n\right] && \text{wegen des Distributivgesetzes für Addition und Multiplikation}\\
&= (n+1)\left[\frac{n+2}{2}\right]\\
&= \frac{1}{2}(n+1)\,(n+2),
\end{aligned}$$

was $A(n+1)$ entspricht.

Ende der Vorlesung 2

Ende der Woche 1

§ 4 MENGENLEHRE

Literatur: Deiser, 2022b, Kapitel 1.2

Georg Cantor, Begründer der Mengenlehre, hat 1895 folgenden Versuch der Definition einer Menge angegeben:

> „Unter einer **Menge** verstehen wir jede Zusammenfassung X von bestimmten wohlunterschiedenen Objekten x unserer Anschauung oder unseres Denkens (welche die **Elemente** von X genannt werden) zu einem Ganzen."

Diese ursprüngliche Definition hat allerdings Schwächen, wie wir gleich noch sehen werden.

Wir bezeichnen Mengen oft mit Großbuchstaben. Ist X eine Menge (englisch: set) und x ein Element (englisch: element) von X, so notieren wir diese Beziehung als $x \in X$ (seltener auch $X \ni x$) und lesen „x ist Element von X" oder kurz „x in X" oder auch „X enthält x". Das Symbol $x \notin X$ (oder $X \not\ni x$) drückt aus, dass x *kein* Element von X ist.

Mengen sind vollständig durch ihre Elemente bestimmt. Zwei Mengen X und Y sind also genau dann **gleich** (englisch: equality of sets), wenn sie dieselben Elemente enthalten. In Symbolen:

$$X = Y \quad \text{ist definiert als die Wahrheit der Aussage} \quad \forall x \in X\ (x \in Y)\ \wedge\ \forall y \in Y\ (y \in X).$$

Mengen können beispielsweise durch Aufzählung ihrer Elemente in geschweiften Klammern {} angegeben werden, etwa

$$X \coloneqq \{2, 3, 5\}.$$

Da Mengen nur aus „wohlunterschiedenen“ Elementen bestehen und es auf die Reihenfolge nicht ankommt, könnten wir dieselbe Menge auch als

$$X \coloneqq \{5, 2, 3, 2\}$$

beschreiben. Wichtige Mengen sind die **Zahlbereiche** (englisch: number systems)

$\mathbb{N} \coloneqq \{1, 2, 3, \ldots\}$	Menge der **natürlichen Zahlen**[26],
$\mathbb{N}_0 \coloneqq \{0, 1, 2, 3, \ldots\}$	Menge der **natürlichen Zahlen mit Null**,
$\mathbb{Z} \coloneqq \{0, 1, -1, 2, -2, \ldots\}$	Menge der **ganzen Zahlen**[27],
$\widetilde{\mathbb{Q}} \coloneqq \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\}$	(vorläufige) Menge der **rationalen Zahlen**[28],
$\mathbb{R}$	Menge der **reellen Zahlen**[29],
$\mathbb{C} \coloneqq \{a + b\,i \mid a, b \in \mathbb{R}\}$	Menge der **komplexen Zahlen**[30],

die hier nur informell definiert werden. Für die wirkliche Definition der rationalen Zahlen $\mathbb{Q}$ verweisen wir auf das Ende von § 5. Elementare Eigenschaften der komplexen Zahlen $\mathbb{C}$ werden in Anhang A besprochen.

Eine weitere Möglichkeit, Mengen anzugeben, besteht darin, Elemente anhand bestimmter Eigenschaften zu sammeln. Es sei dazu A eine Aussageform mit Grundbereich X, der eine Menge sein soll. Dann können wir

$$Y \coloneqq \left\{x \in X \,\middle|\, A(x)\right\} \tag{4.1}$$

betrachten, bestehend aus den Elementen von X, für die $A(x)$ eine wahre Aussage ist. Diese Konstruktion heißt **Mengenkomprehension** (englisch: set comprehension).

Hier erkennt man ein Problem der sehr freien Definition einer Menge nach Cantor. Sie lässt es zu, X als die Menge aller Mengen zu definieren. Wählen wir dann $A(x)$ als die Aussageform „enthält sich nicht selbst“, so definiert

$$R \coloneqq \{x \in X \mid x \notin x\}$$

also die „Menge aller Mengen, die sich nicht selbst enthalten“. Stellen wir jetzt die Frage, ob R sich selbst enthält, so erkennen wir das Problem:

- Falls R sich selbst enthält ($R \in R$), dann liegt das daran, dass R die Komprehensionsbedingung $R \notin R$ erfüllt.

- Falls R sich nicht selbst enthält ($R \notin R$), dann erfüllt R die Komprehensionsbedingung $R \notin R$ nicht, also gilt $R \in R$.

---

[26] englisch: natural numbers

[27] englisch: integer numbers, lateinisch: integer: ganz, unversehrt

[28] englisch: rational numbers, lateinisch: ratio: Verhältnis

[29] englisch: real numbers

[30] englisch: complex numbers

In Kurzform erhalten wir den Widerspruch $R \in R \Leftrightarrow R \notin R$. Dieser Widerspruch ist als **Russell-Paradoxon** (englisch: Russell's paradox) oder **Russell-Antinomie** der „naiven" Cantorschen Mengenlehre bekannt geworden, entdeckt 1901 von Russell und unabhängig etwa zeitgleich von Zermelo.[31]

Die Auflösung in der modernen, axiomatischen Mengenlehre nach Zermelo und Fraenkel (**ZF-Mengenlehre**) (englisch: ZF set theory) besteht darin, den Mengenbegriff geeignet einzuschränken, sodass Konstruktionen wie die „Menge aller Mengen" nicht mehr möglich sind. In dieser Lehrveranstaltung können wir die zugehörigen Axiome[32] nicht behandeln und verweisen auf spätere Spezialveranstaltungen. Wir weisen aber darauf hin, dass die Mengenkomprehension (4.1) in Form des sogenannten Aussonderungsaxioms als Konstruktionsprinzip von Mengen weiterhin vorkommt. Wesentlich ist nur eben, dass der Grundbereich X der Aussageform A eine Menge im Sinne der ZF-Axiome sein muss.[33]

Intervalle lassen sich beispielsweise über Mengenkomprehension definieren:

Beispiel 4.1 (Mengenkomprehension)**.**
Es seien $a, b \in \mathbb{R}$. Dann heißt

$[a, b] := \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$ **abgeschlossenes Intervall**[34],
$(a, b] := \{x \in \mathbb{R} \mid a < x \leqslant b\}$ **links offenes, rechts abgeschlossenes Intervall**[35],
$[a, b) := \{x \in \mathbb{R} \mid a \leqslant x < b\}$ **links abgeschlossenes, rechts offenes Intervall**[36],
$(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$ **offenes Intervall**[37],
$[a, \infty) := \{x \in \mathbb{R} \mid a \leqslant x\}$ **rechtsseitig unendliches abgeschlossenes Intervall**[38],
$(a, \infty) := \{x \in \mathbb{R} \mid a < x\}$ **rechtsseitig unendliches offenes Intervall**[39],
$(-\infty, b] := \{x \in \mathbb{R} \mid x \leqslant b\}$ **linksseitig unendliches abgeschlossenes Intervall**[40],
$(-\infty, b) := \{x \in \mathbb{R} \mid x < b\}$ **linksseitig unendliches offenes Intervall**[41],
$(-\infty, \infty) := \{x \in \mathbb{R} \mid \top\} = \mathbb{R}$ **beidseitig unendliches Intervall**[42].

Dabei ist $\{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$ eine gebräuchliche Kurzschreibweise für $\{x \in \mathbb{R} \mid a \leqslant x \wedge x \leqslant b\}$. Die Intervalle der Form $[a, b]$, $(a, b]$, $[a, b)$ und (a, b) heißen **endliche Intervalle** (englisch: finite intervals) oder **beschränkte Intervalle** (englisch: bounded intervals) mit **Endpunkten** (englisch: end points) $a, b \in \mathbb{R}$. Diese sind leer, wenn $b < a$ bzw. $b \leqslant a$ gilt. Die Bedeutung der Eigenschaften **offen** (englisch: open) und **abgeschlossen** (englisch: closed) wird in der Lehrveranstaltung *Analysis* behandelt.

Wir definieren für $a, b \in \mathbb{Z}$ auch

$[\![a, b]\!] := [a, b] \cap \mathbb{Z}$ **ganzzahliges Intervall** (englisch: integer interval).

---

[31] Eine bekannte andere Formulierung des Russell-Paradoxons ist die folgende. In einem Dorf lebt ein (männlicher) Barbier, der alle Männer rasiert, die sich nicht selbst rasieren. Rasiert der Dorfbarbier sich selbst?

[32] Bei Interesse können Sie sich aber unter https://de.wikipedia.org/wiki/Zermelo-Fraenkel-Mengenlehre#Die_Axiome_von_ZF_und_ZFC einen Eindruck verschaffen.

[33] Ist der Grundbereich keine Menge, so landet man beim Begriff der **Klasse** (englisch: class), siehe etwa Deiser, 2022a, Kapitel 3. Ein wichtiges Beispiel ist die **Klasse aller Mengen** (englisch: class of all sets).

[34] englisch: closed interval

[35] englisch: left-open, right-closed interval

[36] englisch: left-closed, right-open interval

[37] englisch: open interval. Bei der Notation (a, b) für offene Intervalle besteht eine Verwechslungsgefahr mit den Elementen (a, b) des kartesischen Produkts von zwei Mengen, siehe Definition 4.8.

[38] englisch: unbounded above, closed interval

[39] englisch: unbounded above, open interval

[40] englisch: unbounded below, closed interval

[41] englisch: unbounded below, open interval

[42] englisch: unbounded above and below interval

Definition 4.2 (Teilmenge, Obermenge).
Für Mengen A und B definieren wir:

(i) A ist eine **Teilmenge** (englisch: subset) von B, kurz: $A \subseteq B$, wenn jedes Element von A auch ein Element von B ist, kurz: $\forall a \in A \; (a \in B)$. In diesem Fall sagen wir auch, B sei eine **Obermenge** (englisch: superset) von A, und schreiben $B \supseteq A$.

(ii) A ist eine **echte Teilmenge** (englisch: proper subset) von B, kurz: $A \subsetneq B$, falls $A \subseteq B$ und $A \neq B$ gilt. In diesem Fall sagen wir auch, B sei eine **echte Obermenge** (englisch: proper superset) von A, und schreiben $B \supsetneq A$.

Die Teilmengenbeziehung $\subseteq$ zwischen Mengen heißt auch **Inklusion** (englisch: inclusion).[43]

Beispielsweise erzeugt die Mengenkomprehension (4.1) immer eine Teilmenge $Y \subseteq X$. Außerdem gelten die echten Inklusionen

$$\mathbb{N} \subsetneq \mathbb{N}_0 \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}.$$

Quizfrage 4.1: Wie kann man sich davon überzeugen, dass die Inklusionen echt sind?

In der axiomatischen Mengenlehre gibt es genau eine Menge, die keine Elemente enthält, die **leere Menge** (englisch: empty set) $\emptyset$.

Definition 4.3 (Schnitt, disjunkte Mengen, Vereinigung, Differenz, symmetrische Differenz).

(i) Es sei $\mathcal{U}$ eine nichtleere Menge von Mengen. Dann heißt die Menge

$$\bigcap \mathcal{U} := \left\{ x \,\middle|\, \forall U \in \mathcal{U} \; (x \in U) \right\} \tag{4.2}$$

die **Schnittmenge**, der **Durchschnitt** oder **Schnitt** (englisch: intersection) von $\mathcal{U}$. Sind die Elemente von $\mathcal{U}$ über eine nichtleere Indexmenge I indiziert, gilt also $\mathcal{U} = \{U_i \,|\, i \in I\}$, so schreiben wir auch

$$\bigcap_{i \in I} U_i := \left\{ x \,\middle|\, \forall i \in I \; (x \in U_i) \right\}. \tag{4.3}$$

Besteht speziell $\mathcal{U} = \{U_1, U_2\}$ aus nur zwei Elementen, so schreiben wir auch

$$U_1 \cap U_2 := \left\{ x \,\middle|\, x \in U_1 \;\land\; x \in U_2 \right\}. \tag{4.4}$$

Gilt $\bigcap \mathcal{U} = \emptyset$ bzw. $\bigcap_{i \in I} U_i = \emptyset$ bzw. $U_1 \cap U_2 = \emptyset$, so heißen die Elemente von $\mathcal{U}$ bzw. die Mengen U_i bzw. die Mengen U_1 und U_2 **disjunkt** (englisch: disjoint).

(ii) Es sei $\mathcal{U}$ eine (möglicherweise leere) Menge von Mengen. Dann heißt die Menge

$$\bigcup \mathcal{U} := \left\{ x \,\middle|\, \exists U \in \mathcal{U} \; (x \in U) \right\} \tag{4.5}$$

die **Vereinigungmenge** oder die **Vereinigung** (englisch: union) von $\mathcal{U}$. Sind die Elemente von $\mathcal{U}$ über eine Indexmenge I indiziert, gilt also $\mathcal{U} = \{U_i \,|\, i \in I\}$, so schreiben wir auch

$$\bigcup_{i \in I} U_i := \left\{ x \,\middle|\, \exists i \in I \; (x \in U_i) \right\}. \tag{4.6}$$

Besteht speziell $\mathcal{U} = \{U_1, U_2\}$ aus nur zwei Elementen, so schreiben wir auch

$$U_1 \cup U_2 := \left\{ x \,\middle|\, x \in U_1 \;\lor\; x \in U_2 \right\}. \tag{4.7}$$

---

[43] lateinisch: includere: einschließen

Definition 4.4 (Differenz, symmetrische Differenz, Komplement)**.**
Für Mengen X und Y definieren wir

(i) die **Differenzmenge** (englisch: set difference) von Y in X

$$X \setminus Y := \{x \in X \mid x \notin Y\}, \tag{4.8}$$

kurz auch als „**X ohne Y**“ bezeichnet.

(ii) die **symmetrische Differenz** (englisch: symmetric difference) von X und Y

$$X \triangle Y := (X \setminus Y) \cup (Y \setminus X). \tag{4.9}$$

Ist weiter X irgendeine Menge und $A \subseteq X$ eine Teilmenge, so definieren wir

(iii) das **Komplement** (englisch: complement) von A in X

$$A^c := X \setminus A = \{x \in X \mid x \notin A\}. \tag{4.10}$$

Da die Menge X im Symbol A^c nicht angegeben wird, muss sie dabei aus dem Zusammenhang klar sein.

Quizfrage 4.2: Was sind $X \triangle X$ und $X \triangle \emptyset$?

Lemma 4.5 (Eigenschaften von Schnitt und Vereinigung)**.**
Es seien X, Y und Z Mengen. Dann gilt:

$$X \cap Y = Y \cap X \qquad \textbf{Kommutativität von } \cap \tag{4.11a}$$

$$X \cup Y = Y \cup X \qquad \textbf{Kommutativität von } \cup \tag{4.11b}$$

$$(X \cap Y) \cap Z = X \cap (Y \cap Z) \qquad \textbf{Assoziativität von } \cap \tag{4.12a}$$

$$(X \cup Y) \cup Z = X \cup (Y \cup Z) \qquad \textbf{Assoziativität von } \cup \tag{4.12b}$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \qquad \textbf{Distributivität} \tag{4.13a}$$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \qquad \textbf{Distributivität} \tag{4.13b}$$

$$X \setminus Y = X \setminus (X \cap Y) \tag{4.14}$$

$$X \cap Y = X \quad \Leftrightarrow \quad X \subseteq Y \tag{4.15a}$$

$$X \cup Y = Y \quad \Leftrightarrow \quad X \subseteq Y \tag{4.15b}$$

Sind A und B Teilmengen einer Menge X, bzgl. der wir das Komplement nehmen, so gilt weiter:

$$(A \cap B)^c = A^c \cup B^c \qquad \textbf{De Morgansches Gesetz} \tag{4.16a}$$

$$(A \cup B)^c = A^c \cap B^c \qquad \textbf{De Morgansches Gesetz} \tag{4.16b}$$

$$(A^c)^c = A \qquad \text{Komplementbildung ist } \textbf{involutorisch}^{44} \tag{4.17}$$

$$A \subseteq B \quad \Leftrightarrow \quad B^c \subseteq A^c \tag{4.18}$$

---

[44] auch: selbst-invers, englisch: involutory, self-inverse

Beweis. Der Beweis kann durch Ausnutzung von $X = Y \Leftrightarrow \forall x\ (x \in X \leftrightarrow x \in Y)$ und $X \subseteq Y \Leftrightarrow \forall x\ (x \in X \to x \in Y)$ auf Satz 1.9 zurückgeführt werden. Die Details werden hier nicht ausgeführt. □

Zur Vereinfachung der Notation vereinbaren wir auch hier wieder Bindungsregeln:

$$\cdot^c \text{ bindet stärker als } \setminus \text{ bindet stärker als } \cap \text{ bindet stärker als } \cup, \tag{4.19}$$

wodurch wir beispielsweise das erste Distributivgesetz auch als $X \cap (Y \cup Z) = X \cap Y \cup X \cap Z$ schreiben könnten.

Definition 4.6 (Potenzmenge)**.**
Für jede Menge A heißt

$$\mathcal{P}(A) := \{B \mid B \subseteq A\} \tag{4.20}$$

die **Potenzmenge** (englisch: power set) von A.

In der axiomatischen Mengenlehre nach Zermelo und Fraenkel gibt es das Potenzmengenaxiom, das garantiert, dass jede Menge eine Potenzmenge besitzt.

Beispiel 4.7 (Potenzmenge)**.**

(i) Für $A = \emptyset$ ist $\mathcal{P}(A) = \{\emptyset\}$.

(ii) Für $A = \{a\}$ ist $\mathcal{P}(A) = \big\{\emptyset,\ \{a\}\big\}$.

(iii) Für $A = \{a,\ b\}$ ist $\mathcal{P}(A) = \big\{\emptyset,\ \{a\},\ \{b\},\ \{a,\ b\}\big\}$.

Definition 4.8 (kartesisches Produkt endlich vieler Mengen)**.**

(i) Für Mengen A und B definieren wir das **kartesische Produkt** (englisch: Cartesian product) oder **Kreuzprodukt** (englisch: cross product)

$$A \times B := \{(a, b) \mid a \in A \ \wedge\ b \in B\}. \tag{4.21}$$

Die Elemente des kartesischen Produkts heißen **geordnete Paare** (englisch: ordered pairs) oder einfach **Paare** (englisch: pairs) (a, b).

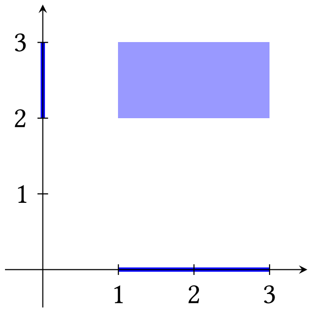
(ii) Analog können wir auch das kartesische Produkt von mehr als zwei Mengen definieren, etwa $A \times B \times C$, dessen Elemente **Tripel** (englisch: triplets) (a, b, c) sind. Allgemeiner heißen die Elemente $(a_1, a_2, \ldots, a_n)$ des Produkts $\bigtimes_{i=1}^n A_i$ von $n \geqslant 2$ Mengen **n-Tupel** (englisch: n-tuples). Dabei gilt $a_i \in A_i$ für $i = 1, \ldots, n$.

(iii) Wir schreiben $A^2 = A \times A$ und allgemeiner $A^n = \bigtimes_{i=1}^n A$ für das kartesische Produkt einer Menge A mit sich selbst.

Beispiel 4.9 (kartesisches Produkt)**.**

(i) Ist $A = \{\text{Kreuz}, \text{Pik}, \text{Herz}, \text{Karo}\}$ und $B = \{7, 8, 9, 10, \text{Bube}, \text{Dame}, \text{König}, \text{As}\}$, so entsprechen die Elemente des kartesischen Produkts $A \times B$ gerade den 32 Karten eines Skatspiels, also (Kreuz, 7), (Kreuz, 8) usw. bis (Karo, As).

(ii) Für Intervalle $A = [1, 3]$ und $B = [2, 3]$ können wir das **mehrdimensionale Intervall** (englisch: multi-dimensional interval) $A \times B = \{(x_1, x_2) \mid 1 \leqslant x_1 \leqslant 3 \ \wedge\ 2 \leqslant x_2 \leqslant 3\} \subseteq \mathbb{R} \times \mathbb{R}$ wie folgt illustrieren:



Ende der Vorlesung 3

§ 5 RELATIONEN

Literatur: Deiser, 2022b, Kapitel 1.3

Relationen[45] geben Beziehungen zwischen Objekten an wie beispielsweise $1 \leqslant 3$ oder $5 \in \mathbb{N}$ oder $3 \mid 756$ („3 teilt 756“).

Definition 5.1 (Relation)**.**

Es seien X und Y Mengen. Ist $R \subseteq X \times Y$, so heißt (R, X, Y) eine **Relation** (englisch: relation) **zwischen** X und Y. Die Menge R heißt der **Graph der Relation** (englisch: graph of a relation). Im Fall $Y = X$ sprechen wir von einer **homogenen Relation** (englisch: homogeneous relation) **auf** X.

Wenn X und Y klar sind, sagt man auch oft, R selbst sei die Relation. Statt $(x, y) \in R$ schreiben wir auch $x \, R \, y$, um die Lesart „x steht in Relation zu y“ zu erleichtern.

Beispiel 5.2 (Relation)**.**

(i) Ist X die Menge der Teilnehmenden an der Lehrveranstaltung *Lineare Algebra I* und $Y = \{\text{Mathematik}, \text{Physik}, \text{Informatik}\}$ eine Menge von Studienfächern, so ergibt die Beziehung „Die teilnehmende Person x studiert das Fach y.“ eine Relation zwischen X und Y.

(ii) Wir sagen, die Zahl $x \in \mathbb{Z}$ **teilt** (englisch: divides) die Zahl $y \in \mathbb{Z}$, in Symbolen: $x \mid y$, wenn eine Zahl $n \in \mathbb{Z}$ existiert, sodass $y = n\,x$ gilt. Insbesondere teilt jede ganze Zahl die Zahl 0, und die Zahl 1 teilt jede ganze Zahl.

Die folgende Tabelle stellt die **Teilbarkeitsrelation** (englisch: divisibility relation) „Die Zahl x teilt die Zahl y.“ auf der Menge $X = Y = \{0, 1, 2, \dots, 10\} = [\![0, 10]\!]$ dar:

---

[45] lateinisch: relatio: Verhältnis, Beziehung

$x \mid y$	0	1	2	3	4	5	6	7	8	9	10
0	•										
1	•	•	•	•	•	•	•	•	•	•	•
2	•		•		•		•		•		•
3	•			•			•			•	
4	•				•				•		
5	•					•					•
6	•						•				
7	•							•			
8	•								•		
9	•									•	
10	•										•

(iii) Es sei $X = Y = \mathbb{R}$ und $R = \big\{(x, y) \in \mathbb{R}^2 \,\big|\, x \leqslant y\big\}$ die **gewöhnliche Kleiner-Gleich-Relation auf $\mathbb{R}$** (englisch: usual less-or-equal relation).

(iv) Es sei X eine Menge, $\mathcal{P}(X)$ die Potenzmenge und $R = \big\{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \,\big|\, A \subseteq B\big\}$ die **Inklusionsrelation** (englisch: inclusion relation).

(v) Auf einer beliebigen Menge X heißt die Menge

$$\Delta_X \coloneqq \big\{(x, y) \in X \times X \,\big|\, x = y\big\} \tag{5.1}$$

die **Diagonale** (englisch: diagonal) in $X \times X$. Die Relation $\mathrm{id}_X \coloneqq (\Delta_X, X, X)$ heißt die **Gleichheitsrelation** (englisch: equality relation) oder **Identitätsrelation** (englisch: identity) auf der Menge X.

(vi) Auf einer beliebigen Menge X heißt die Relation $U_X \coloneqq (U, X, X)$ mit $U = X \times X$ die **universelle Relation** (englisch: universal relation).

Quizfrage 5.1: Können Sie weitere Beispiele für Relationen benennen?

Definition 5.3 (Komposition von Relationen)**.**
Es seien X, Y und Z Mengen sowie (R, X, Y) und (S, Y, Z) zwei Relationen. Dann heißt die Relation $(S \circ R, X, Z)$ mit

$$S \circ R \coloneqq \big\{(x, z) \in X \times Z \,\big|\, \exists y \in Y \text{ mit } (x, y) \in R \text{ und } (y, z) \in S\big\} \tag{5.2}$$

die **Komposition** (englisch: composition, lateinisch: componere: zusammenstellen), die **Hintereinanderausführung**, die **Verknüpfung** oder die **Verkettung** von R und S. Um die Reihenfolge klar zu benennen, sagt man auch „S **nach** R“.

Quizfrage 5.2: Durch die Komposition welcher Relationen kann man die Relation „Onkel sein von“ ausdrücken?

Definition 5.4 (Umkehrrelation)**.**
Es seien X und Y Mengen und (R, X, Y) eine Relation. Dann heißt (R^{-1}, Y, X) die **Umkehrrelation** (englisch: reverse relation) oder **inverse Relation** (englisch: inverse relation) von R, wobei

$$R^{-1} \coloneqq \big\{(b, a) \in Y \times X \,\big|\, (a, b) \in R\big\} \subseteq Y \times X$$

definiert ist.

Quizfrage 5.3: Wie bezeichnet man die Umkehrrelationen von „kleiner oder gleich sein als“, „Teilmenge sein von“ bzw. „Teiler sein von“?

Quizfrage 5.4: Wie könnte man die Umkehrrelationen der Teilbarkeitsrelation auf $\mathbb{Z}$ bezeichnen?

Wir definieren nun einige wichtige Eigenschaften, die Relationen auf einer Menge besitzen können.

Definition 5.5 (Eigenschaften homogener Relationen)**.**

Es sei X eine Menge und (R, X, X) eine Relation auf X.

(i) R heißt **reflexiv** (englisch: reflexive), wenn gilt:

$$(x, x) \in R \quad \text{für alle } x \in X.$$

(ii) R heißt **symmetrisch** (englisch: symmetric), wenn gilt:

$$(x, y) \in R \quad \Rightarrow \quad (y, x) \in R.$$

(iii) R heißt **antisymmetrisch** (englisch: antisymmetric), wenn gilt:

$$(x, y) \in R \text{ und } (y, x) \in R \quad \Rightarrow \quad x = y.$$

(iv) R heißt **transitiv** (englisch: transitive), wenn gilt:

$$(x, y) \in R \text{ und } (y, z) \in R \quad \Rightarrow \quad (x, z) \in R.$$

(v) R heißt **total** (englisch: total), wenn gilt:

$$(x, y) \in R \text{ oder } (y, x) \in R \quad \text{für alle } x, y \in X.$$

Quizfrage 5.5: Die Reflexivität von R kann man auch als $\operatorname{id}_X \subseteq R$ ausdrücken. Wie sieht das für die anderen Eigenschaften aus?

Beispiel 5.6 (Eigenschaften homogener Relationen)**.**

- Die Teilbarkeitsrelation $|$ auf $\mathbb{Z}$ ist reflexiv und transitiv, aber nicht symmetrisch, antisymmetrisch oder total.
- Die Teilbarkeitsrelation $|$ auf $\mathbb{N}_0$ ist reflexiv, antisymmetrisch und transitiv, aber nicht symmetrisch oder total.
- Die Relation „x liebt y“ auf einer Menge von Personen hat in der Regel keine der fünf genannten Eigenschaften.

§ 5.1 ORDNUNGSRELATIONEN

Definition 5.7 (Ordnungsrelation)**.**
Es sei X eine Menge.

(i) Eine Relation (R, X, X) auf X heißt eine **Ordnungsrelation**, **Halbordnung** oder **partielle Ordnung** (englisch: partial ordering), wenn sie reflexiv, antisymmetrisch und transitiv ist. Das Paar (X, R) heißt dann eine **halbgeordnete Menge** (englisch: partially ordered set).

(ii) Ist die Relation R zusätzlich total, dann heißt sie eine **Totalordnung** (englisch: total ordering). Das Paar (X, R) heißt dann eine **totalgeordnete Menge** (englisch: totally ordered set).

Ordnungsrelationen werden oft mit Symbolen wie $\leqslant$, $\preccurlyeq$ oder $\subseteq$ notiert. Unter Verwendung der Notation $\preccurlyeq$ können wir für eine Ordnungsrelation auf X also festhalten, dass für alle $x, y, z \in X$ gilt:

$$x \preccurlyeq x, \tag{5.3a}$$

$$x \preccurlyeq y \text{ und } y \preccurlyeq x \quad \Rightarrow \quad x = y, \tag{5.3b}$$

$$x \preccurlyeq y \text{ und } y \preccurlyeq z \quad \Rightarrow \quad x \preccurlyeq z. \tag{5.3c}$$

Die Idee von Ordnungsrelationen ist es, Elemente einer Menge bezüglich einer bestimmten Eigenschaft zu vergleichen. Bei einer Totalordnung ist dabei jedes Element mit jedem Element vergleichbar, bei einer Halbordnung nicht unbedingt.

Beispiel 5.8 (Halbordnungen und Totalordnungen)**.**

(i) Die Identitätsrelation id_X ist eine Halbordnung auf jeder Menge X.

(ii) Die universelle Relation U_X ist *keine* Halbordnung auf jeder Menge X, die mindestens zwei Elemente enthält.

(iii) Die Kleiner-Gleich-Relation $\leqslant$ ist eine Totalordnung auf jeder Teilmenge von $\mathbb{R}$.

(iv) Die Inklusionsrelation $\subseteq$ ist eine Halbordnung auf der Potenzmenge $\mathcal{P}(X)$ jeder beliebigen Menge X. Sie ist eine totale Ordnung dann und nur dann, wenn X entweder kein oder genau ein Element enthält.

(v) Die Teilbarkeitsrelation $\mid$ ist eine Halbordnung auf $\mathbb{N}$.

Lemma 5.9 (Halbordnungen $\preccurlyeq$ und $\succcurlyeq$)**.**
Es sei $\preccurlyeq$ eine Halbordnung auf einer Menge X. Dann ist auch die inverse Relation $\succcurlyeq$ eine Halbordnung auf X. Ist $\preccurlyeq$ eine Totalordnung, dann auch $\succcurlyeq$.

Beweis. Dieser Beweis ist Teil von Hausaufgabe 2.3. □

Definition 5.10 (Vergleichbarkeit, obere und untere Schranken, Supremum und Infimum, maximale und minimale Elemente, Maximum und Minimum)**.**
Es sei X mit der Relation $\preccurlyeq$ eine halbgeordnete Menge.

(i) Zwei Elemente $x, y \in X$ heißen **vergleichbar** (englisch: comparable), wenn $x \preccurlyeq y$ oder $y \preccurlyeq x$ gilt.

(*ii*) $b \in X$ heißt eine **obere Schranke** (englisch: upper bound) von $A \subseteq X$, wenn gilt:

$$x \preccurlyeq b \quad \text{für alle } x \in A. \qquad \text{(„Ganz } A \text{ ist } \preccurlyeq.\text{“)}$$

(*iii*) $b \in X$ heißt ein **Supremum** (englisch: supremum, lateinisch: supremum: das Größte) oder **kleinste obere Schranke** (englisch: least upper bound) von $A \subseteq X$, wenn gilt:

$$b \text{ ist eine obere Schranke von } A \text{, und für jede obere Schranke } \widehat{b} \text{ von } A \text{ gilt: } b \preccurlyeq \widehat{b}.$$

(*iv*) $b \in X$ heißt ein **maximales Element** (englisch: maximal element) von $A \subseteq X$, wenn gilt:

$$b \in A, \text{und für alle } x \in A \text{ gilt: } b \preccurlyeq x \;\Rightarrow\; x = b. \qquad \text{(„Kein Element von } A \text{ ist größer.“)}$$

(*v*) $b \in X$ heißt ein **Maximum** (englisch: maximum) von $A \subseteq X$, wenn gilt:

$$b \in A, \text{und für alle } x \in A \text{ gilt: } x \preccurlyeq b. \qquad \text{(„Ganz } A \text{ ist höchstens so groß.“)}$$

(*vi*) $a \in X$ heißt eine **untere Schranke** (englisch: lower bound) von $A \subseteq X$, wenn gilt:

$$a \preccurlyeq x \quad \text{für alle } x \in A. \qquad \text{(„Ganz } A \text{ ist } \succcurlyeq.\text{“)}$$

(*vii*) $a \in X$ heißt ein **Infimum** (englisch: infimum, lateinisch: infimum: das Kleinste) oder **größte untere Schranke** (englisch: greatest lower bound) von $A \subseteq X$, wenn gilt:

$$a \text{ ist eine untere Schranke von } A \text{, und für jede untere Schranke } \widehat{a} \text{ von } A \text{ gilt: } \widehat{a} \preccurlyeq a.$$

(*viii*) $a \in X$ heißt ein **minimales Element** (englisch: minimal element) von $A \subseteq X$, wenn gilt:

$$a \in A, \;\text{ und für alle } x \in A \text{ gilt: } x \preccurlyeq a \;\Rightarrow\; x = a. \qquad \text{(„Kein Element von } A \text{ ist kleiner.“)}$$

(*ix*) $a \in X$ heißt ein **Minimum** (englisch: minimum) von $A \subseteq X$, wenn gilt:

$$a \in A, \text{und für alle } x \in A \text{ gilt: } a \preccurlyeq x. \qquad \text{(„Ganz } A \text{ ist mindestens so groß.“)}$$

Wenn $A \subseteq X$ eine obere Schranke besitzt, so heißt A **nach oben beschränkt** (englisch: bounded above), ansonsten **nach oben unbeschränkt** (englisch: unbounded above). Wenn $A \subseteq X$ eine untere Schranke besitzt, so heißt A **nach unten beschränkt** (englisch: bounded below), ansonsten **nach unten unbeschränkt** (englisch: unbounded below).

Wir zeigen nun einige ausgewählte Eigenschaften.

Lemma 5.11 (Eigenschaften und Beziehungen zwischen Supremum und Maximum, Infimum und Minimum)**.**
Es sei X mit der Relation $\preccurlyeq$ eine halbgeordnete Menge und $A \subseteq X$.

(*i*) Existiert ein Supremum von A, so ist dieses eindeutig.

(*ii*) Existiert ein Maximum von A, so ist dieses eindeutig.

(*iii*) Ist b das Maximum von A, so ist b gleichzeitig das Supremum von A.

(*iv*) Hat A ein Supremum b, so gilt: Gehört b zu A, so ist b das Maximum von A. Gehört b nicht zu A, so besitzt A kein Maximum.

Analoge Aussagen gelten auch für das Infinum und Minimum von A.

Beweis. Aussage (*i*): Wir nehmen an, $b \in X$ und $\widehat{b} \in X$ seien beides Suprema von A. Dann sind b und $\widehat{b}$ beides obere Schranken. Da b ein Supremum von A ist, gilt $b \preccurlyeq \widehat{b}$. Da $\widehat{b}$ ein Supremum von A ist, gilt $\widehat{b} \preccurlyeq b$. Aufgrund der Antisymmetrie von $\preccurlyeq$ folgt nun $b = \widehat{b}$

Aussage (*ii*): Wir nehmen an, $b \in X$ und $\overline{b} \in X$ seien beides Maxima von A. Dann gehören b und $\overline{b}$ beide zu A. Da b ein Maximum von A ist, gilt $\overline{b} \preccurlyeq b$. Da $\overline{b}$ ein Maximum von A ist, gilt $b \preccurlyeq \overline{b}$. Aufgrund der Antisymmetrie von $\preccurlyeq$ folgt nun $b = \overline{b}$

Aussage (*iii*): Es sei b das Maximum von A. Es gilt also $b \in A$ und $x \preccurlyeq b$ für alle $x \in A$. Das heißt aber, dass b eine obere Schranke von A ist. Ist nun $\overline{b}$ eine weitere obere Schranke von A, dann gilt $x \preccurlyeq \overline{b}$ für alle $x \in A$, insbesondere $b \preccurlyeq \overline{b}$. Das zeigt, dass b das Supremum von A ist.

Aussage (*iv*): Es sei b das Supremum von A. Insbesondere ist b eine obere Schranke von A, es gilt also $x \preccurlyeq b$ für alle $x \in A$. Falls nun b zu A gehört, dann ist b per Definition das Maximum von A. Falls jedoch b nicht zu A gehört, so ist b per Definition kein Maximum von A. Ein Maximum von A kann auch nicht existieren, sonst wäre es nach Aussage (*iii*) gleichzeitig das Supremum, also gleich b. □

Beispiel 5.12 (Schranken, extremale Elemente, Maxima und Minima, Suprema und Infima)**.**

(*i*) In den natürlichen Zahlen $\mathbb{N}$ mit der gewöhnlichen Totalordnung $\preccurlyeq$ ist die Zahl 1 das Minimum und damit das Infimum. Eine obere Schranke existiert nicht.

(*ii*) Es sei X eine beliebige nichtleere Menge. In der Potenzmenge $\mathcal{P}(X)$ mit der Halbordnung $\subseteq$ ist $\emptyset$ das Minimum von $\mathcal{P}(X)$ und X das Maximum von $\mathcal{P}(X)$.

Hat X mindestens zwei Elemente, dann besitzt die Teilmenge $A = \mathcal{P}(X) \setminus \{\emptyset\}$ das Infimum $\emptyset$, aber kein Minimum. Die minimalen Elemente von A sind genau die einelementigen Teilmengen von X.

Quizfrage 5.6: Können Sie sich eine Menge mit einer Halbordnung oder einer totalen Ordnung vorstellen, die kein maximales Element besitzt?

§ 5.2 ÄQUIVALENZRELATION

Definition 5.13 (Äquivalenzrelation)**.**
Es sei X eine Menge. Eine Relation (R, X, X) auf X heißt eine **Äquivalenzrelation** (englisch: equivalence relation), wenn sie reflexiv, symmetrisch und transitiv ist. Elemente $x, y \in X$, die $x \mathrel{R} y$ erfüllen, heißen **(zueinander) äquivalent** (englisch: equivalent).

Äquivalenzrelationen werden oft mit Symbolen wie $=$, $\sim$ oder $\equiv$ notiert. Unter Verwendung der Notation $\sim$ können wir für eine Äquivalenzrelation auf X also festhalten, dass für alle $x, y, z \in X$ gilt:

$$x \sim x, \tag{5.4a}$$

$$x \sim y \quad\Rightarrow\quad y \sim x, \tag{5.4b}$$

$$x \sim y \text{ und } y \sim z \quad\Rightarrow\quad x \sim z. \tag{5.4c}$$

Die Idee von Äquivalenzrelationen ist es, die Elemente einer Menge, die eine bestimmte Eigenschaft gemeinsam haben, zusammenzugruppieren und als gleichwertig zu betrachten.

Beispiel 5.14 (Äquivalenzrelationen).

(*i*) Die Identitätsrelation id_X ist eine Äquivalenzrelation auf jeder Menge X.

(*ii*) Die universelle Relation U_X ist eine Äquivalenzrelation auf jeder Menge X.

(*iii*) Es sei $m \in \mathbb{N}$ fest gewählt. Auf der Menge $X = \mathbb{Z}$ ist durch

$$x \overset{m}{\equiv} y \quad \Leftrightarrow \quad \exists n \in \mathbb{Z}\; (x - y = n\, m) \tag{5.5}$$

eine Äquivalenzrelation erklärt (**Quizfrage 5.7:** Details?). Anders ausgedrückt, x und y unterscheiden sich nur um ein Vielfaches von m, also, $m \mid (x - y)$. Diese Relation heißt **Kongruenzrelation modulo** m (englisch: congruence relation modulo m).[46]

Definition 5.15 (Äquivalenzklasse, Repräsentant, Repräsentantensystem).
Es sei X eine Menge mit der Äquivalenzrelation $\sim$.

(*i*) Für $x \in X$ heißt die Menge

$$[x] \coloneqq \{y \in X \mid y \sim x\} \tag{5.6}$$

die **Äquivalenzklasse** (englisch: equivalence class) von x bzgl. $\sim$. Statt $[x]$ schreibt man manchmal auch $[x]_\sim$ oder auch $x / \sim$.

(*ii*) Jedes Element einer Äquivalenzklasse heißt ein **Repräsentant** (englisch: representative, lateinisch: repraesentare: darstellen) dieser Äquivalenzklasse.

(*iii*) Eine Menge $S \subseteq X$, die aus jeder Äquivalenzklasse genau einen Repräsentanten enthält, heißt ein **Repräsentantensystem** (englisch: system of representatives) von $\sim$.

Beispiel 5.16 (Äquivalenzklasse, Repräsentant).

(*i*) Wir betrachten eine beliebige Menge X mit der Identitätsrelation. Dann gilt $[x] = \{x\}$ für alle $x \in X$. Jede Äquivalenzklasse hat also nur ein Element und damit einen eindeutigen Repräsentanten. Das einzige Repräsentantensystem ist X selbst.

(*ii*) Wir betrachten eine beliebige Menge X mit der universellen Relation. Dann gilt $[x] = X$ für alle $x \in X$. Falls $X \neq \emptyset$ ist, dann gibt es also nur eine Äquivalenzklasse, und diese enthält alle Elemente von X. In diesem Fall ist jede einelementige Teilmenge von X ein Repräsentantensystem.

(*iii*) Die Äquivalenzklassen der Kongruenzrelation modulo m ($m \in \mathbb{N}$) heißen auch die **Restklassen modulo** m (englisch: residue classes).[47] Die Restklasse von $a \in \mathbb{Z}$ modulo m ist also

$$\begin{aligned} [a] &= \{y \in \mathbb{Z} \mid y \overset{m}{\equiv} a\} \\ &= \{y \in \mathbb{Z} \mid \exists n \in \mathbb{Z}\; (y - a = n\, m)\} \\ &= \{a + n\, m \mid n \in \mathbb{Z}\} \\ &= a + m\,\mathbb{Z}. \end{aligned}$$

Das Repräsentantensystem $\{0, 1, \ldots, m - 1\}$ heißt das **natürliche Repräsentantensystem** (englisch: natural system of representatives) der Kongruenzrelation modulo m.

---

[46] Oft wird diese Relation statt $x \overset{m}{\equiv} y$ als $x \equiv y \pmod{m}$ geschrieben.

[47] Der Name leitet sich aus der Tatsache ab, dass die Elemente einer Restklasse durch die Eigenschaft charakterisiert sind, dass sie bei ganzzahliger Division durch m denselben Rest lassen.

(*iv*) Speziell im Fall $m = 2$ gibt es genau zwei Äquivalenzklassen (Restklassen):

$$\begin{aligned}[0] &= \{y \in \mathbb{Z} \,|\, y \overset{2}{\equiv} 0\} \\ &= \{y \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ (y - 0 = 2\,n)\} \\ &= \{y \in \mathbb{Z} \,|\, y \text{ ist gerade}\}, \\[1em] [1] &= \{y \in \mathbb{Z} \,|\, y \overset{2}{\equiv} 1\} \\ &= \{y \in \mathbb{Z} \,|\, \exists n \in \mathbb{Z}\ (y - 1 = 2\,n)\} \\ &= \{y \in \mathbb{Z} \,|\, y \text{ ist ungerade}\}.\end{aligned}$$

Das natürliche Repräsentantensystem ist $\{0, 1\}$, ein anderes ist $\{-2, 4339\}$.

Satz 5.17 (Äquivalenzklassen sind gleich oder disjunkt)**.**
Es sei X eine Menge mit der Äquivalenzrelation $\sim$. Weiter seien $[x]$ und $[y]$ zwei Äquivalenzklassen. Dann sind diese entweder gleich oder disjunkt.

Beweis. Nehmen wir an, $[x]$ und $[y]$ seien nicht disjunkt. Das heißt, sie haben ein Element $z \in X$ gemeinsam. Es sei nun $\overline{x}$ ein beliebiges Element aus $[x]$. Dann gilt

$$\overline{x} \sim x \sim z.$$

Wegen der Transitivität von $\sim$ ist also $\overline{x}$ äquivalent zu z, das nach Voraussetzung zu $[y]$ gehört. Damit haben wir $[x] \subseteq [y]$ gezeigt. Die umgekehrte Inklusion folgt analog. □

Definition 5.18 (Partition)**.**
Es sei X eine nichtleere Menge und $\mathcal{U}$ eine Menge von Teilmengen von X, also $\mathcal{U} \subseteq \mathcal{P}(X)$. $\mathcal{U}$ heißt eine **Partition** (englisch: partition) oder **disjunkte Zerlegung** von X, wenn gilt:

(*i*) Für alle $x \in X$ gibt es eine Menge $U \in \mathcal{U}$, die x enthält.

(*ii*) Für alle $U, V \in \mathcal{U}$ gilt, dass U und V entweder gleich sind oder disjunkt.

(*iii*) $\emptyset \notin \mathcal{U}$.

Zu Eigenschaft (*i*) sagen wir auch, dass die Mengen in $\mathcal{U}$ die Menge X **überdecken** (englisch: to cover) oder eine **Überdeckung** (englisch: cover, covering) von X darstellen. Zu Eigenschaft (*ii*) sagen wir, dass die Mengen in $\mathcal{U}$ **paarweise disjunkt** (englisch: pairwise disjoint) sind.

Satz 5.19 (Partitionen werden genau durch Äquivalenzrelationen erzeugt)**.**

(*i*) Es sei X eine nichtleere Menge mit der Äquivalenzrelation $\sim$. Dann bildet die Menge der Äquivalenzklassen $\big\{[x] \,\big|\, x \in X\big\}$ eine Partition von X.

(*ii*) Es sei X eine nichtleere Menge und $\mathcal{U}$ eine Partition von X. Dann gibt es eine eindeutig bestimmte Äquivalenzrelation $\sim$, sodass $\mathcal{U}$ genau aus den Äquivalenzklassen von $\sim$ besteht.

Wir könnten diesen Satz etwas ungenau auch so ausdrücken, dass die Partition einer Menge X „dasselbe“ ist wie eine Äquivalenzrelationen auf X.

Beweis. Aussage (i): Zur Abkürzung sei $\mathcal{U} := \{[x] \mid x \in X\}$ die Menge der Äquivalenzklassen. Wir weisen die Eigenschaften der Definition 5.18 nach. Zunächst ist jedes $x \in X$ Element seiner Äquivalenzklasse $[x]$, da ja $x \sim x$ gilt. Das zeigt Eigenschaft (i). Nach Satz 5.17 sind Äquivalenzklassen paarweise disunkt. Das zeigt Eigenschaft (ii). Schließlich sind Äquivalenzklassen nicht leer. Damit ist auch Eigenschaft (iii) gezeigt.

Der Beweis von Aussage (ii) ist Teil von Hausaufgabe 2.3. ☐

Definition 5.20 (Quotientenmenge, Invarianz).
Es sei X eine nichtleere Menge mit der Äquivalenzrelation $\sim$.

(i) Die Menge der Äquivalenzklassen

$$X/\!\sim := \{[x] \mid x \in X\} \tag{5.7}$$

heißt auch die **Quotientenmenge** (englisch: quotient set) oder die **Faktormenge** (englisch: factor set) von $\sim$.

(ii) Eine Aussageform A auf X heißt **invariant** (englisch: invariant) oder **wohldefiniert** (englisch: well-defined) unter $\sim$, wenn $x \sim y$ impliziert, dass $A(x)$ und $A(y)$ denselben Wahrheitswert haben.

Die Invarianz ist wichtig, wenn man eine Aussageform auf der Quotientenmenge dadurch definieren möchte, dass man sie auf den Elementen jeder Äquivalenzklasse definiert. Dabei ist sicherzustellen, dass sich tatsächlich für jedes Element einer Äquivalenzklasse derselbe Wahrheitswert ergibt.

Beispiel 5.21 (wohldefinierte Aussageformen).

(i) Die Aussageform „x ist eine gerade ganze Zahl" ist unter der Kongruenzrelation $\overset{2}{\equiv}$ wohldefiniert, da die Restklassen $[0]$ und $[1]$ jeweils nur aus geraden bzw. nur aus ungeraden ganzen Zahlen bestehen.

(ii) Dieselbe Aussageform ist jedoch unter der Kongruenzrelation $\overset{3}{\equiv}$ nicht wohldefiniert, da die Restklassen $[0]$, $[1]$ und $[2]$ jeweils sowohl gerade als auch ungerade ganze Zahlen enthalten.

Die Menge der rationalen Zahlen wurde zu Beginn von § 4 vorläufig als

$$\widetilde{\mathbb{Q}} := \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\}$$

eingeführt. Darin werden sind aber beispielsweise $\frac{1}{2}$, $\frac{3}{6}$ und $\frac{-2}{-4}$ unterschiedliche Elemente, die wir jedoch miteinander identifizieren wollen. Zu diesen Zweck verwenden wir die Äquivalenzrelation

$$\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \quad \Leftrightarrow \quad m_1 \cdot n_2 = m_2 \cdot n_1. \tag{5.8}$$

Das führt uns zur Definition

$$\mathbb{Q} := \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\} \ / \ \sim \tag{5.9}$$

für die **rationalen Zahlen**. Statt der Äquivalenzklasse $\left[\frac{m}{n}\right]$ schreiben wir üblicherweise weiter $\frac{m}{n}$, arbeiten also immer mit Repräsentanten. Das erklärt auch die übliche Notation $\frac{1}{2} = \frac{3}{6} = \frac{-2}{-4}$ an Stelle von $\frac{1}{2} \sim \frac{3}{6} \sim \frac{-2}{-4}$.

Ende der Vorlesung 4

Ende der Woche 2

§ 6 ABBILDUNGEN

Literatur: Deiser, 2022b, Kapitel 1.3, Deiser, 2022b, Kapitel 1.4

In diesem Abschnitt geht es um den grundlegenden Begriff der Abbildung oder Funktion. Eine Abbildung ist dabei nichts anderes als eine spezielle Relation.

Definition 6.1 (weitere Eigenschaften von Relationen)**.**
Es seien X und Y Mengen. Eine Relation (R, X, Y) zwischen X und Y heißt

(i) **linkstotal** (englisch: left-total), falls für alle $x \in X$ ein $y \in Y$ existiert, sodass $x \, R \, y$ gilt.

(ii) **rechtseindeutig** (englisch: right-unique), falls für alle $x \in X$ und alle $y_1, y_2 \in Y$ gilt: $x \, R \, y_1 \wedge x \, R \, y_2 \Rightarrow y_1 = y_2$.

