Vorlesungsskript
Lineare Algebra

Wintersemester 2025–Sommersemester 2026

Roland Herzog [*]

2025-10-13

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

Teile dieses Skripts orientieren sich an früheren Vorlesungen von Jan Johannes (Universität Heidelberg).

Änderungen gegenüber bereits veröffentlichten Versionen werden in dieser Farbe gekennzeichnet.

Material für 27 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-ğabr*, „das Zusammenfügen gebrochener Teile“, englisch: algebra) hat ihren Ursprung in der Beschreibung von Lösungsverfahren linearer und quadratischer Gleichungen. Heute verstehen wir den Begriff Algebra deutlich weiter, es geht jedoch immer um Strukturen, Abbildungen zwischen Strukturen und die in ihnen geltenden „Rechenregeln“. 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, 2024b, Kapitel 1.1; Deiser, 2022, Anhang 1; Magnus u. a., 2023, Kapitel 1–14; Velleman, 2019

Definition 1.1 (Aussage, Wahrheitswert)**.**
Eine **Aussage** (englisch: statement, proposition) 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 $\bot$, 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 P, Q usw.

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

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

(*ii*) Q: Am 17.10.2025 ist London die Hauptstadt von Frankreich.
Dieses ist eine falsche Aussage.

(*iii*) R: 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*) S: Das Team des VfL Wolfsburg ist in der Saison 2025/26 deutscher Meister in der Frauen-Fußball-Bundesliga.
Dieses ist eine Aussage, deren Wahrheitswert wir im Moment aber nicht kennen.

(*v*) T: Es gibt unendlich viele Primzahlzwillinge.
Dieses ist ebenfalls eine 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 geben einen Junktor über seine **Wahrheitswerttabelle** (auch: **Wahrheitstafel**, englisch: truth table) an.

Definition 1.3 (Junktoren)**.**

Im Folgenden seien P und Q Aussagen. Wir definieren die folgenden ein- und zweistellige Junktoren:

(*i*) $\neg$ **Negation**[2] (**Verneinung**)
Die Operation $\neg P$ (sprich: „nicht P“) heißt **Negation**. $\neg P$ ist wahr, wenn P falsch ist, und falsch, wenn P wahr ist.

P	$\neg P$
W	F
F	W

(*ii*) $\wedge$ **Konjunktion**[3] (**Und-Verknüpfung**)
Die Aussage $P \wedge Q$ (sprich: „P und Q“) ist dann wahr, wenn P und Q beide wahr sind, ansonsten falsch.

P	Q	$P \wedge Q$
W	W	W
W	F	F
F	W	F
F	F	F

[1] siehe Primzahlzwillingsvermutung
[2] englisch: negation, lateinisch: negare: verneinen
[3] englisch: conjunction, lateinisch: coniungere: verbinden

(*iii*) $\vee$ **Disjunktion**[4] (**Oder-Verknüpfung**)

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

P	Q	$P \vee Q$
W	W	W
W	F	W
F	W	W
F	F	F

(*iv*) $\rightarrow$ **Implikation**[5] (**Konditional**[6], **Wenn-Dann-Verknüpfung**)

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

P	Q	$P \rightarrow Q$
W	W	W
W	F	F
F	W	W
F	F	W

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

(*v*) $\leftrightarrow$ **Äquivalenz**[7] (**Bikonditional**, **Genau-Dann-Wenn-Verknüpfung**)

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

P	Q	$P \leftrightarrow Q$
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 P und Q 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 Junktoren $\neg$ sowie $\wedge$, $\vee$, $\rightarrow$ und $\leftrightarrow$ zusammensetzen? Reicht evtl. sogar eine Teilmenge davon aus?

[4] englisch: disjunction, lateinisch: disiungere: trennen, unterscheiden
[5] englisch: implication, lateinisch: implicare: verwickeln
[6] lateinisch: conditio: Bedingung
[7] englisch: equivalence, lateinisch: aequivalens: gleichwertig

Beispiel 1.4 (Symbolisierung von Sätzen der Umgangssprache[8])**.**
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.

(*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.

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

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

Lemma 1.5 (Umschreibung von $\to$ und $\leftrightarrow$)**.**
Es seien P und Q Aussagen.

(*i*) Die Aussagen

- $P \to Q$
- $(\neg P) \vee Q$
- $(\neg Q) \to (\neg P)$

haben dieselben Wahrheitstafeln.

(*ii*) Die Aussagen

- $P \leftrightarrow Q$
- $(P \to Q) \wedge (Q \to P)$

haben dieselben Wahrheitstafeln.

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

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

P	Q	$P \to Q$	$(\neg P) \vee Q$	$\neg Q$	$\neg P$	$(\neg Q) \to (\neg P)$
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 Gegenstand der Übung. □

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

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

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

$$\begin{aligned} (\neg P) \wedge Q &\quad \text{gleichwertig mit} \quad \neg P \wedge Q \\ \text{und} \quad (\neg(P \wedge Q)) \to (Q \vee (\neg Q)) &\quad \text{gleichwertig mit} \quad \neg(P \wedge Q) \to Q \vee \neg Q. \end{aligned}$$

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

Wir bestimmen jetzt die Wahrheitstafeln einiger zusammengesetzter Aussagen.

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

(i) $\neg(\neg P \wedge \neg Q)$

P	Q	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg(\neg P \wedge \neg Q)$
W	W	F	F	F	W
W	F	F	W	F	W
F	W	W	F	F	W
F	F	W	W	W	F

Beachte: Diese Wahrheitstafel ist offenbar dieselbe wie die von $P \vee Q$.

(*ii*) $P \vee Q \to Q \wedge R$

P	Q	R	$P \vee Q$	$Q \wedge R$	$P \vee Q \to Q \wedge R$
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*) $\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$

P	Q	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$
W	W	F	F	W
W	F	W	W	W
F	W	W	W	W
F	F	W	W	W

△

Die Aussage aus Punkt (*iii*) $\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$ hat also immer den Wahrheitswert W, unabhängig von den Wahrheitswerten der Aussagen P und Q. Eine solche Aussage nennt man eine **Tautologie**[9] (englisch: tautology) oder ein **logisches Gesetz**. Die Aussage aus Punkt (*i*) bedeutet, dass auch $\neg(\neg P \wedge \neg Q) \leftrightarrow P \vee Q$ eine Tautologie ist. Tautologien spielen eine entscheidende Rollen in mathematischen Beweisen, siehe § 3.

Definition 1.7 (logische Implikation, logische Äquivalenz)**.**
Es seien P und Q Aussagen.

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

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

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

$$\neg \quad \text{bindet stärker als} \quad \wedge$$
$$\wedge \quad \text{bindet stärker als} \quad \vee$$

[9] altgriechisch: *ταυτο*: dasselbe

$$\begin{aligned} \vee &\quad \text{bindet stärker als} \quad \rightarrow \\ \rightarrow &\quad \text{bindet stärker als} \quad \leftrightarrow \\ \leftrightarrow &\quad \text{bindet stärker als} \quad \Rightarrow \\ \Rightarrow &\quad \text{bindet stärker als} \quad \Leftrightarrow . \end{aligned} \tag{1.2}$$

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

(*i*) Die Aussage $(P \to Q) \wedge P$ impliziert die Aussage Q, kurz: $(P \to Q) \wedge P \Rightarrow Q$, denn $(P \to Q) \wedge P \to Q$ ist eine Tautologie:

P	Q	$P \to Q$	$(P \to Q) \wedge P$	$(P \to Q) \wedge P \to Q$
W	W	W	W	W
W	F	F	F	W
F	W	W	F	W
F	F	W	F	W

(*ii*) Die Aussage $(P \to Q) \wedge \neg Q$ impliziert die Aussage $\neg P$, kurz: $(P \to Q) \wedge \neg Q \Rightarrow \neg P$, denn $(P \to Q) \wedge \neg Q \to \neg P$ ist eine Tautologie:

P	Q	$P \to Q$	$(P \to Q) \wedge \neg Q$	$(P \to Q) \wedge \neg Q \to \neg P$
W	W	W	F	W
W	F	F	F	W
F	W	W	F	W
F	F	W	W	W

(*iii*) Die Aussagen $\neg(P \wedge Q)$ und $\neg P \vee \neg Q$ sind logisch äquivalent, kurz: $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$, denn $\neg(P \wedge Q) \leftrightarrow \neg P \vee \neg Q$ ist eine Tautologie, wie in Beispiel 1.6 gerade schon gezeigt wurde. △

Satz 1.9 (logische Implikationen und Äquivalenzen)**.**
Es seien P, Q und R Aussagen. Es gelten die folgenden Implikationen und Äquivalenzen.

$$\neg(\neg P) \Leftrightarrow P \qquad \text{doppelte Verneinung}[10] \tag{1.3}$$

$$P \Rightarrow \top \qquad \text{„Aus Beliebigem folgt Wahres.“}[11] \tag{1.4a}$$
$$\bot \Rightarrow P \qquad \text{„Aus Falschem folgt Beliebiges.“}[12] \tag{1.4b}$$

$$P \wedge P \Leftrightarrow P \qquad \textbf{Idempotenz von } \wedge[13] \tag{1.5a}$$
$$P \vee P \Leftrightarrow P \qquad \textbf{Idempotenz von } \vee \tag{1.5b}$$

$$P \wedge \top \Leftrightarrow P \qquad \textbf{Neutralität von } \wedge\top[14] \tag{1.6a}$$
$$P \vee \bot \Leftrightarrow P \qquad \textbf{Neutralität von } \vee\bot \tag{1.6b}$$

$$P \wedge \bot \Leftrightarrow \bot \qquad \textbf{Absorption bei } \wedge[15] \tag{1.7a}$$
$$P \vee \top \Leftrightarrow \top \qquad \textbf{Absorption bei } \vee \tag{1.7b}$$

$$P \wedge \neg P \quad \Leftrightarrow \quad \bot \qquad \textbf{Komplementarität bei } \wedge^{16} \qquad (1.8a)$$
$$P \vee \neg P \quad \Leftrightarrow \quad \top \qquad \textbf{Komplementarität bei } \vee^{17} \qquad (1.8b)$$

$$P \wedge Q \quad \Leftrightarrow \quad Q \wedge P \qquad \textbf{Kommutativität von } \wedge^{18} \qquad (1.9a)$$
$$P \vee Q \quad \Leftrightarrow \quad Q \vee P \qquad \textbf{Kommutativität von } \vee \qquad (1.9b)$$

$$(P \vee Q) \vee R \quad \Leftrightarrow \quad P \vee (Q \vee R) \qquad \textbf{Assoziativität von } \vee^{19} \qquad (1.10a)$$
$$(P \wedge Q) \wedge R \quad \Leftrightarrow \quad P \wedge (Q \wedge R) \qquad \textbf{Assoziativität von } \wedge \qquad (1.10b)$$

$$\neg(P \wedge Q) \quad \Leftrightarrow \quad \neg P \vee \neg Q \qquad \textbf{De Morgansches Gesetz}^{20} \qquad (1.11a)$$
$$\neg(P \vee Q) \quad \Leftrightarrow \quad \neg P \wedge \neg Q \qquad \textbf{De Morgansches Gesetz} \qquad (1.11b)$$

$$P \wedge (Q \vee R) \quad \Leftrightarrow \quad (P \wedge Q) \vee (P \wedge R) \qquad \textbf{Distributivität}^{21} \qquad (1.12a)$$
$$P \vee (Q \wedge R) \quad \Leftrightarrow \quad (P \vee Q) \wedge (P \vee R) \qquad \textbf{Distributivität} \qquad (1.12b)$$

$$(P \to Q) \wedge P \quad \Rightarrow \quad Q \qquad \textbf{modus ponendo ponens} \qquad (1.13a)$$
$$(P \to Q) \wedge \neg Q \quad \Rightarrow \quad \neg P \qquad \textbf{modus tollendo tollens} \qquad (1.13b)$$
$$(P \to \neg Q) \wedge P \quad \Rightarrow \quad \neg Q \qquad \textbf{modus ponendo tollens}^{22} \qquad (1.13c)$$
$$(\neg P \to Q) \wedge \neg P \quad \Rightarrow \quad Q \qquad \textbf{modus tollendo ponens}^{23} \qquad (1.13d)$$

$$(P \to Q) \wedge (Q \to R) \quad \Rightarrow \quad P \to R \qquad \textbf{Kettenschluss}^{24}. \qquad (1.14)$$

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

Quizfrage 1.3: Können Sie einfache Beispiele in Alltagssprache angeben, bei denen die vier logischen Implikationen (1.13a)–(1.13d) benutzt werden?

Ende der Vorlesung 1

[10] lateinisch: duplex negatio affirmat
[11] lateinisch: verum ex quolibet
[12] lateinisch: ex falso quodlibet
[13] englisch: idempotence, lateinisch: idem: dasselbe, lateinisch: potentia: Vermögen, Kraft
[14] englisch: neutrality, lateinisch: neutrum: keines von beiden
[15] englisch: absorption, lateinisch: absorbere: einsaugen, verschlingen
[16] englisch: complementarity, lateinisch: complementum: Ergänzung, Vollendung
[17] Gesetz vom ausgeschlossenen Dritten, lateinisch: tertium non datur
[18] englisch: commutativity, lateinisch: commutare: tauschen, vertauschen
[19] englisch: associativity, lateinisch: associare: verbinden, beigesellen
[20] englisch: De Morgan's law
[21] englisch: distributivity, lateinisch: distribuere: verteilen, aufteilen
[22] Der modus ponendo tollens wird häufig als $\neg(P \wedge Q) \wedge P \;\Rightarrow\; \neg Q$ geschrieben.
[23] Der modus tollendo ponens wird häufig als $(P \vee Q) \wedge \neg P \;\Rightarrow\; Q$ geschrieben.
[24] englisch: chain inference

§ 2 Prädikatenlogik

Literatur: Deiser, 2022, Anhang 1; 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 aus § 1 nicht wie erforderlich symbolisieren. Die Schwierigkeit ist, dass wir in der Aussagenlogik keine Aussagen mit Variablen zur Verfügung haben. Wir benötigen dazu die **Prädikatenlogik**[25], 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 zusätzlich

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

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

  Die Anzahl der Variablen einer Aussageform heißt deren **Stelligkeit** (englisch: arity).
- **Quantoren** (englisch: quantifier), und zwar

$\forall$	„für alle"	**Allquantor**[26]
$\exists$	„es existiert (mindestens) ein"	**Existenzquantor**[27]
$\exists!$	„es existiert genau ein"	**Eindeutigkeitsquantor**[28].

Für die Symbole der Prädikatenlogik sollen folgende Bindungsregeln gelten:

$$\begin{aligned} \forall, \exists \text{ und } \exists! &\text{ binden stärker als } \neg \\ \neg &\text{ bindet stärker als } \wedge \\ \wedge &\text{ bindet stärker als } \vee \\ \vee &\text{ bindet stärker als } \to \\ \to &\text{ bindet stärker als } \leftrightarrow \\ \leftrightarrow &\text{ bindet stärker als } \Rightarrow \\ \Rightarrow &\text{ bindet stärker als } \Leftrightarrow . \end{aligned} \tag{2.1}$$

Zu jedem Quantor geben wir den **Grundbereich** (auch: **Individuenbereich**, **Diskursuniversum**, **Domäne**, englisch: universe of discourse, domain of discourse) an. In der Regel nimmt

[25] genauer: Prädikatenlogik erster Stufe, englisch: predicate logic, first order logic
[26] englisch: universal quantifier
[27] englisch: existential quantifier
[28] englisch: uniqueness quantifier

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

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

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

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

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

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

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

Diese letzte Aussage (*iv*) könnten wir beispielsweise äquivalent auch auf folgende Weisen ausdrücken:

(*v*) Jeder Ort in Deutschland ist nicht gleichzeitig Stadt und hat mehr als 100 000 Einwohner.
$\forall x \in O\ (\neg(E(x) \wedge S(x)))$

(*vi*) Jeder Ort in Deutschland ist entweder keine Stadt oder hat weniger als 100 000 Einwohner oder beides.
$\forall x \in O\ (\neg E(x) \vee \neg S(x))$

(*vii*) Für alle Orte in Deutschland gilt: Wenn sie 100 000 oder mehr Einwohner haben, sind sie keine Stadt.
$\forall x \in O\ (E(x) \to \neg S(x))$

(*viii*) Für alle Orte in Deutschland gilt: Wenn sie eine Stadt sind, haben sie weniger als 100 000 Einwohner.
$\forall x \in O\ (S(x) \to \neg E(x))$

Die Äquivalenz der Aussagen (*iv*) bis (*viii*) können wir mit Hilfe von (2.2b), des De Morganschen Gesetzes (1.11a) und der Definition von $\to$ zeigen. △

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 zur *Analysis* zu den Begriffen „Stetigkeit“ und „gleichmäßige Stetigkeit“)

Die Funktion $f\colon (a,b) \to \mathbb{R}$ ist stetig:
$$\forall x \in (a,b)\ \forall \varepsilon > 0\ \exists \delta > 0\ \forall y \in (a,b)\ \underbrace{\big(|x-y| < \delta \ \Rightarrow\ |f(x)-f(y)| < \varepsilon\big)}_{\text{vierstellige Aussageform}}.$$

Die Funktion $f\colon (a,b) \to \mathbb{R}$ ist gleichmäßig stetig:
$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in (a,b)\ \forall y \in (a,b)\ \underbrace{\big(|x-y| < \delta \ \Rightarrow\ |f(x)-f(y)| < \varepsilon\big)}_{\text{dieselbe vierstellige Aussageform}}.$$

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

Satz 2.2 (logische Implikationen und Äquivalenzen von Aussagen mit Quantoren)**.**
Es seien P, Q einstellige Aussageformen mit gemeinsamem Grundbereich und R eine zweistellige Aussageform. Es gelten die folgenden Implikationen und Äquivalenzen.[29]

$\neg(\forall x\ P(x))$	$\Leftrightarrow$	$\exists x\ (\neg P(x))$	Negation des Allquantors	(2.2a)
$\neg(\exists x\ P(x))$	$\Leftrightarrow$	$\forall x\ (\neg P(x))$	Neg. des Existenzquantors	(2.2b)
$\forall x\ (P(x) \wedge Q(x))$	$\Leftrightarrow$	$\forall x\ P(x) \wedge \forall x\ Q(x)$	**Distributivität**	(2.3a)
$\exists x\ (P(x) \vee Q(x))$	$\Leftrightarrow$	$\exists x\ P(x) \vee \exists x\ Q(x)$	**Distributivität**	(2.3b)
$(\forall x\ P(x)) \vee (\forall x\ Q(x))$	$\Rightarrow$	$\forall x\ (P(x) \vee Q(x))$		(2.4a)
$\exists x\ (P(x) \wedge Q(x))$	$\Rightarrow$	$(\exists x\ P(x)) \wedge (\exists x\ Q(x))$		(2.4b)
$\forall x\ (P(x) \to Q(x))$	$\Rightarrow$	$(\forall x\ P(x)) \to (\forall x\ Q(x))$		(2.5a)
$\exists x\ (P(x) \to Q(x))$	$\Leftrightarrow$	$(\forall x\ P(x)) \to (\exists x\ Q(x))$		(2.5b)

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

§ 3 Beweismuster

Literatur: Deiser, 2024b, Kapitel 1.1; Magnus u. a., 2023, Kapitel 15–21

In einem Beweis versuchen wir in der Regel, für gegebene Aussagen P, Q die Implikation $P \Rightarrow Q$ nachzuweisen. Das heißt, wir müssen nachweisen, dass $P \to Q$ eine Tautologie ist. Meistens besteht die Prämisse P selbst aus einer Konjunktion (Und-Verknüpfung) und/oder

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

Disjunktion (Oder-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) z. B. 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, vor allem dann nicht, wenn die Aussagen Variablen enthalten. Vielmehr werden wir Schlussregeln anwenden, die auf Tautologien beruhen. Solche Tautologien haben wir in Satz 1.9 und Satz 2.2 bereits aufgeführt.

Folgende Beweismuster für Implikationen $P \Rightarrow Q$ werden häufig verwendet:

(1) Beim **direkten Beweis** (englisch: direct proof) wird $P \Rightarrow Q$, typischerweise unter Verwendung von Axiomen und bereits bewiesenen Sätzen, direkt mit Hilfe von Schlussregeln hergeleitet. Ein Vergleich mit der Wahrheitswerttabelle der Implikation $P \to Q$ (Definition 1.3) zeigt, dass nur das Fall „P ist wahr, und Q ist falsch“ ausgeschlossen werden muss. Dazu nehmen wir typischerweige die Aussage P als wahr an und zeigen, dass dann auch die Aussage Q wahr ist.

(2) Beim **indirekten Beweis** oder **Beweis durch Kontraposition** (englisch: indirect proof, proof by contrapositive, lateinisch: contra: gegen, lateinisch: positio: Position, Stellung) nutzen wir die Äquivalenz $(P \to Q) \Leftrightarrow (\neg Q \to \neg P)$ aus. Wir führen also einen direkten Beweis für $\neg Q \Rightarrow \neg P$. Dazu nehmen wir die Aussage Q als falsch an und zeigen, dass dann die Aussage P auch falsch ist.

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

(4) Beim **Beweis durch Fallunterscheidung** (englisch: proof by distinction of cases) nutzen wir die Äquivalenz $(P \wedge R \to Q) \wedge (P \wedge \neg R \to Q) \Leftrightarrow P \to Q$. Dabei ist R irgendeine weitere Aussage. Wir nehmen also zunächst die Aussagen P und R als wahr an und zeigen, dass dann auch die Aussage Q wahr ist. Anschließend nehmen wir die Aussage P weiterhin als wahr aber die Aussage R als falsch an und zeigen, dass dann wiederum die Aussage Q wahr ist. Manchmal wird die Aussage R in weitere Teilaussagen zerlegt, sodass mehr als die zwei Fälle „R ist wahr“ und „R ist falsch“ abgebildet werden können.

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:

$$P(m,n) : m^2 < n^2$$
$$Q(m,n) : m < n$$

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

$$\forall m \in \mathbb{N}\ \forall n \in \mathbb{N}\ (P(m,n) \Rightarrow Q(m,n)).$$

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

	$m^2 < n^2$	nach Definition von P
$\Rightarrow$	$0 < n^2 - m^2$	nach Subtraktion von m^2
$\Rightarrow$	$0 < (n-m)(n+m)$	nach Rechenregeln in $\mathbb{N}$
$\Rightarrow$	$0 < n - m$	da $n + m > 0$ und nach Regeln von $<$ in $\mathbb{N}$
$\Rightarrow$	$m < n$	nach Rechenregeln in $\mathbb{N}$.

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 P und Q 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**[30]

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 $(\sin(x))^2 + (\cos(x))^2 = 1$ 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, Widerspruch.

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 $n \in \mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ 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.

[30] Dieses Beispiel ist Thiele, 1979 entnommen.

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 3.1: Wieviele Implikationen wären zu zeigen, wenn man die Äquivalenz der Aussagen A_i und A_j für $i, j = 1, \ldots, n$ 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 $P(n)$ für alle ganzen Zahlen $n \geqslant n_0$ ab einem gewissen Startindex $n_0 \in \mathbb{Z}$ zeigen wollen. In diesem Fall zeigen wir am **Induktionsanfang** (englisch: base case) die Wahrheit der Aussage $P(n_0)$. Oft wird der Induktionsanfang bei $n_0 = 0$ oder $n_0 = 1$ gesetzt.

Im **Induktionsschritt** (englisch: induction step) wird für beliebiges $n \geqslant n_0$ die Aussage $P(n) \Rightarrow P(n+1)$ gezeigt. Dabei heißt $P(n)$ die **Induktionsannahme** oder **Induktionsvoraussetzung** (englisch: induction hypothesis). Bei Bedarf kann sogar auf alle vorgehenden Aussagen $P(n_0), \ldots, P(n)$ zurückgegriffen werden, also $P(n_0) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)$ gezeigt werden.[31]

Expertenwissen: vollständige Induktion für allgemeinere Indexmengen

Man muss eine Indexmenge wie $\{n \in \mathbb{Z} \mid n \geqslant n_0\}$ nicht notwendig aufsteigend traversieren. Wenn man z. B. beweisen kann, dass $P(n) \Rightarrow P(2n)$ für alle $n \in \mathbb{N}$ mit $n \geqslant n_0$ gilt sowie $P(n) \Rightarrow P(n-1)$ für $n - 1 \geqslant n_0$, so hat man auch alles gezeigt.

Außerdem kann man die vollständige Induktion auch für Aussageformen über der gesamten Menge $\mathbb{Z}$ durchführen und benötigt dann zusätzlich zum Schritt von n auf $n+1$ den Schritt von n auf $n-1$.

Schließlich erfordert die Induktion nicht einmal totalgeordnete Indexmengen (Definition 5.28). Allgemein kann man fundierte Mengen nehmen, das sind halbgeordnete Mengen, deren nichtleere Teilmengen mindestens ein minimales Element besitzen.

[31] 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 $\frac{1}{2}n\,(n+1)$, also: Für alle $n \in \mathbb{N}$ gilt

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

Induktionsanfang bei $n_0 = 1$: $P(1)$ lautet: $\sum_{j=1}^{1} j = \frac{1}{2} \cdot 1 \cdot 2$, was eine wahre Aussage ist. Wir zeigen nun im Induktionsschritt, dass $P(n)$ auch $P(n+1)$ impliziert. Zu zeigen ist für beliebiges $n \in \mathbb{N}$ also $\sum_{j=1}^{n+1} j = \frac{1}{2}(n+1)\,(n+2)$, wobei die Aussagen $\sum_{j=1}^{n} j = \frac{1}{2}n\,(n+1)$ verwendet werden darf.

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

was $P(n+1)$ entspricht. △

Ende der Vorlesung 2

Ende der Woche 1

§ 4 Mengenlehre

Literatur: Deiser, 2024b, Kapitel 1.2; Deiser, 2024a, Kapitel 1.1; Jänich, 2008, Kapitel 1.1; Jänich, 2008, Kapitel 6

Mengen sind das klassische Fundament der Mathematik. 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:

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

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

$$X := \{2, 3, 5\}.$$

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

$$X := \{5, 2, 3, 2\}$$

beschreiben. Bei der „Konstruktion“ der Menge wird das doppelte Vorkommen des Elements 2 also ignoriert.

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

$$\mathbb{N} := \{1, 2, 3, \ldots\} \qquad \text{Menge der } \textbf{natürlichen Zahlen}^{32} \tag{4.1a}$$

$$\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\} \qquad \text{Menge der } \textbf{natürlichen Zahlen mit Null} \tag{4.1b}$$

$$\mathbb{Z} := \{0, 1, -1, 2, -2, \ldots\} \qquad \text{Menge der } \textbf{ganzen Zahlen}^{33} \tag{4.1c}$$

$$\widetilde{\mathbb{Q}} := \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\} \qquad \text{vorläufige Menge der } \textbf{rationalen Zahlen}^{34} \tag{4.1d}$$

$$\mathbb{R} \qquad \text{Menge der } \textbf{reellen Zahlen}^{35} \tag{4.1e}$$

$$\mathbb{C} := \{a + b\,i \mid a, b \in \mathbb{R}\} \qquad \text{Menge der } \textbf{komplexen Zahlen}^{36}, \tag{4.1f}$$

die hier nur informell definiert werden. Für die tatsächliche Definition der rationalen Zahlen $\mathbb{Q}$ verweisen wir auf (5.18). Die mengentheoretische Konstruktion der Zahlbereiche aus (4.1) wird in Anhang A angedeutet.

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

$$Y := \{x \in X \mid P(x)\} \tag{4.2}$$

betrachten, bestehend aus den Elementen von X, für die $P(x)$ 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 beispielsweise zu, X als die Menge aller Mengen zu definieren. Wählen wir dann $P(x)$ als die Aussageform „enthält sich nicht selbst“, so definiert

$$Z := \{x \in X \mid x \notin x\}$$

also die „Menge aller Mengen, die sich nicht selbst enthalten“. Stellen wir jetzt die Frage, ob Z sich selbst enthält, so ergibt sich folgendes Problem:

[32] englisch: natural numbers
[33] englisch: integer numbers, lateinisch: integer: ganz, unversehrt
[34] englisch: rational numbers, lateinisch: ratio: Verhältnis
[35] englisch: real numbers
[36] englisch: complex numbers

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

In Kurzform erhalten wir den Widerspruch $Z \in Z \Leftrightarrow Z \notin Z$. 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.[37]

Die Auflösung in der 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[38] nicht behandeln und verweisen auf spätere Spezialveranstaltungen. Wir weisen aber darauf hin, dass die Mengenkomprehension (4.2) in Form des sogenannten **Aussonderungsaxioms** (englisch: axiom schema of separation) als Konstruktionsprinzip von Mengen weiterhin vorkommt. Wesentlich ist nur eben, dass der Grundbereich X der Aussageform P eine Menge im Sinne der ZF-Axiome sein muss.[39]

Intervalle in den reellen Zahlen lassen sich beispielsweise über Mengenkomprehension definieren:[40]

Beispiel 4.1 (Mengenkomprehension)**.**

Es seien $a, b \in \mathbb{R}$. Dann heißt

$$
\begin{aligned}
[a,b] &:= \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\} && \textbf{abgeschlossenes Intervall}[41]\\
(a,b] &:= \{x \in \mathbb{R} \mid a < x \leqslant b\} && \textbf{links offenes, rechts abgeschlossenes Intervall}[42]\\
[a,b) &:= \{x \in \mathbb{R} \mid a \leqslant x < b\} && \textbf{links abgeschlossenes, rechts offenes Intervall}[43]\\
(a,b) &:= \{x \in \mathbb{R} \mid a < x < b\} && \textbf{offenes Intervall}[44]\\
[a,\infty) &:= \{x \in \mathbb{R} \mid a \leqslant x\} && \textbf{rechtsseitig unendliches abgeschlossenes Intervall}[45]\\
(a,\infty) &:= \{x \in \mathbb{R} \mid a < x\} && \textbf{rechtsseitig unendliches offenes Intervall}[46]\\
(-\infty,b] &:= \{x \in \mathbb{R} \mid x \leqslant b\} && \textbf{linksseitig unendliches abgeschlossenes Intervall}[47]\\
(-\infty,b) &:= \{x \in \mathbb{R} \mid x < b\} && \textbf{linksseitig unendliches offenes Intervall}[48]\\
(-\infty,\infty) &:= \{x \in \mathbb{R} \mid \top\} = \mathbb{R} && \textbf{beidseitig unendliches Intervall}[49].
\end{aligned}
$$

[37] 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?

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

[39] Ist der Grundbereich keine Menge, so landet man beim Begriff der **Klasse** (englisch: class), siehe etwa Deiser, 2024a, Kapitel 3. Stark vereinfacht gesagt ist eine Klasse ein Objekt, das „zu groß" ist, um eine Menge zu sein. Ein wichtiges Beispiel ist die **Klasse aller Mengen** (englisch: class of all sets).

[40] Hierbei ist „$\leqslant$" die übliche Totalordnung auf $\mathbb{R}$. Mehr dazu in Definition 5.28 und Anhang A.

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 Intervalle sind leer, falls $b < a$ bzw. $b \leqslant a$ sein sollte. Die Bedeutung der Eigenschaften **offen** (englisch: open) und **abgeschlossen** (englisch: closed) wird typischerweise in Lehrveranstaltungen zur *Analysis* behandelt.

Wir definieren für $a, b \in \mathbb{Z}$ auch das **ganzzahlige Intervall** (englisch: integer interval)

$$[\![a, b]\!] := [a, b] \cap \mathbb{Z}.$$

Schließlich werden wir selbsterklärende Symbole wie $\mathbb{R}_{\geqslant 0}$, $\mathbb{Q}_{\neq 0}$ usw. verwenden. △

Definition 4.2 (Teilmenge, Obermenge)**.**
Für Mengen X und Y definieren wir:

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

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

Die Teilmengenbeziehung $\subseteq$ zwischen Mengen heißt auch **Inklusion** (englisch: inclusion, lateinisch: includere: einschließen) △

Beispielsweise erzeugt die Mengenkomprehension (4.2), also $Y = \{x \in X \mid P(x)\}$, immer eine Teilmenge $Y \subseteq X$. Außerdem gelten die echten Inklusionen

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

für die Zahlbereiche aus (4.1). **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) $\emptyset$. Eine Menge heißt **nichtleer** (englisch: non-empty set), wenn sie von $\emptyset$ verschieden ist, also mindestens ein Element enthält. Wir schreiben dann $X \neq \emptyset$.

[41] englisch: closed interval
[42] englisch: left-open, right-closed interval
[43] englisch: left-closed, right-open interval
[44] 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.
[45] englisch: unbounded above, closed interval
[46] englisch: unbounded above, open interval
[47] englisch: unbounded below, closed interval
[48] englisch: unbounded below, open interval
[49] englisch: unbounded above and below interval

Definition 4.3 (Durchschnitt, disjunkte Mengen, Vereinigung, disjunkte Vereinigung)**.**

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

$$\bigcap \mathcal{A} := \{x \mid \forall A \in \mathcal{A}\ (x \in A)\} \tag{4.3a}$$

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

$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I\ (x \in A_i)\}. \tag{4.3b}$$

Ist speziell $\mathcal{A} = \{A_1, A_2\}$, so schreiben wir statt $\bigcap\{A_1, A_2\}$ auch

$$A_1 \cap A_2 := \{x \mid x \in A_1 \ \wedge\ x \in A_2\}. \tag{4.3c}$$

Gilt $\bigcap \mathcal{A} = \emptyset$ bzw. $\bigcap_{i \in I} A_i = \emptyset$ bzw. $A_1 \cap A_2 = \emptyset$, so heißen die Elemente von $\mathcal{A}$ bzw. die Mengen A_i bzw. die Mengen A_1 und A_2 **disjunkt** (englisch: disjoint).

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

$$\bigcup \mathcal{A} := \{x \mid \exists A \in \mathcal{A}\ (x \in A)\} \tag{4.4a}$$

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

$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I\ (x \in A_i)\}. \tag{4.4b}$$

Ist speziell $\mathcal{A} = \{A_1, A_2\}$, so schreiben wir statt $\bigcup\{A_1, A_2\}$ auch

$$A_1 \cup A_2 := \{x \mid x \in A_1 \ \vee\ x \in A_2\}. \tag{4.4c}$$

(*iii*) Sind die Elemente von $\mathcal{A}$ aus Aussage (*ii*) **paarweise disjunkt** (englisch: pairwise disjoint), gilt also $A \cap B = \emptyset$ für alle $A, B \in \mathcal{A}$ mit $A \neq B$, dann können wir das verdeutlichen, indem wir für die Vereinigungsmenge (4.4a)

$$\bigcup\!\!\!\!\cdot\ \mathcal{A} := \{x \mid \exists A \in \mathcal{A}\ (x \in A)\} \tag{4.5a}$$

schreiben und von der **disjunkten Vereinigungmenge** oder von der **disjunkten Vereinigung** (englisch: disjoint union) von $\mathcal{A}$ sprechen. Sind die Elemente von $\mathcal{A}$ über eine Indexmenge I indiziert, gilt also $\mathcal{A} = \{A_i \mid i \in I\}$ und gilt $A_i \cap A_j = \emptyset$ für alle $i, j \in I$ mit $i \neq j$, so schreiben wir auch

$$\bigcup_{i \in I}\!\!\!\!\cdot\ A_i := \{x \mid \exists i \in I\ (x \in A_i)\}. \tag{4.5b}$$

Ist speziell $\mathcal{A} = \{A_1, A_2\}$ mit $A_1 \cap A_2 = \emptyset$, so schreiben wir auch

$$A_1 \mathbin{\dot\cup} A_2 := \{x \mid x \in A_1 \ \vee\ x \in A_2\}. \tag{4.5c}$$

△

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

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

$$X \setminus Y := \{x \in X \mid x \notin Y\}, \tag{4.6}$$

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

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

$$X \triangle Y := (X \setminus Y) \cup (Y \setminus X). \tag{4.7}$$

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

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

$$Y^c := X \setminus Y = \{x \in X \mid x \notin Y\}. \tag{4.8}$$

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

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

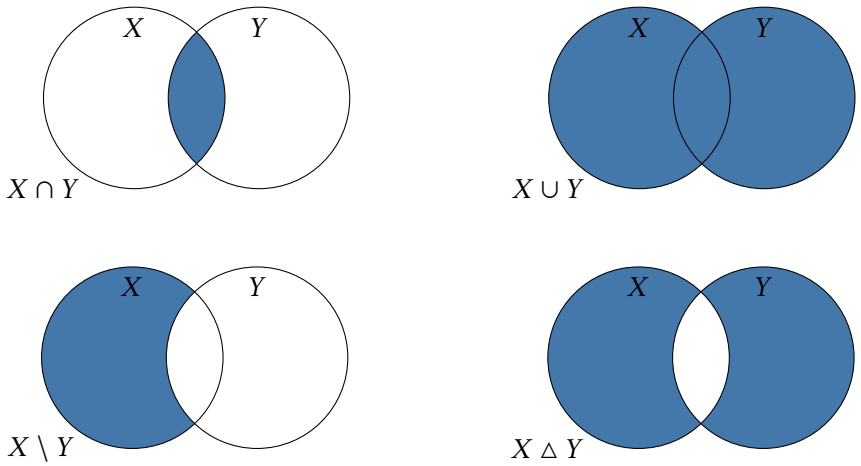


Abbildung 4.1.: Darstellung der Mengenoperationen $X \cap Y$, $X \cup Y$, $X \setminus Y$ und $X \triangle Y$ aus Definition 4.4.

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

$$X \cap Y = Y \cap X \qquad \textbf{Kommutativität von } \cap \tag{4.9a}$$
$$X \cup Y = Y \cup X \qquad \textbf{Kommutativität von } \cup \tag{4.9b}$$

$$(X \cap Y) \cap Z = X \cap (Y \cap Z) \qquad \textbf{Assoziativität von } \cap \qquad (4.10a)$$
$$(X \cup Y) \cup Z = X \cup (Y \cup Z) \qquad \textbf{Assoziativität von } \cup \qquad (4.10b)$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \qquad \textbf{Distributivität} \qquad (4.11a)$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \qquad \textbf{Distributivität} \qquad (4.11b)$$

$$X \setminus Y = X \setminus (X \cap Y) \qquad (4.12)$$

$$X \cap Y = X \quad \Leftrightarrow \quad X \subseteq Y \qquad (4.13a)$$
$$X \cup Y = Y \quad \Leftrightarrow \quad X \subseteq Y. \qquad (4.13b)$$

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

$$(Y \cap Z)^c = Y^c \cup Z^c \qquad \textbf{De Morgansches Gesetz} \qquad (4.14a)$$
$$(Y \cup Z)^c = Y^c \cap Z^c \qquad \textbf{De Morgansches Gesetz} \qquad (4.14b)$$

$$(Y^c)^c = Y \qquad \text{Komplementbildung ist } \textbf{involutorisch}^{50} \qquad (4.15)$$

$$Y \subseteq Z \quad \Leftrightarrow \quad Z^c \subseteq Y^c. \qquad (4.16)$$

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

Zur Vereinfachung der Notation vereinbaren wir auch hier wieder Bindungsregeln:

$$\begin{aligned} \cdot^c &\text{ bindet stärker als } \setminus \\ \setminus &\text{ bindet stärker als } \cap \\ \cap &\text{ bindet stärker als } \cup\,. \end{aligned} \qquad (4.17)$$

Dadurch könnten wir beispielsweise das erste Distributivgesetz (4.11a) auch als $X \cap (Y \cup Z) = X \cap Y \cup X \cap Z$ schreiben. Es gilt jedoch auch hier, dass Klammern zur Verdeutlichung nicht schaden können.

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

$$\mathcal{P}(X) := \{A \mid A \subseteq X\} \qquad (4.18)$$

die **Potenzmenge** (englisch: power set) von X. △

Die Potenzmenge von X ist also die Menge aller Teilmengen von X. In der axiomatischen Mengenlehre nach Zermelo und Fraenkel gibt es das Potenzmengenaxiom, das garantiert, dass jede Menge eine Potenzmenge besitzt.

[50] auch: selbst-invers, englisch: involutory, involutive, self-inverse, lateinisch: involvere: einwickeln

Beispiel 4.7 (Potenzmenge).

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

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

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

Definition 4.8 (kartesisches Produkt endlich vieler Mengen).

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

$$X \times Y := \{(x, y) \,|\, x \in X \ \wedge \ y \in Y\}. \tag{4.19}$$

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

(*ii*) Analog können wir auch das kartesische Produkt von mehr als zwei Mengen definieren, etwa $X \times Y \times Z$, dessen Elemente **Tripel** (englisch: triplets) (x, y, z) sind.

(*iii*) Allgemeiner heißen die Elemente $(x_1, x_2, \ldots, x_n)$ des Produkts $\bigtimes_{i=1}^n X_i = X_1 \times \cdots \times X_n$ von $n \in \mathbb{N}_0$ Mengen *n*-**Tupel** (englisch: *n*-tuples).[51] Dabei gilt $x_i \in X_i$ für $i = 1, \ldots, n$.

(*iv*) Die Einträge $x_1, \ldots, x_n$ eines n-Tupels $(x_1, \ldots, x_n)$ für $n \in \mathbb{N}_0$ heißen die **Komponenten** (englisch: components) des Tupels. Die Anzahl der Komponenten eines Tupels heißt dessen **Länge** (englisch: length).

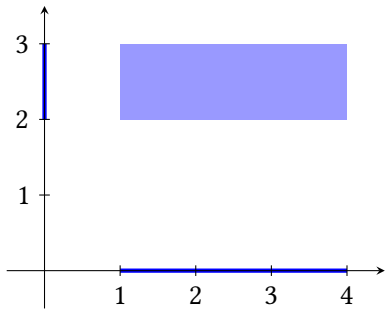
(*v*) Wir schreiben $X^2 = X \times X$ und allgemeiner $X^n = \bigtimes_{i=1}^n X$ für das kartesische Produkt einer Menge X mit sich selbst für $n \in \mathbb{N}_0$. Dabei verstehen wir unter X^0 die Menge $\{()\}$, die nur das **leere Tupel** (englisch: empty tuple) enthält. △

Beispiel 4.9 (kartesisches Produkt).

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

(*ii*) Das kartesische Produkt von Intervallen in $\mathbb{R}$ heißt ein **mehrdimensionales Intervall** (englisch: multi-dimensional interval).

Für $X = [1, 4]$ und $Y = [2, 3]$ können wir das mehrdimensionale Intervall $X \times Y = \{(x_1, x_2) \,|\, 1 \leqslant x_1 \leqslant 4 \ \wedge \ 2 \leqslant x_2 \leqslant 3\} \subseteq \mathbb{R} \times \mathbb{R}$ wie folgt illustrieren:



△

Ende der Vorlesung 3

[51] Ein Paar ist also ein 2-Tupel, ein Tripel ist ein 3-Tupel.

§ 5 Relationen

Literatur: Deiser, 2024b, Kapitel 1.3

Relationen geben Beziehungen zwischen Objekten an wie beispielsweise „$1 \leqslant 3$“ oder „$5 \in \mathbb{N}$“ oder „$3 \mid 756$“ („3 teilt 756“) oder „Berlin ist die Hauptstadt von Deutschland“.

Definition 5.1 (Relation)**.**

Es seien X und Y Mengen.

(*i*) Ist $R \subseteq X \times Y$, so heißt (R, X, Y) eine (**zweistellige**) **Relation** (englisch: relation, lateinisch: relatio: Verhältnis, Beziehung) **zwischen** X und Y. Die Menge R heißt der **Graph der Relation** (englisch: graph of a relation).

(*ii*) Sind $R, S \subseteq X \times Y$ zwei Relationen zwischen X und Y und gilt $R \subseteq S$, dann heißt R eine **Teilrelation** (englisch: subrelation) **von** S, und S heißt eine **Oberrelation** (englisch: superrelation) **von** R.

(*iii*) 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, $R \subseteq X \times Y$ 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.

Beachte: Zwei Relationen (R_1, X_1, Y_1) und (R_2, X_2, Y_2) sind genau dann gleich, wenn $X_1 = Y_1$, $X_2 = Y_2$ und $R_1 = R_2$ gilt.

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) $x \mid y$ („Die Zahl x teilt die Zahl y.“) auf der Menge $X = Y = \{0, 1, 2, \ldots, 10\} = [\![0, 10]\!]$ dar:

x \ 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 $R = \{(x, y) \in \mathbb{R}^2 \mid x \leqslant y\}$ 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 $R = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid A \subseteq B\}$ die **Teilmengenrelation** (englisch: subset relation) oder **Inklusionsrelation** (englisch: inclusion relation) auf $\mathcal{P}(X)$.

(*v*) Auf einer beliebigen Menge X heißt die Menge

$$\Delta_X := \{(x, y) \in X \times X \mid x = y\} \tag{5.1}$$

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

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

Quizfrage 5.1: Können Sie weitere Beispiele für Relationen benennen?

Definition 5.3 (Einschränkung von Relationen)**.**
Es seien X und Y Mengen und (R, X, Y) eine Relation zwischen X und Y. Sind $A \subseteq X$ und $B \subseteq Y$ Teilmengen, dann heißt $(R|_{A\times B}, A, B)$ mit

$$R|_{A\times B} := \{(x, y) \in R \mid x \in A,\ y \in B\} \tag{5.2}$$

die **Einschränkung** oder **Restriktion** (englisch: restriction, lateinisch: restringere: zurückziehen) von f **auf** $A \times B$. △

Im Falle einer homogenen Relation auf X mit Teilmenge $A \subseteq X$ betrachtet man häufig die Einschränkung $R|_{A\times A}$, die dann wiederum eine homogene Relation, und zwar auf der Teilmenge $A \subseteq X$, ist.

Definition 5.4 (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

$$S \circ R \coloneqq \{(x, z) \in X \times Z \mid \exists y \in Y \text{ mit } (x, y) \in R \text{ und } (y, z) \in S\} \tag{5.3}$$

die **Komposition** (englisch: composition, lateinisch: componere: zusammenstellen), die **Hintereinanderausführung** 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 „ist Onkel von“ ausdrücken? Und die Relation „ist Urgroßmutter von“?

Lemma 5.5 (Rechenregeln für die Komposition von Relationen)**.**
Es seien X, Y, Z und W Mengen sowie (R, X, Y), (R_1, X, Y), (R_2, X, Y) sowie (S, Y, Z), (S_1, Y, Z), (S_2, Y, Z) und (T, Z, W) Relationen.

(*i*) Die Komposition ist assoziativ, d. h., es gilt

$$(T \circ S) \circ R = T \circ (S \circ R). \tag{5.4}$$

(*ii*) Für $\circ$ und $\cup$ gelten die **Distributivgesetze**

$$(S_1 \cup S_2) \circ R = (S_1 \circ R) \cup (S_2 \circ R), \tag{5.5a}$$
$$S \circ (R_1 \cup R_2) = (s \circ R_1) \cup (s \circ R_2). \tag{5.5b}$$

Beweis. □

Beachte: Für $\circ$ und $\cap$ gelten die Distributivgesetze nicht! (**Quizfrage 5.3:** Beispiel?)

Definition 5.6 (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

$$R^{-1} \coloneqq \left\{(y, x) \in Y \times X \,\middle|\, (x, y) \in R\right\} \subseteq Y \times X$$

definiert ist. △

Quizfrage 5.4: Wie bezeichnet man die Umkehrrelationen von „kleiner oder gleich sein als“, „Teilmenge sein von“ bzw. „Teiler sein von“?

Quizfrage 5.5: Wie könnte man die Umkehrrelationen der Teilbarkeitsrelation auf $\mathbb{Z}$ bezeichnen? Welche Darstellung hat diese Umkehrrelation als Tabelle wie in Beispiel 5.2?

Lemma 5.7 (Die Umkehrrelation kommutiert mit der Vereinigung)**.**

(*i*) Es seien R_1, R_2 Relationen zwischen den Mengen X und Y. Dann gilt

$$(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}. \tag{5.6a}$$

(*ii*) Es sei $\mathcal{R}$ eine Menge von Relationen zwischen den Mengen X und Y. Dann gilt

$$\left(\bigcup \mathcal{R}\right)^{-1} = \bigcup \{R^{-1} \mid R \in \mathcal{R}\} \tag{5.6b}$$

Beweis. Aussage (*i*):

$$\begin{aligned}(R_1 \cup R_2)^{-1} &= \{(y,x) \mid (x,y) \in R_1 \text{ oder } (x,y) \in R_2\} \\ &= \{(y,x) \mid (x,y) \in R_1\} \cup \{(y,x) \mid (x,y) \in R_2\} \\ &= R_1^{-1} \cup R_2^{-1}.\end{aligned}$$

Der Beweis von Aussage (*ii*) erfolgt analog. □

Quizfrage 5.6: Was ist die Umkehrrelation von „ist Onkel von“ und von „ist Urgroßmutter von“?

Definition 5.8 (Potenzen homogener Relationen)**.**
Es sei X eine Menge und (R, X, X) eine Relation auf X. Wir definieren die **Potenzen** (englisch: powers, lateinisch: potentia: Macht, Kraft, Vermögen) von R für $n \in \mathbb{Z}$ rekursiv durch

$$R^0 := \mathrm{id}_X \tag{5.7a}$$
$$R^{n+1} := R^n \circ R \quad \text{für } n \in \mathbb{N}_0 \tag{5.7b}$$
$$R^{-n} := (R^n)^{-1} \quad \text{für } n \in \mathbb{N}. \tag{5.7c}$$

△

Quizfrage 5.7: Wenn R die Relation „Elternteil sein von“ ist, was ist dann die Relation R^2? Und was bedeutet R^{-2}?

Wir definieren nun einige wichtige Eigenschaften, die homogene Relationen besitzen können.

Definition 5.9 (Eigenschaften homogener Relationen)**.**
Es sei X eine Menge und R 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 **irreflexiv** (englisch: irreflexive), wenn gilt:

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

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

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

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

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

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

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

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

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

Quizfrage 5.8: Die Reflexivität von R kann man auch als $\mathrm{id}_X \subseteq R$ ausdrücken. Wie sieht das für die anderen Eigenschaften aus?

Beispiel 5.10 (Eigenschaften homogener Relationen)**.**

(*i*) Die Teilbarkeitsrelation | auf $\mathbb{Z}$ ist reflexiv und transitiv, aber nicht irreflexiv, symmetrisch, antisymmetrisch oder total.

(*ii*) Die Teilbarkeitsrelation | auf $\mathbb{N}_0$ ist reflexiv, antisymmetrisch und transitiv, aber nicht irreflexiv, symmetrisch oder total.

(*iii*) Die Relation „x liebt y“ auf einer Menge von Personen hat in der Regel keine der sechs genannten Eigenschaften. $\triangle$

Da Relationen Mengen sind, können wir auch Durchschnitte von Relationen betrachten.

Definition 5.11 (Durchschnitt von Relationen)**.**
Es sei $\mathcal{R}$ eine nichtleere Menge von Relationen zwischen den Mengen X und Y. Dann heißt die Relation

$$\bigcap \mathcal{R} := \left\{(x, y) \,\middle|\, \forall R \in \mathcal{R}\ ((x, y) \in R)\right\} \tag{5.8}$$

der **Durchschnitt** der Relationen in $\mathcal{R}$. $\triangle$

Beispiel 5.12 (Durchschnitt von Relationen)**.**

(*i*) Der Durchschnitt der Relationen „$\leqslant$“ und „$\geqslant$“ auf der Menge $\mathbb{R}$ ist die Diagonale $\Delta_{\mathbb{R}}$.

(*ii*) Der Durchschnitt der Relation „teilbar durch 2“ und „teilbar durch 3“ auf $\mathbb{Z}$ ist die Relation „teilbar durch 6“. $\triangle$

Lemma 5.13 (Eigenschaften homogener Relationen unter Durchschnitten)**.**
Es sei X eine Menge und $\mathcal{R}$ eine nichtleere Menge von Relationen auf X.

(*i*) Sind alle $R \in \mathcal{R}$ reflexiv, dann auch $\bigcap \mathcal{R}$.

(*ii*) Sind alle $R \in \mathcal{R}$ symmetrisch, dann auch $\bigcap \mathcal{R}$.

(*iii*) Sind alle $R \in \mathcal{R}$ transitiv, dann auch $\bigcap \mathcal{R}$.

Quizfrage 5.9: Warum führen wir keine entsprechenden Aussagen für irreflexive, antisymmetrische und totale Relationen auf?

Beweis. Aussage (*i*): Es sei $x \in X$, dann gilt $(x, x) \in R$ für alle $R \in \mathcal{R}$, also auch $(x, x) \in \bigcap \mathcal{R}$.

Aussage (*ii*): Es sei $(x, y) \in \bigcap \mathcal{R}$, also $(x, y) \in R$ für alle $R \in \mathcal{R}$. Dann folgt $(y, x) \in R$ für alle $R \in \mathcal{R}$, also $(y, x) \in \bigcap \mathcal{R}$.

Aussage (*iii*): Es seien $(x, y) \in \bigcap \mathcal{R}$ und $(y, z) \in \bigcap \mathcal{R}$, also $(x, y) \in R$ und $(y, z) \in R$ für alle $R \in \mathcal{R}$. Dann folgt $(x, z) \in R$ für alle $R \in \mathcal{R}$, also $(x, z) \in \bigcap \mathcal{R}$. □

Die Beobachtung, dass Reflexivität, Symmetrie und Transitivität unter Durchschnittsbildung erhalten bleiben, ermöglicht es uns, entsprechende **Hüllen** homogener Relationen zu definieren, siehe auch Anhang C. Dabei geht es darum, um welche Paare eine Relation mindestens erweitert werden muss, damit sie die gewünschte Eigenschaft erhält.

Definition 5.14 (Hüllen homogener Relationen)**.**
Es sei X eine Menge und R eine Relation auf X.