Definition 6.2 (Funktion)**.**
Es seien X und Y Mengen. Eine linkstotale und rechtseindeutige Relation (f, X, Y) zwischen X und Y heißt **Abbildung** (englisch: map) oder **Funktion** (englisch: function) **von X in Y** oder **auf X mit Werten in Y**. Die Menge X heißt der **Definitionsbereich** (englisch: domain) oder die **Definitionsmenge** und die Menge Y der **Zielmenge** (englisch: codomain) von f. Ist $Y = X$, so spricht man auch von einer Funktion von X **in sich**.

Den Sachverhalt, dass f eine Funktion von X in Y ist, drücken wir auch in der Form

$$f \colon X \to Y \quad \text{oder} \quad X \xrightarrow{f} Y \quad \text{oder} \quad Y \xleftarrow{f} X$$

aus. Statt $x f y$ schreiben wir $y = f(x)$ oder $x \mapsto f(x)$ und sagen, x werde **abgebildet auf** $f(x)$. Auch die kompakten Schreibweisen

$$X \ni x \mapsto f(x) \in Y \quad \text{oder} \quad f \colon \begin{cases} X \to Y \\ x \mapsto f(x) \end{cases}$$

für die Definition einer Funktion sind üblich.

Beachte: Zwei Funktionen sind genau dann gleich, wenn sie in ihren Definitionsbereichen, Zielmengen und ihren Abbildungsvorschriften übereinstimmen.

Die Menge

$$\big\{(x, f(x)) \,\big|\, x \in X\big\} \subseteq X \times Y \tag{6.1}$$

heißt der **Graph** (englisch: graph) der Funktion $f \colon X \to Y$.[48]

Beispiel 6.3 (Abbildungen)**.**

(i) Es seien X und Y Mengen und $y_0 \in Y$. Dann heißt die Abbildung f mit

$$X \ni x \mapsto f(x) \coloneqq y_0 \in Y$$

die **konstante Funktion** (englisch: constant function) auf X mit dem Wert y_0.

---

[48] Der Begriff des Graphen einer Funktion stimmt also überein mit dem Begriff des Graphen der Funktion als Relation, vgl. Definition 5.1.

(ii) Es seien X und Y Mengen mit $X \subseteq Y$. Dann heißt die Abbildung $i_{X \to Y}$ mit

$$X \ni x \mapsto i_{X \to Y}(x) \coloneqq x$$

die **kanonische** oder **natürliche Injektion** (englisch: canonical injection, natural injection) oder die **kanonische** oder **natürliche Einbettung** (englisch: canonical embedding, natural embedding) von X in Y.

(iii) Im Fall $X = Y$ heißt die kanonische Einbettung auch die **Identität** (englisch: identity) oder **identische Abbildung** (englisch: identity map) von X in Y und wird mit id_X bezeichnet, also

$$X \ni x \mapsto \mathrm{id}_X(x) \coloneqq x.$$

Der Graph von id_X ist also gerade die Diagonale Δ_X, siehe (5.1).

Definition 6.4 (Bild, Einschränkung, Fortsetzung).
Es sei $f \colon X \to Y$ eine Funktion.[49]

(i) Für $A \subseteq X$ heißt

$$f(A) \coloneqq \{f(x) \mid x \in A\} \tag{6.2}$$

die **Bildmenge** oder kurz das **Bild** (englisch: image) von f **auf** A oder das **Bild** von A **unter** f.

(ii) Ist $A \subseteq X$, dann heißt die Funktion $f|_A$

$$A \ni x \mapsto f|_A(x) \coloneqq f(x) \in Y$$

die **Einschränkung** oder **Restriktion** (englisch: restriction, lateinisch: restringere: zurückziehen) von f auf A.

(iii) Gilt zusätzlich $f(A) \subseteq B$, so bezeichnen wir mit $f|_A^B$ die Einschränkung von f auf A, wobei zusätzlich die Zielmenge durch B ersetzt wird, also die Funktion

$$A \ni x \mapsto f|_A^B(x) \coloneqq f(x) \in B.$$

Gilt insbesondere $f(X) \subseteq B$, dann bezeichnet $f|^B$ die Funktion

$$X \ni x \mapsto f|^B(x) \coloneqq f(x) \in B,$$

bei der gegenüber f nur die Zielmenge ersetzt wird.

(iv) Ist $C \supseteq X$ und $D \supseteq Y$, dann heißt eine Funktion $g \colon C \to D$, die auf X mit f übereinstimmt, für die also $g|_X^Y = f$ gilt, eine **Fortsetzung** (englisch: extension) von f.

An Stelle von $f|_A$ schreibt man auch manchmal $f \restriction A$.

Beispiel 6.5 (Bild, Einschränkung, Fortsetzung).
Wir betrachten die Funktionen[50]

$$\begin{aligned}
\mathbb{R} \ni x \mapsto f(x) &\coloneqq \sin(x) \in \mathbb{R} && \text{mit dem Bild } [-1, 1],\\
\mathbb{R} \ni x \mapsto g(x) &\coloneqq \sin(x) \in [-1, 1] && \text{mit dem Bild } [-1, 1],\\
\frac{\pi}{2}\mathbb{Z} \ni x \mapsto h(x) &\coloneqq \sin(x) \in [-1, 1] && \text{mit dem Bild } \{-1, 0, 1\},\\
\frac{\pi}{2}\mathbb{Z} \ni x \mapsto i(x) &\coloneqq \sin(x) \in \{-1, 0, 1\} && \text{mit dem Bild } \{-1, 0, 1\}.
\end{aligned}$$

Dann sind g, h und i Einschränkungen von f, und f ist eine Fortsetzung von g, h und i.

---

[49] Wir sagen damit insbesondere, dass X und Y Mengen sind.

[50] Hierbei bedeutet $\frac{\pi}{2}\mathbb{Z}$ die Menge der ganzzahligen Vielfachen von $\frac{\pi}{2}$.

Definition 6.6 (Urbild)**.**
Es sei $f\colon X \longrightarrow Y$ eine Funktion. Für $B \subseteq Y$ heißt die Menge

$$f^{-1}(B) \coloneqq \{x \in X \mid f(x) \in B\} \tag{6.3}$$

die **Urbildmenge** oder das **Urbild** (englisch: pre-image) von B **unter** f.

Beispiel 6.7 (Urbild)**.**
Wir betrachten die Funktion

$$\mathbb{R} \ni x \mapsto x^2 \in \mathbb{R}.$$

Dann ist

$$f^{-1}(\{y\}) = \begin{cases} \big\{\sqrt{y}, -\sqrt{y}\big\} & \text{falls } y > 0, \\ \{0\} & \text{falls } y = 0, \\ \emptyset & \text{falls } y < 0. \end{cases}$$

Satz 6.8 (Bilder und Urbilder von Vereinigungen und Durchschnitten)**.**
Es sei $f\colon X \longrightarrow Y$ eine Funktion. Weiter seien I und J irgendwelche Indexmengen und $\{X_i \mid i \in I\}$ eine Menge von Teilmengen von X sowie $\{Y_j \mid j \in J\}$ eine Menge von Teilmengen von Y. Dann gilt:

$$f\Big(\bigcup_{i \in I} X_i\Big) = \bigcup_{i \in I} f(X_i) \tag{6.4a}$$

$$f\Big(\bigcap_{i \in I} X_i\Big) \subseteq \bigcap_{i \in I} f(X_i) \tag{6.4b}$$

$$f^{-1}\Big(\bigcup_{j \in J} Y_j\Big) = \bigcup_{j \in J} f^{-1}(Y_j) \tag{6.4c}$$

$$f^{-1}\Big(\bigcap_{j \in J} Y_j\Big) = \bigcap_{j \in J} f^{-1}(Y_j) \tag{6.4d}$$

Beweis. Wir beweisen hier nur (6.4a) und (6.4c). Die Aussagen (6.4b) und (6.4d) sind Teil von Hausaufgabe 3.1.

Zum Beweis von (6.4a):

$$\begin{aligned} & y \in f\Big(\bigcup_{i \in I} X_i\Big) \\ \Leftrightarrow\quad & \exists i \in I \; \exists x \in X_i \; (y = f(x)) && \text{nach Definition (4.6) der Vereinigungsmenge} \\ \Leftrightarrow\quad & \exists i \in I \; (y \in f(X_i)) && \text{nach Definition (6.2) des Bildes } f(X_i) \\ \Leftrightarrow\quad & y \in \bigcup_{i \in I} f(X_i) && \text{nach Definition (4.6) der Vereinigungsmenge.} \end{aligned}$$

Zum Beweis von (6.4c):

$$\begin{aligned} & x \in f^{-1}\Big(\bigcup_{j \in J} Y_j\Big) \\ \Leftrightarrow\quad & \exists y \in \bigcup_{j \in J} Y_j \; \big(y = f(x)\big) && \text{nach Definition (6.3) des Urbildes} \\ \Leftrightarrow\quad & \exists j \in J \; \exists y \in Y_j \; \big(y = f(x)\big) && \text{nach Definition (4.6) der Vereinigungsmenge} \\ \Leftrightarrow\quad & \exists j \in J \; \big(x \in f^{-1}(Y_j)\big) && \text{nach Definition (6.3) des Urbildes} \\ \Leftrightarrow\quad & x \in \bigcup_{j \in J} f^{-1}(Y_j) && \text{nach Definition (4.6) der Vereinigungsmenge.} \end{aligned}$$

□

Beispiel 6.9 (Bilder und Urbilder von Vereinigungen und Durchschnitten)**.**
In (6.4b) gilt i. A. nicht die Gleichheit, wie folgendes Beispiel zeigt: Es sei

$$\mathbb{R}^2 \ni (x, y) \mapsto f(x, y) \coloneqq x \in \mathbb{R}.$$

Für die Mengen $A \coloneqq \{(0,0)\}$ und $B = \{(0,1)\}$ gilt

$$\begin{aligned} & f(A \cap B) = f(\emptyset) = \emptyset, \\ \text{aber} \quad & f(A) \cap f(B) = \{0\} \cap \{0\} = \{0\}. \end{aligned}$$

§ 6.1 INJEKTIVITÄT UND SURJEKTIVITÄT

Definition 6.10 (Injektivität, Surjektivität, Bijektivität)**.**
Eine Funktion $f\colon X \longrightarrow Y$ heißt

(*i*) **surjektiv** (englisch: surjective, onto) oder **rechtstotal** (englisch: right-total), wenn $f(X) = Y$ gilt.[51] Man sagt auch, f bilde X **auf** Y ab.

Äquivalent dazu ist

$$\forall y \in Y \ (f^{-1}(\{y\}) \neq \emptyset)$$

(*ii*) **injektiv** (englisch: injective, one-to-one) oder **linkseindeutig** (englisch: left-unique), wenn für alle $x_1, x_2 \in X$ gilt: $f(x_1) = f(x_2) \quad \Rightarrow \quad x_1 = x_2$.[52]

Äquivalent dazu ist

$$\forall y \in Y \ (f^{-1}(\{y\}) \text{ hat kein oder genau ein Element})$$

(*iii*) **bijektiv** (englisch: bijective), wenn f surjektiv und injektiv ist.[53]

Äquivalent dazu ist

$$\forall y \in Y \ (f^{-1}(\{y\}) \text{ hat genau ein Element})$$

Als Substantive sind die Bezeichnungen **Surjektion** (englisch: surjection), **Injektion** (englisch: injection) und **Bijektion** (englisch: bijection) geläufig.

Quizfrage 6.1: Können Sie (nicht-mathematische) Beispiele für injektive, surjektive bzw. bijektive Funktionen benennen?

Lemma 6.11 (Bijektiv-Machen einer injektiven Funktion)**.**
Es sei $f\colon X \longrightarrow Y$ eine injektive Funktion. Dann ist $f|^{f(X)}$ (also die Einschränkung der Zielmenge auf die tatsächliche Bildmenge) bijektiv.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 3.2. □

Beispiel 6.12 (Injektivität, Surjektivität, Bijektivität)**.**

---

[51] Die Surjektivität von f wird manchmal auch durch die Schreibweise $f\colon X \twoheadrightarrow Y$ ausgedrückt.
[52] Die Injektivität von f wird manchmal auch durch die Schreibweise $f\colon X \rightarrowtail Y$ ausgedrückt.
[53] Die Bijektivität von f wird manchmal auch durch die Schreibweise $f\colon X \rightarrowtail\!\!\!\!\!\twoheadrightarrow Y$ ausgedrückt.

(*i*) Die Funktion

$$\mathbb{R} \ni x \mapsto x^2 \in \mathbb{R}$$

ist nicht surjektiv und nicht injektiv.

(*ii*) Die Funktion

$$\mathbb{R} \ni x \mapsto x^2 \in \mathbb{R}_{\geqslant 0}$$

ist surjektiv, aber nicht injektiv. Hierbei ist $\mathbb{R}_{\geqslant 0} = \{x \in \mathbb{R} \mid x \geqslant 0\}$ die Menge der nichtnegativen reellen Zahlen.

(*iii*) Die Funktion

$$\mathbb{R}_{\geqslant 0} \ni x \mapsto x^2 \in \mathbb{R}$$

ist injektiv, aber nicht surjektiv.

(*iv*) Die Funktion

$$\mathbb{R}_{\geqslant 0} \ni x \mapsto x^2 \in \mathbb{R}_{\geqslant 0}$$

ist bijektiv.

(*v*) Sind X und Y Mengen mit $X \subseteq Y$, dann ist die kanonische Injektion $i_{X \to Y}$ injektiv.

Definition 6.13 (Komposition von Funktionen)**.**
Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ Funktionen. Die Funktion

$$X \ni x \mapsto h(x) \coloneqq g(f(x)) \in Z$$

heißt die **Komposition** (englisch: composition, lateinisch: componere: zusammenstellen), die **Hintereinanderausführung**, die **Verknüpfung** oder die **Verkettung** von f und g. Sie wird auch mit $h = g \circ f$ bezeichnet. Um die Reihenfolge klar zu benennen, sagt man auch „g **nach** f“.

Wir können den Sachverhalt aus Definition 6.13 auch durch

$$\begin{tikzcd}
Z & Y \arrow[l, "g"'] & X \arrow[l, "f"'] \arrow[ll, bend left, "g\circ f"]
\end{tikzcd}$$

illustrieren.

Die Voraussetzung, dass die Zielmenge von f mit der Definitionsmenge von g übereinstimmt, kann relaxiert werden. Die Komposition $g \circ f$ ist definiert, solange $f(X) \subseteq Y$ gilt.

Beispiel 6.14 (Komposition von Funktionen)**.**
Es seien

$$\begin{aligned} \mathbb{R} \ni x &\mapsto f(x) \coloneqq x^2 \in \mathbb{R}, \\ \mathbb{R} \ni x &\mapsto g(x) \coloneqq x + 1 \in \mathbb{R}. \end{aligned}$$

Dann sind $f(\mathbb{R}) \subseteq \mathbb{R}$ und $g(\mathbb{R}) \subseteq \mathbb{R}$, also sind sowohl $g \circ f$ als auch $f \circ g$ definiert. Sie sind gegeben durch

$$\begin{aligned} \mathbb{R} \ni x &\mapsto (g \circ f)(x) \coloneqq x^2 + 1 \in \mathbb{R}, \\ \mathbb{R} \ni x &\mapsto (f \circ g)(x) \coloneqq (x+1)^2 \in \mathbb{R}. \end{aligned}$$

Bemerkung 6.15 (Komposition mit der Identität und mit der kanonischen Einbettung).
Es sei $f\colon X \to Y$ eine Funktion. Dann gilt

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f, \tag{6.5}$$

$$f|_A = f \circ i_{A \to X} \qquad \text{für } A \subseteq X, \tag{6.6}$$

$$f = (i_{Y \to B} \circ f)|^Y \qquad \text{für } B \supseteq Y. \tag{6.7}$$

Lemma 6.16 (Komposition von Funktionen ist assoziativ).
Es seien $f\colon X \to Y$, $g\colon Y \to Z$ und $h\colon Z \to W$ Funktionen. Dann gilt $(h \circ g) \circ f = h \circ (g \circ f)$, d. h., die Komposition von Funktionen ist assoziativ.

Beweis. Für $x \in X$ gilt

$$\begin{aligned} & \big((h \circ g) \circ f\big)(x) = (h \circ g)(f(x)) = h(g(f(x))) \\ \text{und} \quad & \big(h \circ (g \circ f)\big)(x) = h\big((g \circ f)(x)\big) = h(g(f(x))). \end{aligned}$$

Folglich stimmen $(h \circ g) \circ f\colon X \to W$ und $h \circ (g \circ f)\colon X \to W$ in Definitionsbereich, Zielmenge und Abbildungsvorschrift überein. □

Lemma 6.17 (Komposition injektiver und surjektiver Funktionen).
Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ Funktionen.

(*i*) Sind f und g beide injektiv, so ist auch $g \circ f$ injektiv.

(*ii*) Sind f und g beide surjektiv, so ist auch $g \circ f$ surjektiv.

(*iii*) Ist $g \circ f$ injektiv, so ist f injektiv.

(*iv*) Ist $g \circ f$ surjektiv, so ist g surjektiv.

Beweis. Aussage (*i*): Für $x_1, x_2 \in X$ gelte $(g \circ f)(x_1) = (g \circ f)(x_2)$, also $g(f(x_1)) = g(f(x_2))$. Aus der Injektivität von g folgt $f(x_1) = f(x_2)$, und aus der Injektivität von f folgt weiter $x_1 = x_2$. Also ist $g \circ f$ injektiv.

Aussage (*ii*): Es sei $z \in Z$. Aufgrund der Surjektität von g gibt es ein $y \in Y$, sodass $z = g(y)$ gilt. Wegen der Surjektivität von f gibt es ein $x \in X$, sodass $y = f(x)$ gilt. Es gilt also $z = g(y) = g(f(x)) = (g \circ f)(x)$, d. h., $z \in (g \circ f)(X)$.

Aussage (*iii*): Es seien $x_1, x_2 \in X$, sodass $f(x_1) = f(x_2)$ gilt. Dann gilt auch $g(f(x_1)) = g(f(x_2))$, und wegen der Injektivität von $g \circ f$ folgt $x_1 = x_2$, d. h., f ist injektiv.

Aussage (*iv*): Es sei $z \in Z$. Aufgrund der Surjektivität von $g \circ f$ gibt es ein $x \in X$, sodass $z = g(f(x))$ gilt. Das heißt aber $z = g(y)$ für $y = f(x)$, also ist g surjektiv. □

Folgerung 6.18 (Komposition zur Identität).
Es seien $f\colon X \to Y$ und $g\colon Y \to X$ Funktionen. Wenn $g \circ f = \mathrm{id}_X$ ist, dann ist f injektiv und g surjektiv.

Beweis. Die Identitätsabbildung id_X ist bijektiv. Aus Lemma 6.17, Aussagen (*iii*) und (*iv*) folgt daher, dass f injektiv und g surjektiv ist. □

Ende der Vorlesung 5

---

§ 6.2 UMKEHRABBILDUNG

Lemma 6.19 (Charakterisierung der Bijektivität)**.**
Es sei $f : X \longrightarrow Y$ eine Funktion. Dann sind äquivalent:

(i) f ist bijektiv.

(ii) Für alle $y \in Y$ gibt es genau ein $x \in X$ mit der Eigenschaft $f(x) = y$.

(iii) Es existiert eine Abbildung $g \colon Y \longrightarrow X$ mit der Eigenschaft $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$. Die Abbildung g ist eindeutig bestimmt und notwendig bijektiv.

Beweis. Aussage (i) $\Longrightarrow$ Aussage (ii): Es sei f bijektiv, also surjektiv und injektiv. Ist $y \in Y$ beliebig, dann folgt aus der Surjektivität die Existenz eines $x_1 \in X$ mit $f(x_1) = y$. Ist $x_2 \in X$ ein weiteres Element mit $f(x_2) = y$, dann folgt aus der Injektivität $x_1 = x_2$.

Aussage (ii) $\Longrightarrow$ Aussage (iii): Wir definieren die Abbildung $g \colon Y \longrightarrow X$ wie folgt: Wir setzen für $y \in Y$ als $g(y)$ das nach Voraussetzung eindeutig definierte $x \in X$, für das $y = f(x)$ gilt. Für diese Funktion haben wir also $g(y) = x \Leftrightarrow f(x) = y$.

$$(g \circ f)(x) = g(f(x)) = x \quad \text{für alle } x \in X$$

sowie

$$(f \circ g)(y) = f(g(y)) = y \quad \text{für alle } y \in Y.$$

Damit ist $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ gezeigt.

Es sei nun $\widehat{g} \colon Y \longrightarrow X$ eine weitere Funktion mit der Eigenschaft $f \circ \widehat{g} = \mathrm{id}_Y$. Dann gilt

$$\begin{aligned} g &= g \circ \mathrm{id}_Y && \text{nach (6.5)} \\ &= g \circ (f \circ \widehat{g}) && \text{nach Voraussetzung} \\ &= (g \circ f) \circ \widehat{g} && \text{nach Lemma 6.16} \\ &= \mathrm{id}_X \circ \widehat{g} && \text{nach Voraussetzung} \\ &= \widehat{g} && \text{nach (6.5).} \end{aligned}$$

Aussage (iii) $\Longrightarrow$ Aussage (i): Die Abbildung $g \circ f = \mathrm{id}_X$ ist bijektiv, insbesondere injektiv. Aus Lemma 6.17 (iii) folgt also, dass f injektiv ist. Die Abbildung $f \circ g = \mathrm{id}_Y$ ist bijektiv, insbesondere surjektiv. Aus Lemma 6.17 (iv) folgt also, dass f surjektiv ist. □

Die Funktion $g \colon Y \longrightarrow X$ aus Aussage (iii) heißt die **Umkehrfunktion**, **Umkehrabbildung**, **inverse Funktion** oder **inverse Abbildung** (englisch: inverse map) von f. Sie wird mit $f^{-1} \colon Y \longrightarrow X$ bezeichnet. Für ihre Abbildungsvorschrift gilt $f^{-1}(y) = x \Leftrightarrow y = f(x)$. Die Funktion $f : X \longrightarrow Y$ heißt **invertierbar** (englisch: invertible), wenn die Umkehrfunktion existiert. Nach Lemma 6.19 ist das genau dann der Fall, wenn f bijektiv ist.

Bemerkung 6.20 (Umkehrfunktion)**.**
Das Symbol f^{-1} für die Umkehrfunktion muss vom Urbild der Funktion f unterschieden werden. Wenn die Umkehrfunktion von $f : X \longrightarrow Y$ existiert, so gilt jedoch

$$\underbrace{f^{-1}(\{y\})}_{\text{Urbild von } \{y\}} = \{\underbrace{f^{-1}(y)}_{\text{Wert der Umkehrfunktion bei } y}\}.$$

Satz 6.21 (Umkehrfunktion der Komposition).

Es seien $f\colon X \longrightarrow Y$ und $g\colon Y \longrightarrow Z$ bijektive Funktionen. Dann ist auch $g \circ f$ bijektiv, und die Umkehrfunktion ist gegeben durch

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{6.8}$$

Quizfrage 6.2: Wie erklärt man sich anschaulich, dass sich bei der Umkehrfunktion die Reihenfolge ändert?

Beweis. Die Bijektivität von $g \circ f$ folgt sofort aus Lemma 6.17, Aussagen (i) und (ii). Wir wissen über die Abbildungsvorschrift

$$\begin{aligned} & (g \circ f)^{-1}(z) = x \\ \Leftrightarrow\quad & (g \circ f)(x) = z \\ \Leftrightarrow\quad & g(f(x)) = z \\ \Leftrightarrow\quad & f(x) = g^{-1}(z) \\ \Leftrightarrow\quad & x = f^{-1}(g^{-1}(z)) \\ \Leftrightarrow\quad & x = (f^{-1} \circ g^{-1})(z) \end{aligned}$$

für alle $x \in X$ und $z \in Z$. Das bedeutet aber $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Lemma 6.22 (Charakterisierung der Injektivität).

Es sei $f\colon X \longrightarrow Y$ eine Funktion und $X \neq \emptyset$. Dann sind äquivalent:

(i) f ist injektiv.

(ii) Es existiert eine Abbildung $g\colon Y \longrightarrow X$ mit der Eigenschaft $g \circ f = \mathrm{id}_X$. Eine solche Abbildung heißt eine **Linksinverse** (englisch: left inverse) von f. Sie ist notwendig surjektiv. Ihre Einschränkung $g|_{f(X)}$ auf das Bild von f ist eindeutig.

Beweis. Aussage (i) ⟹ Aussage (ii): Wir definieren zunächst eine Abbildung $\overline{g}\colon f(X) \longrightarrow X$ wie folgt: Wir setzen für $y \in f(X)$ als $\overline{g}(y)$ das wegen der Injektivität eindeutig definierte $x \in X$, für das $y = f(x)$ gilt. Für diese Funktion haben wir also $\overline{g}(y) = x \Leftrightarrow f(x) = y$ und damit

$$(\overline{g} \circ f)(x) = \overline{g}(f(x)) = x \quad \text{für alle } x \in X.$$

Damit ist $\overline{g} \circ f = \mathrm{id}_X$ gezeigt. Aufgrund von Folgerung 6.18 ist $\overline{g}$ surjektiv. Wir setzen nun $\overline{g}\colon f(X) \longrightarrow X$ zu $g\colon X \longrightarrow X$ fort. Dazu wählen wir irgendein $x_0 \in X$ und setzen $g(y) \coloneqq \overline{g}(y)$ für $y \in f(X)$ und $g(y) \coloneqq x_0$ für $y \in Y \setminus f(X)$. Die Funktion g erbt die Surjektivität von $\overline{g}$.

Angenommen, $h\colon Y \longrightarrow X$ sei eine andere Linksinverse von f. Dann gilt für $y \in f(X)$ aufgrund der Injektivität von f: Es gibt genau ein $x \in X$ mit der Eigenschaft $y = f(x)$. Wegen $h(y) = h(f(x)) = x$ und ebenso $g(y) = g(f(x)) = x$ müssen g und h auf $f(X)$ übereinstimmen. □

Eine analoge Charakterisierung der Surjektivität folgt erst in Satz 6.34, weil wir dafür interessanterweise das Auswahlaxiom benötigen.

§ 6.3 MÄCHTIGKEIT VON MENGEN

Mit Hilfe von Funktionen können wir Mengen in ihrer Mächtigkeit, das heißt vereinfacht gesagt bzgl. der Anzahl ihrer Elemente, vergleichen.

Definition 6.23 (Gleichmächtigkeit von Mengen)**.**
Es seien X und Y Mengen. Wir sagen, X sei **gleichmächtig** (englisch: equinumerous) zu Y, wenn es eine bijektive Abbildung $f \colon X \to Y$ gibt. Wir schreiben in diesem Fall $X \sim Y$.

Die Gleichmächtigkeit von Mengen ist eine Äquivalenzrelation auf der Klasse aller Mengen, siehe Hausaufgabe 3.3. Die Äquivalenzklassen heißen **Kardinalzahlen** (englisch: cardinal numbers).

Definition 6.24 (Endlichkeit, Abzählbarkeit, Überabzählbarkeit)**.**
Es sei X eine Menge.

(i) X heißt **endlich** (englisch: finite), wenn $X \sim [\![1, n]\!]$ für ein $n \in \mathbb{N}_0$ gilt, ansonsten **unendlich** (englisch: infinite).

(ii) Wenn X endlich ist mit $X \sim [\![1, n]\!]$, dann heißt $n \in \mathbb{N}_0$ die **Mächtigkeit** oder **Kardinalität** (englisch: cardinality) von X. Wir schreiben dann: $\#X = n$.[54]

(iii) X heißt **abzählbar unendlich** (englisch: countably infinite), wenn $X \sim \mathbb{N}$ gilt.

(iv) X heißt **abzählbar** (englisch: countable), wenn X entweder endlich oder abzählbar unendlich ist, ansonsten **überabzählbar** (englisch: uncountable).

Beachte: Die leere Menge $\emptyset$ ist nur zu sich selbst gleichmächtig. Sie ist die einzige Menge mit Mächtigkeit 0.

Beispiel 6.25 (Gleichmächtigkeit von Mengen, Abzählbarkeit, Überabzählbarkeit)**.**

(i) Die Menge der ganzen Zahlen $\mathbb{Z}$ ist gleichmächtig zur Menge der geraden ganzen Zahlen $\{2\,n \mid n \in \mathbb{Z}\}$. Sie ist abzählbar unendlich.

(ii) Die Menge der rationalen Zahlen $\mathbb{Q}$ ist abzählbar unendlich.
(Beweis in der Lehrveranstaltung *Analysis*)

(iii) Die Vereinigung abzählbar vieler abzählbarer Mengen ist wieder abzählbar.

(iv) Die Menge der reellen Zahlen $\mathbb{R}$ ist überabzählbar.
(Beweis in der Lehrveranstaltung *Analysis*)

Lemma 6.26 (Veränderung der Kardinalität um 1)**.**
Es sei X eine endliche Menge und $x \in X$. Dann gilt

$$\#X = \#(X \setminus \{x\}) + 1. \tag{6.9}$$

Beweis. Es sei $n = \#(X \setminus \{x\}) \in \mathbb{N}_0$. Es gibt also eine bijektive Abbildung $\widehat{f} \colon \{1, \ldots, n\} \to X \setminus \{x\}$. Wir definieren $f \colon \{1, \ldots, n+1\} \to X$ durch $f(i) \coloneqq \widehat{f}(i)$ für $i = 1, \ldots, n$ und $f(n+1) \coloneqq x$. Dann ist f ebenfalls bijektiv, d. h., $\#X = n + 1 = \#(X \setminus \{x\}) + 1$. □

---

[54] In dieser Lehrveranstaltung verwenden wir das Symbol # nur für endliche Mengen.

Satz 6.27 (Funktionen auf endlichen Mengen).

Es seien X und Y endliche, gleichmächtige Mengen und $f\colon X \to Y$ eine Funktion. Dann sind äquivalent:

(i) f ist injektiv.

(ii) f ist surjektiv.

(iii) f ist bijektiv.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Wir führen einen Induktionsbeweis nach der Mächtigkeit $n = \#X = \#Y$. Der Induktionsanfang ist der Fall $n = 0$, also $X = Y = \emptyset$. Dann ist die einzig mögliche Abbildung die leere Abbildung, diese ist bijektiv. Im Induktionsschritt schließen wir von n auf $n+1$ für $n \in \mathbb{N}_0$. Es sei also nun $\#X = \#Y = n+1$. Wir wählen ein $x \in X$ und setzen $y := f(x)$. Dann gilt aufgrund von Lemma 6.26 $\#X \setminus \{x\} = \#Y \setminus \{y\} = n$.

Wir bezeichnen mit $\widehat{f}\colon X \setminus \{x\} \to Y \setminus \{y\}$ die Einschränkung von f. Diese ist aufgrund der vorausgesetzten Injektivität definiert, denn x ist das einzige Element von X, das durch f auf y abgebildet wird. Außerdem erbt $\widehat{f}$ die Injektivität von f. Nach Induktionsvoraussetzung ist $\widehat{f}$ daher auch surjektiv, alle Elemente von $Y \setminus \{y\}$ liegen also im Bild von $\widehat{f}$ und damit im Bild von f. Da auch y im Bild von f liegt, ist f tatsächlich surjektiv.

Aussage (ii) $\Rightarrow$ Aussage (i): Wir führen auch hier einen Induktionsbeweis nach der Mächtigkeit $n = \#X = \#Y$. Der Induktionsanfang beinhaltet die Fälle $n = 0$ und $n = 1$. Im Fall $n = 0$ ist $X = Y = \emptyset$, dann ist die einzig mögliche Abbildung die leere Abbildung, diese ist bijektiv. Im Fall $n = 1$ gibt es nur eine mögliche Abbildung, diese ist ebenfalls bijektiv. Im Induktionsschritt schließen wir von n auf $n+1$ für $n \in \mathbb{N}$. Es sei also nun $\#X = \#Y = n+1$. Wir führen einen Widerspruchsbeweis, nehmen also an, dass f surjektiv, aber *nicht* injektiv ist. Dann gibt es ein $\overline{y} \in Y$, sodass das Urbild $f^{-1}(\{\overline{y}\})$ (mindestens) aus zwei verschiedenen Elemente besteht, sagen wir $\overline{x}, \overline{\overline{x}} \in f^{-1}(\{\overline{y}\})$ und $\overline{x} \neq \overline{\overline{x}}$. Wir wählen außerdem ein $\widehat{y} \in Y \setminus \{\overline{y}\}$ aus, was wegen $\#Y = n+1 \geqslant 2$ möglich ist. Dazu existiert ein $\widehat{x}$ mit $f(\widehat{x}) = \widehat{y}$. Wegen $\widehat{y} \neq \overline{y}$ ist $\widehat{x} \neq \overline{x}$ und $\widehat{x} \neq \overline{\overline{x}}$.

Wir konstruieren nun eine Funktion $\widehat{f}\colon X \setminus \{\overline{x}\} \to Y \setminus \{\overline{y}\}$ durch

$$\widehat{f}(x) := \begin{cases} f(x) & \text{im Fall } f(x) \neq \overline{y}, \\ \widehat{y} & \text{im Fall } f(x) = \overline{y}. \end{cases}$$

Dann ist $\widehat{f}$ ebenfalls surjektiv, denn:

(1) Für jedes $y \in Y \setminus \{\overline{y}, \widehat{y}\}$ existiert aufgrund der Surjektivität von f ein $x \in X$ mit $\widehat{f}(x) = f(x) = y$, und wegen $f(\overline{x}) = \overline{y}$ ist $x \in X \setminus \{\overline{x}\}$.

(2) Außerdem gilt $f(\overline{\overline{x}}) = \overline{y}$, also $\widehat{f}(\overline{\overline{x}}) = \widehat{y}$.

Aufgrund von Lemma 6.26 gilt wieder $\#X \setminus \{\overline{x}\} = \#Y \setminus \{\overline{y}\} = n$. Nach Induktionsvoraussetzung ist $\widehat{f}$ daher auch injektiv. Jedoch enthält $\widehat{f}^{-1}(\{\widehat{y}\})$ neben $\widehat{x}$ auch noch mindestens das weitere Element $\overline{\overline{x}} \in f^{-1}(\{\overline{y}\})$. Das steht im Widerspruch zur Injektivität von $\widehat{f}$.

Wir haben jetzt Aussage (i) $\Leftrightarrow$ Aussage (ii) bewiesen. Da die Bijektivität sich aus Surjektivität und Injektivität zusammensetzt, gilt auch Aussage (i) $\Leftrightarrow$ Aussage (ii) $\Leftrightarrow$ Aussage (iii). ☐

Beachte: Die Aussage von Satz 6.27 ist falsch, wenn X und Y zwar gleichmächtig, aber nicht endlich sind, siehe Hausaufgabe 3.3.

Der Begriff der Gleichmächtigkeit von Mengen erlaubt noch keinen Vergleich von Mengen. Dazu dient folgende Definition.

Definition 6.28 (Vergleich der Mächtigkeit von Mengen).
Es seien X und Y Mengen. Wir sagen, X sei **höchstens gleichmächtig** (englisch: at most equinumerous) zu Y, wenn es eine bijektive Abbildung von X auf eine Teilmenge von Y gibt. Wir schreiben in diesem Fall $X \precsim Y$.

Die Reflexivität und Transitivität der Relation $\precsim$ sind leicht einzusehen. (**Quizfrage 6.3:** Details?) Der Beweis der Antisymmetrie ist jedoch aufwändig und erfordert den Satz von Cantor-Bernstein-Schröder, der äquivalent zum Auswahlaxiom (siehe § 6.5) ist. Unter Zuhilfenahme des Auswahlaxioms kann man außerdem zeigen, dass zwei Mengen bzgl. $\precsim$ stets vergleichbar sind. Es folgt, dass $\precsim$ sogar eine totale Ordnung auf der Klasse aller Mengen ist.

§ 6.4 Familien und Folgen

Definition 6.29 (Familie von Elementen, Teilfamilie, Oberfamilie, Folge, endliche Folge).
Es seien I und Y Mengen.

(i) Eine Abbildung
$$I \ni i \mapsto y(i) \coloneqq y_i \in Y$$
heißt eine **Familie von Elementen** (englisch: family of elements) aus Y mit der **Indexmenge** (englisch: index set) I. Kurz wird diese auch mit $(y_i)_{i \in I}$ bezeichnet.

(ii) Ist $I_0 \subseteq I$, dann heißt $(y_i)_{i \in I_0}$ eine **Teilfamilie** (englisch: subfamily) von $(y_i)_{i \in I}$, und $(y_i)_{i \in I}$ heißt eine **Oberfamilie** (englisch: superfamily) von $(y_i)_{i \in I_0}$.

(iii) Ist I abzählbar unendlich, gilt also $I \sim \mathbb{N}$, so heißt $(y_i)_{i \in I}$ eine **abzählbar unendliche Familie** (englisch: countably infinite family). Ist speziell $I = \mathbb{N}$ oder allgemeiner $I = \{n \in \mathbb{Z} \mid n \geqslant n_0\}$ mit einem Startindex $n_0 \in \mathbb{Z}$, so heißt $(y_i)_{i \in I}$ eine **Folge** (englisch: sequence) in Y.

(iv) Ist I endlich, gilt also $I \sim [\![1, n]\!]$ für ein $n \in \mathbb{N}_0$, so heißt $(y_i)_{i \in I}$ eine **endliche Familie** (englisch: finite family). Ist speziell $I = [\![1, n]\!]$, so heißt $(y_i)_{i \in I}$ eine **endliche Folge** (englisch: finite sequence) in Y.

Bemerkung 6.30 (Familien und Mengen).

(i) Im Unterschied zu einer Menge kann eine Familie $(y_i)_{i \in I}$ Elemente mehrfach enthalten.

(ii) Jeder Familie $(y_i)_{i \in I}$ von Elementen aus Y können wir eine Menge $\{y_i \mid i \in I\} \subseteq Y$ zuordnen.

(iii) Wir können eine endliche Folge auch als **n-Tupel** (englisch: n-tuple) $(y_1, y_2, \dots, y_n)$ notieren. Während $(y_i)_{i \in I}$ keine Reihenfolge hat (da I als Menge ungeordnet ist), hat ein n-Tupel jedoch eine festgelegte Reihenfolge.

Beispiel 6.31 (Folge).
Die Abbildung
$$\mathbb{N} \ni n \mapsto y_n \coloneqq \frac{1}{n} \in \mathbb{R}$$
ist eine Folge in $\mathbb{R}$ mit der Standard-Indexmenge $\mathbb{N}$. Kurz wird diese Folge auch als $\left(\frac{1}{n}\right)_{n \in \mathbb{N}}$ bezeichnet.

§ 6.5 DAS AUSWAHLAXIOM

Das **Auswahlaxiom** (englisch: axiom of choice) der axiomatischen Mengenlehre besagt: Ist $\mathcal{U}$ eine Menge von nichtleeren Mengen, dann gibt es eine Funktion $F\colon \mathcal{U} \to \bigcup \mathcal{U}$, sodass gilt:

$$\forall U \in \mathcal{U} \; \bigl(F(U) \in U\bigr).$$

Eine solche Funktion F heißt **Auswahlfunktion** (englisch: choice function) für $\mathcal{U}$, weil sie aus jedem Element U von $\mathcal{U}$ irgendein Element auswählt. Das Auswahlaxiom besagt also, dass es möglich ist, aus jedem Element von $\mathcal{U}$ ein Element auszuwählen, selbst wenn $\mathcal{U}$ überabzählbar viele Mengen als Elemente enthält und man daher nicht in der Lage ist, ein Verfahren anzugeben, nach dem die Auswahl geschehen soll.

Das Auswahlaxiom ist kein fester Bestandteil der axiomatischen Mengenlehre nach Zermelo und Fraenkel, sondern es kann dazugenommen werden oder auch nicht.[55] Es wird aber wohl von den meisten Mathematiker:innen akzeptiert. In Fällen, in denen $\mathcal{U}$ nur endlich viele Mengen enthält, wird das Auswahlaxiom nicht benötigt, weil seine Aussage bereits aus den anderen Axiomen folgt. Wir werden in der Vorlesung darauf hinweisen, wenn ein Resultat von der Hinzunahme des Auswahlaxioms abhängt. Einige Beispiele folgen bereits in diesem Abschnitt, siehe Satz 6.34.

Definition 6.32 (allgemeines kartesisches Produkt).
Es sei I eine ~~nichtleere~~ Indexmenge und $(A_i)_{i\in I}$ eine Familie von Mengen. Dann ist das **kartesische Produkt** (englisch: Cartesian product) dieser Familie von Mengen gegeben durch

$$\bigtimes_{i\in I} A_i \coloneqq \left\{ F\colon I \to \bigcup_{i\in I} A_i \;\middle|\; F(i) \in A_i \text{ für alle } i \in I \right\}. \tag{6.10}$$

Das kartesische Produkt einer Familie von Mengen besteht also aus *Funktionen* auf der Indexmenge I, deren Funktionswerte jeweils im richtigen Faktor liegen. Im Fall $I = \emptyset$ besteht das kartesische Produkt (6.10) aus dem einzigen Element $F\colon \emptyset \to \emptyset$.

Bemerkung 6.33 (Allgemeine kartesische Produkte).
Das **kartesische Produkt** hatten wir bisher nur für endlich viele Mengen definiert, siehe Definition 4.8. Die allgemeine Definition 6.32 erfordert den Funktionenbegriff, der nun zur Verfügung steht. Die Definition 6.32 lässt sich als Verallgemeinerung der Definition 4.8 verstehen: Ist nämlich die Indexmenge $I = [\![1, n]\!]$, so ist $\bigtimes_{i\in I} A_i$ nach (6.10) die Menge aller n-elementigen Folgen. Wenn wir eine solche endliche Folge gemäß der natürlichen Kleiner-Gleich-Ordnung der Indexmenge I als n-Tupel $(a_1, a_2, \dots, a_n)$ schreiben, so haben wir ein Element aus $\bigtimes_{i\in I} A_i$ gemäß Definition 4.8. Diese Zuordnung ist bijektiv.

Wenn alle Mengen $A_i = A$ sind, so schreiben wir statt $\bigtimes_{i\in I} A$ auch A^I. Es ist also beispielsweise

$\mathbb{R}^{\mathbb{N}}$ die Menge aller Folgen mit Werten in $\mathbb{R}$,
$\{0,1\}^A$ die Menge aller $\{0,1\}$-wertigen (binären) Funktionen auf einer Menge A.

Letztere wird manchmal als Schreibweise für die Potenzmenge $\mathcal{P}(A)$ verwendet. (**Quizfrage 6.4:** Inwiefern ist diese Schreibweise gerechtfertigt?)

---

[55] Man spricht von den ZF-Axiomen (ohne das Auswahlaxiom) und von den ZFC-Axiomen (mit Auswahlaxiom).

Das Auswahlaxiom hat eine ganze Menge äquivalenter, teilweise überraschender Charakterisierungen, von denen der nächste Satz (ohne Beweis) einige angibt.

Satz 6.34 (zum Auswahlaxiom äquivalente Aussagen)**.**
Folgende Aussagen sind in der Mengenlehre von Zermelo-Fraenkel äquivalent:

- (i) Es gilt das Auswahlaxiom.
- (ii) Ist I eine beliebige Menge und $(A_i)_{i\in I}$ eine Familie nichtleerer Mengen, so ist das kartesische Produkt $\bigtimes_{i\in I} A_i$ eine nichtleere Menge.
- (iii) Jede Äquivalenzrelation besitzt ein vollständiges Repräsentantensystem.
- (iv) Es sei $f\colon X \to Y$ eine beliebige Funktion. Dann sind äquivalent:
  - (a) f ist surjektiv.
  - (b) Es existiert eine Abbildung $h\colon Y \to X$ mit der Eigenschaft $f \circ h = \mathrm{id}_Y$. Eine solche Abbildung heißt eine **Rechtsinverse** (englisch: right inverse) von f. Sie ist notwendig injektiv.
- (v) Es gilt das Lemma von Zorn 6.35.

Lemma 6.35 (**Lemma von Zorn**[56])**.**
Es sei X mit der Relation $\preccurlyeq$ eine halbgeordnete Menge. Weiter besitze jede totalgeordnete Teilmenge $A \subseteq X$ eine obere Schranke in X.[57] Dann existiert in X ein maximales Element.

Wir werden das Auswahlaxiom in Gestalt des Lemmas von Zorn 6.35 später noch verwenden. Wie angekündigt werden wir darauf hinweisen, wenn ein Resultat von der Hinzunahme des Auswahlaxioms oder der Verwendung eines zu ihm äquivalenten Resultats abhängt.

Die Schwierigkeiten in der intuitiven Erfassung des Auswahlaxioms und des äquivalenten Lemmas von Zorn 6.35 (sowie des ebenfalls äquivalenten Wohlordnungssatzes (englisch: well-ordering theorem), den wir hier nicht angeben) werden in folgendem Zitat gut erfasst, das von dem Mathematiker Jerry Lloyd Bona stammt:

> „The Axiom of Choice is obviously true, the well-ordering theorem is obviously false; and who can tell about Zorn's Lemma?“

Ende der Vorlesung 6

Ende der Woche 3

---

[56] englisch: Zorn's lemma

[57] X kann also nicht die leere Menge sein.

Kapitel 2 Algebraische Strukturen

In diesem Kapitel geht es um die grundlegenden algebraischen Strukturen, Abbildungen zwischen Strukturen und die in ihnen geltenden Rechenregeln.

§ 7 HALBGRUPPEN UND GRUPPEN

Literatur: Beutelspacher, 2014, Kapitel 9, Deiser, 2022b, Kapitel 3.4, Fischer, Springborn, 2020, Kapitel 2.2

Definition 7.1 (Verknüpfung)**.**
Es sei X eine Menge. Eine **(innere) Verknüpfung** (englisch: (inner) operation) auf X ist eine Abbildung $\star\colon X \times X \to X$.

Wir schreiben $a \star b$ statt $\star(a, b)$.

Beispiel 7.2 (Verknüpfung)**.**

(i) Ist X endlich, so können wir eine Verknüpfung auf X mit Hilfe einer **Verknüpfungstafel** oder **Vernüpfungstabelle** (englisch: Cayley table) definieren, zum Beispiel

$$+_2\colon \{0,1\} \times \{0,1\} \to \{0,1\} \quad \text{mit der Verknüpfungstafel}$$

$+_2$	0	1
0	0	1
1	1	0

$$\cdot_2\colon \{0,1\} \times \{0,1\} \to \{0,1\} \quad \text{mit der Verknüpfungstafel}$$

$\cdot_2$	0	1
0	0	0
1	0	1

Quizfrage 7.1: Wo kommen die Definitionen dieser Verknüpfungen her?

Beachte: Die Konvention ist, dass die Zeile das erste Argument (a) und die Spalte das zweite Argument (b) einer Verknüpfung ($a \star b$) angibt.

(ii) Die bekannten Verknüpfungen + und · in $\mathbb{N}$

$$\begin{aligned} +\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad &\text{mit } (x, y) \mapsto x + y \\ \cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad &\text{mit } (x, y) \mapsto x \cdot y \end{aligned}$$

sind Verknüpfungen auf $\mathbb{N}$. Analoges gilt für die Mengen $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.

(*iii*) Es sei X eine Menge und $\mathbb{R}^X = \{f \mid f\colon X \to \mathbb{R}\}$. Dann sind durch die punktweise Addition und die punktweise Multiplikation

$$\begin{aligned} +\colon \mathbb{R}^X \times \mathbb{R}^X \to \mathbb{R}^X \quad &\text{mit } (f,g) \mapsto f+g, \text{definiert durch } (f+g)(x) \coloneqq f(x)+g(x) \\ \cdot\colon \mathbb{R}^X \times \mathbb{R}^X \to \mathbb{R}^X \quad &\text{mit } (f,g) \mapsto f\cdot g, \text{definiert durch } (f\cdot g)(x) \coloneqq f(x)\cdot g(x) \end{aligned}$$

Verknüpfungen auf der Menge der Funktionen $X \to \mathbb{R}$ definiert. (**Quizfrage 7.2:** Was benötigt man als Minimalvoraussetzung, um die Menge Y^X der Funktionen $X \to Y$ mit einer Verknüpfung ausstatten zu können?)

(*iv*) Es sei X eine Menge und $X^X = \{f \mid f\colon X \to X\}$. Dann ist durch die Komposition

$$\circ\colon X^X \times X^X \to X^X \quad \text{mit } (f,g) \mapsto f \circ g, \text{definiert durch } (f\circ g)(x) \coloneqq f(g(x))$$

eine Verknüpfung auf der Menge der Funktionen $X \to X$ definiert.

§ 7.1 HALBGRUPPEN

Definition 7.3 (Halbgruppe).
Eine **Halbgruppe** (englisch: semigroup) $(H,\star)$ ist eine Menge H mit einer **assoziativen Verknüpfung** (englisch: associative operation) $\star$ auf H. Das heißt, es gilt $\star\colon H \times H \to H$ und

$$(x \star y) \star z = x \star (y \star z) \quad \text{für alle } x, y, z \in H. \tag{7.1}$$

Wegen der Assoziativität von $\star$ dürfen wir für die Verknüpfung von drei oder mehr Elementen wie bei $x \star y \star z$ die Klammern weglassen.

Beispiel 7.4 (Halbgruppen).
Beispiele für Halbgruppen sind:

(*i*) $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{N}_0,+)$, $(\mathbb{N}_0,\cdot)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},+)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},+)$, $(\mathbb{C},\cdot)$

(*ii*) $(\{0,1\},+_2)$ und $(\{0,1\},\cdot_2)$ aus Beispiel 7.2

(*iii*) $(\mathbb{R}^X,+)$ und $(\mathbb{R}^X,\cdot)$. Sie erben die Assoziativität von $(\mathbb{R},+)$ und $(\mathbb{R},\cdot)$.

(*iv*) $(X^X,\circ)$. Die Assoziativität von $\circ$ wurde in Lemma 6.16 gezeigt.

(*v*) Ist X eine Menge, dann sind $(\mathcal{P}(X),\cap)$, $(\mathcal{P}(X),\cup)$ und $(\mathcal{P}(X),\triangle)$ Halbgruppen.