(*i*) Die **reflexive Hülle** (englisch: reflexive hull) von R ist definiert als[52]

$$R^? := \bigcap \{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\}. \tag{5.9a}$$

(*ii*) Die **symmetrische Hülle** (englisch: symmetrische hull) von R ist definiert als

$$R^{\text{sym}} := \bigcap \{S \subseteq X \times X \mid S \text{ ist symmetrisch und } R \subseteq S\}. \tag{5.9b}$$

(*iii*) Die **transitive Hülle** (englisch: transitive hull) von R ist definiert als

$$R^+ := \bigcap \{S \subseteq X \times X \mid S \text{ ist transitiv und } R \subseteq S\}. \tag{5.9c}$$

(*iv*) Die **reflexiv-transitive Hülle** (englisch: reflexive-transitive hull) von R ist definiert als

$$R^* := \bigcap \{S \subseteq X \times X \mid S \text{ ist reflexiv und transitiv und } R \subseteq S\}. \tag{5.9d}$$

(*v*) Die **reflexiv-symmetrisch-transitive Hülle** (englisch: reflexive-symmetric-transitive hull) von R ist definiert als

$$R^\sim := \bigcap \{S \subseteq X \times X \mid S \text{ ist reflexiv, symmetrisch und transitiv und } R \subseteq S\}. \tag{5.9e}$$

An Stelle der Bezeichnung **reflexive Hülle** wird auch der Begriff **reflexiver Abschluss** verwendet, analog für die anderen Begriffe.[53] △

Aufgrund der Konstruktion sollte klar sein, dass die Hüllenbildung eine Relation nur vergrößern kann, es gilt also

$$R \subseteq R^?, \quad R \subseteq R^{\text{sym}}, \quad R \subseteq R^+, \quad R \subseteq R^* \quad \text{und} \quad R \subseteq R^\sim. \tag{5.10}$$

Aufgrund von Lemma 5.13 gilt außerdem, dass die reflexive Hülle reflexiv ist, die symmetrische Hülle symmetrisch usw. Das folgende Resultat zeigt schließlich, dass die Hüllenbildung genau dann „nichts hinzufügt“, wenn die Relation die gewünschte Eigenschaft bereits besitzt.

[52] Andere Bezeichnungen für die reflexive Hülle sind auch $R^=$ oder R^r.

[53] Zusätzlich zu den Begriffen in Definition 5.14 könnten wir noch die **reflexiv-symmetrische Hülle** und die **symmetrisch-transitive Hülle** definieren, diese haben jedoch für uns geringere Bedeutung.

Lemma 5.15 (Hüllenbildung erkennt Eigenschaften)**.**
Es sei X eine Menge und R eine Relation auf X. Dann gilt:

(*i*) R ist reflexiv genau dann, wenn $R^? = R$ gilt.

(*ii*) R ist symmetrisch genau dann, wenn $R^{\text{sym}} = R$ gilt.

(*iii*) R ist transitiv genau dann, wenn $R^+ = R$ gilt.

(*iv*) R ist reflexiv und transitiv genau dann, wenn $R^* = R$ gilt.

(*v*) R ist reflexiv, symmetrisch und transitiv genau dann, wenn $R^\sim = R$ gilt.

Beweis. Aussage (*i*): Es sei zunächst R reflexiv, dann ist R ein Element der Menge $\{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\}$, über die in (5.9a) der Durchschnitt gebildet wird. Damit folgt $R^? \subseteq R$. Andererseits gilt auch die umgekehrte Inklusion$R \subseteq R^?$ wegen (5.10).

Umgekehrt gelte $R^? = R$. Wäre R nicht reflexiv, dann gäbe es ein $x \in X$ mit $(x, x) \notin R$. Jedoch gehört (x, x) zu jeder reflexiven Relation S mit der Eigenschaft $R \subseteq S$ und damit auch zu

$$\bigcap \{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\} = R^?.$$

Damit erhalten wir den Widerspruch $R \subsetneq R^?$.

Die weiteren Aussagen (*ii*) bis (*v*) zeigt man analog. □

Bemerkung 5.16 (Eigenschaften der verschiedenen Hüllen)**.**
Per Konstruktion ist die reflexive Hülle $R^?$ der Relation R auf X die kleinste reflexive Oberrelation von R auf X. Genauer: Es gilt $R^? \subseteq S$ für jede reflexive Oberrelation S von R. („Jede andere reflexive Relation auf X, die R enthält, ist größer als die reflexive Hülle.“)

Mit Hilfe der Begriffe für Ordnungsrelationen (§ 5.2) können wir das auch wie folgt ausdrücken: $R^?$ ist das Minimum der Teilmenge $\{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\}$ bzgl. der Inklusionshalbordnung in der Menge aller Relationen auf X (also in der Potenzmenge $\mathcal{P}(X \times X)$).

Analoge Aussagen gelten für die anderen Hüllen aus Definition 5.14. △

Die Definition 5.14 liefert eine recht abstrakte Definition der verschiedenen Hüllen homogener Relationen. Wir wollen diese Hüllen daher nun charakterisieren.

Satz 5.17 (Darstellung der Hüllen homogener Relationen)**.**
Es sei X eine Menge und R eine Relation auf X. Dann gilt:

$$R^? = \bigcup_{n \in \{0,1\}} R^n = R \cup \Delta_X \qquad \text{reflexive Hülle} \tag{5.11a}$$

$$R^{\text{sym}} = \bigcup_{n \in \{-1,1\}} R^n = R \cup R^{-1} \qquad \text{symmetrische Hülle} \tag{5.11b}$$

$$R^+ = \bigcup_{n \in \mathbb{N}} R^n \qquad \text{transitive Hülle} \tag{5.11c}$$

$$R^* = \bigcup_{n \in \mathbb{N}_0} R^n \qquad \text{reflexiv-transitive Hülle} \tag{5.11d}$$

$$R^{\sim} = \bigcup_{n\in\mathbb{N}_0} (R \cup R^{-1})^n \qquad \text{reflexiv-symmetrisch-transitive Hülle.} \tag{5.11e}$$

Beweis. Wir beweisen (5.11a). Die Gleichheit $\bigcup_{n\in\{0,1\}} R^n = R \cup \Delta_X$ ist klar wegen $R^1 = R$ und $R^0 = \Delta_X$. Wir führen den Beweis in zwei Schritten:

Schritt 1: $R^? \supseteq R \cup \Delta_X$: Es sei S eine beliebige reflexive Oberrelation von R, also eine der Mengen, die im Durchschnitt in (5.9a) vorkommt. Dann enthält S neben R wegen der Reflexivität notwendigerweise auch Δ_X als Teilmenge. Also gilt $R \cup \Delta_X \subseteq S$. Da S beliebig war, haben wir

$$R \cup \Delta_X \subseteq \bigcap \{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\} = R^?.$$

Schritt 2: $R^? \subseteq R \cup \Delta_X$: Da die Relation $R \cup \Delta_X$ eine reflexive Oberrelation von R ist, kommt sie als eine der Mengen S im Durchschnitt in (5.9a) vor. Daher gilt:

$$R^? = \bigcap \{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\} \subseteq R \cup \Delta_x.$$

Der Beweis der weiteren Aussagen läuft nach demselben Prinzip und ist Übung. □

Das folgende Resultat zeigt, dass die reflexiv-transitive Hülle übereinstimmt mit der reflexiven Hülle der transitiven Hülle und auch mit der transitiven Hülle der reflexiven Hülle. Das ist keinesfalls selbstverständlich und gilt für allgemeine mehrfache Hüllen nicht!

Folgerung 5.18 (Sequenzielle Hüllenbildung)**.**
Es sei X eine Menge und R eine Relation auf X. Dann gilt:

$$R^* = (R^+)^? = (R^?)^+. \tag{5.12}$$

Beweis. Unter Benutzung von (5.11) folgt

$$(R^+)^? = (R^+) \cup \Delta_X = \left(\bigcup_{n\in\mathbb{N}} R^n\right) \cup \Delta_X = \bigcup_{n\in\mathbb{N}_0} R^n = R^*.$$

Andererseits bekommen wir mit Hilfe des Distributivgesetzes (5.5) für $\cup$ und $\circ$ die Aussage

$$\begin{aligned}(R \cup \Delta_X)^2 &= (R \cup \Delta_X) \circ (R \cup \Delta_X)\\ &= R^2 \cup (\Delta_X \circ R) \cup (R \circ \Delta_X) \cup (\Delta_X \circ \Delta_X)\\ &= R^2 \cup R \cup \Delta_X\end{aligned}$$

und analog (per Induktion)

$$(R \cup \Delta_X)^n = \bigcup_{k=0}^{n} R^k$$

für alle $n \in \mathbb{N}$. Daher folgt

$$(R^?)^+ = (R \cup \Delta_X)^+ = \bigcup_{n\in\mathbb{N}} (R \cup \Delta_X)^n = \bigcup_{n\in\mathbb{N}} \bigcup_{k=0}^{n} R^k = \bigcup_{n\in\mathbb{N}_0} R^n = R^*.$$ □

Ende der Vorlesung 4

Ende der Woche 2

§ 5.1 Äquivalenzrelation

Definition 5.19 (Äquivalenzrelation)**.**
Es sei X eine Menge. Eine Relation R auf X heißt eine **Äquivalenzrelation** (englisch: equivalence relation) auf X, wenn sie

reflexiv, symmetrisch und transitiv

ist. Elemente $x, y \in X$, die $x\,R\,y$ erfüllen, heißen **(zueinander) äquivalent** (englisch: equivalent, lateinisch: aequivalens: gleichwertig). △

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:

$$x \sim x \qquad \text{Reflexivität,} \tag{5.13a}$$

$$x \sim y \quad \Rightarrow \quad y \sim x \qquad \text{Symmetrie,} \tag{5.13b}$$

$$x \sim y \quad \text{und} \quad y \sim z \quad \Rightarrow \quad x \sim z \qquad \text{Transitivität.} \tag{5.13c}$$

Die Idee von Äquivalenzrelationen ist es, die Elemente einer Menge, die eine bestimmte Eigenschaft gemeinsam haben, zusammenzugruppieren und als gleichwertig zu betrachten. Wir erhalten dadurch eine „gröbere Version“ der Menge.

Wir können jede Relation R durch Übergang zu ihrer reflexiv-symmetrisch-transitiven Hülle $R^{\sim}$, siehe (5.11e), zu einer Äquivalenzrelation „aufwerten“. Daher sprechen wir bei $R^{\sim}$ auch von der **Äquivalenzhülle** (englisch: equivalence hull).

Beispiel 5.20 (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 $\mathbb{Z}$ ist durch

$$x \overset{m}{\equiv} y \quad \Leftrightarrow \quad \exists n \in \mathbb{Z}\ (x - y = n\,m) \tag{5.14}$$

eine Äquivalenzrelation erklärt (**Quizfrage 5.10:** Details?). Anders ausgedrückt, x und y unterscheiden sich nur um ein Vielfaches von m, also, $m \mid (x - y)$. Diese Relation heißt die **Kongruenzrelation modulo** m (englisch: congruence relation modulo m, lateinisch: congruere: zusammentreffen, übereinstimmen) auf $\mathbb{Z}$.[54] △

Definition 5.21 (Äquivalenzklasse, Repräsentant, Repräsentantensystem)**.**
Es sei X eine Menge mit der Äquivalenzrelation $\sim$.

(*i*) Für $x \in X$ heißt die Menge

$$[x] \coloneqq \{y \in X \mid y \sim x\} \tag{5.15}$$

die **Äquivalenzklasse** (englisch: equivalence class) von x bzgl. $\sim$.

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

(*ii*) Statt $[x]$ schreibt man manchmal auch $[x]_\sim$ oder auch $x/\sim$, um die Äquivalenzrelation zu betonen.

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

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

Beispiel 5.22 (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 einzig mögliche 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 einzige 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).[55] Die Restklasse von $a \in \mathbb{Z}$ modulo m ist also[56]

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

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

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

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

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

Das natürliche Repräsentantensystem ist $\{0, 1\}$, ein anderes ist $\{-2, 43\}$. △

Satz 5.23 (Äquivalenzklassen sind entweder 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.

[55] 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.

[56] Die Notationen $m\,\mathbb{Z} = \{m\,z \mid z \in \mathbb{Z}\}$ („Zahl mal Menge“) und $a + m\,\mathbb{Z} = setDef\, a + m\, zz \in \mathbb{Z}$ („Zahl plus Zahl mal Menge“) werden später in Bemerkung 7.20 nochmal in einem allgemeineren Kontext erklärt.

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

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

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

Definition 5.24 (Partition)**.**

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

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

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

(iii) $\emptyset \notin \mathcal{A}$. △

Zu Eigenschaft (i) sagen wir auch, dass die Mengen in $\mathcal{A}$ die Menge X **überdecken** (englisch: to cover) oder eine **Überdeckung** (englisch: cover, covering) von X darstellen. Eigenschaft (ii) besagt, dass die Mengen in $\mathcal{A}$ paarweise disjunkt sind. Kurz gesagt ist eine Partition von X also die Darstellung von X als disjunkte Vereinigung nichtleerer Teilmengen.

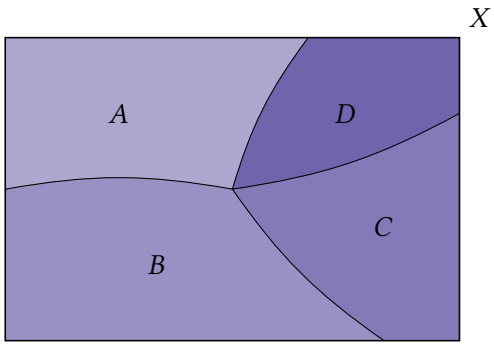


Abbildung 5.1.: Illustration der Partition einer Menge X in vier Teilmengen (Definition 5.24).

Satz 5.25 (Partitionen werden durch Äquivalenzrelationen erzeugt und umgekehrt)**.**

Es sei X eine nichtleere Menge.

(i) Ist $\sim$ eine Äquivalenzrelation, dann bildet die Menge der Äquivalenzklassen $\{[x] \mid x \in X\}$ eine Partition von X.

(ii) Ist $\mathcal{A}$ eine Partition von X, dann gibt es eine eindeutig bestimmte Äquivalenzrelation $\sim$, sodass $\mathcal{A}$ genau aus den Äquivalenzklassen von $\sim$ besteht.

Beweis. Aussage (i): Zur Abkürzung sei $\mathcal{A} := \{[x] \mid x \in X\}$ die Menge der Äquivalenzklassen zur Äquivalenzrelation $\sim$. Wir weisen die drei Eigenschaften der Definition 5.24 nach. Zunächst ist jedes $x \in X$ Element seiner Äquivalenzklasse $[x]$, da ja $x \sim x$ gilt. Das zeigt Eigenschaft (i). Nach Satz 5.23 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 Gegenstand der Übung. □

Beachte: Verschiedene Äquivalenzrelationen erzeugen verschiedene Partionen und umgekehrt. Etwas ungenau ausgedrückt sind also die Partitionen einer Menge X „dasselbe“ wie die Äquivalenzrelationen auf X.[57]

Definition 5.26 (Faktormenge, Invarianz)**.**
Es sei X eine nichtleere Menge mit der Äquivalenzrelation $\sim$.

(i) Die Menge der Äquivalenzklassen

$$X/\sim := \{[x] \mid x \in X\} \tag{5.16}$$

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

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

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

Beispiel 5.27 (wohldefinierte Aussageformen)**.**

(i) Die Aussageform „x ist eine gerade ganze Zahl“ auf $\mathbb{Z}$ 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 auf $\mathbb{Z}$ 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 in (4.1) vorläufig als

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

[57] Genauer werden wir mit Hilfe der Begriffe aus § 6 sagen können, dass die Menge aller Äquivalenzrelationen auf einer Menge X durch die Abbildung aus dem Beweis bijektiv auf die Menge aller Partitionen auf X abgebildet wird.

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

$$\frac{m_1}{n_1} \sim \frac{m_2}{n_2} \quad \Leftrightarrow \quad m_1 \cdot n_2 = m_2 \cdot n_1 \tag{5.17}$$

auf $\widetilde{\mathbb{Q}}$. Das führt uns zur Definition

$$\mathbb{Q} := \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z},\ n \in \mathbb{Z} \setminus \{0\} \right\} \ / \ \sim \tag{5.18}$$

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

§ 5.2 Ordnungsrelationen

Definition 5.28 (Ordnungsrelation)**.**
Es sei X eine Menge.

(*i*) Eine Relation R auf X heißt eine **Ordnungsrelation**, **Halbordnung** oder **partielle Ordnung** (englisch: order relation, partial order) auf X, wenn sie

reflexiv, antisymmetrisch und transitiv

ist. Das Paar (X, R) heißt dann eine **(halb-)geordnete Menge** oder **partiell geordnete Menge** (englisch: partially ordered set, poset).

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

(*iii*) Ist eine Halbordnung R zusätzlich total, gilt also für beliebige $x, y \in X$ stets $x \,R\, y$ oder $y \,R\, x$, dann heißt sie eine **Totalordnung** (englisch: total order) oder eine **lineare Ordnung** (englisch: linear order). 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:

$$x \preccurlyeq x \qquad \text{Reflexivität,} \tag{5.19a}$$

$$x \preccurlyeq y \quad \text{und} \quad y \preccurlyeq x \quad \Rightarrow \quad x = y \qquad \text{Antisymmetrie,} \tag{5.19b}$$

$$x \preccurlyeq y \quad \text{und} \quad y \preccurlyeq z \quad \Rightarrow \quad x \preccurlyeq z \qquad \text{Transitivität.} \tag{5.19c}$$

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 notwendigerweise.

Quizfrage 5.11: Lässt sich jede Relation auf einer Menge X durch Hüllenbildung zu einer Halbordnung machen?

Beispiel 5.29 (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, da sie dann nicht antisymmetrisch ist.

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

(*iv*) Die Teilmengenrelation $\subseteq$ ist eine Halbordnung auf der Potenzmenge $\mathcal{P}(X)$ jeder beliebigen Menge X. Die Teilmengenrelation wird auch **Inklusionshalbordnung** (englisch: inclusion order) genannt. 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 $\mathbb{N}$, nicht aber auf $\mathbb{Z}$. (**Quizfrage 5.12:** Warum nicht?) △

Lemma 5.30 (Halbordnungen $\leqslant$ und $\geqslant$)**.**
Es sei $\leqslant$ eine Halbordnung auf einer Menge X. Dann ist auch die inverse Relation $\geqslant$ eine Halbordnung auf X. Ist $\leqslant$ eine Totalordnung, dann auch $\geqslant$.

Beweis. Dieser Beweis ist Gegenstand der Übung. □

Wir klären jetzt, welche Art der Relation die **gewöhnliche Echt-Kleiner-Relation auf** $\mathbb{R}$, z. B. auf der Menge $\mathbb{R}$, ist.

Definition 5.31 (strenge Ordnungsrelation)**.**
Es sei X eine Menge.

(*i*) Eine Relation R auf X heißt eine **strenge Ordnungsrelation**, **strenge Halbordnung** oder **strenge partielle Ordnung** (englisch: strict order relation, strict partial order), wenn sie

irreflexiv und transitiv

ist. Das Paar (X, R) heißt dann eine **streng halbgeordnete Menge** (englisch: strictly partially ordered set).

(*ii*) Ist eine strenge Halbordnung R zusätzlich total, dann heißt sie eine **strenge Totalordnung** (englisch: strict total order). Das Paar (X, R) heißt dann eine **streng totalgeordnete Menge** (englisch: strictly totally ordered set). △

Strenge Ordnungsrelationen werden oft mit Symbolen wie $<$, $\lneq$, $\prec$, $\precneqq$ oder $\subsetneq$ notiert. Unter Verwendung der Notation $\prec$ können wir für eine strenge Ordnungsrelation auf X also festhalten, dass für alle $x, y, z \in X$ gilt:

$$x \not\prec x \quad \text{Irreflexivität,} \tag{5.20a}$$

$$x \prec y \quad \text{und} \quad y \prec z \quad \Rightarrow \quad x \prec z \quad \text{Transitivität.} \tag{5.20b}$$

Beachte: Strenge Ordnungsrelationen sind auch antisymmetrisch, denn die Annahme $x \prec y$ und $y \prec x$ impliziert $x \prec x$, was der Irreflexivität widerspricht. Es kann also nicht vorkommen, dass $x \prec y$ und $y \prec x$ gleichzeitig gelten, damit ist die Relation $\prec$ antisymmetrisch.

Lemma 5.32 (Beziehungen zwischen Ordnungsrelationen und strengen Ordnungsrelationen)**.**
Es sei X eine Menge.

(*i*) Ist $\preccurlyeq$ eine Ordnungsrelation auf X, dann ist $\prec := \preccurlyeq \setminus \Delta_X$ eine strenge Ordnungsrelation auf X, genannt die **zugehörige strenge Ordnungsrelation** (englisch: associated strict order relation).

(*ii*) Ist $\prec$ eine strenge Ordnungsrelation auf X, dann ist $\preccurlyeq := \prec \cup \Delta_X$ eine Ordnungsrelation auf X, genannt die **zugehörige Ordnungsrelation** (englisch: associated order relation).

Beachte: Für die so definierten Relationen $\preccurlyeq$ und $\prec$ gilt also $x \prec y \Leftrightarrow (x \preccurlyeq y) \wedge (x \neq y)$.

Beweis. □

In einer strengen Ordnungsrelation $\prec$ nennen wir zwei Elemente $x, y \in X$ **vergleichbar**, wenn $x \prec y$ oder $y \prec x$ oder $x = y$ gilt. Das ist genau dann der Fall, wenn x und y in der zugehörigen Ordnungsrelation $\preccurlyeq$ vergleichbar sind.

Bemerkung 5.33 (Überdeckungsrelation, Hasse-Diagramm)**.**

(*i*) Es sei $\preccurlyeq$ eine Halbordnung auf einer Menge X und $\prec$ die zugehörige strenge Halbordnung. Dann heißt die Teilrelation $\lessdot$ von $\prec$, definiert durch

$$x \lessdot y \quad \Leftrightarrow \quad \nexists z \in X \ (x \prec z \prec y) \tag{5.21}$$

die zu $\preccurlyeq$ gehörige **Überdeckungsrelation** (englisch: covering relation). Gilt $x \lessdot y$, dann sagen wir auch, x sei ein **direkter Vorgänger** (englisch: immediate predecessor) von y und y sei ein **direkter Nachfolger** (englisch: immediate successor) von x.

(*ii*) Das **Hasse-Diagramm** (englisch: Hasse diagram) oder (englisch: order diagram) der Halbordnung $\preccurlyeq$ ist ein gerichteter Graph, der die Elemente von X als Knoten enthält. Die Kante von x nach y wird genau dann eingeführt, wenn $x \lessdot y$ gilt. Das Hasse-Diagramm bildet also die Relation „direkter Nachfolger von“ ab.

(*iii*) Ist X eine endliche Menge[58], dann kann $\preccurlyeq$ als die reflexiv-transitive Hülle von $\lessdot$ wiedergewonnen werden: $\preccurlyeq \ = \ \lessdot^*$.[59] △

Definition 5.34 (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*) $b \in X$ heißt eine **obere Schranke** (englisch: upper bound) von $A \subseteq X$, wenn gilt:

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

[58] Der Begriff der endlichen Menge wird in Definition 6.32 formal eingeführt.

[59] Für unendliche partiell oder totalgeordnete Mengen gilt zwar immer noch $\lessdot^* \ \subseteq \ \preccurlyeq$, aber möglicherweise gewinnen wir nicht die gesamte Ordnungsrelation $\preccurlyeq$ zurück. Die Überdeckungsrelation $\lessdot$ kann sogar leer sein, z. B. ist das für die gewöhnliche Kleiner-Gleich-Relation auf $\mathbb{R}$ der Fall.

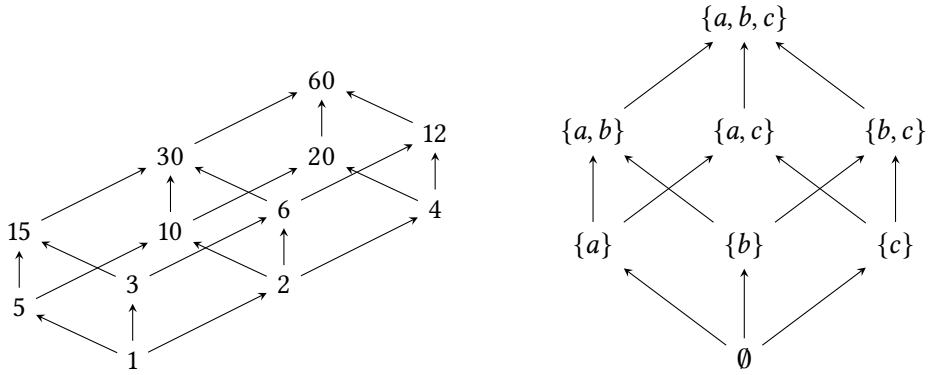


Abbildung 5.2.: Links: Hasse-Diagramm (Bemerkung 5.33) der Halbordnung | (Teilbarkeitsrelation) auf der Menge der Teiler von 60 in $\mathbb{N}$. Rechts: Hasse-Diagramm der Halbordnung $\subseteq$ (Inklusionshalbordnung) auf der Potenzmenge von $\{a, b, c\}$. Die Pfeile der Kanten können hier auch weggelassen werden, weil sie sich aus der Anordnung der Knoten (von unten nach oben) ergeben.

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

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

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

In diesem Fall schreiben wir $b = \sup A$.

(*iv*) $b \in X$ heißt das **Maximum** (englisch: maximum) von $A \subseteq X$, wenn b eine obere Schranke von A ist, die zu A gehört, wenn also gilt:

$$b \in A \quad \text{und} \quad x \preccurlyeq b \quad \text{für alle } x \in A.$$

In diesem Fall schreiben wir $b = \max A$.

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

$$b \in A, \quad \text{und für alle } x \in A \text{ gilt:} \quad b \preccurlyeq x \implies x = b.$$

(„Kein Element von A ist echt größer als b.“)

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

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

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

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

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

In diesem Fall schreiben wir $a = \inf A$.

(*ix*) $a \in X$ heißt das **Minimum** (englisch: minimum) von $A \subseteq X$, wenn a eine untere Schranke von A ist, die zu A gehört, wenn also gilt:

$$a \in A \quad \text{und} \quad a \preccurlyeq x \quad \text{für alle } x \in A.$$

In diesem Fall schreiben wir $a = \min A$.

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

$$a \in A, \quad \text{und für alle } x \in A \text{ gilt: } \quad x \preccurlyeq a \implies x = a.$$

(„Kein Element von A ist echt kleiner als a.“)

△

Beachte: Sind b_1, b_2 zwei maximale Elemente von A, dann sind sie entweder gleich oder nicht vergleichbar, denn: Aus der Vergleichbarkeit, etwa $b_1 \preccurlyeq b_2$, folgt nach Definition bereits $b_2 = b_1$. Eine analoge Aussage gilt für minimale Elemente.

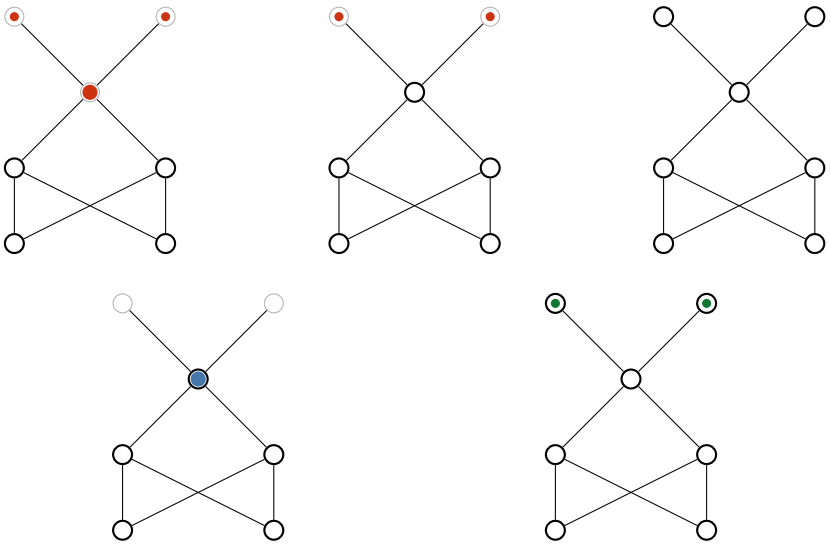


Abbildung 5.3.: Illustration der Begriffe aus Definition 5.34 für verschiedene Teilmengen $A \subseteq X$ einer halbgeordneten Menge X mit Hilfe ihres Hasse-Diagramms. Elemente von A sind als ○ gekennzeichnet, Elemente von $X \setminus A$ als ○. Oben links: Teilmenge A mit mehreren oberen Schranken (●), von denen eine (●) die kleinste (das Supremum von A) ist. Oben Mitte: Teilmenge A mit mehreren oberen Schranken ohne Supremum. Oben rechts: Die gesamte Menge X besitzt keine oberen Schranken. Unten links: Teilmenge A mit einem Maximum (●), das gleichzeitig das einzige maximale Element von A ist. Unten rechts: Teilmenge A mit mehreren maximalen Elementen (●).

Wir zeigen nun einige ausgewählte Eigenschaften, die insbesondere die Sprechweisen „das“ Supremum, „das“ Maximum, „das“ Infimum und „das“ Minimum rechtfertigen.

Lemma 5.35 (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. Es ist dann auch das einzige maximale Element von A.

(*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.

(*v*) Ist $\preccurlyeq$ eine Totalordnung auf A, dann gilt: Ist b ein maximales Element von A, so ist b auch das Maximum von A.

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, $b_1 \in X$ und $b_2 \in X$ seien beides Maxima von A. Dann gehören b_1 und b_2 beide zu A. Da b_1 ein Maximum von A ist, gilt $b_2 \preccurlyeq b_1$, und da auch b_2 ein Maximum von A ist, gilt ebenfalls $b_1 \preccurlyeq b_2$. Aufgrund der Antisymmetrie von $\preccurlyeq$ folgt nun $b_1 = b_2$.

Das Maximum b_1 von A ist außerdem ein maximales Element von A, denn für beliebiges $x \in A$ gilt $x \preccurlyeq b_1$, sodass zusätzlich $b_1 \preccurlyeq x$ dann aufgrund der Antisymmetrie $x = b_1$ impliziert.

Wäre nun $b_2 \in A$ ein anderes maximales Element von A, dann wäre $b_2 \preccurlyeq b_1$ (aufgrund der Maximum-Eigenschaft von b_1), was der Nicht-Vergleichbarkeit verschiedener maximaler Elemente widerspricht.

Aussage (*iii*): Es sei b_1 das Maximum von A. Es gilt also $b_1 \in A$ und $x \preccurlyeq b_1$ für alle $x \in A$. Das heißt aber, dass b_1 eine obere Schranke von A ist. Ist nun b_2 eine weitere obere Schranke von A, dann gilt $x \preccurlyeq b_2$ für alle $x \in A$, insbesondere $b_1 \preccurlyeq b_2$. Das zeigt, dass b_1 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.

Aussage (*v*): Es sei nun $\preccurlyeq$ eine Totalordnung auf X und b ein maximales Element von A. Für beliebiges $x \in A$ sind x und b vergleichbar. Die Annahme $b \prec x$ führt wegen der Eigenschaft, dass b maximales Element von A ist, zu dem Widerspruch $x = b$. Es muss also $x \preccurlyeq b$ gelten, was b als Maximum von A bestätigt. □

Beispiel 5.36 (Schranken, extremale Elemente, Maxima und Minima, Suprema und Infima)**.**

(*i*) In den natürlichen Zahlen $\mathbb{N}$ mit der gewöhnlichen Totalordnung $\leqslant$ ist die Zahl 1 das Minimum und damit das Infimum der Menge $\mathbb{N}$. Die Menge $\mathbb{N}$ besitzt keine obere Schranke, also auch kein Supremum und kein Maximum.

(*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 $P = \mathcal{P}(X) \setminus \{\emptyset\}$ das Infimum $\emptyset$, aber kein Minimum. Die minimalen Elemente von P sind genau die einelementigen Teilmengen von X. △

Quizfrage 5.13: Können Sie sich eine Menge mit einer Halbordnung oder einer totalen Ordnung vorstellen, die kein maximales Element besitzt?

Quizfrage 5.14: Können Sie sich eine Menge mit einer Halbordnung vorstellen, die ein eindeutiges maximales Element besitzt, das aber kein Maximum ist?

Expertenwissen: partielle Ordnung auf der Menge der Äquivalenzrelationen

Es seien X eine Menge und $\sim_1$ und $\sim_2$ zwei Äquivalenzrelationen auf X. Die Äquivalenzrelation $\sim_1$ heißt **feiner** (englisch: finer) als $\sim_2$, und $\sim_2$ heißt **gröber** (englisch: coarser) als $\sim_1$, wenn für alle $x, y \in X$ gilt:

$$x \sim_1 y \quad \Rightarrow \quad x \sim_2 y.$$

Mit anderen Worten: Jede Äquivalenzklasse von $\sim_1$ ist in einer Äquivalenzklasse von $\sim_2$ enthalten: $[x]_{\sim_1} \subseteq [x]_{\sim_2}$ für alle $x \in X$.

In dem Fall heißt $\sim_1$ auch eine **Verfeinerung** (englisch: refinement) von $\sim_2$, und $\sim_2$ heißt eine **Vergröberung** (englisch: coarsening) von $\sim_1$. Wir schreiben auch $\sim_1 \leqslant \sim_2$.

Die Relation $\leqslant$ ist eine partielle Ordnung auf der Menge aller Äquivalenzrelationen auf X. In dieser Ordnungsrelation ist die universelle Relation $X \times X$ das Maximum, und die Diagonale Δ_X ist das Minimum.

Ende der Vorlesung 5

§ 6 Abbildungen

Literatur: Deiser, 2024a, Kapitel 1.3; Deiser, 2024b, Kapitel 1.4; Jänich, 2008, Kapitel 1.2

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 kurz 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. Zu gegebenem $x \in X$ heißt das eindeutige $y \in Y$ mit $x\,f\,y$ das **Bild** (englisch: image) oder der **Funktionswert** (englisch: function value) **von** f **an der Stelle** x oder **von** x **unter** f. Dieser wird auch mit $f(x)$ bezeichnet. Wir sagen auch, f **bilde** x auf $f(x)$ **ab** (englisch: f maps x to $f(x)$) und schreiben dafür $x \mapsto f(x)$. Für die Definition einer Funktion sind daher auch die kompakten Schreibweisen

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

üblich.

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

Die Menge

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

heißt der **Graph** (englisch: graph) der Funktion $f\colon X \to Y$.[60]

Beispiel 6.3 (Abbildungen)**.**

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

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

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

(*ii*) Die Funktion

$$X \ni x \mapsto \mathrm{id}_X(x) := x \in X$$

heißt die **Identität** (englisch: identity) oder **identische Abbildung** (englisch: identity map) **von** X **in sich**. Der Graph von id_X ist die Diagonale $\Delta_X = \{(x, y) \in X \times X \mid x = y\}$, siehe (5.1).

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

(*iii*) Ist die Definitionsmenge $X = \emptyset$ die leere Menge und Y eine beliebige Menge, dann existiert genau eine Funktion $f\colon \emptyset \to Y$, die **leere Funktion** (englisch: empty function).

(*iv*) Ist die Zielmenge $Y = \emptyset$ die leere Menge, dann existiert eine Funktion $f\colon X \to \emptyset$ genau dann, wenn auch X die leere Menge ist. △

Definition 6.4 (Bild, Einschränkung, Fortsetzung)**.**
Es sei $f\colon X \to Y$ eine Funktion.[61]

(*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** von f **auf** A.[62]

(*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.

Beachte: Es wird nicht gefordert, dass $B \subseteq Y$ gilt.

(*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. △

Beispiel 6.5 (Bild, Einschränkung, Fortsetzung)**.**
Wir betrachten die Funktionen[63]

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

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

[61] Wir sagen damit insbesondere, dass X und Y Mengen sind.
[62] vgl. Definition 5.3.
[63] Hierbei bedeutet $\frac{\pi}{2}\mathbb{Z} = \{\frac{\pi}{2} z \mid z \in \mathbb{Z}\}$ („Zahl mal Menge“) die Menge der ganzzahligen Vielfachen von $\frac{\pi}{2}$. Diese Notation wird später in Bemerkung 7.20 nochmal in einem allgemeineren Kontext erklärt.

Definition 6.6 (Urbild)**.**
Es sei $f\colon X \to Y$ eine Funktion.

(*i*) 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.

(*ii*) Ist $B \subseteq Y$ einelementig, also $B = \{y\}$ für ein $y \in Y$, dann heißt das Urbild

$$f^{-1}(\{y\}) \coloneqq \{x \in X \mid f(x) = y\} \tag{6.4}$$

auch die **Faser** (englisch: fiber) von y **unter** f. △

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

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

Dann ist

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

△

Satz 6.8 (Bilder und Urbilder von Vereinigungen und Durchschnitten)**.**
Es sei $f\colon X \to Y$ 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:

$$f\Big(\bigcup_{i\in I} X_i\Big) = \bigcup_{i\in I} f(X_i) \tag{6.5a}$$

$$f\Big(\bigcap_{i\in I} X_i\Big) \subseteq \bigcap_{i\in I} f(X_i) \tag{6.5b}$$

$$f^{-1}\Big(\bigcup_{j\in J} Y_j\Big) = \bigcup_{j\in J} f^{-1}(Y_j) \tag{6.5c}$$

$$f^{-1}\Big(\bigcap_{j\in J} Y_j\Big) = \bigcap_{j\in J} f^{-1}(Y_j). \tag{6.5d}$$

Beweis. Wir beweisen hier nur (6.5a) und (6.5c). Die Aussagen (6.5b) und (6.5d) sind Gegenstand der Übung.

Zum Beweis von (6.5a):

$$\begin{aligned} & y \in f\Big(\bigcup_{i\in I} X_i\Big) \\ \Leftrightarrow\quad & \exists i \in I\ \exists x \in X_i\ (y = f(x)) && \text{nach Definition (4.4b) der Vereinigungsmenge} \\ \Leftrightarrow\quad & \exists i \in I\ (y \in f(X_i)) && \text{nach Definition (6.2) des Bildes } f(X_i) \end{aligned}$$

$$\Leftrightarrow \quad y \in \bigcup_{i \in I} f(X_i) \qquad \text{nach Definition (4.4b) der Vereinigungsmenge.}$$

Zum Beweis von (6.5c):

$$\begin{aligned}
& x \in f^{-1}\Big(\bigcup_{j \in J} Y_j\Big) \\
\Leftrightarrow \quad & \exists y \in \bigcup_{j \in J} Y_j \ \big(y = f(x)\big) && \text{nach Definition (6.3) des Urbildes} \\
\Leftrightarrow \quad & \exists j \in J \ \exists y \in Y_j \ \big(y = f(x)\big) && \text{nach Definition (4.4b) der Vereinigungsmenge} \\
\Leftrightarrow \quad & \exists j \in J \ \big(x \in f^{-1}(Y_j)\big) && \text{nach Definition (6.3) des Urbildes} \\
\Leftrightarrow \quad & x \in \bigcup_{j \in J} f^{-1}(Y_j) && \text{nach Definition (4.4b) der Vereinigungsmenge.}
\end{aligned}$$ □

Beispiel 6.9 (Bilder und Urbilder von Vereinigungen und Durchschnitten).
In (6.5b) gilt i. A. nicht die Gleichheit, wie folgendes Beispiel zeigt: Es sei

$$\mathbb{R} \ni x \mapsto y_0 \in \mathbb{R}$$

eine konstante Funktion. Für die disjunkten Mengen $X_1 = \{0\}$ und $X_2 = \{1\}$ gilt

$$\begin{aligned}
& f(X_1 \cap X_2) = f(\emptyset) = \emptyset, \\
\text{aber} \quad & f(X_1) \cap f(X_2) = \{y_0\} \cap \{y_0\} = \{y_0\}.
\end{aligned}$$ △

§ 6.1 Injektivität und Surjektivität

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

(*i*) **surjektiv** (englisch: surjective, onto, französisch: sur: auf, lateinisch: iacere: werfen), eine **Surjektion** (englisch: surjection) oder **rechtstotal** (englisch: right-total), wenn $f(X) = Y$ gilt.[64] Man sagt auch, f bilde X **auf** Y ab.

Äquivalent dazu sind:

- Für alle $y \in Y$ gibt es mindestens ein $x \in X$ mit der Eigenschaft $f(x) = y$.
- Jedes Element der Zielmenge Y hat ein nichtleeres Urbild:

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

(*ii*) **injektiv** (englisch: injective, one-to-one, lateinisch: in: hinein), eine **Injektion** (englisch: injection), eine **Einbettung** (englisch: embedding) oder **linkseindeutig** (englisch: left-unique), wenn für alle $x_1, x_2 \in X$ gilt: $f(x_1) = f(x_2) \implies x_1 = x_2$.[65]

Äquivalent dazu sind:

[64] Die Surjektivität von f wird manchmal auch durch die Schreibweise $f\colon X \twoheadrightarrow Y$ ausgedrückt.
[65] Die Injektivität von f wird manchmal auch durch die Schreibweise $f\colon X \rightarrowtail Y$ ausgedrückt.

- Für alle $y \in Y$ gibt es höchstens ein $x \in X$ mit der Eigenschaft $f(x) = y$.
- Das Urbild jedes Elements der Zielmenge Y ist maximal einelementig:

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

(*iii*) **bijektiv** (englisch: bijective, lateinisch: bi- (Vorsilbe): beide) oder eine **Bijektion** (englisch: bijection), wenn f surjektiv und injektiv ist.[66]

Äquivalent dazu sind:

- Für alle $y \in Y$ gibt es genau ein $x \in X$ mit der Eigenschaft $f(x) = y$.
- Das Urbild jedes Elements der Zielmenge Y ist genau einelementig ist:

$$\forall y \in Y \left(f^{-1}(\{y\}) \text{ hat genau ein Element}\right). \qquad \triangle$$

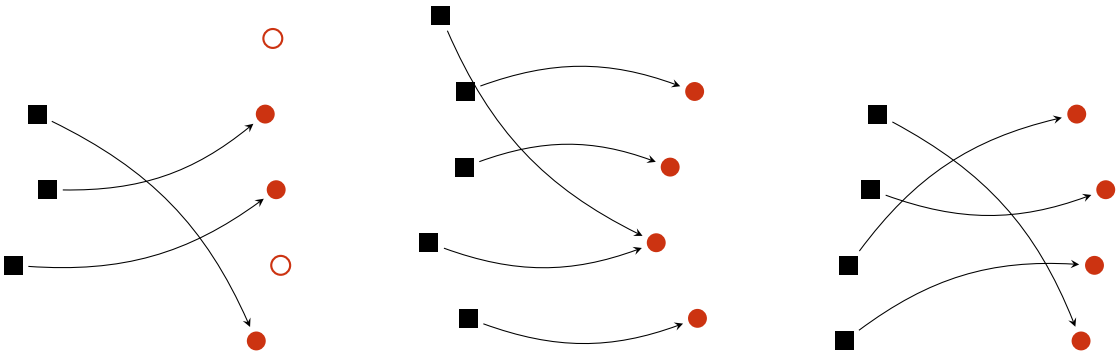


Abbildung 6.1.: Darstellung einer injektiven, aber nicht surjektiven Abbildung (links), einer surjektiven, aber nicht injektiven Abbildung (Mitte) sowie einer bijektiven Abbildung (rechts), siehe Definition 6.10.

Bemerkung 6.11 (Einbettung)**.**

(*i*) Der Name **Einbettung** für eine injektive Abbildung $f\colon X \to Y$ rührt daher, dass durch f mit $f(X)$ ein Abbild der Menge X in der Menge Y entsteht, wobei jedes Element von $f(X)$ ein einelementiges Urbild in X hat: $f^{-1}(\{f(x)\}) = \{x\}$. Dadurch wird $f|^{f(X)}$ zu einer Bijektion (Lemma 6.12), und X kann mit seiner Bildmenge $f(X) \subseteq Y$ identifiziert werden. Durch diese Identifikation wird X in Y eingebettet.

(*ii*) Sind X und Y Mengen mit $X \subseteq Y$, dann heißt die injektive Abbildung $i_{Y \leftarrow X}$ mit

$$X \ni x \mapsto i_{Y \leftarrow X}(x) := x \in Y$$

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. $\triangle$

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

[66] Die Bijektivität von f wird manchmal auch durch die Schreibweise $f\colon X \twoheadrightarrow Y$ ausgedrückt.

Lemma 6.12 (Bijektiv-Machen einer injektiven Funktion)**.**
Es sei $f\colon X \to Y$ eine injektive Funktion. Dann ist $f|^{f(X)}$ (erhalten durch die Einschränkung der Zielmenge auf die tatsächliche Bildmenge) bijektiv.

Beweis. Der Beweis ist Gegenstand der Übung. □

Beispiel 6.13 (Injektivität, Surjektivität, Bijektivität)**.**

(*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.

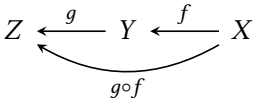
(*iv*) Die Funktion
$$\mathbb{R}_{\geqslant 0} \ni x \mapsto x^2 \in \mathbb{R}_{\geqslant 0}$$
ist bijektiv.

(*v*) Ist X eine nichtleere Menge und $\sim$ eine Äquivalenzrelation auf X, dann heißt die Abbildung
$$\pi\colon X \ni x \mapsto [x] \in X/\sim, \tag{6.6}$$
die jedem Element seine Äquivalenzklasse zuordnet, die **kanonische Surjektion** (englisch: canonical surjection). Diese ist surjektiv.

(*vi*) Die leere Funktion $f\colon \emptyset \to Y$ ist für beliebige Mengen Y injektiv. Sie ist bijektiv genau dann, wenn $Y = \emptyset$ ist. △

Definition 6.14 (Komposition von Funktionen)**.**
Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ Funktionen. Die Funktion $g \circ f$, definiert durch
$$X \ni x \mapsto (g \circ f)(x) \coloneqq g(f(x)) \in Z,$$
heißt die **Komposition** (englisch: composition, lateinisch: componere: zusammenstellen), die **Hintereinanderausführung** oder die **Verkettung** von f und g. Um die Reihenfolge klar zu benennen, sagt man auch „g **nach** f“. △

Wir können den Sachverhalt aus Definition 6.14 durch das nebenstehende Bild illustrieren. Die Voraussetzung, dass die Zielmenge von f mit der Definitionsmenge von g übereinstimmt, kann relaxiert werden: Die Komposition $g \circ f$ von $f\colon X \to \widetilde{Y}$ und $g\colon Y \to Z$ ist definiert, sofern $f(X) \subseteq Y$ gilt.



Beispiel 6.15 (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

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

Die Komposition von Funktionen f, g ist also, selbst wenn $g \circ f$ und $f \circ g$ beide definiert sind, i. A. nicht kommutativ.

Bemerkung 6.16 (Komposition mit der Identität und mit der kanonischen Einbettung)**.**
Es sei $f\colon X \to Y$ eine Funktion. Dann gilt

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f \tag{6.7a}$$
$$f|_A = f \circ i_{X \leftarrow A} \qquad \text{für } A \subseteq X \tag{6.7b}$$
$$i_{Y \leftarrow B} \circ (f|^B) = f \qquad \text{für } Y \supseteq B \supseteq f(X). \tag{6.7c}$$

△

Lemma 6.17 (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. □

Definition 6.18 (Potenzen von Funktionen)**.**
Es sei $f\colon X \to X$ eine Funktion.

(*i*) Wir definieren die **Potenzen** von f für $n \in \mathbb{N}_0$ rekursiv durch

$$f^0 \coloneqq \mathrm{id}_X \tag{6.8a}$$
$$f^{n+1} \coloneqq f^n \circ f \quad \text{für } n \in \mathbb{N}_0. \tag{6.8b}$$

(*ii*) f heißt eine **Involution** (englisch: involution), wenn $f^2 = \mathrm{id}_X$ gilt.

(*iii*) f heißt eine **Funktion endlicher Ordnung** (englisch: function of finite order), wenn es ein $n \in \mathbb{N}$ gibt mit der Eigenschaft $f^n = \mathrm{id}_X$. In diesem Fall heißt die kleinste Zahl $n \in \mathbb{N}$ mit dieser Eigenschaft die **Ordnung** von f. Falls kein $n \in \mathbb{N}$ mit der Eigenschaft $f^n = \mathrm{id}_x$ existiert, so heißt f eine **Funktion unendlicher Ordnung** (englisch: function of infinite order). △

Beachte: Jede Funktion $f\colon X \to X$ der Ordnung 2 ist eine Involution. Allerdings ist nicht jede Involution eine Funktion der Ordnung 2. (**Quizfrage 6.2:** Warum nicht?)

Quizfrage 6.3: Warum definieren wir (im Gegensatz zu Definition 5.8) keine negativen Potenzen von Funktionen?

Lemma 6.19 (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 $g \circ f$ injektiv und f surjektiv, dann ist g injektiv.

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

(*vi*) Ist $g \circ f$ surjektiv und g injektiv, dann ist f surjektiv.

Beachte: Aus den Aussagen (*i*) und (*ii*) folgt sofort, dass die Komposition bijektiver Funktionen bijektiv ist.

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 seien $y_1, y_2 \in Y$, sodass $g(y_1) = g(y_2)$ gilt. Aufgrund der Surjektivität von f gibt es $x_1, x_2 \in X$, sodass $y_1 = f(x_1)$ und $y_2 = f(x_2)$ gilt. Es folgt $g(f(x_1)) = g(f(x_2))$, und aufgrund der Injektivität von $g \circ f$ folgt $x_1 = x_2$, also auch $y_1 = y_2$, d. h., g ist injektiv.

Aussage (*v*): 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.

Aussage (*vi*): Ist $g \circ f$ surjektiv und g injektiv, dann ist f surjektiv. Es sei $y \in Y$ und $z \coloneqq g(y)$. Aufgrund der Surjektivität von $g \circ f$ gibt es ein $x \in X$, sodass $g(f(x)) = z$ gilt. Nun gilt also $z = g(y) = g(f(x))$, und da g injektiv ist, folgt $y = f(x)$, d. h., f ist surjektiv. □

Folgerung 6.20 (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 6.19, Aussagen *(iii)* und *(v)* folgt daher, dass f injektiv und g surjektiv ist. □

Folgerung 6.21 (Funktionen endlicher Ordnung sind bijektiv)**.**
Es sei $f\colon X \to X$ eine Funktion endlicher Ordnung. Dann ist f bijektiv. Insbesondere ist jede Involution bijektiv.

Beweis. Nach Voraussetzung gibt es ein $n \in \mathbb{N}$, sodass $f^n = \mathrm{id}_X$ gilt. Ist $n = 1$, so ist nichts zu zeigen, denn id_X ist bijektiv. Andernfalls ergibt sich aus $f^n = f \circ f^{n-1} = \mathrm{id}_X$ mit Folgerung 6.20 die Surjektivität von f. Weiter ergibt sich aus $f^n = f^{n-1} \circ f = \mathrm{id}_X$ mit Folgerung 6.20 die Surjektivität von f. □

Ende der Vorlesung 6

Ende der Woche 3

§ 6.2 Umkehrfunktion

Definition 6.22 (Umkehrfunktion)**.**
Es sei $f\colon X \to Y$ eine Funktion. Wenn eine Funktion $g\colon Y \to X$ existiert, sodass

$$g \circ f = \mathrm{id}_X \quad \text{und} \quad f \circ g = \mathrm{id}_Y \tag{6.9}$$

gilt, dann heißt f **invertierbar** (englisch: invertible). Die (eindeutig bestimmte) Funktion $g\colon Y \to X$ heißt die **Umkehrfunktion** oder **Umkehrabbildung**, **inverse Funktion** (englisch: inverse function) oder **inverse Abbildung** (englisch: inverse map) von f. Sie wird auch mit $f^{-1}\colon Y \to X$ bezeichnet. △

Lemma 6.23 (Umkehrfunktionen sind eindeutig)**.**
Es sei $f\colon X \to Y$ eine invertierbare Funktion. Sind $g, \widehat{g}\colon Y \to X$ beides Umkehrfunktionen von f, dann ist $g = \widehat{g}$.

Beweis. Es gilt

$$\begin{aligned}
g &= g \circ \mathrm{id}_Y && \text{nach (6.7a)} \\
&= g \circ (f \circ \widehat{g}) && \text{nach Voraussetzung} \\
&= (g \circ f) \circ \widehat{g} && \text{nach Lemma 6.17} \\
&= \mathrm{id}_X \circ \widehat{g} && \text{nach Voraussetzung} \\
&= \widehat{g} && \text{nach (6.7a).}
\end{aligned}$$

□

Lemma 6.24 (Charakterisierung der Invertierbarkeit)**.**
Es sei $f\colon X \to Y$ eine Funktion. Dann sind äquivalent:

(*i*) f ist invertierbar.

(*ii*) f ist bijektiv.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $f\colon X \to Y$ invertierbar und $f^{-1}\colon Y \to X$ die Umkehrfunktion. Die Abbildung $f^{-1} \circ f = \mathrm{id}_X$ ist bijektiv, insbesondere injektiv. Aus Lemma 6.19 (*iii*) folgt also, dass f injektiv ist. Auch die Abbildung $f \circ f^{-1} = \mathrm{id}_Y$ ist bijektiv, insbesondere surjektiv. Aus Lemma 6.19 (*v*) folgt also, dass f auch surjektiv ist.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Wir konstruieren eine Abbildung $g\colon Y \to X$ wie folgt: Wir definieren für beliebiges $y \in Y$ den Funktionswert $g(y)$ als das nach Voraussetzung eindeutig definierte $x \in X$, für das $y = f(x)$ gilt. Für diese Funktion haben wir also $g(y) = x \Leftrightarrow f(x) = y$ und daher

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

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, d. h., f ist invertierbar, und g ist die zugehörige Umkehrfunktion. □

Bemerkung 6.25 (Umkehrfunktion)**.**

(*i*) Die Bedingung (6.9), also

$$f^{-1} \circ f = \mathrm{id}_X \quad \text{und} \quad f \circ f^{-1} = \mathrm{id}_Y$$

zeigt nicht nur, dass $f^{-1}\colon Y \to X$ die Umkehrfunktion von $f\colon X \to Y$ ist, sondern auch, dass f die Umkehrfunktion von f^{-1} ist. Insbesondere ist mit f auch f^{-1} bijektiv, und die Invertierung einer Funktion ist **involutorisch**, denn es gilt $(f^{-1})^{-1} = f$.

(*ii*) Für die Abbildungsvorschrift der Umkehrfunktion gilt $f^{-1}(y) = x \Leftrightarrow y = f(x)$.

(*iii*) Wenn wir wissen, dass eine Funktion $f\colon X \to Y$ bijektiv (invertierbar) ist, dann reicht es aus, für eine Funktion $g\colon Y \to X$ eine der beiden Bedingungen aus (6.9) zu prüfen, um zu bestätigen, dass g die Umkehrfunktion von f ist, denn:

$$\begin{aligned} f \circ g = \mathrm{id}_Y \quad &\Rightarrow \quad f^{-1} \circ f \circ g = f^{-1} \quad \Rightarrow \quad g = f^{-1}, \\ g \circ f = \mathrm{id}_X \quad &\Rightarrow \quad g \circ f \circ f^{-1} = f^{-1} \quad \Rightarrow \quad g = f^{-1}. \end{aligned}$$

Wenn die Bijektivität von f aber nicht bestätigt ist, dann kann aus der Erfüllung nur einer der beiden Bedingungen aus (6.9) nicht geschlossen werden, dass f invertierbar und g die Umkehrfunktion ist, vgl. Sätze 6.29 und 6.46. △

Beispiel 6.26 (Umkehrfunktion)**.**

(*i*) Die Funktion $f\colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = 2x + 1$ ist invertierbar. Um ihre Umkehrfunktion zu bestimmen, lösen wir $y = 2x + 1$ nach x auf, erhalten also $x = \frac{1}{2}(y - 1)$. Die Umkehrfunktion ist also gegeben durch $f^{-1}(y) = \frac{1}{2}(y - 1)$.