(*vi*) Es sei Σ eine nichtleere Menge und $\Sigma^* \coloneqq \bigcup_{n\in\mathbb{N}_0} \Sigma^n$, also die Menge von Tupeln beliebiger Länge. Wir definieren eine Verknüpfung $\circ$ auf Σ^* durch die Konkatenation von Tupeln:

$$(x_1,\ldots,x_n) \circ (y_1,\ldots,y_m) \coloneqq (x_1,\ldots,x_n,y_1,\ldots,y_m).$$

Dann ist $(\Sigma^*,\circ)$ eine Halbgruppe.[1]

Beispiel 7.5 (Gegenbeispiele).
Keine Halbgruppen sind:

---

[1] Diese findet Anwendung bei der Definition formaler Sprachen in der Informatik. Dort ist Σ in der Regel endlich und heißt das **Alphabet** (englisch: alphabet) und Σ^* die **Kleenesche Hülle** (englisch: Kleene star) von Σ. Die Elemente von Σ^* heißen **Worte** über dem Alphabet Σ. Sie werden in der Regel ohne die Klammern notiert, also etwa $ab \circ ba = abba$.

(i) $(\mathbb{N}, -)$, denn $-$ („Minus“) ist keine Verknüpfung auf $\mathbb{N}$, da beispielsweise $1 - 1$ kein Wert in $\mathbb{N}$ zugeordnet ist.

(ii) $(\mathbb{Z}, -)$, denn $-$ („Minus“) ist zwar eine Verknüpfung auf $\mathbb{Z}$, ist aber nicht assoziativ.

(iii) $(\mathbb{N}, \wedge)$ mit $a \wedge b := a^b$. Es ist zwar $\wedge\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ eine Verknüpfung, sie ist aber nicht assoziativ. Beispielsweise ist

$$2 \wedge (3 \wedge 2) = 2^9 \quad \text{aber} \quad (2 \wedge 3) \wedge 2 = 8^2.$$

Definition 7.6 (neutrales Element).
Es sei $(H, \star)$ eine Halbgruppe. Ein Element $e \in H$ heißt **neutrales Element** (englisch: neutral element) von $(H, \star)$, wenn gilt:

$$e \star x = x \star e = x \quad \text{für alle } x \in H. \tag{7.2}$$

Falls in $(H, \star)$ ein neutrales Element existiert, dann heißt $(H, \star)$ auch ein **Monoid** (englisch: monoid).

Lemma 7.7 (neutrale Elemente sind eindeutig).
Es sei $(H, \star)$ eine Halbgruppe. Sind e_1 und e_2 beides neutrale Elemente von $(H, \star)$, dann gilt $e_1 = e_2$.

Beweis. Es gilt

$$e_1 = e_1 \star e_2 = e_2.$$

□

Beispiel 7.8 (Halbgruppen mit und ohne neutrale Elemente).

(i) $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ haben alle das neutrale Element 0.

(ii) $(\mathbb{N}, +)$ besitzt kein neutrales Element.

(iii) $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ haben alle das neutrale Element 1.

(iv) $(\{0, 1\}, +_2)$ aus Beispiel 7.2 besitzt das neutrale Element 0.

(v) $(\{0, 1\}, \cdot_2)$ aus Beispiel 7.2 besitzt das neutrale Element 1.

(vi) $(\mathcal{P}(X), \cap)$ besitzt das neutrale Element X.

(vii) $(\mathcal{P}(X), \cup)$ besitzt das neutrale Element $\emptyset$.

(viii) $(\mathcal{P}(X), \triangle)$ besitzt das neutrale Element $\emptyset$.

(ix) $(\Sigma^*, \circ)$ aus Beispiel 7.4 besitzt das neutrale Element $()$, genannt das **leere Tupel** (englisch: empty tuple) oder das **leere Wort** (englisch: empty word).

Definition 7.9 (Rechts- und Linkstranslation).
Es sei $(H, \star)$ eine Halbgruppe. Für festes $a \in H$ heißt die Abbildung

$$\star_a\colon H \ni x \mapsto x \star a \in H \quad \text{die **Rechtstranslation** (englisch: right translation) mit } a, \tag{7.3a}$$

$$_a\star\colon H \ni x \mapsto a \star x \in H \quad \text{die **Linkstranslation** (englisch: left translation) mit } a. \tag{7.3b}$$

Beispiel 7.10 (Rechts- und Linkstranslation).

(i) In $(\mathbb{R}, +)$ ist die Rechtstranslation mit $a = \sqrt{2}$ gegeben durch die Abbildung $x \mapsto x + \sqrt{2}$. Sie ist wegen der Kommutativität von $+$ identisch zur Linkstranslation mit a.

(*ii*) In $(\mathbb{R}^\mathbb{R}, \circ)$ und $g = x \mapsto 2\,x$ ist die Rechtstranslation mit g gegeben durch

$$\circ_g \colon \mathbb{R}^\mathbb{R} \ni f \mapsto f \circ g \in \mathbb{R}^\mathbb{R}, \quad \text{wobei } f(g(x)) = f(2\,x),$$

während die Linkstranslation mit g gegeben ist durch

$$_g\circ \colon \mathbb{R}^\mathbb{R} \ni f \mapsto g \circ f \in \mathbb{R}^\mathbb{R}, \quad \text{wobei } g(f(x)) = 2\,f(x).$$

Quizfrage 7.3: Wie lässt sich der Begriff **neutrales Element** in einer Halbgruppe mit Hilfe der Begriffe **Rechtstranslation** und **Linkstranslation** ausdrücken?

Definition 7.11 (invertierbare Elemente)**.**
Es sei $(H, \star)$ eine Halbgruppe mit neutralem Element e. Ein Element $a \in H$ heißt **invertierbar** (englisch: invertible) oder eine **Einheit** (englisch: unit) von $(H, \star)$, wenn ein $b \in H$ existiert mit

$$a \star b = b \star a = e. \tag{7.4}$$

In diesem Fall heißt b ein zu a **inverses Element** (englisch: inverse element) oder ein **Inverses** zu a.

Beachte: b ist Inverses zu a genau dann, wenn a Inverses zu b ist!

Lemma 7.12 (inverse Elemente sind eindeutig)**.**
Es sei $(H, \star)$ eine Halbgruppe mit neutralem Element e. Ist $a \in H$ invertierbar und sind b_1 und b_2 beides Inverse zu a, dann gilt $b_1 = b_2$.

Beweis. Es gilt

$$\begin{aligned} b_1 &= b_1 \star e \\ &= b_1 \star (a \star b_2) \\ &= (b_1 \star a) \star b_2 \\ &= e \star b_2 \\ &= b_2. \end{aligned}$$

□

Quizfrage 7.4: Welches Element eines Monoids ist immer invertierbar? Was ist sein Inverses?

Bemerkung 7.13 (abkürzende Schreibweisen)**.**

(*i*) Das inverse Element von a wird oft mit a' bezeichnet.

(*ii*) Bezeichnet man die Verknüpfung $\star$ einer Halbgruppe H als „Addition“ und notiert sie als „+“ o. ä., so nennt man ein eventuell existierendes neutrales Element auch **Nullelement** (englisch: additive identity) „0_H“.

Für $n \in \mathbb{N}$ und $a \in H$ ist $n\,a$ eine Abkürzung für $a + \cdots + a$ (n-mal). (**Quizfrage 7.5:** Warum ist $a + \cdots + a$ auch ohne Setzen von Klammern wohldefiniert?)

Besitzt H das neutrale Element 0_H, so definieren wir auch $0\,a \coloneqq 0_H$.

Ist weiter $a \in H$ invertierbar, so notieren wir die Inverse als $-a$. Dann ist auch $n\,a$ invertierbar für $n \in \mathbb{N}_0$, und wir setzen $(-n)\,a \coloneqq -(n\,a)$. Insbesondere ist $(-1)\,a \coloneqq -a$ und $(-0)\,a = -(0\,a) = -0_H = 0_H$.

Es gilt

$$n\,(m\,a) = (n \cdot m)\,a \quad \text{und} \quad (n+m)\,a = n\,a + m\,a \tag{7.5}$$

für alle $n, m \in \mathbb{N}$ bzw. $n, m \in \mathbb{N}_0$ bzw. $n, m \in \mathbb{Z}$.

Die Bezeichnung $a - b$ steht für $a + (-b)$, vorausgesetzt, b ist invertierbar.

(*iii*) Bezeichnet man die Verknüpfung dagegen als „Multiplikation“ und notiert sie als „$\cdot$“, so nennt man ein eventuell existierendes neutrales Element auch **Einselement** (englisch: multiplicative identity) „1_H“.

Für $n \in \mathbb{N}$ und $a \in H$ ist a^n eine Abkürzung für $a \cdot \cdots \cdot a$ (n-mal).

Besitzt H das neutrale Element 1_H, so definieren wir auch $a^0 \coloneqq 1_H$.

Ist weiter $a \in H$ invertierbar, so notieren wir die Inverse als a^{-1}. Dann ist auch a^n invertierbar für $n \in \mathbb{N}_0$, und wir setzen $a^{-n} = (a^n)^{-1}$. Insbesondere ist $a^{-0} = (a^0)^{-1} = 1_H^{-1} = 1_H$.

Es gilt

$$(a^n)^m = a^{n \cdot m} \quad \text{und} \quad a^{n+m} = a^n \cdot a^m \tag{7.6}$$

für alle $n, m \in \mathbb{N}$ bzw. $n, m \in \mathbb{N}_0$ bzw. $n, m \in \mathbb{Z}$.

(*iv*) Bezeichnet man die Verknüpfung dagegen als „Komposition“ und notiert sie als „$\circ$“, so nennt man ein eventuell existierendes neutrales Element auch **Identität** (englisch: identity) „id“. In diesem Fall verwenden wir ebenfalls die multiplikative Notation, z. B. ist a^n eine Abkürzung für $a \circ \cdots \circ a$ (n-mal).

Beispiel 7.14 (invertierbare Elemente).

(*i*) In $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind alle Elemente invertierbar. Das Inverse von a wird mit $-a$ bezeichnet.

(*ii*) In $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ und $(\mathbb{C}, \cdot)$ sind alle Elemente bis auf 0 invertierbar. Das Inverse von a wird mit a^{-1} oder $1/a$ bezeichnet.

Die Bezeichnung $\frac{a}{b}$ steht für ab^{-1}, vorausgesetzt, b ist invertierbar.

(*iii*) In $(\mathbb{N}_0, +)$ ist nur das Element 0 invertierbar. Die Inverse von 0 ist wiederum 0.

(*iv*) In $(\mathbb{Z}, \cdot)$ sind nur 1 und -1 invertierbar. Beide sind zu sich selbst invers.

(*v*) In $(\{0, 1\}, +_2)$ aus Beispiel 7.2 sind beide Elemente invertierbar. Beide sind zu sich selbst invers.

(*vi*) In $(\{0, 1\}, \cdot_2)$ aus Beispiel 7.2 ist nur das Element 1 invertierbar. Es ist zu sich selbst invers.

(*vii*) In $(X^X, \circ)$ sind genau die bijektiven Funktionen $X \longrightarrow X$ invertierbar.

Quizfrage 7.6: Welches sind die invertierbaren Elemente in den Monoiden $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$ und $(\mathcal{P}(X), \triangle)$?

Ende der Vorlesung 7

§ 7.2 GRUPPEN

Definition 7.15 (Gruppe).
Es sei $(H, \star)$ ein Monoid. $(H, \star)$ heißt **Gruppe** (englisch: group), wenn jedes Element aus H ein Inverses besitzt.

Beachte: Es gilt also: $(G, \star)$ Gruppe $\Rightarrow$ $(G, \star)$ Monoid $\Rightarrow$ $(G, \star)$ Halbgruppe.

Beispiel 7.16 (Gruppen und Gegenbeispiele).

(*i*) Es sei $(H, \star)$ ein Monoid. Dann ist die Teilmenge der invertierbaren Elemente

$$E(H, \star) \coloneqq \{a \in H \mid a \text{ ist invertierbar}\} \tag{7.7}$$

eine Gruppe, genannt die **Einheitengruppe** (englisch: unit group, group of units) $E(H, \star)$ von $(H, \star)$.

(*ii*) $(\mathbb{Z}, +)$ ist eine Gruppe mit neutralem Element 0. Das Inverse zu $a \in \mathbb{Z}$ ist $-a \in \mathbb{Z}$, denn $a + (-a) = 0 = (-a) + a$. Dasselbe gilt für $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$.

(*iii*) $(\mathbb{Z}, \cdot)$ ist ein Monoid, aber keine Gruppe, da nur 1 und -1 invertierbar sind.

(*iv*) $(\mathbb{Q}_{\neq 0}, \cdot)$ ist eine Gruppe mit neutralem Element 1. Das Inverse zu $a \in \mathbb{Q}_{\neq 0}$ ist $1/a \in \mathbb{Q}_{\neq 0}$. Dasselbe gilt für $(\mathbb{R}_{\neq 0}, \cdot)$ und $(\mathbb{C}_{\neq 0}, \cdot)$.

(*v*) Für $m \in \mathbb{N}$ bildet die Menge $\mathbb{Z}_m \coloneqq \{0, 1, \ldots, m-1\}$ mit der Verknüpfung $+_m$ eine abelsche Gruppe (siehe Definition 7.19). Dabei ist $+_m$ die **Addition modulo** m (englisch: addition modulo m) definiert als[2]

$$\begin{aligned} a +_m b &\coloneqq \begin{cases} a + b, & \text{falls } a + b \leqslant m - 1 \\ a + b - m, & \text{falls } a + b \geqslant m \end{cases} \\ &= \text{der natürliche Repräsentant von } a + b \text{ in der Restklasse } [a + b] \text{ modulo } m \\ &= \text{Rest von } a + b \text{ bei ganzzahliger Division durch } m. \end{aligned} \tag{7.8}$$

Diese Gruppe heißt die **additive Gruppe von $\mathbb{Z}$ modulo** m (englisch: additive group of $\mathbb{Z}$ modulo m), geschrieben $(\mathbb{Z}_m, +_m)$.

Den Fall $m = 2$ kennen wir bereits als $(\{0, 1\}, +_2)$ aus Beispiel 7.2.

(*vi*) Für $m \in \mathbb{N}$, $m \geqslant 2$, bildet die Menge $\mathbb{Z}_m$ mit der Verknüpfung $\cdot_m$ ein kommutatives Monoid. Dabei ist $\cdot_m$ die **Multiplikation modulo** m (englisch: multiplication modulo m) definiert als[3]

$$\begin{aligned} a \cdot_m b &\coloneqq \text{der natürliche Repräsentant von } a \cdot b \text{ in der Restklasse } [a \cdot b] \text{ modulo } m \\ &= \text{Rest von } a \cdot b \text{ bei ganzzahliger Division durch } m. \end{aligned} \tag{7.9}$$

Dieses Monoid heißt das **multiplikative Monoid von $\mathbb{Z}$ modulo** m (englisch: multiplicative monoid of $\mathbb{Z}$ modulo m), geschrieben $(\mathbb{Z}_m, \cdot_m)$.

$(\mathbb{Z}_m, \cdot_m)$ ist genau dann eine Gruppe, wenn $m = 1$ ist, also wenn $\mathbb{Z}_m = \{0\}$ gilt. In diesem Fall ist $(\mathbb{Z}_1, \cdot_1)$ isomorph (Definition 8.1) zu $(\mathbb{Z}_1, +_1)$.

Den Fall $m = 2$ kennen wir bereits als $(\{0, 1\}, \cdot_2)$ aus Beispiel 7.2.

---

[2] Beispielsweise ist $3 +_6 5 = 2$, weil $3 + 5 = 8$ ist und $8 \overset{6}{\equiv} 2$ gilt.

[3] Beispielsweise ist $3 \cdot_6 5 = 3$, weil $3 \cdot 5 = 15$ ist und $15 \overset{6}{\equiv} 3$ gilt.

(*vii*) $(\mathbb{R}^X, +)$ ist eine Gruppe.

(*viii*) $(\mathbb{R}^X, \cdot)$ ist keine Gruppe, wenn $X \neq \emptyset$ ist, da die Funktionen, die irgendwo den Wert 0 annehmen, keine invertierbaren Elemente sind. $((\mathbb{R}_{\neq 0})^X, \cdot)$ ist jedoch für jede Menge X eine Gruppe.

(*ix*) $(X^X, \circ)$ ist keine Gruppe, sobald X zwei oder mehr Elemente enthält, denn dann gibt es Funktionen $X \to X$, die nicht bijektiv sind. Wenn X jedoch null- oder einelementig ist, dann ist $(X^X, \circ)$ eine Gruppe.

Quizfrage 7.7: Können Sie die Additions- und Multiplikationstabellen für $\mathbb{Z}_m$ im Fall $m = 5$ und $m = 8$ aufstellen? Haben Sie eine Vermutung, welche Elemente in $(\mathbb{Z}_m, \cdot_m)$ invertierbar sind?

Satz 7.17 (Rechenregeln für Inverse)**.**
Es sei $(G, \star)$ eine Gruppe mit neutralem Element e.

(*i*) Es gelten die **Kürzungsregeln** (englisch: cancellation rules)

$$a \star b_1 = a \star b_2 \quad \Rightarrow \quad b_1 = b_2 \tag{7.10a}$$

$$b_1 \star a = b_2 \star a \quad \Rightarrow \quad b_1 = b_2 \tag{7.10b}$$

für $a, b_1, b_2 \in G$.

(*ii*) In einer Gruppe reicht es für den Nachweis, dass $a \in G$ und $b \in G$ Inverse voneinander sind, aus, diese in einer der beiden Reihenfolgen miteinander zu verknüpfen:

$$a \star b = e \quad \Rightarrow \quad b = a', \tag{7.11a}$$

$$a \star b = e \quad \Rightarrow \quad a = b'. \tag{7.11b}$$

(*iii*) Die Invertierung ist **involutorisch** (englisch: involutory), d. h., für alle $a \in G$ gilt

$$(a')' = a. \tag{7.12}$$

(*iv*) Für das inverse Element zu $a \star b$ für $a, b \in G$ gilt

$$(a \star b)' = b' \star a'. \tag{7.13}$$

Beweis. Aussage (*i*):

$$\begin{aligned}
& a \star b_1 = a \star b_2 && \\
\Rightarrow \quad & a' \star (a \star b_1) = a' \star (a \star b_2) && a' \text{ existiert in der Gruppe } (G, \star) \\
\Rightarrow \quad & (a' \star a) \star b_1 = (a' \star a) \star b_2 && \text{wegen der Assoziativität von } \star \\
\Rightarrow \quad & e \star b_1 = e \star b_2 && \text{da } a' \text{ invers zu } a \text{ ist} \\
\Rightarrow \quad & b_1 = b_2 && \text{wegen der Eigenschaften von } e.
\end{aligned}$$

Die Aussage (7.10b) folgt analog.

Aussage (*ii*): Es gilt $a \star b = e$ und ebenso $a \star a' = e$. Nach (7.10a) muss also $b = a'$ gelten. Weiter gilt $a \star b = e$ und ebenso $b' \star b = e$. Nach (7.10b) muss also $a = b'$ gelten.

Aussage (*iii*): Wir müssen nachweisen, dass a die Inverse zu a' ist. Wegen $a \star a' = a' \star a = e$ ist das aber der Fall.

Aussage (iv): Wir müssen nachweisen, dass $b' \star a'$ die Inverse zu $a \star b$ ist. Wir haben

$$\begin{aligned}(a \star b) \star (b' \star a') &= a \star (b \star b') \star a' && \text{wegen der Assoziativität von } \star \\ &= a \star e \star a' && \text{da } b' \text{ invers zu } b \text{ ist} \\ &= a \star a' && \text{wegen der Eigenschaften von } e \\ &= e && \text{da } a' \text{ invers zu } a \text{ ist.}\end{aligned}$$

☐

Das folgende Lemma gibt mit Hilfe von Rechts- und Linkstranslationen eine notwendige und eine hinreichende Bedingung dafür an, wann eine Halbgruppe sogar eine Gruppe ist.

Lemma 7.18 (Gruppenkriterium mit Rechts- und Linkstranslationen)**.**

(i) Ist $(G, \star)$ eine Gruppe und ist $a \in G$ beliebig, so sind die Rechts- und Linkstranslation $\star_a$ und ${}_a\star$ bijektive Abbildungen $G \to G$.

(ii) Ist $(H, \star)$ eine nichtleere Halbgruppe und gilt für alle $a \in H$, dass die Rechts- und Linkstranslationen $\star_a$ und ${}_a\star$ surjektive Abbildungen sind, dann ist $(H, \star)$ eine Gruppe.

Beweis. Dieser Beweis ist Teil von Hausaufgabe 4.3. ☐

Definition 7.19 (kommutative Halbgruppe, kommutatives Monoid, kommutative Gruppe)**.**
Eine Halbgruppe bzw. ein Monoid bzw. eine Gruppe $(H, \star)$ heißt **kommutativ** (englisch: commutative) oder **abelsch** (englisch: Abelian), wenn

$$x \star y = y \star x \quad \text{für alle } x, y \in H \tag{7.14}$$

gilt.

Beispiel 7.20 (kommutative Halbgruppen und Gruppen)**.**
$(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, +)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$ sind alle kommutativ. Beispielsweise ist $(\mathbb{N}, +)$ eine kommutative Halbgruppe (aber kein Monoid), $(\mathbb{N}_0, +)$ ein kommutatives Monoid (aber keine Gruppe) und $(\mathbb{Z}, +)$ eine kommutative Gruppe.

Weitere Beispiele folgen in der Übung.

§ 7.3 Die symmetrische Gruppe

Definition 7.21 (symmetrische Gruppe)**.**
Es sei X eine nichtleere Menge und $S(X) \coloneqq \{f \colon X \to X \mid f \text{ ist bijektiv}\}$. Dann heißt $(S(X), \circ)$ die **symmetrische Gruppe** (englisch: symmetric group) auf X. Jedes Element von $S(X)$ heißt eine **Permutation** (englisch: permutation) von X.

Ist $X = [\![1, n]\!]$ für $n \in \mathbb{N}$, so schreiben wir auch S_n und sprechen von der **symmetrischen Gruppe vom Grad** n (englisch: symmetric group of degree n). Jedes $\sigma \in S_n$ heißt eine **Permutation** (englisch: permutation) von $[\![1, n]\!]$.

Beachte: Nach Beispiel 7.14 *(vii)* ist $S(X)$ tatsächlich eine Gruppe. Das neutrale Element ist id_X. Wenn X drei oder mehr Elemente enthält, dann ist $(S(X), \circ)$ nicht kommutativ, ansonsten kommutativ.

Eine Permutation $\sigma \in S_n$ können wir in der Form

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

notieren. Die Anzahl der Elemente von S_n für $n \in \mathbb{N}$ ist gleich $n!$ („n Fakultät").

Beispiel 7.22 (symmetrische Gruppe vom Grad 3)**.**
Die symmetrische Gruppe S_3 hat $3! = 6$ Elemente:

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{(Drehungen)},$$
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{(Spiegelungen)}.$$

Sie lassen sich identifizieren mit den Kongruenzabbildungen, die ein gleichseitiges Dreieck mit den Eckpunkten 1, 2 und 3 auf sich selbst überführen. Wegen

$$\sigma_4 \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2$$
$$\sigma_3 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_1$$

ist S_3 wie erwartet tatsächlich nicht kommutativ.

Definition 7.23 (Transposition)**.**
Eine Permutation $\sigma \in S_n$, $n \in \mathbb{N}$, heißt eine **Transposition** (englisch: transposition), wenn es Zahlen $i, j \in [\![1, n]\!]$ mit $i \neq j$ gibt, sodass gilt:

$$\sigma(k) = \begin{cases} j & \text{für } k = i, \\ i & \text{für } k = j, \\ k & \text{sonst.} \end{cases} \tag{7.15}$$

Wir notieren σ dann auch als $\tau(i, j)$.

Eine Transposition vertauscht also genau zwei Elemente von $[\![1, n]\!]$ und lässt den Rest unverändert. Offenbar gilt für jede Transposition

$$\tau^2 = \tau \circ \tau = \mathrm{id}, \quad \text{also } \tau^{-1} = \tau. \tag{7.16}$$

Transpositionen sind also selbstinvers.

In S_1 gibt es keine Transpositionen. (**Quizfrage 7.8:** Wieviele verschiedene Transpositionen gibt es in S_n?)

Satz 7.24 (Darstellung von Permutationen als Komposition von Transpositionen)**.**
Es sei $n \in \mathbb{N}$. Jede Permutation $\sigma \in S_n$ lässt sich als Komposition von $0 \leqslant r \leqslant n - 1$ Transpositionen schreiben.

Beweis. Wir zeigen die Behauptung für $n \geqslant 1$ durch vollständige Induktion. Induktionsanfang: Das einzige Element von

$$S_1 = \left\{\mathrm{id}_{\{1\}}\right\}$$

ist eine Komposition von $r = 0$ Transpositionen.

Induktionsannahme: Die Behauptung sei für $n \in \mathbb{N}$ bereits bewiesen. Induktionsschritt: Wir betrachten eine Permutation $\sigma \in S_{n+1}$.

Fall 1: Falls $\sigma(n+1) = n+1$ gilt, dann gilt für die Einschränkung $\widehat{\sigma}\colon [\![1,n]\!] \to [\![1,n]\!]$ von σ die Eigenschaft $\widehat{\sigma} \in S_n$. Aufgrund der Induktionsannahme besitzt $\widehat{\sigma}$ die Darstellung $\widehat{\sigma} = \tau_1 \circ \cdots \circ \tau_r$ mit $0 \leqslant r \leqslant n-1$ mit Transpositionen τ_i auf S_n. Setzen wir diese Transpositionen durch $n+1 \mapsto n+1$ zu Transpositionen auf S_{n+1} fort, die wir weiterhin mit τ_i bezeichnen, so ergibt sich die Darstellung $\sigma = \tau_1 \circ \cdots \circ \tau_r$.

Fall 2: Falls $\sigma(n+1) = m$ für ein $1 \leqslant m \leqslant n$ gilt, dann betrachte die Transposition $\tau(m, n+1) \in S_{n+1}$. Für $\widetilde{\sigma} \coloneqq \tau(m,n+1) \circ \sigma \in S_{n+1}$ gilt dann $\widetilde{\sigma}(n+1) = n+1$. Aufgrund von **Fall** 1 gilt $\widetilde{\sigma} = \tau_1 \circ \cdots \circ \tau_r$ mit $0 \leqslant r \leqslant n-1$. Schließlich zeigt $\sigma = \tau(m,n+1) \circ \widetilde{\sigma} = \tau(m,n+1) \circ \tau_1 \circ \cdots \circ \tau_r$ die Behauptung.

□

Die Darstellung einer Permutation als Komposition von Transpositionen ist nicht eindeutig. Jedoch ist Anzahl der benötigten Transpositionen entweder immer gerade oder immer ungerade, wie wir gleich beweisen werden (Folgerung 7.30).

Definition 7.25 (Fehlstand, Signum einer Permutation).
Es sei $n \in \mathbb{N}$ und σ eine Permutation in S_n.

(*i*) Ein Indexpaar $(i,j) \in [\![1,n]\!]^2$ heißt ein **Fehlstand** (englisch: inversion) von σ, wenn $i < j$ und $\sigma(i) > \sigma(j)$ gilt.

(*ii*) Die Zahl[4]

$$\operatorname{sgn} \sigma \coloneqq \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i} \tag{7.17}$$

heißt das **Signum** (englisch: sign, lateinisch: signum: Zeichen) von σ.

Beispiel 7.26 (Fehlstand, Signum einer Permutation).
Die Permutation

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

von S_3 hat genau zwei Fehlstände, nämlich $(1,3)$ und $(2,3)$. Es gilt

$$\begin{aligned} \operatorname{sgn} \sigma_1 &= \frac{\sigma(2)-\sigma(1)}{2-1} \frac{\sigma(3)-\sigma(1)}{3-1} \frac{\sigma(3)-\sigma(2)}{3-2} \\ &= \frac{3-2}{2-1} \frac{1-2}{3-1} \frac{1-3}{3-2} \\ &= 1. \end{aligned}$$

Die Permutation

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

---

[4] Definitionsgemäß wird das im Fall $n = 1$ leere Produkt als 1 interpretiert.

hat genau drei Fehlstände, nämlich $(1,2)$, $(1,3)$ und $(2,3)$. Es gilt

$$\begin{aligned}\operatorname{sgn}\sigma_4 &= \frac{\sigma(2)-\sigma(1)}{2-1}\,\frac{\sigma(3)-\sigma(1)}{3-1}\,\frac{\sigma(3)-\sigma(2)}{3-2} \\ &= \frac{2-3}{2-1}\,\frac{1-3}{3-1}\,\frac{1-2}{3-2} \\ &= -1.\end{aligned}$$

Bemerkung 7.27 (zu Definition 7.25)**.**
Da in den Faktoren des Produkts in (7.17) dieselben ganzen Zahlen — abgesehen vom Vorzeichen — jeweils einmal im Zähler und einmal im Nenner vorkommen, ist das Signum einer Permutation immer entweder +1 oder −1. Das Signum einer Permutation gibt die **Parität** (englisch: parity) der Anzahl der Fehlstände an, also ob diese gerade oder ungerade ist, da wir für jedes Indexpaar (i,j) mit $i<j$ den Faktor −1 erhalten, wenn es sich um ein Fehlstand handelt, und ansonsten den Faktor +1. Es gilt also

$$\operatorname{sgn}\sigma = (-1)^{\text{Anzahl der Fehlstände von }\sigma}. \tag{7.18}$$

Dementsprechend nennen wir $\sigma \in S_n$ eine **gerade Permutation** (englisch: even permutation), wenn $\operatorname{sgn}\sigma = 1$ ist und eine **ungerade Permutation** (englisch: odd permutation), wenn $\operatorname{sgn}\sigma = -1$ gilt.

Lemma 7.28 (Signum einer Transposition)**.**
Ist $\tau \in S_n$, $n \in \mathbb{N}$, eine Transposition, so gilt $\operatorname{sgn}\tau = -1$.

Beweis. Wir betrachten eine beliebige Transposition $\tau(i,j)$ in S_n, wobei notwendigerweise $n \geqslant 2$ gilt. O. B. d. A. können wir $i<j$ voraussetzen, also haben wir

$$\tau(i,j) = \begin{pmatrix}1 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots n \\ 1 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots n\end{pmatrix}.$$

$\tau(i,j)$ hat also genau die Fehlstände

$$\begin{aligned}&(i,i+1),\dots,(i,j) &&\text{Anzahl: } j-i \\ &(i+1,j),\dots,(j-1,j) &&\text{Anzahl: } j-i-1.\end{aligned}$$

Daher gilt $\operatorname{sgn}\tau(i,j) = (-1)^{2\,(j-i)-1} = -1$. □

Satz 7.29 (Signum ist verträglich mit Komposition von Permutationen)**.**
Es sei $n \in \mathbb{N}$ und σ_1, σ_2 zwei Permutationen in S_n. Dann gilt

$$\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (\operatorname{sgn}\sigma_1)\cdot(\operatorname{sgn}\sigma_2). \tag{7.19}$$

Beweis. Wir führen den Beweis in drei Schritten.

Schritt 1: Wir beweisen den Satz zunächst für den Spezialfall, dass σ_1 eine Transposition benachbarter Elemente ist, sagen wir $\sigma_1 = \tau(k,k+1)$ für ein $k \in [\![1,n-1]\!]$.

Wenn $\sigma_2^{-1}(k) < \sigma_2^{-1}(k+1)$ gilt, dann ist $(\sigma_2^{-1}(k), \sigma_2^{-1}(k+1))$ kein Fehlstand von σ_2, jedoch ein Fehlstand von $\tau(k,k+1)\circ\sigma_2$. Wenn andererseits $\sigma_2^{-1}(k) > \sigma_2^{-1}(k+1)$ gilt, dann ist $(\sigma_2^{-1}(k), \sigma_2^{-1}(k+1))$ ein Fehlstand von σ_2, aber kein Fehlstand von $\tau(k,k+1)\circ\sigma_2$. Die anderen Fehlstände von σ_2 und $\tau(k,k+1)\circ\sigma_2$ sind dieselben. Daher ist die Anzahl der Fehlstände von σ_2 und von $\tau(k,k+1)\circ\sigma_2$ um 1 verschieden. Damit ist

$$\operatorname{sgn}\bigl(\tau(k,k+1)\circ\sigma_2\bigr) = -\operatorname{sgn}\sigma_2 = \bigl(\operatorname{sgn}\tau(k,k+1)\bigr)\cdot(\operatorname{sgn}\sigma_2)$$

gezeigt.

Schritt 2: Wir beweisen den Satz für den Spezialfall, dass $\tau(k,\ell)$ eine beliebige Transposition ist. Wir haben o. B. d. A. $\ell > k$, daher können wir $\tau(k,\ell)$ in der Form

$$\underbrace{\tau(k,\ell) = \tau(k,k+1) \circ \cdots \circ \tau(\ell-2,\ell-1)}_{} \circ \underbrace{\tau(\ell,\ell-1) \circ \cdots \circ \tau(k+1,k)}_{},$$

also als Komposition von $(2\,(\ell-k)-1)$ Transpositionen benachbarter Elemente schreiben. Aufgrund von **Schritt** 1 und der Assoziativität der Komposition haben wir nun also

$$\begin{aligned}
&\operatorname{sgn}\big(\tau(k,\ell) \circ \sigma_2\big) \\
&\quad = \operatorname{sgn}\big(\tau(k,k+1) \circ \cdots \circ \tau(\ell-2,\ell-1) \circ \tau(\ell,\ell-1) \circ \cdots \circ \tau(k+1,k) \circ \sigma_2\big) \\
&\quad = \big(\operatorname{sgn}\tau(k,k+1)\big) \cdot \operatorname{sgn}\big(\cdots \circ \tau(\ell-2,\ell-1) \circ \tau(\ell,\ell-1) \circ \cdots \circ \tau(k+1,k) \circ \sigma_2\big) \\
&\quad = \cdots \\
&\quad = \big(\operatorname{sgn}\tau(k,k+1)\big) \cdots \big(\operatorname{sgn}\tau(\ell-2,\ell-1)\big)\big(\operatorname{sgn}\tau(\ell,\ell-1)\big) \cdots \big(\operatorname{sgn}\tau(k+1,k)\big)(\operatorname{sgn}\sigma_2) \\
&\quad = \cdots \\
&\quad = \big(\operatorname{sgn}\tau(k,\ell)\big) \cdot (\operatorname{sgn}\sigma_2).
\end{aligned}$$

Schritt 3: Schließlich können wir den allgemeinen Fall zeigen.

Ist $\sigma_1 \in S_n$ eine beliebige Permutation, so können wir sie nach Satz 7.24 als Komposition von Transpositionen $\sigma_1 = \tau_1 \circ \cdots \circ \tau_r$ schreiben.

Unter Benutzung von **Schritt** 2 und der Assoziativität der Komposition folgt nun ähnlich wie im Beweis von **Schritt** 2:

$$\begin{aligned}
&\operatorname{sgn}\big(\sigma_1 \circ \sigma_2\big) \\
&\quad = \operatorname{sgn}\big(\tau_1 \circ \cdots \circ \tau_r \circ \sigma_2\big) \\
&\quad = (\operatorname{sgn}\tau_1) \cdot \operatorname{sgn}\big(\cdots \circ \tau_r \circ \sigma_2\big) \\
&\quad = \cdots \\
&\quad = (\operatorname{sgn}\tau_1) \cdots (\operatorname{sgn}\tau_r)(\operatorname{sgn}\sigma_2) \\
&\quad = \cdots \\
&\quad = \operatorname{sgn}\big(\tau_1 \circ \cdots \circ \tau_r\big) \cdot \operatorname{sgn}(\sigma_2).
\end{aligned}$$

□

Folgerung 7.30 (zu Satz 7.29)**.**
Es sei $n \in \mathbb{N}$ und σ eine Permutation in S_n.

(i) Ist $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ dargestellt als Komposition[5] von $s \in \mathbb{N}_0$ Permutationen $\sigma_i \in S_n$, so gilt $\operatorname{sgn}\sigma = (\operatorname{sgn}\sigma_1) \cdots (\operatorname{sgn}\sigma_s)$.

(ii) Ist insbesondere $\sigma = \tau_1 \circ \cdots \circ \tau_r$ dargestellt als Komposition von $r \in \mathbb{N}$ Transpositionen in S_n, so gilt $\operatorname{sgn}\sigma = (-1)^r$.

(iii) Es gilt $\operatorname{sgn}\operatorname{id} = 1$.

(iv) Es gilt $\operatorname{sgn}\sigma = \operatorname{sgn}\sigma^{-1}$.

---

[5] Vereinbarungsgemäß ist die Verknüpfung von null Permutationen das neutrale Element in S_n, also die identische Abbildung id.

Beweis. Nach Satz 7.29 ist das Signum einer Komposition von zwei Permutationen gleich dem Produkt der Signa der beiden Faktoren. Wie im Beweis von Satz 7.29 können wir die Aussage leicht auf mehr als zwei Faktoren ausdehnen. Die Fälle $s = 0$ und $s = 1$ sind trivial. Das zeigt Aussage (i).

Das Signum einer Transposition ist nach Lemma 7.28 gleich -1. Aussage (ii) folgt damit aus Aussage (i).

Die identische Abbildung ist Produkt von null Transpositionen, also gilt $\operatorname{sgn} \operatorname{id} = (-1)^0 = 1$, also Aussage (iii).

Schließlich gilt

$$1 = \operatorname{sgn} \operatorname{id} = \operatorname{sgn}(\sigma \circ \sigma^{-1}) = (\operatorname{sgn} \sigma) \cdot (\operatorname{sgn} \sigma^{-1}),$$

also $\operatorname{sgn} \sigma^{-1} = 1/\operatorname{sgn} \sigma = \operatorname{sgn} \sigma$, da $\operatorname{sgn} \sigma \in \{\pm 1\}$ ist. Das zeigt Aussage (iv). □

Ende der Vorlesung 8

Ende der Woche 4

§ 7.4 UNTERGRUPPEN

Definition 7.31 (Untergruppe).
Es sei $(G, \star)$ eine Gruppe.

(i) Eine Teilmenge $U \subseteq G$ heißt **abgeschlossen** (englisch: closed) bzgl. $\star$, wenn $\star\colon G \times G \to G$ eingeschränkt werden kann zu $\star_U : U \times U \to U$. In diesem Fall heißt $\star_U$ die auf U **induzierte (innere) Verknüpfung** (englisch: induced operation, lateinisch: inducere: hineinführen).

(ii) Eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq G$ heißt eine **Untergruppe** (englisch: subgroup) von $(G, \star)$, wenn $(U, \star_U)$ selbst wieder eine Gruppe ist. Manchmal schreibt man dies als $(U, \star_U) \leqslant (G, \star)$.

(iii) Eine Untergruppe $(U, \star_U)$ von $(G, \star)$ heißt **echt** (englisch: proper subgroup), wenn $U \subsetneq G$ gilt.

Beachte: Die Assoziativität wird von $\star$ auf $\star_U$ vererbt. Ist $(G, \star)$ abelsch, dann auch $(U, \star)$.

Lemma 7.32 (neutrale und inverse Elemente in einer Untergruppe).
Es sei $(U, \star_U)$ eine Untergruppe der Gruppe $(G, \star)$. Dann ist das neutrale Element e_U von $(U, \star_U)$ gleich dem neutralen Element e von $(G, \star)$. Außerdem gilt für alle $a \in U$, dass das Inverse von a in U übereinstimmt mit dem Inversen von a in G.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 5.1. □

Aufgrund dieser Erkenntnis benötigen wir also keine neue Notation für das neutrale Element und die Inversen in einer Untergruppe. Außerdem schreiben wir ab jetzt einfach $\star$ statt $\star_U$.

Die Prüfung einer Teilmenge $U \subseteq G$ auf die Untergruppen-Eigenschaft lässt sich mit folgendem Kriterium abkürzen:

Satz 7.33 (Untergruppenkriterium).
Es sei $(G, \star)$ eine Gruppe und $U \subseteq G$. Dann sind äquivalent:

(i) $(U, \star)$ ist eine Untergruppe von $(G, \star)$.

(*ii*) $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a \star b' \in U$.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $(U, \star)$ eine Untergruppe von $(G, \star)$. Dann enthält U notwendigerweise das neutrale Element e von $(G, \star)$, da es nach Lemma 7.32 auch das neutrale Element in $(U, \star)$ ist. Für $a, b \in U$ gilt $b' \in U$ nach Lemma 7.32. Da U bzgl. $\star$ abgeschlossen ist, folgt $a \star b' \in U$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*):

Schritt 1: U enthält das neutrale Element e von $(G, \star)$:

Da U nichtleer ist, existiert ein $a \in U$. Mit dem dazu inversen Element a' gilt aufgrund der Voraussetzung $a \star a' \in U$, also $e \in U$ für das neutrale Element e von $(G, \star)$.

Schritt 2: U enthält die Inversen seiner Elemente:

Es sei $a \in U$, dann gilt $a' = e \star a'$, und aufgrund der Voraussetzung liegt $a' \in U$.

Schritt 3: U ist abgeschlossen bzgl. $\star$:

Für $a, b \in U$ liegt auch $b' \in U$, also ist $a \star b = a \star (b')'$ aufgrund der Voraussetzung ebenfalls ein Element von U.

Zusammenfassend haben wir also gezeigt, dass U bzgl. $\star$ abgeschlossen ist (**Schritt 3**), also bildet $(U, \star)$ eine Halbgruppe. Weiter zeigt **Schritt 1**, dass $(U, \star)$ ein Monoid mit dem neutralen Element e von $(G, \star)$ ist. Schließlich zeigt **Schritt 2**, dass alle Elemente von U ein Inverses in U besitzen, also ist $(U, \star)$ eine Gruppe und wegen $U \subseteq$ eine Untergruppe von $(G, \star)$. □

Quizfrage 7.9: Könnte man an Stelle von Aussage (*ii*) in Satz 7.33 äquivalent auch $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a' \star b \in U$ fordern?

Beispiel 7.34 (Untergruppen)**.**

(*i*) Es sei $(G, \star)$ eine Gruppe mit neutralem Element e. Dann sind $(\{e\}, \star)$ und $(G, \star)$ Untergruppen von $(G, \star)$. Diese heißen die **trivialen Untergruppe** (englisch: trivial subgroups).

(*ii*) $(\mathbb{R}_{>0}, \cdot)$ ist eine Untergruppe von $(\mathbb{R}_{\neq 0}, \cdot)$.

(*iii*) Für jede Zahl $m \in \mathbb{N}$ ist $m\mathbb{Z} \coloneqq \{m\,z \mid z \in \mathbb{Z}\}$ mit der Verknüpfung $+$ eine Untergruppe der Gruppe $(\mathbb{Z}, +)$.

(*iv*) Für $n \geqslant 2$ ist

$$\begin{aligned} A_n &\coloneqq \{\sigma \in S_n \mid \sigma \text{ ist Komposition einer geraden Anzahl von Transpositionen}\} \\ &= \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\} \end{aligned} \tag{7.20}$$

eine Untergruppe von S_n, genannt die **alternierende Gruppe** (englisch: alternating group) vom Grad n. Sie hat $\frac{1}{2}n!$ Elemente.

(*v*) In S_3 besteht die alternierende Untergruppe A_3 in der Notation von Beispiel 7.22 gerade aus $\{\sigma_0, \sigma_1, \sigma_2\}$. Diese entsprechen bei Interpretation als Kongruenzabbildungen eines gleichseitigen Dreiecks auf sich selbst gerade den Drehungen.

Quizfrage 7.10: Können Sie eine Gruppe finden, die außer den trivialen Untergruppen keine weiteren Untergruppen besitzt?

Beachte: Die Menge der Untergruppen einer Gruppe $(G, \star)$ sind bzgl. der Eigenschaft „ist Untergruppe von“ partiell geordnet.

Lemma 7.35 (Durchschnitt von Untergruppen)**.**
Es sei $(G, \star)$ eine Gruppe und $(U_i, \star)_{i \in I}$ eine Familie von Untergruppen mit der nichtleeren Indexmenge I. Dann ist auch $\bigcap_{i \in I} U_i$ mit $\star$ eine Untergruppe von $(G, \star)$.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 5.1. □

Definition 7.36 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe, Ordnung eines Elements)**.**
Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

(i) Dann heißt

$$\langle E \rangle := \bigcap \Big\{ U \,\Big|\, (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U \Big\} \tag{7.21}$$

die von E **erzeugte Untergruppe** (englisch: subgroup generated by E) in $(G, \star)$.

Beachte: Bezeichnen wir mit $\mathcal{R}$ die Menge auf rechten Seite von (7.21), über die der Durchschnitt gebildet wird, dann ist $\langle E \rangle$ das Minimum der Menge $\mathcal{R}$ bzgl. der Inklusionshalbordnung und sogar das Minimum der Menge $\mathcal{R}$ bzgl. der Halbordnung „ist Untergruppe von“.

Ist speziell $E = \{a\}$ für ein $a \in G$, so schreiben wir auch $\langle a \rangle$ statt $\langle \{a\} \rangle$ und nennen $\langle a \rangle$ die von a erzeugte **zyklische Untergruppe** (englisch: cyclic subgroup) von $(G, \star)$.

(ii) Gilt $\langle E \rangle = G$, dann heißt E ein **Erzeugendensystem** (englisch: generating set) von $(G, \star)$. Falls ein endliches Erzeugendensystem von G existiert, so heißt G **endlich erzeugt** (englisch: finitely generated).

(iii) Die Gruppe $(G, \star)$ heißt **zyklisch** (englisch: cyclic), wenn es ein $a \in G$ gibt, sodass gilt: $\langle a \rangle = G$. In diesem Fall heißt a ein **Erzeuger** (englisch: generator) von G.

(iv) Ein Element $a \in G$ heißt von **Ordnung** $n \in \mathbb{N}$ (englisch: order), wenn $n \in \mathbb{N}$ die kleinste Zahl ist, für die (in multiplikativer Notation) $a^n = 1$ gilt. Falls kein $n \in \mathbb{N}$ existiert, sodass $a^n = 1$ ist, so heißt a von **unendlicher Ordnung** (englisch: infinite order). Wir schreiben $\operatorname{ord}(a) = n$ bzw. $\operatorname{ord}(a) = \infty$.

Satz 7.37 (Darstellung der erzeugten Untergruppe)**.**
Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$. Dann gilt für die von E erzeugte Untergruppe:

$$\langle E \rangle = \Big\{ a_1 \star \cdots \star a_n \,\Big|\, \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \; (a_i \in E \cup E') \Big\}, \tag{7.22}$$

wobei E' die Menge der Inversen von E bezeichnet. (Im Fall $n = 0$ interpretieren wir wie üblich die Verknüpfung von null Elementen in der rechten Menge als das neutrale Element e. Insbesondere im Fall $E = \emptyset$ ist also $\langle E \rangle = \{e\}$.)

Beweis. Zur Abkürzung bezeichnen wir die Menge auf der rechten Seite von (7.22) mit M. Wir führen den Beweis in zwei Schritten.

Schritt 1: $\langle E \rangle \supseteq M$: Es sei U eine beliebige Untergruppe von G, die im Durchschnitt (7.21) vorkommt. U enthält also E als Teilmenge. Da U eine Untergruppe ist, enthält U auch E'. Da schließlich U abgeschlossen bzgl. $\star$ ist, enthält U auch alle Verknüpfungen endlich vieler Elemente aus $E \cup E'$. Also gilt $U \supseteq M$. Da dies für jede beliebige Untergruppe aus dem Durchschnitt in (7.21) gilt, gilt auch $\langle E \rangle \supseteq M$.

Schritt 2: $\langle E \rangle \subseteq M$: Wir zeigen zunächst, dass M selbst eine Untergruppe von G ist. Dazu überprüfen wir das Untergruppenkriterium (Satz 7.33). Offensichtlich ist $M \neq \emptyset$, denn M enthält mindestens e. Sind $a_1 \star \cdots \star a_n$ und $b_1 \star \cdots \star b_m$ zwei Elemente aus M, so ist auch $(a_1 \star \cdots \star a_n) \star (b_1 \star \cdots \star b_m)'$ ein Element aus M. Also ist M eine Untergruppe von G. Zusätzlich ist klar, dass $E \subseteq M$ gilt. (**Quizfrage 7.11:** Details?) Das heißt, M ist eine derjenigen Untergruppen von G, über die in der Definition von $\langle E \rangle$ der Durchschnitt gebildet wird. Folglich gilt $\langle E \rangle \subseteq M$.

□

Beispiel 7.38 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe, Ordnung eines Elements)**.**

(*i*) In der Gruppe $(\mathbb{Z}, +)$ erzeugt das Element $m \in \mathbb{Z}$ die zyklische Untergruppe $\langle m \rangle = m\,\mathbb{Z}$.

(*ii*) Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch. Sie hat die Erzeuger 1 und -1, es gilt also $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$.

(*iii*) In S_3 gilt mit den Bezeichnungen aus Beispiel 7.22, also

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{(Drehungen)}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{(Spiegelungen)}$$

die Beziehung

$$\sigma_1^2 = \sigma_2 \quad \text{und} \quad \sigma_1^3 = \sigma_0 = \mathrm{id}_{\{1,2,3\}}.$$

Folglich ist

$$\langle \sigma_1 \rangle = \{\sigma_0, \sigma_1, \sigma_2\} = A_3$$

die alternierende Untergruppe, vgl. Beispiel 7.34. Wegen $\sigma_2^2 = \sigma_1$ und $\sigma_2^3 = \sigma_0$ gilt auch $\langle \sigma_2 \rangle = A_3$. Wegen $\sigma_3^2 = \sigma_4^2 = \sigma_5^2 = \mathrm{id}_{\{1,2,3\}}$ gilt $\langle \sigma_3 \rangle = \{\sigma_0, \sigma_3\}$, $\langle \sigma_4 \rangle = \{\sigma_0, \sigma_4\}$ und $\langle \sigma_5 \rangle = \{\sigma_0, \sigma_5\}$. Wollen wir ganz S_3 erzeugen, so müssen wir mindestens zwei Permutationen auswählen. Beispielsweise ist $\{\sigma_1, \sigma_3\}$ (eine Drehung, eine Spiegelung) ein Erzeugendensystem von S_3.

Bemerkung 7.39 (abkürzende Schreibweisen)**.**
Es sei $(H, \star)$ eine Halbgruppe, $a \in H$ sowie $A, B \subseteq H$. Zur Abkürzung vereinbaren wir folgende Schreibweisen:

$$a \star B \coloneqq \{a \star b \,|\, b \in B\}, \tag{7.23a}$$

$$B \star a \coloneqq \{b \star a \,|\, b \in B\}, \tag{7.23b}$$

$$A \star B \coloneqq \{a \star b \,|\, a \in A, \; b \in B\}, \tag{7.23c}$$

$$A' \coloneqq \{a' \,|\, a \in A \text{ ist invertierbar}\}. \tag{7.23d}$$

Wenn A bzw. B die leere Menge ist, ist das Ergebnis in allen obigen Fällen die leere Menge. Mit Hilfe dieser Abkürzungen können wir z. B. das Untergruppenkriterium Satz 7.33 (*ii*) als $U \neq \emptyset$ und $U \star U' \subseteq U$ formulieren.

Ende der Vorlesung 9

Lemma 7.40 (von Untergruppe induzierte Äquivalenzrelationen)**.**
Es sei $(G, \star)$ eine Gruppe und $(U, \star)$ eine Untergruppe. Dann sind durch

$$a \sim^U b \quad \Leftrightarrow \quad b \in a \star U \quad \Leftrightarrow \quad a' \star b \in U \tag{7.24a}$$

$$a \,{}^U\!\!\sim b \quad \Leftrightarrow \quad a \in U \star b \quad \Leftrightarrow \quad a \star b' \in U \tag{7.24b}$$

für $a, b \in G$ zwei Äquivalenzrelationen auf G erklärt.[6] Für die Äquivalenzklassen gilt:

$$[a]_{\sim^U} = a \star U \tag{7.25a}$$

$$[a]_{{}^U\!\sim} = U \star a. \tag{7.25b}$$

Jede der Äquivalenzklassen $[a]_{\sim^U}$ und $[a]_{{}^U\!\sim}$ ist gleichmächtig zu U.

Beweis. Wir zeigen zunächst, dass die beiden angegebenen Bedingungen in (7.24) tatsächlich äquivalent sind. Wir haben

$$\begin{aligned}
& b \in a \star U \\
\Leftrightarrow \quad & \exists c \in U \; (b = a \star c) \\
\Leftrightarrow \quad & \exists c \in U \; (a' \star b = a' \star a \star c) \qquad \text{„}\Leftarrow\text{“ folgt aus der Kürzungsregel (7.10a)} \\
\Leftrightarrow \quad & \exists c \in U \; (a' \star b = c) \\
\Leftrightarrow \quad & a' \star b \in U.
\end{aligned}$$

Wir weisen nun für $a \sim^U b$ die Eigenschaften einer Äquivalenzrelation nach. Das neutrale Element von U und G wird wieder mit e bezeichnet.

Schritt 1: $\sim^U$ ist reflexiv:

Es sei $a \in G$, dann ist $a' \star a = e \in U$, da U Untergruppe ist.

Schritt 2: $\sim^U$ ist symmetrisch:

Es gelte $a \sim^U b$, also $a' \star b \in U$. Dann ist auch das Inverse $(a' \star b)' \in U$, da U Untergruppe ist. Für das Inverse gilt nach Satz 7.17 *(iii)* und *(iv)*:

$$(a' \star b)' = b' \star (a')' = b' \star a \in U.$$

Das heißt aber $b \sim^U a$.

Schritt 3: $\sim^U$ ist transitiv:

Es gelte $a \sim^U b$ und $b \sim^U c$, also $a' \star b \in U$ und $b' \star c \in U$. Aufgrund der Untergruppeneigenschaft von U ist auch $a' \star b \star b' \star c = a' \star c \in U$. Das heißt aber $a \sim^U c$.

Die Darstellung der Äquivalenzklasse (7.25a) folgt sofort aus (7.24a).

Um zu zeigen, dass U und $[a]_{\sim^U} = a \star U$ gleichmächtig sind (Definition 6.23), betrachten wir die Abbildung $U \ni b \mapsto a \star b \in a \star U$. Diese Abbildung ist nach Definition von $a \star U$ surjektiv. Außerdem ist sie injektiv, denn aus $a \star b = a \star c$ folgt mit der Kürzungsregel (7.10a) $b = c$.

Der Beweis für (7.24b) und (7.25b) geht analog. □

---

[6] Für diese Relationen gibt es in der Literatur keine einheitliche Notation.

Die Äquivalenzklasse $[a]_{\sim^U} = a \star U$ heißt auch die **Linksnebenklasse** (englisch: left coset) von U nach a.[7] Weil $\sim^U$ eine Äquivalenzrelation ist, bilden die Linksnebenklassen der Untergruppe U eine Partition der Gruppe G (Satz 5.19). Man notiert die Quotientenmenge als $G \,/ \sim^U$ oder auch als $G \,/\, U$.

Die Äquivalenzklasse $[a]_{{}^U\sim} = U \star a$ heißt auch die **Rechtsnebenklasse** (englisch: right coset) von U nach a. Weil auch ${}^U\sim$ eine Äquivalenzrelation ist, bilden auch die Rechtsnebenklassen der Untergruppe U eine Partition der Gruppe G. Man notiert die Quotientenmenge als $G \,/\, {}^U\sim$ oder auch als $U \backslash G$.

Folgerung 7.41 (zu Lemma 7.40)**.**

Es sei $(G, \star)$ eine abelsche Gruppe und $(U, \star)$ eine Untergruppe. Dann sind die Äquivalenzrelationen $a \sim^U b$ und $a \,{}^U\!\sim b$ identisch. Entsprechend gilt für die Nebenklassen $a \star U = U \star a$ für alle $a \in G$.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 5.3. □

Wann immer $a \sim^U b$ und $a \,{}^U\!\sim b$ identisch sind, schreiben wir auch einfach $a \overset{U}{\sim} b$ und sprechen von **Nebenklassen** (englisch: cosets) $[a]_{\overset{U}{\sim}} = U \star a = a \star U$ von U.

Beispiel 7.42 (Nebenklassen)**.**

(i) In der abelschen Gruppe $(\mathbb{Z}, +)$ erzeugt die Untergruppe $m\mathbb{Z}$ für $m \in \mathbb{N}$ gerade die Kongruenzrelation modulo m, d. h., $\overset{m\mathbb{Z}}{\sim}$ und $\overset{m}{\equiv}$ stimmen überein. Die Nebenklassen von $m\mathbb{Z}$ gilt (auch **Restklassen modulo** m genannt, vgl. Beispiel 5.16)

$$[a] = \{a + n\,m \mid n \in \mathbb{Z}\} = a + m\mathbb{Z}$$

partitionieren die ganzen Zahlen $\mathbb{Z}$ in m gleichmächtige Restklassen, $[0], [1], \ldots, [m-1]$.

(ii) Die Standardkonstruktion einer nicht messbaren Teilmenge von $\mathbb{R}$ (Satz von Vitali) verwendet die Nebenklassen von $\mathbb{Q}$ in der abelschen Gruppe $(\mathbb{R}, +)$, zusammen mit dem Auswahlaxiom.

Aus Lemma 7.40 folgt der folgende wichtige **Satz von Lagrange** (englisch: Lagrange's theorem) der Gruppentheorie:

Satz 7.43 (Satz von Lagrange)**.**

Es sei $(G, \star)$ eine endliche Gruppe und $(U, \star)$ eine Untergruppe. Dann gilt $\#U \mid \#G$, d. h., die Kardinalität der Untergruppe ist ein Teiler der Kardinalität der Gruppe.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 5.3. □

---

[7] Merke: Bei den *Links*nebenklassen $a \star U$ steht der Repräsentant a *links* vom U. Im Relationszeichen $\sim^U$ steht die Tilde $\sim$ ebenfalls links vom U.

§ 8 HOMOMORPHISMEN VON HALBGRUPPEN UND GRUPPEN

Literatur: Beutelspacher, 2014, Kapitel 9.2.3, Fischer, Springborn, 2020, Kapitel 2.2

Homomorphismen (englisch: homomorphisms, altgriechisch: *ομος*: gemeinsam, altgriechisch: *μορφή*: Form) sind die **strukturverträglichen Abbildungen** (englisch: structurally compatible maps) zwischen algebraischen Strukturen. In diesem Abschnitt geht es speziell um Homomorphismen von Halbgruppen und Gruppen.

Definition 8.1 (Halbgruppenhomomorphismus)**.**
Es seien $(H_1, \star)$ und $(H_2, \square)$ zwei Halbgruppen.

(*i*) Eine Abbildung $f\colon H_1 \to H_2$ heißt **strukturverträglich** oder ein **(Halbgruppen-)Homomorphismus** (englisch: semigroup homomorphism) von $(H_1, \star)$ in $(H_2, \square)$, wenn gilt:

$$f(a \star b) = f(a) \mathbin{\square} f(b) \quad \text{für alle } a, b \in H_1. \tag{8.1}$$

(*ii*) Im Fall $(H_1, \star) = (H_2, \square)$ sprechen wir auch von einem **(Halbgruppen-)Endomorphismus** (englisch: semigroup endomorphism, altgriechisch: *ἔνδον*: innen).

(*iii*) Ist $f\colon H_1 \to H_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Halbgruppen-)Isomorphismus** (englisch: semigroup isomorphism, altgriechisch: *ἴσος*: gleich). In diesem Fall nennen wir $(H_1, \star)$ und $(H_2, \square)$ auch zueinander **isomorphe Halbgruppen** (englisch: isomorphic semigroups) und schreiben

$$(H_1, \star) \cong (H_2, \square).$$

(*iv*) Im Fall $(H_1, \star) = (H_2, \square)$ und $f\colon H_1 \to H_2$ bijektiv sprechen wir auch von einem **(Halbgruppen-) Automorphismus** (englisch: semigroup automorphism, altgriechisch: *αυτος*: selbst).[8]

Quizfrage 8.1: Welche Art von Relation ist die Isomorphie auf der Klasse aller Halbgruppen?

Bemerkung 8.2 (Halbgruppenhomomorphismus als kommutatives Diagramm)**.**
Wir können den Sachverhalt, dass $f\colon (H_1, \star) \to (H_2, \square)$ ein Halbgruppenhomomorphismus ist, durch das folgende **kommutative Diagramm** (englisch: commutative diagram) ausdrücken:[9]

$$\begin{tikzcd}
H_1 \times H_1 \arrow[r, "f \times f"] \arrow[d, "\star"] & H_2 \times H_2 \arrow[d, "\square"] \\
H_1 \arrow[r, "f"] & H_2
\end{tikzcd}$$

Ein solches Diagramm heißt **kommutativ** (englisch: commutative diagram), wenn alle Pfade mit demselben Ausgangs- und demselben Endpunkt dasselbe Ergebnis produzieren.

---

[8] Ein Automorphismus ist somit ein bijektiver Endomorphismus oder auch ein Isomorphismus von einer Halbgruppe/Monoid/Gruppe auf sich selbst.

[9] Die Abbildung $f \times f$ ist dabei definiert durch $f \times f\colon H_1 \times H_1 \ni (a, b) \mapsto (f(a), f(b)) \in H_2 \times H_2$.

Wenn $(M_1, \star)$ und $(M_2, \square)$ beides Monoide sind, so können wir ganz analog zu Definition 8.1 die Begriffe **(Monoid-)Homomorphismus**, **-Endomorphismus**, **-Isomorphismus** und **-Automorphismus** (englisch: monoid homomorphism, endomorphism, isomorphism, automorphism) definieren. Zusätzlich zu (8.1) fordert man dabei aber noch, dass für die Einselemente gilt:

$$f(e_1) = e_2. \tag{8.2}$$

Die Monoide $(M_1, \star)$ und $(M_2, \square)$ heißen zueinander **isomorph**, wenn es zwischen ihnen einen Monoidisomorphismus gibt. Wir schreiben dann $(M_1, \star) \cong (M_2, \square)$.

Sind $(G_1, \star)$ und $(G_2, \square)$ beides Gruppen, so ergeben sich die Begriffe **(Gruppen-)Homomorphismus**, **-Endomorphismus**, **-Isomorphismus** und **-Automorphismus** (englisch: group homomorphism, endomorphism, isomorphism, automorphism). Hier wiederum muss man die Bedingung (8.2) nicht separat fordern, denn sie folgt aus (8.1); siehe Lemma 8.5. Die Gruppen $(G_1, \star)$ und $(G_2, \square)$ heißen zueinander **isomorph**, wenn es zwischen ihnen einen Gruppenisomorphismus gibt. Wir schreiben dann $(G_1, \star) \cong (G_2, \square)$.

Bemerkung 8.3 (zu Definition 8.1)**.**
Zwei zueinander isomorphe Halbgruppen/Monoide/Gruppen können und müssen, was ihre algebraischen Eigenschaften als Halbgruppen/Monoide/Gruppen angeht, nicht unterschieden werden.

Beispiel 8.4 (Homomorphismen von Halbgruppen und Gruppen)**.**

(*i*) Es sei Σ eine nichtleere Menge und $(\Sigma^*, \circ)$ die Halbgruppe der Tupel über Σ mit der Konkatenation $\circ$, siehe Beispiel 7.4. Die Abbildung $\#\colon (\Sigma^*, \circ) \to (\mathbb{N}_0, +)$, die die Kardinalität eines Tupels angibt, ist ein Monoidhomomorphismus, denn es gilt

$$\begin{aligned} &\#\big((x_1, \dots, x_n) \circ (y_1, \dots, y_m)\big) = \#(x_1, \dots, x_n) + \#(y_1, \dots, y_m) = n + m \\ \text{und} \quad &\#() = 0. \end{aligned}$$

Genau dann, wenn Σ einelementig ist, ist # auch bijektiv, also ein Monoidisomorphismus.

(*ii*) Für $a > 0$, $a \neq 1$ ist $\log_a\colon (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ ist wegen

$$\log_a(x \cdot y) = \log_a(x) + \log_a(y)$$

ein Gruppenhomomorphismus. Weiter ist $\log_a$ bijektiv, also sogar ein Gruppenisomorphismus.

(*iii*) Zwischen beliebigen Gruppen $(G_1, \star)$ und $(G_2, \square)$ gibt es immer den **trivialen Homomorphismus** (englisch: trivial homomorphism) $f\colon G_1 \ni a \mapsto f(a) := e_2 \in G_2$. Für einige Paare von Gruppen ist das auch der einzig mögliche Homomorphismus.

(*iv*) Für festes $n \in \mathbb{Z}$ ist die Abbildung (vgl. (7.6))

$$G \ni a \mapsto a^n \in G$$

in einer *abelschen* Gruppe $(G, \cdot)$ ein Gruppenendomorphismus.

(*v*) Die sgn-Abbildung ist ein Gruppenhomomorphismus von der symmetrischen Gruppe S_n (für festes $n \in \mathbb{N}$) in die Gruppe $(\{\pm 1\}, \cdot)$, denn es gilt nach Satz 7.29

$$\operatorname{sgn}(\sigma_1 \circ \sigma_2) = (\operatorname{sgn} \sigma_1) \cdot (\operatorname{sgn} \sigma_2).$$

Genau für $n = 2$ ist sgn auch bijektiv, also ein Gruppenisomorphismus.

(*vi*) Die in Beispiel 7.22 vorgenommene „Identifikation“ der symmetrischen Gruppe S_3 mit der Gruppe der Kongruenzabbildungen eines gleichseitigen Dreiecks stellt einen Gruppenisomorphismus dar.

(*vii*) Die Abbildung

$$\mathbb{R} \ni f(x) := \exp(ix) = \cos(x) + i\sin(x) \in \mathbb{C}$$

ist ein Gruppenhomomorphismus $(\mathbb{R}, +) \longrightarrow (\mathbb{C}, \cdot)$, denn es gilt $f(x+y) = f(x) \cdot f(y)$, also

$$\begin{aligned} & \exp(i(x+y)) = \exp(ix) \cdot \exp(iy) \\ \Leftrightarrow \quad & \cos(x+y) + i\sin(x+y) = \big(\cos(x) + i\sin(x)\big) \cdot \big(\cos(y) + i\sin(y)\big). \end{aligned}$$

Nehmen wir den Real- bzw. Imaginärteil der linken und der rechten Seite, so ergeben sich die **Additionstheoreme** für die Winkelsumme

$$\cos(x+y) = \cos(x) \cdot \cos(y) - \sin(x) \cdot \sin(y) \tag{8.3a}$$

$$\sin(x+y) = \sin(x) \cdot \cos(y) + \cos(x) \cdot \sin(y). \tag{8.3b}$$

Lemma 8.5 (Eigenschaften von Gruppenhomomorphismen)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \longrightarrow G_2$ ein Homomorphismus. Dann gilt:

(*i*) $f(e_1) = e_2$.

(*ii*) $(f(a))' = f(a')$.

Beweis. Es gilt

$$\begin{aligned} f(e_1) \,\square\, e_2 &= f(e_1) && \text{da } e_2 \text{ neutrales Element in } (H_2, \square) \text{ ist} \\ &= f(e_1 \star e_1) && \text{da } e_1 \text{ neutrales Element in } (H_1, \star) \text{ ist} \\ &= f(e_1) \,\square\, f(e_1) && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Die Verknüpfung dieses Ausdrucks von links mit dem Inversen von $f(e_1)$, also die Anwendung der Kürzungsregel (7.10a), zeigt $e_2 = f(e_1)$, also Aussage (*i*).

Die Aussage (*ii*) folgt aus

$$\begin{aligned} f(a') \,\square\, f(a) &= f(a' \star a) && \text{da } f \text{ Homomorphismus ist} \\ &= f(e_1) && \text{da } e_1 \text{ neutrales Element in } (H_1, \star) \text{ ist} \\ &= e_2 && \text{wegen Aussage } (i). \end{aligned}$$

Aus (7.11b) folgt nun $f(a') = (f(a))'$. □

Beachte: Gruppenhomomorphismen bilden neutrale Elemente auf neutrale Element ab und inverse Elemente auf inverse Elemente. Das Lemma 8.5 gilt i. A. nicht, wenn $(G_2, \square)$ keine Gruppe, sondern nur ein Monoid ist!

Quizfrage 8.2: Kann $f\colon (\mathbb{Z}, +) \ni n \mapsto n + 1 \in (\mathbb{Z}, +)$ ein Gruppenhomomorphismus sein?

Wir wollen nun Gruppenhomomorphismen genauer studieren.

Definition 8.6 (Bild und Kern eines Gruppenhomomorphismus).
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f \colon G_1 \longrightarrow G_2$ ein Homomorphismus.

(*i*) Das **Bild** (englisch: image) von f ist definiert als

$$\operatorname{Bild}(f) \coloneqq \{f(x) \in G_2 \mid x \in G_1\} = f(G_1). \tag{8.4}$$

(*ii*) Der **Kern** (englisch: kernel) von f ist definiert als

$$\operatorname{Kern}(f) \coloneqq \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\}). \tag{8.5}$$

Lemma 8.7 (Bild und Kern sind Untergruppen).
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f \colon G_1 \longrightarrow G_2$ ein Homomorphismus.

(*i*) $\operatorname{Bild}(f)$ ist eine Untergruppe von $(G_2, \square)$.

(*ii*) $\operatorname{Kern}(f)$ ist eine Untergruppe von $(G_1, \star)$.

Beweis. Aussage (*i*): Wir überprüfen das Untergruppenkriterium (Satz 7.33). Es gilt $e_2 = f(e_1)$ nach Lemma 8.5, also $e_2 \in \operatorname{Bild}(f)$ und $\operatorname{Bild}(f) \neq \emptyset$. Weiter seien a_2, b_2 irgendwelche Elemente in $\operatorname{Bild}(f)$. Wir müssen zeigen: $a_2 \square b_2' \in \operatorname{Bild}(f)$.

Nach Definition von $\operatorname{Bild}(f)$ gibt es $a_1, b_1 \in G_1$ mit $f(a_1) = a_2$ und $f(b_1) = b_2$. Daher ist

$$\begin{aligned} a_2 \square b_2' &= f(a_1) \square (f(b_1))' && \text{nach Voraussetzung} \\ &= f(a_1) \square f(b_1') && \text{nach Lemma 8.5} \\ &= f(a_1 \star b_1') && \text{da } f \text{ Homomorphismus ist} \end{aligned}$$

und damit $a_2 \square b_2' \in \operatorname{Bild}(f)$.

Aussage (*ii*): Wir überprüfen wiederum das Untergruppenkriterium. Es gilt $f(e_1) = e_2$, also $e_1 \in \operatorname{Kern}(f)$ und $\operatorname{Kern}(f) \neq \emptyset$. Weiter seien a, b irgendwelche Elemente in $\operatorname{Kern}(f)$. Wir müssen zeigen: $a \star b' \in \operatorname{Kern}(f)$.

$$\begin{aligned} f(a \star b') &= f(a) \square f(b') && \text{da } f \text{ Homomorphismus ist} \\ &= f(a) \square (f(b))' && \text{nach Lemma 8.5} \\ &= e_2 \square e_2' && \text{da } a, b \in \operatorname{Kern}(f) \text{ liegen} \\ &= e_2 && \text{da } e_2' = e_2 \text{ ist.} \end{aligned}$$

Damit ist $a \star b' \in \operatorname{Kern}(f)$ gezeigt. □

Beispiel 8.8 (Bild und Kern sind Untergruppen).

(*i*) Für die Abbildung $\# \colon (\Sigma^*, \circ) \longrightarrow (\mathbb{N}_0, +)$ aus Beispiel 8.4 gilt:

$$\operatorname{Bild}(\#) = \mathbb{N}_0 \quad \text{und} \quad \operatorname{Kern}(\#) = \{()\},$$

wobei () das leere Tupel kennzeichnet.

(*ii*) Für die Abbildung $\operatorname{sgn}\colon (S_n, \circ) \to (\{\pm 1\}, \cdot)$ aus Beispiel 8.4 gilt im Fall $n \geqslant 2$:

$$\operatorname{Bild}(\operatorname{sgn}) = \{\pm 1\} \quad \text{und} \quad \operatorname{Kern}(\operatorname{sgn}) = A_n,$$

die alternierende Gruppe, vgl. (7.20).

(*iii*) Für die Abbildung $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 (\mathbb{R}_{\neq 0}, \cdot)$ gilt

$$\operatorname{Bild}(f) = \mathbb{R}_{>0} \quad \text{und} \quad \operatorname{Kern}(f) = \{\pm 1\}.$$

Lemma 8.9 (Charakterisierung der Injektivität)**.**

Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann sind äquivalent:

(*i*) f ist injektiv.

(*ii*) $\operatorname{Kern}(f) = \{e_1\}$.

(*iii*) Die einzige Lösung der Gleichung $f(a) = e_2$ ist $a = e_1$.

Beachte: Um die Injektivität einer *beliebigen* Abbildung zu zeigen, müssen wir sicherstellen, dass niemals zwei verschiedene Elemente der Definitionsmenge auf dasselbe Element in der Zielmenge abgebildet werden (Definition 6.10). Wenn wir aber wissen, dass diese Abbildung ein Gruppenhomomorphismus ist, vereinfacht sich dieser Nachweis erheblich. Wir müssen dann nur noch zeigen, dass neben dem neutralen Element e_1 kein weiteres Element auf das neutrale Element e_2 abgebildet wird.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Nach Lemma 8.5 gilt $f(e_1) = e_2$. Ist f injektiv, dann wird kein weiteres Element von G_1 auf e_2 abgebildet, also gilt $\operatorname{Kern}(f) = \{e_1\}$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Umgekehrt gelte $\operatorname{Kern}(f) = \{e_1\}$. Es seien weiter $a, b \in G_1$ mit $f(a) = f(b)$. Dann folgt

$$\begin{aligned} f(a \star b') &= f(a) \square f(b') \\ &= f(a) \square (f(b))' \\ &= f(a) \square (f(a))' \\ &= e_2, \end{aligned}$$

also $a \star b' \in \operatorname{Kern}(f) = \{e_1\}$. Daher muss $a \star b' = e_1$ gelten, also wegen der Eindeutigkeit inverser Elemente $a = b$. Das zeigt die Injektivität von f.

Die Äquivalenz von Aussage (*ii*) und Aussage (*iii*) ist einfach zu sehen, weil $\operatorname{Kern}(f)$ gerade aus den Lösungen der Gleichung $f(a) = e_2$ besteht und nach Lemma 8.5 $f(e_1) = e_2$ gilt. ☐

Ende der Vorlesung 10

Ende der Woche 5

---

§ 8.1 NORMALTEILER

Wir hatten in Lemma 7.40 gesehen, dass jede Untergruppe $(U, \star)$ einer Gruppe $(G, \star)$ zwei Äquivalenzrelationen $\sim^U$ und ${}^U\!\sim$ auf G induziert, deren Äquivalenzklassen durch $a \star U$ bzw. $U \star a$ gegeben und die i. A. verschieden sind.

Definition 8.10 (Normalteiler)**.**
Es sei $(G, \star)$ eine Gruppe. Eine Untergruppe $(N, \star)$ heißt eine **normale Untergruppe** (englisch: normal subgroup) oder **Normalteiler** von $(G, \star)$, wenn gilt:

$$a \star N = N \star a \quad \text{für alle } a \in G. \tag{8.6}$$

Manchmal schreibt man dies als $(N, \star) \trianglelefteq (G, \star)$.

Anders ausgedrückt ist $(N, \star)$ genau dann eine normale Untergruppe, wenn die durch sie induzierten Äquivalenzrelationen $\sim^N$ und ${}^N\!\sim$ (siehe Lemma 7.40) übereinstimmen.

Beachte: Die Relation „ist Normalteiler von“ ist zwar reflexiv und antisymmetrisch, aber im Gegensatz zur Relation „ist Untergruppe von“ i. A. nicht transitiv!

Beispiel 8.11 (Normalteiler)**.**

(i) In jeder Gruppe $(G, \star)$ sind die trivialen Untergruppen $(\{e\}, \star)$ und $(G, \star)$ Normalteiler.

(ii) In einer abelschen Gruppe $(G, \star)$ ist jede Untergruppe ein Normalteiler (Folgerung 7.41).

Lemma 8.12 (Kerne von Gruppenhomomorphismen sind Normalteiler)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt:

(i) Für alle $a \in G_1$ gilt:

$$f^{-1}(\{f(a)\}) = a \star \operatorname{Kern}(f) = \operatorname{Kern}(f) \star a.$$

(ii) $\operatorname{Kern}(f)$ ist ein Normalteiler von G_1.

Beachte: Das Urbild eines Elements in der Bildmenge $f(G_1)$ ist also immer eine Nebenklasse von $\operatorname{Kern}(f)$.

Beweis. Wir zeigen zunächst die Aussage (i) in mehreren Schritten.

Schritt 1: $f^{-1}(\{f(a)\}) \subseteq \operatorname{Kern}(f) \star a$:

Es sei $b \in f^{-1}(\{f(a)\})$, also $f(b) = f(a)$. Dann gilt also

$$\begin{aligned} e_2 &= f(b) \square (f(a))' \\ &= f(b) \square f(a') && \text{nach Lemma 8.5} \\ &= f(b \star a') && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Das heißt aber, dass $b \star a' \in f^{-1}(\{e_2\}) = \operatorname{Kern}(f)$ liegt. Mit anderen Worten, $b \in \operatorname{Kern}(f) \star a$.

Schritt 2: $f^{-1}(\{f(a)\}) \subseteq a \star \mathrm{Kern}(f)$:

Ganz analog zu **Schritt 1** gilt auch

$$\begin{aligned} e_2 &= (f(a))' \square f(b) \\ &= f(a') \square f(b) && \text{nach Lemma 8.5} \\ &= f(a' \star b) && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Das heißt aber $a' \star b \in f^{-1}(\{e_2\}) = \mathrm{Kern}(f)$ und daher $b \in a \star \mathrm{Kern}(f)$.

Schritt 3: $\mathrm{Kern}(f) \star a \subseteq f^{-1}(\{f(a)\})$:

Es sei $b \in \mathrm{Kern}(f)$. Wir müssen $b \star a \in f^{-1}(\{f(a)\})$ zeigen, also $f(b \star a) = f(a)$. Das folgt aber sofort aus

$$\begin{aligned} f(b \star a) &= f(b) \square f(a) && \text{da } f \text{ Homomorphismus ist} \\ &= e_2 \square f(a) && \text{da } b \in \mathrm{Kern}(f) \text{ ist} \\ &= f(a). \end{aligned}$$

Schritt 4: $a \star \mathrm{Kern}(f) \subseteq f^{-1}(\{f(a)\})$:

Es sei $b \in \mathrm{Kern}(f)$. Wir müssen $a \star b \in f^{-1}(\{f(a)\})$ zeigen, also $f(a \star b) = f(a)$. Das folgt aber sofort aus

$$\begin{aligned} f(a \star b) &= f(a) \square f(b) && \text{da } f \text{ Homomorphismus ist} \\ &= f(a) \square e_2 && \text{da } b \in \mathrm{Kern}(f) \text{ ist} \\ &= f(a). \end{aligned}$$

Aus Lemma 8.7 wissen wir, dass $\mathrm{Kern}(f)$ eine Untergruppe von G_1 ist. Aus Aussage (i) folgt $a \star \mathrm{Kern}(f) = \mathrm{Kern}(f) \star a$ für alle $a \in G_1$, also ist $\mathrm{Kern}(f)$ ein Normalteiler von G_1. Das zeigt Aussage (ii).

□

Wenn $(N, \star)$ ein Normalteiler einer Gruppe $(G, \star)$ ist, dann können wir die Faktormenge $G / \overset{N}{\sim} = G / N$ mit einer Gruppenverknüpfung $\tilde{\star}$ ausstatten. Aus der Faktormenge wird damit die **Faktorgruppe** (englisch: factor group) oder **Quotientengruppe** (englisch: quotient group) von G nach N. Man sagt auch: „Aus der Gruppe $(G, \star)$ wird der Normalteiler N ausfaktorisiert.“

Satz 8.13 (Faktorgruppe)**.**
Es sei $(G, \star)$ eine Gruppe mit neutralem Element e und $(N, \star)$ einer ihrer Normalteiler. Dann gilt:

(i) Auf der Faktormenge

$$G / N = \big\{ [a] = a \star N \,\big|\, a \in G \big\}$$

ist $\tilde{\star}$, definiert als

$$[a] \,\tilde{\star}\, [b] := [a \star b], \tag{8.7}$$

eine assoziative Verknüpfung, bzgl. der $(G / N, \tilde{\star})$ eine Gruppe bildet. Das neutrale Element ist $[e] = N$, und für die Inversen gilt $[a]' = [a']$.

(*ii*) Die Abbildung

$$\pi\colon \begin{cases} G \to G \,/\, N \\ a \mapsto [a], \end{cases} \tag{8.8}$$

die jedem Element $a \in G$ seine Nebenklasse $[a]$ zuordnet, ist ein surjektiver Gruppenhomomorphismus. Sie heißt die **kanonische Surjektion** (englisch: canonical surjection) von G auf $G \,/\, N$. Es gilt $\operatorname{Kern}(\pi) = N$.

(*iii*) Wenn $(G, \star)$ abelsch ist, dann auch $(G \,/\, N, \tilde{\star})$.

Beweis. Aussage (*i*): Wir müssen zunächst zeigen, dass $\tilde{\star}$ überhaupt eine Verknüpfung auf $G \,/\, N$ darstellt, also dass (8.7) wohldefiniert ist, da wir dort ja Bezug auf konkrete Repräsentanten $a, b \in G$ nehmen. Es seien also $a_1, a_2, b_1, b_2 \in G$ gegeben, wobei $a_1 \overset{N}{\sim} a_2$ und $b_1 \overset{N}{\sim} b_2$ angenommen wird, d. h., $a_1 \star N = a_2 \star N$ und $b_1 \star N = b_2 \star N$. Dann gilt

$$\begin{aligned}
[a_2] \mathbin{\tilde{\star}} [b_2] &= [a_2 \star b_2] \\
&= (a_2 \star b_2) \star N && \text{nach (7.25)} \\
&= a_2 \star (b_2 \star N) && \text{da } \star \text{ assoziativ ist} \\
&= a_2 \star (N \star b_2) && \text{da } N \text{ Normalteiler ist} \\
&= a_2 \star N \star b_2 && \text{da } \star \text{ assoziativ ist} \\
&= a_2 \star N \star N \star b_2 && \text{da } N \text{ Untergruppe ist} \\
&= (a_2 \star N) \star (N \star b_2) && \text{da } \star \text{ assoziativ ist} \\
&= (a_1 \star N) \star (N \star b_1) && \text{da } a_1 \overset{N}{\sim} a_2 \text{ und } b_1 \overset{N}{\sim} b_2 \\
&= (a_1 \star N) \star (b_1 \star N) && \text{da } N \text{ Normalteiler ist} \\
&= [a_1] \mathbin{\tilde{\star}} [b_1].
\end{aligned}$$

Damit ist $\tilde{\star}$ als Verknüpfung auf $G \,/\, N$ wohldefiniert. Die Assoziativität von $\tilde{\star}$ ergibt sich aus der Assoziativität von $\star$ und der Normalteilereigenschaft, denn es gilt:

$$\begin{aligned}
([a] \mathbin{\tilde{\star}} [b]) \mathbin{\tilde{\star}} [c] &= [a \star b] \mathbin{\tilde{\star}} [c] = (a \star b \star N) \star (c \star N) = (a \star b \star N) \star (N \star c) \\
&= a \star b \star N \star c = a \star b \star c \star N \\
[a] \mathbin{\tilde{\star}} ([b] \mathbin{\tilde{\star}} [c]) &= [a] \mathbin{\tilde{\star}} [b \star c] = (a \star N) \star (b \star c \star N) = (a \star N) \star (N \star b \star c) \\
&= a \star N \star b \star c = a \star b \star c \star N
\end{aligned}$$

Damit haben wir zunächst $(G \,/\, N, \tilde{\star})$ als Halbgruppe bestätigt.

Als nächstes zeigen wir, dass $[e] = e \star N = N$ das neutrale Element von $(G \,/\, N, \tilde{\star})$ ist. Dazu sei $a \in G$ beliebig. Dann gilt gemäß Definition (8.7)

$$[e] \mathbin{\tilde{\star}} [a] = [e \star a] = [a] \quad \text{sowie} \quad [a] \mathbin{\tilde{\star}} [e] = [a \star e] = [a].$$

Also ist $(G \,/\, N, \tilde{\star})$ ein Monoid mit neutralem Element $[e]$.

Nun zeigen wir, dass jedes $[a] \in G \,/\, N$ invertierbar ist mit Inverser $[a]' = [a']$:

$$[a] \mathbin{\tilde{\star}} [a'] = [a \star a'] = [e] \quad \text{sowie} \quad [a'] \mathbin{\tilde{\star}} [a] = [a' \star a] = [e].$$

Aussage (*ii*): Die Eigenschaft, ein Gruppenhomomorphismus zu sein, bedeutet $\pi(a \star b) = \pi(a) \mathbin{\tilde{\star}} \pi(b)$. Nach Definition von π heißt das aber gerade $[a \star b] = [a] \mathbin{\tilde{\star}} [b]$, was gerade die Definition von $\tilde{\star}$ war.

Die Surjektivität von π ist klar, denn ein beliebiges Element $[a]$ von $G\,/\,N$ ist gerade das Bild von a unter π. Es gilt $\text{Kern}(\pi) = \pi^{-1}([e]) = N$.

Aussage (iii): Falls $(G, \star)$ abelsch ist, dann gilt

$$[a] \mathbin{\tilde{\star}} [b] = [a \star b] = [b \star a] = [b] \mathbin{\tilde{\star}} [a],$$

also ist auch $(G\,/\,N, \tilde{\star})$ abelsch. □

Bemerkung 8.14 (Faktorgruppe).
Praktisch können wir die Faktorgruppe $(G\,/\,N, \tilde{\star})$ benutzen, um wie in der Gruppe $(G, \star)$ zu „rechnen", wobei jedoch Elemente a, b in derselben Äquivalenzklasse (für die also $a \star b' \in N$ gilt) nicht mehr unterschieden werden. Die Faktorgruppe $(G\,/\,N, \tilde{\star})$ ist also eine „gröbere Version" der Gruppe $(G, \star)$.

Beispiel 8.15 (Faktorgruppe).

(i) Es sei $(G, \star)$ eine beliebige Gruppe. Dann ist die triviale Untergruppe $\{e\}$ nach Beispiel 8.11 ein Normalteiler. Die zugehörige Faktorgruppe $(G\,/\,\{e\}, \tilde{\star})$ ist isomorph zur Ausgangsgruppe $(G, \star)$ selbst.

(ii) Es sei $(G, \star)$ eine beliebige Gruppe. Dann ist die triviale Untergruppe G nach Beispiel 8.11 ein Normalteiler. Die zugehörige Faktorgruppe $(G\,/\,G, \tilde{\star})$ ist isomorph zu $(\{e\}, \star)$.

(iii) In der abelschen Gruppe $(\mathbb{Z}, +)$ ist jede Untergruppe der Form $m\,\mathbb{Z}$ mit $m \in \mathbb{N}$ ein Normalteiler. Die Elemente der Faktorgruppe $(\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+})$ sind die Nebenklassen von $m\,\mathbb{Z}$, also die Mengen der Form $[a] = a + m\,\mathbb{Z}$, vgl. Beispiel 7.42. Es gilt

$$[a] \mathbin{\tilde{+}} [b] = [a + b].$$

Die Faktorgruppe $(\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+})$ ist isomorph zu einer uns bereits bekannten Gruppe, nämlich zur additiven Gruppe modulo m $(\mathbb{Z}_m, +_m)$ aus Beispiel 7.16 mittels des Isomorphismus $[a] \mapsto$ natürlicher Repräsentant von a in $\mathbb{Z}_m$. Beispielsweise können wir für $m = 5$ wie folgt rechnen:

$$\begin{tikzcd} \text{in } (\mathbb{Z}\,/\,5\,\mathbb{Z}, \tilde{+}) & {[-21]} \arrow[d, mapsto] & \tilde{+} & {[9]} \arrow[d, mapsto] & = & {[-12]} \arrow[d, mapsto] \\ \text{in } (\mathbb{Z}_5, +_5) & 4 & +_5 & 4 & = & 3 \end{tikzcd}$$

(iv) In der abelschen Gruppe $(\mathbb{R}_{\neq 0}, \cdot)$ ist die Untergruppe $(\{\pm 1\}, \cdot)$ ein Normalteiler. Die Elemente der Faktorgruppe sind die Nebenklassen

$$[a] = a \cdot \{\pm 1\} = \{a, -a\}$$

für $a \in \mathbb{R}_{\neq 0}$. Ein mögliches Repräsentantensystem ist $\mathbb{R}_{>0}$.

Bemerkung 8.16 (Normalteiler sind genau die Kerne von Gruppenhomomorphismen).
Es sei $(G_1, \star)$ eine Gruppe. Nach Lemma 8.12 ist für jeden beliebigen Gruppenhomomorphismus $f\colon G_1 \to G_2$ in irgendeine Gruppe $(G_2, \square)$ die Untergruppe $\text{Kern}(f)$ immer ein Normalteiler von $(G_1, \star)$.

Umgekehrt kann man zeigen, dass jeder Normalteiler von dieser Form ist. Also gilt: Jeder Normalteiler von $(G_1, \star)$ ist der Kern eines geeignet gewählten Gruppenhomomorphismus von $(G_1, \star)$ in eine geeignet gewählte Gruppe $(G_2, \square)$.

§ 8.2 HOMOMORPHIESATZ FÜR GRUPPEN

Mit Hilfe des Wissens aus § 8.1 können wir nun die Struktur von Gruppenhomomorphismen analysieren. Der folgende Struktursatz besagt, dass ein Gruppenhomomorphismus $f\colon G_1 \to G_2$ „nebenklassenweise" wirkt. Er bildet also eine gesamte Nebenklasse von $\operatorname{Kern}(f)$ auf ein- und dasselbe Element von G_2 ab und verschiedene Nebenklassen auf verschiedene Elemente. Das geschieht zudem strukturverträglich. Dadurch ist das $\operatorname{Bild}(f)$ eines solchen Gruppenhomomorphismus bereits im Wesentlichen (d. h. bis auf Isomorphie) festgelegt ist durch $(G_1, \star)$ und die Untergruppe $\operatorname{Kern}(f)$.

Satz 8.17 (Homomorphiesatz für Gruppen[10]).
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt

$$G_1 \,/\, \operatorname{Kern}(f) \cong \operatorname{Bild}(f) \tag{8.9a}$$

mit dem Isomorphismus

$$I([a]) \coloneqq f(a) \quad \text{für } [a] = a \star \operatorname{Kern}(f) \in G_1 \,/\, \operatorname{Kern}(f). \tag{8.9b}$$

Beweis. Wir bezeichnen die neutralen Elemente von G_1 und G_2 mit e_1 bzw. e_2.

Wir definieren $I\colon G_1 \,/\, \operatorname{Kern}(f) \to \operatorname{Bild}(f)$ wie in (8.9).

Schritt 1: Wir müssen zunächst zeigen, dass I als Abbildung wohldefiniert ist, da wir in der Definition (8.9b) Bezug auf den konkreten Repräsentanten $a \in G_1$ nehmen.

Es seien dazu $a, b \in G_1$ gegeben mit $a \overset{\operatorname{Kern}(f)}{\sim} b$, d. h., $a \star \operatorname{Kern}(f) = b \star \operatorname{Kern}(f)$. Dann gilt

$$\begin{aligned} f(a \star \operatorname{Kern}(f)) &= f(a) \square f(\operatorname{Kern}(f)) && \text{da } f \text{ Homomorphismus ist} \\ &= \{f(a)\} && \text{da } f(\operatorname{Kern}(f)) = \{e_2\} \text{ gilt} \end{aligned}$$

und analog $f(b \star \operatorname{Kern}(f)) = \{f(b)\}$. Aus $a \star \operatorname{Kern}(f) = b \star \operatorname{Kern}(f)$ folgt also $f(a) = f(b)$. Außerdem ist nach Definition von I klar, dass I in $\operatorname{Bild}(f)$ abbildet. Damit ist I wohldefiniert.

Schritt 2: Als nächstes zeigen wir, dass I ein Homomorphismus ist. In der Tat gilt

$$\begin{aligned} I([a] \mathbin{\tilde\star} [b]) &= I([a \star b]) && \text{nach Definition (8.7) von } \tilde\star \\ &= f(a \star b) && \text{nach Definition von } I \\ &= f(a) \square f(b) && \text{da } f \text{ Homomorphismus ist} \\ &= I([a]) \square I([b]) && \text{nach Definition von } I. \end{aligned}$$

Schritt 3: Es bleibt zu zeigen, dass I surjektiv und injektiv ist. Wenn $a_2 \in \operatorname{Bild}(f)$ ist, dann existiert $a_1 \in G_1$ mit

$$a_2 = f(a_1) = I([a_1]).$$

Das zeigt die Surjektivität von I.

---

[10] englisch: fundamental theorem on group homomorphisms

Für die Injektivität genügt es nach Lemma 8.9 zu zeigen, dass $\operatorname{Kern}(I)$ nur aus dem neutralen Element des Definitionsbereiches $G_1 \,/\, \operatorname{Kern}(f)$ besteht, d. h., aus $[e_1] = \operatorname{Kern}(f)$, vgl. Satz 8.13. Es gilt

$$\begin{aligned}
\operatorname{Kern}(I) &= \big\{[a] \in G_1 \,/\, \operatorname{Kern}(f) \,\big|\, I([a]) = e_2\big\} && \text{nach Definition von } \operatorname{Kern}(I) \\
&= \big\{[a] \in G_1 \,/\, \operatorname{Kern}(f) \,\big|\, f(a) = e_2\big\} && \text{nach Definition von } I \\
&= \big\{[a] \in G_1 \,/\, \operatorname{Kern}(f) \,\big|\, a \in \operatorname{Kern}(f)\big\} && \text{nach Definition von } \operatorname{Kern}(f) \\
&= \big\{a \star \operatorname{Kern}(f) \,\big|\, a \in \operatorname{Kern}(f)\big\} && \text{wegen } [a] = a \star \operatorname{Kern}(f) \text{, siehe (7.25)} \\
&= \big\{\operatorname{Kern}(f)\big\} && \text{denn } \operatorname{Kern}(f) \text{ ist Untergruppe von } (G_2, \square) \\
& && \text{nach Lemma 8.7.}
\end{aligned}$$

□

Beispiel 8.18 (Homomorphiesatz für Gruppen).

(i) Wir betrachten für festes $n \in \mathbb{N}$ die Abbildung $\operatorname{sgn}\colon S_n \to (\{\pm 1\}, \cdot)$, vgl. Beispiele 8.4 und 8.8. Es gilt $\operatorname{Kern}(\operatorname{sgn}) = A_n$. Für $n \geqslant 2$ sind die Elemente der Faktorgruppe $S_n \,/\, \operatorname{Kern}(\operatorname{sgn}) = S_n \,/\, A_n$ die beiden Nebenklassen

$$\begin{aligned}
[\mathrm{id}] &= \mathrm{id} \circ A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} && \text{(gerade Permutationen)}, \\
[\tau] &= \tau \circ A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = -1\} && \text{(ungerade Permutationen)},
\end{aligned}$$

wobei τ irgendeine Transposition in S_n ist. Gemäß Homomorphiesatz 8.17 ist

$$S_n \,/\, \operatorname{Kern}(\operatorname{sgn}) = S_n \,/\, A_n \cong \operatorname{Bild}(\operatorname{sgn}) = \{\pm 1\}.$$

Es werden alle geraden Permutationen $A_n = \operatorname{Kern}(\operatorname{sgn})$ ausfaktorisiert.

Im Fall $n = 1$ gilt $A_1 = S_1$, daher gibt es nur die eine Nebenklasse

$$[\mathrm{id}] = \mathrm{id} \circ S_1 = \{\mathrm{id}\}.$$

Der Homomorphiesatz 8.17 besagt daher in diesem Fall

$$S_1 \,/\, \operatorname{Kern}(\operatorname{sgn}) = S_1 \,/\, A_1 \cong \operatorname{Bild}(\operatorname{sgn}) = \{1\}.$$

(ii) Für die Abbildung $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 \in (\mathbb{R}_{\neq 0}, \cdot)$ aus Beispiel 8.8 und Beispiel 8.15 gilt

$$\mathbb{R}_{\neq 0} \,/\, \operatorname{Kern}(f) = \mathbb{R}_{\neq 0} \,/\, \{\pm 1\} \cong \operatorname{Bild}(f) = \mathbb{R}_{>0}.$$

Durch $\operatorname{Kern}(f) = \{\pm 1\}$ wird das Vorzeichen ausfaktorisiert.

Ende der Vorlesung 11

---

§ 9 RINGE

Literatur: Bosch, 2014, Kapitel 5.1, Fischer, Springborn, 2020, Kapitel 2.3

Ein Ring ist eine algebraische Struktur mit zwei Verknüpfungen, die gewissen Gesetzmäßigkeiten folgen. In Anlehnung an die wichtigen Beispiele $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit den Verknüpfungen „Addition“ und „Multiplikation“ bezeichnen wir diese Verknüpfungen mit $+$ und $\cdot$.

Definition 9.1 (Ring)**.**
Ein **Ring** (englisch: ring) $(R, +, \cdot)$ ist eine Menge R mit zwei (inneren) Verknüpfungen $+$ („Addition“) und $\cdot$ („Multiplikation“), die die folgenden Bedingungen erfüllen:

(i) $(R, +)$ ist eine abelsche Gruppe.

(ii) $(R, \cdot)$ ist eine Halbgruppe.

(iii) Es gelten die **Distributivgesetze** (englisch: distributive laws)

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{9.1a}$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \tag{9.1b}$$

für alle $a, b, c \in R$.

Ein Ring $(R, +, \cdot)$ heißt **kommutativ** (englisch: commutative ring), wenn die Halbgruppe $(R, \cdot)$ kommutativ ist.[11]

Wie üblich vereinbaren wir, dass $\cdot$ stärker bindet als $+$ („Punkt- vor Strichrechnung“), also könnten wir die rechte Seite in (9.1a) auch in der Form $a \cdot b + a \cdot c$ schreiben.

Wie in Gruppen in additiver Notation üblich (Bemerkung 7.13), bezeichnen wir das neutrale Element bzgl. $+$ als **Nullelement** (englisch: additive identity) und schreiben dafür zunächst „0_R“. Außerdem bezeichnen wir das bzgl. $+$ inverse Element von $a \in R$ mit $-a$. Die Bezeichnung $a - b$ steht für $a + (-b)$.

Falls $(R, \cdot)$ ein Monoid ist, so bezeichnen wir das neutrale Element bzgl. $\cdot$ als **Einselement** (englisch: multiplicative identity) und schreiben dafür zunächst „1_R“. In diesem Fall heißt $(R, +, \cdot)$ auch ein **Ring mit Eins** (englisch: ring with unity) oder ein **unitärer Ring** (englisch: unitary ring). Existiert dann zu $a \in R$ bzgl. $\cdot$ ein inverses Element, so bezeichnen wir dieses mit a^{-1}.

Wir vereinbaren, dass $\cdot$ stärker bindet als $+$ und $-$, sodass wir beispielsweise statt $(a \cdot b) + (a \cdot c)$ auch $a \cdot b + a \cdot c$ schreiben können. Außerdem können wir $-a \cdot b$ schreiben statt $-(a \cdot b)$.

Beispiel 9.2 (Ring)**.**

(i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.

(ii) Der **Nullring** (englisch: zero ring) ist der (bis auf Isomorphie) eindeutig bestimmte Ring mit $R = \{0_R\}$ und den dadurch eindeutig bestimmten Verknüpfungen $0_R + 0_R = 0_R$ und $0_R \cdot 0_R = 0_R$. Da 0_R auch das neutrale Element bzgl. $\cdot$ ist, ist der Nullring ein Ring mit Eins, und es gilt $1_R = 0_R$. Er ist der einzige Ring, in dem das Nullelement und das Einselement identisch sind, siehe Lemma 9.3.

(iii) Für $m \in \mathbb{N}$ ist $(m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring. Im Fall $m \neq 1$ besitzt er kein Einselement. Im Fall $m = 1$ ist $1 \in \mathbb{Z}$ das Einselement.

---

[11] In diesem Fall fallen die beiden Distributivgesetze (9.1a) und (9.1b) zusammen. Es reicht also, eines von beiden zu prüfen.

(*iv*) Für $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit Einselement 1, denn nach Beispiel 7.16 ist $(\mathbb{Z}_m, +_m)$ eine abelsche Gruppe und $(\mathbb{Z}_m, \cdot_m)$ ein kommutatives Monoid. Er wird der **Ring von $\mathbb{Z}$ modulo m** (englisch: ring of $\mathbb{Z}$ modulo m) genannt. Im Fall $m = 1$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ der Nullring.