(*ii*) Die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(x) = 2x - 1$ ist nicht invertierbar. Sie ist zar injektiv, aber nicht surjektiv. Durch Einschränkung der Zielmenge auf die ungeraden Zahlen $U := \{n \in \mathbb{N} \mid n \text{ ist ungerade}\}$ wird $f|^U$ bijektiv (Lemma 6.12). Es ist dann $(f|^U)^{-1}(y) = \frac{1}{2}(y+1)$.

(*iii*) Die Funktion $f\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ mit $f(x) = x^2$ ist bijektiv (Beispiel 6.13). Die Umkehrfunktion f^{-1} heißt die **Wurzelfunktion** (englisch: square root function), geschrieben $f^{-1}(y) = \sqrt{y}$. △

Bemerkung 6.27 (Umkehrfunktion)**.**

Das Symbol f^{-1} für die Umkehrfunktion muss vom Urbild der Funktion f unterschieden werden. Wenn die Umkehrfunktion von $f\colon X \to Y$ existiert, so gilt jedoch

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

Satz 6.28 (Umkehrfunktion der Komposition)**.**

Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ bijektive Funktionen. Dann ist auch $g \circ f$ bijektiv, und für die Umkehrfunktion gilt

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{6.10}$$

Quizfrage 6.4: Wie erklärt man sich anschaulich, dass sich bei der Umkehrfunktion die Reihenfolge ändert?

Beweis. Die Bijektivität von $g \circ f$ folgt sofort aus Lemma 6.19, Aussagen (*i*) und (*ii*). Aufgrund der Assoziativität der Komposition von Funktionen (Lemma 6.17) und Bemerkung 6.16 gilt

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_Z.$$

Da die Bijektivität von $g \circ f$ bereits bekannt ist, reicht das nach Bemerkung 6.25 aus, um zu bestätigen, dass $f^{-1} \circ g^{-1}$ die Umkehrfunktion von $g \circ f$ ist. □

Satz 6.29 (Charakterisierung der Injektivität)**.**

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

(*i*) f ist injektiv.

(*ii*) Es existiert eine Abbildung $g\colon Y \to X$ 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.

(*iii*) Für beliebige Mengen X_0 und beliebige Abbildungen $f_1, f_2\colon X_0 \to X$ gilt: Aus $f \circ f_1 = f \circ f_2$ folgt $f_1 = f_2$.

(**Quizfrage 6.5:** Welche Implikationen stimmen nicht mehr, wenn $X = \emptyset$ ist?)

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

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

Damit ist $\widetilde{g} \circ f = \mathrm{id}_X$ gezeigt. Aufgrund von Folgerung 6.20 ist $\widetilde{g}$ surjektiv. Wir setzen nun $\widetilde{g}\colon f(X) \to X$ zu $g\colon Y \to X$ fort. Dazu wählen wir irgendein $x_0 \in X$ und setzen $g(y) \coloneqq \widetilde{g}(y)$ 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 $\widetilde{g}$.

Angenommen, $h\colon Y \to X$ 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.

Die weiteren Implikationen sind Bestandteil einer Übung. □

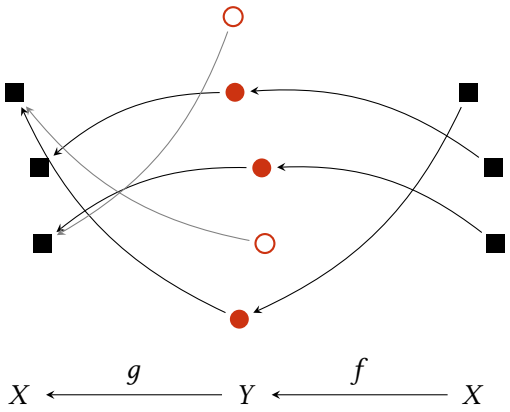


Abbildung 6.2.: Jede injektive Funktion $f\colon X \to Y$ mit $X \neq \emptyset$ besitzt eine Linksinverse $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$ (Satz 6.29). Die Linksinverse ist surjektiv und i. A. nicht eindeutig, ihre Einschränkung $g|_{f(X)}$ jedoch schon.

Beispiel 6.30 (Linksinverse)**.**
Die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = n + 3$ ist injektiv (aber nicht bijektiv). Jede Funktion $g\colon \mathbb{N} \to \mathbb{N}$ mit $g(n) = n - 3$ für $n \geqslant 4$ und $g(1), g(2), g(3) \in \mathbb{N}$ beliebig ist eine Linksinverse von f. △

Eine Charakterisierung der Surjektivität analog zu Satz 6.29 folgt erst in Satz 6.46, weil wir dafür interessanterweise das Auswahlaxiom benötigen.

§ 6.3 Mächtigkeit von Mengen

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

Definition 6.31 (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 Übung. Die Äquivalenzklassen heißen **Kardinalzahlen** (englisch: cardinal numbers).

Definition 6.32 (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: $\#X = n$.[67]

(*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 Mächtigkeit einer endlichen Menge ist eindeutig bestimmt. Die leere Menge $\emptyset$ ist nur zu sich selbst gleichmächtig. Sie ist die einzige Menge mit Mächtigkeit 0. Teilmengen endlicher Mengen sind endlich. Teilmengen abzählbarer Mengen sind abzählbarer.

Beispiel 6.33 (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.[68]

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

(*iv*) Die Menge der reellen Zahlen $\mathbb{R}$ ist überabzählbar.[69] △

Lemma 6.34 (Veränderung der Kardinalität um 1).
Es sei X eine endliche Menge und $x \in X$. Dann gilt

$$\#X = \#(X \setminus \{x\}) + 1. \tag{6.11}$$

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

Satz 6.35 (Funktionen auf endlichen Mengen).
Es seien X und Y endliche, gleichmächtige Mengen und $f\colon X \to Y$ eine Funktion. Dann sind äquivalent:

[67] In dieser Lehrveranstaltung verwenden wir das Symbol # nur für endliche Mengen.
[68] Ein Beweis erfolgt typischerweise in der Lehrveranstaltung *Analysis*.
[69] Ein Beweis erfolgt typischerweise in der Lehrveranstaltung *Analysis*.

(*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 $n = \#X = \#Y \in \mathbb{N}_0$. 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 $y \coloneqq f(x)$. Dann gilt aufgrund von Lemma 6.34 $\#X \setminus \{x\} = \#Y \setminus \{y\} = n$.

Wir bezeichnen mit $\widetilde{f}\colon X \setminus \{x\} \to Y \setminus \{y\}$ 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 $\widetilde{f}$ die Injektivität von f. Nach Induktionsvoraussetzung ist $\widetilde{f}$ daher auch surjektiv, alle Elemente von $Y \setminus \{y\}$ liegen also im Bild von $\widetilde{f}$ 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 ebenfalls nur eine mögliche Abbildung, auch diese ist 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 $y_0 \in Y$, sodass das Urbild $f^{-1}(\{y_0\})$ aus (mindestens) zwei verschiedenen Elementen besteht, sagen wir $x_{01}, x_{02} \in f^{-1}(\{y_0\})$ und $x_{01} \neq x_{02}$. Wir wählen außerdem ein $y_1 \in Y \setminus \{y_0\}$ aus, was wegen $\#Y = n+1 \geqslant 2$ möglich ist. Dazu existiert ein x_1 mit $f(x_1) = y_1$. Wegen $y_1 \neq y_0$ ist $x_1 \neq x_{01}$ und $x_1 \neq x_{02}$.

Wir konstruieren nun eine Funktion $\widetilde{f}\colon X \setminus \{x_{01}\} \to Y \setminus \{y_0\}$ durch

$$\widetilde{f}(x) \coloneqq \begin{cases} f(x) & \text{im Fall } f(x) \neq y_0, \\ y_1 & \text{im Fall } f(x) = y_0. \end{cases}$$

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

(1) Für jedes $y \in Y \setminus \{y_0, y_1\}$ existiert aufgrund der Surjektivität von f ein $x \in X$ mit $\widetilde{f}(x) = f(x) = y$, und wegen $f(x_{01}) = y_0$ ist $x \in X \setminus \{x_{01}\}$.

(2) Außerdem gilt $f(x_{02}) = y_0$, also $\widetilde{f}(x_{02}) = y_1$.

Aufgrund von Lemma 6.34 gilt wieder $\#X \setminus \{x_{01}\} = \#Y \setminus \{y_0\} = n$. Nach Induktionsvoraussetzung ist $\widetilde{f}$ daher auch injektiv. Jedoch enthält $\widetilde{f}^{-1}(\{y_1\})$ neben x_1 auch noch mindestens das weitere Element $x_{02} \in f^{-1}(\{y_0\})$. Das steht im Widerspruch zur Injektivität von $\widetilde{f}$.

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*). $\square$

Beachte: Die Aussage von Satz 6.35 ist falsch, wenn X und Y zwar gleichmächtig, aber nicht endlich sind, siehe Übung.

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

Definition 6.36 (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 injektive Abbildung $f\colon X \to Y$ gibt. Wir schreiben in diesem Fall $X \preccurlyeq Y$ oder auch $Y \succcurlyeq X$. △

Bemerkung 6.37 (Mächtigkeit von Mengen)**.**

(*i*) Man kann zeigen, dass $X \preccurlyeq Y$ äquivalent ist zu. Es gilt $X = \emptyset$, oder es existiert eine surjektive Abbildung $g\colon Y \to X$.[70]

(*ii*) Die Relation $\preccurlyeq$ induziert eine Ordnungsrelation auf der Klasse aller Kardinalzahlen. Die Reflexivität und Transitivität sind dabei leicht einzusehen. (**Quizfrage 6.6:** Details?) Der Beweis der Antisymmetrie ist jedoch aufwändig und erfordert den Satz von Cantor-Bernstein-Schröder.

(*iii*) Der Satz von Cantor besagt, dass jede Menge echt weniger mächtig ist als ihre Potenzmenge, also $X \precnsim \mathcal{P}(X)$ mit der zu $\preccurlyeq$ gehörenden strengen Ordnungsrelation.[71]

(*iv*) Unter Zuhilfenahme des Auswahlaxioms (siehe § 6.5) kann man sogar zeigen, dass zwei Mengen bzgl. $\preccurlyeq$ stets vergleichbar sind. Es folgt, dass $\preccurlyeq$ sogar eine totale Ordnung auf der Klasse aller Kardinalzahlen induziert.

(*v*) Die natürlichen Zahlen sind ein Repräsentant der Äquivalenzklasse der kleinsten unendlichen Mengen. Es gilt also $\mathbb{N} \preccurlyeq X$ für alle unendlichen Mengen X. (Diese Aussage ist unabhängig vom Auswahlaxiom.) △

§ 6.4 Familien und Folgen

Definition 6.38 (Familie, Teilfamilie, Oberfamilie)**.**
Es seien I und Y Mengen.

(*i*) Eine Abbildung

$$y\colon I \ni i \mapsto y(i) \coloneqq y_i \in Y$$

heißt eine **Familie** (englisch: family) **in** Y oder **Familie mit Werten in** Y mit der **Indexmenge** (englisch: index set) I. Kurz wird diese auch mit $(y_i)_{i\in I}$ bezeichnet.

(*ii*) Für $i \in I$ heißt y_i das **Mitglied** (englisch: member) der Familie $(y_i)_{i\in I}$ zum Index i.

(*iii*) 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 $(y_i)_{i\in I_0}$. Die Teil- bzw. Oberfamilie heißt **echt** (englisch: proper subfamiliy, proper superfamily) im Fall $I_0 \subsetneq I$.

[70] siehe etwa Deiser, 2024a, Kapitel 1.4

[71] Es gibt also für jede Menge X eine injektive Abbildung $X \to \mathcal{P}(X)$, aber niemals eine surjektive Abbildung $X \to \mathcal{P}(X)$.

(*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) mit n Mitgliedern.

(*v*) Ist I unendlich, so heißt $(y_i)_{i\in I}$ eine **unendliche Familie** (englisch: infinite family).

(*vi*) 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).

(*vii*) Ist $I = \emptyset$, so heißt $(y_i)_{i\in I}$ die **leere Familie** (englisch: empty family) **in** Y, andernfalls eine **nichtleere Familie** (englisch: non-empty familiy) **in** Y. Wir schreiben die leere Familie kurz auch als $()$.

(*viii*) Zwei Familien $(y_i)_{i\in I}$ und $(z_j)_{j\in J}$ heißen **gleichmächtig**, wenn $I \sim J$ gilt. △

In der Übung definieren wir noch die **Konkatenation** (englisch: concatenation) $F_1 \parallel F_2$ von zwei oder auch von beliebig vielen Familien $\Big\|_{i\in I} F_i$.

Da die Indexmenge I einer Familie im Allgemeinen ungeordnet ist, also keine Ordnungsrelation auf I gegeben ist, haben auch die Mitglieder der Familie $(y_i)_{i\in I}$ keine natürliche Reihenfolge. Wenn I jedoch totalgeordnet ist, dann kann diese Ordnung auf die Familie übertragen werden.

Definition 6.39 (geordnete Familie, Folge, endliche Folge, Tupel)**.**
Es seien I und Y Mengen.

(*i*) Ist I totalgeordnet, dann heißt eine Familie $(y_i)_{i\in I}$ in Y auch eine **geordnete Familie**.

(*ii*) 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.[72] Wir nennen die **Mitglieder einer Folge** auch **Glieder** (englisch: terms) der Folge oder **Folgenglieder**.

(*iii*) Ist speziell $I = [\![1, n]\!]$, so heißt $(y_i)_{i\in I}$ eine **endliche Folge** (englisch: finite sequence) **in** Y mit n Mitgliedern oder der **Länge** n (englisch: length).[73]

(*iv*) Wir können eine endliche Folge mit der Indexmenge $I = [\![1, n]\!]$ auch als n-**Tupel** (englisch: n-tuple) $(y_1, y_2, \ldots, y_n)$ notieren.[74] Insbesondere kann die leere Folge als $()$ geschrieben werden. △

Bemerkung 6.40 (Mengen und Familien)**.**

(*i*) Mengen und Familien sind konzeptionell eng verwandt, aber keine identischen Konzepte.

Jeder Familie $(y_i)_{i\in I}$ in Y können wir die **Menge ihrer Mitglieder** (englisch: set of family members) $\{y_i \mid i \in I\} \subseteq Y$ zuordnen.

Umgekehrt können wir jeder Menge Y durch Indizierung über sich selbst eine Familie in Y zuordnen, nämlich die Abbildung $Y \ni y \mapsto y \in Y$.

(*ii*) Im Unterschied zu einer Menge, die jedes ihrer Elemente nur einmal enhält, können Mitglieder einer Familie $(y_i)_{i\in I}$ mehrfach mit verschiedenen Indizes i vorkommen. △

Beispiel 6.41 (Folge)**.**

[72] Dabei wird die übliche Totalordnung „$\leqslant$“ auf $\mathbb{Z}$ genutzt, eingeschränkt auf I.
[73] Auch hier wird die übliche Totalordnung auf $\mathbb{N}$ genutzt, eingeschränkt auf I.
[74] Wir nutzen dabei also die übliche Totalordnung auf $\mathbb{N}$.

(*i*) Die Abbildung

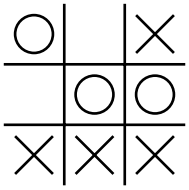
$$\mathbb{N} \ni n \mapsto y_n := \frac{1}{n} \in \mathbb{R}$$

ist eine Folge in $\mathbb{R}$ mit der Standard-Indexmenge $\mathbb{N}$. Kurz wird diese Folge auch als $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ notiert.

(*ii*) Die endliche Folge (notiert als Tupel) in $[\![1,3]\!] \times [\![1,3]\!]$

$$\big((1,3),(1,1),(3,1),(2,2),(3,3),(2,3),(3,2)\big)$$

könnte den Verlauf einer Partie Tic-Tac-Toe darstellen (bei der der erste Spieler (Kreuz) gewonnen hat).



△

§ 6.5 Das Auswahlaxiom

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

$$\forall A \in \mathcal{A}\ \big(F(A) \in A\big).$$

Eine solche Funktion F heißt eine **Auswahlfunktion** (englisch: choice function) für $\mathcal{A}$, weil sie aus jeder Menge $A \in \mathcal{A}$ irgendein Element auswählt und als Funktionswert $F(A)$ setzt. Das Auswahlaxiom besagt also, dass es möglich ist, aus jeder Menge $A \in \mathcal{A}$ ein Element auszuwählen, selbst wenn $\mathcal{A}$ aus überabzählbar vielen verschiedenen Mengen besteht und man daher nicht in der Lage ist, ein Verfahren anzugeben, nach dem die Auswahl geschehen soll.

Das Auswahlaxiom ist ein optionaler Bestandteil der axiomatischen Mengenlehre nach Zermelo und Fraenkel, es kann also dazugenommen werden oder auch nicht.[75] Es wird aber wohl von den meisten Mathematiker:innen akzeptiert. In Fällen, in denen $\mathcal{A}$ nur endlich viele Mengen enthält, wird das Auswahlaxiom nicht benötigt, weil seine Aussage bereits aus den anderen Axiomen folgt. Wir werden in der Vorlesung auf diese Weise[AoC] darauf hinweisen, wenn ein Resultat von der Hinzunahme des Auswahlaxioms abhängt. Einige Beispiele folgen bereits in diesem Abschnitt, siehe Satz 6.46.

Definition 6.42 (allgemeines kartesisches Produkt)**.**
Es sei I eine Menge, und weiter sei A_i eine Menge für jedes $i \in I$. Dann ist das **kartesische Produkt** dieser Mengen gegeben durch

$$\bigtimes_{i\in I} A_i := \left\{F\colon I \to \bigcup_{i\in I} A_i \,\middle|\, F(i) \in A_i \text{ für alle } i \in I\right\}. \tag{6.12}$$

△

Das kartesische Produkt der Mengen A_i besteht also aus *Funktionen* auf der Indexmenge I, deren Funktionswerte jeweils im richtigen „Faktor“ A_i liegen.[76] Im Fall $I = \emptyset$ besteht das kartesische Produkt (6.12) aus dem einen einzigen Element $F\colon \emptyset \to \emptyset$, der leeren Funktion, besteht.

[75] Man spricht von den ZF-Axiomen (ohne das Auswahlaxiom) und von den ZFC-Axiomen (mit Auswahlaxiom).
[76] Im Unterschied dazu liegen bei einer Familie (Definition 6.38) alle Funktionswerte in derselben Menge.

Bemerkung 6.43 (allgemeines kartesisches Produkt)**.**

(*i*) Wir hatten das **kartesische Produkt** bisher nur für endlich viele Mengen definiert, siehe Definition 4.8. Die allgemeine Definition 6.42 erfordert den Begriff der Funktion, der nun zur Verfügung steht.

(*ii*) Die Definition 6.42 lässt sich als Verallgemeinerung der Definition 4.8 verstehen: Ist nämlich die Indexmenge $I = [\![1, n]\!]$ für $n \in \mathbb{N}_0$, so ist $\bigtimes_{i\in I} A_i$ nach (6.12) die Menge aller Funktionen $F\colon [\![1, n]\!] \to \bigcup_{i=1}^{n} A_i$ mit $F(i) =: a_i \in A_i$. Wenn wir die Funktionswerte als n-Tupel $(a_1, a_2, \ldots, a_n)$ schreiben, so haben wir ein Element aus $\bigtimes_{i\in I} A_i$ gemäß Definition 4.8. Die Zuordnung $F \mapsto (a_1, a_2, \ldots, a_n)$ ist bijektiv.

(*iii*) 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.

Dabei wird $\{0,1\}^A$ manchmal auch als Schreibweise für die Potenzmenge $\mathcal{P}(A)$ verwendet. (**Quizfrage 6.7:** Inwiefern ist diese Schreibweise gerechtfertigt?) △

Wir benötigen das Auswahlaxiom beispielsweise, um das Gegenstück zu Satz 6.29 für die Charakterisierung der Surjektivität zu beweisen:

Satz 6.44 (Charakterisierung der Surjektivität$^{\text{AoC}}$)**.**
Es sei $f\colon X \to Y$ eine Funktion. Dann sind äquivalent:

(*i*) f ist surjektiv.

(*ii*) 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.

(*iii*) Für beliebige Mengen Z und beliebige Abbildungen $g_1, g_2\colon Y \to Z$ gilt: Aus $g_1 \circ f = g_2 \circ f$ folgt $g_1 = g_2$.

Wir zeigen wechselseitig alle Äquivalenzen untereinander, um zu erkennen, wo das Auswahlaxiom benötigt wird.

Beweis. Aussage (*i*) ⇒ Aussage (*ii*)$^{\text{AoC}}$: Es sei f surjektiv. Wir definieren die gesuchte Rechtsinverse $h\colon Y \to X$, indem wir zu jedem $y \in Y$ irgendein Element aus der nichtleeren Menge $f^{-1}(\{y\})$ auswählen.$^{\text{AoC}}$ Mit anderen Worten, h ist eine Auswahlfunktion zur Menge $\{f^{-1}(\{y\}) \mid y \in Y\}$. Für diese Funktion h gilt in der Tat $f(h(y)) = y$ für alle $y \in Y$, also $f \circ h = \mathrm{id}_Y$.

Aussage (*ii*) ⇒ Aussage (*i*): Da id_Y bijektiv ist, impliziert $f \circ h = \mathrm{id}_Y$ insbesondere (Lemma 6.19), dass f surjektiv ist.

Aussage (*i*) ⇒ Aussage (*iii*): Es seien f surjektiv, Z eine Menge und $g_1, g_2\colon Y \to Z$ Funktionen mit der Eigenschaft $g_1 \circ f = g_2 \circ f$. Angenommen, $g_1 \neq g_2$. Dann gibt es ein $y \in Y$ mit $g_1(y) \neq g_2(y)$. Da f surjektiv ist, existiert ein $x \in X$ mit $f(x) = y$. Es gilt also $g_1(f(x)) = g_2(f(x))$, also auch $g_1(y) = g_2(y)$, ein Widerspruch.

Aussage (iii) $\Rightarrow$ Aussage (i): Angenommen, f sei nicht surjektiv, und es sei $y_0 \in Y \setminus f(X)$. Wähle $Z := \{0,1\}$ und definiere $g_1, g_2 \colon Y \to Z$ durch

$$g_1(y) := 0 \quad \text{und} \quad g_2(y) := \begin{cases} 1 & \text{für } y = y_0, \\ 0 & \text{sonst.} \end{cases}$$

Dann haben wir $g_1 \circ f = g_2 \circ f$, aber $g_1 \neq g_2$.

Aussage (ii) $\Rightarrow$ Aussage (iii): Es seien Z eine Menge und $g_1, g_2 \colon Y \to Z$ beliebige Funktionen. Aus $g_1 \circ f = g_2 \circ f$ folgt $(g_1 \circ f) \circ h = (g_2 \circ f) \circ h$, also aufgrund der Assoziativität auch $g_1 \circ (f \circ h) = g_2 \circ (f \circ h)$, d. h., $g_1 = g_2$.

Aussage (iii) $\Rightarrow$ Aussage $(ii)^{\text{AoC}}$: Diese Aussage folgt aus den bereits bewiesenen Implikationen Aussage (iii) $\Rightarrow$ Aussage (i) und Aussage (i) $\Rightarrow$ Aussage $(ii)^{\text{AoC}}$.[77] □

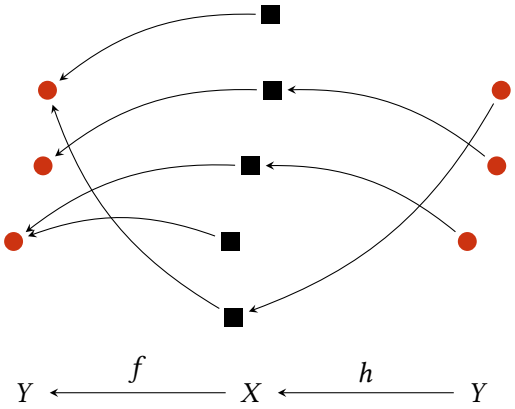


Abbildung 6.3.: Jede surjektive Funktion $f \colon X \to Y$ besitzt eine Rechtsinverse $h \colon Y \to X$ mit $f \circ h = \mathrm{id}_X$ (Satz 6.44). Die Rechtsinverse ist injektiv und i. A. nicht eindeutig.

Beispiel 6.45 (Rechtsinverse)**.**
Die Funktion $f \colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = \frac{1}{2}n$ für $n \in \mathbb{N}$ gerade und $f(n) = \frac{1}{2}(n+1)$ für $n \in \mathbb{N}$ ungerade ist surjektiv (aber nicht bijektiv). Jede Funktion $h \colon \mathbb{N} \to \mathbb{N}$ mit $h(n) \in \{2n-1, 2n\}$ für $n \in \mathbb{N}$ ist eine Rechtsinverse von f. △

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

Satz 6.46 (zum Auswahlaxiom äquivalente Aussagen)**.**
Folgende Aussagen sind in der Mengenlehre von Zermelo und Fraenkel äquivalent:

[77] Hier stellt sich die Frage, ob wir nicht vielleicht Aussage (iii) $\Rightarrow$ Aussage (ii) auch direkt beweisen könnten, ohne den Umweg über Aussage (i) zu gehen, um damit vielleicht die Abhängigkeit vom Auswahlaxiom loszuwerden. Das ist aber nicht möglich, denn könnten wir Aussage (iii) $\Rightarrow$ Aussage (ii) ohne das Auswahlaxiom beweisen, dann hätten wir zusammen mit Aussage (i) $\Rightarrow$ Aussage (iii) auch Aussage (i) $\Rightarrow$ Aussage (ii) ohne Auswahlaxiom bewiesen, was im Widerspruch zu Satz 6.46 steht.

(*i*) Es gilt das Auswahlaxiom.

(*ii*) Es sei I eine Menge, und weiter sei A_i eine Menge für jedes $i \in I$. Dann ist das kartesische Produkt $\bigtimes_{i \in I} A_i$ eine nichtleere Menge (Definition 6.42).

(*iii*) Jede Äquivalenzrelation besitzt ein Repräsentantensystem (Definition 5.21).

(*iv*) Jede surjektive Funktion besitzt eine Rechtsinverse (Satz 6.44).

(*v*) Es gilt der Wohlordnungssatz 6.47.

(*vi*) Es gilt das Lemma von Zorn 6.48.

Satz 6.47 (Wohlordnungssatz[78]).
Jede nichtleere Menge besitzt eine **Wohlordnung**, d. h., eine Totalordnung, bei der jede nichtleere Teilmenge ein kleinstes Element besitzt.[79]

Lemma 6.48 (Lemma von Zorn[80]).
Es sei X mit der Relation $\preccurlyeq$ eine halbgeordnete Menge. Weiter besitze jede totalgeordnete Teilmenge $P \subseteq X$ eine obere Schranke in X.[81] Dann existiert in X ein maximales Element.

Wir werden das Auswahlaxiom in Gestalt des Lemmas von Zorn 6.48 später noch verwenden (Satz 13.5) und aufgrund seiner Äquivalenz zum Auswahlaxiom auch dann durch die Markierung$^{\text{AoC}}$ darauf hinweisen.

Die Schwierigkeiten in der intuitiven Erfassung des Auswahlaxioms und des äquivalenten Wohlordnungssatzes 6.47 und des Lemmas von Zorn 6.48 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 7

[78] englisch: well-ordering theorem
[79] Beispielsweise ist die gewöhnliche Kleiner-Gleich-Relation eine Wohlordnung auf $\mathbb{N}$, aber nicht auf $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$.
[80] englisch: Zorn's lemma
[81] 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, 2024b, Kapitel 3.4; Fischer, Springborn, 2020, Kapitel 2.2

Definition 7.1 (Verknüpfung, Operation)**.**
Es sei M eine Menge. Eine Abbildung $\star\colon M \times M \to M$ heißt eine **(innere) Verknüpfung** oder **(innere) Operation** (englisch: (inner) operation) **auf** M. △

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

Beispiel 7.2 (Verknüpfung)**.**

(*i*) Ist M endlich, so können wir eine Verknüpfung auf M mit Hilfe einer **Verknüpfungstafel** oder **Verknüpfungstabelle** (englisch: Cayley table) definieren. Beispielsweise sehen die Verknüpfungstafeln für die **Addition modulo** 2 (englisch: addition modulo 2) und die **Multiplikation modulo** 2 (englisch: multiplication modulo 2) wie folgt aus:

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

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

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

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

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

Quizfrage 7.1: Wenn wir 0 mit *false* und 1 mit *true* identifizieren, welchen logischen Operationen (Junktoren) aus Definition 1.3 entsprechen dann $+_2$ und $\cdot_2$?

(*ii*) Die bekannten Rechenoperationen $+$ und $\cdot$ in $\mathbb{N}$

$$+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad \text{mit } (a, b) \mapsto a + b$$
$$\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad \text{mit } (a, b) \mapsto a \cdot b$$

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

(*iii*) Es seien X und Y Mengen, und auf Y sei die Verknüpfung $\star$ definiert. Dann können wir diese Verknüpfung auf die Menge der Funktionen $Y^X = \{f \mid f\colon X \to Y\}$ übertragen, indem wir sie punktweise anwenden:

$$\star\colon Y^X \times Y^X \to Y^X \quad \text{mit } f \star g \text{ definiert durch} \quad (f \star g)(x) \coloneqq f(x) \star g(x).$$

(*iv*) Beispielsweise übertragen sich die Verknüpfungen + und $\cdot$ von der Menge $\mathbb{R}$ auf die Menge der Funktionen $\mathbb{R}^X = \{f \mid f\colon X \to \mathbb{R}\}$. Es sind also die punktweise Addition und die punktweise Multiplikation durch

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

als Verknüpfungen auf der Menge der Funktionen $X \to \mathbb{R}$ definiert.

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

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

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

$$(a \star b) \star c = a \star (b \star c) \quad \text{für alle } a, b, c \in H. \tag{7.1}$$

△

Wegen der Assoziativität von $\star$ dürfen wir bei der Verknüpfung von drei oder mehr Elementen wie bei $a \star b \star c$ die Klammern weglassen.

Beispiel 7.4 (Halbgruppen, vgl. Beispiel 7.2 für die Verknüpfungen)**.**

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

(*ii*) $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ sind Halbgruppen.

(*iii*) $(\{0,1\}, +_2)$ und $(\{0,1\}, \cdot_2)$ aus Beispiel 7.2 sind Halbgruppen.

(*iv*) Es sei X eine Menge und $(H, \star)$ eine Halbgruppe. Dann ist $(H^X, \star)$ eine Halbgruppe. Die Assoziativität wird also auf die punktweise Verknüpfung vererbt.

(*v*) Insbesondere sind $(\mathbb{N}^X, +)$, $(\mathbb{N}_0^X, +)$, $(\mathbb{Z}^X, +)$, $(\mathbb{Q}^X, +)$, $(\mathbb{R}^X, +)$, $(\mathbb{C}^X, +)$ und $(\mathbb{N}^X, \cdot)$, $(\mathbb{N}_0^X, \cdot)$, $(\mathbb{Z}^X, \cdot)$, $(\mathbb{Q}^X, \cdot)$, $(\mathbb{R}^X, \cdot)$, $(\mathbb{C}^X, \cdot)$ Halbgruppen.

(*vi*) Es sei X eine Menge, dann ist $(X^X, \circ)$ eine Halbgruppe. Die Assoziativität der Komposition $\circ$ wurde in Lemma 6.17 gezeigt.

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

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

$$(x_1, \dots, x_n) \,\|\, (y_1, \dots, y_m) := (x_1, \dots, x_n, y_1, \dots, y_m).$$

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

Beispiel 7.5 (Gegenbeispiele)**.**
Keine Halbgruppen sind:

(*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 $\mathbb{Z}$, sie ist aber nicht assoziativ. Beispielsweise ist

$$3 - (2 - 1) = 2, \quad \text{aber} \quad (3 - 2) - 1 = 0.$$

(*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:

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

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

Beachte: Im Unterschied zu einer Halbgruppe ist ein Monoid immer nichtleer.

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, vgl. Beispiel 7.4 zu Halbgruppen)**.**

(*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.

[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 üblicherweise ohne die Klammern und Kommata notiert, also etwa $ab \circ ba = abba$.

(*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*) Es sei X eine Menge und $(H, \star)$ ein Monoid mit neutralem Element e. Dann ist $(H^X, \star)$ ein Monoid mit neutralem Element f, gegeben durch die konstante Funktion $f\colon X \to H$ mit $f(x) = e$ für alle $x \in X$.

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

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

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

(*x*) $(\Sigma^*, \circ)$ 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 (Links- und Rechtstranslation)**.**
Es sei $(H, \star)$ eine Halbgruppe. Für festes $b \in H$ heißen die Abbildungen

$$ {}_b\star\colon H \ni a \mapsto b \star a \in H \quad \text{die } \textbf{Linkstranslation}^{2}\textbf{um } b, \tag{7.3a} $$

$$ \star_b\colon H \ni a \mapsto a \star b \in H \quad \text{die } \textbf{Rechtstranslation}^{3}\textbf{um } b. \tag{7.3b} $$

△

Beispiel 7.10 (Links- und Rechtstranslation)**.**

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

(*ii*) In der Halbgruppe $(\mathbb{R}^{\mathbb{R}}, \circ)$ ist die Linkstranslation mit g, definiert durch $g(x) = 2\,x$, gegeben durch

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

während die Rechtstranslation mit g gegeben ist durch

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

Quizfrage 7.2: Wie lässt sich der Begriff **neutrales Element** in einer Halbgruppe mit Hilfe der Begriffe **Linkststranslation** und **Rechtstranslation** ausdrücken?

Definition 7.11 (Unterhalbgruppe, Untermonoid)**.**
Es sei $(H, \star)$ eine Halbgruppe.

(*i*) Eine Teilmenge $U \subseteq H$ heißt **abgeschlossen** (englisch: closed) bzgl. $\star$, wenn $\star\colon H \times H \to H$ eingeschränkt werden kann zu $\star_U\colon U \times U \to U$.[4] In diesem Fall heißt $\star_U$ die auf U **induzierte (innere) Verknüpfung** (englisch: induced (inner) operation, lateinisch: inducere: hineinführen).

[2] englisch: left translation, lateinisch: translatio: Übertragung, Verschiebung

[3] englisch: right translation

[4] Mit der Notation aus Bemerkung 7.20 können wir die Abgeschlossenheit von U auch als $U \star U \subseteq U$ schreiben.

(*ii*) Eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq H$ mit der Verknüpfung $\star_U$ heißt **Unterhalbgruppe** (englisch: subsemigroup) **von** $(H, \star)$.[5] Manchmal schreibt man dies als $(U, \star_U) \leqslant (H, \star)$.

(*iii*) Ist $(H, \star)$ ein Monoid mit neutralem Element e, dann heißt eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq H$, die auch das neutrale Element e enthält, ein **Untermonoid** (englisch: submonoid) **von** $(H, \star)$.

(*iv*) Eine Unterhalbgruppe oder ein Untermonoid $(U, \star_U)$ von $(H, \star)$ heißt **echt** (englisch: proper subsemigroup, proper submonoid), wenn $U \subsetneq H$ gilt. △

Der Einfachheit halber werden wir in Zukunft statt $\star_U$ einfach $\star$ schreiben. Wir werden außerdem auch einfach die Menge U als Unterhalbgruppe bzw. Untermonoid von $(H, \star)$ bezeichnen, weil sich die Verknüpfung auf U ja durch Einschränkung der Verknüpfung $\star$ auf H ergibt.

Beispiel 7.12 (Unterhalbgruppe, Untermonoid)**.**

(*i*) Die geraden Zahlen bilden ein Untermonoid von $(\mathbb{Z}, +)$ mit neutralem Element 0.

(*ii*) Es seien a, b, c paarweise verschieden. $(\mathcal{P}(\{a, b\}), \cap)$ bildet zwar eine Unterhalbgruppe des Monoids $(\mathcal{P}(\{a, b, c\}), \cap)$, aber kein Untermonoid, denn das neutrale Element $\{a, b, c\}$ fehlt in $\mathcal{P}(\{a, b\})$. Vielmehr ist $(\mathcal{P}(\{a, b\}), \cap)$ ein Monoid mit einem anderen neutralen Element, nämlich $\{a, b\}$, siehe Beispiel 7.8. △

Bemerkung 7.13 („Unterhalbgruppe sein“ und „Untermonoid sein“ sind Ordnungsrelationen)**.**

(*i*) Die Relation „ist Unterhalbgruppe von“ ist eine partielle Ordnung auf der Klasse aller Halbgruppen.

Insbesondere ist die Menge aller Unterhalbgruppen einer bestimmten Halbgruppe $(H, \star)$ durch die Unterhalbgruppenhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein.[6]

(*ii*) Auch die Relation „ist Untermonoid von“ ist eine partielle Ordnung auf der Klasse aller Monoide.

Insbesondere ist die Menge aller Untermonoide eines bestimmten Monoids $(H, \star)$ durch die Untermonoidhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein. △

Definition 7.14 (invertierbare Elemente)**.**
Es sei $(H, \star)$ ein Monoid. Ein Element $a \in H$ heißt **invertierbar** (englisch: invertible) oder eine **Einheit** (englisch: unit) von $(H, \star)$, wenn ein $a' \in H$ existiert mit

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

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

[5] Da die Assoziativät durch die Einschränkung der Verknüpfung nicht verlorengeht, ist $(U, \star_U)$ wieder eine Halbgruppe mit der eingeschränkten Verknüpfung $\star_U$.

[6] Das heißt: Sind H_1, H_2 Unterhalbgruppen von H, und gilt $H_1 \subseteq H_2$, dann ist H_1 auch eine Unterhalbgruppe von H_2.

Lemma 7.15 (inverse Elemente sind eindeutig)**.**
Es sei $(H, \star)$ ein Monoid mit neutralem Element e. Ist $a \in H$ invertierbar und sind a'_1 und a'_2 beides Inverse zu a, dann gilt $a'_1 = a'_2$.

Beweis. Es gilt

$$\begin{aligned} a'_1 &= a'_1 \star e \\ &= a'_1 \star (a \star a'_2) \\ &= (a'_1 \star a) \star a'_2 \\ &= e \star a'_2 \\ &= a'_2. \end{aligned}$$

□

Beachte: Die Definition (7.4) besagt nicht nur, dass a' das Inverse zu a ist, sondern auch, dass a das Inverse zu a' ist. Die Invertierung ist also **involutorisch** (englisch: involutory), d. h., für alle invertierbaren $a \in H$ gilt

$$(a')' = a. \tag{7.5}$$

Quizfrage 7.3: Welches Element eines Monoids ist immer invertierbar? Was ist sein Inverses?

Lemma 7.16 (invertierbare Elemente bilden ein Untermonoid)**.**
Es sei $(H, \star)$ ein Monoid mit neutralem Element e. Dann bildet die Teilmenge der invertierbaren Elemente

$$E := \{a \in H \mid a \text{ ist invertierbar}\} \tag{7.6}$$

ein Untermonoid von $(H, \star)$. Sind $a, b \in E$ und a', b' die zugehörigen inversen Elemente in H, dann gilt für das zu $a \star b$ inverse Element

$$(a \star b)' = b' \star a'. \tag{7.7}$$

Beweis. Zunächst gilt für das neutrale Element $e \in E$ wegen $e \star e = e$, also $e' = e$. Es seien nun $a, b \in E$. Dann gilt

$$\begin{aligned} &(a \star b) \star (b' \star a') = a \star (b \star b') \star a' = a \star e \star a' = a \star a' = e \\ \text{und} \quad &(b' \star a') \star (a \star b) = b' \star (a' \star a) \star b = b' \star e \star b = b' \star b = e. \end{aligned}$$

Das zeigt, dass $a \star b$ wieder invertierbar und dass $b' \star a'$ das Inverse zu $a \star b$ ist, also (7.7). Das heißt aber auch, dass E bzgl. $\star$ abgeschlossen ist, also bildet E ein Untermonoid von $(H, \star)$. □

Beispiel 7.17 (invertierbare Elemente in Monoiden)**.**

(*i*) $(\mathbb{N}, +)$ besitzt kein neutrales Element, also können wir auch nicht von invertierbaren Elementen sprechen.

(*ii*) In $(\mathbb{N}_0, +)$ ist nur das neutrale Element 0 invertierbar.

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

(*iv*) In $(\mathbb{N}, \cdot)$ ist nur das neutrale Element 1 invertierbar.

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

(*vi*) 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 $1/a$ oder $\frac{1}{a}$ bezeichnet. Allgemeiner steht $\frac{a}{b}$ für $a \cdot b^{-1} = b^{-1} \cdot a$, wobei $b \neq 0$ vorausgesetzt wird.[7]

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

(*viii*) In $(\{0,1\}, \cdot_2)$ aus Beispiel 7.2 ist nur das neutrale Element 1 invertierbar.

(*ix*) In $(X^X, \circ)$ sind die invertierbaren Elemente genau die bijektiven Funktionen $X \to X$, also die invertierbaren Funktionen. △

Quizfrage 7.4: Was sind die invertierbaren Elemente in den Monoiden $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \cup)$ und $(\mathcal{P}(X), \triangle)$?

Lemma 7.18 (invertierbare Elemente können gekürzt werden)**.**
Es sei $(H, \star)$ ein Monoid. Ist $a \in H$ invertierbar, dann gelten die **Kürzungsregeln** (englisch: cancellation rules)

$$a \star b_1 = a \star b_2 \quad \Rightarrow \quad b_1 = b_2 \tag{7.8a}$$
$$b_1 \star a = b_2 \star a \quad \Rightarrow \quad b_1 = b_2 \tag{7.8b}$$

für beliebige $b_1, b_2 \in H$.

Beweis. Es gilt

$$\begin{aligned}
& a \star b_1 = a \star b_2 \\
\Rightarrow\ & a' \star (a \star b_1) = a' \star (a \star b_2) && \text{denn } a \text{ ist invertierbar} \\
\Rightarrow\ & (a' \star a) \star b_1 = (a' \star a) \star b_2 && \text{wegen der Assoziativität von } \star \\
\Rightarrow\ & e \star b_1 = e \star b_2 && \text{da } a' \text{ invers zu } a \text{ ist} \\
\Rightarrow\ & b_1 = b_2 && \text{wegen der Eigenschaften von } e.
\end{aligned}$$

Die Aussage (7.8b) folgt analog. □

Lemma 7.19 (Nachweis von Inversen)**.**
Es sei $(H, \star)$ ein Monoid mit neutralem Element e und $a, b \in H$. Gilt $a \star b = e$ und ist a oder b bereits als invertierbar bekannt, dann sind a und b beide invertierbar und gegenseitig Inverse voneinander.

Beachte: Wenn man also schon weiß, dass z. B. das Element a eines Monoids invertierbar ist, dann reicht es für den Nachweis, dass ein Element b das Inverse zu a ist, aus, a und b in einer der beiden Reihenfolgen miteinander zu verknüpfen

[7] Aus dem Symbol $\frac{a}{b}$ geht (anders als bei $a - b$) nicht hervor, ob $a \cdot b^{-1}$ oder $b^{-1} \cdot a$ gemeint ist. Wir verwenden daher das Symbol $\frac{a}{b}$ in allgemeinen, multiplikativ notierten Halbgruppen (Bemerkung 7.20) nur dann, wenn die Verknüpfung kommutativ ist (Definition 7.27), wenn also $a \cdot b^{-1} = b^{-1} \cdot a$ gilt.

Beweis. Es sei a invertierbar und $a \star b = e$. Das inverse Element zu a sei a'. Dann gilt $a' = a' \star (a \star b) = (a' \star a) \star b = b$. Ist dagegen b invertierbar und $a \star b = e$ und ist b' das inverse Element zu b, dann gilt $b' = (a \star b) \star b' = a \star (b \star b') = a$. □

Bemerkung 7.20 (abkürzende Schreibweisen in Halbgruppen)**.**

(*i*) Wir haben als „neutrale" Notation der Verknüpfung einer Halbgruppe H das Symbol $\star$ gewählt, e als Bezeichnung für das neutrale Element und a' für das zu a inverse Element (sofern existent).

Für Teilmengen $A, B \subseteq H$ und $c \in H$ definieren wir die Mengenschreibweisen[8]

$$\begin{aligned} c \star A &:= \{c \star a \mid a \in A\}, \\ A \star c &:= \{a \star c \mid a \in A\}, \\ A \star B &:= \{a \star b \mid a \in A,\ b \in B\}. \end{aligned}$$

Ist $(H, \star)$ ein Monoid und sind alle Elemente in A invertierbar, so definieren wir auch

$$A' := \{a' \mid a \in A\}.$$

(*ii*) Bezeichnen wir dagegen die Verknüpfung einer Halbgruppe H als „Addition" und notieren sie als „+" o. ä. (**additive Notation**, englisch: additive notation), so nennen wir ein eventuell existierendes neutrales Element auch **Nullelement** (englisch: additive identity, zero element) oder **Null** (englisch: zero), geschrieben als „0_H" oder einfach 0.

Für $n \in \mathbb{N}$ und $a \in H$ ist $n\,a$ eine Abkürzung für $a + \cdots + a$ (n-mal).[9] (**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 $0\,a := 0_H$.

Ist weiter $a \in H$ invertierbar, so notieren wir das Inverse als $-a$. Dann ist auch $n\,a$ invertierbar für $n \in \mathbb{N}_0$, und wir setzen $(-n)\,a := -(n\,a) = n\,(-a)$. (**Quizfrage 7.6:** Warum gilt $-(n\,a) = n\,(-a)$?) Insbesondere ist $(-1)\,a := -a$ und $(-0)\,a := -(0\,a) = -0_H = 0_H$.

Es gilt

$$n\,(m\,a) = (n \cdot m)\,a \quad \text{und} \quad (n+m)\,a = n\,a + m\,a \tag{7.9}$$

für alle $n, m \in \mathbb{N}$ bzw. $n, m \in \mathbb{N}_0$ bzw. $n, m \in \mathbb{Z}$. (**Quizfrage 7.7:** Ist Ihnen in (7.9) bei jeder Operation klar, worum es sich handelt?)

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

Für Teilmengen $A, B \subseteq H$ und $c \in H$ definieren wir die Mengenschreibweisen

$$\begin{aligned} c + A &:= \{c + a \mid a \in A\}, \\ A + c &:= \{a + c \mid a \in A\}, \\ A + B &:= \{a + b \mid a \in A,\ b \in B\}. \end{aligned}$$

Ist $(H, +)$ ein Monoid und sind alle Elemente in A invertierbar, so definieren wir auch

$$-A := \{-a \mid a \in A\}.$$

[8] Im Fall $A = \emptyset$ sind auch die Mengen $c \star A$, $A \star c$, $A \star B$ und A' leer. Auch im Fall $B = \emptyset$ ist $A \star B$ die leere Menge.

[9] Zur Verdeutlichung notieren wir vorübergehend alle Vorfaktoren in dieser Farbe. Diese sind keine Elemente der Halbgruppe, sondern Elemente aus $\mathbb{N}$ bzw. $\mathbb{Z}$.

(*iii*) Bezeichnen wir die Verknüpfung einer Halbgruppe H als „Multiplikation“ und notieren sie als „$\cdot$“ o. ä. (**multiplikative Notation**, englisch: multiplicative notation), so nennen wir ein eventuell existierendes neutrales Element auch **Einselement** (englisch: multiplicative identity, one element, unit element) oder **Eins** (englisch: one, unit), geschrieben als „1_H“ oder einfach 1.

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

Besitzt $(H, \cdot)$ das neutrale Element 1_H, so definieren wir auch $a^0 := 1_H$.

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

Es gilt

$$(a^n)^m = a^{n \cdot m} \quad \text{und} \quad a^{n+m} = a^n \cdot a^m \tag{7.10}$$

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

Für Teilmengen $A, B \subseteq H$ und $c \in H$ definieren wir die Mengenschreibweisen

$$\begin{aligned} c \cdot A &:= \{c \cdot a \mid a \in A\}, \\ A \cdot c &:= \{a \cdot c \mid a \in A\}, \\ A \cdot B &:= \{a \cdot b \mid a \in A,\ b \in B\}. \end{aligned}$$

Ist $(H, \cdot)$ ein Monoid und sind alle Elemente in A invertierbar, so definieren wir auch

$$A^{-1} := \{a^{-1} \mid a \in A\}.$$

(*iv*) Bezeichnen wir die Verknüpfung einer Halbgruppe H als „Komposition“ und notieren sie als „$\circ$“ o. ä. (**Kompositionsnotation**, englisch: compositional notation), so nennen wir ein eventuell existierendes neutrales Element auch **Identität** (englisch: identity), geschrieben als „id_H“ oder einfach „id“. In diesem Fall benutzen wir dieselbe Notation wie im Fall multiplikativer Notation:

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

Besitzt $(H, \circ)$ das neutrale Element id_H, so definieren wir auch $a^0 := \mathrm{id}_H$.

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

Es gilt

$$(a^n)^m = a^{n \cdot m} \quad \text{und} \quad a^{n+m} = a^n \circ a^m \tag{7.11}$$

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

Für Teilmengen $A, B \subseteq H$ und $c \in H$ definieren wir die Mengenschreibweisen

$$\begin{aligned} c \circ A &:= \{c \circ a \mid a \in A\}, \\ A \circ c &:= \{a \circ c \mid a \in A\}, \\ A \circ B &:= \{a \circ b \mid a \in A,\ b \in B\}. \end{aligned}$$

Ist $(H, \circ)$ ein Monoid und sind alle Elemente in A invertierbar, so definieren wir auch

$$A^{-1} := \{a^{-1} \mid a \in A\}. \qquad \triangle$$

Ende der Vorlesung 8

Ende der Woche 4

§ 7.2 Gruppen

Definition 7.21 (Gruppe)**.**
Ein Monoid $(H, \star)$ heißt eine **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 7.22 (Gruppen und Gegenbeispiele, vgl. Beispiel 7.17 zu Monoiden und ihren invertierbaren Elementen)**.**

(*i*) $(\mathbb{N}_0, +)$ ist ein Monoid, aber keine Gruppe, da nur das neutrale Element 0 invertierbar ist.

(*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 $a^{-1} = 1/a \in \mathbb{Q}_{\neq 0}$. Dasselbe gilt für $(\mathbb{R}_{\neq 0}, \cdot)$ und $(\mathbb{C}_{\neq 0}, \cdot)$.

(*v*) Für $m \in \mathbb{N}$ bildet die Menge $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ mit der Verknüpfung $+_m$ eine Gruppe. Dabei ist die **Addition modulo** m (englisch: addition modulo m) $+_m$ definiert als[10]

$$\begin{aligned} a +_m b &:= \begin{cases} a + b, & \text{falls } a + b \leqslant m - 1 \\ a + b - m, & \text{falls } a + b \geqslant m \end{cases} \\ &= \text{der natürliche Repräsentant von } a + b \text{ in der Restklasse } [a + b] \text{ modulo } m \\ &= \text{Rest von } a + b \text{ bei ganzzahliger Division durch } m. \end{aligned} \tag{7.12}$$

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 $m \in \mathbb{N}$ bildet die Menge $\mathbb{Z}_m$ mit der Verknüpfung $\cdot_m$ ein Monoid. Dabei ist $\cdot_m$ die **Multiplikation modulo** m (englisch: multiplication modulo m) definiert als[11]

$$\begin{aligned} a \cdot_m b &:= \text{der natürliche Repräsentant von } a \cdot b \text{ in der Restklasse } [a \cdot b] \text{ modulo } m \\ &= \text{Rest von } a \cdot b \text{ bei ganzzahliger Division durch } m. \end{aligned} \tag{7.13}$$

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

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

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

$(\mathbb{Z}_m, \cdot_m)$ ist genau dann eine Gruppe, wenn $m = 1$ ist, also wenn $\mathbb{Z}_m = \{0\}$ gilt.[12]

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

(*vii*) Es sei X eine Menge und $(G, \star)$ eine Gruppe. Dann ist $(G^X, \star)$ eine Gruppe.

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

(*ix*) $(\mathbb{R}^X, \cdot)$ 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.

(*x*) $(X^X, \circ)$ 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.

(*xi*) Die **Kleinsche Vierergruppe** (englisch: Klein four-group) K_4 ist eine kommutative Gruppe mit vier Elementen und der folgenden Verknüpfungstafel:

$\circ$	e	h	v	r
e	e	h	v	r
h	h	e	r	v
v	v	r	e	h
r	r	v	h	e

Das neutrale Element wird hier als e bezeichnet. Jedes Element ist selbstinvers. Die Gruppe kann verstanden werden als die **Symmetriegruppe** (englisch: symmetry group) eines Rechtecks $\begin{smallmatrix} D & & C \\ & \square & \\ A & & B \end{smallmatrix}$, also als die Menge der Abbildungen eines Rechtecks auf sich selbst. Dabei steht

e für die identische Abbildung $\begin{smallmatrix} D & & C \\ & \square & \\ A & & B \end{smallmatrix}$

h für die horizontale Spiegelung $\begin{smallmatrix} C & & D \\ & \square & \\ B & & A \end{smallmatrix}$

v für die vertikale Spiegelung $\begin{smallmatrix} A & & B \\ & \square & \\ D & & C \end{smallmatrix}$

r für die Drehung um 180° $\begin{smallmatrix} B & & A \\ & \square & \\ C & & D \end{smallmatrix}$. △

Lemma 7.23 (Einheitengruppe, vgl. Lemma 7.16)**.**
Es sei $(H, \star)$ ein Monoid. Dann ist das Untermonoid der invertierbaren Elemente (Lemma 7.16)

$$E \coloneqq \{a \in H \mid a \text{ ist invertierbar}\} \tag{7.14}$$

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

Beweis. Wir wissen nach Lemma 7.16 bereits, dass E ein Monoid ist (nämlich ein Untermonoid von H). Per Definition sind alle Elemente von E invertierbar, also ist E eine Gruppe. □

[12] In diesem Fall ist $(\mathbb{Z}_1, \cdot_1)$ isomorph (Definition 8.1) zu $(\mathbb{Z}_1, +_1)$, also abgesehen von der Notation dieselbe Gruppe.

Beispiel 7.24 (Einheitengruppe)**.**

(*i*) Es sei X eine Menge und $(H, \star)$ ein Monoid. Die Einheitengruppe von $(H^X, \star)$ besteht genau aus denjenigen Funktionen $X \to H$, die nur Funktionswerte in der Einheitengruppe von H annehmen. (**Quizfrage 7.8:** Wie sieht das Inverse eines Elements der Einheitengruppe von H^X aus?)