(*v*) Es sei $(G, +)$ eine abelsche Gruppe. Wir definieren

$$\operatorname{End}(G) := \{f\colon G \to G \mid f \text{ ist Endomorphismus}\} \tag{9.2}$$

und statten $\operatorname{End}(G)$ mit den Verknüpfungen

$$\begin{aligned} +\colon \operatorname{End}(G) \times \operatorname{End}(G) &\to \operatorname{End}(G) \quad \text{mit } (f, g) \mapsto f + g, \text{definiert durch } (f + g)(x) := f(x) + g(x) \\ \circ\colon \operatorname{End}(G) \times \operatorname{End}(G) &\to \operatorname{End}(G) \quad \text{mit } (f, g) \mapsto f \circ g, \text{definiert durch } (f \circ g)(x) := f(g(x)) \end{aligned}$$

aus. Dann ist $(\operatorname{End}(G), +, \circ)$ ein Ring mit Einselement id_G, genannt der **Endomorphismenring** (englisch: ring of endomorphisms) der abelschen Gruppe $(G, +)$. Er ist i. A. nicht kommutativ.

Quizfrage 9.1: Warum definieren wir den Endomorphismenring nur für Endomorphismen auf abelschen Gruppen und nicht allgemeiner für Endomorphismen auf beliebigen Gruppen?

Lemma 9.3 (Rechenregeln in Ringen)**.**
Es sei $(R, +, \cdot)$ ein Ring mit dem Nullelement 0_R. Für $a, b \in R$ gilt:

(*i*) $0_R \cdot a = 0_R = a \cdot 0_R$

(*ii*) $a \cdot (-b) = -a \cdot b = (-a) \cdot b$

(*iii*) $(-a) \cdot (-b) = a \cdot b$

(*iv*) Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R, aber nicht der Nullring, dann gilt $1_R \neq 0_R$.

Beachte: Hat R das Einselement 1_R, dann folgt aus Aussage (*ii*) insbesondere $-b = (-1_R) \cdot b$.

Beweis. Aussage (*i*): Es gilt

$$\begin{aligned} 0_R + 0_R \cdot a &= 0_R \cdot a && \text{da } 0_R \text{ das neutrale Element von } (R, +) \text{ ist} \\ &= (0_R + 0_R) \cdot a && \text{da } 0_R \text{ das neutrale Element von } (R, +) \text{ ist} \\ &= 0_R \cdot a + 0_R \cdot a && \text{wegen des Distributivgesetzes (9.1b).} \end{aligned}$$

Die Anwendung der Kürzungsregel (7.10a) in der Gruppe $(R, +)$, also die Addition von $-(0_R \cdot a)$ zu beiden Seiten der Gleichung, zeigt $0_R \cdot a = 0_R \cdot a$. Das zweite Resultat, $a \cdot 0_R = 0_R$, folgt analog.

Aussage (*ii*): Wir zeigen zunächst, dass $a \cdot (-b) = -a \cdot b$ gilt, also dass $a \cdot (-b)$ das Inverse zu $a \cdot b$ in der Gruppe $(R, +)$ ist. Gemäß (7.11) reicht dafür der Nachweis von $a \cdot (-b) + a \cdot b = 0_R$ aus, also der einseitige Test. In der Tat haben wir

$$\begin{aligned} a \cdot (-b) + a \cdot b &= a \cdot (-b + b) && \text{wegen des Distributivgesetzes (9.1a)} \\ &= a \cdot 0_R \\ &= 0_R && \text{nach Aussage } (i). \end{aligned}$$

Die Aussage $(-a) \cdot b = -a \cdot b$ folgt analog.

Aussage (iii): Wir haben

$$\begin{aligned}(-a)\cdot(-b) &= -(a\cdot(-b)) && \text{nach Aussage } (ii)\\ &= -(-a\cdot b) && \text{nach Aussage } (ii)\\ &= a\cdot b && \text{nach (7.12) (doppelte Invertierung).}\end{aligned}$$

Aussage (iv): Es sei R ein Ring mit Einselement 1_R. Wir führen den Beweis durch Kontraposition. Wir nehmen also $1_R = 0_R$ an. Nun sei $a \in R$ beliebig. Dann gilt

$$\begin{aligned}a &= a\cdot 1_R && \text{da } 1_R \text{ das neutrale Element von } (R,\cdot) \text{ ist}\\ &= a\cdot 0_R && \text{da } 1_R = 0_R \text{ angenommen wurde}\\ &= 0_R && \text{nach Aussage } (i).\end{aligned}$$

Der Ring R besteht also nur aus dem Nullelement 0_R, d. h., R ist der Nullring. □

Wir verwenden auch in Ringen $(R,+,\cdot)$ und insbesondere in der Gruppe $(R,+)$ die Schreibweise aus Bemerkung 7.13. Es gilt also für $n \in \mathbb{N}$

$$n\,a \coloneqq a + \cdots + a.$$

Besitzt $(R,+,\cdot)$ das Einselement 1_R, dann gilt nach Distributivgesetz weiter

$$n\,a = a+\cdots+a = 1_R\cdot a+\cdots+1_R\cdot a = (1_R+\cdots+1_R)\ \cdot a = (n\,1_R)\ \cdot a.$$

Weiter ist $(-n)\,a \coloneqq -(n\,a)$ und $0\,a \coloneqq 0_R$.

Definition 9.4 (Charakteristik eines Ringes)**.**
Es sei R ein Ring mit Einselement 1_R.

(i) Wenn es eine Zahl $n \in \mathbb{N}$ gibt, sodass $n\,1_R = 0_R$ gilt, so nennen wir die kleinste solche Zahl

$$\min\{n \in \mathbb{N} \mid n\,1_R = 0_R\}$$

die **Chakteristik** (englisch: characteristic) von R, kurz $\operatorname{char}(R)$.

(ii) Gilt hingegen $n\,1_R \neq 0_R$ für alle $n \in \mathbb{N}$, so sagen wir, R habe die **Chakteristik** (englisch: characteristic) 0 und schreiben $\operatorname{char}(R) = 0$.

Beispiel 9.5 (Charakteristik eines Ringes)**.**

(i) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ haben Charakteristik 0.

(ii) Der Nullring ist (bis auf Isomorphie) der einzige Ring mit Charakteristik 1, also der einzige Ring, in dem $1_R = 0_R$ gilt, vgl. Lemma 9.3.

(iii) Der Ring von $\mathbb{Z}$ modulo m $(\mathbb{Z}_m, +_m, \cdot_m)$ hat Charakteristik $m \in \mathbb{N}$.

(iv) Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ aus dem folgenden Beispiel 9.6 hat ebenfalls Charakteristik $m \in \mathbb{N}$.

Beispiel 9.6 (Restklassenring modulo m).
Es sei $m \in \mathbb{N}$. Wir erinnern an die Faktorgruppe $\mathbb{Z} / m\,\mathbb{Z}$ aus Beispiel 8.15 mit den Elementen $[a] = a + m\,\mathbb{Z}$ (für $a \in \mathbb{Z}$), der kommutativen Verknüpfung $[a] \mathbin{\tilde{+}} [b] = [a+b]$ und dem neutralen Element $[0]$. $(\mathbb{Z} / m\,\mathbb{Z}, \tilde{+})$ bildet eine kommutative Gruppe.

Weiter bildet $(\mathbb{Z} / m\,\mathbb{Z}, \tilde{\cdot})$ mit der Verknüpfung $[a] \mathbin{\tilde{\cdot}} [b] = [a \cdot b]$ ein kommutatives Monoid mit dem neutralen Element $[1]$, siehe auch Hausaufgabe 6.1.

Schließlich können wir zeigen, dass die Distributivgesetze (9.1a) und (9.1b) gelten, denn:

$$\begin{aligned} [a] \mathbin{\tilde{\cdot}} ([b] \mathbin{\tilde{+}} [c]) &= [a] \mathbin{\tilde{\cdot}} [b+c] && \text{nach Definition von } \tilde{+} \\ &= [a \cdot (b+c)] && \text{nach Definition von } \tilde{\cdot} \\ &= [a \cdot b + a \cdot c] && \text{nach Distributivgesetz in } \mathbb{Z} \\ &= [a \cdot b] \mathbin{\tilde{+}} [a \cdot c] && \text{nach Definition von } \tilde{+} \\ &= [a] \mathbin{\tilde{\cdot}} [b] \mathbin{\tilde{+}} [a] \mathbin{\tilde{\cdot}} [c] && \text{nach Definition von } \tilde{\cdot}. \end{aligned}$$

Das zweite Distributivgesetz (9.1b) ist wegen der Kommutativität der Halbgruppe $(\mathbb{Z} / m\,\mathbb{Z}, \tilde{\cdot})$ automatisch erfüllt. Daher bildet $(\mathbb{Z} / m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ einen kommutativen Ring mit Eins, genannt der **Restklassenring modulo m** ~~oder **Ring von $\mathbb{Z}$ modulo m** (englisch: ring of $\mathbb{Z}$ modulo m)~~. Im Fall $m = 1$ ist $(\mathbb{Z} / m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ der Nullring.

Die Verknüpfungstafeln für $\mathbb{Z} / m\,\mathbb{Z}$ für $m \in \{1, 2, 3, 4\}$ lauten:

$\tilde{+}$	$[0]$
$[0]$	$[0]$

$\tilde{\cdot}$	$[0]$
$[0]$	$[0]$

$\tilde{+}$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\tilde{\cdot}$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

$\tilde{+}$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\tilde{\cdot}$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

$\tilde{+}$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\tilde{\cdot}$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Die für $m = 4$ in $\mathbb{Z} / m\,\mathbb{Z}$ erstmalig auftretende Situation $[2] \mathbin{\tilde{\cdot}} [2] = [0]$ wollen wir benennen:

Definition 9.7 (Nullteiler, Nullteilerfreiheit, Integritätsring).
Es sei $(R, +, \cdot)$ ein Ring.

(i) Das Element $a \in R$ heißt ein **Linksnullteiler** (englisch: left zero divisor), wenn es ein $b \in R \setminus \{0_R\}$ gibt, sodass $a \cdot b = 0_R$ gilt. Das Element b heißt ein **Rechtsnullteiler** (englisch: right zero divisor), wenn es ein $a \in R \setminus \{0_R\}$ gibt, sodass $a \cdot b = 0_R$ gilt.

(ii) Der Ring $(R, +, \cdot)$ heißt **nullteilerfrei** (englisch: ring with no zero divisors), wenn es außer dem Nullelement 0_R keine weiteren Links- oder Rechtsnullteiler gibt, wenn also gilt:

$$\forall a, b \in R \; (a \cdot b = 0_R \implies a = 0_R \text{ oder } b = 0_R). \tag{9.3}$$

(Anders gesagt: Aus $a \neq 0_R$ und $b \neq 0_R$ folgt $a \cdot b \neq 0_R$.)

(iii) Ein Ring $(R, +, \cdot)$ heißt **Integritätsring** oder **Integritätsbereich** (englisch: integral domain), wenn gilt: $(R, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit Eins ungleich dem Nullring.

Quizfrage 9.2: Ist der Nullring nullteilerfrei?

Beispiel 9.8 (Integritätsringe und Gegenbeispiele)**.**

(i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Integritätsringe.

(ii) Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist ein Integritätsring genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist; siehe Satz 9.9.

(iii) Es sei X eine Menge, $(R, +, \cdot)$ ein Ring und $R^X = \{f \mid f \colon X \to R\}$. Definieren wir ähnlich wie in Beispiel 7.2 die Verknüpfungen $+$ und $\cdot$ auf R^X als

$$\begin{aligned} +\colon R^X \times R^X &\to R^X \quad \text{mit } (f, g) \mapsto f + g, \text{definiert durch } (f + g)(x) \coloneqq f(x) + g(x), \\ \cdot\colon R^X \times R^X &\to R^X \quad \text{mit } (f, g) \mapsto f \cdot g, \text{definiert durch } (f \cdot g)(x) \coloneqq f(x) \cdot g(x), \end{aligned}$$

dann ist $(R^X, +, \cdot)$ ein Ring. $(R^X, +, \cdot)$ ist kommutativ genau dann, wenn $(R, +, \cdot)$ kommutativ ist. $(R^X, +, \cdot)$ besitzt ein Einselement genau dann, $(R, +, \cdot)$ ein Einselement besitzt.

Beachte: Wenn $(R, +, \cdot)$ nicht der Nullring ist, dann ist $(R^X, +, \cdot)$ nicht nullteilerfrei, sobald X zwei oder mehr Elemente enthält!

Quizfrage 9.3: Wie sieht man das?

Satz 9.9 (Nullteilerfreiheit des Restklassenringes)**.**
Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist ein Integritätsring genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist.

Beweis. Für $m = 1$ ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ der Nullring und damit kein Integritätsring. Wir betrachten also im Weiteren nur den Fall $m \geqslant 2$, für den $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ein kommutativer Ring ungleich dem Nullring und mit dem Einselement $[1]$ ist. Die Frage, ob dieser Ring ein Integritätsring ist, hängt also genau an der Nullteilerfreiheit. Das Nullelement von $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist $[0]$.

Es sei $m \in \mathbb{N}$, $m \geqslant 4$, *keine* Primzahl, lässt sich also schreiben als $m = a \cdot b$ für Zahlen $a, b \in [\![2, m-1]\!]$. Die zugehörigen Restklassen $[a]$ und $[b]$ sind ungleich $[0]$ (**Quizfrage 9.4:** Warum?) Es gilt

$$\begin{aligned} [0] &= [m] && \text{da } 0 \overset{m}{\equiv} m \\ &= [a \cdot b] && \text{da } m = a \cdot b \\ &= [a] \mathbin{\tilde{\cdot}} [b] && \text{nach Definition von } \tilde{\cdot}. \end{aligned}$$

Damit ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ *nicht* nullteilerfrei.

Es sei nun umgekehrt $m \in \mathbb{N}$, $m \geqslant 2$, eine Primzahl. Wir nehmen an, $[a]$ und $[b]$ seien Elemente aus $\mathbb{Z}/m\mathbb{Z}$ mit $[0] = [a] \mathbin{\tilde{\cdot}} [b] = [a \cdot b]$. Das heißt aber, da 0 und $a \cdot b$ in derselben Restklasse modulo m liegen, dass $a \cdot b = m\,z$ gilt für irgendein $z \in \mathbb{Z}$. Da m eine Primzahl ist, kommt m in der (vorzeichenbehafteten) Primfaktorzerlegung von $a \cdot b$ vor. Das heißt, dass a oder b den Primfaktor m enthält, also gilt $m \mid a$ oder $m \mid b$, woraus $[a] = [0]$ oder $[b] = [0]$ folgt. Damit ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ nullteilerfrei. ☐

Definition 9.10 (Unterring, vgl. Definition 7.31 einer Untergruppe)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(i) Eine Teilmenge $U \subseteq R$ heißt ein **Unterring** (englisch: subring) von $(R, +, \cdot)$, wenn U bzgl. $+$ und bzgl. $\cdot$ abgeschlossen ist und wenn $(U, +, \cdot)$ selbst wieder ein Ring ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, +)$ eine Untergruppe von $(R, +)$ ist und wenn $(U, \cdot)$ bzgl. $\cdot$ abgeschlossen ist.

(ii) Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R, dann fordern wir für einen **Unterring mit Eins** (englisch: subring with unity) $(U, +, \cdot)$ zusätzlich zu Eigenschaft (i), dass $1_R \in U$ liegt.[12]

Beachte: Es reicht nicht aus, zu fordern, dass $(U, \cdot)$ *irgendein* neutrales Element besitzt.

(iii) Ein Unterring $(U, +, \cdot)$ von $(R, +, \cdot)$ heißt **echt** (englisch: proper subring), wenn $U \subsetneq R$ gilt.

Definition 9.11 (Ringhomomorphismus, vgl. Definition 8.1 eines Halbgruppenhomomorphismus)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ zwei Ringe.

(i) Eine Abbildung $f \colon R_1 \to R_2$ heißt **strukturverträglich** oder ein **(Ring-)Homomorphismus** (englisch: ring homomorphism) von $(R_1, +_1, \cdot_1)$ in $(R_2, +_2, \cdot_2)$, wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in R_1, \tag{9.4a}$$

$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in R_1. \tag{9.4b}$$

Besitzen beide Ringe ein Einselement 1_{R_1} bzw. 1_{R_2} und fordern wir zusätzlich

$$f(1_{R_1}) = 1_{R_2} \tag{9.4c}$$

dann nennen wir f genauer einen **Homomorphismus von Ringen mit Eins** (englisch: homomorphism of rings with unity).

(ii) Wie in Definition 8.1 sprechen wir im Fall $(R_1, +_1, \cdot_1) = (R_2, +_2, \cdot_2)$ von einem **(Ring-)Endomorphismus** (englisch: ring endomorphism) bzw. von einem **Endomorphismus eines Ringes mit Eins** (englisch: endomorphism of a ring with unity).

(iii) Ist $f \colon R_1 \to R_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Ring-)Isomorphismus** (englisch: ring isomorphism) bzw. von einem **Isomorphismus von Ringen mit Eins** (englisch: endomorphism of a ring with unity). In diesem Fall nennen wir $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ auch zueinander **isomorphe Ringe** (englisch: isomorphic rings) bzw. zueinander **isomorphe Ringe mit Eins** (englisch: isomorphic rings with unity) und schreiben

$$(R_1, +_1, \cdot_1) \cong (R_2, +_2, \cdot_2).$$

(iv) Im Fall $(R_1, +_1, \cdot_1) = (R_2, +_2, \cdot_2)$ und $f \colon R_1 \to R_2$ bijektiv sprechen wir auch von einem **(Ring-) Automorphismus** (englisch: ring automorphism) bzw. von einem **Automorphismus eines Ringes mit Eins** (englisch: automorphism of a ring with unity).

---

[12] Dadurch ist der Unterring $(U, +, \cdot)$ dann natürlich selbst wieder ein Ring mit dem Einselement 1_R.

(v) Das **Bild** (englisch: image) und der **Kern** eines Ringhomomorphismus $f\colon R_1 \to R_2$ sind definiert als

$$\operatorname{Bild}(f) \coloneqq \{f(x) \in R_2 \,|\, x \in R_1\} = f(R_1), \tag{9.5}$$

$$\operatorname{Kern}(f) \coloneqq \{x \in R_1 \,|\, f(x) = 0_{R_2}\} = f^{-1}(\{0_{R_2}\}). \tag{9.6}$$

Die Beziehung (9.4a) besagt, dass $f\colon (R_1, +_1) \to (R_2, +_2)$ ein Gruppenhomomorphismus ist. Aus Lemma 8.5 folgt damit für die Nullelemente 0_{R_1} bzw. 0_{R_2} notwendigerweise

$$f(0_{R_1}) = 0_{R_2}. \tag{9.7}$$

Weiter bedeutet (9.4b), dass $f\colon (R_1, \cdot_1) \to (R_2, \cdot_2)$ ein Halbgruppenhomomorphismus ist. (9.4b) und (9.4c) zusammen bedeuten, dass $f\colon (R_1, \cdot_1) \to (R_2, \cdot_2)$ ein Monoidhomomorphismus ist.

Beispiel 9.12 (Ringhomomorphismen)**.**

(i) Die Abbildung

$$f\colon (\mathbb{Z}, +, \cdot) \ni a \mapsto [a] = a + m\,\mathbb{Z} \in (\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$$

ist ein surjektiver Ringhomomorphismus zwischen zwei kommutativen Ringen mit Eins, denn: f ist als kanonische Surjektion der Faktorgruppe nach Satz 8.13 und Beispiel 8.15 ein surjektiver Gruppenhomomorphismus $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+})$, und außerdem ist $f\colon (\mathbb{Z}, \cdot) \to (\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{\cdot})$ ein Monoidhomomorphismus, siehe Beispiel 9.6 und Hausaufgabe 6.1.

Es gilt

$$\operatorname{Bild}(f) = \mathbb{Z}\,/\,m\,\mathbb{Z},$$

$$\operatorname{Kern}(f) = f^{-1}([0]) = m\,\mathbb{Z}.$$

(ii) Für $m \in \mathbb{N}$ ist die Abbildung

$$f\colon (\mathbb{Z}_m, +_m, \cdot_m) \ni a \mapsto [a] = a + m\,\mathbb{Z} \in (\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$$

ein Ringisomorphismus zwischen dem Ring von $\mathbb{Z}$ modulo m (Beispiel 9.2) und dem Restklassenring modulo m (Beispiel 9.6), beides kommutative Ringe mit Eins, denn: f ist nach Beispiel 8.15 ein Gruppenisomorphismus $f\colon (\mathbb{Z}_m, +_m) \to (\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+})$, und außerdem ist $f\colon (\mathbb{Z}_m, \cdot_m) \to (\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{\cdot})$ nach Hausaufgabe 6.1 ein Monoidisomorphismus.

Es gilt

$$\operatorname{Bild}(f) = \mathbb{Z}\,/\,m\,\mathbb{Z},$$

$$\operatorname{Kern}(f) = f^{-1}([0]) = \{0\}.$$

Ende der Vorlesung 12

Ende der Woche 6

§ 10 KÖRPER

Literatur: Beutelspacher, 2014, Kapitel 2, Bosch, 2014, Kapitel 1.3, Fischer, Springborn, 2020, Kapitel 2.3, Deiser, 2022b, Kapitel 2.2

Ein Körper ist — wie ein Ring — eine algebraische Struktur mit zwei Verknüpfungen. In Anlehnung an die wichtigen Beispiele $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit den Verknüpfungen „Addition“ und „Multiplikation“ bezeichnen wir diese Verknüpfungen wieder mit $+$ und $\cdot$.

Definition 10.1 (Körper)**.**
Ein **Körper** (englisch: field) $(K, +, \cdot)$ ist eine Menge K mit zwei (inneren) Verknüpfungen $+$ („Addition“) und $\cdot$ („Multiplikation“), die die folgenden Bedingungen erfüllen:

(*i*) $(K, +)$ ist eine abelsche Gruppe. Das Nullelement bezeichnen wir mit 0_K.

(*ii*) $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe. Das Einselement bezeichnen wir mit 1_K.

(*iii*) Es gelten die **Distributivgesetze** (englisch: distributive laws)

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{10.1a}$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \tag{10.1b}$$

für alle $a, b, c \in K$.[13]

Oft wird $K \setminus \{0_K\}$ als K^* oder als $K^\times$ abgekürzt. Wir verwenden diese Bezeichnungen jedoch hier nicht.

Beispiel 10.2 (Körper und Gegenbeispiele)**.**

(*i*) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper mit dem Nullelement 0 und dem Einselement 1.

(*ii*) $(\mathbb{Z}_2, +_2, \cdot_2)$ aus Beispiel 7.16 mit den Verknüpfungstafeln aus Beispiel 7.2 ist ein Körper mit dem Nullelement 0 und dem Einselement 1.

(*iii*) Der Restklassenring $(\mathbb{Z} / 4\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ mit dem Nullelement $[0]$ und dem Einselement $[1]$ aus Beispiel 9.6 ist *kein* Körper, da $[2]$ nicht das Nullelement ist und $[2] \mathbin{\tilde{\cdot}} [a] \neq [1]$ für alle $a \in \mathbb{Z}$ gilt und damit $[2]$ kein multiplikatives Inverses besitzt.

(*iv*) Es sei X eine Menge. Für die bisher besprochenen algebraischen Strukturen S (Halbgruppe, Monoid, Gruppe, Ring) galt, dass S^X, ausgestattet punktweise mit der oder den Verknüpfung(en) von S, die algebraische Struktur erbt, also ebenfalls Halbgruppe, Monoid, Gruppe oder Ring ist.

Wenn jedoch $(K, +, \cdot)$ ein Körper ist, dann ist $(K^X, +, \cdot)$ i. A. *kein* Körper, sondern nur ein kommutativer Ring mit Eins. (**Quizfrage 10.1:** Woran liegt das?)

Lemma 10.3 (Eigenschaften eines Körpers)**.**
Es sei $(K, +, \cdot)$ ein Körper mit dem Nullelement 0_K und dem Einselement 1_K. Dann gilt:

(*i*) $0_K \neq 1_K$. Ein Körper hat also mindestens zwei Elemente.

(*ii*) $(K, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit dem Einselement 1_K ungleich dem Nullring, also ein Integritätsring.

---

[13] Wie bereits in kommutativen Ringen fallen die beiden Distributivgesetze (10.1a) und (10.1b) zusammen. Es reicht also, eines von beiden zu prüfen.

(*iii*) Es gelten die **Kürzungsregeln** (englisch: cancellation rules)

$$a \cdot b_1 = a \cdot b_2 \quad \Rightarrow \quad b_1 = b_2 \tag{10.2a}$$
$$b_1 \cdot a = b_2 \cdot a \quad \Rightarrow \quad b_1 = b_2 \tag{10.2b}$$

für $a, b_1, b_2 \in K$ mit $a \neq 0_K$.

Beweis. Aussage (*i*): Nach Definition 10.1 ist $K \setminus \{0_K\}$ eine Gruppe mit dem Einselement 1_K, also muss $0_K \neq 1_K$ gelten.

Aussage (*ii*): Nach Definition 10.1 ist $(K, +)$ eine abelsche Gruppe mit dem Nullelement 0_K. Wenn wir zeigen können, dass $(K, \cdot)$ ein abelsches Monoid mit dem Einselement 1_K ist, dann ist $(K, +, \cdot)$ per Definition 9.1 ein abelscher Ring mit dem Einselement 1_K. Dieser ist nach Aussage (*i*) nicht der Nullring. Wenn wir anschließend zeigen können, dass $(K, +, \cdot)$ nullteilerfrei ist, dann ist Aussage (*ii*) gezeigt.

Schritt 1: Wir zeigen: $0_K \cdot a = 0_K = a \cdot 0_K$ für alle $a \in K$.

Dieses Ergebnis folgt wie im Beweis von Lemma 9.3, Aussage (*i*): $0_K + 0_K \cdot a = 0_K \cdot a = (0_K + 0_K) \cdot a = 0_K \cdot a + 0_K \cdot a$ und daher $0_K \cdot a = 0_K$. Analog können wir $a \cdot 0_K = 0_K$ zeigen.

Schritt 2: Wir zeigen: $\cdot$ ist eine *assoziative* Verknüpfung auf ganz K:

Per Definition ist $\cdot$ eine Verknüpfung auf ganz K. Die Assoziativität $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ist klar, wenn nur Elemente $a, b, c \in K \setminus \{0_K\}$ verknüpft werden, da $(K \setminus \{0_K\}, \cdot)$ eine Gruppe ist. Wenn eines oder mehrere Elemente a, b, c aber das Nullelement 0_K sind, dann gilt wegen **Schritt** 1, dass sowohl $a \cdot (b \cdot c)$ als auch $(a \cdot b) \cdot c$ gleich 0_K sind. Die Assoziativität von $\cdot$ gilt also auf ganz K.

Schritt 3: Wir zeigen: $\cdot$ ist eine *kommutative* Verknüpfung auf ganz K:

Die Kommutativität $a \cdot b = b \cdot a$ ist klar, wenn nur Elemente $a, b \in K \setminus \{0_K\}$ verknüpft werden, da $(K \setminus \{0_K\}, \cdot)$ eine kommutative Gruppe ist. Wenn eines oder mehrere Element a, b aber das Nullelement 0_K sind, dann gilt wegen **Schritt** 1, dass sowohl $a \cdot b$ als auch $b \cdot a$ gleich 0_K sind. Die Kommutativität von $\cdot$ gilt also auf ganz K.

Schritt 4: Wir zeigen: 1_K ist neutrales Element bzgl. $\cdot$ auf ganz K:

Wir wissen bereits $1_K \cdot a = a \cdot 1_K$ für alle $a \in K \setminus \{0_K\}$. Ist nun $a = 0_K$, so gilt wegen **Schritt** 1 $1_K \cdot a = a \cdot 1_K = 0_K$. Damit ist 1_K neutrales Element bzgl. $\cdot$ auf ganz K.

Damit haben wir bisher gezeigt, dass $(K, \cdot)$ ein abelsches Monoid mit dem Einselement 1_K ist, also ist $(K, +, \cdot)$ per Definition 9.1 ein abelscher Ring mit dem Einselement 1_K, der Aussage (*i*) nicht der Nullring ist.

Schritt 5: Wir zeigen: Der Ring $(K, +, \cdot)$ ist nullteilerfrei.

Wenn $a, b \in K \setminus \{0_K\}$ sind, dann ist auch $a \cdot b \in K \setminus \{0_K\}$, da per Definition $(K \setminus \{0\}, \cdot)$ eine Gruppe und damit insbesondere $K \setminus \{0\}$ abgeschlossen bzgl. $\cdot$ ist. Das heißt, $(K, +, \cdot)$ ist nullteilerfrei.

Aussage (iii): Für $a, b_1, b_2 \in K \setminus \{0\}$ sind die Kürzungsregeln (10.2) nichts anderes als die Kürzungsregeln (7.10) in der Gruppe $(K \setminus \{0\}, \cdot)$. Wir zeigen (10.2a) in den verbleibenden Fällen. Ist $b_1 = 0_K$, dann folgt aus Aussage (i) und der Voraussetzung $0_K = a \cdot b_1 = a \cdot b_2$. Wegen der Nullteilerfreiheit und $a \neq 0_K$ folgt weiter $b_2 = 0_K$, also $b_1 = b_2$. Ist andererseits $b_2 = 0_K$, dann folgt aus Aussage (i) und der Voraussetzung $0_K = a \cdot b_2 = a \cdot b_1$. Wegen der Nullteilerfreiheit und $a \neq 0_K$ folgt weiter $b_1 = 0_K$, also wiederum $b_1 = b_2$.

Die Aussage (10.2b) können wir analog beweisen. □

Beachte: Die Rechenregeln in Ringen aus Lemma 9.3 gelten also auch in Körpern.

Die Definition 9.4 der Charakteristik eines Ringes wird auch auf Körper angewendet. Für Körper ist die Charakteristik entweder 0 oder eine Primzahl.

Satz 10.4 (Wann ist ein Ring ein Körper?).
Es sei K eine Menge mit zwei (inneren) Verknüpfungen $+$ und $\cdot$. Dann sind die folgenden Aussagen äquivalent:

(i) $(K, +, \cdot)$ ist ein Körper, dessen Nullelement mit 0_K und dessen Einselement mit 1_K bezeichnet werden.

(ii) $(K, +, \cdot)$ ist ein kommutativer Ring mit dem Einselement 1_K und dem Nullelement $0_K \neq 1_K$, wobei zu jedem $a \in K \setminus \{0_K\}$ ein Inverses bzgl. $\cdot$ in K existiert.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Nach Lemma 10.3 ist $(K, +, \cdot)$ ein kommutativer Ring mit dem Einselement 1_K und dem Nullelement $0_K \neq 1_K$. Da $(K \setminus \{0_K\}, \cdot)$ eine Gruppe ist, existiert zu jedem $a \in K \setminus \{0_K\}$ ein Inverses bzgl. $\cdot$.

Aussage (ii) $\Rightarrow$ Aussage (i): Nach Voraussetzung ist $(K, +)$ eine abelsche Gruppe mit dem Nullelement 0_K. Weiter gelten die Distributivgesetze (10.1) nach Voraussetzung. Es bleibt zu zeigen, dass $(K \setminus \{0_K\}, \cdot)$ eine abelsche Gruppe mit dem Einselement 1_K ist.

Nach Voraussetzung ist $(K, \cdot)$ ein abelsches Monoid mit neutralem Element 1_K. Aus der Eigenschaft $\forall a \in K \setminus \{0\} \; \exists a^{-1} \in K \; (a \cdot a^{-1} = a^{-1} \cdot a = 1_K)$ folgt die Nullteilerfreiheit:

$$a \cdot b = 0_K \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_K = 0_K.$$

Also ist $K \setminus \{0_K\}$ bzgl. $\cdot$ abgeschlossen. Damit erbt $(K \setminus \{0_K\}, \cdot)$ die Eigenschaft, ein abelsches Monoid mit dem Einselement 1_K zu sein, von $(K, \cdot)$. Da jedes Element $a \in K \setminus \{0_K\}$ nach Voraussetzung ein Inverses a^{-1} bzgl. $\cdot$ mit $a^{-1} \in K$ besitzt und a^{-1} wegen $a \cdot 0_K = 0_K \neq 1_K$ sogar in $K \setminus \{0_K\}$ liegen muss, ist $(K \setminus \{0_K\}, \cdot)$ als abelsche Gruppe bestätigt. Das heißt, $(K, +, \cdot)$ ist ein Körper. □

Satz 10.5 (endliche Integritätsringe sind Körper).
Es sei $(R, +, \cdot)$ ein Integritätsring mit endlich vielen Elementen. Dann ist $(R, +, \cdot)$ ein Körper.

Beweis. Es sei $(R, +, \cdot)$ ein Integritätsring, also ein kommutativer, nullteilerfreier Ring mit dem Einselement 1_R ungleich dem Nullring. Wir wissen also bereits: $(R, +)$ ist eine abelsche Gruppe mit dem Nullelement 0_R, und $(R, \cdot)$ ist eine abelsche Halbgruppe mit dem Einselement $1_R \neq 0_R$ (Lemma 9.3). Aus der Nullteilerfreiheit folgt, dass $R \setminus \{0_R\}$ bzgl. $\cdot$ abgeschlossen ist, also ist auch $(R \setminus \{0_R\}, \cdot)$ ein abelsches Monoid mit dem Einselement 1_R.

Es bleibt zu zeigen, dass $(R \setminus \{0_R\}, \cdot)$ sogar eine Gruppe ist. Dazu nutzen wir das Gruppenkriterium Lemma 7.18. Zu beliebigem $a \in R \setminus \{0\}$ betrachten wir die Rechtstranslation $\cdot_a$ auf dem Monoid $R \setminus \{0\}$. Diese ist injektiv, denn nach Distributivgesetz (9.1b) gilt

$$b \cdot a = c \cdot a \quad \Rightarrow \quad b \cdot a - c \cdot a = 0_R \quad \Rightarrow \quad (b - c) \cdot a = 0_R,$$

und da R nullteilerfrei und $a \neq 0_R$ ist, folgt $b = c$. Da nun R und damit $R \setminus \{0\}$ eine endliche Menge ist, gilt nach Satz 6.27, dass $\cdot_a$ auch surjektiv.

Ein analoges Argument zeigt, dass auch alle Linkstranslationen auf $R \setminus \{0\}$ surjektiv sind. Aus dem Gruppenkriterium Lemma 7.18 folgt nun, dass $(R \setminus \{0\}, \cdot)$ eine Gruppe ist. □

Folgerung 10.6 (Körpereigenschaft des Restklassenringes und des Ringes von $\mathbb{Z}$ modulo m, vgl. Satz 9.9)**.**
Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ sowie der zu ihm isomorphe Ring (Beispiel 9.12) von $\mathbb{Z}$ modulo m $(\mathbb{Z}_m, +_m, \cdot_m)$ sind Körper genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist. In diesem Fall nennen wir sie auch **Restklassenkörper modulo m** oder **Körper von $\mathbb{Z}$ modulo m** (englisch: field of $\mathbb{Z}$ modulo m).

Beweis. In Satz 9.9 haben wir gezeigt, dass $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ genau dann ein Integritätsbereich ist, wenn $m \in \mathbb{N}$ eine Primzahl ist. Da aber $\mathbb{Z}/m\mathbb{Z}$ nur endlich viele (nämlich m) Elemente hat, ist Integritätsbereich zu sein gleichbedeutend mit der Körpereigenschaft.

Nach Beispiel 9.12 sind $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ und $(\mathbb{Z}_m, +_m, \cdot_m)$ als Ringe isomorph, also gelten dieselben Eigenschaften auch für $(\mathbb{Z}_m, +_m, \cdot_m)$. □

Definition 10.7 (Unterkörper, vgl. Definition 9.10 eines Unterringes)**.**
Es sei $(K, +, \cdot)$ ein Körper.

(*i*) Eine Teilmenge $U \subseteq K$ heißt ein **Teilkörper** oder **Unterkörper** (englisch: subfield) von $(K, +, \cdot)$, wenn U bzgl. + und bzgl. · abgeschlossen ist und wenn $(U, +, \cdot)$ selbst wieder ein Körper ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, +)$ eine Untergruppe von $(K, +)$ ist und wenn $(U \setminus \{0\}, \cdot)$ eine Untergruppe von $(K \setminus \{0\}, \cdot)$ ist.

(*ii*) Ein Unterkörper $(U, +, \cdot)$ von $(K, +, \cdot)$ heißt **echt** (englisch: proper subfield), wenn $U \subsetneq K$ gilt.

Beispiel 10.8 (Unterkörper)**.**

(*i*) $(\mathbb{Q}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{R}, +, \cdot)$.

(*ii*) $(\mathbb{R}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{C}, +, \cdot)$.

Definition 10.9 (Körperhomomorphismus, vgl. Definition 9.11 eines Ringhomomorphismus)**.**
Es seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ zwei Körper.

(*i*) Eine Abbildung $f\colon K_1 \to K_2$ heißt **strukturverträglich** oder ein **(Körper-)Homomorphismus** (englisch: field homomorphism) von $(K_1, +_1, \cdot_1)$ in $(K_2, +_2, \cdot_2)$, wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in K_1, \tag{10.3a}$$

$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in K_1, \tag{10.3b}$$

$$f(1_{K_1}) = 1_{K_2}. \tag{10.3c}$$

(*ii*) Wie in Definition 8.1 sprechen wir im Fall $(K_1, +_1, \cdot_1) = (K_2, +_2, \cdot_2)$ von einem **(Körper-)Endomorphismus** (englisch: field endomorphism).

(*iii*) Ist $f\colon K_1 \to K_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Körper-)Isomorphismus** (englisch: field isomorphism) In diesem Fall nennen wir $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ auch zueinander **isomorphe Körper** (englisch: isomorphic fields) und schreiben

$$(K_1, +_1, \cdot_1) \cong (K_2, +_2, \cdot_2).$$

(*iv*) Im Fall $(K_1, +_1, \cdot_1) = (K_2, +_2, \cdot_2)$ und $f\colon K_1 \to K_2$ bijektiv sprechen wir auch von einem **(Körper-) Automorphismus** (englisch: field automorphism).

Da die Bedingungen (10.3) mit denen aus (9.4) übereinstimmen, ist ein Körperhomomorphismus nichts anderes als ein Ringhomomorphismus, der speziell zwischen Körpern eingesetzt wird. Insbesondere haben wir auch hier wie in (9.7) wieder

$$f(0_{K_1}) = 0_{K_2}. \tag{10.4}$$

Interessanterweise gilt weiter, dass Körperhomomorphismen automatisch injektiv sind, denn nehmen wir $a \neq b$, aber $f(a) = f(b)$ an, so ergibt sich der Widerspruch

$$\begin{aligned}
1_{K_2} &= f(1_{K_1}) && \text{wegen (10.3c)}\\
&= f\big((a -_1 b)^{-1} \cdot_1 (a -_1 b)\big) && \text{da } a -_1 b \neq 0_{K_1} \text{ vorausgesetzt wurde}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 f(a -_1 b) && \text{wegen (10.3a)}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 \big(f(a) -_2 f(b)\big) && \text{wegen (10.3b)}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 0_{K_2} && \text{da } f(a) = f(b) \text{ vorausgesetzt wurde}\\
&= 0_{K_2} && \text{nach Lemma 9.3.}
\end{aligned}$$

§ 11 POLYNOME

Literatur: Beutelspacher, 2014, Kapitel 6, Bosch, 2014, Kapitel 5, Fischer, Springborn, 2020, Kapitel 2.3

Definition 11.1 (Polynom).
Es sei $(R, +, \cdot)$ ein kommutativer Ring.[14] Ein **Polynom** (englisch: polynomial, altgriechisch: *πολύ*: viel, altgriechisch: *όνομα*: Name) über R in der Variablen t ist ein formaler Ausdruck der Gestalt

$$a_n \cdot t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_1 \cdot t + a_0 \quad \text{oder auch} \quad \sum_{i=0}^{n} a_i \cdot t^i. \tag{11.1}$$

Dabei ist $n \in \mathbb{N}_0$. Die Zahlen $a_i \in R$ heißen die **Koeffizienten** (englisch: coefficients) des Polynoms.

Bemerkung 11.2 (Polynom).

(*i*) Die Variable t ist ein willkürlich gewähltes Symbol. Später werden wir für t geeignete Objekte einsetzen. Da zunächst unspezifiert ist, welche Objekte für die Variable t eingesetzt werden können, ist die Bedeutung der „Potenzen“ t^j, deren „Multiplikation“ mit den Koeffizienten $a_j \in R$ sowie die „Addition“ der daraus entstehenden Terme im Moment unklar. Daher verstehen wir (11.1) zunächst als formalen Ausdruck.

---

[14] Tatsächlich ist R oft sogar ein Körper.

(*ii*) $a_1 \cdot t$ ist eine abkürzende Schreibweise für $a_1 \cdot t^1$, und a_0 ist eine abkürzende Schreibweise für $a_0 \cdot t^0$.

(*iii*) Die Reihenfolge der „Summanden“ in (11.1) ist unerheblich. Die Polynome $3 \cdot t^2 + 2 \cdot t$ und $2 \cdot t + 3 \cdot t^2$ werden also miteinander identifiziert.

(*iv*) Ist ein Koeffizient $a_i = 0_R \in R$, so lässt man häufig den entsprechenden „Summanden“ in der Darstellung (11.1) einfach weg. Die Polynome $3 \cdot t^2 + 0 \cdot t$ und $3 \cdot t^2$ werden also miteinander identifiziert.

(*v*) Ist ein Koeffizient $a_i = 1_R$ in einem Ring mit dem Einselement 1_R, so lässt man den Koeffizienten 1_R in der Darstellung (11.1) manchmal weg, sofern es sich nicht um a_0 handelt. Die Polynome $1_R \cdot t^2$ und t^2 werden also miteinander identifiziert.

(*vi*) Die Menge aller Polynome über dem kommutativen Ring R in der Variablen t wird mit $R[t]$ bezeichnet.

(*vii*) Zwei Polynome sind gleich, wenn die entsprechenden Koeffizienten gleich sind.

(*viii*) Sind alle Koeffizienten gleich $0_R \in R$, so heißt das Polynom das **Nullpolynom** (englisch: zero polynomial), geschrieben 0_R.

(*ix*) Ist R ein Ring mit dem Einselement 1_R und sind alle Koeffizienten gleich $0_R \in R$ bis auf $a_0 = 1_R \in R$, so heißt das Polynom das **Einspolynom** (englisch: constant one polynomial), geschrieben 1_R.

(*x*) Ist R ein Ring mit dem Einselement 1_R, dann heißt ein Polynom der Form t^n das **Monom** (englisch: monomial) **vom Grad** $n \in \mathbb{N}_0$.[15]

(*xi*) Ein Polynom der Form $a_0 \in R \subseteq R[t]$ heißt ein **konstantes Polynom** (englisch: constant polynomial).

(*xii*) Ein Polynom der Form $a_0 + a_1 \cdot t \in R[t]$ mit $a_1 \neq 0_R$ heißt ein **lineares Polynom** (englisch: linear polynomial).

Beispiel 11.3 (Polynome).

(*i*) $p = \frac{3}{4} \cdot t^2 - 7 \cdot t + \frac{1}{2} = \frac{1}{2} + \frac{3}{4} \cdot t^2 - 7 \cdot t \in \mathbb{Q}[t]$ ist ein Polynom über dem Körper $\mathbb{Q}$.

(*ii*) $p = s^5 - \frac{\sqrt{2}}{3} \cdot s + \frac{2}{5} \in \mathbb{R}[s]$ ist ein Polynom über dem Körper $\mathbb{R}$.

(*iii*) $p = [1] \mathbin{\tilde{\cdot}} X^3 \mathbin{\tilde{+}} [3] \mathbin{\tilde{\cdot}} X^2 \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} X \in (\mathbb{Z} / 4\,\mathbb{Z})[X]$ ist ein Polynom über dem Restklassenring $\mathbb{Z} / 4\,\mathbb{Z}$.

Wir definieren nun zwei Verknüpfungen + („Addition“) und · („Multiplikation“) auf der Menge $R[t]$ der Polynome über dem kommutativen Ring $(R, +, \cdot)$.[16] Es seien $p, q \in R[t]$ gegeben mit den Darstellungen

$$p = a_m \cdot t^m + \cdots + a_1 \cdot t + a_0 = \sum_{i=0}^{m} a_i \cdot t^i \tag{11.2a}$$

$$q = b_n \cdot t^n \;\; + \cdots + b_1 \cdot t + b_0 = \sum_{i=0}^{n} b_i \cdot t^i \tag{11.2b}$$

---

[15] Der Begriff des Grades für beliebige Polynome wird in Definition 11.8 eingeführt.

[16] Es ist Absicht, dass die Verknüpfungen in $R[t]$ genauso benannt werden wie die Verknüpfungen im Koeffizientenring R. Dadurch wird $(R, +, \cdot)$ zu einem Unterring von $(R[t], +, \cdot)$, nämlich dem Unterring der konstanten Polynome.

und $m, n \in \mathbb{N}_0$. Zur Abkürzung setzen wir außerdem $N := \max\{m, n\}$ und füllen in (11.2) nicht notierte Terme mit Nullkoeffizienten auf. Dann definieren wir die **Addition von Polynomen** (englisch: addition of polynomials)

$$p + q := (a_N + b_N) \cdot t^N + \dots + (a_1 + b_1) \cdot t + (a_0 + b_0) = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) \cdot t^i \tag{11.3a}$$

sowie die **Multiplikation von Polynomen** (englisch: multiplication of polynomials)

$$p \cdot q := c_{m+n} \cdot t^{m+n} + \dots + c_1 \cdot t + c_0 \qquad = \sum_{k=0}^{m+n} c_k \cdot t^k, \tag{11.3b}$$

wobei c_k für $k \in \mathbb{N}_0$ als

$$c_k := \sum_{i=0}^{k} a_i \cdot b_{k-i} = \sum_{\substack{i,j=0 \\ i+j=k}}^{k} a_i \cdot b_j \tag{11.3c}$$

gesetzt wird. Man nennt die aus (11.3c) entstehende Folge $(c_k)_{k \in \mathbb{N}_0}$, also

$$\begin{aligned} c_0 &= a_0 \cdot b_0 \\ c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0 \\ c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 \quad \text{usw.} \end{aligned}$$

die **Faltung** (englisch: convolution, lateinisch: convolvere: zusammenrollen) der Folgen $(a_i)_{i \in \mathbb{N}_0}$ und $(b_i)_{i \in \mathbb{N}_0}$.

Quizfrage 11.1: Wie kann man sich die Faltung der Koeffizientenfolgen $(a_i)_{i \in \mathbb{N}_0}$ und $(b_i)_{i \in \mathbb{N}_0}$ grafisch vorstellen?

Definition 11.4 (Polynomring).

Es sei $(R, +, \cdot)$ ein kommutativer Ring. Mit den zwei Verknüpfungen (11.3) wird $(R[t], +, \cdot)$ zu einem kommutativen Ring, genannt der **Polynomring** (englisch: polynomial ring) **über** R in der Variablen t. R heißt der **Koeffizientenring** (englisch: coefficient ring, ring of coefficients) von $R[t]$.

Das Nullelement von $R[t]$ ist das Nullpolynom 0_R. Besitzt R das Einselement 1_R, dann ist $(R[t], +, \cdot)$ ebenfalls ein Ring mit Einselement 1_R, dem Einspolynom. Das Symbol + aus (11.1) ist die gleichnamige Verknüpfung (11.3a) aus dem Polynomring. Das Symbol $\cdot$ aus (11.1) ist die gleichnamige Verknüpfung (11.3b) aus dem Polynomring, wobei ein Faktor ein Polynom der Form $a_i \in R$ ist und der andere Faktor ein Monom.

Bemerkung 11.5 (Polynomring als Erweiterung von $(R, +, \cdot)$).

Wenn R ein Ring mit Eins, aber nicht der Nullring ist, so können wir den Polynomring $(R[t], +, \cdot)$ algebraisch auch verstehen als die (bis auf Ring-Isomorphie eindeutige) kleinstmögliche Erweiterung des kommutativen Ringes von $(R, +, \cdot)$ zu einem kommutativen Ring, der zusätzlich das freie Element $t \notin R$ enthält. Dadurch wird $(R, +, \cdot)$ zu ein Unterring von $(R[t], +, \cdot)$, dem Unterring der konstanten Polynome.

Quizfrage 11.2: Wie sieht der Polynomring $R[t]$ aus, wenn R der Nullring ist?

Bemerkung 11.6 (Polynomring als Folgenring)**.**

Wir können ein Polynom identifizieren mit der Folge $\mathbb{N}_0 \to R$ (vgl. Definition 6.29) seiner in aufsteigender Reihenfolge der „Potenzen" sortierten Koeffizienten, von denen nur endlich viele ungleich $0_R \in R$ sind. Man sagt, eine solche Folge habe **endlichen Träger**[17] (englisch: finite support). Diese Teilmenge von $R^{\mathbb{N}_0}$ notieren wir in dieser Lehrveranstaltung als $(R^{\mathbb{N}_0})_{00}$.

Beispielsweise kann das Polynom $t - t^2 + 3 \in \mathbb{Z}[t]$ identifiziert werden mit der endlich getragenen Folge $(3, 1, -1, 0, 0, \ldots)$ seiner Koeffizienten in $\mathbb{Z}$. Das Polynom p aus (11.2a) wird identifiziert mit der endlich getragenen Folge $(a_0, a_1, \ldots, a_m, 0, 0, \ldots)$. Statten wir dann $(R^{\mathbb{N}_0})_{00}$ mit der elementweisen Addition $+$ der Folgenelemente und der Faltung als Multiplikation $c = a \cdot b$ wie in (11.3c) aus, so wird $((R^{\mathbb{N}_0})_{00}, +, \cdot)$ ebenfalls zu einem kommutativen Ring, der zu $R[t]$ isomorph ist.