(*ii*) Es sei X eine Menge. Die Einheitengruppe des Monoids $(X^X, \circ)$ (Beispiel 7.22) besteht genau aus den invertierbaren (bijektiven) Funktionen $X \to X$. △

Quizfrage 7.9: Können Sie die Multiplikationstabellen für $(\mathbb{Z}_m, \cdot_m)$ im Fall $m = 5$ und $m = 8$ aufstellen (Beispiel 7.22)? Haben Sie eine Vermutung, was die Einheitengruppe von $(\mathbb{Z}_m, \cdot_m)$ für $m \in \mathbb{N}$ ist, also welche Elemente in $(\mathbb{Z}_m, \cdot_m)$ invertierbar sind?

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

Lemma 7.25 (Gruppenkriterium mit Links- und Rechtstranslationen („**Sudoku-Kriterium**“))**.**

(*i*) Ist $(G, \star)$ eine Gruppe, so sind die Links- und Rechtstranslationen $\star_a$ und ${}_a\star$ für alle $a \in G$ bijektive Abbildungen $G \to G$.

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

Beweis. Dieser Beweis ist Gegenstand der Übung. □

Beispiel 7.26 (Sudoku-Kriterium)**.**
Gegeben ist die Menge $M := \{\heartsuit, \boxtimes, \CIRCLE, \otimes, \blacklozenge, \rhd\}$ mit zwei Verknüpfungen $\star$ und $\square$ wie folgt:

$\star$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\blacklozenge$	$\CIRCLE$	$\rhd$	$\heartsuit$	$\otimes$	$\blacklozenge$	$\boxtimes$
$\boxtimes$	$\heartsuit$	$\otimes$	$\CIRCLE$	$\rhd$	$\boxtimes$	$\blacklozenge$
$\heartsuit$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\CIRCLE$	$\blacklozenge$	$\heartsuit$	$\rhd$	$\boxtimes$	$\CIRCLE$	$\otimes$
$\otimes$	$\rhd$	$\boxtimes$	$\blacklozenge$	$\heartsuit$	$\otimes$	$\CIRCLE$
$\rhd$	$\otimes$	$\blacklozenge$	$\boxtimes$	$\CIRCLE$	$\rhd$	$\heartsuit$

$\square$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\blacklozenge$	$\blacklozenge$	$\CIRCLE$	$\heartsuit$	$\blacklozenge$	$\heartsuit$	$\CIRCLE$
$\boxtimes$	$\boxtimes$	$\CIRCLE$	$\otimes$	$\blacklozenge$	$\heartsuit$	$\rhd$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\CIRCLE$	$\CIRCLE$	$\blacklozenge$	$\heartsuit$	$\CIRCLE$	$\heartsuit$	$\blacklozenge$
$\otimes$	$\otimes$	$\CIRCLE$	$\boxtimes$	$\heartsuit$	$\heartsuit$	$\otimes$
$\rhd$	$\rhd$	$\blacklozenge$	$\otimes$	$\CIRCLE$	$\heartsuit$	$\boxtimes$

Beide Verknüpfungen sind assoziativ, d. h., $(M, \star)$ und $(M, \square)$ sind beides Halbgruppen. Die Funktionswerte der Linkstranslationen finden wir in den Zeilen der jeweiligen Verknüpfungstafel, während sich die Funktionswerte der Rechtstranslationen in den Spalten wiederfinden.

Bei $(M, \star)$ handelt es sich tatsächlich um eine Gruppe, denn alle Linkstranslationen und alle Rechtstranslationen sind surjektiv. Das erkennen wir daran, dass in jeder Zeile und in jeder Spalte der Verknüpfungstafel alle Elemente der Menge M vorkommen.[13] Das neutrale Element ist $\heartsuit$, denn die entsprechende Zeile ist identisch mit der Zeile aus dem Tabellenkopf.

[13] Da M endlich ist, kommen die Elemente von M in jeder Zeile und jeder Spalte jeweils genau einmal vor. Die Translationen sind also sogar alle bijektiv, vgl. Satz 6.35.

$(M, \square)$ ist dagegen keine Gruppe, da beispielsweise die Linkstranslation (Zeile) mit $\heartsuit$ nicht surjektiv ist. △

Definition 7.27 (kommutative Verknüpfung, Halbgruppe, Monoid, Gruppe)**.**

(*i*) Es sei M eine Menge mit einer Verknüpfung $\star$. Die Elemente $a, b \in M$ **vertauschen** oder **kommutieren** (englisch: commute) bzgl. der Verknüpfung $\star$, wenn $a \star b = b \star a$ gilt.

(*ii*) Die Verknüpfung $\star$ auf der Menge M heißt **kommutativ** (englisch: commutative) oder **abelsch** (englisch: Abelian), wenn $a \star b = b \star a$ für alle $a, b \in M$ gilt.

(*iii*) Eine Halbgruppe bzw. ein Monoid bzw. eine Gruppe $(H, \star)$ heißt **kommutativ** oder **abelsch**, wenn die Verknüpfung $\star$ kommutativ ist. △

Bemerkung 7.28 (zur abkürzenden Notation in Halbgruppen (Bemerkung 7.20))**.**

(*i*) Es ist üblich, die additive Notation (Bemerkung 7.20) nur für kommutative Verknüpfungen zu verwenden. Nur im kommutativen Fall verwenden wir auch das Summenzeichen, etwa in den Ausdrücken

$$\sum_{j=1}^{n} a_j \quad \text{oder} \quad \sum_{a \in A} a.$$

(*ii*) Multiplikativ notierte Verknüpfungen können kommutativ oder nicht kommutativ sein. Nur im kommutativen Fall verwenden wir auch das Produktzeichen, etwa in den Ausdrücken

$$\prod_{j=1}^{n} a_j \quad \text{oder} \quad \prod_{a \in A} a.$$

(*iii*) Als Komposition notierte Verknüpfungen sind i. d. R. nicht kommutativ. △

Beispiel 7.29 (kommutative Halbgruppen und Gruppen, vgl. Beispiele 7.4 und 7.22)**.**

Die Verknüpfungen „+“ und „·“ auf $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind kommutativ. Beispielsweise ist also $(\mathbb{N}, +)$ eine kommutative Halbgruppe, $(\mathbb{N}_0, +)$ ein kommutatives Monoid, und $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind kommutative Gruppen. △

§ 7.3 Die symmetrische Gruppe

Definition 7.30 (symmetrische Gruppe)**.**

Es sei X eine Menge und $S(X) := \{f \colon X \to X \mid f \text{ ist bijektiv}\}$. 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 $n \in \mathbb{N}_0$, so schreiben wir statt $S([\![1, n]\!])$ 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 7.24 ist $S(X)$ tatsächlich eine Gruppe, nämlich die Einheitengruppe von $(X^X, \circ)$. Das neutrale Element ist id_X. Wenn X drei oder mehr Elemente enthält, dann ist $(S(X), \circ)$ nicht kommutativ, ansonsten kommutativ.

Im Folgenden werden wir nur noch symmetrische Gruppen S_n für $n \in \mathbb{N}_0$ betrachten. Eine Permutation $\sigma \in S_n$ können wir z. B. 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 $n \in \mathbb{N}_0$ ist gleich $n!$ („n Fakultät“). Das stimmt auch für $n = 0$, denn es gilt $0! = 1$, und die einzige Permutation ist die leere Permutation.

Beispiel 7.31 (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, vgl. Abbildung 7.1. 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 oben behauptet tatsächlich nicht kommutativ. △

Definition 7.32 (Transposition)**.**
Eine Permutation $\sigma \in S_n$, $n \in \mathbb{N}_0$, heißt eine **Transposition** (englisch: transposition, lateinisch: transponere: umstellen), 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 verschiedene Elemente von $[\![1, n]\!]$ und lässt den Rest unverändert. (Daher gibt es Transpositionen nur im Fall $n \geqslant 2$.) Offenbar gilt für jede Transposition

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

Transpositionen sind also Involutionen (Definition 6.18) und damit selbstinverse Elemente der Gruppe S_n.

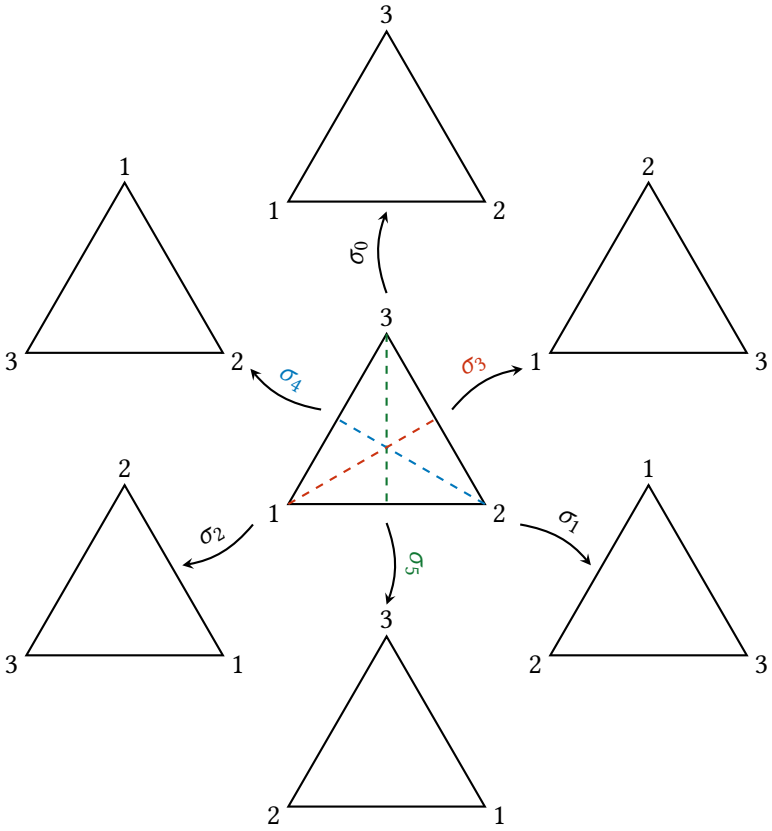


Abbildung 7.1.: Illustration der Elemente der symmetrischen Gruppe S_3, siehe Beispiel 7.31. Die Permutationen σ_0, σ_1 und σ_2 entsprechenden Drehungen. Die Permutationen σ_3, σ_4 und σ_5 sind genau die Transpositionen. Sie entsprechenden den Spiegelungen um die farbig eingezeichneten Achsen.

(**Quizfrage 7.10:** Wieviele verschiedene Transpositionen gibt es in S_n?)

(**Quizfrage 7.11:** Können Sie eine Vermutung anstellen, welche Permutationen von S_n neben den Transpositionen noch selbstinvers sind?)

Satz 7.33 (Darstellung von Permutationen als Komposition von Transpositionen)**.**
Es sei $n \in \mathbb{N}_0$. Jede Permutation $\sigma \in S_n$ lässt sich als Komposition von $0 \leqslant r \leqslant n-1$ Transpositionen schreiben (bzw. $r = 0$ im Fall $n = 0$).[14]

Beweis. Wir zeigen die Behauptung für $n \in \mathbb{N}_0$ durch vollständige Induktion. Induktionsanfang: Das einzige Element von

$$S_0 = \{\emptyset \to \emptyset\}$$

ist eine Komposition von $r = 0$ Transpositionen. Ebenso ist das einzige Element von

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

[14] Insbesondere bildet die Menge der Transpositionen also ein Erzeugendensystem von S_n.

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 $\widetilde{\sigma} := \tau(m,n+1) \circ \sigma \in S_{n+1}$ gilt dann $\widetilde{\sigma}(n+1) = n+1$. Aufgrund von Fall 1 gilt $\widetilde{\sigma} = \tau_1 \circ \cdots \circ \tau_r$ mit $0 \leqslant r \leqslant n-1$. Die Behauptung folgt jetzt aus der Darstellung $\sigma = \tau(m,n+1) \circ \widetilde{\sigma} = \tau(m,n+1) \circ \tau_1 \circ \cdots \circ \tau_r$. □

Beispiel 7.34 (Darstellung von Permutationen als Komposition von Transpositionen)**.**

Wir können die Zerlegung einer Permutation $\sigma \in S_n$ bestimmen, indem wir die Bilder durch wiederholte Anwendung von Transpositionen z. B. von hinten nach vorne in die richtige Reihenfolge bringen, etwa:

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} \xrightarrow{\tau(4,1)\circ} \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$$ die 4 ist jetzt an der richtigen Stelle

$$\xrightarrow{\tau(3,1)\circ} \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$$ auch die 3 ist jetzt an der richtigen Stelle

$$\xrightarrow{\tau(2,1)\circ} \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$ auch die 1 und die 2 sind jetzt an der richtigen Stelle.

Das heißt also,

$$\tau(2,1) \circ \tau(3,1) \circ \tau(4,1) \circ \sigma = \mathrm{id} \quad \text{oder aber} \quad \sigma = \tau(4,1) \circ \tau(3,1) \circ \tau(2,1). \qquad \triangle$$

Man kann allgemein zeigen, dass genau solche zyklischen Vertauschungen σ wie in Beispiel 7.34 nicht mit weniger als $r = n-1$ (hier also $r = 3$) Permutationen dargestellt werden können. Die obere Schranke für die benötigte Anzahl an Transpositionen aus Satz 7.33 ist also scharf.

Die Darstellung einer Permutation als Komposition von Transpositionen ist nicht eindeutig. Jedoch ist die Anzahl der benötigten Transpositionen entweder immer gerade oder immer ungerade, wie wir gleich beweisen werden (Folgerung 7.41).

Definition 7.35 (Fehlstand, Signum einer Permutation)**.**

Es sei $n \in \mathbb{N}_0$ 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[15]

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

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

Beispiel 7.36 (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

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

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 7.37 (zu Definition 7.35)**.**
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 7.38 (Transpositionen sind ungerade)**.**
Ist $\tau \in S_n$, $n \in \mathbb{N}_0$, eine Transposition, so gilt $\operatorname{sgn}\tau = -1$.

[15] Definitionsgemäß wird das im Fall $n = 0$ und $n = 1$ leere Produkt als das neutrale Element der Multiplikation (hier in $\mathbb{Q}$), also als 1, interpretiert.

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

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

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

Beispiel 7.39 (Transpositionen sind ungerade)**.**
Zur Veranschaulichung des Beweises von Lemma 7.38 betrachten wir die Permutation in S_7

$$\tau(i,j) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 \end{pmatrix}$$

mit $i = 3$ und $j = 6$. Diese hat genau die Fehlstände $(3,4)$, $(3,5)$, $(3,6)$ sowie $(4,6)$, $(5,6)$. △

Satz 7.40 (Signum ist verträglich mit der Komposition von Permutationen)**.**
Es sei $n \in \mathbb{N}_0$ 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. Notwendigerweise gilt wieder $n \geqslant 2$, damit überhaupt Permutationen existieren.

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 sind die Anzahlen der Fehlstände von σ_2 und von $\tau(k,k+1) \circ \sigma_2$ um 1 verschieden. Damit ist

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

gezeigt.

Schritt 2: Wir beweisen den Satz für den Spezialfall, dass $\tau(k,\ell)$ eine beliebige Transposition ist.

Wir können o. B. d. A. $\ell > k$ annehmen, 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 jeweils benachbarter Elemente schreiben.[16] Aufgrund von Schritt 1 und der Assoziativität der Komposition haben wir nun also

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

Schritt 3: Schließlich können wir den allgemeinen Fall zeigen.

Ist $\sigma_1\in S_n$ eine beliebige Permutation, so können wir sie nach Satz 7.33 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:

$$\begin{aligned}
&\operatorname{sgn}(\sigma_1\circ\sigma_2)\\
&\quad=\operatorname{sgn}(\tau_1\circ\cdots\circ\tau_r\circ\sigma_2)\\
&\quad=(\operatorname{sgn}\tau_1)\cdot\operatorname{sgn}(\cdots\circ\tau_r\circ\sigma_2)\\
&\quad=\cdots\\
&\quad=(\operatorname{sgn}\tau_1)\cdots(\operatorname{sgn}\tau_r)(\operatorname{sgn}\sigma_2)\\
&\quad=\cdots\\
&\quad=\operatorname{sgn}(\tau_1\circ\cdots\circ\tau_r)\cdot\operatorname{sgn}(\sigma_2).
\end{aligned}$$

□

Folgerung 7.41 (zu Satz 7.40)**.**
Es sei $n\in\mathbb{N}_0$ und σ eine Permutation in S_n.

(*i*) Ist $\sigma=\sigma_1\circ\cdots\circ\sigma_s$ dargestellt als Komposition[17] 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 $\operatorname{sgn}\mathrm{id}=1$.

(*iv*) Es gilt $\operatorname{sgn}\sigma=\operatorname{sgn}\sigma^{-1}$.

[16] Beispielsweise im Fall $k=3$ und $\ell=6$ haben wir

$$\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&4&5&6&7\end{pmatrix}\xrightarrow{\tau(4,3)\circ}\begin{pmatrix}1&2&3&4&5&6&7\\1&2&4&3&5&6&7\end{pmatrix}\xrightarrow{\tau(5,4)\circ}\begin{pmatrix}1&2&3&4&5&6&7\\1&2&5&3&4&6&7\end{pmatrix}\xrightarrow{\tau(6,5)\circ}\begin{pmatrix}1&2&3&4&5&6&7\\1&2&6&3&4&5&7\end{pmatrix}$$
$$\xrightarrow{\tau(4,5)\circ}\begin{pmatrix}1&2&3&4&5&6&7\\1&2&6&3&5&4&7\end{pmatrix}\xrightarrow{\tau(3,4)\circ}\begin{pmatrix}1&2&3&4&5&6&7\\1&2&6&4&5&3&7\end{pmatrix}.$$

wodurch in der Tat $3\leftrightarrow 6$ getauscht sind.

[17] Vereinbarungsgemäß ist die Verknüpfung von null Permutationen das neutrale Element in S_n, also die identische Abbildung id.

Beweis. Aussage (i): Nach Satz 7.40 ist das Signum einer Komposition von zwei Permutationen gleich dem Produkt der Signa der beiden Faktoren. Wie im Beweis von Satz 7.40 können wir die Aussage leicht auf mehr als zwei Faktoren ausdehnen. Die Fälle $s = 0$ und $s = 1$ sind trivial.

Aussage (ii): Das Signum einer Transposition ist nach Lemma 7.38 gleich -1. Aussage (ii) folgt damit aus Aussage (i).

Aussage (iii): Die identische Abbildung ist Produkt von null Transpositionen, also gilt $\operatorname{sgn} \mathrm{id} = (-1)^0 = 1$.

Aussage (iv): Schließlich gilt

$$1 = \operatorname{sgn} \mathrm{id} = \operatorname{sgn}(\sigma \circ \sigma^{-1}) = (\operatorname{sgn} \sigma) \cdot (\operatorname{sgn} \sigma^{-1}),$$

also $\operatorname{sgn} \sigma^{-1} = 1/\operatorname{sgn} \sigma = \operatorname{sgn} \sigma$, da $\operatorname{sgn} \sigma \in \{\pm 1\}$ ist. □

Ende der Vorlesung 9

§ 7.4 Untergruppen

Definition 7.42 (Untergruppe)**.**
Es sei $(G, \star)$ eine Gruppe.

(i) Eine Teilmenge $U \subseteq G$ heißt eine **Untergruppe** (englisch: subgroup) **von** $(G, \star)$, wenn U bzgl. $\star$ abgeschlossen und wenn $(U, \star)$ selbst wieder eine Gruppe ist. Manchmal schreibt man dies als $(U, \star) \leqslant (G, \star)$.

(ii) Eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq G$ heißt eine **Untergruppe** (englisch: subgroup) **von** $(G, \star)$, wenn $(U, \star)$ selbst wieder eine Gruppe ist. Manchmal schreibt man dies als $(U, \star) \leqslant (G, \star)$.

(iii) Eine Untergruppe $(U, \star)$ von $(G, \star)$ heißt **echt** (englisch: proper subgroup), wenn $U \subsetneq G$ gilt. △

Beachte: Die Assoziativität wird von $\star$ auf $\star$ vererbt. Ist $(G, \star)$ kommutativ, dann auch $(U, \star)$. Wie bereits bei Unterhalbgruppen werden wir in Zukunft auch einfach die Menge U als Untergruppe von $(G, \star)$ bezeichnen.

Bei Untermonoiden (Definition 7.11) hatten wir gefordert, dass ihr neutrales Element dasselbe ist wie im „Obermonoid“. Bei Untergruppen ergibt sich das von selbst:

Lemma 7.43 (neutrale und inverse Elemente in einer Untergruppe)**.**
Es sei U eine Untergruppe der Gruppe $(G, \star)$. Dann ist das neutrale Element e_U von $(U, \star)$ 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 der Übung. □

Aufgrund dieser Erkenntnis benötigen wir also keine neue Notation für das neutrale Element und die Inversen in einer Untergruppe. Wir halten weiterhin fest, dass eine Untergruppe die Eigenschaft $U \star U = U$ erfüllt. (**Quizfrage 7.12:** Warum?)

Die Prüfung einer Teilmenge $U \subseteq G$ auf die Untergruppen-Eigenschaft lässt sich mit folgendem Kriterium erreichen:

Satz 7.44 (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 $a \star b' \in U$.[18]

(*iii*) $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a' \star b \in U$.[19]

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 7.43 auch das neutrale Element in $(U, \star)$ ist. Für $a, b \in U$ gilt $b' \in U$ nach Lemma 7.43. 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 $U \subseteq G$ eine Untergruppe von $(G, \star)$.

Der Beweis von Aussage (*i*) $\Rightarrow$ Aussage (*iii*) und Aussage (*iii*) $\Rightarrow$ Aussage (*i*) läuft analog. □

Beispiel 7.45 (Untergruppen)**.**

(*i*) Es sei $(G, \star)$ eine Gruppe mit neutralem Element e. Dann sind $\{e\}$ und G Untergruppen von $(G, \star)$. Diese heißen die **trivialen Untergruppen** (englisch: trivial subgroups).

(*ii*) $\mathbb{Q}_{>0}$ ist eine Untergruppe von $(\mathbb{Q}_{\neq 0}, \cdot)$, und $\mathbb{R}_{>0}$ ist eine Untergruppe von $(\mathbb{R}_{\neq 0}, \cdot)$.

[18] kurz: $U \star U' \subseteq U$
[19] kurz: $U' \star U \subseteq U$

(*iii*) Für jede Zahl $m \in \mathbb{N}$ ist $m\mathbb{Z} = \{m\,z \mid z \in \mathbb{Z}\}$ mit der Verknüpfung + eine Untergruppe der Gruppe $(\mathbb{Z}, +)$. Das sind auch bereits alle möglichen Untergruppen von $(\mathbb{Z}, +)$.

(*iv*) Die Menge $\{\pm 1\}$ ist eine Untergruppe von $(\mathbb{Q}_{\neq 0}, \cdot)$, von $(\mathbb{R}_{\neq 0}, \cdot)$ und von $(\mathbb{C}_{\neq 0}, \cdot)$.

(*v*) Die Menge $\{\pm 1, \pm i\}$ ist eine Untergruppe von $(\mathbb{C}_{\neq 0}, \cdot)$.

(*vi*) Die Menge $\{z \in \mathbb{C} \mid |z| = 1\}$ ist eine Untergruppe von $(\mathbb{C}_{\neq 0}, \cdot)$.

(*vii*) Für $n \in \mathbb{N}_0$ ist

$$\begin{aligned} A_n &:= \{\sigma \in S_n \mid \sigma \text{ ist Komposition einer geraden Anzahl von Transpositionen}\} \\ &= \{\sigma \in S_n \mid \operatorname{sgn}\sigma = 1\} \end{aligned} \tag{7.20}$$

eine Untergruppe von S_n, genannt die **alternierende Gruppe** (englisch: alternating group) vom Grad n. Für $n = 0, 1$ stimmt sie mit S_n überein. Für $n \geqslant 2$ ist A_n eine echte Untergruppe von S_n mit $\frac{1}{2}n!$ Elementen.

(*viii*) In S_3 besteht die alternierende Untergruppe A_3 in der Notation von Beispiel 7.31 gerade aus $\{\sigma_0, \sigma_1, \sigma_2\}$. Diese entsprechen bei Interpretation als Kongruenzabbildungen eines gleichseitigen Dreiecks auf sich selbst (Abbildung 7.1) gerade den Drehungen. △

Quizfrage 7.13: Können Sie eine Gruppe finden, die außer den trivialen Untergruppen keine weiteren Untergruppen besitzt?

Bemerkung 7.46 („Untergruppe sein“ ist eine Ordnungsrelation, vgl. Bemerkung 7.13 zu Unterhalbgruppen und Untermonoiden)**.**

(*i*) Die Relation „ist Untergruppe von“ ist eine partielle Ordnung auf der Klasse aller Gruppen.

(*ii*) Insbesondere ist die Menge aller Untergruppen einer bestimmten Gruppe $(G, \star)$ durch die Untergruppenhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein (Abbildung 7.2).

(*iii*) Ist $U \subseteq H$ ein Untermonoid des Monoids $(H, \star)$ und ist $(U, \star)$ zusätzlich eine Gruppe, dann sprechen wir auch kurz von einer **Untergruppe** $(U, \star)$ **des Monoids** $(H, \star)$. Das trifft genau dann zu, wenn $(U, \star)$ eine Gruppe ist und das neutrale Element $e \in H$ enthält. (**Quizfrage 7.14:** Klar?)

(*iv*) In diesem Sinne ist die Einheitengruppe E eines Monoids $(H, \star)$ mit neutralem Element e die größte Untergruppe von $(H, \star)$, also: E ist das Maximum der Menge

$$\{U \subseteq H \mid (U, \star) \text{ ist Gruppe mit } e \in U\}$$

bzgl. der Inklusionshalbordnung (und auch bzgl. der Untergruppen-Halbordnung). Alle weiteren Untergruppen von $(H, \star)$, die e enthalten, sind also Teilmengen (und sogar Untergruppen) von E. △

Lemma 7.47 (Durchschnitt von Untergruppen)**.**
Es sei $(G, \star)$ eine Gruppe.

(*i*) Ist $(U_i)_{i \in I}$ eine nichtleere Familie von Untergruppen von $(G, \star)$, dann ist auch $\bigcap_{i \in I} U_i$ eine Untergruppe von $(G, \star)$.

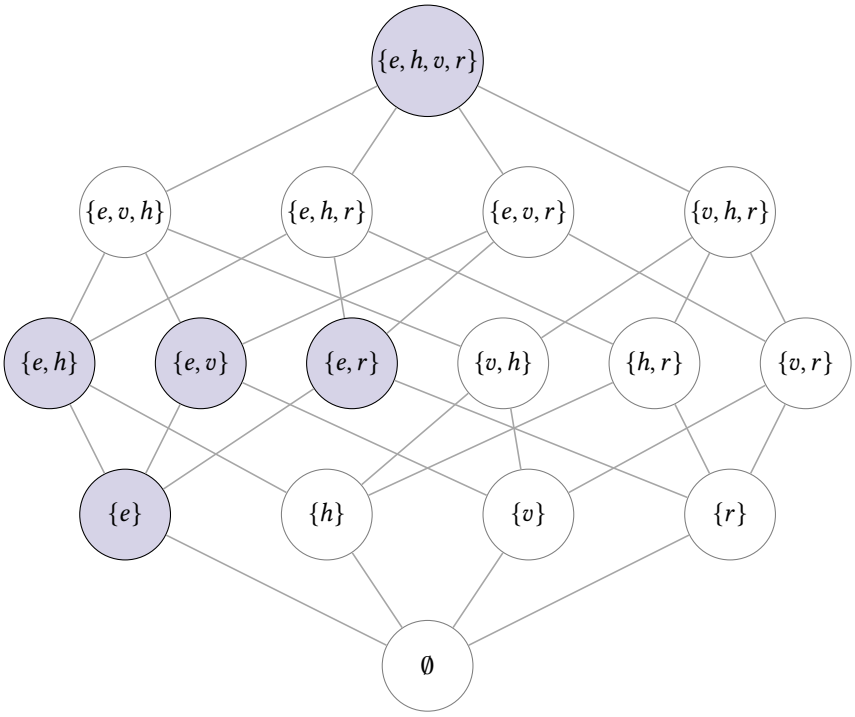


Abbildung 7.2.: Hasse-Diagramm der Inklusionshalbordnung auf der Kleinschen Vierergruppe $K_4 = \{e, h, v, r\}$ (Beispiel 7.22). Hervorgehoben sind die fünf Untergruppen von K_4. Diese Teilmenge ist durch die Halbordnung „ist Untergruppe von“ partiell geordnet, welche mit der Inklusionshalbordnung übereinstimmt (Bemerkung 7.46). Für Untergruppen U_1, U_2 von K_4 gilt also: U_1 ist Untergruppe von U_2 genau dann, wenn U_1 Teilmenge von U_2 ist. Im Diagramm erkennen wir das durch einen aufsteigenden Pfad von U_1 nach U_2.
Anhand des Diagramms können wir außerdem die von einer Teilmenge $E \subseteq K_4$ erzeugte Untergruppe $\langle E \rangle$ (Definition 7.48) ablesen. Dazu suchen wir ausgehend von E einen kürzesten aufsteigenden Pfad zu einer der Untergruppen. Kürzeste Pfade sind i. A. nicht eindeutig, die dadurch erreichte Untergruppe jedoch schon. Beispielsweise gilt $\langle v, h \rangle = \{e, h, v, r\}$, und es gibt zwei mögliche Pfade.

(*ii*) Ist $\mathcal{U}$ eine nichtleere Menge von Untergruppen von $(G, \star)$, dann ist auch $\bigcap \mathcal{U}$ eine Untergruppe von $(G, \star)$.

Beweis. Dieser Beweis ist Gegenstand der Übung. □

In Definition 5.14 hatten wir die Hüllenbildung einer Menge betrachtet, sodass die kleinstmögliche Oberrelation mit den gewünschten Eigenschaften entsteht. Analog dazu betrachten wir jetzt die Anreicherung der Teilmenge einer Gruppe zu einer Untergruppe.

Definition 7.48 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe)**.**
Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

(*i*) Die Menge

$$\langle E\rangle := \bigcap \{U \mid U \text{ ist Untergruppe von } (G,\star) \text{ und } E \subseteq U\} \tag{7.21}$$

heißt die **von E erzeugte Untergruppe** (englisch: subgroup generated by E) oder auch die **Untergruppenhülle** (englisch: subgroup hull) oder der **Untergruppenabschluss** (englisch: subgroup closure) **von E in $(G,\star)$**.

Ist speziell E die endliche Menge $E = \{a_1, \dots, a_n\}$ mit $a_i \in G$ und $n \in \mathbb{N}_0$, so schreiben wir auch $\langle a_1, \dots, a_n\rangle$ statt $\langle\{a_1, \dots a_n\}\rangle$.

(*ii*) Die von einem einzelnen Element $a \in G$ erzeugte Untergruppe $\langle a\rangle$ heißt die **von a erzeugte zyklische Untergruppe** (englisch: cyclic subgroup) von $(G,\star)$.

(*iii*) 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).

(*iv*) Gilt $\langle a\rangle = G$ für ein $a \in G$, so heißt die Gruppe $(G,\star)$ **zyklisch** (englisch: cyclic) oder **zyklisch erzeugt** (englisch: cyclically generated). Ein solches Element $a \in G$ heißt ein **Erzeuger** (englisch: generator) **von** G.

(*v*) Ein Element $a \in G$ heißt ein **Gruppenelement endlicher Ordnung** (englisch: group element of finite order), wenn es ein $n \in \mathbb{N}$ gibt mit der Eigenschaft (in multiplikativer Notation) $a^n = 1$. In diesem Fall heißt die kleinste Zahl $n \in \mathbb{N}$ mit dieser Eigenschaft die **Ordnung** von a. Falls kein $n \in \mathbb{N}$ mit der Eigenschaft $a^n = 1$ existiert, so heißt a ein **Gruppenelement unendlicher Ordnung** (englisch: group element of infinite order).[20] △

Bemerkung 7.49 (Eigenschaften der Untergruppenhülle, vgl. Bemerkung 5.16 zu Eigenschaften von Hüllen von Relationen)**.**
Per Konstruktion ist $\langle E\rangle$ ist die kleinste Untergruppe von $(G,\star)$, die die Teilmenge $E \subseteq G$ enthält. Genauer: $\langle E\rangle$ ist das Minimum der Menge

$$\{U \mid U \text{ ist Untergruppe von } (G,\star) \text{ und } E \subseteq U\}$$

bzgl. der Untergruppen-Halbordnung (und auch bzgl. der Inklusionshalbordnung). △

Da Definition 7.48 nur eine abstrakte Definition der von einer Menge erzeugten Untergruppe liefert, wollen wir diese nun charakterisieren.

Satz 7.50 (Darstellung der erzeugten Untergruppe)**.**
Es sei $(G,\star)$ eine Gruppe und $E \subseteq G$. Dann gilt für die von E erzeugte Untergruppe:

$$\langle E\rangle = \left\{a_1 \star \cdots \star a_n \,\middle|\, \exists n \in \mathbb{N}_0\ \forall i = 1, \dots, n\ (a_i \in E \cup E')\right\}, \tag{7.22}$$

wobei E' die Menge der Inversen von E bezeichnet, vgl. Bemerkung 7.20.[21]

[20] Die Ordnung einer bijektiven Funktion $f\colon X \to X$ (Definition 6.18) ist also nichts anderes als die Ordnung von f als Element der Gruppe der bijektiven Funktionen $X \to X$.

[21] Im Fall $n = 0$ interpretieren wir wie üblich die Verknüpfung von null Elementen als das neutrale Element e der Gruppe. Insbesondere im Fall $E = \emptyset$ ergibt sich 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 7.44). 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 7.15:** 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 7.51 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe)**.**

(*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 7.31, also

$$\sigma_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad \sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad \sigma_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \qquad \text{(Drehungen)}$$

$$\sigma_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad \sigma_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \quad \sigma_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \qquad \text{(Spiegelungen)}$$

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 7.45. 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.

(*iv*) Die Bewegungen des Zauberwürfels (ausgehend von der gelösten Position in einer beliebig, aber fest gewählten Orientierung) können als eine Untergruppe der symmetrischen Gruppe S_{48} auf den 48 nicht-zentralen Facetten des Würfels modelliert werden. Diese Untergruppe wird z. B. erzeugt von der sechselementigen Menge der Drehungen der sechs Seiten des Würfels im Uhrzeigersinn. Sie hat 43 252 003 274 489 856 000 $\approx 4.3 \cdot 10^{19}$ Elemente, während S_{48} etwa $1.2 \cdot 10^{61}$ Elemente hat. △

Die Vereinigung $U_1 \cup U_2$ von zwei Untergruppen einer Gruppe G ist i. A. keine Untergruppe von G.[22] Wir betrachten daher stattdessen die kleinste Untergruppe von G, die $U_1 \cup U_2$ enthält, also die von $U_1 \cup U_2$ erzeugte Untergruppe $\langle U_1 \cup U_2 \rangle$ (englisch: join of two subgroups). Diese hat folgende Darstellung:

Folgerung 7.52 (zu Satz 7.50: Untergruppenhülle der Vereinigung zweier Untergruppen)**.**
Es seien $(G, \star)$ eine Gruppe und U_1, U_2 Untergruppen von G. Dann gilt für die von $U_1 \cup U_2$ erzeugte Untergruppe:

$$\langle U_1 \cup U_2 \rangle = \left\{ a_1 \star b_1 \star a_2 \star b_2 \cdots \star a_n \star b_n \,\middle|\, \exists n \in \mathbb{N}_0 \ \forall i = 1, \ldots, n \ (a_i \in U_1, b_i \in U_2) \right\}. \tag{7.23}$$

Beweis. □

Abschließend geben wir noch ein Resultat zur Untergruppenhülle von Vereinigung und Schnitt zweier beliebiger Teilmengen einer Gruppe an:

Folgerung 7.53 (zu Satz 7.50: Untergruppenhülle von Vereinigung und Schnitt)**.**
Es sei $(G, \star)$ eine Gruppe und $E_1, E_2 \subseteq G$. Dann gilt:

$$\langle E_1 \cup E_2 \rangle = \big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle, \tag{7.24a}$$
$$\langle E_1 \cap E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cap \langle E_2 \rangle \big\rangle. \tag{7.24b}$$

Beweis. Übung □

§ 7.5 Untergruppen induzieren Äquivalenzrelationen

Definition 7.54 (Links- und Rechtsnebenklassen einer Untergruppe)**.**
Es sei $(G, \star)$ eine Gruppe und U eine Untergruppe.

(*i*) Eine Menge der Form $a \star U$ heißt eine **Linksnebenklasse** (englisch: left coset) **von** U.[23]

(*ii*) Eine Menge der Form $U \star a$ heißt eine **Rechtsnebenklasse** (englisch: right coset) **von** U.[24] △

Satz 7.55 (Links- und Rechtsnebenklassen partitionieren eine Gruppe)**.**
Es sei $(G, \star)$ eine Gruppe, U eine Untergruppe und $a, b \in G$.

(*i*) Die Linksnebenklassen $a \star U$ und $b \star U$ sind entweder gleich oder disjunkt.

(*ii*) Die Rechtsnebenklassen $U \star a$ und $U \star b$ sind entweder gleich oder disjunkt.

[22] Tatsächlich gilt: $U_1 \cup U_2$ ist genau dann eine Untergruppe, wenn $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ gilt (Übung).

[23] Die Linksnebenklasse $a \star U$ ist also die Linkstranslation von U um das Element a. Bei den Linksnebenklassen $a \star U$ steht der Repräsentant a links vom U.

[24] Die Rechtsnebenklasse $U \star a$ ist also die Rechtstranslation von U um das Element a. Bei den Rechtsnebenklassen $a \star U$ steht der Repräsentant a rechts vom U.

Beweis. Aussage (*i*): Wir nehmen an, dass $a \star U$ und $b \star U$ nicht disjunkt sind. Es existiert also ein $c \in (a \star U) \cap (b \star U)$, d. h., es existieren $u_1, u_2 \in U$, sodass $a \star u_1 = b \star u_2$ gilt. Daraus folgt

$$a \star u = a \star u_1 \star u_1' \star u = b \star u_2 \star u_1' \star u \quad \text{für alle } u \in U.$$

Da U abgeschlossen ist unter Verknüpfung und Inversenbildung, gehört $u_2 \star u_1' \star u$ zu U. Das zeigt $a \star U \subseteq b \star U$. Analog folgt $b \star U \subseteq a \star U$ aus

$$b \star u = b \star u_2 \star u_2' \star u = a \star u_1 \star u_2' \star u \quad \text{für alle } u \in U.$$

Insgesamt erhalten wir also, dass zwei nicht-disjunkte Linksnebenklassen $a \star U$ und $b \star U$ bereits gleich sind.

Der Beweis von Aussage (*ii*) erfolgt analog. □

Jede Nebenklasse $a \star U$ enthält das Element a (ist also nichtleer), da das neutrale Element von G auch zu U gehört. Damit bilden die Linksnebenklassen eine Partition von G. Nach Satz 5.25 („Partitionen sind dasselbe wie Äquivalenzrelationen“) existiert also eine eindeutig bestimmte Äquivalenzrelation ${\sim^U}$, deren Äquivalenzklassen genau die Linksnebenklassen sind. Analog existiert eine eindeutig bestimmte Äquivalenzrelation ${}^U{\sim}$, deren Äquivalenzklassen genau die Rechtsnebenklassen sind. Wir halten dieses Ergebnis fest als

Folgerung 7.56 (von einer Untergruppe induzierte Äquivalenzrelationen)**.**
Es sei $(G, \star)$ eine Gruppe und U eine Untergruppe.

(*i*) Dann sind durch

$$a \sim^U b \quad \Leftrightarrow \quad a \star U = b \star U \quad \Leftrightarrow \quad b \in a \star U \quad \Leftrightarrow \quad a \in b \star U \tag{7.25a}$$
$$a \,{}^U\!\sim b \quad \Leftrightarrow \quad U \star a = U \star b \quad \Leftrightarrow \quad b \in U \star a \quad \Leftrightarrow \quad a \in U \star b \tag{7.25b}$$

für $a, b \in G$ zwei Äquivalenzrelationen[25] auf G erklärt, deren Äquivalenzklassen gerade die Links- bzw. die Rechtsnebenklassen von U sind.

(*ii*) Jede der Äquivalenzklassen ist gleichmächtig zu U.

(*iii*) Ist L ein Repräsentantensystem der Linksnebenklassen, dann ist $R := L'$ ein Repräsentantensystem der Rechtsnebenklassen.

Beweis. Aussage (*i*): Aus Satz 5.25 („Partitionen sind dasselbe wie Äquivalenzrelationen“) folgt, dass die durch $a \sim^U b \Leftrightarrow a \star U = b \star U$ definierte Relation eine Äquivalenzrelation ist, deren Äquivalenzklassen genau die Linksnebenklassen von U sind. Es bleiben die weiteren Äquivalenzen in (7.25a) zu zeigen. Die Mengen $a \star U$ und $b \star U$ enthalten a bzw. b und sind beide Linksnebenklassen von U. Sie sind genau dann gleich, wenn $b \in a \star U$ gilt. Analog sind sie auch genau dann gleich, wenn $a \in b \star U$ gilt.

Die Aussagen in (7.25b) zeigt man analog.

[25] Für diese Relationen gibt es in der Literatur keine einheitliche Notation. Wir benutzen $\sim^U$ mit dem Symbol $\sim$ links von U für die Relation, deren Äquivalenzklassen die Linksnebenklassen sind. Entsprechend bezeichnet ${}^U\!\sim$ mit dem Symbol $\sim$ rechts von U die Äquivalenzrelation, deren Äquivalenzklassen die Rechtsnebenklassen sind.

Aussage (ii): Für jedes $a \in G$ ist die Abbildung bildet die Linkstranslation um a die Menge U bijektiv auf die Linksnebenklasse $a \star U$ ab. Das zeigt die Gleichmächtigkeit von U und $a \star U$. Analog zeigt die Rechtstranslation um a die Gleichmächtigkeit von U und $U \star a$.

Aussage (iii): Es sei L ein Repräsentantensystem der Linksnebenklassen und $U \star a$ eine der Rechtsnebenklassen. Zu zeigen ist, dass $U \star a$ durch genau ein Element aus $R := L'$ repräsentiert wird.

Schritt 1: Zur Existenz: Die Linksnebenklasse $a' \star U$ wird durch (genau) ein $\ell \in L$ repräsentiert, also gilt $\ell \in a' \star U$, d. h., $\ell = a' \star u$ für ein $u \in U$. Daher ist $\ell' = (a' \star u)' = u' \star a \in L' = R$ ein Element der Rechtsnebenklasse $U \star a$.

Schritt 2: Zur Eindeutigkeit: Nehmen wir an, $r_1, r_2 \in R$ repräsentieren die gleiche Rechtsnebenklasse $U \star a$. Es existieren also $u_1, u_2 \in U$ mit $r_1 = u_1 \star a$ und $r_2 = u_2 \star a$. Das zeigt $r_1' = a' \star u_1 \in a' \star U$ und $r_2' = a' \star u_2 \in a' \star U$. Damit repräsentieren $r_1', r_2' \in R' = L$ dieselbe Linksnebenklasse $a' \star U$. Es folgt $r_1' = r_2'$ und damit $r_1 = r_2$. □

Die durch die Links- bzw. Rechtsnebenklassen definierten Äquivalenzrelationen ${}^{U}\!\sim$ und $\sim^{U}$ heißen die von der Untergruppe U **induzierten Äquivalenzrelationen** (englisch: induced equivalence relations) **auf** G. Wir schreiben:

$$G \,/\, U \text{ für die Faktormenge } G \,/\, {}^{U}\!\sim \quad \text{(die Menge der Linksnebenklassen)}, \tag{7.26a}$$

$$U \setminus G \text{ für die Faktormenge } G \,/\, \sim^{U} \quad \text{(die Menge der Rechtsnebenklassen)}. \tag{7.26b}$$

Folgerung 7.57 (induzierte Äquivalenzrelationen in abelschen Gruppen)**.**

Es sei $(G, \star)$ eine abelsche Gruppe und U eine Untergruppe. Dann gilt $a \star u = u \star a$ für alle $u \in U$ und $a \in G$. Insbesondere gilt also $a \star U = U \star a$ für alle $a \in G$. Die Äquivalenzrelationen $a \sim^{U} b$ und $a \,{}^{U}\!\sim b$ sind also identisch.

Beweis. Der Beweis ist Gegenstand der Übung. □

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) $a \star U = U \star a$ von U. Wir werden später in § 8.1 sehen, dass solche Untergruppen auch in nicht-kommutativen Gruppen vorkommen.

Bemerkung 7.58 (induzierte Äquivalenzrelationen verallgemeinern die Gleichheitsrelation)**.**

(i) Im Fall der trivialen Untergruppe $U = \{e\}$ gilt $a \star U = U \star a$ für alle $a \in G$ (Links- und Rechtsnebenklassen stimmen überein) und weiter

$$a \overset{U}{\sim} b \quad \Leftrightarrow \quad b \in a \star U = \{a\} \quad \Leftrightarrow \quad a = b.$$

Jede Nebenklasse $a \star U = U \star a$ enthält also nur das Element a.

(*ii*) Wenn die Untergruppe U größer wird, werden auch die Äquivalenzklassen größer. Wir erhalten dadurch eine Verallgemeinerung, eine „gröbere Version“ der Gleichheit. Die Wahl von U bestimmt, welche Unterschiede „nicht gesehen“ oder „ausfaktorisiert“ werden sollen. Zwei Elemente a, b der Gruppe werden als „gleichwertig“ (äquivalent) betrachtet, wenn sie sich nur um ein Element in U unterscheiden (bei Multiplikation von links bzw. von rechts), also wenn $b \in a \star U$ gilt bei Verwendung von Linksnebenklassen bzw. $b \in U \star a$ bei Rechtsnebenklassen.

(*iii*) Im Extremfall $U = G$ gibt es in G/U und $U \backslash G$ jeweils nur eine einzige Äquivalenzklasse, nämlich die gesamte Gruppe G. Es werden also überhaupt keine Elemente mehr unterschieden. △

Beispiel 7.59 (Nebenklassen)**.**

(*i*) In der symmetrischen Gruppe $(S_3, \circ)$ sind die Links- bzw. Rechtsnebenklassen der Untergruppe $U = \{\sigma_0, \sigma_5\}$ (mit den Bezeichnungen aus Beispiel 7.31 und Abbildung 7.1) gerade die Mengen

$$\sigma_0 \circ U = \{\sigma_0, \sigma_5\} \quad \begin{smallmatrix} & & 3 & & & & 3 & \\ & \diagup & & \diagdown & & \diagup & & \diagdown \\ 1 & & & & 2 & 2 & & & 1 \end{smallmatrix} \qquad U \circ \sigma_0 = \{\sigma_0, \sigma_5\} \quad \begin{smallmatrix} & & 3 & & & & 3 & \\ & \diagup & & \diagdown & & \diagup & & \diagdown \\ 1 & & & & 2 & 2 & & & 1 \end{smallmatrix}$$

$$\sigma_1 \circ U = \{\sigma_1, \sigma_3\} \quad \begin{smallmatrix} & & 1 & & & & 2 & \\ & \diagup & & \diagdown & & \diagup & & \diagdown \\ 2 & & & & 3 & 1 & & & 3 \end{smallmatrix} \qquad U \circ \sigma_1 = \{\sigma_1, \sigma_4\} \quad \begin{smallmatrix} & & 1 & & & & 1 & \\ & \diagup & & \diagdown & & \diagup & & \diagdown \\ 2 & & & & 3 & 3 & & & 2 \end{smallmatrix}$$

$$\sigma_2 \circ U = \{\sigma_2, \sigma_4\} \quad \begin{smallmatrix} & & 2 & & & & 1 & \\ & \diagup & & \diagdown & & \diagup & & \diagdown \\ 3 & & & & 1 & 3 & & & 2 \end{smallmatrix} \qquad U \circ \sigma_2 = \{\sigma_2, \sigma_3\} \quad \begin{smallmatrix} & & 2 & & & & 2 & \\ & \diagup & & \diagdown & & \diagup & & \diagdown \\ 3 & & & & 1 & 1 & & & 3 \end{smallmatrix}.$$

Die beiden durch U induzierten Äquivalenzrelationen sind hier also verschieden.

Man erkennt, dass innerhalb einer Rechtsnebenklasse (rechte Spalte) zwei Permutationen nicht unterschieden werden, wenn sie sich nur um die horizontale Spiegelung σ_5 unterscheiden. Eine eventuelle nachträgliche Spiegelung σ_5 wird also aus einer Permutation σ „ausfaktorisiert“. Im Unterschied dazu wird bei den Linksnebenklassen nicht unterschieden zwischen Permutation, die mit einer eventuellen Spiegelung σ_5 beginnen.

(*ii*) In der abelschen Gruppe $(\mathbb{Z}, +)$ erzeugt die Untergruppe $m\mathbb{Z}$ für $m \in \mathbb{N}$ gerade die Kongruenzrelation modulo m, d. h., die Äquivalenzrelationen $\overset{m\mathbb{Z}}{\sim}$ und $\overset{m}{\equiv}$ stimmen überein. Die Nebenklassen $[a] = a + m\mathbb{Z}$ werden auch **Restklassen modulo** m genannt, vgl. Beispiel 5.22), und sie partitionieren die ganzen Zahlen $\mathbb{Z}$ in m gleichmächtige Restklassen, $[0], [1], \ldots, [m-1]$.

(*iii*) 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.[AoC] △

Aus der in Folgerung 7.57 festgestellten Gleichmächigkeit der Äquivalenzklassen folgt der folgende wichtige **Satz von Lagrange** (englisch: Lagrange's theorem) der Gruppentheorie:

Satz 7.60 (Satz von Lagrange)**.**
Es sei $(G, \star)$ eine endliche Gruppe und U 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 der Übung. □

Folgerung 7.61 (Gruppen, deren Elementanzahl eine Primzahl ist)**.**
Es sei $(G, \star)$ eine endliche Gruppe, deren Kardinalität eine Primzahl ist. Dann gilt:

(*i*) G besitzt nur die trivialen Untergruppen $\{e\}$ und G.

(*ii*) G ist zyklisch, und jedes Element $a \in G \setminus \{e\}$ ist ein Erzeuger.

(*iii*) G ist abelsch.

Beweis. Aussage (*i*): Nach dem Satz von Lagrange 7.60 kommt als Kardinalität von U nur 1 oder $\#G$ in Frage.

Aussage (*ii*): Für $a \in G \setminus \{e\}$ ist $\langle a \rangle$ eine Untergruppe von G, die von $\{e\}$ verschieden ist. Es muss also $\langle a \rangle = G$ gelten.

Aussage (*iii*): Zyklisch erzeugte Gruppen sind immer abelsch. (**Quizfrage 7.16:** Warum ist das so?) □

Ende der Vorlesung 10

Ende der Woche 5

§ 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 (Homomorphismus von Halbgruppen)**.**
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 **Homomorphismus von Halbgruppen** (englisch: semigroup homomorphism), wenn gilt:

$$f(a \star b) = f(a) \square f(b) \quad \text{für alle } a, b \in H_1. \tag{8.1}$$

(*ii*) Ist $f\colon H_1 \to H_2$ strukturverträglich und gilt $(H_1, \star) = (H_2, \square)$, so sprechen wir auch von einem **Endomorphismus einer Halbgruppe** (englisch: semigroup endomorphism, altgriechisch: *ένδον*: innen).

(*iii*) Ist $f\colon H_1 \to H_2$ strukturverträglich und bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus von Halbgruppen** (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*) Ist $f\colon H_1 \to H_2$ strukturverträglich und bijektiv und gilt $(H_1, \star) = (H_2, \square)$, so sprechen wir auch von einem **Automorphismus einer Halbgruppe** (englisch: semigroup automorphism, altgriechisch: *αυτος*: selbst).[26] △

Expertenwissen: Halbgruppenhomomorphismus als kommutatives Diagramm

Wir können den Sachverhalt, dass $f\colon (H_1, \star) \to (H_2, \square)$ ein Homomorphismus von Halbgruppen ist, auch durch das folgende **kommutative Diagramm** (englisch: commutative diagram) ausdrücken:

$$\begin{array}{ccc} H_1 \times H_1 & \xrightarrow{f\times f} & H_2 \times H_2 \\ \downarrow{\scriptstyle \star} & & \downarrow{\scriptstyle \square} \\ H_1 & \xrightarrow{f} & H_2 \end{array}$$

Die Abbildung $f \times f$ ist dabei definiert durch $f \times f\colon H_1 \times H_1 \ni (a, b) \mapsto (f(a), f(b)) \in H_2 \times H_2$. Ein solches Diagramm heißt **kommutativ** (englisch: commutative diagram), wenn alle Pfade mit demselben Ausgangs- und demselben Endpunkt dasselbe Ergebnis produzieren.

Beachte: Einen surjektiven Homomorphismus von Halbgruppen nennt man manchmal auch einen **Epimorphismus von Halbgruppen** (englisch: semigroup epimorphism). Einen injektiven Homomorphismus von Halbgruppen nennt man manchmal auch einen **Monomorphismus von Halbgruppen** (englisch: semigroup monomorphism). Wir werden diese Bezeichnungen aber nicht verwenden.

Satz 8.2 (Komposition von Halbgruppenhomomorphismen, Inverse von Halbgruppenisomorphismen)**.**
Es seien $(H_1, \star)$, $(H_2, \square)$ und $(H_3, \bullet)$ drei Halbgruppen.

(*i*) Sind $f\colon H_1 \to H_2$ und $g\colon H_2 \to H_3$ Halbgruppenhomomorphismen, dann ist auch $g \circ f\colon H_1 \to H_3$ ein Halbgruppenhomomorphismus.

(*ii*) Ist $f\colon H_1 \to H_2$ ein Halbgruppenisomorphismus, dann ist auch $f^{-1}\colon H_2 \to H_1$ ein Halbgruppenisomorphismus.

Beweis. □

[26] Ein Automorphismus einer Halbgruppe ist somit ein bijektiver Endomorphismus oder auch ein Isomorphismus von einer Halbgruppe auf sich selbst.

Folgerung 8.3 (Isomorphie von Halbgruppen ist eine Äquivalenzrelation)**.**
Isomorphie ist eine Äquivalenzrelation auf der Klasse aller Halbgruppen.

Beweis. Jede Halbgruppe ist zu sich selbst isomorph über die identische Abbildung. Die Transitivität und Symmetrie folgen aus Satz 8.2. □

Definition 8.4 (Homomorphismus von Monoiden)**.**
Wenn $(M_1, \star)$ und $(M_2, \square)$ beides Monoide sind, so können wir ganz analog zu Definition 8.1 die Begriffe **Homomorphismus**, **Endomorphismus**, **Isomorphismus** und **Automorphismus** (englisch: monoid homomorphism, endomorphism, isomorphism, automorphism) definieren. Zusätzlich zu (8.1) fordern wir 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 Isomorphismus von Monoiden gibt. Wir schreiben dann $(M_1, \star) \cong (M_2, \square)$. △

Bemerkung 8.5 (zu Monoidhomomorphismen)**.**

(*i*) Homomorphismen sind wie oben bemerkt die strukturverträglichen Abbildungen zwischen jeglicher Art algebraischer Strukturen. Für Monoide besteht diese Struktur aus der Verknüpfung und dem Einselement, daher kommt die Forderung (8.2) hinzu. Sie folgt nicht bereits aus (8.1).

(*ii*) Es reicht allerdings an Stelle von (8.2) aus, lediglich zu fordern, dass $f(e_1)$ invertierbar ist, denn daraus folgt bereits (8.2):

$$\begin{aligned} f(e_1) \square f(e_1) &= f(e_1 \star e_1) && \text{da } f \text{ Halbgruppenhomomorphismus ist} \\ &= f(e_1) && \text{da } e_1 \text{ neutrales Element in } (H_1, \star) \text{ ist} \\ &= f(e_1) \square e_2 && \text{da } e_2 \text{ neutrales Element in } (H_2, \square) \text{ ist.} \end{aligned} \tag{8.3}$$

Da $f(e_1)$ als invertierbar vorausgesetzt wurde, zeigt die Kürzungsregel (7.8a) nun $f(e_1) = e_2$. △

Definition 8.6 (Homomorphismus von Gruppen)**.**
Wenn $(G_1, \star)$ und $(G_2, \square)$ beides Gruppen sind, so können wir ganz analog zu Definition 8.1 die Begriffe **Homomorphismus**, **Endomorphismus**, **Isomorphismus** und **Automorphismus** (englisch: group homomorphism, endomorphism, isomorphism, automorphism) definieren. Die Bedingung (8.2) müssen wir für Gruppen nicht explizit fordern, denn sie folgt ja schon wie in (8.3), da $f(e_1)$ als Element der Gruppe $(G_2, \square)$ notwendig invertierbar ist.

Die Gruppen $(G_1, \star)$ und $(G_2, \square)$ heißen zueinander **isomorph**, wenn es zwischen ihnen einen Gruppenisomorphismus gibt. Wir schreiben dann $(G_1, \star) \cong (G_2, \square)$. △

Beachte: Satz 8.2 und Folgerung 8.3 gelten sinngemäß auch für Monoide und Gruppen.

Beispiel 8.7 (Homomorphismen von Halbgruppen und Gruppen)**.**

(*i*) Es sei Σ eine nichtleere Menge und $(\Sigma^*, \circ)$ das Monoid der Tupel über Σ mit der Konkatenation $\circ$, siehe Beispiele 7.4 und 7.8. Die Abbildung $\#\colon (\Sigma^*, \|) \to (\mathbb{N}_0, +)$, die die Länge eines Tupels angibt, ist ein Monoidhomomorphismus, denn es gilt

$$\#\big((x_1, \dots, x_n) \parallel (y_1, \dots, y_m)\big) = \#(x_1, \dots, x_n) + \#(y_1, \dots, y_m) = n + m$$
$$\text{und} \quad \#() = 0.$$

Genau dann, wenn Σ einelementig ist, ist $\#$ auch bijektiv, also ein Monoidisomorphismus.

(*ii*) Es seien X eine Menge und $(Y, \star)$ eine Halbgruppe oder ein Monoid oder eine Gruppe. Dann ist die Abbildung $\Phi\colon (Y^X, \star) \ni f \mapsto f(x_0) \in (Y, \star)$, die eine Funktion $f\colon X \to Y$ an einer festen Stelle x_0 auswertet, ein Homomorphismus von Halbgruppen bzw. Monoiden bzw. Gruppen, denn es gilt

$$\Phi(f \star g) = (f \star g)(x_0) = f(x_0) \star g(x_0) = \Phi(f) \star \Phi(g).$$

(*iii*) Für $a > 0$, $a \neq 1$, ist $\log_a\colon (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ aufgrund des Logarithmusgesetzes

$$\log_a(x \cdot y) = \log_a(x) + \log_a(y)$$

ein Gruppenhomomorphismus. Weiter ist $\log_a$ bijektiv, also sogar ein Gruppenisomorphismus. Die Umkehrabbildung

$$(\mathbb{R}, +) \ni x \mapsto a^x \in (\mathbb{R}_{>0}, \cdot)$$

ist folglich ebenfalls ein Gruppenisomorphismus, erfüllt also insbesondere

$$a^{x+y} = a^x \cdot a^y.$$

(*iv*) Die Betrags-Abbildung

$$(\mathbb{C}, \cdot) \ni z \mapsto |z| \in (\mathbb{R}_{\geq 0}, \cdot)$$

ist ein Homomorphismus von Monoiden, denn es gilt $|w \cdot z| = |w| \cdot |z|$ für alle $w, z \in \mathbb{C}$. Ihre Einschränkung

$$(\mathbb{C}_{\neq 0}, \cdot) \ni z \mapsto |z| \in (\mathbb{R}_{>0}, \cdot)$$

ist ein Homomorphismus von Gruppen.

(*v*) 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. (**Quizfrage 8.1:** Können Sie ein Beispiel finden?)

(*vi*) Es sei $(H, \star)$ ein Monoid und $g \in H$ ein invertierbares Element. Dann ist die Abbildung

$$H \ni a \mapsto g \star a \star g' \in H, \tag{8.4}$$

genannt die **Konjugation mit** g (englisch: conjugation), ein Endomorphismus des Monoids $(H, \star)$.

(*vii*) In einer Gruppe $(G, \cdot)$ ist für jedes feste $a \in G$ die Abbildung

$$(\mathbb{Z}, +) \ni n \mapsto a^n \in G$$

ein Gruppenhomomorphismus. Dieser ist surjektiv genau dann, wenn a ein Erzeuger (Definition 7.48) von G ist.

(*viii*) Für festes $n \in \mathbb{Z}$ ist die Abbildung (vgl. (7.10))

$$G \ni a \mapsto a^n \in G$$

in einer *abelschen* Gruppe $(G, \cdot)$ ein Gruppenendomorphismus. (**Quizfrage 8.2:** Wo geht die Kommutativität der Verknüpfung ein?)

(*ix*) 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 7.40

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

Genau für $n = 2$ ist sgn auch bijektiv, also ein Gruppenisomorphismus.

(*x*) Die in Beispiel 7.31 und Abbildung 7.1 vorgenommene „Identifikation" der symmetrischen Gruppe S_3 mit der Gruppe der Kongruenzabbildungen eines gleichseitigen Dreiecks stellt einen Gruppenisomorphismus dar.

(*xi*) Die Abbildung

$$\mathbb{R} \ni f(x) := \exp(ix) := \cos(x) + i\sin(x) \in \mathbb{C}$$

ist ein Gruppenhomomorphismus $(\mathbb{R}, +) \to (\mathbb{C}, \cdot)$, 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 daraus die **Additionstheoreme** (englisch: angle addition theorems) für die Winkelsumme

$$\cos(x+y) = \cos(x)\cdot\cos(y) - \sin(x)\cdot\sin(y), \tag{8.5a}$$
$$\sin(x+y) = \sin(x)\cdot\cos(y) + \cos(x)\cdot\sin(y). \tag{8.5b}$$

(*xii*) Die Abbildung

$$(\mathbb{Z}, \cdot) \ni n \mapsto 0 \in (\mathbb{Z}, \cdot)$$

ist ein Homomorphismus von Halbgruppen, aber kein Homomorphismus von Monoiden, denn $f(1) = 0 \neq 1$. △

Expertenwissen: Wann sind Halbgruppenhomomorphismen auch Monoidhomomorphismen?

Das Beispiel 8.7 (*xii*) zeigt, dass Homomorphismen von Halbgruppen tatsächlich nicht notwendigerweise das neutrale Element auf das neutrale Element abbilden, dass also (8.2) tatsächlich i. A. nicht aus der Strukturverträglichkeit (8.1) folgt. Es gibt aber ein Kriterium (für das Ziel-Monoid), das absichert, dass doch *jeder* Halbgruppenhomomorphismus auch ein Monoidhomomorphismus ist:

Es seien $(H_1, \star)$ und $(H_2, \square)$ Monoide mit den neutralen Elementen e_1 bzw. e_2. Dann sind äquivalent:

(*i*) Jeder Halbgruppenhomomorphismus $f\colon H_1 \to H_2$ ist auch ein Monoidhomomorphismus.

(*ii*) Es gibt in $(H_2, \square)$ genau ein Element mit der Eigenschaft $y \square y = y$. (Dieses ist dann notwendigerweise gleich e_2.)

Quizfrage 8.3: Beweis?

Das folgende Resultat zeigt, dass Monoid- und Gruppenhomomorphismen inverse Elemente auf inverse Elemente abbilden:

Lemma 8.8 (Eigenschaften von Monoid- und Gruppenhomomorphismen)**.**
Es seien $(H_1, \star)$ und $(H_2, \square)$ Monoide mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Monoidhomomorphismus. Ist $a \in H_1$ invertierbar, dann ist auch $f(a) \in H_2$ invertierbar, und es gilt $(f(a))' = f(a')$. Insbesondere gilt das auch für Gruppenhomomorphismen.

Beweis. Es gilt

$$\begin{aligned} f(a') \square f(a) &= f(a' \star a) && \text{da } f \text{ Monoidhomomorphismus ist} \\ &= f(e_1) && \text{da } e_1 \text{ neutrales Element in } (H_1, \star) \text{ ist} \\ &= e_2 && \text{wegen (8.2).} \end{aligned}$$

Ganz analog folgt auch $f(a) \square f(a') = e_2$. Das zeigt, dass $f(a)$ invertierbar und dass $f(a')$ das zu $f(a)$ inverse Element ist. □

Quizfrage 8.4: Kann $f\colon (\mathbb{Z}, +) \ni n \mapsto n + 1 \in (\mathbb{Z}, +)$ ein Gruppenhomomorphismus sein?

Bemerkung 8.9 (zu Definitionen 8.1, 8.4 und 8.6, Lemma 8.8)**.**
Zwei zueinander isomorphe Halbgruppen bzw. Monoide bzw. Gruppen können und müssen, was ihre algebraischen Eigenschaften als Halbgruppen bzw. Monoide bzw. Gruppen angeht, nicht unterschieden werden. △

Expertenwissen: Transport von Struktur

Bisher haben wir gesehen, dass die Homomorphismus-Eigenschaft die Kompatibilität einer Abbildungen mit *bestehenden* Strukturen wie Halbgruppen oder Gruppen beschreibt. Wir können aber auch mittels einer Abbildung Struktur auf eine andere Menge übertragen, wobei die Abbildung dann automatisch zu einem Homomorphismus wird.

Es sei $(H_1, \star)$ eine Halbgruppe und $(H_2, \square)$ eine Menge mit einer Verknüpfung, von der keine weiteren Eigenschaften bekannt sind. Ist $f\colon H_1 \to H_2$ irgendeine surjektive strukturverträgliche Abbildung, die also (8.1) erfüllt, dann ist $\square$ automatisch assoziativ, also $(H_2, \square)$ eine Halbgruppe. Ist $(H_1, \star)$ ein Monoid mit neutralem Element e_1, so ist auch $(H_2, \square)$ ein Monoid, und zwar mit dem neutralen Element $e_2 := f(e_1)$. Ist $(H_1, \star)$ eine Gruppe, so ist auch $(H_2, \square)$ eine Gruppe. Ist die Verknüpfung $\star$ kommutativ, dann auch $\square$. (**Quizfrage 8.5:** Beweis dieser Aussagen?)

Durch die Surjektivität und die Strukturverträglichkeit von f werden also Eigenschaften von $(H_1, \star)$ auf $(H_2, \square)$ transportiert.

Wir wollen nun Gruppenhomomorphismen genauer studieren.

Definition 8.10 (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 $f\colon G_1 \to G_2$ ein Homomorphismus.

(*i*) Das **Bild** (englisch: image) von f ist definiert als

$$\mathrm{Bild}(f) := \{f(a_1) \in G_2 \mid a_1 \in G_1\} = f(G_1). \tag{8.6}$$

(*ii*) Der **Kern** (englisch: kernel) von f ist definiert als

$$\mathrm{Kern}(f) := \{a_1 \in G_1 \mid f(a_1) = e_2\} = f^{-1}(\{e_2\}). \tag{8.7}$$

△

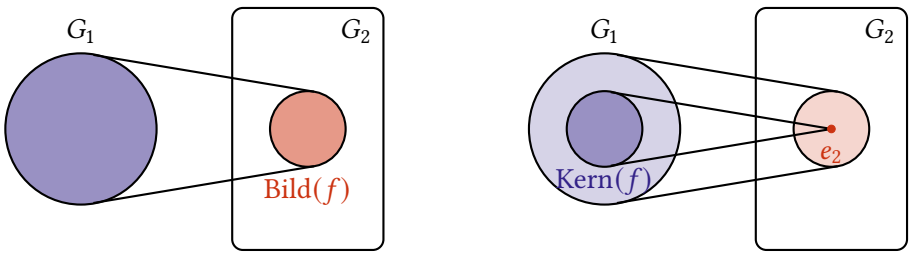


Abbildung 8.1.: Illustration des Bildes (links) und des Kerns (rechts) eines Gruppenhomomorphismus $f\colon G_1 \to G_2$, siehe Definition 8.10.

Lemma 8.11 (Bild und Kern sind Untergruppen)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt:

(*i*) $\mathrm{Bild}(f)$ ist eine Untergruppe von $(G_2, \square)$.

(*ii*) $\mathrm{Kern}(f)$ ist eine Untergruppe von $(G_1, \star)$.

Beweis. Wir bezeichnen die neutralen Elemente von G_1 bzw. G_2 mit e_1 bzw. e_2.

Aussage (*i*): Wir überprüfen das Untergruppenkriterium (Satz 7.44). Nach Lemma 8.8 gilt $e_2 = f(e_1)$, also $e_2 \in \mathrm{Bild}(f)$ und $\mathrm{Bild}(f) \neq \emptyset$. Weiter seien a_2, b_2 irgendwelche Elemente in $\mathrm{Bild}(f)$. Wir müssen zeigen: $a_2 \square b_2' \in \mathrm{Bild}(f)$.

Nach Definition von $\mathrm{Bild}(f)$ gibt es $a_1, b_1 \in G_1$ mit $f(a_1) = a_2$ und $f(b_1) = b_2$. Daher ist

$$\begin{aligned} a_2 \square b_2' &= f(a_1) \square (f(b_1))' && \text{nach Voraussetzung} \\ &= f(a_1) \square f(b_1') && \text{nach Lemma 8.8} \\ &= f(a_1 \star b_1') && \text{da } f \text{ Homomorphismus ist} \end{aligned}$$

und damit $a_2 \square b_2' \in \text{Bild}(f)$.

Aussage (*ii*): Wir überprüfen wiederum das Untergruppenkriterium. Es gilt $f(e_1) = e_2$, also $e_1 \in \text{Kern}(f)$ und $\text{Kern}(f) \neq \emptyset$. Weiter seien a_1, b_1 irgendwelche Elemente in $\text{Kern}(f)$. Wir müssen zeigen: $a_1 \star b_1' \in \text{Kern}(f)$.

$$\begin{aligned} f(a_1 \star b_1') &= f(a_1) \square f(b_1') && \text{da } f \text{ Homomorphismus ist} \\ &= f(a_1) \square (f(b_1))' && \text{nach Lemma 8.8} \\ &= e_2 \square e_2' && \text{da } a_1, b_1 \in \text{Kern}(f) \text{ liegen} \\ &= e_2 && \text{da } e_2' = e_2 \text{ ist.} \end{aligned}$$

Damit ist $a_1 \star b_1' \in \text{Kern}(f)$ gezeigt. □

Beispiel 8.12 (Bild und Kern sind Untergruppen)**.**

(*i*) Für die Abbildung $\#\colon (\Sigma^*, \circ) \to (\mathbb{N}_0, +)$ aus Beispiel 8.7 gilt:

$$\text{Bild}(\#) = \mathbb{N}_0 \quad \text{und} \quad \text{Kern}(\#) = \{()\},$$

wobei $()$ das leere Tupel kennzeichnet. Mit anderen Worten: Das leere Tupel ist das einzige Tupel der Länge 0.

(*ii*) Für die Abbildung $\text{sgn}\colon (S_n, \circ) \to (\{\pm 1\}, \cdot)$ aus Beispiel 8.7 gilt im Fall $n \geqslant 2$:

$$\text{Bild}(\text{sgn}) = \{\pm 1\} \quad \text{und} \quad \text{Kern}(\text{sgn}) = A_n,$$

die alternierende Gruppe, vgl. (7.20). Mit anderen Worten: Die alternatierende Gruppe besteht genau aus den geraden Permutationen.

(*iii*) Für die Abbildung $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 \in (\mathbb{R}_{\neq 0}, \cdot)$ gilt

$$\text{Bild}(f) = \mathbb{R}_{>0} \quad \text{und} \quad \text{Kern}(f) = \{\pm 1\}. \qquad \triangle$$

Das folgende Resultat zeigt, dass Gruppenhomomorphismen genau dann injektiv sind, wenn ihr Kern die minimale Größe hat:

Lemma 8.13 (Charakterisierung der Injektivität von Gruppenhomomorphismen)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann sind äquivalent:

(*i*) f ist injektiv.

(*ii*) $\text{Kern}(f) = \{e_1\}$.

(*iii*) Die einzige Lösung der Gleichung $f(a) = e_2$ ist $a = e_1$.

Beachte: Um die Injektivität einer beliebigen Abbildung zwischen zwei Mengen 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 $G_1 \to G_2$ ist, vereinfacht sich dieser Nachweis erheblich. Wir müssen dann nur noch zeigen, dass neben dem neutralen Element $e_1 \in G_1$ kein weiteres Element auf das neutrale Element $e_2 \in G_2$ abgebildet wird.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Nach Lemma 8.8 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 8.8 $f(e_1) = e_2$ gilt. □

Wir zeigen nun, dass Gruppenhomomorphismen bereits durch ihre Bilder auf einem Erzeugendensystem eindeutig festgelegt sind.

Satz 8.14 (Eindeutigkeitssatz für Gruppenhomomorphismen)**.**

Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen. Weiter seien $f, g\colon G_1 \to G_2$ Homomorphismen, und für ein Erzeugendensystem $E \subseteq G_1$ gelte $f(e) = g(e)$ für alle $e \in E$. Dann ist $f = g$.

Beweis. Es sei $a \in G_1$ beliebig. Dann gibt es nach (7.22) ein $n \in \mathbb{N}_0$ und $a_1, \dots, a_n \in E \cup E'$ mit

$$a = a_1 \star \cdots \star a_n.$$

Für diejenigen a_j mit $a_j \in E$ gilt $f(a_j) = g(a_j)$ nach Voraussetzung. Für diejenigen a_j mit $a_j \in E'$ gilt $a_j' \in E$ und daher nach Lemma 8.8 und nach Vorausetzung $f(a_j)' = f(a_j') = g(a_j') = g(a_j)'$, also wiederum $f(a_j) = g(a_j)$. Wir haben also

$$\begin{aligned} f(a) &= f(a_1 \star \cdots \star a_n) && \text{aufgrund der Darstellung von } a \\ &= f(a_1) \square \cdots \square f(a_n) && \text{da } f \text{ Homomorphismus ist} \\ &= g(a_1) \square \cdots \square g(a_n) && \text{nach Voraussetzung} \\ &= g(a_1 \star \cdots \star a_n) && \text{da } g \text{ Homomorphismus ist} \\ &= g(a) && \text{aufgrund der Darstellung von } a. \end{aligned}$$

□

Ende der Vorlesung 11

§ 8.1 Normalteiler und Faktorgruppen

Wir hatten in Satz 7.55 und Folgerung 7.57 gesehen, dass jede Untergruppe $(U, \star)$ einer Gruppe $(G, \star)$ zwei Äquivalenzrelationen auf G induziert, deren Äquivalenzklassen die Gestalt $a \star U$ bzw. $U \star a$ haben. Diese von U induzierten Äquivalenzrelationen sind (außer in Abelschen Gruppen, Folgerung 7.57) i. A. verschieden (Beispiel 7.59). Wir betrachten im Folgenden aber den Fall, dass sie übereinstimmen:

Definition 8.15 (Normalteiler)**.**

Es sei $(G, \star)$ eine Gruppe. Eine Untergruppe N heißt eine **normale Untergruppe** (englisch: normal subgroup) oder ein **Normalteiler** von $(G, \star)$, wenn gilt:

$$a \star N = N \star a \quad \text{für alle } a \in G. \tag{8.8}$$

Manchmal notiert man die Eigenschaft, dass $(N, \star)$ ein Normalteiler der Gruppe $(G, \star)$ ist, als $(N, \star) \trianglelefteq (G, \star)$. △

Beachte: In (8.8) steht die Gleichheit der beiden Mengen $a \star N$ und $N \star a$. Es wird nicht gefordert, dass $a \star n = n \star a$ für alle $n \in N$ gilt!

Bemerkung 8.16 (Normalteiler)**.**

(*i*) Die definierende Gleichung (8.8) können wir auch so lesen, dass Normalteiler N genau diejenigen Untergruppen einer Gruppe sind, die gegenüber der Konjugation (8.4) mit beliebigen Gruppenelementen invariant sind:

$$a \star N \star a' \subseteq N \quad \text{für alle } a \in G. \tag{8.9}$$

(**Quizfrage 8.6:** Warum folgt aus der Inklusion (8.9) bereits die Gleichheit $a \star N \star a' = N$?)

(*ii*) Die Relation „ist Normalteiler von“ ist zwar reflexiv und antisymmetrisch, aber im Gegensatz zur Relation „ist Untergruppe von“ i. A. nicht transitiv! Im Gegensatz zur Untergruppenrelation ist die Normalteilerrelation also keine Ordnungsrelation. △

Beispiel 8.17 (Normalteiler)**.**

(*i*) In jeder Gruppe $(G, \star)$ sind die trivialen Untergruppen $\{e\}$ und G Normalteiler.

(*ii*) In einer abelschen Gruppe $(G, \star)$ ist *jede* Untergruppe ein Normalteiler (Folgerung 7.57).

(*iii*) Das **Zentrum**[27] (englisch: center)

$$Z := \{z \in G \mid a \star z = z \star a \text{ für alle } a \in G\} \tag{8.10}$$

einer Gruppe $(G, \star)$ ist ein Normalteiler.

[27] Das Zentrum einer Gruppe besteht also aus denjenigen Elementen, die mit allen Gruppenelementen kommutieren.

(*iv*) Der **Kommutator** (englisch: commutator) der Elemente a, b einer Gruppe $(G, \star)$ ist definiert als

$$[a, b] := a \star b \star a' \star b' = (a \star b) \star (b \star a)'. \tag{8.11}$$

Beachte: a und b kommutieren genau dann (bzgl. $\star$), wenn $[a, b]$ das neutrale Element e der Gruppe $(G, \star)$ ergibt. (**Quizfrage 8.7:** Klar?)

Die **Kommutator(unter)gruppe** (englisch: commutator subgroup) der Gruppe $(G, \star)$ ist die von den Kommutatoren von G erzeugte Untergruppe, also

$$\left\langle \{ [a, b] \,\middle|\, a, b \in G \} \right\rangle. \tag{8.12}$$

Sie wird kurz auch in der Form $\left\langle [G, G] \right\rangle$ oder (ungenau) als $[G, G]$ notiert. Die Kommutatorgruppe ist ein Normalteiler von $(G, \star)$. △

Lemma 8.18 (Kerne von Gruppenhomomorphismen sind Normalteiler)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen und $f : G_1 \to G_2$ ein Homomorphismus. Dann gilt:

(*i*) Die Elemente von G_1, die denselben Funktionswert wie $a \in G_1$ haben, sind genau die Elemente der Nebenklasse von $\mathrm{Kern}(f)$ zu a:

$$f^{-1}(\{f(a)\}) = a \star \mathrm{Kern}(f) = \mathrm{Kern}(f) \star a.$$

(*ii*) $\mathrm{Kern}(f)$ ist ein Normalteiler von G_1.

Beweis. Wir bezeichnen die neutralen Elemente von G_1 und G_2 mit e_1 bzw. e_2.

Wir zeigen zunächst die Aussage (*i*) in mehreren Schritten.

Schritt 1: $f^{-1}(\{f(a)\}) \subseteq \mathrm{Kern}(f) \star a$:
Es sei $b \in f^{-1}(\{f(a)\})$, also $f(b) = f(a)$. Dann gilt also

$$\begin{aligned} e_2 &= f(b) \square (f(a))' \\ &= f(b) \square f(a') && \text{nach Lemma 8.8} \\ &= f(b \star a') && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Das heißt aber, dass $b \star a' \in f^{-1}(\{e_2\}) = \mathrm{Kern}(f)$ liegt. Mit anderen Worten: $b \in \mathrm{Kern}(f) \star a$.

Schritt 2: $\mathrm{Kern}(f) \star a \subseteq f^{-1}(\{f(a)\})$:
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 3: $f^{-1}(\{f(a)\}) \subseteq a \star \operatorname{Kern}(f)$:

Ganz analog zu Schritt 1 gilt auch

$$\begin{aligned} e_2 &= (f(a))' \square f(b) \\ &= f(a') \square f(b) && \text{nach Lemma 8.8} \\ &= f(a' \star b) && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Das heißt aber $a' \star b \in f^{-1}(\{e_2\}) = \operatorname{Kern}(f)$ und daher $b \in a \star \operatorname{Kern}(f)$.

Schritt 4: $a \star \operatorname{Kern}(f) \subseteq f^{-1}(\{f(a)\})$:

Es sei $b \in \operatorname{Kern}(f)$. Wir müssen $a \star b \in f^{-1}(\{f(a)\})$ zeigen, also $f(a \star b) = f(a)$. Das folgt aber sofort aus

$$\begin{aligned} f(a \star b) &= f(a) \square f(b) && \text{da } f \text{ Homomorphismus ist} \\ &= f(a) \square e_2 && \text{da } b \in \operatorname{Kern}(f) \text{ ist} \\ &= f(a). \end{aligned}$$

Aus Lemma 8.11 wissen wir, dass $\operatorname{Kern}(f)$ eine Untergruppe von G_1 ist. Aus Aussage (i) folgt $a \star \operatorname{Kern}(f) = \operatorname{Kern}(f) \star a$ für alle $a \in G_1$, also ist $\operatorname{Kern}(f)$ ein Normalteiler von G_1. Das zeigt Aussage (ii). □

Bemerkung 8.19 (Urbilder von Normalteilern sind Normalteiler)**.**
Es gilt sogar folgende Verallgemeinerung der Aussage (ii) aus Lemma 8.18: Urbilder von Normalteilern unter Gruppenhomomorphismen sind Normalteiler. △

Quizfrage 8.8: Ist auch das Bild eines Gruppenhomomorphismus immer ein Normalteiler?

Lemma 8.20 (Durchschnitt von Normalteilern, vgl. Lemma 7.47 zu Untergruppen)**.**
Es sei $(G, \star)$ eine Gruppe.

- (i) Ist $(N_i)_{i \in I}$ eine nichtleere Familie von Normalteilern von $(G, \star)$, dann ist auch $\bigcap_{i \in I} N_i$ ein Normalteiler von G.
- (ii) Ist $\mathcal{N}$ eine nichtleere Menge von Normalteilern von $(G, \star)$, dann ist auch $\bigcap \mathcal{N}$ ein Normalteiler von $(G, \star)$.

Beweis. □

Der nun folgende Satz zeigt: Wenn $(N, \star)$ ein Normalteiler der Gruppe $(G, \star)$ ist, dann können wir die Faktormenge G / N mit einer Gruppenverknüpfung $\tilde{\star}$ ausstatten, die mit $\star$ kompatibel ist. Aus der Faktormenge wird damit die **Faktorgruppe** (englisch: factor group) oder **Quotientengruppe** (englisch: quotient group) **von** G **nach** N. Wir sagen auch: „Der Normalteiler N wird aus der Gruppe $(G, \star)$ ausfaktorisiert."

Satz 8.21 (Faktorgruppe)**.**

- (i) Es sei $(G, \star)$ eine Gruppe und $(N, \star)$ einer ihrer Normalteiler. Dann gilt:

(a) Auf der Faktormenge[28]

$$G/N = \big\{[a] = a \star N \,\big|\, a \in G\big\}$$

ist $\tilde{\star}$, definiert als

$$[a] \,\tilde{\star}\, [b] \coloneqq [a \star b] \quad \text{für } a, b \in G, \tag{8.13}$$

eine assoziative Verknüpfung, bzgl. der $(G/N, \tilde{\star})$ eine Gruppe bildet. Das neutrale Element ist $[e] = N$, und für die Inversen gilt $[a]' = [a']$.

(b) Die Abbildung

$$\pi\colon \begin{cases} G \to G/N \\ a \mapsto [a], \end{cases} \tag{8.14}$$

die jedem Element $a \in G$ seine Nebenklasse $[a] = a \star N$ zuordnet, ist ein surjektiver Gruppenhomomorphismus. Sie heißt die **kanonische Surjektion** (englisch: canonical surjection) **von** G **auf** G/N.[29] Es gilt $\operatorname{Kern}(\pi) = N$.

(c) Wenn $(G, \star)$ abelsch ist, dann auch $(G/N, \tilde{\star})$.

(*ii*) Es sei $(G, \star)$ eine Gruppe und U irgendeine Untergruppe. Ist die Verknüpfung (8.13) auf der Menge der Linksnebenklassen G/U (oder auf der Menge der Rechtsnebenklassen $U \setminus G$) wohldefiniert, dann ist U notwendigerweise ein Normalteiler von G.

Beweis. Aussage (*i*): Wir zeigen zunächst Aussage (a) in mehreren Schritten.

Schritt 1: Wir müssen zunächst zeigen, dass $\tilde{\star}$ überhaupt eine Verknüpfung auf G/N darstellt, also dass (8.13) wohldefiniert ist, da wir dort ja Bezug auf konkrete Repräsentanten $a, b \in G$ der Äquivalenzklassen $[a], [b]$ nehmen. Es seien also $a_1, a_2, b_1, b_2 \in G$ gegeben, wobei $[a_1] = [a_2]$ und $[b_1] = [b_2]$ angenommen wird, d. h., $a_1 \star N = a_2 \star N = N \star a_1 = N \star a_2$ und $b_1 \star N = b_2 \star N = N \star b_1 = N \star b_2$. Dann gilt

$$\begin{aligned}
[a_1] \,\tilde{\star}\, [b_1] &= [a_1 \star b_1] && \text{per Definition von } \tilde{\star} \\
&= (a_1 \star b_1) \star N && \text{nach Definition der Äquivalenzklassen} \\
&= (a_1 \star b_1) \star (N \star N) && \text{da } N \text{ Untergruppe ist, also } N \star N = N \\
&= ((a_1 \star b_1) \star N) \star N && \text{da } \star \text{ assoziativ ist} \\
&= (N \star (a_1 \star b_1)) \star N && \text{da } N \text{ Normalteiler ist} \\
&= (N \star a_1) \star (b_1 \star N) && \text{da } \star \text{ assoziativ ist.}
\end{aligned}$$

Ganz analog gilt auch

$$[a_2] \,\tilde{\star}\, [b_2] = (N \star a_2) \star (b_2 \star N),$$

und mit der Voraussetzung folgt $[a_1] \tilde{\star} [b_1] = [a_2] \tilde{\star} [b_2]$. Damit ist $\tilde{\star}$ als Verknüpfung auf G/N wohldefiniert.

[28] Aus Gründen der Lesbarkeit schreiben wir für die Äquivalenzklasse $a \star N = N \star a$ (Nebenklasse) auch $[a]$.
[29] Die kanonische Surjektion als Abbildung auf die Faktormenge wurde in (6.6) schon eingeführt.

Schritt 2: Die Assoziativität von $\tilde{\star}$ ergibt sich aus der Assoziativität von $\star$ und der Normalteilereigenschaft, denn es gilt mit ähnlichen Argumenten wie eben

$$\begin{aligned}([a] \mathbin{\tilde{\star}} [b]) \mathbin{\tilde{\star}} [c] &= [a \star b] \mathbin{\tilde{\star}} [c] = (a \star b \star N) \star (c \star N) = (a \star b \star N) \star (N \star c) \\ &= a \star b \star N \star c = a \star b \star c \star N\end{aligned}$$

und auch

$$\begin{aligned}[a] \mathbin{\tilde{\star}} ([b] \mathbin{\tilde{\star}} [c]) &= [a] \mathbin{\tilde{\star}} [b \star c] = (a \star N) \star (b \star c \star N) = (a \star N) \star (N \star b \star c) \\ &= a \star N \star b \star c = a \star b \star c \star N.\end{aligned}$$

Damit haben wir zunächst $(G/N, \tilde{\star})$ als Halbgruppe bestätigt.

Schritt 3: Wir notieren das neutrale Element von G als e und zeigen, 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 (8.13)

$$[e] \mathbin{\tilde{\star}} [a] = [e \star a] = [a] \quad \text{sowie} \quad [a] \mathbin{\tilde{\star}} [e] = [a \star e] = [a].$$

Also ist $(G/N, \tilde{\star})$ ein Monoid mit neutralem Element $[e]$.

Schritt 4: 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 (b): 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 $[a \star b] = [a] \mathbin{\tilde{\star}} [b]$, 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 $\operatorname{Kern}(\pi) = \pi^{-1}([e]) = N$.

Aussage (c): 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.

Nun zur umgekehrten Aussage *(ii)*: Es sei dazu U irgendeine Untergruppe von G. Wir führen den Beweis nur für den Fall, dass (8.13) auf der Menge der Linksnebenklassen G/U wohldefiniert ist. Es seien dazu $a \in G$ und $u \in U$ beliebig. Dann gilt $[u] = U = [e]$, und die Wohldefiniertheit liefert

$$[a] = [e \star a] = [e] \mathbin{\tilde{\star}} [a] = [u] \mathbin{\tilde{\star}} [a] = [u \star a],$$

also $a \star U = u \star a \star U$ oder $U = a' \star u \star a \star U$. Das heißt aber, dass $a' \star u \star a \in U$ liegt. (**Quizfrage 8.9:** Warum?) Da $u \in U$ beliebig war, haben wir $a' \star U \star a \subseteq U$ für alle $a \in G$. Nach Bemerkung 8.16 ist U ein Normalteiler von G. □

Bemerkung 8.22 (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 $b \in a \star N$ gilt) nicht mehr unterschieden, sondern miteinander identifiziert werden. Die Faktorgruppe $(G/N, \tilde{\star})$ ist also eine „gröbere Version“ der Gruppe $(G, \star)$. Wegen $[a] \mathbin{\tilde{\star}} [b] = [a \star b]$ rechnen wir mit Nebenklassen, indem wir stellvertretend mit Repräsentanten rechnen. △

Beispiel 8.23 (Faktorgruppe)**.**

(*i*) Es sei $(G, \star)$ eine beliebige Gruppe. Dann ist $N = \{e\}$, eine der beiden trivialen Untergruppen von G, nach Beispiel 8.17 ein Normalteiler. Die zugehörige Faktorgruppe $(G/\{e\}, \tilde{\star})$ ist isomorph zur Ausgangsgruppe $(G, \star)$ selbst.

(*ii*) Es sei $(G, \star)$ eine beliebige Gruppe und $N = G$ die andere triviale Untergruppe von G. G ist nach Beispiel 8.17 ein Normalteiler. Die zugehörige Faktorgruppe $(G/G, \tilde{\star})$ ist isomorph zu $(\{e\}, \star)$.

(*iii*) Es sei $(G, \star)$ eine beliebige Gruppe und K die Kommutatoruntergruppe von G (Beispiel 8.17). Dann ist die Faktorgruppe $(G/K, \tilde{\star})$ kommutativ.

Tatsächlich ist $(G/N, \tilde{\star})$ genau dann kommutativ, wenn der ausfaktorisierte Normalteiler N die Kommutatoruntergruppe von G enthält.

(*iv*) Für $m \in \mathbb{N}$ ist $m\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$. Da $(\mathbb{Z}, +)$ abelsch ist, ist jede dieser Untergruppen 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 7.59. Es gilt

$$[a] \tilde{+} [b] = [a + b].$$

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 7.22 mittels des Isomorphismus $[a] \mapsto$ natürlicher Repräsentant von a in $\mathbb{Z}_m$. Beispielsweise können wir für $m = 5$ wie folgt rechnen:

$$\begin{array}{lccccc} \text{in } (\mathbb{Z}/5\mathbb{Z}, \tilde{+}) & [-21] & \tilde{+} & [9] & = & [-12] \\ & \downarrow & & \downarrow & & \downarrow \\ \text{in } (\mathbb{Z}_5, +_5) & 4 & +_5 & 4 & = & 3 \end{array}$$

(*v*) In der abelschen Gruppe $(\mathbb{Q}_{\neq 0}, \cdot)$ ist die Untergruppe $(\{\pm 1\}, \cdot)$ ein Normalteiler. Die Elemente der Faktorgruppe sind die Nebenklassen

$$[a] = a \cdot \{\pm 1\} = \{a, -a\}$$

für $a \in \mathbb{Q}_{\neq 0}$. Ein mögliches Repräsentantensystem sind die positiven rationalen Zahlen $\mathbb{Q}_{>0}$. Durch $\mathbb{Q}_{\neq 0}/\{\pm 1\}$ wird also „das Vorzeichen ausfaktorisiert“. Dieselbe Konstruktion können wir in $\mathbb{R}_{\neq 0}$ und $\mathbb{C}_{\neq 0}$ durchführen. △

Bemerkung 8.24 (Normalteiler sind genau die Kerne von Gruppenhomomorphismen)**.**

Es sei $(G_1, \star)$ eine Gruppe.

(*i*) Nach Lemma 8.18 ist die Untergruppe $\mathrm{Kern}(f)$ für jeden beliebigen Gruppenhomomorphismus $f\colon G_1 \to G_2$ in irgendeine Gruppe $(G_2, \square)$ immer ein Normalteiler von $(G_1, \star)$.

(*ii*) Umgekehrt gilt auch, dass jeder Normalteiler N von $(G_1, \star)$ der Kern eines Gruppenhomomorphismus ist. Dazu wählen wir einfach $G_2 := (G_1/N, \tilde{\star})$ als Zielgruppe und die kanonische Surjektion $\pi\colon G_1 \to G_1/N$ als Gruppenhomomorphismus. Dann gilt $\mathrm{Kern}(\pi) = N$. △

§ 8.2 Der 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.[30] 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 den Normalteiler $\operatorname{Kern}(f)$.

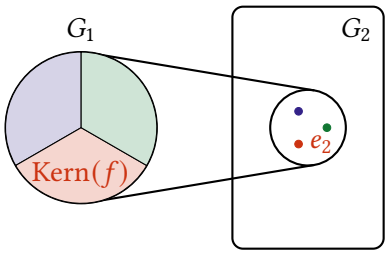


Abbildung 8.2.: Illustration des Homomorphiesatzes für Gruppenhomomorphismen 8.25. Alle Elemente einer Nebenklasse des Normalteilers $\operatorname{Kern}(f)$ werden auf ein- und dasselbe Element von G_2 abgebildet und verschiedene Nebenklassen auf verschiedene Elemente.

Satz 8.25 (Homomorphiesatz für Gruppen[31]).
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt

$$G_1 / \operatorname{Kern}(f) \cong \operatorname{Bild}(f) \tag{8.15a}$$

mit dem Isomorphismus

$$I([a]) \coloneqq f(a) \quad \text{für } [a] = a \star \operatorname{Kern}(f) \in G_1 / \operatorname{Kern}(f). \tag{8.15b}$$

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 (8.15).

Schritt 1: Wir müssen zunächst zeigen, dass I als Abbildung wohldefiniert ist, da wir in der Definition (8.15b) Bezug auf den konkreten Repräsentanten $a \in G_1$ nehmen.

Es seien dazu $a, b \in G_1$ gegeben mit $a \overset{U}{\sim} b$ für $U = \operatorname{Kern}(f)$, d. h., $a \star \operatorname{Kern}(f) = b \star \operatorname{Kern}(f)$. Dann folgt

$$\begin{aligned} f(a \star \operatorname{Kern}(f)) &= f(a) \square f(\operatorname{Kern}(f)) && \text{da } f \text{ Homomorphismus ist} \\ &= \{f(a)\} && \text{da } f(\operatorname{Kern}(f)) = \{e_2\} \text{ gilt} \end{aligned}$$

[30] Anders ausgedrückt: Die Fasern (Definition 6.6) von f sind gerade die Nebenklassen von $\operatorname{Kern}(f)$.
[31] englisch: fundamental theorem on group homomorphisms

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

$$\begin{aligned} I([a] \mathbin{\tilde{\star}} [b]) &= I([a \star b]) && \text{nach Definition (8.13) von } \tilde{\star} \\ &= f(a \star b) && \text{nach Definition von } I \\ &= f(a) \square f(b) && \text{da } f \text{ Homomorphismus ist} \\ &= I([a]) \square I([b]) && \text{nach Definition von } I. \end{aligned}$$

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

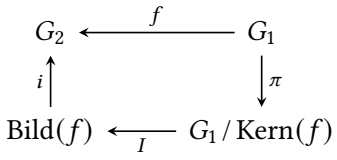
$$a_2 = f(a_1) = I([a_1]).$$

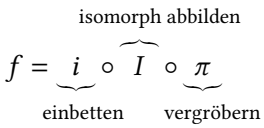
Das zeigt die Surjektivität von I.

Für die Injektivität genügt es nach Lemma 8.13 zu zeigen, dass $\operatorname{Kern}(I)$ nur aus dem neutralen Element des Definitionsbereichs $G_1 / \operatorname{Kern}(f)$ besteht, d. h., aus $[e_1] = \operatorname{Kern}(f)$, vgl. Satz 8.21. Es gilt

$$\begin{aligned} &\operatorname{Kern}(I) \\ &\quad = \big\{[a] \in G_1 / \operatorname{Kern}(f) \,\big|\, I([a]) = e_2\big\} && \text{nach Definition von Kern}(I) \\ &\quad = \big\{[a] \in G_1 / \operatorname{Kern}(f) \,\big|\, f(a) = e_2\big\} && \text{nach Definition von } I \\ &\quad = \big\{[a] \in G_1 / \operatorname{Kern}(f) \,\big|\, a \in \operatorname{Kern}(f)\big\} && \text{nach Definition von Kern}(f) \\ &\quad = \big\{a \star \operatorname{Kern}(f) \,\big|\, a \in \operatorname{Kern}(f)\big\} && \text{wegen } [a] = a \star \operatorname{Kern}(f) \\ &\quad = \big\{\operatorname{Kern}(f)\big\} && \text{da Kern}(f) \text{ Untergruppe ist.} \quad \square \end{aligned}$$

Wir stellen den Homomorphiesatz für Gruppen 8.25 auch noch einmal schematisch mit Hilfe eines kommutativen Diagrammes dar.[32] Dazu sei $i\colon \operatorname{Bild}(f) \ni a \mapsto a \in G_2$ der injektive Homomorphismus der kanonischen Einbettung.





Expertenwissen: universelle Eigenschaft von Faktorgruppen

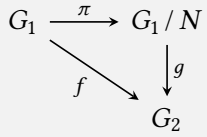
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen und $f\colon G_1 \to G_2$ ein Homomorphismus. Weiter sei N eine normale Untergruppe von G_1. Dann sind äquivalent:

(*i*) $N \subseteq \operatorname{Kern}(f)$, also $f(N) = \{e_2\}$.

(*ii*) Der Homomorphismus f **faktorisiert durch** (englisch: factors through) die kanonische Surjektion $\pi\colon G_1 \to G_1 / N$, d. h., es gibt einen eindeutig bestimmten

[32] Ein solches Diagramm heißt **kommutativ** (englisch: commutative diagram), wenn alle Pfade mit demselben Ausgangs- und demselben Endpunkt dasselbe Ergebnis produzieren.

Homomorphismus $g\colon G_1 / N \to G_2$ mit $f = g \circ \pi$.



Diese Eigenschaft nennt sich die **universelle Eigenschaft von Faktorgruppen** (englisch: universal property of quotient groups), denn sie charakterisiert Faktorgruppen bis auf Isomorphie eindeutig. Gilt also die obige Äquivalenzaussage mit irgendeiner Gruppe H an Stelle von G_1 / N und einem surjektiven Gruppenhomomorphismus $\pi\colon G_1 \to H$, dann ist H isomorph zu G_1 / N. Die universelle Eigenschaft ermöglicht es, Faktorgruppen (bis auf Isomorphie) zu definieren, ohne die konkrete Konstruktion über Nebenklassen zu verwenden.

Bemerkung 8.26 (mögliche Gruppenhomomorphismen)**.**
Wegen $G_1 / \operatorname{Kern}(f) \cong \operatorname{Bild}(f)$ legen die Normalteiler einer Gruppe $(G_1, \star)$ im Wesentlichen die möglichen Gruppenhomomorphismen fest, die von G_1 aus möglich sind. Zu jedem Normalteiler N gibt es einen natürlichen, surjektiven Gruppenhomomorphismus $\pi\colon G_1 \to G_1 / N$. Dieser ist gewissermaßen der „Prototyp“ eines Gruppenhomomorphismus auf G_1, der N als Kern hat. Jeder andere Gruppenhomomorphismus $f\colon G_1 \to G_2$ mit $\operatorname{Kern}(f) = N$ ist dann nur eine „eingebettete“ Version dieses Prototyps, also $f = i \circ \pi$ mit dem injektiven Homomorphismus $i\colon G_1 / N \to G_2$ der kanonischen Einbettung und $\operatorname{Bild}(i) = \operatorname{Bild}(f)$. △

Beispiel 8.27 (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 8.7 und 8.12. 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 gleichmächtigen Nebenklassen

$$[\mathrm{id}] = \mathrm{id} \circ A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} \quad \text{(gerade Permutationen)},$$
$$[\tau] = \tau \circ A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = -1\} \quad \text{(ungerade Permutationen)},$$

wobei τ irgendeine Transposition in S_n ist. Gemäß Homomorphiesatz 8.25 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 8.25 besagt daher in diesem Fall

$$S_1 / \operatorname{Kern}(\operatorname{sgn}) = S_1 / A_1 \cong \operatorname{Bild}(\operatorname{sgn}) = \{1\}.$$

Ähnliches gilt im Fall $n = 0$.

(*ii*) Für die Abbildung $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 \in (\mathbb{R}_{\neq 0}, \cdot)$ aus Beispiel 8.12 und Beispiel 8.23 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.

(*iii*) Für die Abbildung $f\colon (\mathbb{C}_{\neq 0}, \cdot) \ni z \mapsto |z| \in (\mathbb{R}_{\neq 0}, \cdot)$ gilt

$$\mathbb{C}_{\neq 0} / \operatorname{Kern}(f) = \mathbb{R}_{\neq 0} / K \cong \operatorname{Bild}(f) = \mathbb{R}_{>0},$$

wobei $K \coloneqq \{z \in \mathbb{C}_{\neq 0} \mid |z| = 1$ der Einheitskreis in $\mathbb{C}$ ist. Durch $\operatorname{Kern}(f) = K$ wird die Lage von z auf der Kreislinie mit Radius $|z|$ ausfaktorisiert. △

Ende der Vorlesung 12

Ende der Woche 6

§ 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 das Leit-Beispiel $\mathbb{Z}$ mit den Verknüpfungen „Addition“ und „Multiplikation“ bezeichnen wir diese Verknüpfungen häufig mit + und ·.

Definition 9.1 (Ring)**.**

Ein **Ring** (englisch: ring) $(R, +, \cdot)$ ist eine Menge R mit zwei (inneren) Verknüpfungen + („Addition“) und · („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.[33] In diesem Fall fallen die beiden Distributivgesetze (9.1a) und (9.1b) zusammen, sind also untereinander äquivalent. △

[33] Die Bezeichnung „abelscher Ring“ ist nicht üblich, sie wird manchmal sogar für eine andere Eigenschaft verwendet als für die Kommutativität der Multiplikation.

Wie in Gruppen in additiver Notation üblich (Bemerkung 7.20), bezeichnen wir das neutrale Element eines Ringes $(R, +, \cdot)$ bzgl. $+$ als **Nullelement** (englisch: additive identity) und schreiben dafür zunächst „0_R“. Außerdem benennen wir das bzgl. $+$ inverse Element zu $a \in R$ mit $-a$. Die Bezeichnung $a - b$ steht für $a + (-b)$.

Falls die Halbgruppe $(R, \cdot)$ sogar 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, unital ring). Existiert dann zu $a \in R$ bzgl. $\cdot$ ein inverses Element, so bezeichnen wir dieses mit a^{-1}.

Wie üblich vereinbaren wir, dass $\cdot$ stärker bindet als $+$ („Punkt- vor Strichrechnung“), also könnten wir z. B. die rechte Seite in (9.1a) auch in der Form $a \cdot b + a \cdot c$ schreiben. Außerdem können wir $-a \cdot b$ schreiben statt $-(a \cdot b)$.

Beispiel 9.2 (Ring, vgl. Beispiel 7.22 zu Gruppen)**.**

(*i*) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.

(*ii*) Ein Ring $(R, +, \cdot)$ heißt ein **Nullring** (englisch: zero ring), wenn R nur aus einem Element besteht, also wenn $R = \{0_R\}$ gilt. Dadurch sind die Verknüpfungen eindeutig bestimmt: $0_R + 0_R = 0_R$ und $0_R \cdot 0_R = 0_R$. Da 0_R notwendigerweise auch das neutrale Element bzgl. $\cdot$ ist, ist ein Nullring ein Ring mit Eins, und es gilt $1_R = 0_R$.

Nullringe sind die einzigen Ringe, in dem das Nullelement und das Einselement identisch sind, siehe Lemma 9.3. Ein Nullring ist bis auf Isomorphie (Definition 9.17) eindeutig bestimmt, daher wird oft auch die Bezeichnung „**der Nullring**“ verwendet.

(*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.

(*iv*) Für $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit Einselement $1 \in \mathbb{Z}_m$, denn nach Beispiel 7.22 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 $(\mathbb{Z}_m, +_m, \cdot_m)$ ein Nullring.

(*v*) Es sei X eine Menge und $(R, +, \cdot)$ ein Ring. Dann ist $R^X = \{f \mid f \colon X \to R\}$, ausgestattet mit der punktweisen Addition und der punktweisen Multiplikation, ein Ring. Das Nullelement in $(R^X, +, \cdot)$ ist die **Nullfunktion** (englisch: zero function, constant function zero) $x \mapsto 0_R$. Besitzt R das Einselement 1_R, dann ist die **Einsfunktion** (englisch: constant function one) $x \mapsto 1_R$ das Einselement von $(R^X, +, \cdot)$.

Quizfrage 9.1: Wann ist $(R^X, +, \cdot)$ ein Nullring? Wann ist er kommutativ?

(*vi*) Es sei $(G, +)$ eine abelsche Gruppe. Wir definieren

$$\operatorname{End}(G) \coloneqq \{f \colon G \to G \mid f \text{ ist Endomorphismus}\} \tag{9.2}$$

und statten $\operatorname{End}(G)$ mit den Verknüpfungen

$$+ \colon \begin{cases} \operatorname{End}(G) \times \operatorname{End}(G) \to \operatorname{End}(G) \\ (f, g) \mapsto f + g, \end{cases}$$

definiert durch die punktweise Addition $(f+g)(x) \coloneqq f(x)+g(x)$ für $x \in G$, und

$$\circ\colon \begin{cases} \mathrm{End}(G) \times \mathrm{End}(G) \to \mathrm{End}(G) \\ (f,g) \mapsto f \circ g, \end{cases}$$

definiert durch die Komposition $(f \circ g)(x) \coloneqq f(g(x))$, aus. Dann ist $(\mathrm{End}(G), +, \circ)$ ein Ring mit Einselement id_G, genannt der **Endomorphismenring** (englisch: ring of endomorphisms) der abelschen Gruppe $(G,+)$. Er ist i. A. nicht kommutativ.

Quizfrage 9.2: Warum definieren wir den Endomorphismenring nur auf abelschen Gruppen und nicht allgemeiner auf beliebigen Gruppen?

(*vii*) Ist X eine Menge, dann ist $(\mathcal{P}(X), \triangle, \cap)$ ein kommutativer Ring mit Einselement X.

(*viii*) Ist X eine nichtleere Menge, dann ist $(\mathcal{P}(X), \triangle, \cup)$ ist kein Ring, da das Distributivgesetz nicht gilt. △

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 kein Nullring, dann gilt $1_R \neq 0_R$.

Beachte: Hat $(R,+,\cdot)$ das Einselement 1_R, dann folgt aus Aussage (*ii*) insbesondere $-b = (-1_R)\cdot b$. („Das additive Inverse ergibt sich auch durch Multiplikation mit dem additiven Inversen des Einselements.“)

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 (7.8b) in der Gruppe $(R,+)$, also die Addition von $-(0_R \cdot a)$ zu beiden Seiten der Gleichung, zeigt $0_R = 0_R \cdot a$. 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. Da $(R,+)$ eine abelsche Gruppe ist (oder auch wegen Lemma 7.19) reicht dafür der Nachweis von $a \cdot (-b) + a \cdot b = 0_R$ aus, also der einseitige Test. In der Tat haben wir

$$\begin{aligned} a \cdot (-b) + a \cdot b &= a \cdot (-b + b) && \text{wegen des Distributivgesetzes (9.1a)} \\ &= a \cdot 0_R \\ &= 0_R && \text{nach Aussage (}i\text{).} \end{aligned}$$

Die Aussage $(-a) \cdot b = -a \cdot b$ folgt analog.

Aussage (*iii*): Wir haben

$$\begin{aligned}(-a)\cdot(-b) &= -(a\cdot(-b)) && \text{nach Aussage } (ii)\\ &= -(-a\cdot b) && \text{nach Aussage } (ii)\\ &= a\cdot b && \text{denn Invertierung ist involutorisch, siehe (7.5).}\end{aligned}$$

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 ein Nullring. □

Wir verwenden auch in Ringen $(R,+,\cdot)$ und insbesondere in der Gruppe $(R,+)$ die Schreibweisen aus Bemerkung 7.20. Es gilt also für $n \in \mathbb{N}$

$$n\,a := a + \cdots + a \quad \text{und} \quad a^n := a \cdot \cdots \cdot a.$$

Weiter ist $(-n)\,a := -(n\,a) = n\,(-a)$ und $0\,a := 0_R$. Besitzt $(R,+,\cdot)$ das Einselement 1_R, dann gilt nach dem Distributivgesetz (9.1b) weiter

$$n\,a = a + \cdots + a = 1_R\cdot a + \cdots + 1_R\cdot a = (1_R + \cdots + 1_R)\cdot a = (n\,1_R)\cdot a.$$

und analog $n\,a = a\cdot(n\,1_R)$. Dann definieren wir auch $a^0 := 1_H$. Ist $a \in R$ zudem multiplikativ invertierbar, so ist $a^{-n} := (a^n)^{-1} = (a^{-1})^n$.