Ende der Vorlesung 13

Beispiel 11.7 (Addition und Multiplikation von Polynomen)**.**

(*i*) Für die Polynome

$$\begin{aligned} p &= \frac{3}{4} \cdot t^2 - 7 \cdot t + \frac{1}{2} \\ q &= -\frac{1}{2} \cdot t^3 - t + 1 \end{aligned}$$

über dem Körper $(\mathbb{Q}, +, \cdot)$ gilt

$$\begin{aligned} p + q &= \Big(0 - \frac{1}{2}\Big) \cdot t^3 + \Big(\frac{3}{4} + 0\Big) \cdot t^2 + \big(-7 + (-1)\big) \cdot t + \Big(\frac{1}{2} + 1\Big) \\ &= -\frac{1}{2} \cdot t^3 + \frac{3}{4} \cdot t^2 - 8 \cdot t + \frac{3}{2} \\ p \cdot q &= \Big(0 + 0 + \frac{3}{4} \cdot (-\frac{1}{2}) + 0 + 0 + 0\Big) \cdot t^5 + \Big(0 + (-7) \cdot (-\frac{1}{2}) + 0 + 0 + 0\Big) \cdot t^4 \\ &\quad + \Big(\frac{1}{2} \cdot (-\frac{1}{2}) + 0 + \frac{3}{4} \cdot (-1) + 0\Big) \cdot t^3 + \Big(0 + (-7) \cdot (-1) + \frac{3}{4} \cdot 1\Big) \cdot t^2 \\ &\quad + \Big(\frac{1}{2} \cdot (-1) + (-7) \cdot 1\Big) \cdot t + \Big(\frac{1}{2} \cdot 1\Big) \\ &= -\frac{3}{8} \cdot t^5 + \frac{7}{2} \cdot t^4 - t^3 + \frac{31}{4} \cdot t^2 - \frac{15}{2} \cdot t + \frac{1}{2}. \end{aligned}$$

Berechnung der Koeffizienten des Produkts $p \cdot q$ mittels Faltungstabelle:

	$\frac{1}{2}$	-7	$\frac{3}{4}$	0
1	$\frac{1}{2}$	-7	$\frac{3}{4}$	0
-1	$-\frac{1}{2}$	7	$-\frac{3}{4}$	0
0	0	0	0	0
$-\frac{1}{2}$	$-\frac{1}{4}$	$\frac{7}{2}$	$-\frac{3}{8}$	0

---

[17] Der **Träger einer Folge** (englisch: support of a sequence) mit Werten in einem Ring (oder allgemeiner mit Werten in einer additiven Gruppe) ist die Menge derjenigen Indizes, deren Folgenglieder ungleich dem Nullelement sind.

Die Summation entlang der Diagonalen ergibt wiederum die Koeffizienten

$$\begin{aligned}
c_0 &= \frac{1}{2}, & c_1 &= -\frac{1}{2} - 7 = -\frac{15}{2}, & c_2 &= 0 + 7 + \frac{3}{4} = \frac{31}{4}, \\
c_3 &= -\frac{1}{4} + 0 - \frac{3}{4} + 0 = -1, & c_4 &= \frac{7}{2} + 0 + 0 = \frac{7}{2}, & c_5 &= -\frac{3}{8} + 0 = -\frac{3}{8}.
\end{aligned}$$

(*ii*) Für die Polynome

$$\begin{aligned}
p &= [1] \mathbin{\tilde{\cdot}} X^3 \mathbin{\tilde{+}} [-3] \mathbin{\tilde{\cdot}} X^2 \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} X & &\text{oder auch } p = X^3 \mathbin{\tilde{+}} X^2 \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} X \\
q &= [-1] \mathbin{\tilde{\cdot}} X \mathbin{\tilde{+}} [7] & &\text{oder auch } q = [3] \mathbin{\tilde{\cdot}} X \mathbin{\tilde{+}} [3]
\end{aligned}$$

über dem Restklassenring $\mathbb{Z} / 4\,\mathbb{Z}$ gilt

$$\begin{aligned}
(p \mathbin{\tilde{+}} q)(X) &= [1] \mathbin{\tilde{\cdot}} X^3 \;\tilde{+}\; [1] \mathbin{\tilde{\cdot}} X^2 \;\tilde{+}\; \big([2] \mathbin{\tilde{+}} [-1]\big) \mathbin{\tilde{\cdot}} X \;\tilde{+}\; [7] \\
&= [1] \mathbin{\tilde{\cdot}} X^3 \;\tilde{+}\; [1] \mathbin{\tilde{\cdot}} X^2 \;\tilde{+}\; [1] \mathbin{\tilde{\cdot}} X \;\tilde{+}\; [3],
\end{aligned}$$

$$\begin{aligned}
(p \mathbin{\tilde{\cdot}} q)(X) &= [1] \mathbin{\tilde{\cdot}} [-1] \mathbin{\tilde{\cdot}} X^4 \;\tilde{+}\; \big([-3] \mathbin{\tilde{\cdot}} [-1] \mathbin{\tilde{+}} [1] \mathbin{\tilde{\cdot}} [7]\big) \mathbin{\tilde{\cdot}} X^3 \\
&\qquad \tilde{+}\; \big([-3] \mathbin{\tilde{\cdot}} [7] \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} [-1]\big) \mathbin{\tilde{\cdot}} X^2 \;\tilde{+}\; [2] \mathbin{\tilde{\cdot}} [7] \mathbin{\tilde{\cdot}} X \\
&= [3] \mathbin{\tilde{\cdot}} X^4 \;\tilde{+}\; [2] \mathbin{\tilde{\cdot}} X^3 \;\tilde{+}\; [1] \mathbin{\tilde{\cdot}} X^2 \;\tilde{+}\; [2] \mathbin{\tilde{\cdot}} X.
\end{aligned}$$

Zur Vereinfachung der Notation lassen wir in Zukunft das Multiplikationszeichen zwischen Koeffizient und Potenz einer Variable auch oft weg.

Definition 11.8 (Grad eines Polynoms, führender Koeffizient, monisches Polynom)**.**
Es sei p ein Polynom über dem kommutativen Ring R mit den Koeffizienten $a_j \in R$, $j \in \mathbb{N}_0$.

(*i*) Der **Grad** (englisch: degree) ist definiert als[18]

$$\deg(p) \coloneqq \begin{cases} -\infty, & \text{falls alle } a_j = 0_R \text{ sind, also } p = 0_R, \\ \max\{j \in \mathbb{N}_0 \mid a_j \neq 0_R\} & \text{sonst.} \end{cases} \tag{11.4}$$

Ein Polynom vom Grad 0 oder $-\infty$ heißt **konstant** (englisch: constant).

(*ii*) Wenn $p \neq 0_R$ (also nicht das Nullpolynom) ist, dann heißt $\ell(p) \coloneqq a_{\deg(p)}$ auch der **führende Koeffizient** (englisch: leading coefficient) oder der **Leitkoeffizient** von p. Für $p = 0_R$ definieren wir $\ell(0_R) = 0_R$.

(*iii*) Ist R ein Ring mit dem Einselement 1_R und gilt $\ell(p) = 1_R$, dann heißt das Polynom p **normiert** oder **monisch** (englisch: monic).

Quizfrage 11.3: Was weiß man über das Produkt zweier monischer Polynome?

Beispiel 11.9 (Grad eines Polynoms, führender Koeffizient, monisches Polynom)**.**

(*i*) Das Polynom $p = \frac{3}{4}\,t^2 - 7\,t + \frac{1}{2} \in \mathbb{Q}[t]$ über dem Körper $\mathbb{Q}$ besitzt $\deg(p) = 2$. Das Polynom p ist nicht monisch, da $\ell(p) = \frac{3}{4} \neq 1 \in \mathbb{Q}$ ist.

(*ii*) Das Polynom $p = [-7]\,X^3 \mathbin{\tilde{+}} [-3]\,X^2 \mathbin{\tilde{+}} [2]\,X^2 \in (\mathbb{Z} / 4\,\mathbb{Z})[X]$ über dem Restklassenring $\mathbb{Z} / 4\,\mathbb{Z}$ besitzt $\deg(3)$. Das Polynom p ist monisch, da $\ell(p) = [-7] = [1] \in \mathbb{Z} / 4\,\mathbb{Z}$ ist.

---

[18] Manchmal wird der Grad des Nullpolynoms abweichend auch als -1 definiert.

Lemma 11.10 (Grad eines Polynoms).
Es sei R ein kommutativer Ring und $p, q \in R[t]$ zwei Polynome. Dann gilt:

(*i*) $\deg(p + q) \leqslant \max\{\deg(p),\ \deg(q)\}$.

(*ii*) $\deg(p \cdot q) \leqslant \deg(p) + \deg(q)$.

(*iii*) Ist R nullteilerfrei, dann gilt sogar $\deg(p \cdot q) = \deg(p) + \deg(q)$.

Dabei sollen formal für $n \in \mathbb{N}_0$ die Beziehungen $\max\{n,\ (-\infty)\} = \max\{(-\infty), n\} = n$ gelten sowie $\max\{(-\infty),\ (-\infty)\} = -\infty$ und $n + (-\infty) = (-\infty) + n = (-\infty) + (-\infty) = -\infty$.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 7.3. ☐

Folgerung 11.11 (der Polynomring als Integritätsring).
Es sei R ein Integritätsring. Dann ist auch $R[t]$ ein Integritätsring.

Beweis. Nach Definition ist R ein kommutativer, nullteilerfreier Ring mit Eins 1_R, und R ist ungleich dem Nullring. Folglich ist $R[t]$ ein kommutativer Ring mit Eins 1_R (Einspolynom) ungleich dem Nullring, da $1_R \neq 0_R$ (Nullpolynom) gilt. Es bleibt zu zeigen, dass $R[t]$ nullteilerfrei ist. Dazu seien $p, q \in R[t]$ beide nicht das Nullpolynom. Aus Lemma 11.10 Aussage (*iii*) folgt $\deg(p \cdot q) = \deg(p) + \deg(q) \geqslant 0$. Damit ist auch $p \cdot q$ nicht das Nullpolynom. ☐

§ 11.1 POLYNOMDIVISION

Lemma 11.12 (Polynomring ist kein Körper).
Der Polynomring $R[t]$ ist niemals ein Körper.

Beweis. Wenn R der Nullring ist, dann ist auch $R[t]$ der Nullring, besitzt also nur ein Element und ist daher kein Körper (Lemma 10.3). Wir betrachten also im Weiteren nur den Fall, dass R nicht der Nullring ist. Wenn $R[t]$ ein Körper wäre, dann wäre 1_R das neutrale Element bzgl. der Multiplikation in $R[t]$ und damit auch in R. Daraus folgt, dass das Polynom $p = 0_R + 1_R \cdot t$ in $R[t]$ existiert. Dieses besitzt aber kein multiplikatives Inverses, denn: Wäre q das Inverse zu p, gälte also $p \cdot q = 1_R$, dann kann q nicht das Nullpolynom sein. Es müsste also $q = b_n\, t^n + \cdots + b_1\, t + b_0$ gelten für irgendwelche Koeffizienten $b_0, b_1, \ldots, b_n$, $n \in \mathbb{N}_0$. Der 0-te Koeffizient von $p \cdot q$ ist aber $0_R \cdot b_0 = 0_R$, und daher kann $p \cdot q$ nicht das Einspolynom sein. ☐

Als Ersatz für das Fehlen multiplikativer Inverser führen wir (wie bereits aus $\mathbb{Z}$ bekannt) eine **Division mit Rest** (englisch: division with remainder) von Polynomen ein. Wir arbeiten dabei für den Rest von § 11.1 mit einem Körper K für die Koeffizienten an Stelle eines kommutativen Ringes R.

Definition 11.13 (Teiler eines Polynoms).
Es seien K ein Körper und $p_1, p_2 \in K[t]$ zwei Polynome. p_2 heißt ein **Teiler** (englisch: divisor) von p_1 (kurz: $p_2 \mid p_1$), wenn es ein weiteres Polynom $q \in K[t]$ gibt, sodass gilt:

$$p_1 = q \cdot p_2. \tag{11.5}$$

Satz 11.14 (Polynomdivision mit Rest).
Es seien K ein Körper und $p_1, p_2 \in K[t]$ zwei Polynome. Ist $p_2 \neq 0_K$ (Nullpolynom), dann gibt es eindeutig bestimmte Polynome $q, r \in K[t]$, genannt der **Quotient** (englisch: quotient) und der **Rest** (englisch: remainder), sodass gilt:

$$p_1 = q \cdot p_2 + r \quad \text{und} \;\; \deg(r) < \deg(p_2). \tag{11.6}$$

Beweis. Wir zeigen zunächst die Existenz der Zerlegung (11.6). Dazu sei $p_2 \in K[t]$ fest und $\deg(p_2) = m \in \mathbb{N}_0$. Wir verwenden vollständige Induktion nach $n := \deg(p_1) \in \mathbb{N}_0 \cup \{-\infty\}$.

Induktionsanfang: Für jedes $n \in \{-\infty\} \cup [\![0, m-1]\!]$ (also wenn $\deg(p_1) < \deg(p_2)$ gilt) setzen wir $q := 0_K$ und $r := p_1$.

Induktionsschritt: Es sei $n \geqslant m$ und die Behauptung für $n-1$ bereits bewiesen. Es sei nun $n = \deg(p_1) \geqslant \deg(p_2)$. Die Darstellungen von p und q seien

$$\begin{aligned} p_1 &= a_n\, t^n \;\; + a_{n-1}\, t^{n-1} \;\; + \cdots + a_1\, t + a_0, \\ p_2 &= b_m\, t^m + b_{m-1}\, t^{m-1} + \cdots + b_1\, t + b_0. \end{aligned}$$

Wir definieren $\widehat{p}_1 := p_1 - a_n\, b_m^{-1}\, t^{n-m} p_2$. Dann ist der Koeffizient von t^n in $\widehat{p}_1$ gleich 0_K. Damit gilt $\deg(\widehat{p}_1) < \deg(p_1)$. Nach Induktionsvoraussetzung existieren also $\widehat{q}, \widehat{r} \in K[t]$ mit der Eigenschaft $\widehat{p}_1 = \widehat{q}_1 \cdot p_2 + \widehat{r}$ und $\deg(\widehat{r}) < \deg(p_2) = m$. Es folgt nun

$$\begin{aligned} p_1 &= \widehat{p}_1 + a_n\, b_m^{-1}\, t^{n-m} p_2 && \text{nach Definition von } \widehat{p}_1 \\ &= \widehat{q}_1 \cdot p_2 + \widehat{r} + a_n\, b_m^{-1}\, t^{n-m} p_2 && \text{gemäß der Zerlegung von } \widehat{p}_1 \\ &= \underbrace{\left(\widehat{q}_1 + a_n\, b_m^{-1}\, t^{n-m}\right)}_{=:q} \cdot p_2 + \underbrace{\widehat{r}}_{=:r} && \text{wegen der Kommutativität und Distributivität im Ring } K[t]. \end{aligned}$$

Dabei gilt $\deg(r) = \deg(\widehat{r}) < \deg(p_2) = m$.

Es bleibt, die Eindeutigkeit der Zerlegung zu bestätigen. Angenommen, es gelte

$$p_1 = q \cdot p_2 + r = \widehat{q} \cdot p_2 + \widehat{r}$$

mit $\deg(r) < \deg(p_2)$ und $\deg(\widehat{r}) < \deg(p_2)$. Dann folgt $(q - \widehat{q}) \cdot p_2 = \widehat{r} - r$ und weiter

$$\begin{aligned} \deg(p_2) &> \deg(r - \widehat{r}) && \text{da } \deg(r - \widehat{r}) \leqslant \max\{\deg(r),\ \deg(-\widehat{r})\} \text{ nach Lemma 11.10} \\ &= \deg((q - \widehat{q}) \cdot p_2) \\ &= \deg(q - \widehat{q}) + \deg(p_2) && \text{nach Lemma 11.10, da } K \text{ als Körper nullteilerfrei ist.} \end{aligned}$$

Deshalb gilt $\deg(q - \widehat{q}) < 0$, woraus $q - \widehat{q} = 0_K$ folgt, also $q = \widehat{q}$. Aus $q \cdot p_2 + r = \widehat{q} \cdot p_2 + \widehat{r}$ folgt dann auch $r = \widehat{r}$. □

Folgerung 11.15 (Polynomdivision mit Rest).
Unter den Voraussetzungen von Definition 11.13 ist q in (11.5) eindeutig bestimmt.

Beispiel 11.16 (Polynomdivision mit Rest).
Die **Polynomdivision** (englisch: polynomial long division) ist ein Verfahren zur Berechnung der Zerlegung (11.6) für zwei gegebene Polynome $p_1, p_2 \in K[t]$. Man sortiert dazu p_1 und p_2 nach absteigenden Potenzen der Variablen und führt dieselben Schritte wie bei einer schriftlichen Division etwa in $\mathbb{Z}$ durch. Sobald der Grad des aktuellen Restes echt kleiner ist als der Grad von p_2, stoppt das Verfahren.

Für p_1~~(t)~~ $= 3t^3 + 2t + 1$ und p_2~~(t)~~ $= t^2 - 4t$ erhalten wir

$$\begin{array}{rrrl}
3t^3 & & +\,2t+1 & = (t^2-4t)(3t+12)+50t+1 \\
\underline{-\,3t^3} & \underline{+\,12t^2} & & \\
& 12t^2 & +\,2t & \\
& \underline{-\,12t^2} & \underline{+\,48t} & \\
& & 50t+1 &
\end{array}$$

Also gilt in diesem Beispiel

$$\underbrace{3t^3+2t+1}_{p_1} = \underbrace{(3t+12)}_{q} \cdot \underbrace{(t^2-4t)}_{p_2} + \underbrace{(50t+1)}_{r}.$$

§ 11.2 Polynomfunktionen

Wir gehen nun der Frage nach, welche Objekte man für die Variable t in einem Polynom

$$p = a_n\,t^n + a_{n-1}\,t^{n-1} + \cdots + a_1\,t + a_0 \tag{11.7}$$

über einem kommutativen Ring $(R, +, \cdot)$ sinnvollerweise einsetzen kann. Die naheliegendste Wahl sind sicherlich Elemente aus R selbst, und nur diese lassen wir im Moment zu.

Genauer betrachtet induziert das Polynom p eine Funktion $\widetilde{p}\colon R \to R$, definiert durch

$$\widetilde{p}(r) \coloneqq a_n\,r^n + a_{n-1}\,r^{n-1} + \cdots + a_1\,r + a_0. \tag{11.8}$$

Die Funktion $\widetilde{p}$ heißt die **Polynomfunktion** (englisch: polynomial function) zum Polynom p oder die vom Polynom p induzierte Polynomfunktion.

Bemerkung 11.17 (induzierte Polynomfunktion)**.**
Die Menge R^R der Funktionen $R \to R$, ausgestattet mit den punktweisen Verknüpfungen $+$ und $\cdot$ aus R, bildet einen kommutativen Ring $(R^R, +, \cdot)$. Die Abbildung

$$\Phi\colon (R[t], +, \cdot) \ni p \mapsto \widetilde{p} \in (R^R, +, \cdot) \tag{11.9}$$

ist ein Ringhomomorphismus zwischen zwei kommutativen Ringen. Wenn R das Einselement 1_R besitzt, dann besitzt $R[t]$ das Einselement 1_R (das Einspolynom) und R^R das Einselement 1_R (die Einsabbildung $R \mapsto 1_R$), und es gilt $\Phi(1_R) = 1_R$.

Φ ist i. A. nicht injektiv. Verschiedene Polynome können also dieselbe Polynomfunktion induzieren. Wir betrachten als Beispiel den Körper $K = (\mathbb{Z}_2, +_2, \cdot_2)$ und das Polynom

$$p = t^2 + t.$$

Dann ist die zugehörige Polynomfunktion $K \to K$ gerade $\widetilde{p}(t) = t^2 +_2 t = t \cdot_2 t +_2 t$. Diese erfüllt $p(0) = 0 \cdot_2 0 +_2 0 = 0 +_2 0 = 0$ sowie $p(1) = 1 \cdot_2 1 +_2 1 = 1 +_2 1 = 0$. Es ist also $\widetilde{p}$ die Nullfunktion, obwohl p nicht das Nullpolynom ist. Da das Nullpolynom ebenfalls die Nullfunktion induziert, ist die Zuordnung $p \mapsto \widetilde{p}$ in der Tat nicht injektiv.

Φ ist i. A. auch nicht surjektiv. Bild(Φ) ist der Unterring der Polynomfunktionen des Ringes $(R^R, +, \cdot)$.

Definition 11.18 (Nullstelle eines Polynoms).
Es sei R ein kommutativer Ring, $p \in R[t]$ ein Polynom und $\widetilde{p}\colon R \to R$ die zugehörige Polynomfunktion. $\lambda \in R$ heißt eine **Nullstelle** (englisch: zero) oder **Wurzel** (englisch: root) von p in R, wenn $\widetilde{p}(\lambda) = 0_R$ gilt.

Beispiel 11.19 (Nullstelle eines Polynoms).

(i) Das Polynom $p = t^2 + 1 \in \mathbb{R}[t]$ besitzt keine Nullstelle in $\mathbb{R}$, weil für die zugehörige Polynomfunktion $\widetilde{p}\colon \mathbb{R} \to \mathbb{R}$ gilt: $\widetilde{p}(t) = t^2 + 1 \geqslant 1$ für alle $t \in \mathbb{R}$.

(ii) Das Polynom $p = t^2 + 1 \in \mathbb{C}[t]$ besitzt aber zwei Nullstellen in $\mathbb{C}$, und zwar i und $-i$.

(iii) Das Polynom $p = t^2 + 1 \in \mathbb{Z}_5[t]$ besitzt in $\mathbb{Z}_5$ genau die Nullstellen 2 und 3, da für die zugehörige Polynomfunktion $\widetilde{p}\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ gilt: $\widetilde{p}(t) = t \cdot_5 t +_5 1$ und damit

$$\begin{aligned}
\widetilde{p}(0) &= 0 \cdot_5 0 +_5 1 = 1,\\
\widetilde{p}(1) &= 1 \cdot_5 1 +_5 1 \ = 2,\\
\widetilde{p}(2) &= 2 \cdot_5 2 +_5 1 = 0,\\
\widetilde{p}(3) &= 3 \cdot_5 3 +_5 1 = 0,\\
\widetilde{p}(4) &= 4 \cdot_5 4 +_5 1 = 2.
\end{aligned}$$

(iv) Das Polynom $p = (t-0) \cdot (t-1) \cdot (t-2) \cdot (t-3) \cdot (t-4) + 1$, besitzt in $\mathbb{Z}_5$ *keine* Nullstelle, denn es gilt $\widetilde{p}(t) = 1$ für alle $t \in \mathbb{Z}_5$. (Ein solches Polynom gibt es für jeden endlichen Körper.)

Lemma 11.20 (Nullstellen und Teiler).
Es seien K ein Körper und $p \in K[t]$ ein Polynom. Dann sind äquivalent:

(i) $\lambda \in K$ ist eine Nullstelle von p.

(ii) Das Polynom $t - \lambda \in K[t]$ ist ein Teiler von p.

In diesem Fall gilt für das eindeutig bestimmte Polynom $q \in K[t]$ mit $p = (t - \lambda) \cdot q$ die Eigenschaft $\deg(q) = \deg(p) - 1$.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Es sei $\lambda \in K$ eine Nullstelle von p, also $\widetilde{p}(\lambda) = 0$. Nach Satz 11.14 gibt es (eindeutig bestimmte) Polynome $q, r \in K[t]$, sodass gilt: $p = q \cdot (t - \lambda) + r$ und $\deg(r) < \deg(t - \lambda) = 1$. Also ist r ein konstantes Polynom. Um es zu bestimmen, ist es ausreichend, den Wert der zugehörigen Polynomfunktion $\widetilde{r}$ an einer Stelle zu kennen. An der Stelle λ gilt

$$\widetilde{r}(\lambda) = \big(\widetilde{p} - \widetilde{q} \cdot (t - \lambda)\big)(\lambda) = \widetilde{p}(\lambda) - \widetilde{q}(\lambda) \cdot (\lambda - \lambda) = \widetilde{p}(\lambda) = 0_K$$

gilt. Also ist r das Nullpolynom, und es folgt $p = q \cdot (t - \lambda)$, d. h., $t - \lambda$ ist ein Teiler von p.

Aussage (ii) $\Rightarrow$ Aussage (i): Es sei $t - \lambda$ ein Teiler von p, also existiert ein $q \in K[t]$ mit der Eigenschaft $p = q \cdot (t - \lambda)$. Das Einsetzen von λ liefert $\widetilde{p}(\lambda) = \widetilde{q}(\lambda) \cdot (\lambda - \lambda) = \widetilde{q}(\lambda) \cdot 0_K = 0_K$. Also ist λ eine Nullstelle von p.

Weiter gilt nach Lemma 11.10 (iii) $\deg(p) = \deg(q \cdot (t - \lambda)) = \deg(q) + 1$. □

Satz 11.21 (Zerlegung eines Polynoms).
Es seien K ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0_K$. Dann gilt:

(*i*) Es existieren $s \in \mathbb{N}_0$, paarweise verschiedene Zahlen $\lambda_1, \ldots, \lambda_s \in K$ sowie Exponenten $n_1, \ldots, n_s \in \mathbb{N}$ und ein Polynom $q \in K[t]$ ohne Nullstelle in K, sodass gilt:

$$p = (t - \lambda_1)^{n_1} \cdot \cdots \cdot (t - \lambda_s)^{n_s} \cdot q. \tag{11.10}$$

Die Zahl $n_i \in \mathbb{N}$ heißt die **Vielfachheit** (englisch: multiplicity) der Nullstelle λ_i. Jedes Polynom $t - \lambda_i \in K[t]$ heißt ein **Linearfaktor** (englisch: linear factor) von p.

(*ii*) Die Nullstellen von p sind genau die Zahlen $\lambda_1, \ldots, \lambda_s \in K$.

Beweis. Aussage (*i*): Wir führen eine Induktion nach $n := \deg(p)$ durch. Im Fall $n = 0$ (Induktionsanfang) ist p ein konstantes Polynom ungleich 0_K, das keine Nullstelle besitzt. Daher ist dann $s = 0$ und $q = p$.

Wir nehmen an, die Behauptung sei bereits gezeigt für Polynome vom Grad $n \in \mathbb{N}_0$. Es sei p nun ein Polynom vom Grad $n + 1$. Wenn p keine Nullstelle besitzt, so gilt die Behauptung mit $s = 0$ und $q = p$. Andernfalls besitzt p eine Nullstelle $\lambda \in K$. Nach Lemma 11.20 ist also $t - \lambda \in K[T]$ ein Teiler von p, d. h., es gilt $p = (t - \lambda) \cdot \widehat{p}$. Aus Lemma 11.10 folgt $n + 1 = \deg(p) = \deg(t - \lambda) + \deg(\widehat{p}) = 1 + \deg(\widehat{p})$, also gilt $\deg(\widehat{p}) = n$. Nach Induktionsvoraussetzung besitzt also $\widehat{p}$ eine Darstellung wie in (11.10), somit auch $p = (t - \lambda) \cdot \widehat{p}$.

Aussage (*ii*): Ist $\mu \in K$ eine Nullstelle von p, dann folgt

$$0 = \widetilde{p}(\mu) = (\mu - \lambda_1)^{n_1} \cdot \cdots \cdot (\mu - \lambda_s)^{n_s} \cdot \widetilde{q}(\mu).$$

Da K als Körper nullteilerfrei ist, muss einer der Faktoren gleich 0_K sein. Da aber q nach Voraussetzung keine Nullstelle besitzt, muss es ein $i \in [\![1, s]\!]$ geben mit $\mu = \lambda_i$.

Umgekehrt ist nach Lemma 11.20 jedes λ_i, $i \in [\![1, s]\!]$, eine Nullstelle von p. □

Beachte: Man kann zeigen, dass die Darstellung (11.10) bis auf die Reihenfolge der Faktoren eindeutig ist.

Folgerung 11.22 (Zerlegung eines Polynoms)**.**
Es seien K ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0_K$. Dann gilt:

(*i*) p hat höchstens $\deg(p) \in \mathbb{N}_0$ viele paarweise verschiedene Nullstellen, also $s \leqslant \deg(p)$.

(*ii*) p hat höchstens $\deg(p) \in \mathbb{N}_0$ viele Nullstellen, wenn diese entsprechend ihrer Vielfachheit gezählt werden, also gilt $\sum_{i=1}^{s} n_i \leqslant \deg(p)$.

Beweis. Aussage (*i*): Es sei (11.10) die (i. W. eindeutige) Zerlegung von p mit $s \in \mathbb{N}_0$ paarweise verschiedenen Nullstellen von p. Dann gilt

$$\begin{aligned} \deg(p) &= \deg(q) + \sum_{i=0}^{s} n_i && \text{nach Lemma 11.10} \\ &\geqslant 0 + \sum_{i=0}^{s} 1 && q \neq 0_K \text{ und die Vielfachheit jeder Nullstelle ist} \geqslant 1 \\ &= s. \end{aligned}$$

Aussage (*ii*): Zählen wir die Nullstellen λ_i in (11.10) gemäß ihrer Vielfachheit n_i, so erhalten wir

$$\begin{aligned} \deg(p) &= \deg(q) + \sum_{i=0}^{s} n_i \quad \text{nach Lemma 11.10} \\ &\geqslant 0 + \sum_{i=1}^{s} n_i. \end{aligned}$$ ☐

In Bemerkung 11.17 hatten wir gesehen, dass die Abbildung Polynom $p \mapsto$ Polynomfunktion $\widetilde{p}$ i. A. nicht injektiv ist, weil auch Nicht-Nullpolynome auf die Nullfunktion abgebildet werden können. Das Beispiel dafür war ein Polynom über dem endlichen Körper $\mathbb{Z}_2$. Wie folgendes Ergebnis zeigt, ist die Endlichkeit des Körpers charakteristisch für die Nichtinjektivität von Φ.

Folgerung 11.23.
Es sei K ein unendlicher Körper. Dann ist die Abbildung $\Phi\colon K[t] \to K^K$ aus (11.9) injektiv.

Beweis. Es seien $p_1, p_2 \in K[t]$ Polynome und $\widetilde{p_1} = \widetilde{p_2}$ die zugehörigen Polynomfunktionen. Wir setzen $q \coloneqq p_1 - p_2$. Wegen $\widetilde{q} = \widetilde{p_1} - \widetilde{p_2} = 0_K$ (**Quizfrage 11.4:** Warum gilt diese Gleichheit?) hat q unendlich viele Nullstellen, nämlich alle Elemente aus K. Das widerspricht Folgerung 11.22, es sei denn, q ist das Nullpolynom. Daher gilt $p_1 = p_2$, d. h., die Injektivität von Φ. ☐

Satz 11.24 (**Fundamentalsatz der Algebra**[19]**).**
Jedes Polynom $p \in \mathbb{C}[t]$ mit $\deg(p) > 0$ hat mindestens eine Nullstelle.

Ein Beweis dieses Satz wird i. d. R. in weiterführenden Veranstaltungen über *Funktionentheorie* oder *Algebra* vorgestellt.

Folgerung 11.25 (nicht-konstante Polynome über den komplexen Zahlen $\mathbb{C}$ zerfallen in Linearfaktoren)**.**

Jedes nicht-konstante Polynom $p \in \mathbb{C}[t]$ zerfällt vollständig in Linearfaktoren. In der Darstellung (11.10) gilt also $\deg(q) = 0$.

Beweis. Der Beweis gelingt mit vollständiger Induktion nach $n = \deg(p)$ und Anwendung des Fundamentalsatzes 11.24. ☐

Ende der Vorlesung 14

Ende der Woche 7

---

[19] englisch: fundamental theorem of algebra

Kapitel 3 Vektorräume

§ 12 VEKTORRÄUME

Literatur: Beutelspacher, 2014, Kapitel 3, Bosch, 2014, Kapitel 1, Fischer, Springborn, 2020, Kapitel 2.4–2.6

Vektorräume sind die zentralen Strukturen in der *linearen* Algebra. Zu einem Vektorraum V gehört immer ein zugrundeliegender Körper, sagen wir $(K, +, \cdot)$. In Anlehnung an dessen Verknüpfungen bezeichnen wir die beiden Verknüpfungen im Vektorraum V mit $\oplus$ und $\odot$.

Definition 12.1 (Vektorraum)**.**
Es sei $(K, +, \cdot)$ ein Körper. Ein **Vektorraum** (englisch: vector space) oder **linearer Raum** (englisch: linear space) $(V, \oplus, \odot)$ **über** K (kurz: ein K-Vektorraum) ist eine Menge V mit einer inneren Verknüpfung $\oplus \colon V \times V \to V$ und einer **äußeren Verknüpfung** (englisch: (outer) operation) $\odot \colon K \times V \to V$, die die folgenden Bedingungen erfüllen:

(*i*) $(V, \oplus)$ ist eine abelsche Gruppe. Das Nullelement bezeichnen wir mit 0_V.

(*ii*) Für die Verknüpfung $\odot$, genannt **skalare Multiplikation** (englisch: scalar multiplication) oder **S-Multiplikation**, gelten die folgenden Gesetze für alle $\alpha, \beta \in K$ und $u, v \in V$: die **„gemischten“ Distributivgesetze**[1] (englisch: „mixed“ distributive laws)

$$\alpha \odot (u \oplus v) = (\alpha \odot u) \oplus (\alpha \odot v) \tag{12.1a}$$

$$(\alpha + \beta) \odot v = (\alpha \odot v) \oplus (\beta \odot v) \tag{12.1b}$$

sowie das **„gemischte“ Assoziativgesetz** (englisch: „mixed“ associative law)

$$(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v). \tag{12.1c}$$

Weiterhin ist das neutrale Element 1_K bzgl. $\cdot$ in K auch neutral bzgl. $\odot$:

$$1_K \odot v = v. \tag{12.1d}$$

(*iii*) In einem K-Vektorraum V heißen die Elemente von V auch **Vektoren** (englisch: vectors). Das Nullelement 0_V von $(V, \oplus)$ heißt auch der **Nullvektor** (englisch: zero vector). Die Elemente von K heißen **Skalare** (englisch: scalars), und K selbst heißt der **Skalarkörper** (englisch: scalar field) von V.

---

[1] Wir bezeichnen die Gesetze hier als „gemischt“, weil in ihnen Skalare $\alpha, \beta \in K$ mit Vektoren $u, v \in V$ gemischt auftauchen.

Bemerkung 12.2 (abkürzende Schreibweisen)**.**

(i) Das Inverse zu $v \in V$ bzgl. $\oplus$ bezeichnen wir mit $\ominus v$. Die Bezeichnung $u \ominus v$ steht für $u \oplus (\ominus v)$.

(ii) Wir vereinbaren, dass $\odot$ stärker bindet als $\oplus$, also könnten wir die rechte Seite in (12.1a) auch in der Form $\alpha \odot u \;\oplus\; \alpha \odot v$ schreiben.

(iii) Die Konvention, dass bei der skalaren Multiplikation $\odot\colon K \times V \to V$ die Skalare auf der linken Seite stehen, ist willkürlich. Wir können parallel auch $\boxdot\colon V \times K \to V$ definieren, und zwar durch $v \boxdot \alpha \coloneqq \alpha \odot v$. Dann gelten auch dafür die Gesetze (12.1), wobei überall $\odot$ durch $\boxdot$ ersetzt wird und die beiden Argumente dieser Verknüpfung vertauscht werden. Aufgrund der Ähnlichkeit unterscheiden wir nicht zwischen der linken skalaren Multiplikation $\odot$ und der rechten skalaren Multiplikation $\boxdot$, sondern schreiben in Zukunft einfach $\odot$ für beide.

(iv) Wir behalten die unterschiedliche Notation der Verknüpfungen „$+$“ in K und „$\oplus$“ in V wie auch von „$\cdot$“ in K und „$\odot$“ in V zur Verdeutlichung zunächst bei. Später werden wir diese jedoch nur noch als „$+$“ bzw. „$\cdot$“ notieren, siehe Bemerkung 12.10.

(v) Wir werden im Folgenden statt von einem „Vektorraum $(V, \oplus, \odot)$ über dem Körper $(K, +, \cdot)$“ auch einfach von einem „Vektorraum $(V, \oplus, \odot)$“ sprechen, wenn der zugrundeliegende Körper aus dem Zusammenhang klar ist oder wenn wir uns nicht explizit auf ihn beziehen müssen.

Beispiel 12.3 (Vektorraum)**.**

(i) **Dieses Beispiel wurde nachträglich hinzugefügt.** Über jedem Körper $(K, +, \cdot)$ gibt es den (bis auf Isomorphie eindeutigen) Vektorraum $(V, \oplus, \odot)$ mit nur einem Element, nämlich $V = \{0_V\}$. Die Verknüpfungen $\oplus$ und $\odot$ sind dann eindeutig festgelegt. Dieser Raum heißt **Nullraum** (englisch: zero vector space) über K.

(ii) Jeder Körper $(K, +, \cdot)$, ausgestattet mit den Verknüpfungen $\oplus \coloneqq +$ und $\odot \coloneqq \cdot$, ist ein Vektorraum über sich selbst.

(iii) Allgemeiner sei $(K, +, \cdot)$ ein Körper und $(U, +, \cdot)$ ein Unterkörper. Dann ist $(K, +, \cdot)$ ein Vektorraum über U. Beispielsweise ist $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum, und $\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum und ein $\mathbb{Q}$-Vektorraum.

(iv) Es sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann ist die Menge

$$K_n \coloneqq \{(x_1, \ldots, x_n) \mid x_i \in K \text{ für } i = 1, \ldots, n\} \tag{12.2}$$

der n-Tupel[2] über K, ausgestattet mit der **komponentenweisen Addition** (englisch: componentwise addition) und der **komponentenweisen skalaren Multiplikation** (englisch: componentwise scalar multiplication)

$$(x_1, \ldots, x_n) \oplus (y_1, \ldots, y_n) \coloneqq (x_1 + y_1, \ldots, x_n + y_n), \tag{12.3a}$$
$$\alpha \odot (x_1, \ldots, x_n) \coloneqq (\alpha \cdot x_1, \ldots, \alpha \cdot y_n), \tag{12.3b}$$

ein Vektorraum über K, genannt der **Vektorraum der Zeilenvektoren** (englisch: row vector space) über K der Dimension n.[3] Der Nullvektor ist der Vektor $(0_K, \ldots, 0_K) \in K_n$.

---

[2] Gemäß Definition 4.8 müssten wir die n-Tupel eigentlich mit K^n bezeichnen. Es ist aber üblich, die Bezeichnung K^n für den Vektorraum der Spaltenvektoren zu verwenden.

[3] Der Begriff der Dimension für beliebige Vektorräume wird in Definition 13.16 eingeführt. Hier dient er zunächst zur Angabe der Anzahl der Einträge in einem Zeilenvektor.

(*v*) Es sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann ist die Menge

$$K^n := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \,\middle|\, x_i \in K \text{ für } i = 1, \ldots, n \right\}, \tag{12.4}$$

ausgestattet mit der **komponentenweisen Addition** (englisch: componentwise addition) und der **komponentenweisen skalaren Multiplikation** (englisch: componentwise scalar multiplication)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \tag{12.5a}$$

$$\alpha \odot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \alpha \cdot x_1 \\ \vdots \\ \alpha \cdot x_n \end{pmatrix}, \tag{12.5b}$$

ein Vektorraum über K, genannt der **Vektorraum der Spaltenvektoren** (englisch: column vector space) oder auch der **Standardvektorraum** (englisch: standard vector space) oder der **Koordinatenraum** (englisch: coordinate space) über K der Dimension n. Der Nullvektor ist der Vektor $\begin{pmatrix} 0_K \\ \vdots \\ 0_K \end{pmatrix}$ in K^n.

(*vi*) Es sei $(K, +, \cdot)$ ein Körper und X eine Menge. Dann ist die Menge $K^X = \{f \mid f \colon X \to K\}$, ausgestattet mit den punktweisen Verknüpfungen

$$\begin{aligned}(f \oplus g)(x) &:= f(x) + g(x), \\ (\alpha \odot f)(x) &:= \alpha \cdot f(x),\end{aligned}$$

ein Vektorraum über K. Der Nullvektor ist die Nullfunktion.

Insbesondere ist die Menge der Folgen $K^{\mathbb{N}}$ mit Werten in K ein Vektorraum.

(*vii*) Es sei $(K, +, \cdot)$ ein Körper und $K[t]$ der Polynomring (Definition 11.4). In $K[t]$ ist die Addition $+$ gemäß (11.3a) erklärt.[4] Ergänzen wir die skalare Multiplikation[5]

$$\alpha \odot \left(a_n\, t^n + \cdots + a_1\, t + a_0\right) := \alpha \cdot a_n\, t^n + \cdots + \alpha \cdot a_1\, t + \alpha \cdot a_0, \tag{12.6}$$

so wird $K[t]$ zu einem Vektorraum über K, genannt der **Polynomraum** (englisch: vector space of polynomials) über K.

Lemma 12.4 (Rechenregeln in Vektorräumen, vgl. Lemma 9.3)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein Vektorraum über K. Dann gilt für $\alpha \in K$ und $v \in V$:

(*i*) $0_K \odot v = 0_V = v \odot 0_K$.

(*ii*) $\alpha \odot 0_V = 0_V$.

(*iii*) $\alpha \odot v = 0_V \quad \Rightarrow \quad \alpha = 0_K$ oder $v = 0_V$.

---

[4] Die zweite Verknüpfung in $K[t]$, also die Multiplikation $\cdot$ von Polynomen gemäß (11.3b), ignorieren wir hier.

[5] Die skalare Multiplikation stimmt überein mit der Multiplikation von Polynomen, wobei einer der Faktoren ein konstantes Polynom ist, das mit einem Element aus K identifiziert werden kann.

(*iv*) $\alpha \odot (\ominus v) = \ominus(\alpha \odot v) = (-\alpha) \odot v$ und insbesondere $\ominus v = (-1_K) \odot v$.

Beweis. Aussage (*i*):

$$\begin{aligned} 0_V \oplus 0_K \odot v &= 0_K \odot v && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= (0_K + 0_K) \odot v && \text{da } 0_K \text{ das neutrale Element von } (K, +) \text{ ist} \\ &= 0_K \odot v \oplus 0_K \odot v && \text{nach Distributivgesetz (12.1b).} \end{aligned}$$

Aus der Kürzungsregel (7.10b) in der Gruppe $(V, \oplus)$ folgt nun $0_V = 0_K \odot v$. Der Beweis der zweiten Gleichheit folgt sofort aus $0_K \odot v = v \odot 0_K$.

Aussage (*ii*): Für beliebiges $\alpha \in K$ gilt

$$\begin{aligned} \alpha \odot 0_V \oplus 0_V &= \alpha \odot 0_V && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= \alpha \odot (0_V \oplus 0_V) && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= \alpha \odot 0_V \oplus \alpha \odot 0_V && \text{nach Distributivgesetz (12.1a).} \end{aligned}$$

Aus der Kürzungsregel (7.10a) in der Gruppe $(V, \oplus)$ folgt nun $0_V = \alpha \odot 0_V$.

Aussage (*iii*): Es seien $\alpha \in K$ und $v \in V$ sowie $\alpha \odot v = 0_V$. Wir nehmen $\alpha \neq 0_K$ an. Dann gilt

$$\begin{aligned} v &= 1_K \odot v && \text{nach (12.1d)} \\ &= (\alpha \cdot \alpha^{-1}) \odot v && \text{da } \alpha \neq 0_K \text{ in der Gruppe } (K \setminus \{0\}, \cdot) \text{ das Inverse } \alpha^{-1} \text{ besitzt} \\ &= \alpha^{-1} \odot (\alpha \odot v) && \text{nach Assoziativgesetz (12.1c)} \\ &= \alpha^{-1} \odot 0_V && \text{nach Voraussetzung} \\ &= 0_V && \text{nach Aussage } (ii). \end{aligned}$$

Aussage (*iv*): Es seien $\alpha \in K$ und $v \in V$. Wir zeigen zunächst, dass $\alpha \odot v$ das Inverse zu $(-\alpha) \odot v$ in der Gruppe $(V, \oplus)$ ist:

$$\begin{aligned} \big[(-\alpha) \odot v\big] \oplus \big[\alpha \odot v\big] &= \big(-\alpha + \alpha\big) \odot v && \text{nach Distributivgesetz (12.1b)} \\ &= 0_K \odot v && \text{da } \alpha \text{ in der Gruppe } (K, +) \text{ das Inverse } -\alpha \text{ besitzt} \\ &= 0_V && \text{nach Aussage } (i). \end{aligned}$$

Das heißt, es gilt $\ominus(\alpha \odot v) = (-\alpha) \odot v$. Insbesondere für $\alpha = 1_K$ erhalten wir

$$\ominus v = \ominus(1_K \odot v) = (-1_K) \odot v. \tag{$*$}$$

Weiter haben wir

$$\begin{aligned} (-\alpha) \odot v &= \big[(-1_K) \cdot \alpha\big] \odot v && \text{nach Lemma 9.3} \\ &= \big[\alpha \cdot (-1_K)\big] \odot v && \text{da } (K, \cdot) \text{ kommutativ ist} \\ &= \alpha \odot \big((-1_K) \odot v\big) && \text{nach Assoziativgesetz (12.1c)} \\ &= \alpha \odot (\ominus v) && \text{nach } (*). \end{aligned}$$

□

Definition 12.5 (Linearkombination)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein Vektorraum über K.

(*i*) Es sei $E \subseteq V$. Ein Vektor der Form

$$\alpha_1 \odot v_1 \oplus \cdots \oplus \alpha_n \odot v_n \quad \text{oder kurz} \quad \sum_{j=1}^{n} \alpha_j \odot v_j \tag{12.7}$$

mit endlich vielen Skalaren $\alpha_j \in K$ und Vektoren ~~*paarweise verschiedenen Vektoren*~~ $v_j \in E$ für $j = 1, \dots, n$ und $n \in \mathbb{N}_0$ heißt eine **Linearkombination** (englisch: linear combination) **der Menge** E oder **Linearkombination von Vektoren der Menge** E.

(*ii*) Es sei $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V. Ein Vektor der Form

$$\alpha_1 \odot v_{i_1} \oplus \cdots \oplus \alpha_n \odot v_{i_n} \quad \text{oder kurz} \quad \sum_{j=1}^{n} \alpha_j \odot v_{i_j} \tag{12.8}$$

mit endlich vielen Indizes $i_j \in I$ ~~, *paarweise verschiedenen Indizes* $i_1, \dots, i_n \in I$~~ und Skalaren $\alpha_j \in K$ ~~und paarweise verschiedenen Vektoren $v_{i_j} \in V$~~ für $j = 1, \dots, n$ und $n \in \mathbb{N}_0$ heißt eine **Linearkombination der Familie** F oder **Linearkombination von Vektoren der Familie** F.

In beiden Fällen heißen die Skalare α_j die **Koeffizienten** (englisch: coefficients) der Linearkombination. Die Linearkombination heißt **trivial** (englisch: trivial linear combination), wenn alle $\alpha_j = 0$ sind. Falls $n = 0$ gilt, so interpretieren wir wie üblich die Addition von null Elementen als den Nullvektor 0_V.

Beachte: Linearkombinationen bestehen immer aus endlich vielen Termen! ~~Außerdem darf jedes Element von E bzw. jedes Element der Indexmenge I höchstens ein Mal vorkommen.~~

Beispiel 12.6 (Linearkombination).

(*i*) Der Vektor $\left(\begin{smallmatrix} 3 \\ -7 \end{smallmatrix}\right)$ ist eine Linearkombination der Menge der Vektoren $\left\{\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)\right\}$ im Standardvektorraum $\mathbb{R}^2$, nämlich

$$\begin{pmatrix} 3 \\ -7 \end{pmatrix} = 3 \odot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus (-7) \odot \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(*ii*) **Dieses Beispiel wurde nachträglich hinzugefügt.** Der Vektor $\left(\begin{smallmatrix} 3 \\ -7 \end{smallmatrix}\right)$ ist eine Linearkombination der Menge der Vektoren $\left\{\left(\begin{smallmatrix} 2 \\ -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 4 \\ 1 \end{smallmatrix}\right)\right\}$ im Standardvektorraum $\mathbb{R}^2$, nämlich

$$\begin{pmatrix} 3 \\ -7 \end{pmatrix} = \frac{31}{6} \odot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus \frac{-11}{6} \odot \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(Zur Bestimmung der Koeffizienten wurde ein lineares Gleichungssystem gelöst, siehe Kapitel 4.)

(*iii*) Die Funktion $[0, 2\pi] \ni x \mapsto \sin(x) \ominus \sqrt{2} \odot \cos(x) \in \mathbb{R}$ ist eine Linearkombination der Menge der Funktionen (Vektoren) $\{\sin, \cos\}$ im Vektorraum der Funktionen $\mathbb{R}^{[0,2\pi]}$.

(*iv*) Das Polynom $3\,t^2 \oplus 5$ im Vektorraum (Polynomraum) $\mathbb{Q}[t]$ ist eine Linearkombination der Menge der Polynome $\{t^2, t, 1\}$, wobei 1 das Einspolynom in $\mathbb{Q}[t]$ bezeichnet. Das Polynom t kommt in der Linearkombination $3\,t^2 \oplus 5$ mit dem Koeffizienten $0 \in \mathbb{Q}$ vor.

Ende der Vorlesung 15

Definition 12.7 (Unterraum).
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein Vektorraum über K.

(i) Eine Teilmenge $U \subseteq V$ heißt ein **Untervektorraum** oder kurz: ein **(linearer) Unterraum** (englisch: vector subspace, linear subspace) von $(V, \oplus, \odot)$, wenn U bzgl. $\oplus$ und bzgl. der skalaren Multiplikation $\odot$ mit Elementen in K abgeschlossen ist und wenn $(U, \oplus, \odot)$ selbst wieder ein Vektorraum ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, \oplus)$ eine Untergruppe von $(V, \oplus)$ ist und wenn U bzgl. der skalaren Multiplikation $\odot$ mit Elementen in K abgeschlossen ist, also $K \odot U \subseteq U$.

(ii) Ein Unterraum $(U, \oplus, \odot)$ von $(V, \oplus, \odot)$ heißt **echt** (englisch: proper subspace), wenn $U \subsetneq V$ gilt.

Beachte: Da $(U, \oplus)$ eine Untergruppe von $(V, \oplus)$ ist, enthält ein Unterraum U immer den Nullvektor 0_V.

Die Prüfung einer Teilmenge $U \subseteq V$ auf die Unterraum-Eigenschaft lässt sich mit folgendem Kriterium bewerkstelligen:

Satz 12.8 (Unterraumkriterium).
Es sei $(K, +, \cdot)$ ein Körper, $(V, \oplus, \odot)$ ein Vektorraum über K und $U \subseteq V$. Dann sind äquivalent:

(i) $(U, \oplus, \odot)$ ist ein Unterraum von $(V, \oplus, \odot)$.

(ii) $U \neq \emptyset$, und für alle $u, v \in U$ und $\alpha \in K$ gilt $u \oplus v \in U$ und $\alpha \odot u \in U$.
(Mit anderen Worten: $U \neq \emptyset$, und es gilt $U \oplus U \subseteq U$ sowie $K \odot U \subseteq U$.)