Definition 9.4 (Charakteristik eines Ringes)**.**
Es sei $(R,+,\cdot)$ 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 **Charakteristik** (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 **Charakteristik** 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*) Nullringe sind die einzigen Ringe mit Charakteristik 1, also die einzigen Ringe, in denen $1_R = 0_R$ 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 8.23 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 $[0]$.

Weiter bildet $(\mathbb{Z}/m\mathbb{Z}, \mathbin{\tilde{\cdot}})$ mit der Verknüpfung $[a] \mathbin{\tilde{\cdot}} [b] = [a \cdot b]$ ein kommutatives Monoid mit dem neutralen Element $[1]$, siehe auch Übung.

Schließlich können wir zeigen, dass die Distributivgesetze (9.1a) und (9.1b) gelten, denn:

$$\begin{aligned}
[a] \mathbin{\tilde{\cdot}} ([b] \mathbin{\tilde{+}} [c]) &= [a] \mathbin{\tilde{\cdot}} [b+c] && \text{nach Definition von } \mathbin{\tilde{+}} \\
&= [a \cdot (b+c)] && \text{nach Definition von } \mathbin{\tilde{\cdot}} \\
&= [a \cdot b + a \cdot c] && \text{nach Distributivgesetz in } \mathbb{Z} \\
&= [a \cdot b] \mathbin{\tilde{+}} [a \cdot c] && \text{nach Definition von } \mathbin{\tilde{+}} \\
&= [a] \mathbin{\tilde{\cdot}} [b] \mathbin{\tilde{+}} [a] \mathbin{\tilde{\cdot}} [c] && \text{nach Definition von } \mathbin{\tilde{\cdot}}.
\end{aligned}$$

Das zweite Distributivgesetz (9.1b) ist wegen der Kommutativität der Halbgruppe $(\mathbb{Z}/m\mathbb{Z}, \mathbin{\tilde{\cdot}})$ ebenfalls erfüllt. Daher bildet $(\mathbb{Z}/m\mathbb{Z}, \mathbin{\tilde{+}}, \mathbin{\tilde{\cdot}})$ einen kommutativen Ring mit Eins, genannt der **Restklassenring modulo** m. Im Fall $m = 1$ ist $(\mathbb{Z}/m\mathbb{Z}, \mathbin{\tilde{+}}, \mathbin{\tilde{\cdot}})$ ein 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 im Fall $m = 4$ 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) **von** R, wenn es ein $b \in R \setminus \{0_R\}$ gibt, sodass $a \cdot b = 0_R$ gilt.

(*ii*) Das Element b heißt ein **Rechtsnullteiler** (englisch: right zero divisor) **von** R, wenn es ein $a \in R \setminus \{0_R\}$ gibt, sodass $a \cdot b = 0_R$ gilt.

(*iii*) Ein Element, das Links- oder Rechtsnullteiler ist, heißt auch einfach ein **Nullteiler** (englisch: zero divisor). Ein Element, das gleichzeitig Links- und Rechtsnullteiler ist, heißt auch einfach ein **zweiseitiger Nullteiler** (englisch: two-sided zero divisor).

(*iv*) Der Ring $(R, +, \cdot)$ heißt **nullteilerfrei** (englisch: ring with no zero divisors), wenn es außer dem trivialen (zweiseitigen) Nullteiler 0_R keine weiteren Links- oder Rechtsnullteiler gibt, wenn also gilt:

$$\forall a, b \in R \ (a \cdot b = 0_R \implies a = 0_R \text{ oder } b = 0_R). \tag{9.3}$$

(„Ein Produkt ist nur dann Null, wenn mindestens einer der Faktoren gleich Null ist.“)

(*v*) Der Ring $(R, +, \cdot)$ heißt ein **Integritätsring** oder **Integritätsbereich** (englisch: integral domain), wenn gilt: $(R, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit Eins, der kein Nullring ist.[34] △

Lemma 9.8 (Charakterisierung von Nullteilern)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(*i*) Für $a \in R$ sind äquivalent:
  (a) a ist kein Linksnullteiler von R.
  (b) Der Gruppenhomomorphismus $(R, +) \ni b \mapsto a \cdot b \in (R, +)$ ist injektiv.
  (c) Für alle $b, c \in R$ gilt: $a \cdot b = a \cdot c$ impliziert $b = c$, d. h., a ist **linkskürzbar** (englisch: left-cancellative).

(*ii*) Für $b \in R$ sind äquivalent:
  (a) a ist kein Rechtsnullteiler von R.
  (b) Der Gruppenhomomorphismus $(R, +) \ni a \mapsto a \cdot b \in (R, +)$ ist injektiv.
  (c) Für alle $b, c \in R$ gilt: $a \cdot b = c \cdot b$ impliziert $a = c$, d. h., a ist **rechtskürzbar** (englisch: right-cancellative).

Beweis. □

Quizfrage 9.3: Ist ein Nullring nullteilerfrei?

Beispiel 9.9 (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 9.11.

(*iii*) Es sei X eine Menge, $(R, +, \cdot)$ ein Ring. Wir betrachten den Ring $(R^X, +, \cdot)$, siehe Beispiel 9.2. Dieser ist genau dann nullteilerfrei, wenn R ein Nullring ist oder wenn $X = \emptyset$ gilt oder wenn (X genau ein Element hat und R nullteilerfrei ist). (**Quizfrage 9.4:** Nachweis?)

[34] Als Merkhilfe für die definierenden Eigenschaften eines Integritätsrings kann man sich an $(\mathbb{Z}, +, \cdot)$ orientieren.

(*iv*) $(\mathcal{P}(X), \triangle, \cap)$ ist genau dann nullteilerfrei, wenn X höchstens ein Element hat. Sobald X zwei verschiedene Elemente a und b hat, sind $A = \{a\}$ und $B = \{b\}$ Mengen ungleich dem Nullelement (der leeren Menge), deren „Multiplikation“ $A \cap B = \emptyset$ das Nullelement ergibt. $(\mathcal{P}(X), \triangle, \cap)$ ist also genau dann ein Integritätsring, wenn X genau ein Element hat. Im Fall $X = \emptyset$ ist $(\mathcal{P}(X), \triangle, \cap)$ ein Nullring. △

Lemma 9.10 (notwendige Bedingung für die Nullteilerfreiheit)**.**
Für jeden nullteilerfreien Ring R mit Eins ist $\operatorname{char}(R)$ entweder gleich 0 oder eine Primzahl.

Beweis. Wäre $\operatorname{char}(R) = n_1 n_2$ mit $n_1, n_2 \in \mathbb{N}_{\geqslant 2}$, dann hätten wir

$$0_R = (n_1 n_2)\, 1_R = (n_1\, 1_R) \cdot (n_2\, 1_R),$$

und aufgrund der Nullteilerfreiheit würde $n_1\, 1_R = 0_R$ oder $n_2\, 1_R = 0_R$ folgen. Das steht aber im Widerspruch dazu, dass $\operatorname{char}(R) = n_1 n_2$ nach Definition 9.4 die kleinste Zahl ist, für die $n_1\, 1_R = 0_R$ gilt. □

Satz 9.11 (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 $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ein Nullring und damit kein Integritätsring. Wir betrachten also im Weiteren nur den Fall $m \geqslant 2$. Das heißt, $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist ein kommutativer Ring ungleich einem Nullring mit dem Einselement $[1]$ (Beispiel 9.6). 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 zunächst $m \in \mathbb{N}$, $m \geqslant 2$, eine Primzahl. Wir nehmen an, $[a]$ und $[b]$ seien Elemente aus $\mathbb{Z}/m\mathbb{Z}$ mit $[0] = [a] \tilde{\cdot} [b] = [a \cdot b]$. 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.

Es sei nun umgekehrt $m \in \mathbb{N}$, $m \geqslant 4$, *keine* Primzahl; sie lässt sich also schreiben als $m = a \cdot b$ mit Zahlen $a, b \in [\![2, m-1]\!]$. Die zugehörigen Restklassen $[a]$ und $[b]$ sind ungleich $[0]$ (**Quizfrage 9.5:** Warum?) Es gilt

$$\begin{aligned} [0] &= [m] && \text{da } 0 \overset{m}{\equiv} m \\ &= [a \cdot b] && \text{da } m = a \cdot b \\ &= [a] \tilde{\cdot} [b] && \text{nach Definition von } \tilde{\cdot}. \end{aligned}$$

Damit ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ *nicht* nullteilerfrei.

□

Definition 9.12 (Unterring, vgl. Definition 7.42 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 und wenn $(U, +, \cdot)$ selbst wieder ein Ring ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, +)$ eine Untergruppe von $(R, +)$ und wenn U eine Unterhalbgruppe von $(R, \cdot)$ ist.

(*ii*) Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R, dann heißt ein Unterring U, der auch das Einselement 1_R enthält, ein **Unterring mit Eins** (englisch: subring with unity).[35]

Beachte: Es reicht nicht aus, zu fordern, dass $(U, \cdot)$ *irgendein* neutrales Element besitzt.

(*iii*) Ein Unterring U von $(R, +, \cdot)$ heißt **echt** (englisch: proper subring), wenn $U \subsetneq R$ gilt. △

Die Prüfung einer Teilmenge $U \subseteq R$ auf die Unterring-Eigenschaft lässt sich mit folgendem Kriterium erreichen:

Satz 9.13 (Unterringkriterium, vgl. Satz 7.44 zum Untergruppenkriterium)**.**

Es sei $(R, +, \cdot)$ ein Ring und $U \subseteq R$. Dann sind äquivalent:

(*i*) $(U, +, \cdot)$ ist ein Unterring von $(R, +, \cdot)$.

(*ii*) $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a - b \in U$ und $a \cdot b \in U$.[36]

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $(U, +, \cdot)$ ein Unterring von $(R, +, \cdot)$. Dann enthält U notwendigerweise das Nullelement 0_R von $(R, +, \cdot)$, also das neutrale Element der Untergruppe $(U, +)$ von $(R, +)$. Für $a, b \in U$ gilt $-b \in U$ nach Lemma 7.43. Da U bzgl. $+$ abgeschlossen ist, folgt $a - b = a + (-b) \in U$, und da U bzgl. $\cdot$ abgeschlossen ist, folgt $a \cdot b \in U$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Nach Voraussetzung erfüllt $(U, +)$ das Untergruppenkriterium (Satz 7.44), also ist $(U, +)$ eine Untergruppe von $(R, +)$. Außerdem ist U nach Voraussetzung abgeschlossen bzgl. $\cdot$, d. h., $(U, \cdot)$ ist eine Unterhalbgruppe von $(R, \cdot)$. Damit ist $(U, +, \cdot)$ ein Unterring von $(R, +, \cdot)$. □

Beispiel 9.14 (Unterring)**.**

(*i*) $(\mathbb{Z}, +, \cdot)$ ist ein Unterring mit Eins von $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ ist ein Unterring mit Eins von $(\mathbb{R}, +, \cdot)$, und $(\mathbb{R}, +, \cdot)$ ist ein Unterring mit Eins von $(\mathbb{C}, +, \cdot)$.

(*ii*) Der Nullring $\{0_R\}$ ist ein Unterring in jedem Ring $(R, +, \cdot)$.

(*iii*) Für $m \in \mathbb{N}$ ist $(m\mathbb{Z}, +, \cdot)$ ein Unterring von $(\mathbb{Z}, +, \cdot)$. Im Fall $m \neq 1$ handelt es sich nicht um einen Unterring mit Eins.

[35] Dadurch ist der Unterring $(U, +, \cdot)$ dann natürlich selbst wieder ein Ring mit demselben Einselement 1_R.
[36] kurz: $U - U \subseteq U$ und $U \cdot U \subseteq U$

(*iv*) Für $k, m \in \mathbb{N}$ ist

$$\{n \mid n \in k\,\mathbb{Z} \cap \mathbb{Z}_m\} = \{0, k, 2\,k, \dots, \} \cap \{0, 1, \dots, m-1\}$$

mit den Operationen $+_m$ und $\cdot_m$ genau dann ein Unterring von $(\mathbb{Z}_m, +_m, \cdot_m)$, wenn $k \mid m$ gilt. Beispielsweise ist $(2\,\mathbb{Z} \cap \mathbb{Z}_4, +_4, \cdot_4)$ ein Unterring von $(\mathbb{Z}_4, +_4, \cdot_4)$, der nur aus den geraden Zahlen, also $\{0, 2\}$ besteht. Die Verknüpfungstafeln hatten wir in Beispiel 9.6 bereits angegeben (für den zu $\mathbb{Z}_4$ isomorphen Restklassenring $\mathbb{Z}/4\,\mathbb{Z}$, siehe Beispiel 9.32):

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Zu beachten sind in $2\,\mathbb{Z} \cap \mathbb{Z}_4$ nur diejenigen Zeilen und Spalten, die zu geraden Zahlen gehören, diese sind farbig hinterlegt.

(*v*) Ist X eine Menge und $Y \subseteq X$, dann ist $(\mathcal{P}(Y), \triangle, \cap)$ ein Unterring von $(\mathcal{P}(X), \triangle, \cap)$. Im Fall $Y \subsetneq X$ handelt es sich nicht um einen Unterring mit Eins. **Beachte:** $(\mathcal{P}(Y), \triangle, \cap)$ hat zwar das Einselement Y, dieses ist aber vom Einselement X in $(\mathcal{P}(X), \triangle, \cap)$ verschieden.

(*vi*) Das **Zentrum**[37]

$$Z := \{z \in R \mid a \cdot z = z \cdot a \text{ für alle } a \in R\} \tag{9.4}$$

eines Ringes $(R, +, \cdot)$ ist ein kommutativer Unterring. △

Bemerkung 9.15 („Unterring sein“ ist eine Ordnungsrelation, vgl. Bemerkung 7.46 zu Untergruppen)**.**

(*i*) Die Relation „ist Unterring von“ ist eine partielle Ordnung auf der Klasse aller Ringe.

(*ii*) Insbesondere ist die Menge aller Unterringe eines bestimmten Ringes $(R, +, \cdot)$ durch die Unterringhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein. △

Lemma 9.16 (Durchschnitt von Unterringen, vgl. Lemma 7.47 zu Untergruppen)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(*i*) Ist $(U_i)_{i \in I}$ eine nichtleere Familie von Unterringen von $(R, +, \cdot)$, dann ist auch $\bigcap_{i \in I} U_i$ ein Unterring von R.

(*ii*) Ist $\mathcal{U}$ eine nichtleere Menge von Unterringen von $(R, +, \cdot)$, dann ist auch $\bigcap \mathcal{U}$ ein Unterring von $(R, +, \cdot)$.

Beweis. Der Beweis ist eine einfache Anwendung des Unterringkriteriums (Satz 9.13). □

[37] Das Zentrum eines Ringes besteht also aus denjenigen Elementen, die multiplikativ mit allen Gruppenelementen kommutieren, vgl. Definition (8.10) für das Zentrum einer Gruppe.

Definition 9.17 (Ringhomomorphismus, vgl. Definitionen 8.1, 8.4 und 8.6 für Homomorphismen von Halbgruppen bzw. Monoiden bzw. Gruppen)**.**
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 **Homomorphismus von Ringen** (englisch: ring homomorphism), wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in R_1, \tag{9.5a}$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in R_1. \tag{9.5b}$$

Besitzen beide Ringe ein Einselement 1_{R_1} bzw. 1_{R_2} und gilt zusätzlich

$$f(1_{R_1}) = 1_{R_2}, \tag{9.5c}$$

dann nennen wir f genauer einen **Homomorphismus von Ringen mit Eins** (englisch: homomorphism of rings with unity).

(*ii*) Ist $f\colon R_1 \to R_2$ strukturverträglich und gilt $(R_1, +_1, \cdot_1) = (R_2, +_2, \cdot_2)$, so sprechen wir auch von einem **Endomorphismus eines Ringes** (englisch: ring endomorphism) bzw. von einem **Endomorphismus eines Ringes mit Eins** (englisch: endomorphism of a ring with unity).

(*iii*) Ist $f\colon R_1 \to R_2$ strukturverträglich und bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus von Ringen** bzw. ein **Isomorphismus von Ringen mit Eins** (englisch: isomorphism 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*) Ist $f\colon R_1 \to R_2$ strukturverträglich und bijektiv und gilt $(R_1, +_1, \cdot_1) = (R_2, +_2, \cdot_2)$, so sprechen wir auch von einem **Automorphismus** (englisch: ring automorphism) **eines Ringes** bzw. von einem **Automorphismus eines Ringes mit Eins** (englisch: automorphism of a ring with unity). △

Beachte: Die Beziehung (9.5a) besagt, dass $f\colon (R_1, +_1) \to (R_2, +_2)$ ein Gruppenhomomorphismus ist. Aus Lemma 8.8 folgt damit für die Nullelemente 0_{R_1} bzw. 0_{R_2} notwendigerweise

$$f(0_{R_1}) = 0_{R_2}. \tag{9.6}$$

Weiter bedeutet (9.5b), dass $f\colon (R_1, \cdot_1) \to (R_2, \cdot_2)$ ein Halbgruppenhomomorphismus ist. (9.5b) und (9.5c) zusammen bedeuten, dass $f\colon (R_1, \cdot_1) \to (R_2, \cdot_2)$ ein Monoidhomomorphismus ist.

An Stelle der Bedingung (9.5c) reicht es auch aus, zu fordern, dass $f(1_{R_1})$ invertierbar ist, vgl. (8.3).

Analog zu Satz 8.2 und Folgerung 8.3 gilt:

Satz 9.18 (Komposition von Ringhomomorphismen, Inverse von Ringisomorphismen, vgl. Satz 8.2 zu Halbgruppenhomomorphismen)**.**
Es seien $(R_1, +_1, \cdot_1)$, $(R_2, +_2, \cdot_2)$ und $(R_3, +_3, \cdot_3)$ drei Ringe.

(*i*) Sind $f\colon R_1 \to R_2$ und $g\colon R_2 \to R_3$ Ringhomomorphismen, dann ist auch $g \circ f\colon R_1 \to R_3$ ein Ringhomomorphismus.

(*ii*) Ist $f\colon R_1 \to R_2$ ein Ringisomorphismus, dann ist auch $f^{-1}\colon R_2 \to R_1$ ein Ringisomorphismus.

Analoge Aussagen gelten für Homomorphismen von Ringen mit Eins.

Folgerung 9.19 (Isomorphie von Ringen ist eine Äquivalenzrelation, vgl. Folgerung 8.3 zur Isomorphie von Halbgruppen)**.**
Isomorphie ist eine Äquivalenzrelation auf der Klasse aller Ringe bzw. auf der Klasse aller Ringe mit Eins.

Lemma 9.20 (Ringe mit Eins und Charakteristik 0 enthalten $\mathbb{Z}$)**.**
Es sei $(R, +, \cdot)$ ein Ring mit Eins und $\operatorname{char}(R) = 0$. Dann enthält R einen Unterring, der isomorph zu $\mathbb{Z}$ ist.

Beweis. □

Definition 9.21 (Bild und Kern eines Ringhomomorphismus, vgl. Definition 8.10 von Bild und Kern eines Gruppenhomomorphismus)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe mit den Nullelementen 0_{R_1} bzw. 0_{R_2}. Weiter sei $f\colon R_1 \to R_2$ ein Homomorphismus.

(*i*) Das **Bild** von f ist definiert als

$$\operatorname{Bild}(f) \coloneqq \{f(a_1) \in R_2 \mid a_1 \in R_1\} = f(R_1). \tag{9.7}$$

(*ii*) Der **Kern** von f ist definiert als

$$\operatorname{Kern}(f) \coloneqq \{a_1 \in R_1 \mid f(a_1) = 0_{R_2}\} = f^{-1}(\{0_{R_2}\}). \tag{9.8}$$

△

Lemma 9.22 (Bild und Kern sind Unterringe, vgl. Lemma 8.11 zur Untergruppeneigenschaft von Bild und Kern eines Gruppenhomomorphismus)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe. Weiter sei $f\colon R_1 \to R_2$ ein Homomorphismus. Dann gilt:

(*i*) $\operatorname{Bild}(f)$ ist ein Unterring von $(R_2, +_2, \cdot_2)$.

(*ii*) $\operatorname{Kern}(f)$ ist ein Unterring von $(R_1, +_1, \cdot_1)$.

Beweis. Wir bezeichnen die Nullelemente von R_1 bzw. R_2 mit 0_{R_1} bzw. 0_{R_2}.

Aussage (*i*): Wir überprüfen das Unterringkriterium (Satz 9.13). Es gilt $f(0_{R_1}) = 0_{R_2}$ nach (9.6), also folgt $0_{R_2} \in \operatorname{Bild}(f)$ und $\operatorname{Bild}(f) \neq \emptyset$. Weiter seien a_2, b_2 irgendwelche Elemente in $\operatorname{Bild}(f)$. Wir müssen zeigen: $a_2 -_2 b_2 \in \operatorname{Bild}(f)$ sowie $a_2 \cdot_2 b_2 \in \operatorname{Bild}(f)$.

Nach Definition von $\mathrm{Bild}(f)$ gibt es $a_1, b_1 \in G_1$ mit $f(a_1) = a_2$ und $f(b_1) = b_2$. Daher ist

$$\begin{aligned} a_2 -_2 b_2 &= f(a_1) -_2 (f(b_1)) && \text{nach Voraussetzung} \\ &= f(a_1 -_1 b_1) && \text{nach Lemma 8.8} \end{aligned}$$

und damit $a_2 -_2 b_2 \in \mathrm{Bild}(f)$. Weiterhin gilt

$$\begin{aligned} a_2 \cdot_2 b_2 &= f(a_1) \cdot_2 (f(b_1)) && \text{nach Voraussetzung} \\ &= f(a_1 \cdot_1 b_1) && \text{da } f\colon (R_1, \cdot_1) \to (R_2, \cdot_2) \text{ Halbgruppenhomomorphismus ist} \end{aligned}$$

und damit $a_2 \cdot_2 b_2 \in \mathrm{Bild}(f)$.

Aussage (ii): Wir überprüfen wiederum das Unterringkriterium. Es gilt $f(0_{R_1}) = 0_{R_2}$ nach (9.6), also $0_{R_1} \in \mathrm{Kern}(f)$ und $\mathrm{Kern}(f) \neq \emptyset$. Weiter seien a_1, b_1 irgendwelche Elemente in $\mathrm{Kern}(f)$. Wir müssen zeigen: $a_1 -_1 b_1 \in \mathrm{Kern}(f)$ sowie $a_1 \cdot_1 b_1 \in \mathrm{Kern}(f)$. Es gilt

$$\begin{aligned} f(a_1 -_1 b_1) &= f(a_1) -_2 f(b_1) && \text{nach Lemma 8.8} \\ &= 0_{R_2} -_2 0_{R_2} && \text{da } a_1, b_1 \in \mathrm{Kern}(f) \text{ liegen} \\ &= 0_{R_2} && \text{da } -0_{R_2} = 0_{R_2} \text{ ist} \end{aligned}$$

und damit $a_1 -_1 b_1 \in \mathrm{Kern}(f)$. Weiterhin gilt

$$\begin{aligned} f(a_1 \cdot_1 b_1) &= f(a_1) \cdot_2 f(b_1) && \text{da } f\colon (R_1, \cdot_1) \to (R_2, \cdot_2) \text{ Halbgruppenhomomorphismus ist} \\ &= 0_{R_2} \cdot_2 0_{R_2} && \text{da } a_1, b_1 \in \mathrm{Kern}(f) \text{ liegen} \\ &= 0_{R_2} && \text{nach Lemma 9.3} \end{aligned}$$

und damit $a_1 \cdot_1 b_1 \in \mathrm{Kern}(f)$. □

Beispiel 9.23 (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 8.21 und Beispiel 8.23 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 Übung.

Es gilt

$$\begin{aligned} \mathrm{Bild}(f) &= \mathbb{Z}/m\mathbb{Z}, \\ \mathrm{Kern}(f) &= f^{-1}([0]) = m\mathbb{Z}. \end{aligned}$$

(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 8.23 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 Übung ein Monoidisomorphismus.

Es gilt

$$\begin{aligned} \text{Bild}(f) &= \mathbb{Z}/m\mathbb{Z}, \\ \text{Kern}(f) &= f^{-1}([0]) = \{0\}. \end{aligned}$$ △

Lemma 9.24 (Charakterisierung der Injektivität von Ringhomomorphismen, vgl. Lemma 8.13 für Gruppenhomomorphismen)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe mit den Nullelementen 0_{R_1} bzw. 0_{R_2}. Weiter sei $f\colon R_1 \to R_2$ ein Homomorphismus. Dann sind äquivalent:

(*i*) f ist injektiv.

(*ii*) $\text{Kern}(f) = \{0_{R_1}\}$.

(*iii*) Die einzige Lösung der Gleichung $f(a) = 0_{R_2}$ ist $a = 0_{R_1}$.

Beweis. □

Ende der Vorlesung 13

§ 9.1 Ideale und Faktorringe

Ideale in Ringen sind spezielle Unterringe, die dieselbe Funktion einnehmen wie Normalteiler in Gruppen (§ 8.1). Mit ihrer Hilfe können wir Faktorringe definieren (also „gröbere Versionen“ gegebener Ringe) und einen Homomorphiesatz für Ringe erhalten.

Definition 9.25 (Ideal, vgl. Definition 8.15 von Normalteilern)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(*i*) Eine Teilmenge $J \subseteq R$ heißt ein **Ideal** (englisch: ideal) von $(R, +, \cdot)$, wenn J ein Unterring von R ist und zusätzlich

$$R \cdot J \subseteq J \quad \text{und} \quad J \cdot R \subseteq J \tag{9.9}$$

gilt.[38]

Beachte: Das ist genau dann erfüllt, wenn $(J, +)$ eine Untergruppe von $(R, +)$ ist und (9.9) gilt.

Manchmal notiert man die Eigenschaft, dass $(J, +, \cdot)$ ein Ideal des Ringes $(R, +, \cdot)$ ist, als $(J, +, \cdot) \trianglelefteq (R, +, \cdot)$.

Beachte: Das ist genau dann erfüllt, wenn $(J, +)$ eine Untergruppe von $(R, +)$ ist und wenn (9.9) gilt, denn (9.9) impliziert ja bereits, dass J bzgl. $\cdot$ abgeschlossen ist.

(*ii*) Ein Ideal $(J, +, \cdot)$ von $(R, +, \cdot)$ heißt **echt** (englisch: proper ideal), wenn $J \subsetneq R$ gilt. △

Bemerkung 9.26 (zum Begriff des Ideals)**.**

[38] Ausgeschrieben heißt das also: $a \in R$ und $j \in J$ impliziert $a\,j \in J$ und $j\,a \in J$.

(*i*) In einer Gruppe $(G, \star)$ war die definierende Eigenschaft einer normalen Untergruppe ($a \star N = N \star a$ für alle $a \in G$) genau die Eigenschaft, die wir benötigt haben, um die Gruppenoperation $\star$ in natürlicher Weise auf die Faktormenge G/N zu vererben (Satz 8.21).

Dieselbe Eigenschaft wird man analog auch in Ringen benötigen. Da $(R, +)$ kommutativ ist, muss sie allerdings nicht explizit gefordert werden, da jede Untergruppe von $(R, +)$ bereits ein Normalteiler ist (Beispiel 8.17). Die Bedingung (9.9) bezieht sich daher ausschließlich auf die zweite Verknüpfung $\cdot$.

(*ii*) Es gibt den Begriff des **Ideals** auch bereits in Halbgruppen $(H, \square)$. Damit ist eine Unterhalbgruppe I gemeint, für die $H \square I \subseteq I$ und $I \square H \subseteq I$ gefordert wird. In diesem Sinne ist ein Ideal in einem Ring $(R, +, \cdot)$ also ein Normalteiler der abelschen Gruppe $(R, +)$ und ein Ideal der Halbgruppe $(R, \cdot)$. △

Lemma 9.27 (Kerne von Ringhomomorphismen sind Ideale, vgl. Lemma 8.18 für Kerne von Gruppenhomomorphismen)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe und $f\colon R_1 \to R_2$ ein Homomorphismus. Dann gilt:

(*i*) Die Elemente von R_1, die denselben Funktionswert wie $a \in R_1$ haben, sind genau die Elemente der additiven Nebenklasse von $\operatorname{Kern}(f)$ zu a:

$$f^{-1}(\{f(a)\}) = a + \operatorname{Kern}(f) = \operatorname{Kern}(f) + a.$$

(*ii*) $\operatorname{Kern}(f)$ ist ein Ideal von R_1.

Beweis. Die Aussage (*i*) folgt sofort aus der Aussage (*i*) in Lemma 8.18, da f ja insbesondere ein Gruppenhomomorphismus $f\colon (R_1, +_1) \to (R_2, +_2)$ ist. Außerdem folgt aus Lemma 8.18, dass $\operatorname{Kern}(f) = \{a \in R_1 \mid f(a) = 0_{R_2}\}$ ein Normalteiler von $(R_1, +_1)$ ist, also insbesondere eine Untergruppe.

Zu zeigen bleibt nach Definition 9.25 eines Ideals $R_1 \cdot_1 \operatorname{Kern}(f) \subseteq \operatorname{Kern}(f)$ und $\operatorname{Kern}(f) \cdot_1 R_1 \subseteq \operatorname{Kern}(f)$. Dazu sei nun $a \in R_1$ und $j \in \operatorname{Kern}(f)$, dann gilt

$$f(a \cdot_1 j) = f(a) \cdot_2 f(j) = f(a) \cdot_2 0_{R_2} = 0_{R_2}$$

nach Lemma 9.3 und analog

$$f(j \cdot_1 a) = f(j) \cdot_2 f(a) = 0_{R_2} \cdot_2 f(a) = 0_{R_2}.$$

Also gehören $a \cdot_1 j$ und $j \cdot_1 a$ wieder zu J, kurz: $R_1 \cdot_1 J \subseteq J$ und $J \cdot_1 R_1 \subseteq J$. □

Bemerkung 9.28 (Urbilder von Idealen sind Ideale, vgl. Bemerkung 8.19 zu Urbildern von Normalteilern)**.**
Es gilt sogar folgende Verallgemeinerung von Lemma 9.27: Urbilder von Idealen unter Ringhomomorphismen sind Ideale. △

Beispiel 9.29 (Ideal)**.**

(*i*) In jedem Ring $(R, +, \cdot)$ sind $\{0\}$ (das **Nullideal**, englisch: zero ideal) und R (das **Einsideal**, englisch: unit ideal) Ideale. Diese heißen die **trivialen Ideale** (englisch: trivial ideals).

(*ii*) Die Mengen der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}$ sind genau die Ideale des Ringes $(\mathbb{Z}, +, \cdot)$.

(*iii*) Ist X eine Menge und $Y \subseteq X$, dann ist $(\mathcal{P}(Y), \triangle, \cap)$ ein Ideal von $(\mathcal{P}(X), \triangle, \cap)$. △

In einer Gruppe $(G, \star)$ konnten wir einen Normalteiler N ausfaktorisieren und dabei die Gruppenoperation $\star$ in natürlicher Weise auf die Faktormenge G/N vererben. Dieselbe Konstruktion werden wir jetzt in Ringen durchführen. Aus der Faktormenge R/J (bestehend aus den additiven Nebenklassen von J in $(R, +, \cdot)$) wird damit der **Faktorring** (englisch: factor ring) oder **Quotientenring** (englisch: quotient ring) **von** R **nach** J. Man sagt auch: „Aus dem Ring $(R, +, \cdot)$ wird das Ideal J ausfaktorisiert."

Satz 9.30 (Faktorring, vgl. Satz 8.21 über Faktorgruppen)**.**

(*i*) Es sei $(R, +, \cdot)$ ein Ring und J eines seiner Ideale. Dann gilt:

(a) Auf der Faktormenge

$$R/J = \left\{ [a] = a + J \,\middle|\, a \in R \right\}$$

sind $\tilde{+}$ und $\tilde{\cdot}$, definiert als

$$[a] \mathbin{\tilde{+}} [b] := [a + b] \quad \text{für } a, b \in R, \tag{9.10a}$$

$$[a] \mathbin{\tilde{\cdot}} [b] := [a \cdot b] \quad \text{für } a, b \in R, \tag{9.10b}$$

assoziative Verknüpfungen, bzgl. der $(R/J, \tilde{+}, \tilde{\cdot})$ einen Ring bildet. Das Nullelement ist $[0_R] = J$, und für die additiven Inversen gilt $\tilde{-}[a] = [-a]$.

(b) Die Abbildung

$$\pi : \begin{cases} R \to R/J \\ a \mapsto [a], \end{cases} \tag{9.11}$$

die jedem Element $a \in R$ seine additive Nebenklasse $[a]$ zuordnet, ist ein surjektiver Ringhomomorphismus. Sie heißt die **kanonische Surjektion von** R **auf** R/J. Es gilt $\operatorname{Kern}(\pi) = J$.

(c) Besitzt R das Einselement 1_R, dann besitzt R/J das Einselement $[1_R]$. Ist dann $a \in R$ bzgl. $\cdot$ invertierbar, so ist auch $[a] \in R/J$ bzgl. $\tilde{\cdot}$ invertierbar, und es gilt $[a]^{-1} = [a^{-1}]$.

(d) Wenn $(R, +, \cdot)$ kommutativ ist, dann auch $(R/J, \tilde{+}, \tilde{\cdot})$.

(*ii*) Es sei $(R, +, \cdot)$ ein Ring und U irgendein Unterring. Ist die Verknüpfung (9.10) auf der Menge der Nebenklassen[39] R/U wohldefiniert, dann ist U notwendigerweise ein Ideal von R.

Beweis. Aussage (*i*): Wir zeigen zunächst Aussage (a). Da $(J, +)$ ein Normalteiler der abelschen Gruppe $(R, +)$ ist, folgt aus Satz 8.21 sofort, dass $(R/J, \tilde{+})$ ebenfalls eine abelsche Gruppe ist. Außerdem folgt $[0_R] = J$ und $\tilde{-}[a] = [-a]$. Es bleibt zu zeigen, dass die Multiplikation (9.10b)

[39] Im Unterschied zu Satz 8.21 müssen hier Links- und Rechtsnebenklassen nicht unterschieden werden, da $(R, +)$ ja kommutativ ist.

wohldefiniert und assoziativ ist und dass die Distributivgesetze gelten. Das erfolgt in mehreren Schritten:

Schritt 1: Wir müssen zunächst zeigen, dass $\tilde{\cdot}$ wohldefiniert ist. Dazu seien $a_1, a_2, b_1, b_2 \in R$ gegeben, wobei $[a_1] = [a_2]$ und $[b_1] = [b_2]$ angenommen wird, d. h., $a_1 + J = a_2 + J$ und $b_1 + J = b_2 + J$. Dann gilt

$$\begin{aligned}
[a_2] \mathbin{\tilde{\cdot}} [b_2] &= [a_2 \cdot b_2] && \text{per Definition von } \tilde{\cdot} \\
&= (a_2 \cdot b_2) + J && \text{nach Definition der Äquivalenzklassen} \\
&\subseteq (a_2 + J) \cdot (b_2 + J) && \text{da } 0 \in J \text{ und } J \cdot J \subseteq J \text{ gelten} \\
&= (a_1 + J) \cdot (b_1 + J) && \text{wegen } [a_1] = [a_2] \text{ und } [b_1] = [b_2] \\
&= [a_1] \mathbin{\tilde{\cdot}} [b_1] && \text{nach Definition der Äquivalenzklassen.}
\end{aligned}$$

Da $[a_2] \mathbin{\tilde{\cdot}} [b_2]$ nicht die leere Menge ist, sind also $[a_2] \mathbin{\tilde{\cdot}} [b_2]$ und $[a_1] \mathbin{\tilde{\cdot}} [b_1]$ nicht disjunkt. Da Äquivalenzklassen aber eine Partition bilden, muss bereits $[a_2] \mathbin{\tilde{\cdot}} [b_2] = [a_1] \mathbin{\tilde{\cdot}} [b_1]$ gelten.

Schritt 2: Die Assoziativität von $\tilde{\cdot}$ folgt aus

$$\begin{aligned}
&\big([a] \mathbin{\tilde{\cdot}} [b]\big) \mathbin{\tilde{\cdot}} [c] = [a \cdot b] \mathbin{\tilde{\cdot}} [c] = (a \cdot b + J) \mathbin{\tilde{\cdot}} (c + J) \subseteq (a \cdot b \cdot c) \mathbin{\tilde{+}} J \\
\text{und} \quad &[a] \mathbin{\tilde{\cdot}} \big([b] \mathbin{\tilde{\cdot}} [c]\big) = [a] \mathbin{\tilde{\cdot}} [b \cdot c] = (a + J) \mathbin{\tilde{\cdot}} (b \cdot c + J) \subseteq (a \cdot b \cdot c) \mathbin{\tilde{+}} J.
\end{aligned}$$

Beide Äquivalenzklassen enthalten also das Element $a \cdot b \cdot c$, sind also nicht disjunkt und müssen daher identisch sein.

Schritt 3: Für die Distributivgesetze (9.1) argumentieren wir ähnlich: Die Äquivalenzklassen

$$[a] \mathbin{\tilde{\cdot}} \big([b] \mathbin{\tilde{+}} [c]\big) \quad \text{und} \quad [a] \mathbin{\tilde{\cdot}} [b] \mathbin{\tilde{+}} [a] \mathbin{\tilde{\cdot}} [c]$$

enthalten beide das Element $a \cdot (b + c) = a \cdot b + a \cdot c$, also sind sie nicht disjunkt und damit identisch. Analog enthalten die Äquivalenzklassen

$$\big([a] \mathbin{\tilde{+}} [b]\big) \mathbin{\tilde{\cdot}} [c] \quad \text{und} \quad [a] \mathbin{\tilde{\cdot}} [c] \mathbin{\tilde{+}} [b] \mathbin{\tilde{\cdot}} [c]$$

beide das Element $(a + b) \cdot c = a \cdot c + b \cdot c$, also sind sie nicht disjunkt und damit identisch.

Aussage (b): Wir wissen bereits aus Satz 8.21, dass π ein surjektiver Gruppenhomomorphismus $(R, +) \to (R/J, \tilde{+})$ mit $\operatorname{Kern}(\pi) = J$ ist. Die Strukturverträglichkeit mit der Multiplikation ist gerade die Aussage (9.10b).

Aussage (c): Wir zeigen, dass $[1_R]$ das Einselement von $(R/J, \tilde{\cdot})$ ist. Für beliebiges $a \in R$ enthält die Äquivalenzklasse $[1_R] \mathbin{\tilde{\cdot}} [a]$ das Element a, also gilt $[1_R] \mathbin{\tilde{\cdot}} [a] = [a]$. Auch die Äquivalenzklasse $[a] \mathbin{\tilde{\cdot}} [1_R]$ enthält das Element a, also gilt auch $[a] \mathbin{\tilde{\cdot}} [1_R] = [a]$.

Ist $a \in R$ invertierbar, so zeigen wir nun, dass $[a]^{-1} = [a^{-1}]$ gilt:

$$[a] \mathbin{\tilde{\cdot}} [a^{-1}] = [a \cdot a^{-1}] = [1_R]$$

und analog

$$[a^{-1}] \mathbin{\tilde{\cdot}} [a] = [a^{-1} \cdot a] = [1_R].$$

Aussage (d): Wenn $\cdot$ kommutativ ist, dann gilt

$$[a] \tilde{\cdot} [b] = [a \cdot b] = [b \cdot a] = [b] \tilde{\cdot} [a],$$

also ist auch $\tilde{\cdot}$ kommutativ.

Aussage *(ii)*: Wir wollen zeigen, dass aus der Wohldefiniertheit (9.10b) folgt, dass U ein Ideal ist, dass also $R \cdot U \subseteq U$ und $U \cdot R \subseteq U$ gilt.[40] Dazu seien $a \in R$ und $u \in U$ beliebig. Dann gilt $[u] = U = [0_R]$, und die Wohldefiniertheit liefert

$$[a \cdot u] = [a] \tilde{\cdot} [u] = [a] \tilde{\cdot} [0] = [a \cdot 0] = [0] = U,$$

also $a \cdot u \in U$. Das zeigt $R \cdot U \subseteq U$. Die Aussage $U \cdot R \subseteq U$ folgt analog aus

$$[u \cdot a] = [u] \tilde{\cdot} [a] = [0] \tilde{\cdot} [a] = [0 \cdot a] = [0] = U. \qquad \square$$

Bemerkung 9.31 (Faktorring, vgl. Bemerkung 8.22 zu Faktorgruppen)**.**
Praktisch können wir den Faktorring $(R/J, \tilde{+}, \tilde{\cdot})$ benutzen, um wie im Ring $(R, +, \cdot)$ zu „rechnen“, wobei jedoch Elemente a, b in derselben Äquivalenzklasse (für die also $a - b \in J$ gilt) nicht mehr unterschieden, sondern miteinander identifiziert werden. Der Faktorring $(R/J, \tilde{+}, \tilde{\cdot})$ ist also eine „gröbere Version“ des Ringes $(R, +, \cdot)$. $\triangle$

Beispiel 9.32 (Faktorring, vgl. Beispiel 9.29 zu Idealen)**.**

(i) Für $m \in \mathbb{N}$ ist der Faktorring $\mathbb{Z}/m\mathbb{Z}$ von $(\mathbb{Z}, +, \cdot)$ der in Beispiel 9.6 bereits eingeführte Restklassenring modulo m. Nach Beispiel 9.23 ist dieser isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$, dem Ring von $\mathbb{Z}$ modulo m.

(ii) Ist X eine Menge und $Y \subseteq X$, dann ist der Faktorring $\mathcal{P}(X)/\mathcal{P}(Y)$ von $(\mathcal{P}(X), \triangle, \cap)$ isomorph zu $(\mathcal{P}(X \setminus Y), \triangle, \cap)$. $\triangle$

Bemerkung 9.33 (Ideale sind genau die Kerne von Ringhomomorphismen, vgl. Bemerkung 8.24 für Gruppenhomomorphismen)**.**
Es sei $(R_1, +_1, \cdot_1)$ ein Ring.

(i) Nach Lemma 9.27 ist der Unterring $\operatorname{Kern}(f)$ für jeden beliebigen Ringhomomorphismus $f\colon R_1 \to R_2$ in irgendeinen Ring $(R_2, +_2, \cdot_2)$ immer ein Ideal von $(R_1, +_1, \cdot_1)$.

(ii) Umgekehrt gilt auch, dass jedes Ideal J von $(R_1, +_1, \cdot_1)$ der Kern eines Ringhomomorphismus ist: Dazu wählen wir einfach $R_2 := (R_1/J, \tilde{+}, \tilde{\cdot})$ als Zielring und die kanonische Surjektion $\pi\colon R_1 \to R_1/J$ als Ringhomomorphismus. Dann gilt $\operatorname{Kern}(\pi) = J$. $\triangle$

Lemma 9.34 (Durchschnitt von Idealen, vgl. Lemma 8.20 zu Normalteilern)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(i) Ist $(J_i, +, \cdot)_{i \in I}$ eine nichtleere Familie von Idealen von $(R, +, \cdot)$, dann ist auch $\bigcap_{i \in I} J_i$ ein Ideal von R.

[40] Die Wohldefiniertheit von (9.10a) würde wie im Beweis von Aussage *(ii)* von Satz 8.21 nur die Information liefern, dass $(U, +)$ ein Normalteiler der Gruppe $(R, +)$ ist, was aber wegen der Kommutativität von $(R, +)$ ohnehin klar ist.

(*ii*) Ist $\mathcal{J}$ eine nichtleere Menge von Idealen von $(R,+,\cdot)$, dann ist auch $\bigcap \mathcal{J}$ ein Ideal von $(R,+,\cdot)$.

Beweis. Der Beweis ist Gegenstand der Übung. □

Definition 9.35 (erzeugtes Ideal, Hauptideal)**.**

Es sei $(R,+,\cdot)$ ein Ring und $E \subseteq R$.

(*i*) Dann heißt

$$(E) := \bigcap \{J \mid (J,+,\cdot) \text{ ist Ideal von } (R,+,\cdot) \text{ und } E \subseteq J\} \tag{9.12}$$

das von E **erzeugte Ideal** (englisch: ideal generated by E) in $(R,+,\cdot)$.

(*ii*) Ist speziell $E = \{a\}$ für ein $a \in R$, so schreiben wir auch (a) statt $(\{a\})$ und nennen (a) das **von a erzeugte Hauptideal** (englisch: principal ideal).

(*iii*) Ein Ideal $(J,+,\cdot)$ heißt ein **Hauptideal**, wenn es ein $a \in R$ gibt, sodass $(a) = J$ gilt. △

Satz 9.36 (Darstellung des erzeugten Ideals)**.**

Es sei $(R,+,\cdot)$ ein Ring, $E \subseteq R$ und $a \in R$.

(*i*) Dann gilt für das von E bzw. von a erzeugte Ideal:

$$(E) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; \left(a_i \in E \cup -E \cup RE \cup ER \cup RER\right) \right\}, \tag{9.13a}$$

$$(a) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; \left(a_i \in \{\pm a\} \cup Ra \cup aR \cup RaR\right) \right\}. \tag{9.13b}$$

(*ii*) Ist $(R,+,\cdot)$ ein Ring mit Eins, dann gilt für das von E bzw. von a erzeugte Ideal:

$$(E) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; \left(a_i \in RER\right) \right\}, \tag{9.14a}$$

$$(a) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; \left(a_i \in RaR\right) \right\}. \tag{9.14b}$$

Insbesondere ist $(1) = R$.

(*iii*) Ist $(R,+,\cdot)$ ein kommutativer Ring, dann gilt für das von E bzw. von a erzeugte Ideal:

$$(E) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; \left(a_i \in E \cup -E \cup RE\right) \right\}, \tag{9.15a}$$

$$(a) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1,\dots,n \; \left(a_i \in \{\pm a\} \cup Ra\right) \right\}. \tag{9.15b}$$

(*iv*) Ist $(R, +, \cdot)$ ein kommutativer Ring mit Eins, dann gilt für das von E bzw. von a erzeugte Ideal:

$$(E) = \left\{ \sum_{i=1}^{n} a_i \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1, \dots, n \; \left(a_i \in R\, E\right) \right\}, \tag{9.16a}$$

$$(a) = R\, a. \tag{9.16b}$$

Insbesondere ist $(1) = R$.

In jedem Fall gilt $(\emptyset) = (0_R) = \{0_R\}$.

Beweis. Der Beweis ist Gegenstand der Übung. □

Beispiel 9.37 (erzeugtes Ideal, vgl. Beispiel 7.51 zu erzeugten Untergruppen)**.**

(*i*) Der **Kommutator** der Elemente a, b eines Ringes $(R, +, \cdot)$ ist definiert als

$$[a, b] \coloneqq a \cdot b - b \cdot a. \tag{9.17}$$

Beachte: Im Unterschied zum Kommutator zweier Elemente in einer Gruppe (8.11) werden hier beide Verknüpfungen zur Definition verwendet. Es gilt aber auch hier wieder, dass a und b genau dann (bzgl. $\cdot$) kommutieren, wenn der Kommutator das neutrale Element (bzgl. $+$) ergibt, wenn also $[a, b] = 0$ gilt. (**Quizfrage 9.6:** Klar?)

Das **Kommutatorideal** (englisch: commutator ideal) eines Ringes $(R, +, \cdot)$ ist das von Kommutatoren von R erzeugte Ideal[41], also

$$\left(\left\{[a, b] \,\middle|\, a, b \in R\right\}\right). \tag{9.18}$$

Es wird kurz auch in der Form $\big([R, R]\big)$ oder (ungenau) als $[R, R]$ notiert.

Ist $(R, +, \cdot)$ ein beliebiger Ring und K sein Kommutatorideal, dann ist der Faktorring $(R/K, \tilde{+}, \tilde{\cdot})$ kommutativ.

Tatsächlich ist $(R/J, \tilde{+}, \tilde{\cdot})$ genau dann kommutativ, wenn das ausfaktorisierte Ideal J das Kommutatorideal von R enthält.

(*ii*) Das Zentrum eines Ringes (Beispiel 9.14) ist i. A. kein Ideal. △

§ 9.2 Der Homomorphiesatz für Ringe

Analog zum Homomorphiesatz für Gruppen Satz 8.25 gibt es einen Homomorphiesatz für Ringe. Er besagt wiederum, dass ein Ringhomomorphismus $f : R_1 \to R_2$ „nebenklassenweise“ wirkt. Er bildet eine gesamte Nebenklasse von $\operatorname{Kern}(f)$ auf ein- und dasselbe Element von R_2 ab und verschiedene Nebenklassen auf verschiedene Elemente. Das geschieht zudem strukturverträglich. Dadurch ist das $\operatorname{Bild}(f)$ eines solchen Ringhomomorphismus bereits im Wesentlichen (d. h. bis auf Isomorphie) festgelegt ist durch $(R_1, +, \cdot)$ und das Ideal $\operatorname{Kern}(f)$.

[41] **Beachte:** Die Kommutatoruntergruppe einer Gruppe (Beispiel 8.17) wurde als die von den Kommutatoren erzeugte Untergruppe definiert, und die Normalteilereigenschaft konnte gezeigt werden. Im Unterschied dazu reicht es hier nicht aus, den von den Kommutatoren erzeugten Unterring zu betrachten, weil dieser i. A. kein Ideal ist.

Satz 9.38 (**Homomorphiesatz für Ringe**[42], vgl. Satz 8.25 für Gruppen)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe. Weiter sei $f\colon R_1 \to R_2$ ein Homomorphismus. Dann gilt

$$R_1 / \operatorname{Kern}(f) \cong \operatorname{Bild}(f) \tag{9.19a}$$

mit dem Isomorphismus

$$I([a]) \coloneqq f(a) \quad \text{für } [a] = a +_1 \operatorname{Kern}(f) \in R_1 / \operatorname{Kern}(f). \tag{9.19b}$$

Beweis. Der Ringhomomorphismus f ist insbesondere auch ein Gruppenhomomorphismus $f\colon (R_1, +_1) \to (R_2, +_2)$. Aus Satz 8.25 folgt daher, dass I ein Isomorphismus der Gruppen $(R_1 / \operatorname{Kern}(f), \tilde{+}_1)$ und $(\operatorname{Bild}(f), +_2)$ ist. Es bleibt zu zeigen, dass I auch ein Ringisomorphismus, also verträglich mit der Multiplikation ist. Dazu seien $a, b \in R_1$ beliebig, dann gilt:

$$\begin{aligned}
I([a] \tilde{\cdot}_1 [b]) &= I([a] \cdot_1 [b]) && \text{per Definition von } \tilde{\cdot}_1 \\
&= f(a \cdot_1 b) && \text{nach Definition von } I \\
&= f(a) \cdot_2 f(b) && \text{da } f \text{ ein Ringhomomorphismus ist} \\
&= I([a]) \cdot_2 I([b]) && \text{nach Definition von } I.
\end{aligned}$$

□

§ 10 Körper

Literatur: Beutelspacher, 2014, Kapitel 2; Bosch, 2014, Kapitel 1.3; Fischer, Springborn, 2020, Kapitel 2.3; Deiser, 2024b, 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 ·. Im Unterschied zu einem kommutativen Ring (wie etwa $\mathbb{Z}$) wird nun aber zusätzlich noch gefordert, dass alle Elemente (außer dem Nullelement) multiplikativ invertierbar sind:

Definition 10.1 (Körper)**.**
Ein **Körper** (englisch: field) $(K, +, \cdot)$ ist ein kommutativer Ring $(K, +, \cdot)$ mit der zusätzlichen Eigenschaft, dass $(K \setminus \{0_K\}, \cdot)$ eine abelsche Gruppe ist.[43] △

Da eine Gruppe nicht leer sein kann, besitzt ein Körper neben dem Nullelement 0_K mindestens noch ein weiteres Element, nämlich das multiplikativ neutrale Einselement $1_K \neq 0_K$. Anders gesagt ist ein Körper also ein kommutativer Ring mit Eins ungleich einem Nullring, in dem jedes Element außer dem Nullelement ein multiplikatives Inverses besitzt. (**Quizfrage 10.1:** Warum wird das Nullelement ausgenommen?)

Ausgeschrieben ist eine Menge mit zwei (inneren) Verknüpfungen + („Addition“) und · („Multiplikation“) also genau dann ein Körper, wenn gilt:

[42] englisch: fundamental theorem on ring homomorphisms

[43] Oft wird $K \setminus \{0_K\}$ in der Literatur als K^* oder als $K^\times$ abgekürzt. Wir verwenden diese Bezeichnungen jedoch hier nicht.

(*i*) $(K, +)$ ist eine abelsche Gruppe.
(Das Nullelement bezeichnen wir mit 0_K.)

(*ii*) $(K, \cdot)$ ist ein abelsches Monoid mit Einselement $1_K \neq 0_K$, in dem alle Elemente außer 0_K invertierbar sind.

(*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 $a, b, c \in K$.[44]

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 7.22 mit den Verknüpfungstafeln aus Beispiel 7.2 ist ein Körper mit dem Nullelement 0 und dem Einselement 1. $\mathbb{Z}_2$ ist also der (bis auf Isomorphie eindeutige) kleinstmögliche Körper.

(*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, aber auch nicht multiplikativ invertierbar ist, denn es gilt $[2] \tilde{\cdot} [a] \neq [1]$ für alle $a \in \mathbb{Z}$.

(*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 (Beispiel 7.4), Monoid (Beispiel 7.8), Gruppe (Beispiel 7.22) oder Ring (Beispiel 9.2) 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 10.2:** Woran liegt das?) △

Satz 10.3 (Körper und Integritätsringe)**.**

(*i*) Jeder Körper $(K, +, \cdot)$ ist ein Integritätsring.[45]

(*ii*) Jeder endliche Integritätsring $(R, +, \cdot)$ ist ein Körper.

Beachte: Wie das Beispiel $\mathbb{Z}$ zeigt, sind unendliche Integritätsringe i. A. keine Körper.

Beweis. Aussage (*i*): Nach Definition 10.1 ist $(K, +, \cdot)$ ein kommutativer Ring mit dem Nullelement 0_K und dem Einselement $1_K \neq 0_K$. Insbesondere ist also K kein Nullring. Es bleibt zu zeigen, dass $(K, +, \cdot)$ nullteilerfrei ist. Es seien dazu $a, b \in K$ mit $a \cdot b = 0_K$. Wenn $a \neq 0_K$ ist, dann ist a als Element der Gruppe $(K \setminus \{0_K\})$ invertierbar, also gilt $b = a^{-1} \cdot 0_K = 0_K$. Ist dagegen $b \neq 0_K$, dann ist b invertierbar, und es folgt $a = 0_K \cdot b^{-1} = 0_K$. Das heißt, $(K, +, \cdot)$ ist nullteilerfrei.

Aussage (*ii*): Es sei $(R, +, \cdot)$ ein Integritätsring, also ein kommutativer, nullteilerfreier Ring mit dem Einselement 1_R ungleich einem Nullring. Wir wissen also bereits: $(R, +)$ ist eine abelsche

[44] Wie bereits in kommutativen Ringen fallen die beiden Distributivgesetze (10.1a) und (10.1b) zusammen. Es reicht also, eines von beiden zu prüfen.

[45] also ein kommutativer, nullteilerfreier Ring mit Eins ungleich einem Nullring, siehe Definition 9.7

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 (9.3) 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 7.25. 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 6.35, dass $\cdot_a$ auch surjektiv ist.

Ein analoges Argument zeigt, dass auch alle Linkstranslationen auf $R \setminus \{0\}$ surjektiv sind. Aus dem Gruppenkriterium Lemma 7.25 folgt nun, dass $(R \setminus \{0\}, \cdot)$ eine Gruppe ist. □

Folgerung 10.4 (Körpereigenschaft des Restklassenringes $\mathbb{Z}/m\mathbb{Z}$ und des Ringes $\mathbb{Z}_m$ von $\mathbb{Z}$ modulo m, vgl. Satz 9.11 zur Nullteilerfreiheit)**.**
Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ sowie der zu ihm isomorphe Ring (Beispiel 9.23) 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 9.11 haben wir gezeigt, dass $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ genau dann ein Integritätsring ist, wenn $m \in \mathbb{N}$ eine Primzahl ist. Da aber $\mathbb{Z}/m\mathbb{Z}$ nur endlich viele (nämlich m) Elemente hat, ist Integritätsring zu sein gleichbedeutend mit der Körpereigenschaft. Nach Beispiel 9.23 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 $(\mathbb{Z}_m, +_m, \cdot_m)$. □

Bemerkung 10.5 (Charakteristik von Körpern)**.**
Die Definition 9.4 der Charakteristik eines Ringes wird auch auf Körper angewendet. Für Körper ist die Charakteristik nach Lemma 9.10 also entweder 0 oder eine Primzahl.

Für die Körper aus Beispiel 10.2 gilt $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$ und $\operatorname{char}(\mathbb{Z}_2) = 2$. Für die Körper $\mathbb{Z}/m\mathbb{Z}$ und $\mathbb{Z}_m$ mit $m \in \mathbb{N}$ prim gilt $\operatorname{char}(\mathbb{Z}/m\mathbb{Z}) = \operatorname{char}(\mathbb{Z}_m) = m$, vgl. Beispiel 9.5. △

Definition 10.6 (Unterkörper, vgl. Definition 9.12 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. $\cdot$ abgeschlossen und wenn $(U, +, \cdot)$ selbst wieder ein Körper ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, +)$ eine Untergruppe von $(K, +)$ 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. △

Beachte: Insbesondere folgt aus Lemma 7.43, dass das Nullelement 0_K von K notwendigerweise auch das Nullelement des Unterkörpers ist, und ebenso, dass das Einselement 1_K auch das Einselement des Unterkörpers ist.

Die Prüfung einer Teilmenge $U \subseteq K$ auf die Unterkörper-Eigenschaft lässt sich mit folgendem Kriterium erreichen:

Satz 10.7 (Unterkörperkriterium, vgl. Unterringkriterium Satz 9.13)**.**
Es sei $(K, +, \cdot)$ ein Körper und $U \subseteq K$. Dann sind äquivalent:

(*i*) $(U, +, \cdot)$ ist ein Unterkörper von $(K, +, \cdot)$.

(*ii*) U besitzt mindestens zwei Elemente, und für alle $a, b \in U$ gilt $a - b \in U$ sowie $a \cdot b^{-1} \in U$, sofern $b \neq 0_K$ ist.[46]

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $(U, +, \cdot)$ ein Unterkörper von $(K, +, \cdot)$. Dann enthält U notwendigerweise das Nullelement 0_K von $(K, +, \cdot)$, also das neutrale Element der Untergruppe $(U, +)$ von $(K, +)$. Für $a, b \in U$ gilt $-b \in U$ nach Lemma 7.43. Da U bzgl. $+$ abgeschlossen ist, folgt $a - b = a + (-b) \in U$. Analog gilt nach Lemma 7.43 auch $b^{-1} \in U$ für $b \neq 0_K$, und da U bzgl. $\cdot$ abgeschlossen ist, folgt $a \cdot b^{-1} \in U$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Nach Voraussetzung erfüllt $(U, +)$ das Untergruppenkriterium (Satz 7.44), also ist $(U, +)$ eine Untergruppe von $(K, +)$. Zudem erfüllt $(U \setminus \{0_K\}, \cdot)$ nach Voraussetzung ebenfalls das Untergruppenkriterium, also ist $(U \setminus \{0_K\}, \cdot)$ eine Untergruppe von $(K \setminus \{0_K\}, \cdot)$. Damit ist $(U, +, \cdot)$ ein Unterkörper von $(K, +, \cdot)$. □

Beispiel 10.8 (Unterkörper)**.**

(*i*) $(\mathbb{Q}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{R}, +, \cdot)$, und $(\mathbb{R}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{C}, +, \cdot)$.

(*ii*) Der Restklassenkörper $\mathbb{Z}/m\mathbb{Z}$ (mit $m \in \mathbb{N}$ prim) und der zu ihm isomorphe Körper $\mathbb{Z}_m$ besitzen keine echten Unterkörper. (**Quizfrage 10.3:** Wie sieht man das?) △

Bemerkung 10.9 („Unterkörper sein“ ist eine Ordnungsrelation, vgl. Bemerkung 9.15 zu Unterringen)**.**

(*i*) Die Relation „ist Unterkörper von“ ist eine partielle Ordnung auf der Klasse aller Körper.

(*ii*) Insbesondere ist die Menge aller Unterkörper eines bestimmten Körpers $(K, +, \cdot)$ durch die Unterkörperhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein. △

Lemma 10.10 (Durchschnitt von Unterkörpern, vgl. Lemma 9.16 zu Unterringen)**.**
Es sei $(K, +, \cdot)$ ein Körper.

(*i*) Ist $(U_i, +, \cdot)_{i \in I}$ eine nichtleere Familie von Unterkörpern von $(K, +, \cdot)$, dann ist auch $\bigcap_{i \in I} U_i$ ein Unterkörper von $(K, +, \cdot)$.

(*ii*) Ist $\mathcal{U}$ eine nichtleere Menge von Unterkörpern von $(K, +, \cdot)$, dann ist auch $\bigcap \mathcal{U}$ ein Unterkörper von $(K, +, \cdot)$.

[46] kurz: $U - U \subseteq U$ und $U \cdot (U \setminus \{0_K\})^{-1} \subseteq U$

Beweis. Der Beweis ist eine einfache Anwendung des Unterkörperkriteriums (Satz 10.7). □

Definition 10.11 (Körperhomomorphismus, vgl. Definition 9.17 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 **(Homomorphismus von Körpern** (englisch: field homomorphism), wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in K_1, \tag{10.2a}$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in K_1, \tag{10.2b}$$
$$f(1_{K_1}) = 1_{K_2}. \tag{10.2c}$$

(*ii*) Ist $f\colon K_1 \to K_2$ strukturverträglich und gilt $(K_1, +_1, \cdot_1) = (K_2, +_2, \cdot_2)$, so sprechen wir auch von einem **Endomorphismus eines Körpers** (englisch: field endomorphism).

(*iii*) Ist $f\colon K_1 \to K_2$ strukturverträglich und bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus von Körpern** (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*) Ist $f\colon K_1 \to K_2$ strukturverträglich und bijektiv und gilt $(K_1, +_1, \cdot_1) = (K_2, +_2, \cdot_2)$, so sprechen wir auch von einem **Automorphismus eines Körpers** (englisch: field automorphism). △

Da die Bedingungen (10.2) mit denen aus (9.5) übereinstimmen, ist ein Körperhomomorphismus nichts anderes als ein Homomorphismus von Ringen mit Eins, der speziell zwischen Körpern eingesetzt wird. Insbesondere haben wir auch hier wie in (9.6) wieder

$$f(0_{K_1}) = 0_{K_2}. \tag{10.3}$$

An Stelle der Bedingung (10.2c) reicht es auch aus, zu fordern, dass $f(1_{K_1}) \neq 0_{K_2}$ gilt, denn daraus ergibt sich notwendig $f(1_{K_1}) = 1_{K_2}$, vgl. (8.3). (**Quizfrage 10.4:** Wie nämlich?)

Auch für Körper gilt analog zu Satz 9.18 und Folgerung 9.19:

Satz 10.12 (Komposition von Körperhomomorphismen, Inverse von Körperisomorphismen, vgl. Satz 9.18 zu Ringhomomorphismen)**.**
Es seien $(K_1, +_1, \cdot_1)$, $(K_2, +_2, \cdot_2)$ und $(K_3, +_3, \cdot_3)$ drei Körper.

(*i*) Sind $f\colon K_1 \to K_2$ und $g\colon K_2 \to K_3$ Körperhomomorphismen, dann ist auch $g \circ f\colon K_1 \to K_3$ ein Körperhomomorphismus.

(*ii*) Ist $f\colon K_1 \to K_2$ ein Körperisomorphismus, dann ist auch $f^{-1}\colon K_2 \to K_1$ ein Körperisomorphismus.

Folgerung 10.13 (Isomorphie von Körpern ist eine Äquivalenzrelation, vgl. Folgerung 9.19 zur Isomorphie von Ringen)**.**
Isomorphie ist eine Äquivalenzrelation auf der Klasse aller Körper.

Im Unterschied zu Homomorphismen anderer algebraischer Strukturen sind Körperhomomorphismen immer injektiv:

Lemma 10.14 (Körperhomomorphismen sind injektiv)**.**
Es seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ zwei Körper und $f\colon K_1 \to \mathbb{K}_2$ ein Homomorphismus. Dann ist f injektiv.

Beweis. Wir nehmen $a \neq b$, aber $f(a) = f(b)$ an. Dann ergibt sich der Widerspruch

$$\begin{aligned}
1_{K_2} &= f(1_{K_1}) && \text{wegen (10.2c)}\\
&= f\big((a -_1 b)^{-1} \cdot_1 (a -_1 b)\big) && \text{da } a -_1 b \neq 0_{K_1} \text{ vorausgesetzt wurde}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 f\big(a -_1 b\big) && \text{wegen (10.2a)}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 \big(f(a) -_2 f(b)\big) && \text{wegen (10.2b)}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 0_{K_2} && \text{da } f(a) = f(b) \text{ vorausgesetzt wurde}\\
&= 0_{K_2} && \text{nach Lemma 9.3.}
\end{aligned}$$

□

Beispiel 10.15 (Körperhomomorphismen)**.**

(*i*) Die Einbettungen $(\mathbb{Q}, +, \cdot) \ni x \mapsto x \in (\mathbb{R}, +, \cdot)$ und $(\mathbb{R}, +, \cdot) \ni x \mapsto x \in (\mathbb{C}, +, \cdot)$ sind Körperhomomorphismen.

(*ii*) Der Körper der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$ besitzt außer der Identität keine weiteren Körperautomorphismen.

(*iii*) Auch der Körper der rellen Zahlen $(\mathbb{R}, +, \cdot)$ besitzt außer der Identität keine weiteren Körperautomorphismen.

(*iv*) Die komplexe Konjugation $(\mathbb{C}, +, \cdot) \ni x \mapsto \overline{x} \in (\mathbb{C}, +, \cdot)$ ist ein Körperautomorphismus.

(*v*) Realteil $(\mathbb{C}, +, \cdot) \ni x \mapsto \operatorname{Re} x \in (\mathbb{R}, +, \cdot)$ und Imaginärteil $(\mathbb{C}, +, \cdot) \ni x \mapsto \operatorname{Im} x \in (\mathbb{R}, +, \cdot)$ sind keine Körperhomomorphismen, da sie nicht injektiv sind. △

Lemma 10.16 (Körper mit Charakteristik 0 enthalten $\mathbb{Q}$, vgl. Lemma 9.20 für Ringe mit Eins)**.**
Es sei $(K, +, \cdot)$ ein Körper mit $\operatorname{char}(K) = 0$. Dann enthält K einen Unterkörper, der isomorph zu $\mathbb{Q}$ ist.

Beweis. □

Definition 10.17 (Bild und Kern eines Körperhomomorphismus, vgl. Definition 9.21 von Bild und Kern eines Ringhomomorphismus)**.**
Es seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ Körper mit den Nullelementen 0_{K_1} bzw. 0_{K_2}. Weiter sei $f\colon K_1 \to K_2$ ein Homomorphismus.

(*i*) Das **Bild** von f ist definiert als

$$\operatorname{Bild}(f) := \{f(a_1) \in K_2 \mid a_1 \in K_1\} = f(K_1). \tag{10.4}$$

(*ii*) Der **Kern** von f ist definiert als

$$\operatorname{Kern}(f) \coloneqq \{a_1 \in K_1 \mid f(a_1) = 0_{K_2}\} = f^{-1}(\{0_{K_2}\}) \tag{10.5}$$

△

Analog zu Lemma 9.22 gilt auch bei Körperhomomorphismen wieder, dass das Bild eines Körperhomomorphismus $f\colon K_1 \to K_2$ ein Unterkörper von K_2 ist. (**Quizfrage 10.5:** Beweis?) Der Kern eines Körperhomomorphismus eines Körperhomomorphismus $f\colon K_1 \to K_2$ ist dagegen niemals ein Unterkörper von K_2, da aufgrund der Injektivität von f notwendigerweise $\operatorname{Kern}(f) = \{0_{K_1}\}$ gilt, ein Unterkörper aber mindestens zwei Elemente hat.

Bemerkung 10.18 (Ausfaktorisieren bei Körpern)**.**
Wir hatten in § 8.1 durch Ausfaktorisieren einer normalen Untergruppe eines Gruppe auf der Faktormenge wieder eine Gruppenstruktur erhalten. Analog konnten wir in § 9.1 ein Ideal aus einem Ring ausfaktorisieren und haben auf der Faktormenge eine Ringstruktur erhalten. Diese Idee funktioniert bei Körpern aber nicht. Würden wir für einen Körper K und einen Unterkörper U versuchen, wie in (9.10) die Faktorverknüpfungen $\tilde{+}$ und $\tilde{\cdot}$ einzuführen in der Hoffnung, auf der Faktormenge K/U wieder eine Körperstruktur zu bekommen, dann könnten wir gleichzeitig K auch als Ring betrachten und würden insbesondere auf K/U auch eine Ringstruktur bekommen. Nach Satz 9.30 wird das aber nur dann passieren, wenn U ein Ideal des Ringes K ist. Man kann jedoch zeigen, dass es in einem Körper nur die beiden trivialen Ideale $U_1 = \{0\}$ und $U_2 = K$ gibt. U_1 ist aber kein Unterkörper von K (da einelementig), und K/U_2 besteht nur aus einem einzigen Element (Nebenklasse), worauf sich keine Körperstruktur definieren lässt. △

Abschließend kombinieren wir noch die Begriffe Körper und Ordnungsrelation, was uns zum Begriff des **geordneten Körpers** führt. Dabei handelt es sich um einen Körper mit einer Totalordnung, die in gewissem Sinne mit den Verknüpfungen der Körpers verträglich ist. Das Nullelement spielt dabei eine besondere Rolle:

Definition 10.19 (geordneter Körper)**.**
Es seien $(K, +, \cdot)$ ein Körper mit dem Nullelement 0_K und $\leqslant$ eine Totalordnung auf K.

(*i*) Der Körper heißt **geordnet** (englisch: ordered field) bzgl. der Totalordnung $\leqslant$, wenn

$$\alpha \leqslant \beta \quad \Rightarrow \quad \alpha + \gamma \leqslant \beta + \gamma \tag{10.6a}$$

$$\alpha \geqslant 0_K \text{ und } \beta \geqslant 0_K \quad \Rightarrow \quad \alpha \cdot \beta \geqslant 0_K \tag{10.6b}$$

für alle $\alpha, \beta, \gamma \in K$ gilt.

(*ii*) $\alpha \in K$ heißt **nichtnegativ**, wenn $\alpha \geqslant 0_K$ ist.

(*iii*) $\alpha \in K$ heißt **positiv**, wenn $\alpha \geqslant 0_K$ und $\alpha \neq 0_K$ ist.

(*iv*) $\alpha \in K$ heißt **nichtpositiv**, wenn $\alpha \leqslant 0_K$ ist.

(*v*) $\alpha \in K$ heißt **negativ**, wenn $\alpha \leqslant 0_K$ und $\alpha \neq 0_K$ ist. △

Lemma 10.20 (Rechenregeln in geordneten Körpern).
Es sei $(K, +, \cdot)$ mit der Totalordnung $\leqslant$ ein geordneter Körper. Dann gilt für $\alpha, \beta, \gamma, \delta \in K$:

(i) $\alpha \geqslant 0_K \quad \Leftrightarrow \quad -\alpha \leqslant 0_K$

(ii) $\alpha \leqslant \beta$ und $\gamma \leqslant \delta \quad \Rightarrow \quad \alpha + \gamma \leqslant \beta + \delta$

(iii) $\alpha \leqslant \beta$ und $\gamma \geqslant 0_K \quad \Rightarrow \quad \alpha \cdot \gamma \leqslant \beta \cdot \gamma$

(iv) $\alpha \leqslant \beta$ und $\gamma \leqslant 0_K \quad \Rightarrow \quad \beta \cdot \gamma \leqslant \alpha \cdot \gamma$

(v) $\alpha^2 \geqslant 0_K$

(vi) $\alpha \neq 0_K \quad \Rightarrow \quad \alpha^2 > 0_K$. Insbesondere gilt $1_K > 0_K$.

(vii) $\alpha > 0_K \quad \Rightarrow \quad \alpha^{-1} > 0_K$

$(viii)$ $\beta > \alpha > 0_K \quad \Rightarrow \quad \alpha^{-1} > \beta^{-1} > 0_K$

(ix) $n\,1_K > 0_K$ für alle $n \in \mathbb{N}$. Insbesondere gilt notwendigerweise $\operatorname{char}(K) = 0_K$.

Beweis. Aussage (i):

$$\begin{aligned} & \alpha \geqslant 0_K \quad \Rightarrow \quad 0_K = \alpha + (-\alpha) \geqslant 0_K + (-\alpha) = -\alpha \\ \text{und} \quad & -\alpha \leqslant 0_K \quad \Rightarrow \quad 0_K = -\alpha + \alpha \leqslant 0_K + \alpha = \alpha. \end{aligned}$$

Aussage (ii):

$$\begin{aligned} & \alpha \leqslant \beta \quad \Rightarrow \quad \alpha + \gamma \leqslant \beta + \gamma \\ \text{und} \quad & \gamma \leqslant \delta \quad \Rightarrow \quad \beta + \gamma \leqslant \beta + \delta. \end{aligned}$$

Die Transitivität der Ordnung zeigt, dass dann auch $\alpha + \gamma \leqslant \beta + \delta$ gilt.

Aussage (iii):

$$\begin{aligned} & \alpha \leqslant \beta \\ \Rightarrow \quad & 0_K \leqslant \beta - \alpha \\ \Rightarrow \quad & 0_K \leqslant (\beta - \alpha) \cdot \gamma \qquad \text{wegen } \gamma \geqslant 0_k \\ \Rightarrow \quad & 0_K \leqslant \beta \cdot \gamma - \alpha \cdot \gamma \qquad \text{wegen des Distributivgesetzes (10.1b)} \\ \Rightarrow \quad & \alpha \cdot \gamma \leqslant \beta \cdot \gamma. \end{aligned}$$

Aussage (iv): Aus $\gamma \leqslant 0_K$ folgt $-\gamma \geqslant 0_K$ nach Aussage (i). Weiter folgt mit Aussage (iii) dann $\alpha \cdot (-\gamma) \leqslant \beta \cdot (-\gamma)$, also $\beta \cdot \gamma \leqslant \alpha \cdot \gamma$.

Aussage (v): Nehmen wir zunächst $\alpha \geqslant 0_K$ an. Es folgt $\alpha^2 = \alpha \cdot \alpha \geqslant 0_K$. Im Fall $\alpha \leqslant 0_K$ ist $-\alpha \geqslant 0_K$. Es folgt $\alpha^2 = (-\alpha) \cdot (-\alpha) \geqslant 0_K$.

Aussage (vi): Die Behauptung folgt aus der Nullteilerfreiheit des Körpers K (Satz 10.3). Die Wahl $\alpha = 1_K$ zeigt $\alpha^2 = 1_K \cdot 1_K = 1_K > 0_K$.

Aussage (vii): Wegen $\alpha > 0_K$ ist $\alpha \neq 0_K$, also multiplikativ invertierbar. Das Inverse α^{-1} ist ebenfalls $\neq 0_K$. Die Annahme $\alpha^{-1} < 0_K$ würde $1_K = \alpha \cdot \alpha^{-1} < 0_K$ ergeben. Andererseits ist aber $1_K > 0_K$ nach Aussage (vi), Widerspruch. Also muss $\alpha^{-1} > 0_K$ gelten.

Aussage (*viii*):

$$\begin{aligned} & \beta > \alpha > 0_K \\ \Rightarrow \quad & 1_K > \alpha \cdot \beta^{-1} > 0_K \quad \text{wegen } \beta^{-1} > 0_K \text{ nach Aussage (vii)} \\ \Rightarrow \quad & \alpha^{-1} > \beta^{-1} > 0_K \quad \text{wegen } \alpha^{-1} > 0_K \text{ nach Aussage (vii)} \end{aligned}$$

Aussage (*ix*): Aus Aussage (*vi*) folgt $1_K > 0_K$. Es folgt weiter $1_K + 1_K > 1_K + 0_K = 1_K > 0_K$. Induktiv zeigt man $n\,1_K > 0_K$ für alle $n \in \mathbb{N}$. Folglich ist $n\,1_K \neq 0_K$ für all $n \in \mathbb{N}$, d. h., $\operatorname{char}(K) = 0_K$. □

Beispiel 10.21 (geordneter Körper)**.**

(*i*) Die rationalen Zahlen $\mathbb{Q}$ mit der bekannten Totalordnung bilden einen geordneten Körper.

(*ii*) Die reellen Zahlen $\mathbb{R}$ mit der bekannten Totalordnung bilden einen geordneten Körper.

(*iii*) Die komplexen Zahlen $\mathbb{C}$ sind mit keiner Totalordnung ein geordneter Körper, da $i^2 = -1$ der Aussage (*vi*) aus Lemma 10.20 widerspricht. △

Quizfrage 10.6: Wie würden Sie den Begriff **geordneter Ring** definieren? Welche der Eigenschaften aus Lemma 10.20 gelten noch, welche nicht?

Quizfrage 10.7: Ist auch der Begriff der **geordneten Gruppe** sinnvoll? Wie sieht die Definition aus, und welche Eigenschaften gelten?

Ende der Vorlesung 14

Ende der Woche 7

Kapitel 3 Vektorräume

§ 11 Vektorräume

Literatur: Beutelspacher, 2014, Kapitel 3; Bosch, 2014, Kapitel 1; Fischer, Springborn, 2020, Kapitel 2.4–2.6; Jänich, 2008, Kapitel 2

Vektorräume sind die zentralen Strukturen in der *linearen* Algebra. Zu einem Vektorraum V gehört immer ein zugrundeliegender Körper $(K, +, \cdot)$. In Anlehnung an dessen Verknüpfungen bezeichnen wir die beiden Verknüpfungen im Vektorraum V vorübergehend mit $\oplus$ und $\odot$.

Definition 11.1 (Vektorraum)**.**
Es sei $(K, +, \cdot)$ ein Körper. Ein **Vektorraum** (englisch: vector space) oder **linearer Raum** (englisch: linear space) $(V, \oplus, \odot)$ **über dem Körper** 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, genannt der **Nullvektor** (englisch: zero vector).

(*ii*) Für die Verknüpfung $\odot$, genannt **S-Multiplikation**[1] (englisch: S-multiplication) oder **skalare Multiplikation** (englisch: scalar multiplication), gelten die folgenden Gesetze für alle $\alpha, \beta \in K$ und $u, v \in V$: das **„gemischte" Assoziativgesetz** (englisch: „mixed" associative law)

$$(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v) \tag{11.1a}$$

sowie die **„gemischten" Distributivgesetze**[2] (englisch: „mixed" distributive laws)

$$\alpha \odot (u \oplus v) = (\alpha \odot u) \oplus (\alpha \odot v) \tag{11.1b}$$
$$(\alpha + \beta) \odot v = (\alpha \odot v) \oplus (\beta \odot v). \tag{11.1c}$$

Weiterhin ist das neutrale Element 1_K bzgl. der Multiplikation $\cdot$ im Körper K auch neutral bzgl. der S-Multiplikation $\odot$:

$$1_K \odot v = v. \tag{11.1d}$$

In einem K-Vektorraum V heißen die Elemente von V auch **Vektoren** (englisch: vectors). Die Elemente von K heißen **Skalare** (englisch: scalars), sie werden häufig mit griechischen Kleinbuchstaben $\alpha, \beta, \ldots$ bezeichnet. K selbst heißt der **Skalarkörper** (englisch: scalar field) von V. △

[1] **S-Multiplikation** ist der von uns bevorzugte Begriff, um Verwechslungen mit dem Begriff **Skalarprodukt** auszuschließen, siehe später.

Bemerkung 11.2 (abkürzende Schreibweisen in Vektorräumen)**.**

(*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*) Mit der in Bemerkung 7.20 eingeführten Notation haben wir

$$n\,v = \underbrace{v \oplus \cdots \oplus v}_{n\text{-mal}} = (1_K \odot v) \oplus \cdots \oplus (1_K \odot v) = (1_K + \cdots + 1_K) \odot v = (n\,1_K) \odot v$$

für $n \in \mathbb{N}$. Bezeichnen wir das Element $n\,1_K \in K$ einfach mit n, so erhalten wir also $n\,v = n \odot v$. Tatsächlich gilt das auch für $n \in \mathbb{Z}$. Das werden wir später noch nutzen, um unsere Notation zu vereinfachen (Bemerkung 11.13).

(*iii*) Wir vereinbaren, dass $\odot$ stärker bindet als $\oplus$, also könnten wir die rechte Seite in (11.1b) auch in der Form $\alpha \odot u \;\oplus\; \alpha \odot v$ schreiben.

(*iv*) 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 die andere äußere Verknüpfung $\boxdot\colon V \times K \to V$ definieren, und zwar durch $v \boxdot \alpha := \alpha \odot v$. Dann gelten auch dafür die Gesetze (11.1), 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.

(*v*) 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 11.13. △

Beispiel 11.3 (Vektorraum)**.**

(*i*) Über jedem Körper $(K, +, \cdot)$ gibt es den (bis auf Isomorphie eindeutigen) Vektorraum $(V, \oplus, \odot)$ mit nur einem einzigen Element, nämlich $V = \{0_V\}$. Die Verknüpfungen $\oplus$ und $\odot$ sind dann eindeutig festgelegt. (**Quizfrage 11.1:** Wie nämlich?) Dieser Raum heißt ein **Nullraum** (englisch: zero vector space) über K.

(*ii*) Jeder Körper $(K, +, \cdot)$, ausgestattet mit den Verknüpfungen $\oplus := +\colon K \times K \to K$ und $\odot := \cdot\colon K \times K \to K$, ist ein Vektorraum über sich selbst.

(*iii*) Allgemeiner sei $(K, +, \cdot)$ ein Körper und U ein Unterkörper. Dann ist $(K, +, \cdot)$ ein U-Vektorraum mit den Verknüpfungen $\oplus := +\colon K \times K \to K$ und $\odot := \cdot\colon U \times K \to K$. Beispielsweise ist $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum, und $\mathbb{C}$ ist sowohl ein $\mathbb{R}$-Vektorraum als auch ein $\mathbb{Q}$-Vektorraum.

(*iv*) Es sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann ist die Menge

$$K_n := \left\{ \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \,\middle|\, x_i \in K \text{ für } i = 1, \ldots, n \right\}, \tag{11.2}$$

ausgestattet mit der **komponentenweisen Addition** (englisch: componentwise addition) und der **komponentenweisen S-Multiplikation** (englisch: componentwise S-multiplication)

$$\begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \oplus \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 & \cdots & x_n + y_n \end{pmatrix}, \tag{11.3a}$$

$$\alpha \odot \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} := \begin{pmatrix} \alpha \cdot x_1 & \cdots & \alpha \cdot y_n \end{pmatrix}, \tag{11.3b}$$

ein K-Vektorraum, genannt der **Vektorraum der Zeilenvektoren** (englisch: row vector space) über K der **Dimension** n.[3] Der Nullvektor ist $\begin{pmatrix} 0_K & \cdots & 0_K \end{pmatrix} \in K_n$.

Es wird sich als praktisch erweisen, auch den Fall $n = 0$ zuzulassen. Der Raum K_0 besteht dann nur aus einem Element, dem leeren Zeilenvektor $(\,)$. K_0 ist also ein Nullraum über K. Es gilt $\alpha \odot (\,) = (\,)$ für alle $\alpha \in K$ und $(\,) \oplus (\,) = (\,)$.

(*v*) Es sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann ist die Menge[4]

$$K^n := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| \, x_i \in K \text{ für } i = 1, \ldots, n \right\}, \tag{11.4}$$

ausgestattet mit der **komponentenweisen Addition** (englisch: componentwise addition) und der **komponentenweisen S-Multiplikation** (englisch: componentwise S-multiplication)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \tag{11.5a}$$

$$\alpha \odot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \alpha \cdot x_1 \\ \vdots \\ \alpha \cdot x_n \end{pmatrix}, \tag{11.5b}$$

ein K-Vektorraum, genannt der **Vektorraum der Spaltenvektoren** (englisch: column vector space) oder auch der **Standardvektorraum** (englisch: standard vector space) oder der **Koordinatenraum**[5] (englisch: coordinate space) über K der **Dimension** n. Der Nullvektor ist $\begin{pmatrix} 0_K \\ \vdots \\ 0_K \end{pmatrix}$ in K^n.

Es wird sich auch hier als praktisch erweisen, den Fall $n = 0$ zuzulassen. Der Raum K^0 besteht dann nur aus einem Element, dem leeren Spaltenvektor $(\,)$. K^0 ist also ein Nullraum über K. Es gilt $\alpha \odot (\,) = (\,)$ für alle $\alpha \in K$ und $(\,) \oplus (\,) = (\,)$.

(*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

$$(f \oplus g)(x) := f(x) + g(x),$$
$$(\alpha \odot f)(x) := \alpha \cdot f(x),$$

ein K-Vektorraum.[6] Der Nullvektor ist die **Nullfunktion** (englisch: zero function, constant function zero) $X \ni x \mapsto 0_K \in K$.

[3] Der Begriff der Dimension für beliebige Vektorräume wird in Definition 13.11 eingeführt. Hier dient er zunächst zur Angabe der Anzahl der Einträge in einem Zeilenvektor.

[4] K^n ist hier also nicht als die Menge von n-Tupeln über K zu lesen, siehe Definition 4.8.

[5] Der Begriff **Koordinatenraum** wird später in Satz 19.1 klar werden.

[6] In Beispiel 10.2 hatten wir gesehen, dass K^X i. A. kein Körper ist, sondern nur ein kommutativer Ring mit Eins. Hier zeigt sich nun, dass K^X außerdem ein K-Vektorraum ist.

Insbesondere ist die Menge der Folgen $K^{\mathbb{N}}$ mit Werten in K ein K-Vektorraum, genannt der **Folgenraum** (englisch: sequence space) **über** K.

(*vii*) Allgemeiner sei $(K, +, \cdot)$ ein Körper, $(V, \oplus, \odot)$ ein K-Vektorraum und X eine Menge. Dann ist die Menge $V^X = \{f \mid f\colon X \to V\}$, ausgestattet mit den punktweisen Verknüpfungen

$$\begin{aligned}(f \oplus g)(x) &\coloneqq f(x) \oplus g(x),\\ (\alpha \odot f)(x) &\coloneqq \alpha \odot f(x),\end{aligned}$$

ein K-Vektorraum. Der Nullvektor ist die **Nullfunktion** (englisch: zero function, constant function zero) $X \ni x \mapsto 0_V \in V$.

Insbesondere ist die Menge der Folgen $V^{\mathbb{N}}$ mit Werten in V ein K-Vektorraum, genannt der **Folgenraum über** V. △

Definition 11.4 (kartesisches Produkt von Vektorräumen, vgl. Definition 6.42 des kartesischen Produkts von Mengen)**.**
Es seien $(K, +, \cdot)$ ein Körper, I eine Menge, und weiter sei $(V_i, \oplus_i, \odot_i)$ ein K-Vektorraum für jedes $i \in I$.

(*i*) Das **kartesische Produkt** dieser Vektorräume

$$W \coloneqq \bigtimes_{i\in I} V_i \coloneqq \left\{F\colon I \to \bigcup_{i\in I} V_i \,\middle|\, F(i) \in V_i \text{ für alle } i \in I\right\}, \tag{11.6}$$

ausgestattet mit der punktweisen Addition $\oplus$ und der punktweisen S-Multiplikation $\odot$

$$\begin{aligned}\oplus\colon W \times W \to W \quad &\text{mit } F \oplus G \text{ definiert durch} \quad (F \oplus G)(i) \coloneqq F(i) \oplus_i G(i),\\ \odot\colon K \times W \to W \quad &\text{mit } \alpha \odot F \text{ definiert durch} \quad (\alpha \cdot F)(i) \coloneqq \alpha \odot_i F(i),\end{aligned}$$

ist ein K-Vektorraum. Dieser wird auch der **Produktraum** (englisch: product space) der Vektorräume V_i, $i \in I$, genannt.

(*ii*) Ist $I = [\![1, n]\!]$ für $n \in \mathbb{N}$, so schreiben wir statt $\bigtimes_{i\in I} V_i$ auch $\bigtimes_{i=1}^n V_i$ oder $V_1 \times \cdots \times V_n$ und identifizieren die Elemente $F\colon [\![1, n]\!] \to \bigcup_{i=1}^n V_i$ mit den n-Tupeln $(F(1), \ldots, F(n))$, vgl. Bemerkung 6.43.

(*iii*) Wenn alle Vektorräume $(V_i, \oplus_i, \odot_i) = (V, \oplus, \odot)$ sind, so schreiben wir statt $\bigtimes_{i\in I} V$ auch V^I. Ist zusätzlich $I = [\![1, n]\!]$, so schreiben wir auch $\bigtimes_{i=1}^n V$ oder V^n.

(*iv*) Im Fall $I = \emptyset$ besteht das kartesische Produkt (11.6) aus dem einzigen Element $F\colon \emptyset \to \emptyset$, also der leeren Funktion bzw. dem leeren Tupel $()$. In diesem Fall ist $W = \bigtimes_{i\in I} V_i$ also ein Nullraum über K. △

Lemma 11.5 (Rechenregeln in Vektorräumen, vgl. Rechenregeln in Ringen (Lemma 9.3))**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein K-Vektorraum. Dann gilt für $\alpha \in K$ und $v \in V$:

(*i*) $0_K \odot v = 0_V$.

(*ii*) $\alpha \odot 0_V = 0_V$.

(*iii*) $\alpha \odot (\ominus v) = \ominus(\alpha \odot v) = (-\alpha) \odot v$ und insbesondere $\ominus v = (-1_K) \odot v$.

(*iv*) $(-\alpha) \odot (\ominus v) = \alpha \odot v$.

(*v*) $\alpha \odot v = 0_V \quad \Rightarrow \quad \alpha = 0_K$ oder $v = 0_V$.

Beweis. Aussage (*i*): Wir haben

$$\begin{aligned} 0_V \oplus 0_K \odot v &= 0_K \odot v && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= (0_K + 0_K) \odot v && \text{da } 0_K \text{ das neutrale Element von } (K, +) \text{ ist} \\ &= 0_K \odot v \oplus 0_K \odot v && \text{nach Distributivgesetz (11.1c).} \end{aligned}$$

Aus der Kürzungsregel (7.8b) in der Gruppe $(V, \oplus)$ folgt nun $0_V = 0_K \odot v$.

Aussage (*ii*): Für beliebiges $\alpha \in K$ gilt

$$\begin{aligned} \alpha \odot 0_V \oplus 0_V &= \alpha \odot 0_V && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= \alpha \odot (0_V \oplus 0_V) && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= \alpha \odot 0_V \oplus \alpha \odot 0_V && \text{nach Distributivgesetz (11.1b).} \end{aligned}$$

Aus der Kürzungsregel (7.8a) in der Gruppe $(V, \oplus)$ folgt nun $0_V = \alpha \odot 0_V$.

Aussage (*iii*): 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:

$$\begin{aligned} \big((-\alpha) \odot v\big) \oplus \big(\alpha \odot v\big) &= (-\alpha + \alpha) \odot v && \text{nach Distributivgesetz (11.1c)} \\ &= 0_K \odot v && \text{da } \alpha \text{ in der Gruppe } (K, +) \text{ das Inverse } -\alpha \text{ besitzt} \\ &= 0_V && \text{nach Aussage (}i\text{).} \end{aligned}$$

Das heißt, es gilt $\ominus(\alpha \odot v) = (-\alpha) \odot v$. Insbesondere für $\alpha = 1_K$ erhalten wir

$$\ominus v = \ominus(1_K \odot v) = (-1_K) \odot v. \tag{11.7}$$

Weiter haben wir

$$\begin{aligned} (-\alpha) \odot v &= \big((-1_K) \cdot \alpha\big) \odot v && \text{nach Lemma 9.3} \\ &= \big(\alpha \cdot (-1_K)\big) \odot v && \text{da } (K, \cdot) \text{ kommutativ ist} \\ &= \alpha \odot \big((-1_K) \odot v\big) && \text{nach Assoziativgesetz (11.1a)} \\ &= \alpha \odot (\ominus v) && \text{nach (11.7).} \end{aligned}$$

Aussage (*iv*): Aus Aussage (*iii*) mit $-\alpha$ statt α sowie $-(-\alpha) = \alpha$ folgt sofort

$$(-\alpha) \odot (\ominus v) = (-(-\alpha)) \odot v = \alpha \odot v.$$

Aussage (*v*): Es seien $\alpha \in K$ und $v \in V$ sowie $\alpha \odot v = 0_V$. Nehmen wir $\alpha \neq 0_K$ an, dann gilt

$$\begin{aligned} v &= 1_K \odot v && \text{nach (11.1d)} \\ &= (\alpha^{-1} \cdot \alpha) \odot v && \text{da } \alpha \neq 0_K \text{ in der Gruppe } (K \setminus \{0\}, \cdot) \text{ das Inverse } \alpha^{-1} \text{ besitzt} \\ &= \alpha^{-1} \odot (\alpha \odot v) && \text{nach Assoziativgesetz (11.1a)} \\ &= \alpha^{-1} \odot 0_V && \text{nach Voraussetzung} \\ &= 0_V && \text{nach Aussage (}ii\text{).} \end{aligned}$$

□

Bemerkung 11.6 (Mengen und Familien in Vektorräumen)**.**
Die nun folgenden Definitionen und Resultate bis zum Ende von § 14 geben wir jeweils in zwei Versionen an: für Mengen und für Familien. Beispielsweise geht es in der folgenden Definition 11.7 um Linearkombinationen einer Menge bzw. einer Familie von Vektoren. Die Aussagen sind jeweils konzeptionell gleich, unterscheiden sich jedoch im Detail, vgl. auch Bemerkung 6.40 zu den Unterschieden von Mengen und Familien.

Die Unterscheidung zwischen Mengen und Familien hätten wir beispielsweise auch bereits bei erzeugten Untergruppen (Definition 7.48) und bei erzeugten Idealen (Definition 9.35) machen können. Dort hatten wir nur Mengen als Erzeuger betrachtet. Der Grund, diese Unterscheidung nun bei Vektorräumen zu treffen, liegt darin, dass wir später vor allem bei der Darstellung linearer Abbildungen in Form von Matrizen von der Ordnung auf der Indexmenge einer (endlichen) Familie profitieren werden. △

Definition 11.7 (Linearkombination)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein K-Vektorraum.

Es sei $E \subseteq V$ eine Menge von Vektoren in V. Ist $E_0 \subseteq E$ eine endliche Teilmenge und sind $\alpha_v \in K$, dann heißt der Vektor[7]

$$\sum_{v \in E_0} \alpha_v \odot v \tag{11.8}$$

eine **Linearkombination**[8] **der Menge** E oder eine **Linearkombination von Vektoren der Menge** E.

Es sei $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V. Ist $F_0 = (v_i)_{i \in I_0}$ eine endliche Teilfamilie und sind $\alpha_i \in K$, dann heißt der Vektor

$$\sum_{i \in I_0} \alpha_i \odot v_i \tag{11.9}$$

eine **Linearkombination der Familie** F oder eine **Linearkombination von Vektoren der Familie** F.

Die Skalare α_v bzw. α_i heißen die **Koeffizienten** (englisch: coefficients) der Linearkombination. Eine Linearkombination heißt **trivial** (englisch: trivial linear combination), wenn alle Koeffizienten gleich 0_K sind.

Im Fall $E_0 = \emptyset$ bzw. $I_0 = \emptyset$ interpretieren wir wie üblich die Addition von null Elementen in (11.8) bzw. (11.9) als das neutrale Element, also als den Nullvektor 0_V. △

Beachte: Eine Linearkombination besteht immer aus endlich vielen Termen. Übrigens hat Bernd Ammann (Regensburg) auch eine sehr elegante Lösung, indem er quasi-endliche Familien von Skalaren definiert, das sind solche Familien, in denen nur endlich viele Einträge ungleich Null sind.

Bemerkung 11.8 (Linearkombination)**.**
In der Literatur werden Linearkombinationen an Stelle von (11.8) bzw. (11.9) oft in der Form

$$\alpha_1 \odot v_1 \oplus \cdots \oplus \alpha_n \odot v_n \qquad \alpha_1 \odot v_{i_1} \oplus \cdots \oplus \alpha_n \odot v_{i_n}$$

[7] Wir verwenden das Summenzeichen also auch für die Addition $\oplus$ im Vektorraum $(V, \oplus, \odot)$.
[8] englisch: linear combination

oder kurz $\sum_{j=1}^{n} \alpha_j \odot v_j$ (11.10)

mit endlich vielen Skalaren $\alpha_j \in K$ und Vektoren $v_j \in E$

oder kurz $\sum_{j=1}^{n} \alpha_j \odot v_{i_j}$ (11.11)

mit endlich vielen Indizes $i_j \in I$, Skalaren $\alpha_j \in K$ und Vektoren v_{i_j} aus F

für $j = 1, \dots, n$ und $n \in \mathbb{N}_0$ geschrieben. Diese Notation hat aber einige Nachteile. Insbesondere ist es in (11.10) möglich, dass Vektoren aus E mehrfach gewählt werden, was die Formulierung einiger Resultate erschwert. In (11.11) können zudem Indizes aus I mehrfach vorkommen. (**Quizfrage 11.2:** Warum ist jede Linearkombination im Sinne von (11.8) eine Linearkombination im Sinne von (11.10) und umgekehrt? Und warum ist jede Linearkombination im Sinne von (11.9) auch eine Linearkombination im Sinne von (11.11) und umgekehrt?) △

Beispiel 11.9 (Linearkombination)**.**

(*i*) Der Vektor $\left(\begin{smallmatrix}3\\-7\end{smallmatrix}\right)$ ist eine Linearkombination der Menge von 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

$$\begin{pmatrix}3\\-7\end{pmatrix} = 3 \odot \begin{pmatrix}1\\0\end{pmatrix} \oplus (-7) \odot \begin{pmatrix}0\\1\end{pmatrix}.$$

Die Koeffizienten 3 und -7 sind hier offensichtlich.

Derselbe Vektor $\left(\begin{smallmatrix}3\\-7\end{smallmatrix}\right)$ kann auch als

$$\begin{pmatrix}3\\-7\end{pmatrix} = 8 \odot \begin{pmatrix}1\\0\end{pmatrix} \oplus (-7) \odot \begin{pmatrix}0\\1\end{pmatrix} \oplus (-5) \odot \begin{pmatrix}1\\0\end{pmatrix}$$

geschrieben werden, also als Linearkombination der Form (11.10).

(*ii*) Der Vektor $\left(\begin{smallmatrix}3\\-7\end{smallmatrix}\right)$ ist eine Linearkombination der Menge von 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

$$\begin{pmatrix}3\\-7\end{pmatrix} = \frac{31}{6} \odot \begin{pmatrix}2\\-1\end{pmatrix} \oplus \frac{-11}{6} \odot \begin{pmatrix}4\\1\end{pmatrix}.$$

Die Koeffizienten sind hier nicht offensichtlich. Sie können aber durch Lösen eines linearen Gleichungssystems bestimmt werden, siehe § 16.

(*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 von Vektoren (Funktionen) $\{\sin, \cos\}$ im Vektorraum der Funktionen $\mathbb{R}^{[0,2\pi]}$. △

Definition 11.10 (Unterraum, vgl. Definition 10.6 eines Unterkörpers)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein K-Vektorraum.

(*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 S-Multiplikation $\odot$ mit Elementen in K abgeschlossen und wenn $(U, \oplus, \odot)$ selbst wieder ein Vektorraum ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, \oplus)$ eine Untergruppe von $(V, \oplus)$ und wenn U bzgl. der S-Multiplikation $\odot$ mit Elementen in K abgeschlossen ist.

(*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 erreichen:

Satz 11.11 (Unterraumkriterium, vgl. Unterkörperkriterium Satz 10.7)**.**
Es sei $(K, +, \cdot)$ ein Körper, $(V, \oplus, \odot)$ ein K-Vektorraum 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 $\alpha \odot u \in U$.[9]

(*iii*) $U \neq \emptyset$, und für alle $u, v \in U$ und $\alpha, \beta \in K$ gilt $\alpha \odot u \oplus \beta \odot v \in U$.[10]

Beweis. Aussage (*i*) ⇒ Aussage (*ii*): Es sei $(U, \oplus, \odot)$ ein Unterraum von $(V, \oplus, \odot)$. Dann ist per Definition 11.10 und Definition 11.1 $(U, \oplus)$ 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*) ⇒ 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 (11.1) 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 7.44) 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*) ⇒ 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*) ⇒ 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 11.12 (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 $(\{0_V\}, \oplus, \odot)$ heißt der **Nullunterraum** (englisch: zero vector subspace) von V.

(*ii*) Wir betrachten den Standardvektorraum $V = \mathbb{R}^2$ über dem Körper $\mathbb{R}$.

[9] kurz: $U \oplus U \subseteq U$ und $K \odot U \subseteq U$
[10] kurz: $K \odot U \oplus K \odot U \subseteq U$

(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 11.11 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 $v = \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right) \in U_1$:

$$u \oplus v = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix} \in U_1, \quad \text{denn } (x_1 + y_1) - 2\,(x_2 + y_2) = (x_1 - 2\,x_2) + (y_1 - 2\,y_2) = 0$$

$$\alpha \odot u = \begin{pmatrix} \alpha\,x_1 \\ \alpha\,x_2 \end{pmatrix} \in U_1, \quad \text{denn } \alpha\,x_1 - 2\,(\alpha\,x_2) = \alpha\,(x_1 - 2\,x_2) = 0.$$

(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 $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$. Der Nullvektor ist aber notwendigerweise in jedem Unterraum enthalten, wie wir im Anschluss an Definition 11.10 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 Folgenraum über K. Der **Träger** (englisch: support) einer Folge $(x_n)_{n\in\mathbb{N}}$ ist die Menge derjenigen Indizes, für die $x_n \neq 0_K$ ist, also

$$\operatorname{supp}(x_n)_{n\in\mathbb{N}} = \{n \in \mathbb{N} \mid x_n \neq 0_K\} \subseteq \mathbb{N}. \tag{11.12}$$

Die Teilmenge der **Folgen mit endlichem Träger** (englisch: sequences with finite support) oder **endlich getragenen Folgen** (englisch: finitely supported sequences)

$$(K^{\mathbb{N}})_{00} := \left\{ (x_n)_{n\in\mathbb{N}} \,\middle|\, \operatorname{supp}(x_n)_{n\in\mathbb{N}} \text{ ist endlich} \right\} \tag{11.13}$$

ist ein echter Unterraum von $(K^{\mathbb{N}}, \oplus, \odot)$. (**Quizfrage 11.3:** Kann man den Begriff der endlich getragenen Folgen auf Folgen über einem K-Vektorraum V ausdehnen?) △

Expertenwissen: noch mehr Unterräume des Folgenraumes über $\mathbb{R}$

In Lehrveranstaltungen zur *Analysis* werden die Folgenräume

$$(\mathbb{R}^{\mathbb{N}})_b := \left\{ (y_n)_{n\in\mathbb{N}} \,\middle|\, \exists C \geqslant 0 \text{ für alle } n \in \mathbb{N}\ (|y_n| \leqslant C) \right\} \quad \text{der } \textbf{beschränkten Folgen}^{11}$$

$$(\mathbb{R}^{\mathbb{N}})_c := \left\{ (y_n)_{n\in\mathbb{N}} \,\middle|\, (y_n)_{n\in\mathbb{N}} \text{ ist konvergent} \right\} \quad \text{der } \textbf{konvergenten Folgen}^{12}$$

$$(\mathbb{R}^{\mathbb{N}})_0 := \left\{ (y_n)_{n\in\mathbb{N}} \,\middle|\, (y_n)_{n\in\mathbb{N}} \text{ konvergiert gegen } 0 \right\} \quad \text{der } \textbf{Nullfolgen}^{13}$$

eingeführt. Es gilt

$$(\mathbb{R}^{\mathbb{N}})_{00} \subsetneq (\mathbb{R}^{\mathbb{N}})_0 \subsetneq (\mathbb{R}^{\mathbb{N}})_c \subsetneq (\mathbb{R}^{\mathbb{N}})_b \subsetneq \mathbb{R}^{\mathbb{N}}$$

im Sinne von Teilmengen und von Unterräumen. Diese Definitionen und Aussagen können auf normierte Vektorräume über $\mathbb{R}$ verallgemeinert werden.

Bemerkung 11.13 (Vereinfachung der Notation)**.**

(*i*) Zur Vereinfachung der Notation werden wir in Zukunft für die Verknüpfungen $\oplus$ und $\odot$ in K-Vektorräumen V einfach dieselbe Notation verwenden wie für die Verknüpfungen $+$ und $\cdot$ des zugrundeliegenden Körpers K. Aus den verknüpften Objekten ist entweder ersichtlich, ob die jeweilige Verknüpfung mit Skalaren oder mit Vektoren gemeint ist, oder aber (im Fall $K \subseteq V$) ist die Unterscheidung wegen (11.1d) unerheblich.

(*ii*) Das Zeichen für die Multiplikation $\cdot$ von Vektoren mit Elementen aus dem zugrundeliegenden Körper (oder von zwei Körperelementen) wird sogar oft ganz weggelassen, sofern sich dadurch keine Unklarheiten ergeben. Beispielsweise schreiben wir in Zukunft einfach

$$\begin{pmatrix}3\\1\end{pmatrix} - 2\begin{pmatrix}1\\-1\end{pmatrix} \quad \text{an Stelle von} \quad \begin{pmatrix}3\\1\end{pmatrix} \ominus 2 \odot \begin{pmatrix}1\\-1\end{pmatrix}$$

im Vektorraum $\mathbb{R}^2$ oder

$$\sin - \sqrt{2}\cos \quad \text{an Stelle von} \quad \sin \ominus \sqrt{2} \odot \cos$$

im Vektorraum $\mathbb{R}^{[0,2\pi]}$. Wie in Bemerkung 11.2 erklärt, müssen die Ausdrücke $n\,v$ und $n \odot v := (n\,1_K) \odot v$ für $n \in \mathbb{Z}$ ohnehin nicht unterschieden werden.

(*iii*) Wir werden außerdem das Nullelement 0_K des Skalarkörpers K in Zukunft einfach als 0 notieren, das Einselement 1_K von K als 1 und den Nullvektor von V ebenfalls als 0.

(*iv*) Schließlich werden wir in Zukunft auch von Vektorräumen sprechen, ohne den zugrundeliegenden Körper explizit zu erwähnen, wenn dieser für die Formulierung des jeweiligen Resultats nicht relevant ist. Dennoch besitzt natürlich jeder Vektorraum immer einen konkreten zugrundeliegenden Körper. △

Ende der Vorlesung 15

Wie bereits bei Untergruppen in § 7.4 sowie bei Idealen in § 9.1 beschäftigt uns nun die Frage, wie man Unterräume erzeugen kann.

Lemma 11.14 (Durchschnitt von Unterräumen, vgl. Lemma 10.10 zu Unterkörpern)**.**
Es sei V ein Vektorraum.

(*i*) Ist $(U_i)_I$ eine nichtleere Familie von Unterräumen von $(V, \oplus, \odot)$, dann ist auch $\bigcap_{i\in I} U_i$ ein Unterraum von $(V, \oplus, \odot)$.

[11] englisch: bounded sequences
[12] englisch: convergent sequences
[13] englisch: null sequences

(*ii*) Ist $\mathcal{U}$ eine nichtleere Menge von Unterräumen von $(V, \oplus, \odot)$, dann ist auch $\bigcap \mathcal{U}$ ein Unterraum von $(V, \oplus, \odot)$.

Beweis. Dieser Beweis ist Gegenstand der Übung. □

Definition 11.15 (erzeugter Unterraum, lineare Hülle, Spann, Erzeugendensystem, erzeugende Familie)**.**
Es sei V ein Vektorraum.

(*i*) Ist $E \subseteq V$ eine Teilmenge von Vektoren in V, dann heißt

$$\langle E \rangle := \bigcap \left\{ U \;\middle|\; \begin{array}{l} U \text{ ist Unterraum von } V \\ \text{und } E \subseteq U \end{array} \right\} \tag{11.14}$$

der von E **erzeugte** oder **aufgespannte Unterraum**[14], die **lineare Hülle**[15] $\mathrm{Lin}(E)$ oder auch der **Spann**[16] $\mathrm{Span}(E)$ von E in V.