(iii) $U \neq \emptyset$, und für alle $u, v \in U$ und $\alpha, \beta \in K$ gilt $\alpha \odot u \;\oplus\; \beta \odot v \in U$.
(Mit anderen Worten: $U \neq \emptyset$, und es gilt $K \odot U \;\oplus\; K \odot U \subseteq U$.)

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Es sei $(U, \oplus, \odot)$ ein Unterraum von $(V, \oplus, \odot)$. Dann ist per Definition 12.7 und Definition 12.1 $(U, \oplus)$ eine Gruppe, also eine Untergruppe von $(V, \oplus)$. Insbesondere gilt $0_V \in U$, also $U \neq \emptyset$. Weiter ist U als Unterraum abgeschlossen bzgl. $\oplus$ und bzgl. der skalaren Multiplikation $\odot$ mit Elementen von K.

Aussage (ii) $\Rightarrow$ Aussage (i): Wir müssen zeigen, dass $(U, \oplus, \odot)$ unter der Annahme von Aussage (ii) wieder ein Vektorraum ist. Diese Annahme zeigt insbesondere, dass $\oplus\colon U \times U \to U$ und $\odot\colon K \times U \to U$ eingeschränkt werden können. Die Eigenschaften aus (12.1) bleiben bei dieser Einschränkung erhalten. Es bleibt also nur zu zeigen, dass $(U, \oplus)$ eine abelsche Gruppe ist, also eine Untergruppe von $(V, \oplus)$. Dazu wenden wir das Untergruppenkriterium (Satz 7.33) an. Es gilt nach Voraussetzung $U \neq \emptyset$. Wegen $\ominus u = (-1_K) \odot u$ für $u \in U$ und der Annahme $K \odot U \subseteq U$ gilt $\ominus U \subseteq U$. Aus der Annahme $U \oplus U \subseteq U$ folgt daher weiter $U \oplus (\ominus U) \subseteq U$. Nach dem Untergruppenkriterium ist $(U, \oplus)$ damit eine Untergruppe von $(V, \oplus)$.

Aussage (ii) $\Rightarrow$ Aussage (iii): Wir haben $K \odot U \subseteq U$ nach Voraussetzung, also auch $K \odot U \oplus K \odot U \subseteq U \oplus U \subseteq U$, wobei die letzte Inklusion wiederum nach Voraussetzung gilt.

Aussage (iii) $\Rightarrow$ Aussage (ii): Es gilt nach Voraussetzung $U \oplus U \subseteq K \odot U \oplus K \odot U \subseteq U$ und außerdem $K \odot U = K \odot U \oplus \{0_K\} \odot U \subseteq K \odot U \oplus K \odot U \subseteq U$. □

Beispiel 12.9 (Unterräume).

(i) Es sei $(V, \oplus, \odot)$ ein Vektorraum. Dann sind $(\{0_V\}, \oplus, \odot)$ und $(V, \oplus, \odot)$ Unterräume von $(V, \oplus, \odot)$. Diese heißen die **trivialen Unterräume** (englisch: trivial subspaces). Speziell $(\{0_V\}, \oplus, \odot)$ ist der **Nullraum** (englisch: zero vector space) von V.

(ii) Wir betrachten den Standardvektorraum $V = \mathbb{R}^2$ über dem Körper $\mathbb{R}$.

(a) Die Menge

$$U_1 := \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \,\middle|\, x_1 - 2\,x_2 = 0 \right\}$$

ist ein Unterraum von $V = \mathbb{R}^2$, denn die Aussage (ii) des Unterraumkriteriums Satz 12.8 ist erfüllt: Zunächst gilt $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) \in U_1$, also ist $U_1 \neq \emptyset$. Weiter gilt für alle $\alpha \in \mathbb{R}$ und $u = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in U_1$ sowie $v = \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right) \in U_1$:

$$\begin{aligned} u \oplus v &= \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix} \in U_1, \quad \text{denn } (x_1 + y_1) - 2\,(x_2 + y_2) = (x_1 - 2\,x_2) + (y_1 - 2\,y_2) = 0 \\ \alpha \odot u &= \begin{pmatrix} \alpha\,x_1 \\ \alpha\,x_2 \end{pmatrix} \in U_1, \quad \text{denn } \alpha\,x_1 - 2\,(\alpha\,x_2) = \alpha\,(x_1 - 2\,x_2) = 0. \end{aligned}$$

(b) Die Menge

$$U_2 := \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \,\middle|\, x_1 - 2\,x_2 = 1 \right\}$$

ist kein Unterraum von $V = \mathbb{R}^2$, denn sie enthält nicht den Nullvektor $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$, was aber eine notwendige Bedingung für einen Unterraum darstellt, wie wir im Anschluss an Definition 12.7 bereits gesehen haben.

(c) Die Menge

$$U_3 := \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \,\middle|\, x_1 \geqslant 0,\ x_2 \geqslant 0 \right\}$$

ist kein Unterraum von $V = \mathbb{R}^2$, denn sie erfüllt das Unterraumkriterium nicht. Beispielsweise ist $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \in U_3$, aber $(-1) \odot \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 \\ -1 \end{smallmatrix}\right)$ nicht.

(iii) Es sei $(K, +, \cdot)$ ein Körper und $(K^{\mathbb{N}}, \oplus, \odot)$ der Vektorraum der Folgen mit Werten in K. Dann ist die Menge der Folgen mit endlichem Träger (siehe Bemerkung 11.6) und Werten in K

$$(K^{\mathbb{N}})_{00} := \left\{ (y_i)_{i \in \mathbb{N}} \,\middle|\, \{ i \in \mathbb{N} \mid y_i \neq 0_K \} \text{ ist endlich} \right\} \tag{12.9}$$

ein echter Unterraum von $(K^{\mathbb{N}}, \oplus, \odot)$.

(iv) Es sei $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ der Vektorraum der Folgen mit Werten in $\mathbb{R}$. Dann sind die Mengen

$$(\mathbb{R}^{\mathbb{N}})_b := \left\{ (y_i)_{i \in \mathbb{N}} \,\middle|\, \exists C \geqslant 0\ \forall i \in \mathbb{N}\ (|y_i| \leqslant C) \right\} \quad \text{der beschränkten Folgen}^{6} \tag{12.10a}$$

$$(\mathbb{R}^{\mathbb{N}})_c := \left\{ (y_i)_{i \in \mathbb{N}} \,\middle|\, (y_i)_{i \in \mathbb{N}} \text{ ist konvergent} \right\} \quad \text{der konvergenten Folgen}^{7} \tag{12.10b}$$

$$(\mathbb{R}^{\mathbb{N}})_0 := \left\{ (y_i)_{i \in \mathbb{N}} \,\middle|\, (y_i)_{i \in \mathbb{N}} \text{ konvergiert gegen } 0 \right\} \quad \text{der Nullfolgen}^{8} \tag{12.10c}$$

$$(\mathbb{R}^{\mathbb{N}})_{00} := \left\{ (y_i)_{i \in \mathbb{N}} \,\middle|\, (y_i)_{i \in \mathbb{N}} \text{ hat endlichen Träger} \right\} \quad \text{der Folgen mit endlichem Träger}^{9} \tag{12.10d}$$

jeweils echte Unterräume von $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$. (**Quizfrage 12.1:** Gibt es auch Unterraumbeziehungen untereinander?)

---

[6] englisch: bounded sequences

[7] englisch: convergent sequences

[8] englisch: null sequences

[9] englisch: finitely supported sequences

(v) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Dann ist für jedes $n \in \mathbb{N}_0$ die Menge der **Polynome vom Höchstgrad n** (englisch: polynomials of maximum degree n)

$$K_n[t] \coloneqq \left\{a_n\, t^n + a_{n-1}\, t^{n-1} + \cdots + a_1\, t + a_0 \,\middle|\, a_i \in K \text{ für } i = 0, \ldots, n\right\} \tag{12.11}$$

ein echter Unterraum von $(K[t], +, \cdot)$. (**Quizfrage 12.2:** Bilden auch die Polynome vom Mindestgrad $n \in \mathbb{N}$ einen Unterraum von $K[t]$?) (**Quizfrage 12.3:** Bilden die Polynome von geradem Grad $n \in 2\,\mathbb{N}_0$ einen Unterraum von $K[t]$?)

Bemerkung 12.10 (Vereinfachung der Notation).
Zur Vereinfachung der Notation werden wir in Zukunft für die Verknüpfungen $\oplus$ und $\odot$ in Vektorräumen einfach dieselbe Notation verwenden wie für die Verknüpfungen $+$ und $\cdot$ des zugrundeliegenden Körpers. Aus dem Zusammenhang ist klar, ob die jeweilige Verknüpfung mit Skalaren oder mit Vektoren gemeint ist.

Das Zeichen für die Multiplikation $\cdot$ von Vektoren mit Elementen aus dem zugrundeliegenden Körper oder von Körperelementen untereinander wird sogar oft ganz weggelassen, solange sich dadurch keine Unklarheiten ergeben. Beispielsweise schreiben wir in Zukunft einfach $\sin - \sqrt{2}\cos$ an Stelle von $\sin \ominus \sqrt{2} \odot \cos$.

Wir werden außerdem das Nullelement von K einfach als 0 schreiben, das Einselement von K als 1 und den Nullvektor von V ebenfalls als 0.

Wie bereits bei Untergruppen in § 7.4 beschäftigt uns nun die Frage, wie man Unterräume erzeugen kann.

Lemma 12.11 (Durchschnitt von Unterräumen).
Es sei $(V, +, \cdot)$ ein Vektorraum und $(U_i, +, \cdot)$ eine Familie von Unterräumen mit der nichtleeren Indexmenge I. Dann ist auch $\bigcap_{i \in I} U_i$ mit $+$ und $\cdot$ ein Unterraum von $(V, +, \cdot)$.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 8.3. □

Definition 12.12 (erzeugter Unterraum, lineare Hülle, Erzeugendensystem).
Es sei $(V, +, \cdot)$ ein Vektorraum und $E \subseteq V$.

(i) Dann heißt

$$\langle E \rangle \coloneqq \bigcap \left\{U \,\middle|\, (U, +, \cdot) \text{ ist Unterraum von } (V, +, \cdot) \text{ und } E \subseteq U\right\} \tag{12.12}$$

der von E **erzeugte Unterraum** (englisch: subspace generated by E) oder die **lineare Hülle** (englisch: linear hull) $\operatorname{Lin}(E)$ von E oder auch der **Spann** (englisch: span) $\operatorname{Span}(E)$ von E in $(V, +, \cdot)$.

Beachte: Bezeichnen wir mit $\mathcal{R}$ die Menge auf rechten Seite von (12.12), über die der Durchschnitt gebildet wird, dann ist $\langle E \rangle$ das Minimum der Menge $\mathcal{R}$ bzgl. der Inklusionshalbordnung und sogar das Minimum der Menge $\mathcal{R}$ bzgl. der Halbordnung „ist Unterraum von".

Ist speziell E die endliche Menge $E = \{v_1, \ldots, v_n\}$ für $v_i \in V$ und $n \in \mathbb{N}$, so schreiben wir auch $\langle v_1, \ldots, v_n \rangle$ oder $\operatorname{Lin}(v_1, \ldots v_n)$ oder $\operatorname{Span}(v_1, \ldots, v_n)$ statt $\langle \{v_1, \ldots v_n\} \rangle$ oder $\operatorname{Lin}(\{v_1, \ldots v_n\})$ oder $\operatorname{Span}(\{v_1, \ldots, v_n\})$.

(*ii*) Gilt $\langle E \rangle = V$, dann heißt E ein **Erzeugendensystem** (englisch: generating set) von $(V, +, \cdot)$. Falls ein endliches Erzeugendensystem von V existiert, so heißt V **endlich erzeugt** (englisch: finitely generated).

(*iii*) Wenn $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V ist, definieren wir den von F **erzeugten Unterraum** in $(V, +, \cdot)$ bzw. die **lineare Hülle** $\langle F \rangle$ von F bzw. den **Spann** $\operatorname{Span}(F)$ von F in $(V, +, \cdot)$ als

$$\langle F \rangle \coloneqq \bigcap \Big\{ U \,\Big|\, (U, +, \cdot) \text{ ist Unterraum von } (V, +, \cdot) \text{ und } \{v_i \mid i \in I\} \subseteq U \Big\}. \tag{12.13}$$

Wir nennen F ein **Erzeugendensystem** von $(V, +, \cdot)$, wenn $\langle F \rangle = V$ gilt.

Satz 12.13 (Darstellung des erzeugten Unterraumes)**.**
Es sei $(K, +, \cdot)$ ein Körper, $(V, +, \cdot)$ ein Vektorraum über K und $E \subseteq V$. Dann gilt für den von E erzeugten Unterraum:

$$\langle E \rangle = \left\{ \sum_{i=1}^{n} \alpha_i \, v_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \; (v_i \in E, \; \alpha_i \in K) \right\}. \tag{12.14}$$

(Im Fall $n = 0$ interpretieren wir wie üblich die Linearkombination von null Elementen in der rechten Menge als den Nullvektor 0. Insbesondere im Fall $E = \emptyset$ ist also $\langle E \rangle = \langle \emptyset \rangle = \{0\}$.)

Ist $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V, dann gilt für den von F erzeugten Unterraum:

$$\langle F \rangle = \left\{ \sum_{j=1}^{n} \alpha_j \, v_{i_j} \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall j = 1, \ldots, n \; \exists i_j \in I \; (v_{i_j} \in F, \; \alpha_j \in K) \right\}. \tag{12.15}$$

Beachte: Der von einer Menge E (oder einer Familie F) erzeugte Unterraum stimmt also überein mit der Menge der Linearkombinationen von E (bzw. F).[10] Auf die Reihenfolge der Elemente in F kommt es offenbar nicht an.

Beweis. Zur Abkürzung bezeichnen wir die Menge auf der rechten Seite von (12.14) mit M. Wir führen den Beweis analog zu Satz 7.37 in zwei Schritten.

Schritt 1: $\langle E \rangle \supseteq M$: Es sei U ein beliebiger Unterraum von V, der im Durchschnitt (12.12) vorkommt. U enthält also E als Teilmenge. Da U ein Unterraum ist, enthält U auch alle Linearkombinationen von E. Also gilt $U \supseteq M$. Da dies für jeden beliebigen Unterraum aus dem Durchschnitt in (12.12) gilt, gilt auch $\langle E \rangle \supseteq M$.

Schritt 2: $\langle E \rangle \subseteq M$: Wir zeigen zunächst, dass M selbst ein Unterraum von V ist. Dazu überprüfen wir das Unterraumkriterium (Satz 12.8). Offensichtlich ist $M \neq \emptyset$, denn M enthält mindestens den Nullvektor 0. Sind $\sum_{i=1}^{n} \alpha_i \, v_i$ und $\sum_{j=1}^{m} \beta_j \, w_j$ zwei Elemente aus M, so ist auch $\sum_{i=1}^{n} \alpha_i \, v_i + \sum_{j=1}^{m} \beta_j \, w_j$ ein Element aus M. Zudem ist für jedes $\alpha \in K$ auch $\alpha \sum_{i=1}^{n} \alpha_i \, v_i = \sum_{i=1}^{n} \alpha \, \alpha_i \, v_i$ ein Element aus M. Also ist M ein Unterraum von V. Zusätzlich ist klar, dass $E \subseteq M$ gilt. (**Quizfrage 12.4:** Details?) Das heißt, M ist einer derjenigen Unterräume von V, über die in der Definition von $\langle E \rangle$ der Durchschnitt gebildet wird. Folglich gilt $\langle E \rangle \subseteq M$.

Der Beweis für den Fall (12.15) geht analog. □

Beispiel 12.14 (lineare Hülle)**.**

---

[10] In manchen Büchern wird daher (12.14) auch als Definition des erzeugten Unterraumes verwendet.

(*i*) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Die Menge aller Monome $E = \{1, t, t^2, \dots\}$ bildet ein Erzeugendensystem von $K[t]$. Die Menge der Monome $E = \{1, t, \dots, t^n\}$ bis zum Grad n bildet ein Erzeugendensystem von $K_n[t]$, dem Unterraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$.

(*ii*) In einem Vektorraum V heißt die lineare Hülle

$$\langle v \rangle = \{\alpha\, v \mid \alpha \in K\}$$

eines einzelnen Vektors $v \neq 0$ eine **Gerade** (englisch: line) durch 0 und v. Die lineare Hülle

$$\langle v, w \rangle = \{\alpha\, v + \beta\, w \mid \alpha, \beta \in K\}$$

von zwei Vektoren $v, w \neq 0$ mit $w \notin \langle v \rangle$ heißt eine **Ebene** (englisch: plane) durch 0, v und w. (**Quizfrage 12.5:** Was passiert im Fall $w \in \langle v \rangle$?)

Folgerung 12.15 wurde nachträglich hinzugefügt.

Folgerung 12.15 (zu Satz 12.13: lineare Hülle von Vereinigung und Schnitt)**.**

Es sei $(V, +, \cdot)$ ein Vektorraum und $E_1, E_2 \subseteq V$. Dann gilt:

(*i*)

$$\langle E_1 \cup E_2 \rangle = \big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle. \tag{12.16}$$

(*ii*)

$$\langle E_1 \cap E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cap \langle E_2 \rangle \big\rangle. \tag{12.17}$$

Beweis. Aussage (*i*): Die lineare Hülle ist ordnungserhaltend, d. h., es gilt $E_1 \subseteq \langle E_1 \rangle$ und $E_2 \subseteq \langle E_2 \rangle$. Daraus folgt $E_1 \cup E_2 \subseteq \langle E_1 \rangle \cup \langle E_2 \rangle$ und durch Bildung der linearen Hülle $\langle E_1 \cup E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle$.

Umgekehrt besteht $\langle E_1 \rangle$ nach Satz 12.13 gerade aus den Linearkombinationen von E_1, und $\langle E_2 \rangle$ besteht aus den Linearkombinationen von E_2. Das heißt, $\big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle$ besteht aus Linearkombinationen solcher Vektoren, die ihrerseits eine Linearkombination von E_1 oder eine Linearkombination von E_2 sind. Mit Hilfe des Assoziativgesetzes (12.1c) erhalten wir, dass wir jeden Vektor aus $\big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle$ als Linearkombination von $E_1 \cup E_2$ schreiben können, also $\big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle \subseteq \langle E_1 \cup E_2 \rangle$.

Aussage (*ii*) Wegen $E_1 \subseteq \langle E_1 \rangle$ und $E_2 \subseteq \langle E_2 \rangle$ gilt $E_1 \cap E_2 \subseteq \langle E_1 \rangle \cap \langle E_2 \rangle$. Durch Bildung der linearen Hülle ergibt sich $\langle E_1 \cap E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cap \langle E_2 \rangle \big\rangle$. □

Ende der Vorlesung 16

Ende der Woche 8

---

§ 13 BASIS UND DIMENSION

Literatur: Beutelspacher, 2014, Kapitel 3, Bosch, 2014, Kapitel 1, Fischer, Springborn, 2020, Kapitel 2.5

In diesem Abschnitt beantworten wir die Frage, wie wir einen Vektorraum durch ein möglichst kleines Erzeugendensystem darstellen können und damit Redundanz in der Darstellung vermeiden.

Definition 13.1 (lineare (Un-)abhängigkeit)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K.

(i) Eine Menge $E \subseteq V$ heißt **linear unabhängig** (englisch: linearly independent), wenn in jeder Linearkombination von $n \in \mathbb{N}$ paarweise verschiedenen Vektoren aus E, die den Nullvektor ergibt, notwendig alle Koeffizienten gleich 0 sind, wenn also für alle $n \in \mathbb{N}$ gilt:

$$v_1, \ldots, v_n \in E, \quad v_i \neq v_j \text{ für } i \neq j \quad \text{und} \quad \sum_{\ell=1}^{n} \alpha_\ell \, v_\ell = 0 \quad \Rightarrow \quad \alpha_\ell = 0 \text{ für alle } \ell = 1, \ldots, n. \tag{13.1}$$

(ii) Wenn dagegen eine Linearkombination von $n \in \mathbb{N}$ paarweise verschiedenen Vektoren aus E möglich ist, die den Nullvektor ergibt, wobei nicht alle Koeffizienten gleich 0 sind, dann heißt E **linear abhängig** (englisch: linearly dependent).

(iii) Eine Familie F von Vektoren in V heißt **linear unabhängig**, wenn in jeder Linearkombination von $n \in \mathbb{N}$ Vektoren aus F mit paarweise verschiedenen Indizes, die den Nullvektor ergibt, notwendig alle Koeffizienten gleich 0 sind, wenn also für alle $n \in \mathbb{N}$ gilt:

$$i_1, \ldots, i_n \in I, \quad i_j \neq i_k \text{ für } j \neq k \quad \text{und} \quad \sum_{\ell=1}^{n} \alpha_\ell \, v_{i_\ell} = 0 \quad \Rightarrow \quad \alpha_\ell = 0 \text{ für alle } \ell = 1, \ldots, n. \tag{13.2}$$

(iv) Wenn dagegen eine Linearkombination von $n \in \mathbb{N}$ Vektoren aus F zu paarweise verschiedenen Indizes möglich ist, die den Nullvektor ergibt, wobei nicht alle Koeffizienten gleich 0 sind, dann heißt F **linear abhängig**.

Bemerkung 13.2 (lineare (Un-)abhängigkeit)**.**

(i) Die lineare (Un-)abhängigkeit ist eine Eigenschaft, die sich auf eine Menge oder eine Familie von Vektoren bezieht. Sprechweisen wie „Der Vektor v ist linear unabhängig von $\{v_1, v_2\}$." sind nicht korrekt. Man kann aber sagen, die Menge $\{v\} \cup \{v_1, v_2\}$ sei linear unabhängig.

(ii) Die Menge $\{v\}$ bestehend aus einem einzigen Vektor ist linear unabhängig, falls $v \neq 0$ ist, ansonsten linear abhängig. (Dasselbe gilt für eine einelementige Familie von Vektoren.)

(iii) Eine Menge oder Familie von Vektoren, die den Nullvektor enthält, ist stets linear abhängig.

(iv) Die leere Menge und die leere Familie von Vektoren sind per Definition linear unabhängig.

Die lineare Abhängigkeit einer Menge bzw. einer Familie von Vektoren bedeutet, dass man einen Vektor als Linearkombination der anderen darstellen kann:

Lemma 13.3 (lineare Abhängigkeit ist äquivalent zur Kombinierbarkeit)**.**
Es sei V ein Vektorraum.

(*i*) Es sind äquivalent:

(a) $E \subseteq V$ ist eine linear abhängige Menge.

(b) Es gibt einen Vektor $v \in E$, der als Linearkombination von $E \setminus \{v\}$ darstellbar ist.

(*ii*) Es sind äquivalent:

(a) $F = (v_i)_{i \in I}$ ist eine linear abhängige Familie mit einer Indexmenge I.

(b) Es gibt es einen Vektor v_{i^*} aus der Familie, der als Linearkombination der Familie $(v_i)_{i \in I \setminus \{i^*\}}$ darstellbar ist.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 9.1. ☐

Lemma 13.4 (lineare (Un-)abhängigkeit von Teilmengen und Obermengen).
Es sei V ein Vektorraum.

(*i*) Jede Teilmenge einer Menge linear unabhängiger Vektoren aus V ist ebenfalls linear unabhängig. Jede Teilfamilie einer Familie linear unabhängiger Vektoren aus V ist ebenfalls linear unabhängig.

(*ii*) Jede Obermenge einer Menge linear abhängiger Vektoren aus V ist ebenfalls linear abhängig. Jede Oberfamilie einer Familie linear abhängiger Vektoren aus V ist ebenfalls linear abhängig.

Beweis. Der Beweis ergibt sich unmittelbar aus der Definition 12.12. ☐

Beispiel 13.5 (lineare (Un-)abhängigkeit).

(*i*) Die Teilmenge $\left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\\sqrt{2}\end{pmatrix}, \begin{pmatrix}\sqrt{2}\\1\end{pmatrix}\right\}$ des Vektorraumes $\mathbb{R}^2$ über dem Körper $\mathbb{R}$ ist linear abhängig, denn es gilt

$$(1+\sqrt{2})\begin{pmatrix}1\\1\end{pmatrix} + (-1)\begin{pmatrix}1\\\sqrt{2}\end{pmatrix} + (-1)\begin{pmatrix}\sqrt{2}\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}.$$

(*ii*) Dieselbe Menge ist als Teilmenge des Vektorraumes $\mathbb{R}^2$ über dem Körper $\mathbb{Q}$ jedoch linear unabhängig, denn es gilt

$$\alpha_1 \begin{pmatrix}1\\1\end{pmatrix} + \alpha_2 \begin{pmatrix}1\\\sqrt{2}\end{pmatrix} + \alpha_3 \begin{pmatrix}\sqrt{2}\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix} \quad \Rightarrow \quad \alpha_1 = \alpha_2 = \alpha_3 = 0.$$

(*iii*) Wir betrachten den K-Vektorraum K^X der Funktionen $X \to K$, wobei $(K,+,\cdot)$ ein Körper und X eine Menge ist; siehe Beispiel 12.3. Für $y \in X$ definieren wir die **charakteristische Funktion** (englisch: characteristic function) $e_y \colon X \to K$ durch[11]

$$x \mapsto e_y(x) \coloneqq \delta_{xy} \coloneqq \begin{cases} 1, & \text{falls } x = y, \\ 0, & \text{falls } x \neq y. \end{cases} \tag{13.3}$$

Dann ist die Menge $\{e_y \mid y \in X\}$ linear unabhängig.

(*iv*) Es sei $(K,+,\cdot)$ ein Körper und $(K[t],+,\cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Dann ist die Menge der Monome $E = \{1, t, t^2, \dots\}$ linear unabhängig.

---

[11] Das Symbol δ_{xy} ist das **Kronecker-Delta** (englisch: Kronecker delta). Allgemein ist die **charakteristische Funktion** e_A **einer Menge** $A \subseteq X$ definiert als $e_A(x) = 1$ für $x \in A$ und $e_A(x) = 0$ für $x \notin A$.

Die Bedeutung linear unabhängiger Mengen und Familien von Vektoren stellt folgendes Resultat klar.

Lemma 13.6 (lineare Unabhängigkeit und eindeutige Linearkombination).
Es sei V ein Vektorraum und $(v_i)_{i\in I}$ eine Familie von Vektoren aus V. Dann sind äquivalent:

(*i*) $(v_i)_{i\in I}$ ist linear unabhängig.

(*ii*) Jeder Vektor $v \in \langle (v_i)_{i\in I} \rangle$ lässt sich in eindeutiger Weise (bis auf Summanden mit Nullkoeffizienten) aus Vektoren der Familie $(v_i)_{i\in I}$ linearkombinieren.

Ein analoges Resultat gilt für Mengen von Vektoren aus V.

Beweis. Aussage (*i*) ⇒ Aussage (*ii*): Es sei $(v_i)_{i\in I}$ linear unabhängig und $v \in \langle (v_i)_{i\in I} \rangle$. Nach Satz 12.13 besteht $\langle (v_i)_{i\in I} \rangle$ gerade aus den Linearkombinationen von $(v_i)_{i\in I}$. Es gibt also eine endliche Teilmenge $I_0 \subseteq I$ und Skalare $\alpha_i \in K$, $i \in I_0$ mit der Eigenschaft

$$v = \sum_{i\in I_0} \alpha_i \, v_i. \tag{$*$}$$

Zu zeigen ist noch, dass diese Darstellung eindeutig ist. Wir nehmen dazu an, dass

$$v = \sum_{j\in I_1} \beta_j \, v_j \tag{$**$}$$

eine weitere Darstellung von v als Linearkombination von $(v_i)_{i\in I}$ ist mit endlicher Indexmenge I_1. Wir setzen $N := \{i \in I_0 \mid \alpha_i \neq 0\} \cup \{j \in I_1 \mid \beta_j \neq 0\}$. Dann ist N endlich. Wir haben

$$\begin{aligned} 0 &= v - v \\ &= \sum_{i\in I_0} \alpha_i \, v_i - \sum_{j\in I_1} \beta_j \, v_j \\ &= \sum_{i\in N} \alpha_i \, v_i - \sum_{j\in N} \beta_j \, v_j \quad \text{indem wir } \alpha_i = 0 \text{ für } i \in N \setminus I_0 \text{ und } \beta_j = 0 \text{ für } j \in N \setminus I_1 \text{ ergänzen} \\ &= \sum_{i\in N} (\alpha_i - \beta_i) \, v_i. \end{aligned}$$

Da nach Voraussetzung $(v_i)_{i\in I}$ linear unabhängig ist, muss $\alpha_i - \beta_i = 0$ für alle $i \in N$ gelten, also $\alpha_i = \beta_i$. Die Darstellungen ($*$) und ($**$) unterscheiden sich also nur um eventuell auftauchende Terme mit Nullkoeffizienten.

Aussage (*ii*) ⇒ Aussage (*i*): Es sei $I_0 \subseteq I$ eine beliebige endliche Teilmenge. Wir müssen zeigen, dass $(v_i)_{i\in I_0}$ linear unabhängig ist. Wir untersuchen also die Linearkombination

$$\sum_{i\in I_0} \alpha_i \, v_i = 0.$$

Diese wird erreicht durch die Wahl von $\alpha_i = 0$ für alle $i \in I_0$. Nach Voraussetzung ist das auch die einzig mögliche Wahl der Koeffizienten. Das heißt aber, dass $(v_i)_{i\in I_0}$ linear unabhängig ist. Da I_0 eine beliebige endliche Teilmenge von I war, ist die gesamte Familie $(v_i)_{i\in I}$ linear unabhängig.

Der Beweis für Mengen geht analog. □

Lemma 13.7 (lineare Abhängigkeit bedeutet Redundanz)**.**
Es sei V ein Vektorraum und $(v_i)_{i \in I}$ eine nichtleere Familie von Vektoren aus V. Dann sind äquivalent:

(i) $(v_i)_{i \in I}$ ist linear abhängig.

(ii) Es gibt ein $j \in I$, sodass gilt:
$$\langle (v_i)_{i \in I \setminus \{j\}} \rangle = \langle (v_i)_{i \in I} \rangle.$$

Ein analoges Resultat gilt für nichtleere Mengen von Vektoren aus V.

Beachte: Ist ein Erzeugendensystem eines Vektorraumes linear abhängig, so kann man mindestens ein Element aus dem Erzeugendensystem entfernen, ohne den erzeugten Raum zu verkleinern.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Es sei $(v_i)_{i \in I}$ linear abhängig, d. h., es gibt eine endliche Teilmenge $I_0 \subseteq I$ und Koeffizienten $\alpha_i \in K$, $i \in I_0$, die nicht alle gleich Null sind, sodass
$$\sum_{i \in I_0} \alpha_i \, v_i = 0$$
gilt. Es sei $j \in I_0$ ein Index, für den $\alpha_j \neq 0$ gilt. Dann ist
$$\alpha_j \, v_j = - \sum_{i \in I_0 \setminus \{j\}} \alpha_i \, v_i,$$
also auch
$$v_j = -\alpha_j^{-1} \sum_{i \in I_0 \setminus \{j\}} \alpha_i \, v_i = - \sum_{i \in I_0 \setminus \{j\}} \alpha_j^{-1} \alpha_i \, v_i. \tag{$*$}$$
Das zeigt $v_j \in \langle (v_i)_{i \in I \setminus \{j\}} \rangle$.

Es sei nun $v \in \langle (v_i)_{i \in I} \rangle$ beliebig. Dann gibt es eine endliche Teilmenge $I_1 \subseteq I$ und Koeffizienten $\beta_i \in K$, $i \in I_1$, sodass
$$v = \sum_{i \in I_1} \beta_i \, v_i$$
gilt. Wir wollen zeigen, dass wir v auch ohne Verwendung von v_j linearkombinieren können. Falls $j \notin I_1$ liegt (also v_j ohnehin nicht verwendet wird), dann ist $\langle (v_i)_{i \in I \setminus \{j\}} \rangle$ klar. Falls jedoch $j \in I_1$ liegt, dann ersetze v_j durch ($*$):
$$\begin{aligned} v &= \sum_{i \in I_1} \beta_i \, v_i \\ &= \sum_{i \in I_1 \setminus \{j\}} \beta_i \, v_i + \beta_j \, v_j \\ &= \sum_{i \in I_1 \setminus \{j\}} \beta_i \, v_i - \sum_{i \in I_0 \setminus \{j\}} \beta_j \, \alpha_j^{-1} \alpha_i \, v_i. \end{aligned}$$
Dies ist eine Darstellung von v als Linearkombination aus $(v_i)_{i \in I}$ ohne Verwendung von v_j. Insgesamt gilt also $v \in \langle (v_i)_{i \in I \setminus \{j\}} \rangle$ und damit Aussage (ii).

Aussage (ii) $\Rightarrow$ Aussage (i): Es sei $j \in I$ ein Index, sodass $\langle (v_i)_{i \in I \setminus \{j\}} \rangle = \langle (v_i)_{i \in I} \rangle$ gilt. Dann ist insbesondere $v_j \in \langle (v_i)_{i \in I \setminus \{j\}} \rangle$, d. h., es gibt eine endliche Teilmenge $I_0 \subseteq I$ und Koeffizienten $\alpha_i \in K$, $i \in I_0$, sodass gilt:
$$v_j = \sum_{i \in I_0} \alpha_i \, v_i.$$

Das heißt aber auch

$$\sum_{i \in I_0} \alpha_i \, v_i - 1 \, v_j = 0,$$

d. h., $(v_i)_{i \in I}$ ist linear abhängig.

Der Beweis für Mengen geht analog. □

Im Folgenden interessieren wir uns vor allem für linear unabhängige Erzeugendensysteme, also solche ohne Redundanz.

Definition 13.8 (Basis)**.**
Es sei V ein Vektorraum.

(i) Eine Teilmenge $B \subseteq V$ heißt eine **Basis** (englisch: basis) von V, wenn B linear unabhängig ist und $\langle B \rangle = V$ gilt.

(ii) Eine Familie B von Vektoren aus V heißt eine **Basis** (englisch: basis) von V, wenn B linear unabhängig ist und $\langle B \rangle = V$ gilt.

Beachte: Eine Basis ist also ein linear unabhängiges Erzeugendensystem.

Beispiel 13.9 (Basis)**.**

(i) $\emptyset$ ist die einzige Basis des Nullraumes $\{0\}$ über jedem Körper K.

(ii) Die Menge $E := \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}, \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \right\}$ ist ein Erzeugendensystem des $\mathbb{R}$-Vektorraumes $\mathbb{R}^2$, jedoch keine Basis, da sie linear abhängig ist; siehe Beispiel 13.5. Wenn wir ein beliebiges Element aus E entfernen, so erhalten wir eine Basis von $\mathbb{R}^2$.

(iii) Im Standardvektorraum K^n über einem Körper K (Beispiel 12.3) ist

$$\{e_1, \dots, e_n\} \text{ mit } e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{-ter Eintrag} \tag{13.4}$$

eine Basis, genannt die **kanonische Basis** (englisch: canonical basis), **Standardbasis** (englisch: standard basis) oder **Einheitsbasis** (englisch: unit basis) von K^n.

(iv) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Dann ist die Menge der Monome $E = \{1, t, t^2, \dots\}$ eine Basis von $K[t]$. Die Monome $E = \{1, t, \dots, t^n\}$ bilden eine Basis von $K_n[t]$, dem Unterraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$.

Ende der Vorlesung 17

Satz 13.10 (Charakterisierung von Basen)**.**
Es sei V ein Vektorraum und $B \subseteq V$. Dann sind äquivalent:

(i) B ist eine Basis von V.

(ii) B ist eine maximale linear unabhängige Teilmenge von V.[12] Das heißt: B ist linear unabhängig, und jede echte Obermenge von B ist linear abhängig.

(iii) B ist ein minimales Erzeugendensystem von V.[13] Das heißt: B ist ein Erzeugendensystem, und jede echte Teilmenge von B ist kein Erzeugendensystem.

(iv) Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise (bis auf Summanden mit Nullkoeffizienten) aus Elementen von B linearkombinieren.

Ein analoge Charakterisierung der Basiseigenschaft gilt für Familien B in V.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B \rangle = V$. Für einen beliebigen Vektor $v \in V \setminus B$ gilt $\langle B \cup \{v\} \rangle = V$. Aus Lemma 13.7 („Redundanz bedeutet lineare Abhängigkeit") folgt nun, dass $B \cup \{v\}$ linear abhängig ist.

Aussage (ii) $\Rightarrow$ Aussage (i): Es sei B eine maximale linear unabhängige Teilmenge von V. Zu zeigen ist, dass B ganz V erzeugt. Es sei dazu $v \in V$ beliebig. Nach Definition von $\langle B \rangle$ ist klar, dass $\langle B \rangle \supseteq B$ gilt. Wir können also von $v \in V \setminus B$ und außerdem von $v \neq 0$ ausgehen. (**Quizfrage 13.1:** Warum?) Nach Voraussetzung ist $B \cup \{v\}$ linear abhängig. Es ~~gibt also eine endliche Teilmenge B_0 von B, sodass $B \cup \{v\}$ linear abhängig ist, d. h., es~~ existieren also $n \in \mathbb{N}_0$, $v_i \in B$ und $\alpha_i \in K$, $i = 1, \ldots, n$, sowie $\alpha \in K$, sodass gilt:

$$\sum_{i=1}^{n} \alpha_i \, v_i + \alpha \, v = 0.$$

Dabei ist $\alpha \neq 0$, denn sonst wäre bereits B linear abhängig, was der Voraussetzung widerspricht. Wir erhalten also

$$v = -\sum_{i=1}^{n} \alpha^{-1} \alpha_i \, v_i,$$

d. h., v lässt sich in der Tat aus Elementen von B linearkombinieren. Damit ist $\langle B \rangle = V$ gezeigt.

Aussage (i) $\Rightarrow$ Aussage (iii): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B \rangle = V$. Aus Lemma 13.7 („Redundanz bedeutet lineare Abhängigkeit") folgt nun, dass B keine redundanten Elemente enthält, dass also für alle $v \in B$ gilt: $\langle B \setminus \{v\} \rangle \subsetneq V$.

Aussage (iii) $\Rightarrow$ Aussage (i): Nach Voraussetzung haben wir $\langle B \rangle = V$, und für alle $v \in B$ gilt: $\langle B \setminus \{v\} \rangle \subsetneq V$. Aus Lemma 13.7 („Redundanz bedeutet lineare Abhängigkeit") folgt daher, dass B linear unabhängig ist, also eine Basis.

Aussage (i) $\Rightarrow$ Aussage (iv): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B \rangle = V$. Aus Lemma 13.6 folgt, dass sich jedes $v \in \langle B \rangle = V$ in i. W. eindeutiger Weise aus Elementen von B linearkombinieren lässt.

Aussage (iv) $\Rightarrow$ Aussage (i): Nach Voraussetzung lässt sich jeder Vektor $v \in V$ auf eindeutige Weise (bis auf Summanden mit Nullkoeffizienten) aus Elementen von B linearkombinieren. Also ist $\langle B \rangle = V$, und aus Lemma 13.6 folgt, dass B linear unabhängig ist, also eine Basis von V. □

---

[12] Genauer: B ist ein maximales Element bzgl. der Mengeninklusion (Definition 5.10) in der Menge der linear unabhängigen Teilmengen von V.

[13] Genauer: B ist ein minimales Element bzgl. der Mengeninklusion (Definition 5.10) in der Menge der Erzeugendensysteme von V.

Wir geben nun einige wichtige Resultate zur Existenz von Basen an. Das Hauptresultat — der nachfolgende Basisergänzungssatz — besagt, dass zwischen einer linear unabhängigen, aber möglicherweise zu kleinen Menge (der erzeugte Raum ist nicht alles), und einem Erzeugendensystem, das aber möglicherweise zu groß (linear abhängig) ist, immer eine Basis liegt.

Satz 13.11 (Basisergänzungssatz[14]).
Es sei V ein Vektorraum.

(i) Es sei A eine linear unabhängige Menge von Vektoren aus V und E ein Erzeugendensystem von V mit der Eigenschaft $A \subseteq E$. Dann existiert eine Basis B von V mit $A \subseteq B \subseteq E$.

(ii) Es sei $A = (v_i)_{i \in I_A}$ eine linear unabhängige Familie von Vektoren aus V und $E = (v_i)_{i \in I_E}$ ein Erzeugendensystem von V mit der Eigenschaft $I_A \subseteq I_E$. Dann existiert eine Basis $B = (v_i)_{i \in I_B}$ von V mit $I_A \subseteq I_B \subseteq I_E$.

Beweis. Wir führen den Beweis für Mengen, also den Beweis von Aussage (i).

Wir betrachten die Menge aller linear unabhängigen Teilmengen zwischen A und E, also

$$\mathcal{D} := \{D \subseteq V \mid A \subseteq D \subseteq E, \text{ sodass } D \text{ linear unabhängig ist}\} \subseteq \mathcal{P}(E) \subseteq \mathcal{P}(V).$$

$\mathcal{D}$ ist mit der Mengeninklusion eine halbgeordnete Menge. Wegen $A \in \mathcal{D}$ ist $\mathcal{D} \neq \emptyset$. Ziel ist die Anwendung des Lemmas von Zorn 6.35.

Schritt 1: Jede totalgeordnete Teilmenge $\mathcal{C} \subseteq \mathcal{D}$ besitzt eine obere Schranke S in $\mathcal{D}$:

Wir zeigen, dass $S := \bigcup_{C \in \mathcal{C}} C$ eine obere Schranke (Definition 5.10) der Teilmenge $\mathcal{C}$ in $\mathcal{D}$ ist.

Dazu zeigen wir zunächst, dass S überhaupt Element von $\mathcal{D}$ ist:

(a) Für alle $C \in \mathcal{C} \subseteq \mathcal{D}$ gilt $A \subseteq C \subseteq E$, also auch $A \subseteq \bigcup_{C \in \mathcal{C}} C = S \subseteq E$.

(b) Weiter ist S linear unabhängig, denn: Es sei $\{c_1, \dots, c_n\} \subseteq S$ eine endliche Teilmenge. Für alle c_i existiert $C_i \in \mathcal{C}$ mit $c_i \in C_i$. $\mathcal{C}$ ist aber totalgeordnete Teilmenge, also existiert ein Maximum C_k der endlichen Teilmenge $\{C_1, \dots, C_n\}$ in $\mathcal{C}$. Folglich gilt $C_i \subseteq C_k$ für alle $i = 1, \dots, n$. Damit ist $\{c_1, \dots, c_n\} \subseteq \bigcup_{i=1}^n C_i = C_k$. Dabei ist $C_k \in \mathcal{C} \subseteq \mathcal{D}$ linear unabhängig. Also ist nach Lemma 13.4 auch die Teilmenge $\{c_1, \dots, c_n\}$ linear unabhängig.

Schließlich zeigt $C \subseteq \bigcup_{C \in \mathcal{C}} C = S$ für alle $C \in \mathcal{C}$, dass S tatsächlich eine obere Schranke von $\mathcal{C}$ in $\mathcal{D}$ ist.

Schritt 2: Das Lemma von Zorn 6.35 zeigt nun, dass ein maximales Element B von $\mathcal{D}$ existiert. Das heißt definitionsgemäß: B ist linear unabhängig und erfüllt $A \subseteq B \subseteq E$. Es bleibt zu zeigen, dass B tatsächlich ganz V erzeugt.

Falls $B = E$ gilt, so ist $V = \langle E \rangle = \langle B \rangle$ und der Beweis erbracht. Andernfalls gibt es ein $a \in E \setminus B$, also gilt $B \cup \{a\} \supsetneq B$. B ist aber ein maximales Element von $\mathcal{D}$, also kann $B \cup \{a\}$ nicht zu $\mathcal{D}$ gehören. Wegen $A \subseteq B \cup \{a\} \subseteq E$ muss das daran liegen, dass $B \cup \{a\}$ linear abhängig ist. Aus Lemma 13.7 folgt also $\langle B \cup \{a\} \rangle = \langle B \rangle$ und insbesondere $a \in \langle B \rangle$. Da dieses Argument für jedes $a \in E \setminus B$ gilt, folgt $E \setminus B \subseteq \langle B \rangle$, und natürlich gilt auch $B \subseteq \langle B \rangle$. Es folgt $E \subseteq \langle B \rangle$. Der Übergang zur linearen Hülle zeigt $V = \langle E \rangle \subseteq \big\langle \langle B \rangle \big\rangle = \langle B \rangle$, aber natürlich gilt auch $\langle B \rangle \subseteq V$, also $\langle B \rangle = V$. □

---

[14] englisch: basis extension theorem

Es folgen drei unmittelbare Folgerungen als Spezialfälle des Basisergänzungssatzes 13.11, formuliert nur in der Version für Mengen:

Folgerung 13.12 (Basisexistenzsatz: $A = \emptyset$ und $E = V$)**.**
Jeder Vektorraum V besitzt eine Basis.

Folgerung 13.13 (Basisauswahlsatz: $A = \emptyset$)**.**
Aus jedem Erzeugendensystem E eines Vektorraumes V lässt sich eine Basis auswählen.

Folgerung 13.14 (Basisergänzungssatz: $E = V$)**.**
Jede linear unabhängige Menge A eines Vektorraumes V kann zu einer Basis erweitert werden.

Bemerkung 13.15 (zum Basisergänzungssatzes 13.11)**.**
Der Beweis des Basisergänzungssatzes 13.11 und seiner Folgerungen 13.12 bis 13.14 ist nicht konstruktiv, d. h., wir können ihn nicht zur Grundlage eines Verfahrens machen, um eine Basis zu konstruieren. Beispielsweise können wir keine Basis von $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum (Beispiel 12.3) angeben.

Wenn der Vektorraum V jedoch endlich erzeugt ist, wenn es also ein endliches Erzeugendensystem gibt, dann lässt sich der Basisergänzungssatz 13.11 konstruktiv und ohne Verwendung des Zornschen Lemmas beweisen, indem man die linear unabhängige Menge A Schritt für Schritt durch einzelne Elemente von E ergänzt oder alternativ Schritt für Schritt einzelne Elemente von $E \setminus A$ entfernt.

Wir kommen nun zum wichtigen Begriff der Dimension, der in gewissem Sinne die „Größe“ eines Vektorraumes beschreibt. Aus Gründen der Übersichtlichkeit formulieren wir die Definition nur Basen, die Mengen sind, nicht für Familien.

Definition 13.16 (Dimension eines Vektorraumes)**.**
Es sei V ein Vektorraum.

(i) Wenn V eine Basis B der endlichen Kardinalität $n \in \mathbb{N}_0$ besitzt, so sagen wir, V habe **endliche Dimension** (englisch: finite dimension), genauer: die **Dimension** (englisch: dimension) n, in Symbolen: $\dim V = n$.

(ii) Wenn V keine Basis endlicher Kardinalität besitzt, so sagen wir, V habe **unendliche Dimension** (englisch: infinite dimension), in Symbolen: $\dim V = \infty$.

Zur Verdeutlichung, welcher Körper K verwendet wird, schreiben wir manchmal auch $\dim_K V$.

Bevor wir mit dem Begriff der Dimension arbeiten, muss noch sichergestellt werden, dass dieser wohldefiniert ist, denn ein Vektorraum besitzt i. A. viele verschiedene Basen. Wir werden dazu beweisen, dass in dem Fall, dass ein Vektorraum eine Basis endlicher Kardinalität besitzt, alle seine Basen endliche Kardinalität haben, und zwar alle dieselbe.

Lemma 13.17 (Austauschlemma)**.**
Es sei V ein Vektorraum über dem Körper K und die endliche Menge $B = \{v_1, \ldots, v_n\}$ eine Basis von V mit $n \in \mathbb{N}$. Ist $w = \sum_{i=1}^n \alpha_i \, v_i$ mit Koeffizienten $\alpha_i \in K$ und gilt $\alpha_j \neq 0$ für ein gewisses $j \in [\![1, n]\!]$, dann ist auch $B_0 \coloneqq \{v_1, \ldots, v_{j-1}, w, v_{j+1}, \ldots, v_n\}$ eine Basis von V.

Ein analoges Resultat gilt, wenn die endliche Familie B eine Basis von V ist.

Beweis. Da es bei einer Basis auf die Reihenfolge der Elemente nicht ankommt, nehmen wir aus Bequemlichkeit und o. B. d. A. an, dass $j = 1$ ist. Aus $w = \sum_{i=1}^n \alpha_i \, v_i$ folgt

$$v_1 = \alpha_1^{-1}\Big(w - \sum_{i=2}^n \alpha_i \, v_i\Big). \tag{$*$}$$

Schritt 1: Wir zeigen: $\langle B_0 \rangle = V$.

Es sei dazu $v \in V$. Da B eine Basis ist, gibt es Koeffizienten $\beta_1, \dots, \beta_n \in K$, sodass $v = \sum_{i=1}^n \beta_i \, v_i$ gilt. Durch Einsetzen von ($*$) folgt

$$\begin{aligned} v &= \beta_1 \, \alpha_1^{-1}\Big(w - \sum_{i=2}^n \alpha_i \, v_i\Big) + \sum_{i=2}^n \beta_i \, v_i \\ &= \beta_1 \, \alpha_1^{-1} w - \beta_1 \, \alpha_1^{-1} \sum_{i=2}^n \alpha_i \, v_i + \sum_{i=2}^n \beta_i \, v_i && \text{nach Distributivgesetz (10.1a) in } K \\ &= \beta_1 \, \alpha_1^{-1} w + \sum_{i=2}^n \big(\beta_i - \beta_1 \, \alpha_1^{-1} \alpha_i\big) \, v_i && \text{nach Kommutativ- und Distributivgesetz (10.1b).} \end{aligned}$$

Damit ist gezeigt, dass in der Tat $\langle B_0 \rangle = \langle w, v_2, \dots, v_n \rangle = V$ gilt.

Schritt 2: Wir zeigen: B_0 ist linear unabhängig.

Wir betrachten dazu

$$\begin{aligned} & \beta_1 \, w + \sum_{i=2}^n \beta_i \, v_i = 0 \\ \Rightarrow \quad & \beta_1 \sum_{i=1}^n \alpha_i \, v_i + \sum_{i=2}^n \beta_i \, v_i = 0 \\ \Rightarrow \quad & \beta_1 \, \alpha_1 \, v_1 + \sum_{i=2}^n \big(\beta_1 \, \alpha_i + \beta_i\big) \, v_i = 0. \end{aligned}$$

Da $B = \{v_1, \dots, v_n\}$ linear unabhängig ist, ist das nur möglich, wenn alle Koeffizienten gleich Null sind, also

$$\beta_1 \, \alpha_1 = 0 \quad \text{und} \quad \beta_1 \, \alpha_i + \beta_i = 0 \text{ für } i = 2, \dots, n.$$

Wegen $\alpha_1 \neq 0$ muss $\beta = 0$ sein, woraus dann weiter $\beta_2 = \ldots = \beta_n = 0$ folgt. Das heißt aber, dass $B_0 = \{w, v_2, \dots, v_n\}$ linear unabhängig ist. □

Satz 13.18 (**Austauschsatz von Steinitz**[15]).

Es sei V ein Vektorraum und die endliche Menge $B = \{v_1, \dots, v_n\}$ eine Basis von V mit $\#B = n \in \mathbb{N}_0$. Ist $A = \{a_1, \dots, a_m\}$ eine linear unabhängige Menge in V mit $\#A = m \in \mathbb{N}_0$, dann gilt:

(*i*) $m \leqslant n$.

(*ii*) Es gibt eine $(n - m)$-elementige Teilmenge D von B, sodass $B_0 := A \cup D$ ebenfalls eine Basis von V ist. Es gilt $\#B_0 = n$.

---

[15] englisch: Steinitz exchange theorem

Beweis. Wir führen einen Induktionsbeweis nach der Mächtigkeit $m = \#A$. Den Induktionsanfang setzen wir bei $m = 0$. Dann ist $A = \emptyset$, und Aussage (i) gilt wegen $m = 0 \leqslant n$, und Aussage (ii) gilt mit $D = B$.

Es sei nun $m \geqslant 1$, und es gelten Aussagen (i) und (ii) bereits für $m-1$. Da $\{a_1, \dots, a_m\}$ linear unabhängig ist, ist auch $\{a_1, \dots, a_{m-1}\}$ linear unabhängig. Nach Induktionsannahme gilt $m - 1 \leqslant n$, und es existiert $D = \{v_{i_m}, \dots, v_{i_n}\} \subseteq B$, sodass $B_1 \coloneqq \{a_1, \dots, a_{m-1}, v_{i_m}, \dots v_{i_n}\}$ eine Basis von V ist.

Falls nun $m - 1 = n$ wäre, also $D = \emptyset$, dann wäre bereits $\{a_1, \dots a_{m-1}\}$ eine Basis von V. Nach dem Satz 13.10 über die Charakterisierung von Basen hieße das aber, dass $\{a_1, \dots a_m\}$ linear abhängig wäre, im Widerspruch zur Voraussetzung. Es gilt also $m - 1 < n$, also $m \leqslant n$. Damit ist der Induktionsschritt für Aussage (i) gezeigt. Da B_1 eine Basis von V ist, können wir jeden Vektor, insbesondere a_m, durch die Basiselemente linearkombinieren. Es gibt also Skalare α_j, $j = 1, \dots n$, sodass gilt:

$$a_m = \sum_{j=1}^{m-1} \alpha_j \, a_j + \sum_{j=m}^{n} \alpha_j \, v_{i_j}.$$

Wären alle $\alpha_m = \alpha_{m+1} = \dots \alpha_n = 0$, so würde das die lineare Abhängigkeit von $A = \{a_1, \dots, a_m\}$ zeigen, im Widerspruch zur Voraussetzung. Demzufolge gibt es einen Index $j \in [\![m, n]\!]$ mit $\alpha_j \neq 0$. Nach dem Austauschlemma 13.17 ist $B_0 = B_1 \setminus \{v_{i_j}\} \cup \{a_m\}$ eine Basis von V. Die Kardinalität von B_0 ist $\#B_0 \leqslant \#B_1 - 1 + 1 \leqslant n$. Wäre $a_m \in B_1 \setminus \{v_{i_j}\}$, dann würde aus

$$0 = \sum_{j=1}^{m-1} \alpha_j \, a_j + \sum_{j=m}^{n} \alpha_j \, v_{i_j} - a_m$$

folgen, das B_1 linear abhängig ist, im Widerspruch zur Basiseigenschaft von B_1. Somit folgt $\#B_0 = n$, was den Induktionsschritt für Aussage (ii) zeigt. □

Folgerung 13.19 (endliche Basen sind gleichmächtig)**.**
Es sei V ein Vektorraum.

(i) Wenn V endlich erzeugt ist, dann ist jede Basis von V endlich, und alle Basen haben dieselbe Mächtigkeit.

(ii) Wenn V nicht endlich erzeugt ist, dann ist jede Basis von V unendlich.

Beweis. Wir führen den Beweis für Mengen.

Aussage (i): Wenn V endlich erzeugt ist, dann gibt es ein endliches Erzeugendensystem und nach Basisergänzungssatz 13.11 damit auch eine endliche Basis B von V, sagen wir mit Mächtigkeit $\#B = n \in \mathbb{N}_0$. Es sei B_0 eine weitere (möglicherweise unendliche) Basis von V. Insbesondere jede endliche Teilmenge $B_1 \subseteq B_0$ ist dann ebenfalls linear unabhängig, und nach Satz 13.18 ist $\#B_1 \leqslant n$. Damit muss B_0 selbst endlich sein mit $\#B_0 \leqslant n = \#B$. Durch Tausch der Rollen von B und B_0 folgt auch $\#B \leqslant \#B_0$, also zusammen $\#B = \#B_0$.

Aussage (ii): Wäre B eine endliche Basis, dann wäre B auch ein endliches Erzeugendensystem, und V wäre endlich erzeugt, im Widerspruch zur Voraussetzung. □

Bemerkung 13.20 (Dimensionsbegriff für Vektorräume)**.**

(i) Folgerung 13.19 zeigt, dass der Dimensionsbegriff aus Definition 13.16 wohldefiniert ist.

(ii) Der Beweis von Folgerung 13.19 verwendet den Basisergänzungssatz 13.11, jedoch nur die Version für endlich-dimensionale (endlich erzeugte) Vektorräume, die ohne das Zornsche Lemma und damit ohne das Auswahlaxiom auskommt.

Beispiel 13.21 (Dimension eines Vektorraumes).

(i) Der „Standardvektorraum K^n der Dimension n“ über einem Körper K (Beispiel 12.3) hat tatsächlich die Dimension $n \in \mathbb{N}$.

(ii) Es gilt $\dim_{\mathbb{R}} \mathbb{R} = 1$ und $\dim_{\mathbb{Q}} \mathbb{R} = \infty$.

(iii) Es gilt $\dim_{\mathbb{C}} \mathbb{C} = 1$ und $\dim_{\mathbb{R}} \mathbb{C} = 2$. Eine Basis für $\dim_{\mathbb{R}} \mathbb{C}$ ist $\{1, i\}$.

(iv) Der Nullraum $\{0\}$ ist über jedem Körper der einzige Vektorraum der Dimension 0.

(v) Der Polynomraum $(K[t], +, \cdot)$ über einem Körper $(K, +, \cdot)$ hat unendliche Dimension, da $B = \{1, t, t^2, \dots\}$ eine (abzählbar) unendliche Basis von $K[t]$ ist. Die Monome $B = \{1, t, \dots, t^n\}$ bilden eine Basis von $K_n[t]$, dem Unterraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$. Also gilt $\dim K_n[t] = n + 1$.

Folgerung 13.22 (Dimension, Unterräume und lineare Unabhängigkeit).
Es sei V ein Vektorraum der Dimension $n \in \mathbb{N}_0$.

(i) Ist $A \subseteq V$ eine linear unabhängige Teilmenge, dann gilt $\# A \leqslant n$.

(ii) $A \subseteq V$ ist genau dann eine Basis von V, wenn A linear unabhängig ist und $\# A = n$ gilt.

(iii) Für jeden Unterraum U von V gilt: $0 \leqslant \dim U \leqslant \dim V$.

(iv) Für jeden Unterraum U von V gilt $U = V$ genau dann, wenn $\dim U = \dim V$ ist.

Beweis. Aussage (i): Nach Basisergänzungssatz 13.11 existiert eine Basis B von V mit $A \subseteq B$. Nach Folgerung 13.19 ist $\# B = n$ und daher $\# A \leqslant n$.

Aussage (ii): Ist A eine Basis von V, dann ist A definitionsgemäß linear unabhängig, und nach Folgerung 13.19 gilt $\# A = \dim V = n$. Ist umgekehrt A linear unabhängig und gilt $\# A = n$, so gilt für jede Basis $B \supseteq A$ von V einerseits $\# B \geqslant \# A$, andererseite aber $\# B = \dim V = n$. Also muss $B = A$ sein, d. h., A ist bereits eine Basis.

Aussage (iii): Ist A eine Basis des Unterraumes U von V, dann ist A linear unabhängige Teilmenge von U und damit auch von V. Aus Aussage (i) folgt $\dim U = \# A \leqslant n = \dim V$.

Aussage (iv): Ist $U = V$, dann gilt $\dim U = \dim V$. Nun gelte andererseits $\dim U = \dim V$, und es sei A eine Basis von U. Dann ist A linear unabhängige Teilmenge von U und damit auch von V. Es gilt $\# A = \dim U = \dim V = n$. Aus Aussage ($ii$) folgt, dass A auch eine Basis von V ist, also gilt $U = \langle A \rangle = V$. □

Ende der Vorlesung 18

---

§ 14 SUMMEN VON UNTERRÄUMEN

Literatur: Bosch, 2014, Kapitel 1, Fischer, Springborn, 2020, Kapitel 2.6

§ 14.1 SUMMEN VON ZWEI UNTERRÄUMEN

Aus Lemma 12.11 wissen wir, dass der Durchschnitt $U \cap W$ zweier Unterräume U, W eines Vektorraumes V wieder ein Vektorraum ist. Die Vereinigung $U \cup W$ ist jedoch i. A. kein Unterraum von V.[16]

Es ist naheliegend, statt $U \cup W$ den kleinsten Unterraum von V zu betrachten, der $U \cup W$ enthält, also $\langle U \cup W \rangle$.

Lemma 14.1 (die lineare Hülle der Vereinigung zweier Unterräume ist die Summe.)**.**
Es sei V ein Vektorraum und U, W zwei Unterräume von V. Dann gilt

$$\langle U \cup W \rangle = U + W. \tag{14.1}$$

Wir bezeichnen den Unterraum $U + W$ als die **Summe der Unterräume** U und W (englisch: sum of two subspaces). (**Quizfrage 14.1:** Wie ist der Ausdruck $U + W$ zu verstehen?)

Beweis. Aus Satz 12.13 wissen wir, dass $\langle U \cup W \rangle$ übereinstimmt mit der Menge M aller Linearkombinationen von $U \cup W$. Wir zeigen nun, dass $M = U + W$ gilt. In der Tat sind die Elemente $u + w$ von $U + W$ auch Elemente von M, also $U + W \subseteq M$. Ist umgekehrt $v \in M$, dann hat v eine Darstellung der Form

$$v = \sum_{i=1}^{n} \alpha_i \, u_i + \sum_{j=1}^{m} \beta_j \, w_j$$

mit $n, m \in \mathbb{N}_0$, $\alpha_i, \beta_j \in K$ und $u_i \in U$ sowie $w_j \in W$. Da U und W Unterräume sind, ergibt die erste Summe wieder ein Element von U, und die zweite Summe ergibt ein Element von W. Das zeigt $M \subseteq U + W$, also insgesamt $M = U + W$. □

Bemerkung 14.2 (Ordnung auf der Menge aller Unterräume)**.**
Die Mengeninklusion ist eine Halbordnung auf der Menge aller Unterräume eines gegebenen (möglicherweise unendlich-dimensionalen) Vektorraumes V. Sie stimmt überein mit der Halbordnung „ist Unterraum von". Für je zwei Unterräume U und W ist $U \cap W$ das Infimum von $\{U, W\}$ (Definition 5.10) und $U + W$ das Supremum von $\{U, W\}$. Genau dann, wenn $U \subseteq W$ oder $W \subseteq U$ gilt, ist das Infimum ein Minimum und das Supremum ein Maximum.

Satz 14.3 (Dimension der Summe von zwei Unterräumen)**.**
Es seien V ein Vektorraum und U, W zwei endlich-dimensionale Unterräume von V. Dann gilt

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W). \tag{14.2}$$

---

[16] Tatsächlich gilt: $U \cup W$ ist genau dann ein Unterraum, wenn $U \subseteq W$ oder $W \subseteq U$ gilt (Hausaufgabe 8.3). Ein analoges Resultat gilt auch für Untergruppen (Hausaufgabe 5.1), Unterringe und Unterkörper.

Beweis. $U \cap W$ ist ebenfalls ein endlich-dimensionaler Unterraum von V, besitzt also eine endliche Basis $\{v_1, \dots, v_m\}$ mit $m = \dim(U \cap W) \in \mathbb{N}_0$. Nach dem Basisergänzungssatz 13.11 kann diese Basis zu einer Basis von U bzw. einer Basis von W ergänzt werden. Es gibt also $\{u_1, \dots, u_k\} \subseteq U$ und $\{w_1, \dots, w_\ell\} \subseteq W$ mit $k, \ell \in \mathbb{N}_0$, sodass

$$\begin{aligned} B_U &\coloneqq \{v_1, \dots, v_m,\ u_1, \dots, u_k\} && \text{Basis von } U \\ B_W &\coloneqq \{v_1, \dots, v_m,\ w_1, \dots, w_\ell\} && \text{Basis von } W \end{aligned}$$

ist. Wir zeigen nun, dass $B \coloneqq \{v_1, \dots, v_m,\ u_1, \dots, u_k,\ w_1, \dots, w_\ell\}$ eine Basis von $U + W$ ist. Wegen $B = B_U \cup B_W$ ist B ein Erzeugendensystem von $U + W$. Die lineare Unabhängigkeit von B zeigen wir wie folgt: Wir setzen die Linearkombination

$$\sum_{i=1}^m \alpha_i\, v_i + \sum_{i=1}^k \beta_i\, u_i + \sum_{i=1}^\ell \gamma_i\, w_i = 0$$

an mit Koeffizienten $\alpha_i, \beta_i, \gamma_i \in K$. Definieren wir $u \coloneqq \sum_{i=1}^m \alpha_i\, v_i + \sum_{i=1}^k \beta_i\, u_i \in U$, so gilt

$$u = \sum_{i=1}^\ell (-\gamma_i)\, w_i \in W,$$

also $u \in U \cap W$. Wir haben also

$$\begin{aligned} \text{einerseits} \quad & u \in U && = \langle v_1, \dots, v_m,\ u_1, \dots, u_k \rangle \\ \text{und andererseits} \quad & u \in U \cap W && = \langle v_1, \dots, v_m \rangle. \end{aligned}$$

Aus der Eindeutigkeit der Darstellung (Lemma 13.6) folgt $\beta_1 = \ldots = \beta_k = 0$. Es folgt also

$$\sum_{i=1}^m \alpha_i\, v_i + \sum_{i=1}^\ell \gamma_i\, w_i = 0,$$

und da $B_W = \{v_1, \dots, v_m,\ w_1, \dots, w_\ell\}$ eine Basis ist, folgt $\alpha_1 = \ldots = \alpha_m = 0$ und $\gamma_1 = \ldots = \gamma_\ell = 0$. Das zeigt die lineare Unabhängigkeit von B, also ist B tatsächlich eine Basis von $U + W$.

Die Behauptung (14.2) folgt nun aus

$$\underbrace{m + k + \ell}_{\dim(U+W)} = \underbrace{m + k}_{\dim(U)} + \underbrace{m + \ell}_{\dim(W)} - \underbrace{m}_{\dim(U \cap W)}.$$

□

Beispiel 14.4 (Summe von zwei Unterräumen).

(*i*) Für die Unterräume

$$U = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle \quad \text{und} \quad W = \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle$$

von $\mathbb{R}^2$ gilt

$$U + W = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle = \mathbb{R}^2 \quad \text{und} \quad U \cap W = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}.$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U + W)}_{2} = \underbrace{\dim(U)}_{1} + \underbrace{\dim(W)}_{1} - \underbrace{\dim(U \cap W)}_{0}.$$

(ii) Für die Unterräume

$$U = \left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle \quad \text{und} \quad W = \left\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle$$

von $\mathbb{R}^3$ gilt

$$U + W = \left\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle = \mathbb{R}^3 \quad \text{und} \quad U \cap W = \left\langle \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle.$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U+W)}_{3} = \underbrace{\dim(U)}_{2} + \underbrace{\dim(W)}_{2} - \underbrace{\dim(U \cap W)}_{1}.$$

(iii) Für die Unterräume

$$U = \langle 1, t^2, t^3, t^5 \rangle \quad \text{und} \quad W = \langle t, t^3, t^4 \rangle$$

von $K_5[t]$ über einem beliebigen Körper $(K, +, \cdot)$ gilt

$$U + W = \langle 1, t, t^2, t^3, t^4, t^5 \rangle = K_5[t] \quad \text{und} \quad U \cap W = \langle t^3 \rangle.$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U+W)}_{6} = \underbrace{\dim(U)}_{4} + \underbrace{\dim(W)}_{3} - \underbrace{\dim(U \cap W)}_{1}.$$

Definition 14.5 (direkte Summe von zwei Unterräumen).
Es seien V ein Vektorraum und U, W zwei Unterräume von V. Die Summe $U + W$ heißt **direkt** (englisch: direct sum), wenn $U \cap W = \{0\}$ gilt, in Symbolen: $U \oplus W$.

Beispiel 14.6 (direkte Summe von zwei Unterräumen).
In Beispiel 14.4 ist nur

$$\left\langle \begin{pmatrix}1\\1\end{pmatrix} \right\rangle \oplus \left\langle \begin{pmatrix}1\\-1\end{pmatrix} \right\rangle = \mathbb{R}^2$$

eine direkte Summe. (**Quizfrage 14.2:** Woran erkennt man das?)

Satz 14.7 (Charakterisierung direkter Summen von zwei Unterräumen).
Es seien V ein Vektorraum und U, W zwei Unterräume von V. Dann sind äquivalent:

(i) $V = U \oplus W$.

(ii) Für alle $v \in V$ existieren eindeutige Vektoren $u \in U$ und $w \in W$, sodass $v = u + w$ gilt.

Sind U und W endlich-dimensional, dann sind diese Aussagen desweiteren äquivalent zu

(iii) $\dim(V) = \dim(U) + \dim(W)$ und $\dim(U \cap W) = 0$.

Beweis. Aussage (i) $\Longrightarrow$ Aussage (ii): $V = U \oplus W$ impliziert $V = U + W$. Für gegebenes $v \in V$ gibt es also Vektoren $u \in U$ und $w \in W$, sodass $v = u + w$ gilt. Gilt nun ebenfalls $v = u' + w'$ für Vektoren $u' \in U$ und $w' \in W$, dann gilt

$$u - u' = w' - w \in U \cap W = \{0\}$$

nach Voraussetzung. Daher muss $u = u'$ und $w = w'$ sein.

Aussage (ii) $\Longrightarrow$ Aussage (i): Aus der Voraussetzung folgt sofort $V = U + W$. Zu zeigen ist $U \cap W = \{0\}$.

Für $v \in U \cap W$ zeigen

$$\begin{aligned} v &= v + 0 && \text{mit } v \in U,\ 0 \in W \\ v &= 0 + v && \text{mit } 0 \in U,\ v \in W \end{aligned}$$

und die Eindeutigkeit der Zerlegung, dass $v = 0$ sein muss, also gilt tatsächlich $U \cap W = \{0\}$.

Aussage (i) $\Longrightarrow$ Aussage (iii): Es gilt

$$\begin{aligned} \dim(V) &= \dim(U + W) && \text{da } V = U + W \text{ nach Voraussetzung} \\ &= \dim(U) + \dim(W) - \dim(U \cap W) && \text{nach Dimensionsformel (14.2)} \\ &= \dim(U) + \dim(W) - 0 && \text{da } U \cap W = \{0\} \text{ nach Voraussetzung.} \end{aligned}$$

Aussage (iii) $\Longrightarrow$ Aussage (i): Unter den Voraussetzungen zeigt die Dimensionsformel (14.2):

$$\dim(V) = \dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W) = \dim(U + W).$$

$U + W$ ist also ein Unterraum von V maximaler Dimension und damit identisch zu V. Außerdem zeigt $\dim(U + W) = 0$, dass $U \cap W = \{0\}$ gilt. □

Satz 14.8 (direkte Summe von zwei Unterräumen und Partitionierung einer Basis)**.**
Es sei V ein Vektorraum. Dann gilt:

(i) Ist B eine Basis von V und $\{B_1, B_2\}$ eine Partition[17] von B, dann gilt $V = \langle B_1 \rangle \oplus \langle B_2 \rangle$.

(ii) Sind U_1, U_2 Unterräume von V mit Basen B_1, B_2 und gilt $V = U_1 \oplus U_2$, so ist $B_1 \cup B_2$ eine Basis von V.

Beweis. Aussage (i): Wir zeigen zunächst $V = \langle B_1 \rangle + \langle B_2 \rangle$. Es gilt

$$\begin{aligned} V &= \langle B \rangle && B \text{ ist Basis von } V \\ &= \langle B_1 \cup B_2 \rangle && \text{nach Voraussetzung} \\ &= \big\langle \langle B_1 \rangle \cup \langle B_2 \rangle \big\rangle && \text{nach Folgerung 12.15} \\ &= \langle B_1 \rangle + \langle B_2 \rangle && \text{nach Lemma 14.1 (lineare Hülle der Vereinigung zweier Unterräume)} \\ &\subseteq V. \end{aligned}$$

Damit gilt überall Gleichheit und insbesondere $\langle B_1 \rangle + \langle B_2 \rangle = V$.

Es bleibt $\langle B_1 \rangle \cap \langle B_2 \rangle = \{0\}$ zu zeigen. Nehmen wir also $v \in \langle B_1 \rangle \cap \langle B_2 \rangle$ an, d. h.

$$v = \sum_{i=1}^{n} \alpha_i \, b_i^1 = \sum_{i=1}^{m} \beta_i \, b_i^2$$

für geeignete endliche Teilmengen $\{b_1^1, \ldots, b_n^1\} \subseteq B_1$ und $\{b_1^2, \ldots, b_m^2\} \subseteq B_2$ und Koeffizienten α_i, β_i. Es folgt

$$0 = \sum_{i=1}^{n} \alpha_i \, b_i^1 + \sum_{i=1}^{m} (-\beta_i) \, b_i^2.$$

Da $B = B_1 \cup B_2$ eine Basis ist, ist auch die Teilmenge $\{b_1^1, \ldots, b_n^1,\ b_1^2, \ldots, b_m^2\}$ linear unabhängig. Daraus folgt $\alpha_1 = \ldots = \alpha_n = \beta_1 = \ldots = \beta_m = 0$. Das heißt aber $v = 0$ und damit $\langle B_1 \rangle \cap \langle B_2 \rangle = \{0\}$.

---

[17] Zur Erinnerung, das heißt $B_1, B_2 \neq \emptyset$, $B = B_1 \cup B_2$ und $B_1 \cap B_2 = \emptyset$, vgl. Definition 5.18. Hier wäre sogar $B_1 = \emptyset$ oder $B_2 = \emptyset$ erlaubt.

Aussage (*ii*): Es seien nun U_1, U_2 Unterräume von V mit Basen B_1, B_2. Wir nehmen $V = U_1 \oplus U_2$ an. Wir müssen zeigen, dass $B_1 \cup B_2$ linear unabhängig ist und ganz V erzeugt. Letzteres folgt aus

$$\begin{aligned}
\langle B_1 \cup B_2 \rangle &= \big\langle \langle B_1 \rangle \cup \langle B_2 \rangle \big\rangle && \text{nach Folgerung 12.15} \\
&= \langle U_1 \cup U_2 \rangle && \text{da } B_1 \text{ Basis von } U_1 \text{ und } B_2 \text{ Basis von } U_2 \text{ ist} \\
&= U_1 + U_2 && \text{nach Lemma 14.1 (lineare Hülle der Vereinigung zweier Unterräume)} \\
&= V && \text{nach Voraussetzung.}
\end{aligned}$$

Es seien nun $\{b^1_1, \dots, b^1_n\} \subseteq B_1$ und $\{b^2_1, \dots, b^2_m\} \subseteq B_2$ endliche Teilmengen mit $n, m \in \mathbb{N}_0$. Wir betrachten die Linearkombination

$$\sum_{i=1}^{n} \alpha_i \, b^1_i + \sum_{i=1}^{m} \beta_i \, b^2_i = 0 \quad \text{bzw.} \quad \sum_{i=1}^{n} \alpha_i \, b^1_i = \sum_{i=1}^{m} (-\beta_i) \, b^2_i .$$

Die erste Linearkombination gehört zu U_1, die zweite zu U_2. Wegen $U_1 \cap U_2 = \{0\}$ ist jede Linearkombination der Nullvektor. Da B_1 und B_2 Basen sind, gilt $\alpha_1 = \ldots = \alpha_n = \beta_1 = \ldots = \beta_m = 0$. Das heißt, dass $B_1 \cup B_2$ in der Tat linear unabhängig ist. □

Folgerung 14.9 (Existenz eines komplementären Unterraumes).
Es seien V ein Vektorraum und U ein Unterraum von V. Dann existiert ein weiterer Unterraum W von V, sodass gilt: $V = U \oplus W$.

Beweis. Es sei B_U eine Basis von U. Aus dem Basisergänzungssatz 13.11 folgt die Existenz einer Basis B von V mit $B_U \subseteq B$. Setzen wir $B_W := B \setminus B_U$ und $W := \langle B_W \rangle$, so ist W nach Satz 14.8 (*i*) ein Unterraum mit der gesuchten Eigenschaft. □

Definition 14.10 (komplementärer Unterraum).
Es seien V ein Vektorraum und U ein Unterraum von V.

(*i*) Ein Unterraum W von V heißt ein **zu U komplementärer Unterraum** (englisch: complementary subspace) oder ein **Komplement** (englisch: complement) von U in V, wenn $V = U \oplus W$ gilt.

(*ii*) Die Dimension $\dim(W)$ eines zu U komplementären Unterraumes W heißt die **Kodimension** (englisch: codimension) von U in V, kurz: $\operatorname{codim}(U)$.

Beachte: Komplementäre Unterräume eines Vektorraumes sind i. A. nicht eindeutig. Nur im Fall $U = V$ ist der einzige zu U komplementäre Unterraum der Nullraum $\{0\}$.

Quizfrage 14.3: Was gilt für $\operatorname{codim}(U)$ in einem endlich-dimensionalen Vektorraum?

Beispiel 14.11 (komplementärer Unterraum).

(*i*) Jeder eindimensionale Unterraum W, der nicht identisch mit $U = \left\langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right) \right\rangle$ ist, ist ein Komplement von U in $\mathbb{R}^2$.

(*ii*) Die komplementären Unterräume des Unterraumes $(\mathbb{R}^\mathbb{N})_c$ der konvergenten Folgen im Vektorraum $(\mathbb{R}^\mathbb{N}, +, \cdot)$, siehe Beispiel 12.9, haben keine einfache Darstellung.

§ 14.2 SUMMEN VON FAMILIEN VON UNTERRÄUMEN

Wir beschäftigen uns abschließend noch mit Summen von einer beliebigen Anzahl von Unterräumen eines Vektorraumes.

Definition 14.12 (Summe einer Familie von Unterräumen).
Es seien V ein Vektorraum und $(U_i)_{i \in I}$ eine nichtleere Familie von Unterräumen von V.

(i) Der Unterraum

$$\sum_{i \in I} U_i := \Big\langle \bigcup_{i \in I} U_i \Big\rangle \tag{14.3}$$

heißt die **Summe der Familie von Unterräumen** $(U_i)_{i \in I}$ (englisch: sum of a family of subspaces). Im Fall $I = [\![1, n]\!]$ schreiben wir auch $U_1 + \cdots + U_n$ oder $\sum_{i=1}^n U_i$.

(ii) Die Summe heißt **direkt** (englisch: direct sum), wenn gilt:

$$U_j \cap \sum_{i \in I \setminus \{j\}} U_i = \{0\} \quad \text{für alle } j \in I. \tag{14.4}$$

Wir schreiben dann $\bigoplus_{i \in I} U_i$. Im Fall $I = [\![1, n]\!]$ schreiben wir auch $U_1 \oplus \cdots \oplus U_n$ oder $\bigoplus_{i=1}^n U_i$.

Beispiel 14.13 (Summe einer Familie von Unterräumen).

(i) Für den Standardvektorraum K^n über einem Körper K mit den Basisvektoren e_i, $i = 1, \ldots, n \in \mathbb{N}$, siehe Beispiel 13.9, gilt

$$K^n = \bigoplus_{i=1}^n \langle e_i \rangle.$$

(ii) Für den Polynomraum $(K[t], +, \cdot)$ über einem Körper K mit der Basis $B = \{1, t, t^2, \ldots\}$, siehe Beispiel 13.21, gilt

$$K[t] = \bigoplus_{i \in \mathbb{N}_0} \langle t^i \rangle.$$

Bemerkung 14.14 (Summe einer Familie von Unterräumen).

(i) Die Elemente der Summe einer Familie $(U_i)_{i \in I}$ von Unterräumen haben die Darstellung

$$\begin{aligned} \sum_{i \in I} U_i &= \Big\{ \sum_{i \in I_0} U_i \,\Big|\, I_0 \subseteq I \text{ ist eine endliche Teilfamilie} \Big\} \\ &= \Big\{ \sum_{i \in I_0} u_i \,\Big|\, I_0 \subseteq I \text{ ist eine endliche Teilfamilie und } u_i \in U_i \text{ für alle } i \in I_0 \Big\}. \end{aligned} \tag{14.5}$$

(ii) Im Fall $\#I = 2$ stimmt die Bedingung (14.4), dass die Summe einer Familie von Unterräumen eine direkte Summe ist, überein mit Definition 14.5. Im Fall $\#I > 2$ reicht es jedoch für die Direktheit der Summe nicht aus, dass an Stelle von (14.4) nur paarweise $U_i \cap U_j = \{0\}$ für $i \neq j$ gefordert wird.

Betrachte zum Beispiel die Unterräume

$$U_1 = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \right\rangle, \quad U_2 = \left\langle \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \right\rangle \quad \text{und} \quad U_3 = \left\langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \right\rangle.$$

Dann gilt $U_i \cap U_j = \{0\}$ für alle $i \neq j$, aber $U_1 \cap (U_2 + U_3) = U_1 \cap \mathbb{R}^2 \supsetneq \{0\}$. Das heißt, die Summe der Unterräume U_1, U_2, U_3 ist nicht direkt.

Satz 14.15 (Charakterisierung direkter Summen von Familien von Unterräumen, vgl. Satz 14.7)**.**
Es seien V ein Vektorraum und $(U_i)_{i \in I}$ eine nichtleere Familie von Unterräumen von V. Dann sind äquivalent:

- (i) $V = \bigoplus_{i \in I} U_i$.
- (ii) Für alle $v \in V$ existiert eine endliche Teilfamilie $I_0 \subseteq I$ und Vektoren $u_i \in U_i$, sodass $v = \sum_{i \in I_0} u_i$ gilt, und diese Darstellung ist (bis auf die Summation von Nullvektoren) eindeutig.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 9.4. □

Satz 14.16 (direkte Summe von Unterräumen und Partitionierung einer Basis, vgl. Satz 14.8)**.**
Es sei V ein Vektorraum. Dann gilt:

- (i) Ist B eine Basis von V und $(B_i)_{i \in I}$ eine Partition von B mit nichtleerer Indexmenge I, dann gilt $V = \bigoplus_{i \in I} \langle B_i \rangle$.
- (ii) Ist $(U_i)_{i \in I}$ eine nichtleere Familie von Unterräumen von V mit Basen B_i, $i \in I$, und gilt $V = \bigoplus_{i \in I} U_i$, so ist $\bigcup_{i \in I} B_i$ eine Basis von V.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 9.4. □

Ende der Vorlesung 19

Ende der Woche 9

Kapitel A Die komplexen Zahlen

Die natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \ldots\}$ oder $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ sind ausreichend, um Objekte zu zählen. Gleichungen wie $x + 2 = 1$ sind jedoch in $\mathbb{N}_0$ nicht lösbar. Dafür benötigen wir die Menge der ganzen Zahlen $\mathbb{Z}$. Gleichungen wie $2\,x = 1$ sind aber auch in $\mathbb{Z}$ nicht lösbar. Dafür benötigen wir die Menge der rationalen Zahlen $\mathbb{Q}$. Gleichungen wie $x^2 = 2$ sind aber auch in $\mathbb{Q}$ nicht lösbar. Dafür benötigen wir die Menge der reellen Zahlen $\mathbb{R}$. Gleichungen wie $x^2 = -1$ sind aber auch in $\mathbb{R}$ nicht lösbar. Dafür benötigen wir die Menge der komplexen Zahlen $\mathbb{C}$.

Die komplexen Zahlen lassen sich aus den reellen Zahlen $\mathbb{R}$ aufbauen. Die Menge $\mathbb{C}$ der komplexen Zahlen besteht aus allen Ausdrücken der Form

$$a + b\,i,$$

wobei $a, b \in \mathbb{R}$ sind und i ein Symbol ist, das nicht in $\mathbb{R}$ enthalten ist.

Die **Addition** (englisch: addition) mit dem Symbol $+$ ist definiert durch

$$(a + b\,i) + (c + d\,i) \coloneqq (a + c) + (b + d)\,i.$$

Aufgrund der Kommutativität von $+$ in $\mathbb{R}$ bildet $(\mathbb{C}, +)$ eine kommutative Halbgruppe. Wir prüfen leicht nach, dass $0 + 0\,i$ neutrales Element in $(\mathbb{C}, +)$ ist und dass $a + b\,i$ und $-a - b\,i \coloneqq (-a) + (-b)\,i$ additive Inverse zueinander sind. Wir schreiben daher auch $-(a + b\,i)$ für $(-a) + (-b)\,i$. Wir haben damit gezeigt: $(\mathbb{C}, +)$ eine abelsche Gruppe.

Wir definieren weiter die **Multiplikation** (englisch: multiplication) mit dem Symbol $\cdot$ durch[1]

$$(a + b\,i) \cdot (c + d\,i) \coloneqq (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)\,i.$$

Motiviert ist diese Definition durch das formale Distributivgesetz $(a + b\,i) \cdot (c + d\,i) = a \cdot c + (b\,i) \cdot c + a \cdot (d\,i) + (b\,i) \cdot (d\,i)$, wobei die Kommutativitäts-Regeln $(b\,i) \cdot c = (b \cdot c)\,i$ und $a \cdot (d\,i) = (a \cdot d)\,i$ und $(b\,i) \cdot (d\,i) = (b \cdot d)\,i^2$ gelten sollen sowie $i^2 = -1$. Aufgrund der Kommutativität von $\cdot$ in $\mathbb{R}$ bildet $(\mathbb{C}, \cdot)$ eine kommutative Halbgruppe. Wir prüfen leicht nach, dass $1 + 0\,i$ neutrales Element in $(\mathbb{C}, \cdot)$ ist und dass $a + b\,i$ und $a/(a^2 + b^2) - b/(a^2 + b^2)\,i$ multiplikative Inverse zueinander sind, solange $a + b\,i \neq 0 + 0\,i$ gilt. Wir schreiben daher auch $(a + b\,i)^{-1}$ für $a/(a^2 + b^2) - b/(a^2 + b^2)\,i$. Wir haben damit gezeigt: $(\mathbb{C} \setminus \{0 + 0\,i\}, \cdot)$ eine abelsche Gruppe.

Weiterhin können wir die (wegen der Kommutativität von $\cdot$ zusammenfallenden) Distributivgesetze

$$\begin{aligned}(a + b\,i) \cdot \big((c + d\,i) + (e + f\,i)\big) &= (a + b\,i) \cdot (c + d\,i) + (a + b\,i) \cdot (e + f\,i)\\ \big((a + b\,i) + (c + d\,i)\big) \cdot (e + f\,i) &= (a + b\,i) \cdot (e + f\,i) + (c + d\,i) \cdot (e + f\,i)\end{aligned}$$

nachprüfen. Nach Definition 10.1 ist damit $(\mathbb{C}, +, \cdot)$ ein Körper.

---

[1] Die Einführung von $\mathbb{C}$ als formale Ausdrücke der Form $a + b\,i$ ist der Einführung von Polynomen in Definition 11.1 nicht unähnlich. Die Besonderheit hier ist aber die Festlegung $i^2 = -1$, die es ermöglicht, jede komplexe Zahl als „Polynom maximal ersten Grades“ in i zu schreiben.

Die Abbildung

$$\mathbb{C} \ni z = a + b\,i \mapsto \overline{z} = a - b\,i \in \mathbb{C}$$

ist ein Körperautomorphismus $(\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$. Es gilt also insbesondere

$$\overline{z + w} = \overline{z} + \overline{w} \quad \text{und} \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

für alle $z, w \in \mathbb{C}$. Dabei heißt $\overline{z}$ die zu z **konjugiert komplexe Zahl** (englisch: complex conjugate).

Das Produkt $z \cdot \overline{z}$ einer komplexen Zahl $z = a + b\,i$ mit ihrer konjugiert komplexen Zahl ergibt

$$z \cdot \overline{z} = (a + b\,i) \cdot (a - b\,i) = a^2 + b^2.$$

Mit Hilfe der komplexen Konjugation können wir die oben eingeführte Darstellung der multiplikativen Inversen motivieren, denn es gilt

$$\frac{1}{a + b\,i} = \frac{1}{a + b\,i} \cdot \frac{a - b\,i}{a - b\,i} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\,i.$$

In der Darstellung einer komplexen Zahl $z = a + b\,i$ heißt $a =: \operatorname{Re}(z) \in \mathbb{R}$ der **Realteil** und $b =: \operatorname{Im}(z) \in \mathbb{R}$ der **Imaginärteil**. Es gilt

$$\begin{aligned} \frac{z + \overline{z}}{2} &= \frac{a + b\,i + a - b\,i}{2} = a = \operatorname{Re}(z) \\ \frac{z - \overline{z}}{2\,i} &= \frac{a + b\,i - a + b\,i}{2\,i} = b = \operatorname{Im}(z). \end{aligned}$$

Beachte: $\operatorname{Re}\colon (\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$ und $\operatorname{Im}\colon (\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$ sind keine Körperhomomorphismen! (**Beachte:** Warum nicht?)

Schließlich halten wir fest, dass $\mathbb{R}$ mittels der Identifikation $a = a + 0\,i$ zu einem Teilkörper von $\mathbb{C}$ wird.

Kapitel B Liste algebraischer Strukturen

In der folgenden Tabelle ist X irgendeine Menge und $m \in \mathbb{N}$. Die Abkürzungen „komm.“ und „n. E.“ stehen für „kommutativ“ und „neutrales Element“. Bei Ringen bezieht sich die Kommutativität und die Angabe des neutrale Elements auf die zweite Verknüpfung. Die angegebenen Eigenschaften können in Einzelfällen abweichen, vor allem im Fall $m = 1$ oder wenn X die leere Menge oder eine einelementige Menge ist.

Symbol	Beschreibung	komm.	n. E.	Referenz
Halbgruppen und Monoide				
$(\mathbb{N}, +)$		✓	—	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{N}_0, +)$		✓	0	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{N}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.14 und 7.20
$(\mathbb{N}_0, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{Z}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.14, 7.16 und 7.20
$(\mathbb{Q}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{R}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.14 und 7.20
$(\mathbb{C}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{Z}_m, \cdot_m)$	multiplikatives Monoid $\mathbb{Z}$ modulo m	✓	1	Beispiele 7.2, 7.8, 7.14 und 7.16
$(H^X, +)$	Halbgruppe der Funktionen $X \longrightarrow H$ in die Halbgruppe $(H, +)$	wie in $(H, +)$		Beispiel 10.2
$(\mathbb{N}^X, +)$		✓	—	
$(\mathbb{N}_0^X, +)$		✓	$x \mapsto 0$	
$(H^X, \cdot)$	Halbgruppe der Funktionen $X \longrightarrow H$ in die Halbgruppe $(H, \cdot)$	wie in $(H, \cdot)$		Beispiel 10.2
$(\mathbb{N}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{N}_0^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{Z}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{Q}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{R}^X, \cdot)$		✓	$x \mapsto 1$	Beispiele 7.2, 7.4 und 7.16
$(\mathbb{C}^X, \cdot)$		✓	$x \mapsto 1$	
$(X^X, \circ)$		—	id_X	Beispiele 7.2, 7.4, 7.14 und 7.16
$(\mathcal{P}(X), \cap)$		✓	X	Beispiele 7.4 und 7.8
$(\mathcal{P}(X), \cup)$		✓	$\emptyset$	Beispiele 7.4 und 7.8
$(\mathcal{P}(X), \triangle)$		✓	$\emptyset$	Beispiele 7.4 und 7.8
$(\Sigma^*, \circ)$		—	$()$	Beispiele 7.4 und 7.8

Symbol	Beschreibung	komm.	n. E.	Referenz
Gruppen				
$(\mathbb{Z}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8, 7.14, 7.16, 7.20 und 7.38
$(\mathbb{Q}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8, 7.14, 7.16 und 7.20
$(\mathbb{R}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8, 7.14, 7.16 und 7.20
$(\mathbb{C}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8, 7.14, 7.16 und 7.20
$(\mathbb{Q}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.14 und 7.16
$(\mathbb{R}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.14 und 7.16
$(\mathbb{C}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.14 und 7.16
$(m\,\mathbb{Z}, +)$	ganzzahlige Vielfache von m	✓	1	Beispiele 7.34 und 7.38
$(\mathbb{Z}_m, +_m)$	additive Gruppe $\mathbb{Z}$ modulo m	✓	0	Beispiele 7.2, 7.8, 7.14 und 7.16
$(\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+})$	Faktorgruppe, isomorph zu $(\mathbb{Z}_m, +_m)$	✓	$[1]$	Beispiel 8.15
$(G^X, +)$	Gruppe der Funktionen $X \to G$ in die Gruppe $(G, +)$	wie in $(G, +)$		Beispiel 10.2
$(\mathbb{Z}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{Q}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{R}^X, +)$		✓	$x \mapsto 0$	Beispiele 7.2, 7.4 und 7.16
$(\mathbb{C}^X, +)$		✓	$x \mapsto 0$	
$(G^X, \cdot)$	Gruppe der Funktionen $X \to G$ in die Gruppe $(G, \cdot)$	wie in $(G, \cdot)$		Beispiel 10.2
$(\mathbb{Q}_{\neq 0}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{R}_{\neq 0}^X, \cdot)$		✓	$x \mapsto 1$	Beispiel 7.16
$(\mathbb{C}_{\neq 0}^X, \cdot)$		✓	$x \mapsto 1$	
$(S_n, \circ)$	symmetrische Gruppe auf $[\![1, n]\!]$	—	$\mathrm{id}_{[\![1,n]\!]}$	Definition 7.21
$(A_n, \circ)$	alternierende Gruppe auf $[\![1, n]\!]$	—	$\mathrm{id}_{[\![1,n]\!]}$	Beispiel 7.34

Symbol	Beschreibung	komm.	n. E.	Referenz
Ringe				
$(\{0_R\}, +, \cdot)$	Nullring	✓	0_R	Beispiel 9.2
$(\mathbb{Z}, +, \cdot)$		✓	1	Beispiel 9.2
$(m\,\mathbb{Z}, +, \cdot)$	ganzzahlige Vielfache von m	✓	—	Beispiel 9.2
$(\mathbb{Z}_m, +_m, \cdot_m)$	Ring von $\mathbb{Z}$ modulo m	✓	1	Beispiel 9.2
$(\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$	Restklassenring modulo m, isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$	✓	$[1]$	Beispiel 9.2
$(R^X, +, \cdot)$	Ring der Funktionen $X \to R$ in den Ring $(R, +, \cdot)$	wie in $(R, +, \cdot)$		Beispiele 9.8 und 10.2
$(\mathbb{Z}^X, +, \cdot)$		✓	1	
$(\mathbb{Q}^X, +, \cdot)$		✓	1	
$(\mathbb{R}^X, +, \cdot)$		✓	1	
$(\mathbb{C}^X, +, \cdot)$		✓	1	
$(R[t], +, \cdot)$	Polynomring über dem kommutativen Ring $(R, +, \cdot)$	✓		
$(R^R, +, \cdot)$	Ring der Funktionen $R \to R$ in den Ring $(R, +, \cdot)$	wie in $(R, +, \cdot)$		Bemerkung 11.17
$(\mathrm{End}(G), +, \circ)$	Endomorphismenring der abelschen Gruppe G	—	id_G	Beispiel 9.2
Körper				
$(\mathbb{Q}, +, \cdot)$		✓	1	Beispiele 9.2 und 10.2
$(\mathbb{R}, +, \cdot)$		✓	1	Beispiele 9.2 und 10.2
$(\mathbb{C}, +, \cdot)$		✓	1	Beispiele 9.2 und 10.2
$(\mathbb{Z}_m, +_m, \cdot_m)$	Körper von $\mathbb{Z}$ modulo m für Primzahlen m	✓	1	Beispiel 9.2
$(\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$	Restklassenkörper mod. m für Primz. m, isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$	✓	$[1]$	Beispiel 9.2

Symbol	Beschreibung	komm.	n. E.	Referenz
Vektorräume				
K_n	Zeilenvektoren über einem Körper $(K, +, \cdot)$			Beispiel 12.3
K^n	Spaltenvektoren über einem Körper $(K, +, \cdot)$			Beispiel 12.3
$(K^X, +, \cdot)$	Vektorraum der Funktionen $X \longrightarrow K$ in den Körper $(K, +, \cdot)$			Beispiel 12.3
$(V^X, +, \cdot)$	Vektorraum der Funktionen $X \longrightarrow V$ in den Vektorraum $(V, +, \cdot)$ über dem Körper $(K, +, \cdot)$			
$(K[t], +, \cdot)$	Vektorraum der Polynome (Polynomraum) über dem Körper $(K, +, \cdot)$			Beispiel 12.3
$(K_n[t], +, \cdot)$	Vektorraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$ über dem Körper $(K, +, \cdot)$			Beispiel 12.9
$(K^\mathbb{N}, +, \cdot)$	Folgen mit Werten im Körper $(K, +, \cdot)$			Beispiel 12.9
$(K^\mathbb{N}, +, \cdot)_{00}$	Folgen mit endlichem Träger und Werten im Körper $(K, +, \cdot)$			Beispiel 12.9
$(\mathbb{Q}^\mathbb{N}, +, \cdot)$	Folgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			Beispiel 12.9
$(\mathbb{Q}^\mathbb{N}, +, \cdot)_b$	beschränkte Folgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			Beispiel 12.9
$(\mathbb{Q}^\mathbb{N}, +, \cdot)_c$	konvergente Folgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			Beispiel 12.9
$(\mathbb{Q}^\mathbb{N}, +, \cdot)_0$	Nullfolgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			Beispiel 12.9
$(\mathbb{Q}^\mathbb{N}, +, \cdot)_{00}$	Folgen mit endlichem Träger mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^\mathbb{N}, +, \cdot)$	Folgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^\mathbb{N}, +, \cdot)_b$	beschränkte Folgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^\mathbb{N}, +, \cdot)_c$	konvergente Folgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^\mathbb{N}, +, \cdot)_0$	Nullfolgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^\mathbb{N}, +, \cdot)_{00}$	Folgen mit endlichem Träger mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{C}^\mathbb{N}, +, \cdot)$	Folgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			Beispiel 12.9
$(\mathbb{C}^\mathbb{N}, +, \cdot)_b$	beschränkte Folgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			Beispiel 12.9
$(\mathbb{C}^\mathbb{N}, +, \cdot)_c$	konvergente Folgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			Beispiel 12.9
$(\mathbb{C}^\mathbb{N}, +, \cdot)_0$	Nullfolgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			Beispiel 12.9
$(\mathbb{C}^\mathbb{N}, +, \cdot)_{00}$	Folgen mit endlichem Träger mit Werten im Körper $(\mathbb{C}, +, \cdot)$			Beispiel 12.9

Kapitel C Das griechische Alphabet

Kleinbuchstabe	Großbuchstabe	Name
α	Α	alpha
β	Β	beta
γ	Γ	gamma
δ	Δ	delta
ϵ, ε	Ε	epsilon
ζ	Ζ	zeta
η	Η	eta
θ, ϑ	Θ	theta
ι	Ι	iota
κ, $\varkappa$	Κ	kappa
λ	Λ	lambda
μ	Μ	mu
ν	Ν	nu
ξ	Ξ	xi
ο	Ο	omikron
π, ϖ	Π	pi
ρ, ϱ	Ρ	rho
σ, ς	Σ	sigma
τ	Τ	tau
υ	Υ	ypsilon
ϕ, φ	Φ	phi
χ	Χ	chi
ψ	Ψ	psi
ω	Ω	omega

Kapitel D Abkürzungen

Abkürzung	Bedeutung
bzgl.	bezüglich
d. h.	das heißt
etc.	et cetera
i. A.	im Allgemeinen
i. d. R.	in der Regel
i. W.	im Wesentlichen
o. B. d. A.	ohne Beschränkung der Allgemeinheit
o. ä.	oder ähnlich
usw.	und so weiter
vgl.	vergleiche

Index

Literatur

Beutelspacher, A. (2014). *Lineare Algebra. Eine Einführung in die Wissenschaft der Vektoren, Abbildungen und Matrizen.* 8. Aufl. Springer Fachmedien Wiesbaden. DOI: 10.1007/978-3-658-02413-0.

Bosch, S. (2014). *Lineare Algebra.* 5. Aufl. Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-55260-1.

Deiser, O. (2022a). *Einführung in die Mengenlehre.* URL: https://www.aleph1.info/?call=Puc&permalink=mengenlehre1.

– (2022b). *Grundbegriffe der Mathematik.* URL: https://www.aleph1.info/?call=Puc&permalink=grundbegriffe.

Fischer, G.; B. Springborn (2020). *Lineare Algebra.* 19. Aufl. Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-61645-1.

Magnus, P. D.; T. Button; J. R. Loftis; R. Trueman; A. Thomas-Bolduc; R. Zach; S. Wimmer (2023). *forall x: Dortmund. Eine Einführung in die formale Logik.* URL: https://github.com/sbwimmer/forallx-do.

Thiele, R. (1979). *Mathematische Beweise.* Bd. 99. Leipzig: B. G. Teubner Verlagsgesellschaft. URL: https://mathematikalpha.de/?smd_process_download=1&download_id=26662.