Ist speziell E die endliche Menge $E = \{v_1, \ldots, v_n\}$ für $v_i \in V$ und $n \in \mathbb{N}_0$, so schreiben wir auch $\langle v_1, \ldots, v_n \rangle$ oder $\mathrm{Lin}(v_1, \ldots, v_n)$ oder $\mathrm{Span}(v_1, \ldots, v_n)$ statt $\langle \{v_1, \ldots, v_n\} \rangle$ oder $\mathrm{Lin}(\{v_1, \ldots, v_n\})$ oder $\mathrm{Span}(\{v_1, \ldots, v_n\})$.

(*ii*) Gilt $\langle E \rangle = V$, dann heißt E eine **erzeugende Menge**[17] oder ein **Erzeugendensystem**[18] von V.

(*iii*) Falls eine endliche erzeugende Menge von V existiert, so heißt V **endlich erzeugt**[19].

(*i*) Ist $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V ist, dann heißt

$$\langle F \rangle := \bigcap \left\{ U \;\middle|\; \begin{array}{l} U \text{ ist Unterraum von } V \\ \text{und } \{v_i \mid i \in I\} \subseteq U \end{array} \right\} \tag{11.15}$$

der von F **erzeugte** oder **aufgespannte Unterraum**, die **lineare Hülle** $\mathrm{Lin}(F)$ oder auch der **Spann** $\mathrm{Span}(F)$ von F in V.

Ist speziell F die endliche Familie $F = (v_1, \ldots, v_n)$ für $v_i \in V$ und $n \in \mathbb{N}_0$, so schreiben wir auch $\langle v_1, \ldots, v_n \rangle$ oder $\mathrm{Lin}(v_1, \ldots, v_n)$ oder $\mathrm{Span}(v_1, \ldots, v_n)$ statt $\langle (v_1, \ldots, v_n) \rangle$ oder $\mathrm{Lin}((v_1, \ldots, v_n))$ oder $\mathrm{Span}((v_1, \ldots, v_n))$.

(*ii*) Gilt $\langle F \rangle = V$, dann heißt F eine **erzeugende Familie**[20] oder ein **Erzeugendensystem** von V.

(*iii*) Falls eine endliche erzeugende Familie von V existiert, so heißt V **endlich erzeugt**. △

Beachte: Bezeichnen wir mit $\mathcal{R}$ die Menge auf rechten Seite von (11.14), über die der Durchschnitt gebildet wird, dann ist $\langle E \rangle$ das Minimum der Menge $\mathcal{R}$ bzgl. der Inklusionshalbordnung und auch das Minimum der Menge $\mathcal{R}$ bzgl. der Halbordnung „ist Unterraum von“ auf der Menge aller Unterräume von V.

Quizfrage 11.4: An der verkürzten Schreibweise $\langle v_1, \ldots, v_n \rangle$ kann man nicht mehr erkennen, ob $\{v_1, \ldots, v_n\}$ als Menge oder $(v_1, \ldots, v_n)$ als Familie gemeint war. Warum ist das kein Problem,

[14] englisch: subspace generated by E, subspace spanned by E
[15] englisch: linear hull
[16] englisch: span
[17] englisch: generating set
[18] englisch: generator
[19] englisch: finitely generated
[20] englisch: generating family

auch wenn Vektoren mehrfach vorkommen?

Quizfrage 11.5: Ist der Begriff eines endlich erzeugten Vektorraumes wohldefiniert, unabhängig davon, ob man mit erzeugenden Mengen oder mit erzeugenden Familien arbeitet?

Satz 11.16 (Darstellung des erzeugten Unterraumes)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein K-Vektorraum.

Ist $E \subseteq V$ eine Teilmenge von Vektoren in V, dann gilt für den von E erzeugten Unterraum:

$$\langle E\rangle = \left\{ \sum_{v\in E_0} \alpha_v\, v \;\middle|\; \begin{matrix} E_0 \subseteq E \text{ endlich,} \\ \forall v \in E_0 \ (\alpha_v \in K) \end{matrix} \right\}. \tag{11.16}$$

Ist $F = (v_i)_{i\in I}$ eine Familie von Vektoren in V, dann gilt für den von F erzeugten Unterraum:

$$\langle F\rangle = \left\{ \sum_{i\in I_0} \alpha_i\, v_i \;\middle|\; \begin{matrix} I_0 \subseteq I \text{ endlich,} \\ \forall i \in I_0 \ (\alpha_i \in K) \end{matrix} \right\}. \tag{11.17}$$

Beachte: Der von einer Menge E (oder einer Familie F) erzeugte Unterraum ist also nicht anderes als die Menge der Linearkombinationen von E (bzw. F).[21] Zur Erinnerung: Im Fall $E_0 = \emptyset$ in (11.16) bzw. $I_0 = \emptyset$ in (11.17) interpretieren wir die Linearkombination von null Elementen als den Nullvektor 0. Insbesondere im Fall $E = \emptyset$ ist also $\langle E\rangle = \langle\emptyset\rangle = \{0\}$ der Nullunterraum von V, und auch im Fall der leeren Familie $F = ()$ gilt $\langle F\rangle = \langle()\rangle = \{0\}$.

Beweis. Wir führen den Beweis nur für Mengen E und die Darstellung (11.16). Der Beweis für den Fall (11.17) geht ähnlich. Zur Abkürzung bezeichnen wir die Menge auf der rechten Seite von (11.16) mit M. Wir führen den Beweis analog zu Satz 7.50 (Darstellung der erzeugten Untergruppe) in zwei Schritten.

Schritt 1: $\langle E\rangle \supseteq M$: Es sei U ein beliebiger Unterraum von V, der im Durchschnitt (11.14) 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 (11.14) 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 11.11). Offensichtlich ist $M \neq \emptyset$, denn M enthält mindestens den Nullvektor 0. Sind $\sum_{v\in E_0} \alpha_v\, v$ und $\sum_{v\in E_1} \beta_v\, v$ zwei Elemente aus M, so ist auch $\sum_{v\in E_0} \alpha_v\, v + \sum_{v\in E_1} \beta_v\, v$ ein Element aus M. (**Quizfrage 11.6:** Klar?) Zudem ist für jedes $\alpha \in K$ auch $\alpha \sum_{v\in E_0} \alpha_v\, v = \sum_{v\in E_0} \alpha\, \alpha_v\, v$ ein Element aus M. Also ist M ein Unterraum von V. Zusätzlich ist klar, dass $E \subseteq M$ gilt. (**Quizfrage 11.7:** Warum?) Das heißt, M ist einer derjenigen Unterräume von V, über die in der Definition von $\langle E\rangle$ der Durchschnitt gebildet wird. Folglich gilt $\langle E\rangle \subseteq M$. □

Beispiel 11.17 (lineare Hülle)**.**

(*i*) Es sei K ein Körper und $K^{\mathbb{N}}$ der Folgenraum über K, siehe Beispiel 11.12. Ein Element von $K^{\mathbb{N}}$, also eine Folge $(y_n)_{n\in\mathbb{N}}$ mit Werten in K, heißt die j-te **Standardfolge** (englisch: standard sequence) für $j \in \mathbb{N}$, wenn $y_j = 1$ und $y_n = 0$ für alle $n \neq j$ gilt. Wir bezeichnen die j-te Standardfolge auch mit dem Symbol e_j.[22]

[21] In manchen Büchern wird daher auch (11.16) als Definition des erzeugten Unterraumes verwendet.
[22] Sollten wir das n-te Glied der Folge e_j bezeichnen müssen, so würden wir einen Doppelindex verwenden: $e_{j,n}$.

Die Menge E aller Standardfolgen erzeugt den Unterraum der endlich getragenen Folgen, also $\langle E\rangle = (K^{\mathbb{N}})_{00}$, siehe Beispiel 11.12. (**Quizfrage 11.8:** Warum erzeugen die Standardfolgen nicht den ganzen Folgenraum $K^{\mathbb{N}}$?)

Die Menge $\{e_1, \dots, e_n\}$ bestehend aus der ersten bis zur n-ten Standardfolge, $n \in \mathbb{N}_0$, erzeugt den Unterraum derjenigen Folgen, deren Träger in $[\![1, n]\!]$ liegt, die also nur an den ersten n Stellen von 0 verschieden sein dürfen.

(*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 11.9:** Was passiert im Fall $w \in \langle v\rangle$?) △

Folgerung 11.18 (zu Satz 11.16: lineare Hülle von Vereinigung und Schnitt, vgl. Folgerung 7.53)**.** Es sei V ein Vektorraum.

Sind $E_1, E_2 \subseteq V$ Teilmengen von Vektoren in V, dann gilt

$$\langle E_1 \cup E_2\rangle = \big\langle \langle E_1\rangle \cup \langle E_2\rangle \big\rangle \tag{11.18a}$$
$$\langle E_1 \cap E_2\rangle \subseteq \big\langle \langle E_1\rangle \cap \langle E_2\rangle \big\rangle. \tag{11.18b}$$

Sind $F_1, F_2 \subseteq V$ Familien von Vektoren in V, dann gilt

$$\langle F_1 \cup F_2\rangle = \big\langle \langle F_1\rangle \cup \langle F_2\rangle \big\rangle \tag{11.19a}$$
$$\langle F_1 \cap F_2\rangle \subseteq \big\langle \langle F_1\rangle \cap \langle F_2\rangle \big\rangle. \tag{11.19b}$$

Beweis. Wir beweisen nur die Aussagen für Mengen, zunächst (11.18a): Die lineare Hülle ist offenbar 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 11.16 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 (11.1a) 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 folgt $\big\langle \langle E_1\rangle \cup \langle E_2\rangle \big\rangle \subseteq \langle E_1 \cup E_2\rangle$.

Nun zum Beweis von (11.18b): 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 $\langle E_1 \cap E_2\rangle \subseteq \big\langle \langle E_1\rangle \cap \langle E_2\rangle \big\rangle$. □

§ 12 Lineare Unabhängigkeit

In diesem Abschnitt geht es um die Begriffe der linearen Unabhängigkeit bzw. linearen Abhängigkeit und ihre Konsequenzen.

Definition 12.1 (lineare (Un-)abhängigkeit).
Es sei V ein Vektorraum.

(*i*) Eine Menge $E \subseteq V$ von Vektoren in V heißt **linear unabhängig**[23], wenn in jeder Linearkombination von Vektoren aus E, die den Nullvektor ergibt, notwendig alle Koeffizienten gleich 0 sind, wenn also für jede endliche Teilmenge $E_0 \subseteq E$ gilt:

$$\sum_{v \in E_0} \alpha_v \, v = 0 \quad \Rightarrow \quad \alpha_v = 0 \text{ für alle } v \in E_0. \tag{12.1}$$

(*ii*) Wenn dagegen eine Linearkombination von Vektoren aus E möglich ist, die den Nullvektor ergibt, wobei nicht alle Koeffizienten gleich 0 sind, dann heißt die Menge E **linear abhängig**[24].

(*i*) Eine Familie F von Vektoren in V heißt **linear unabhängig**, wenn in jeder Linearkombination von Vektoren aus F, die den Nullvektor ergibt, notwendig alle Koeffizienten gleich 0 sind, wenn also für jede endlich Teilmenge $I_0 \subseteq I$ der Indizes gilt:

$$\sum_{i \in I_0} \alpha_i \, v_i = 0 \quad \Rightarrow \quad \alpha_i = 0 \text{ für alle } i \in I_0. \tag{12.2}$$

(*ii*) Wenn dagegen eine Linearkombination von Vektoren aus F möglich ist, die den Nullvektor ergibt, wobei nicht alle Koeffizienten gleich 0 sind, dann heißt die Familie F **linear abhängig**. △

Erlauben wir Linearkombinationen der Form (11.10), so müssen wir die Definition 12.1 wie folgt anpassen: Eine Menge $E \subseteq V$ von Vektoren in V heißt **linear unabhängig**, wenn in jeder Linearkombination der Form (11.10) 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:

$$v_1, \dots, v_n \in E \text{ mit } v_i \neq v_j \text{ für } i \neq j \quad \text{und} \quad \sum_{\ell=1}^{n} \alpha_\ell \, v_\ell = 0$$
$$\Rightarrow \quad \alpha_\ell = 0 \text{ für alle } \ell = 1, \dots, n.$$

(**Quizfrage 12.1:** Wie müsste die Definition für den Fall von Familien lauten, wenn Linearkombinationen der Form (11.11) zugelassen werden?)

Beispiel 12.2 (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

$$\alpha_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix} + \alpha_3 \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \Rightarrow \quad \alpha_1 = \alpha_2 = \alpha_3 = 0.$$

[23] englisch: linearly independent
[24] englisch: linearly dependent

(*iii*) Wir betrachten den K-Vektorraum K^X der Funktionen $X \longrightarrow K$, wobei $(K, +, \cdot)$ ein Körper und X eine Menge ist, siehe Beispiel 11.3. Für $y \in X$ definieren wir die **charakteristische Funktion** (englisch: characteristic function) $e_y \colon X \longrightarrow K$ durch[25]

$$x \longmapsto e_y(x) \coloneqq \delta_{xy} \coloneqq \begin{cases} 1, & \text{falls } x = y, \\ 0, & \text{falls } x \neq y. \end{cases} \tag{12.3}$$

Die Menge der charakteristischen Funktionen $\{e_y \mid y \in X\}$ ist linear unabhängig.

(*iv*) Es sei K ein Körper und $K^{\mathbb{N}}$ der Folgenraum über K, siehe Beispiel 11.12. Die Menge der Standardfolgen $\{e_j \mid j \in \mathbb{N}\} \subseteq K^{\mathbb{N}}$, siehe Beispiel 11.17, ist linear unabhängig. △

Bemerkung 12.3 (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 beispielsweise sagen: „Die Menge $\{v\} \cup \{v_1, v_2\}$ ist linear unabhängig."

(*ii*) Die Menge $\{v\}$, bestehend aus einem einzigen Vektor, ist genau dann linear unabhängig, wenn $v \neq 0$ ist. Eine analoge Aussage gilt für eine Familie (v) mit nur einem Mitglied.

(*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. △

Lemma 12.4 (lineare (Un-)abhängigkeit von Teilmengen und Obermengen)**.**
Es sei V ein Vektorraum. Für eine Teilmenge $E \subseteq V$ bzw. für eine Familie $F = (v_i)_{i \in I}$ von Vektoren in V gilt:

(*i*) Ist E linear unabhängig, dann auch jede Teilmenge von E.

(*ii*) Ist jede endliche Teilmenge von E linear unabhängig, dann auch E.

(*iii*) Ist E linear abhängig, dann auch jede Obermenge von E.

(*i*) Ist F linear unabhängig, dann auch jede Teilfamilie von F.

(*ii*) Ist jede endliche Teilfamilie von F linear unabhängig, dann auch F.

(*iii*) Ist F linear abhängig, dann auch jede Oberfamilie von F.

Beweis. Der Beweis ergibt sich unmittelbar aus der Definition 12.1. □

Im Folgenden führen wir einige zur linearen Abhängigkeit bzw. Unabhängigkeit äquivalente Eigenschaften an. Wir beginnen mit der Feststellung, dass die lineare Abhängigkeit einer Menge bzw. einer Familie von Vektoren bedeutet, dass man einen der Vektoren als Linearkombination der anderen darstellen kann:

[25] 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 $x \notin A$.

Lemma 12.5 (lineare Abhängigkeit ist äquivalent zur Kombinierbarkeit)**.**
Es sei V ein Vektorraum. Für eine Teilmenge $E \subseteq V$ bzw. für eine Familie $F = (v_i)_{i\in I}$ von Vektoren in V sind äquivalent:

(i) E ist linear abhängig.	(i) F ist linear abhängig.
(ii) Es gibt einen Vektor $v \in E$, der als Linearkombination der Teilmenge $E \setminus \{v\}$ darstellbar ist.	(ii) Es gibt es einen Index i^*, sodass v_{i^*} als Linearkombination der Teilfamilie $(v_i)_{i\in I\setminus\{i^*\}}$ darstellbar ist.

Beweis. Dieser Beweis ist Gegenstand der Übung. □

Folgerung 12.6 (lineare Abhängigkeit bedeutet Redundanz)**.**
Es sei V ein Vektorraum. Für eine Teilmenge $E \subseteq V$ bzw. für eine Familie $F = (v_i)_{i\in I}$ von Vektoren in V sind äquivalent:

(i) E ist linear abhängig.	(i) F ist linear abhängig.
(ii) Es gibt ein $v \in E$, sodass gilt: $\langle E \setminus \{v\}\rangle = \langle E\rangle$.	(ii) Es gibt ein $i^* \in I$, sodass gilt: $\langle (v_i)_{i\in I\setminus\{i^*\}}\rangle = \langle (v_i)_{i\in I}\rangle$.

Beachte: Ist eine erzeugende Menge (bzw. eine erzeugende Familie) eines Vektorraumes linear abhängig, so kann man mindestens ein Element (bzw. ein Mitglied) aus der erzeugenden Menge (bzw. Familie) entfernen, ohne den erzeugten Unterraum zu verkleinern.

Beweis. Wir führen den Beweis nur für Familien durch, der Beweis für Mengen geht analog.

Aussage (i) $\Rightarrow$ Aussage (ii): Da F linear abhängig ist, gibt es nach Lemma 12.5 einen Index i^*, eine endliche Teilmenge $I_0 \subseteq I \setminus \{i^*\}$ und Koeffizienten α_i für $i \in I_0$, sodass

$$v_{i^*} = \sum_{i\in I_0} \alpha_i v_i \tag{12.4}$$

gilt. Es sei nun $w \in \langle (v_i)_{i\in I}\rangle$. Nach Satz 11.16 ist w dann eine Linearkombination von $(v_i)_{i\in I}$, d. h., es gibt eine endliche Teilmenge $I_1 \subseteq I$ und Koeffizienten β_i, $i \in I_1$, sodass

$$w = \sum_{i\in I_1} \beta_i v_i$$

gilt.

Wir wollen zeigen, dass wir w auch ohne Verwendung von v_{i^*} linearkombinieren können. Falls $i^* \notin I_1$ liegt, dann ist w bereits als Linearkombination von $(v_i)_{i\in I\setminus\{i^*\}}$ dargestellt und nichts zu zeigen. Liegt andererseits $i^* \in I_1$, so ersetzen wir das Vorkommen von v_{i^*} mit Hilfe von (12.4):

$$w = \sum_{i\in I_1} \beta_i v_i = \sum_{i\in I_1\setminus\{i^*\}} \beta_i v_i + \beta_{i^*} v_{i^*} = \sum_{i\in I_1\setminus\{i^*\}} \beta_i v_i + \sum_{i\in I_0} \beta_{i^*}\alpha_i v_i.$$

Also ist w auch bereits eine Linearkombination von $(v_i)_{i\in I\setminus\{i^*\}}$, also $w \in \langle (v_i)_{i\in I\setminus\{i^*\}}\rangle$.

Aussage $(ii) \Rightarrow$ Aussage (i): Der Vektor v_{i^*} ist Mitglied der Familie $(v_i)_{i\in I}$, also gilt erst recht $v_{i^*} \in \langle (v_i)_{i\in I}\rangle$ und nach Voraussetzung $v_{i^*} \in \langle (v_i)_{i\in I\setminus\{i^*\}}\rangle$. Nach Lemma 12.5 ist also $F = (v_i)_{i\in I}$ linear abhängig. □

Das folgende Resultat stellt klar, dass die lineare Unabhängigkeit einer Menge von Vektoren äquivalent dazu ist, dass die Vektoren aus ihrer linearen Hülle eine i. W. eindeutige Darstellung als Linearkombination besitzen:

Lemma 12.7 (lineare Unabhängigkeit und eindeutige Linearkombinationen)**.**
Es sei V ein Vektorraum. Für eine Teilmenge $E \subseteq V$ bzw. für eine Familie $F = (v_i)_{i\in I}$ von Vektoren in V sind äquivalent:

(i) E ist linear unabhängig.	(i) F ist linear unabhängig.
(ii) Jeder Vektor $v \in \langle E\rangle$ lässt sich in eindeutiger Weise (bis auf Summanden mit Nullkoeffizienten) aus Vektoren der Menge E linearkombinieren.	(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 F linearkombinieren.
Sind also $$v = \sum_{v\in E_0} \alpha_v\, v = \sum_{v\in E_1} \beta_v\, v$$ zwei Darstellungen von v mit endlichen Teilmengen $E_0, E_1 \subseteq E$, dann gilt $$\begin{aligned} \alpha_v &= \beta_v \quad \text{für } v \in E_0 \cap E_1,\\ \alpha_v &= 0 \quad \text{für } v \in E_1 \setminus E_0,\\ \beta_v &= 0 \quad \text{für } v \in E_0 \setminus E_1. \end{aligned}$$	Sind also $$v = \sum_{i\in I_0} \alpha_i\, v_i = \sum_{i\in I_1} \beta_i\, v_i$$ zwei Darstellungen von v mit endlichen Teilmengen $I_0, I_1 \subseteq I$, dann gilt $$\begin{aligned} \alpha_i &= \beta_i \quad \text{für } i \in I_0 \cap I_1,\\ \alpha_i &= 0 \quad \text{für } i \in I_1 \setminus I_0,\\ \beta_i &= 0 \quad \text{für } i \in I_0 \setminus I_1. \end{aligned}$$

Beweis. Wir beweisen nur die Aussagen für Familien.

Aussage $(i) \Rightarrow$ Aussage (ii): Es sei $(v_i)_{i\in I}$ linear unabhängig und $v \in \langle (v_i)_{i\in I}\rangle$. Nach Satz 11.16 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 $v = \sum_{i\in I_0} \alpha_i\, v_i$.

Zu zeigen ist noch, dass diese Darstellung i. W. eindeutig ist. Wir nehmen dazu an, dass

$$v = \sum_{i\in I_0} \alpha_i\, v_i = \sum_{j\in I_1} \beta_j\, v_j$$

zwei Darstellungen von v als Linearkombination von $(v_i)_{i\in I}$ ist mit endlichen Indexmengen I_0 und I_1 sind. Dann ist auch $I_{01} := I_0 \cup I_1$ endlich. Wir ergänzen die Koeffizienten durch $\alpha_i := 0$ für $i \in I_1 \setminus I_0$ und $\beta_i := 0$ für $i \in I_0 \setminus I_1$. Dann haben wir

$$0 = v - v = \sum_{i\in I_{01}} \alpha_i\, v_i - \sum_{i\in I_{01}} \beta_i\, v_i = \sum_{i\in I_{01}} (\alpha_i - \beta_i)\, v_i.$$

Da nach Voraussetzung die Familie $(v_i)_{i\in I}$ linear unabhängig ist, muss $\alpha_i - \beta_i = 0$ für alle $i \in I_{01}$ gelten, also $\alpha_i = \beta_i$. Das zeigt die Behauptung.

Aussage (ii) $\Rightarrow$ Aussage (i): Es sei $I_0 \subseteq I$ eine beliebige endliche Teilmenge. Wir 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 (Lemma 12.4). □

Quizfrage 12.2: Wie könnten wir die Aussage (ii) von Lemma 12.7 mit Hilfe von Linearkombinationen der Form (11.10) formulieren?

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; Jänich, 2008, Kapitel 3

§ 13.1 Basis eines Vektorraumes

In diesem Abschnitt beantworten wir die Frage, wie wir einen Vektorraum durch eine möglichst kleine erzeugende Menge (oder erzeugende Familie) darstellen können und damit Redundanz in der Darstellung vermeiden.

Definition 13.1 (Basis).
Es sei V ein Vektorraum.

Eine Menge $B \subseteq V$ von Vektoren in V heißt eine **Basis**[26] **von** V, wenn B linear unabhängig ist und $\langle B\rangle = V$ gilt.

Eine Familie B von Vektoren aus V heißt eine **Basis von** V, wenn B linear unabhängig ist und $\langle B\rangle = V$ gilt. △

Beachte: Eine Basis ist also eine linear unabhängige erzeugende Menge bzw. eine linear unabhängige erzeugende Familie. Zur Unterscheidung sprechen wir auch von einer **Basismenge** (englisch: basic set) bzw. einer **Basisfamilie** (englisch: basic family).

Beispiel 13.2 (Basis).

[26] englisch: basis

(*i*) Die leere Menge $\emptyset$ ist die einzige Basis des Nullraumes $\{0\}$ über jedem Körper K.

(*ii*) Die Menge $E \coloneqq \left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\\sqrt{2}\end{pmatrix}, \begin{pmatrix}\sqrt{2}\\1\end{pmatrix}\right\}$ ist eine erzeugende Familie des $\mathbb{R}$-Vektorraumes $\mathbb{R}^2$, jedoch keine Basis, da sie linear abhängig ist, siehe Beispiel 12.2. 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 11.3) ist

$$\{e_1, \dots, e_n\} \text{ mit } e_i \coloneqq \begin{pmatrix}0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix} \leftarrow i\text{-ter Eintrag} \tag{13.1}$$

eine Basis, genannt die **Standardbasis** (englisch: standard basis) von K^n.

(*iv*) Es sei K ein Körper und $K^{\mathbb{N}}$ der Folgenraum über K, siehe Beispiel 11.12. Die Menge $B = \{e_j \mid j \in \mathbb{N}\}$ aller Standardfolgen ist eine Basis des Unterraumes der endlich getragenen Folgen, also $\langle B\rangle = (K^{\mathbb{N}})_{00}$, siehe Beispiel 11.17. Diese Basis wird die **Standardbasis** von $(K^{\mathbb{N}})_{00}$ genannt. △

Satz 13.3 (Charakterisierung von Basen)**.**
Es sei V ein Vektorraum. Für eine Teilmenge $B \subseteq V$ bzw. für eine Familie $B = (v_i)_{i\in I}$ von Vektoren in V sind äquivalent:

(*i*) B ist eine Basis von V.

(*ii*) B ist eine maximale linear unabhängige Teilmenge von V.[27] Das heißt: B ist linear unabhängig, und jede echte Obermenge von B ist linear abhängig.

(*iii*) B ist eine minimale erzeugende Menge von V.[28] Das heißt: B ist eine erzeugende Menge, und jede echte Teilmenge von B ist keine erzeugende Menge.

(*iv*) Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise (bis auf Summanden mit Nullkoeffizienten) aus Vektoren der

(*i*) B ist eine Basis von V.

(*ii*) B ist eine maximale linear unabhängige Teilfamilie von V.[29] Das heißt: B ist linear unabhängig, und jede echte Oberfamilie von B ist linear abhängig.

(*iii*) B ist eine minimale erzeugende Familie von V.[30] Das heißt: B ist eine erzeugende Familie, und jede echte Teilfamilie von B ist keine erzeugende Familie.

(*iv*) Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise (bis auf Summanden mit

[27] Genauer: B ist ein maximales Element bzgl. der Mengeninklusion (Definition 5.34) in der Menge der linear unabhängigen Teilmengen von V.

[28] Genauer: B ist ein minimales Element bzgl. der Mengeninklusion in der Menge der erzeugenden Mengen von V.

[29] Genauer: Die Familie B ist ein maximales Element bzgl. der Ordnungsrelation „ist Teilfamilie von“ in der Menge der linear unabhängigen Familien in V.

[30] Genauer: Die Familie B ist ein minimales Element bzgl. der Ordnungsrelation „ist Teilfamilie von“ in der Menge der erzeugender Familien von V.

Menge B linearkombinieren.

Nullkoeffizienten) aus Vektoren der Familie $(v_i)_{i\in I}$ linearkombinieren.

Beweis. Wir beweisen nur die Aussagen für Mengen.

Aussage (i) ⇒ 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 Folgerung 12.6 („Redundanz bedeutet lineare Abhängigkeit“) folgt nun, dass $B \cup \{v\}$ linear abhängig ist.

Aussage (ii) ⇒ Aussage (i): Es sei B eine maximale linear unabhängige Teilmenge von V. Zu zeigen ist, dass B ganz V erzeugt. Es sei dazu $\widetilde{v} \in V$ beliebig. Nach Definition von $\langle B\rangle$ ist klar, dass $\langle B\rangle \supseteq B$ gilt. **(Quizfrage 13.1:** Klar?) Wenn also $\widetilde{v} \in B$ ist, dann auch $\widetilde{v} \in \langle B\rangle$, was zu zeigen war. Wir können also von $\widetilde{v} \in V \setminus B$ ausgehen. Nach Voraussetzung ist $B \cup \{\widetilde{v}\}$ als echte Obermenge von B linear abhängig. Es existieren also eine endliche Teilmenge $B_0 \subseteq B$ und Koeffizienten $\alpha_v \in K$ für $v \in B_0$, sodass gilt:

$$\sum_{v\in B_0} \alpha_v v + \widetilde{\alpha}\widetilde{v} = 0,$$

wobei nicht alle Koeffizienten gleich Null sind. Insbesondere ist $\widetilde{\alpha} \neq 0$, denn sonst wäre bereits B linear abhängig, was der Voraussetzung widerspricht. Wir erhalten also

$$\widetilde{v} = -\sum_{v\in B_0} \widetilde{\alpha}^{-1}\alpha_v v,$$

d. h., $\widetilde{v}$ lässt sich in der Tat aus Elementen von B linearkombinieren. Damit ist $\langle B\rangle = V$ gezeigt.

Aussage (i) ⇒ Aussage (iii): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B\rangle = V$. Aus Folgerung 12.6 („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) ⇒ 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 Folgerung 12.6 („Redundanz bedeutet lineare Abhängigkeit“) folgt daher, dass B linear unabhängig ist, also eine Basis.

Aussage (i) ⇒ Aussage (iv): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B\rangle = V$. Aus Lemma 12.7 folgt, dass sich jedes $v \in \langle B\rangle = V$ in i. W. eindeutiger Weise aus Elementen von B linearkombinieren lässt.

Aussage (iv) ⇒ 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 12.7 folgt, dass B linear unabhängig ist, also eine Basis von V. □

Folgerung 13.4 (verschiedene Basen sind bzgl. der Inklusionshalbordnung nicht vergleichbar)**.** Es sei V ein Vektorraum.

Sind die Mengen $B_1, B_2 \subseteq V$ zwei verschiedene Basen von V, dann sind B_1 und B_2 bzgl. der Halbordnung „$\subseteq$“ nicht vergleichbar, d. h., es gilt weder $B_1 \subseteq B_2$ noch $B_2 \subseteq B_1$.

Sind $B_1 = (v_i)_{i\in I_1}$ und $B_2 = (w_i)_{i\in I_2}$ Familien von Vektoren in V und sind die Mengen ihrer Mitglieder $E_1 := \{v_i \mid i \in I_1\}$ und $E_2 := \{w_i \mid i \in I_2\}$ verschieden, dann sind E_1 und E_2

bzgl. der Halbordnung „$\subseteq$“ nicht vergleichbar, d. h., es gilt weder $E_1 \subseteq E_2$ noch $E_2 \subseteq E_1$.

Beweis. Wir führen den Beweis für Mengen. Die Annahme von $B_1 \subsetneq B_2$ oder von $B_2 \subsetneq B_1$ für zwei Basen B_1, B_2 von V widerspräche Aussage (ii) von Satz 13.3. □

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 Unterraum ist nicht der ganze Vektorraum), und einer erzeugenden Menge, die aber möglicherweise zu groß (linear abhängig) ist, immer eine Basis liegt.

Satz 13.5 (Basisergänzungssatz[31 AoC]).
Es sei V ein Vektorraum.

Es sei A eine linear unabhängige Menge von Vektoren aus V und E eine erzeugende Menge von V mit der Eigenschaft $A \subseteq E$. Dann existiert eine Basis B von V mit $A \subseteq B \subseteq E$.

Es sei $A = (v_i)_{i \in I_A}$ eine linear unabhängige Familie von Vektoren aus V und $E = (v_i)_{i \in I_E}$ eine erzeugende Familie von V mit der Eigenschaft $I_A \subseteq I_E$.[32] 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.

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 bzgl. der Mengeninklusion eine halbgeordnete Menge. Wegen $A \in \mathcal{D}$ ist $\mathcal{D} \neq \emptyset$. Ziel ist die Anwendung des Lemmas von Zorn 6.48.

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 5.34) der Teilmenge $\mathcal{C}$ in $\mathcal{D}$ ist.

Dazu zeigen wir zunächst, dass S überhaupt Element von $\mathcal{D}$ ist:

- (i) Für alle $C \in \mathcal{C} \subseteq \mathcal{D}$ gilt $A \subseteq C \subseteq E$, also auch $A \subseteq \bigcup_{C \in \mathcal{C}} C = S \subseteq E$.
- (ii) Weiter ist S linear unabhängig, denn: Es sei $\{c_1, \ldots, c_n\} \subseteq S$ 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 $\{C_1, \ldots, C_n\}$ in $\mathcal{C}$. Folglich gilt $C_i \subseteq C_k$ für alle $i = 1, \ldots, n$. Damit ist $\{c_1, \ldots, c_n\} \subseteq \bigcup_{i=1}^{n} C_i = C_k$. Dabei ist $C_k \in \mathcal{C} \subseteq \mathcal{D}$ linear unabhängig. Also ist nach Lemma 12.4 auch die Teilmenge $\{c_1, \ldots, c_n\}$ 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.

[31] englisch: basis extension theorem
[32] A ist also eine Teilfamilie von E.

Schritt 2: Das Lemma von Zorn 6.48 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 Folgerung 12.6 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 $\langle B \rangle = V$. □

Es folgen drei unmittelbare Folgerungen als Spezialfälle des Basisergänzungssatzes 13.5.

Der Fall $A = \emptyset$ und $E = V$ bzw. $A = ()$ und $E = (v)_{v \in V}$ ergibt:

Folgerung 13.6 (Basisexistenzsatz$^{\text{AoC}}$)**.**
Jeder Vektorraum V besitzt eine Basismenge.

Jeder Vektorraum V besitzt eine Basisfamilie.

Im Fall von $A = \emptyset$ bzw. $A = ()$ erhalten wir:

Folgerung 13.7 (Basisauswahlsatz$^{\text{AoC}}$)**.**
Aus jeder erzeugenden Menge E eines Vektorraumes V lässt sich eine Basis auswählen.

Aus jeder erzeugenden Familie F eines Vektorraumes V lässt sich eine Basis auswählen.

Und $E = V$ bzw. $E = (v)_{v \in V}$ führt schließlich zu:

Folgerung 13.8 (Basisergänzungssatz$^{\text{AoC}}$)**.**
Jede linear unabhängige Menge A eines Vektorraumes V kann zu einer Basismenge erweitert werden.

Jede linear unabhängige Familie A eines Vektorraumes V kann zu einer Basisfamilie erweitert werden.

Bemerkung 13.9 (zum Basisergänzungssatz 13.5)**.**

(*i*) Der Beweis des Basisergänzungssatzes 13.5 und seiner Folgerungen 13.6 bis 13.8 ist nicht konstruktiv, d. h., wir können ihn nicht zur Grundlage eines Verfahrens machen, um eine Basis zu konstruieren. Beispielsweise können wir mit Hilfe dieser Resultate keine konkrete Basis von $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum (Beispiel 11.3) konstruieren, obwohl eine solche existiert.$^{\text{AoC}}$ (**Quizfrage 13.2:** Ist eine Basis des $\mathbb{Q}$-Vektorraumes $\mathbb{R}$ abzählbar oder überabzählbar?)

(*ii*) Wenn der Vektorraum V jedoch endlich erzeugt ist, wenn es also eine endliche erzeugende Menge oder Familie gibt, dann lässt sich der Basisergänzungssatz 13.5 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. Das heißt, auch die Folgerungen 13.6 bis 13.8 benötigen in diesem Fall das Auswahlaxiom nicht. △

Lemma 13.10 (Basis endlicher kartesischer Produkte)**.**

Es seien K ein Körper und $n \in \mathbb{N}_0$. Weiter sei $V := \bigtimes_{j=1}^{n} V_j$ der Produktraum der K-Vektorräume $V_1, \dots, V_n$.

Ist B_j eine Basismenge von V_j für $j = 1, \dots, n$, dann ist

$$\bigcup_{j=1}^{n} \{(0, \dots, 0, \underbrace{v}_{\text{Position } j \text{ im Tupel}}, 0, \dots, 0) \mid v \in B_j\}$$

eine Basismenge von V.

Ist $B_j = (v_i)_{i \in I_j}$ eine Basisfamilie von V_j für $j = 1, \dots, n$, dann ist

$$\Big\|_{j=1}^{n} (0, \dots, 0, \underbrace{v_i}_{\text{Position } j \text{ im Tupel}}, 0, \dots, 0)_{i \in I_j}$$

eine Basisfamilie von V.

(**Quizfrage 13.3:** Gilt ein ähnliches Resultat auch für unendliche Produkte von Vektorräumen?)

Beweis. □

§ 13.2 Dimension eines Vektorraumes

Wir kommen nun zum wichtigen Begriff der Dimension, der in gewissem Sinne die „Größe“ eines Vektorraumes beschreibt.

Definition 13.11 (Dimension eines Vektorraumes)**.**
Es sei V ein Vektorraum.

(i) Wenn V eine endliche Basismenge B der Kardinalität $n \in \mathbb{N}_0$ besitzt, so sagen wir, V habe **endliche Dimension**[33], genauer: die **Dimension**[34] n, in Symbolen: $\dim(V) = n$.

(ii) Wenn V keine endliche Basismenge besitzt, so sagen wir, V habe **unendliche Dimension**[35], in Symbolen: $\dim(V) = \infty$.

(i) Wenn V eine endliche Basisfamilie $B = (v_i)_{i \in I}$ mit $n \in \mathbb{N}_0$ Mitgliedern besitzt, so sagen wir, V habe **endliche Dimension**, genauer: die **Dimension** n, in Symbolen: $\dim(V) = n$.

(ii) Wenn V keine endliche Basisfamilie besitzt, so sagen wir, V habe **unendliche Dimension**, in Symbolen: $\dim(V) = \infty$. △

Zur Verdeutlichung, welcher Körper K verwendet wird, schreiben wir manchmal auch $\dim_K(V)$. Beispielsweise gilt $\dim_{\mathbb{R}}(\mathbb{R}) = 1$, aber $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$.

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 endliche Basismenge besitzt, alle seine Basismengen endlich sind, und zwar alle mit dieselben Kardinalität (Bemerkung 13.15).

Lemma 13.12 (Austauschlemma)**.**

[33] englisch: finite dimension
[34] englisch: dimension
[35] englisch: infinite dimension

Es sei V ein Vektorraum über dem Körper K.

Die endliche Menge $B = \{v_1, \dots, v_n\}$ sei eine Basis von V und $\#B = n \in \mathbb{N}_0$.[36] Ist $w = \sum_{i=1}^n \alpha_i v_i$ mit Koeffizienten $\alpha_i \in K$ und gilt $\alpha_j \neq 0$ für den Index $j \in [\![1, n]\!]$, dann ist auch $B_0 := \{v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_n\}$ eine Basis von V.

Die endliche Familie $B = (v_1, \dots, v_n)$ sei eine Basis von V mit $n \in \mathbb{N}_0$. Ist $w = \sum_{i=1}^n \alpha_i v_i$ mit Koeffizienten $\alpha_i \in K$ und gilt $\alpha_j \neq 0$ für den Index $j \in [\![1, n]\!]$, dann ist auch $B_0 := (v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_n)$ eine Basis von V.

Beweis. Wir führen den Beweis für Mengen.

Da es bei einer Basismenge auf die Reihenfolge der Elemente nicht ankommt, nehmen wir aus Bequemlichkeit und o. B. d. A. an, dass $j = 1$ ist. Aus $w = \sum_{i=1}^n \alpha_i v_i$ mit $\alpha_1 \neq 0$ folgt

$$v_1 = \alpha_1^{-1}\Big(w - \sum_{i=2}^n \alpha_i v_i\Big). \tag{13.2}$$

Schritt 1: Wir zeigen: $\langle B_0 \rangle = V$.

Es sei dazu $v \in V$. Da B eine Basismenge 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 (13.2) folgt

$$\begin{aligned} v &= \beta_1 \alpha_1^{-1}\Big(w - \sum_{i=2}^n \alpha_i v_i\Big) + \sum_{i=2}^n \beta_i v_i \\ &= \beta_1 \alpha_1^{-1} w - \beta_1 \alpha_1^{-1} \sum_{i=2}^n \alpha_i v_i + \sum_{i=2}^n \beta_i v_i \quad \text{nach Distributivgesetz (10.1a) in } K \\ &= \beta_1 \alpha_1^{-1} w + \sum_{i=2}^n \big(\beta_i - \beta_1 \alpha_1^{-1} \alpha_i\big) v_i \end{aligned}$$

nach Kommutativgesetz und Distributivgesetz (10.1b). 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

$$\beta_1 \alpha_1 = 0 \quad \text{und} \quad \beta_1 \alpha_i + \beta_i = 0 \text{ für } i = 2, \dots, n.$$

[36] Das heißt also, dass die Vektoren $v_1, \dots, v_n$ paarweise verschieden sind.

Wegen $\alpha_1 \neq 0$ muss $\beta = 0$ sein, woraus dann weiter $\beta_2 = \ldots = \beta_n = 0$ folgt. Das heißt aber, dass $B_0 = \{w, v_2, \ldots, v_n\}$ linear unabhängig ist. □

Satz 13.13 (**Austauschsatz von Steinitz**[37]).
Es sei V ein Vektorraum.

Die endliche Menge $B = \{v_1, \ldots, v_n\}$ sei eine Basis von V mit $\#B = n \in \mathbb{N}_0$. Ist $A = \{a_1, \ldots, a_m\}$ eine weitere 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 $\#B_0 = n$.

Die endliche Familie $B = (v_1, \ldots, v_n)$ sei eine Basis von V mit $n \in \mathbb{N}_0$. Ist $A = (a_1, \ldots, a_m)$ eine weitere linear unabhängige Familie in V mit $m \in \mathbb{N}_0$, dann gilt:

(*i*) $m \leqslant n$.

(*ii*) Es gibt eine Teilfamilie D von B mit $(n-m)$ Mitgliedern, sodass $B_0 := A \,\|\, D$ ebenfalls eine Basis von V ist. B_0 hat n Mitglieder.

Beweis. Wir führen den Beweis für Mengen, und zwar mit Hilfe vollständiger Induktion nach der Mächtigkeit $m = \#A \in \mathbb{N}_0$. 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 $\{a_1, \ldots, a_m\}$ linear unabhängig ist, ist auch $\{a_1, \ldots, a_{m-1}\}$ linear unabhängig. Nach Induktionsannahme gilt $m - 1 \leqslant n$, und es existiert $D = \{v_{i_m}, \ldots, v_{i_n}\} \subseteq B$, sodass $B_1 := \{a_1, \ldots, a_{m-1}, v_{i_m}, \ldots, v_{i_n}\}$ eine Basis von V ist.

Falls nun $m - 1 = n$ wäre, also $D = \emptyset$, dann wäre bereits $\{a_1, \ldots a_{m-1}\}$ eine Basis von V. Nach dem Satz 13.3 über die Charakterisierung von Basen hieße das aber, dass $\{a_1, \ldots a_m\}$ 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, $j = 1, \ldots n$, sodass gilt:

$$a_m = \sum_{j=1}^{m-1} \alpha_j \, a_j + \sum_{j=m}^{n} \alpha_j \, v_{i_j}.$$

Wären alle $\alpha_m = \alpha_{m+1} = \ldots \alpha_n = 0$, so würde das die lineare Abhängigkeit von $A = \{a_1, \ldots, a_m\}$ zeigen, im Widerspruch zur Voraussetzung. Demzufolge gibt es einen Index $j \in [\![m, n]\!]$ mit $\alpha_j \neq 0$. Nach dem Austauschlemma 13.12 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. □

[37] englisch: Steinitz exchange theorem

Folgerung 13.14 (endliche Basen sind gleichmächtig)**.**
Es sei V ein Vektorraum.

(*i*) Wenn V endlich erzeugt ist, dann ist jede Basismenge von V endlich, und alle Basismengen sind gleichmächtig.

(*ii*) Wenn V nicht endlich erzeugt ist, dann ist jede Basismenge von V unendlich.

(*i*) Wenn V endlich erzeugt ist, dann ist jede Basisfamilie von V endlich, und alle Basisfamilien sind gleichmächtig.

(*ii*) Wenn V nicht endlich erzeugt ist, dann ist jede Basisfamilie von V unendlich.

Beweis. Wir führen den Beweis für Mengen.

Aussage (*i*): Wenn V endlich erzeugt ist, dann gibt es eine endliche erzeugende Menge und nach Basisergänzungssatz 13.5 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 13.13 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 insbesondere B eine endliche erzeugende Menge des Vektorraumes V. Der Vektorraum V wäre damit endlich erzeugt, im Widerspruch zur Voraussetzung. □

Bemerkung 13.15 (Dimensionsbegriff für Vektorräume)**.**

(*i*) Folgerung 13.14 zeigt, dass der Dimensionsbegriff aus Definition 13.11 wohldefiniert ist, wobei wir der Einfachheit halber nicht zwischen verschiedenen Unendlichkeiten unterschieden haben. Sogar für unendlich-dimensionale Vektorräume gilt aber, dass je zwei Basen gleichmächtig sind.[AoC] Daher könnten wir für die Dimension von Vektorräumen genauer auch Kardinalzahlen (Definition 6.31) verwenden und dadurch verschiedene Unendlichkeiten unterscheiden.

(*ii*) Der Beweis von Folgerung 13.14 verwendet den Basisergänzungssatz 13.5, jedoch nur die Version für endlich-dimensionale (endlich erzeugte) Vektorräume, die ohne das Zornsche Lemma und damit ohne das Auswahlaxiom auskommt. △

Beispiel 13.16 (Dimension eines Vektorraumes)**.**

(*i*) Der als „Standardvektorraum K^n der Dimension n“ bezeichnete Vektorraum über einem Körper K (Beispiel 11.3) hat tatsächlich die Dimension $n \in \mathbb{N}_0$, da die Standardbasis $\{e_1, \ldots, e_n\}$ bzw. $(e_1, \ldots, e_n)$ die n paarweise verschiedenen Elemente bzw. Mitglieder hat (Beispiel 13.2).

(*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 Basismenge für den $\mathbb{R}$-Vektorraum $\mathbb{C}$ ist $\{1, i\}$.

(*iv*) Der Nullraum $\{0\}$ ist über jedem Körper der einzige Vektorraum der Dimension 0.

(*v*) Der Folgenraum $K^{\mathbb{N}}$ über einem Körper K hat unendliche Dimension. Auch der Unterraum $(K^{\mathbb{N}})_{00}$ der endlich getragenen Folgen hat unendliche Dimension, da die (abzählbar) unendliche Menge B aller Standardfolgen eine Basis von $(K^{\mathbb{N}})_{00}$ bildet (Beispiel 11.17).

Der Unterraum der Folgen, deren Träger in $[\![1, n]\!]$ liegt, hat Dimension n, da die Standardfolgen $\{e_1, \ldots, e_n\}$ eine Basis bilden. △

Folgerung 13.17 (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 Menge, 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.

(*i*) Ist $A = (v_i)_{i \in I}$ eine linear unabhängige Familie in V, dann gilt $\#I \leqslant n$.

(*ii*) Eine Familie $A = (v_i)_{i \in I}$ in V ist genau dann eine Basis von V, wenn A linear unabhängig ist und $\#I \leqslant n$ gilt.

(*iii*) Für jeden Unterraum U von V gilt: $0 \leqslant \dim(U) \leqslant \dim(V)$.

(*iv*) Für jeden Unterraum U von V ist $U = V$ genau dann, wenn $\dim(U) = \dim(V)$ gilt.

Beweis. Wir führen den Beweis für Mengen.

Aussage (*i*): Nach Basisergänzungssatz 13.5 existiert eine Basis B von V mit $A \subseteq B$. Nach Folgerung 13.14 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 13.14 gilt $\#A = \dim(V) = n$. Ist umgekehrt A linear unabhängig und $\#A = n$, so gilt für jede Basis $B \supseteq A$ von V einerseits $\#B \geqslant \#A$, andererseits 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 $U = \langle A \rangle = V$. □

Lemma 13.18 (Dimension des endlichen kartesischen Produkts endlich-dimensionaler Vektorräume)**.**
Es seien K ein Körper und $V_1, \ldots, V_n$ K-Vektorräume endlicher Dimension für $n \in \mathbb{N}_0$. Dann besitzt das kartesische Produkt (Definition 11.4) die Dimension

$$\dim\Big(\bigtimes_{i=1}^{n} V_i\Big) = \sum_{i=1}^{n} \dim(V_i). \tag{13.3}$$

Beweis. Das Resultat folgt sofort aus Lemma 13.10, weil sich die Kardinalität einer Basis von $\bigtimes_{i=1}^{n} V_i$ als Summe der Kardinalitäten der Basen von V_i, $i = 1, \ldots, n$, ergibt. □

Abschließend betrachten wir die Frage, wieviele Elemente (Vektoren) ein Vektorraum besitzt.

Bemerkung 13.19 (Mächtigkeit von Vektorräumen)**.**
Es sei V ein Vektorraum über einem Körper K.

(*i*) Hat der Vektorraum V unendliche Dimension, dann besitzt er auch unendliche viele Elemente, denn jede Basis von V hat ja bereits unendlich viele Elemente.

(*ii*) Gilt $\dim(V) = 0$, dann gilt $V = \{0\}$, V hat also genau ein Element, und zwar unabhängig vom Körper K.

(*iii*) Gilt $\dim(V) \in \mathbb{N}$, dann kommt es auf die Mächtigkeit des Körpers K an: Ist K endlich, dann besteht der Raum V aus genau $(\#K)^{\dim(V)}$ verschiedenen Vektoren. Ist K dagegen unendlich, dann ist auch V unendlich. △

Ende der Vorlesung 17

§ 14 Summen von Unterräumen

Literatur: Bosch, 2014, Kapitel 1; Fischer, Springborn, 2020, Kapitel 2.6

§ 14.1 Summen von zwei Unterräumen

Aus Lemma 11.14 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.[38]

Statt $U \cup W$ können wir aber den kleinsten Unterraum von V betrachten, der $U \cup W$ enthält, also den von $U \cup W$ erzeugten Unterraum $\langle U \cup W \rangle$:

Lemma 14.1 (die lineare Hülle der Vereinigung zweier Unterräume ist die Summe, vgl. Folgerung 7.52 für Gruppen)**.**
Es seien V ein Vektorraum und U, W zwei Unterräume von V. Dann gilt

$$\langle U \cup W \rangle = U + W. \tag{14.1}$$

Die Menge $U + W$ ist zu verstehen im Sinne der Bemerkung 7.20, also als $U + W = \{u + w \mid u \in U,\ w \in W\}$. $U + W$ heißt die **Summe der Unterräume** U und W (englisch: sum of two subspaces).

Beweis. Aus Satz 11.16 wissen wir, dass $M := \langle U \cup W \rangle$ übereinstimmt mit der Menge aller Linearkombinationen von $U \cup W$. Wir zeigen nun in zwei Schritten, dass $M = U + W$ gilt.

Schritt 1: In der Tat sind die Elemente $u + w$ von $U + W$ auch Linearkombinationen von $U \cup W$, nämlich $1u + 1w$. Also gilt $U + W \subseteq M$.

[38] Tatsächlich gilt: $U \cup W$ ist genau dann ein Unterraum, wenn $U \subseteq W$ oder $W \subseteq U$ gilt (Übung). Ein analoges Resultat gilt auch für Untergruppen (Übung), Unterringe und Unterkörper.

Schritt 2: Ist umgekehrt $v \in M$, dann hat v als Linearkombination von $U \cup W$ eine Darstellung der Form

$$v = \sum_{u \in U_0} \alpha_u \, u + \sum_{w \in W_0} \beta_w \, w$$

mit endlichen Teilmengen $U_0 \subseteq U$ und $W_0 \subseteq W$ und Koeffizienten $\alpha_u, \beta_w \in K$. 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 $M \subseteq U + W$. □

Bemerkung 14.2 („Unterraum sein" ist eine Ordnungsrelation, vgl. Bemerkung 10.9 zu Unterkörpern)**.**

(*i*) Die Relation „ist Unterraum von" ist eine partielle Ordnung auf der Klasse aller Vektorräume (über beliebigen Körpern).

(*ii*) Insbesondere ist die Menge aller Unterräume eines bestimmten Vektorraumes V durch die Unterraumhalbordnung partiell geordnet. Diese Ordnung stimmt mit der Inklusionshalbordnung überein.

(*iii*) Für Unterräume U und W von V ist $U \cap W$ das Infimum von $\{U, W\}$ (Definition 5.34) und $U + W$ das Supremum von $\{U, W\}$. Genau dann, wenn $U \subseteq W$ oder $W \subseteq U$ gilt, ist das Infimum von $\{U, W\}$ ein Minimum und das Supremum ein Maximum von $\{U, W\}$. (**Quizfrage 14.1:** Wie lauten entsprechende Aussagen für Untergruppen, Unterringe und Unterkörper?) △

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

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W). \tag{14.2}$$

Beweis. $U \cap W$ ist ebenfalls ein endlich-dimensionaler Unterraum von V, besitzt also eine endliche Basisfamilie $(v_1, \ldots, v_m)$ mit $m = \dim(U \cap W) \in \mathbb{N}_0$. Nach dem Basisergänzungssatz 13.5 kann diese Basis einerseits zu einer Basis von U und andererseits zu einer Basis von W ergänzt werden. Es gibt also eine Familie $(u_1, \ldots, u_k)$ von Vektoren in U und eine Familie $(w_1, \ldots, w_\ell)$ von Vektoren in W mit $k, \ell \in \mathbb{N}_0$, sodass

$$\begin{aligned} B_U &:= (v_1, \ldots, v_m, \; u_1, \ldots, u_k) && \text{Basis von } U \\ \text{und} \quad B_W &:= (v_1, \ldots, v_m, \; w_1, \ldots, w_\ell) && \text{Basis von } W \end{aligned}$$

ist. Wir zeigen nun, dass $B := (v_1, \ldots, v_m, \; u_1, \ldots, u_k, \; w_1, \ldots, w_\ell)$ eine Basis von $U + W$ ist.

Offenbar ist B eine erzeugende Familie 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 $u := \sum_{i=1}^{m} \alpha_i \, v_i + \sum_{i=1}^{k} \beta_i \, u_i \in U$, 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 12.7) folgt $\beta_1 = \dots = \beta_k = 0$. Es gilt 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 $\alpha_1 = \dots = \alpha_m = 0$ und $\gamma_1 = \dots = \gamma_\ell = 0$. Das zeigt die lineare Unabhängigkeit von B, also ist B tatsächlich eine Basis von $U + W$.

Die Behauptung (14.2) folgt nun aus

$$\underbrace{m + k + \ell}_{\dim(U+W)} = \underbrace{m + k}_{\dim(U)} + \underbrace{m + \ell}_{\dim(W)} - \underbrace{m.}_{\dim(U\cap W)} \qquad \square$$

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

$$U = \langle e_1, e_3, e_4, e_6 \rangle \quad \text{und} \quad W = \langle e_2, e_4, e_5 \rangle$$

des Vektorraumes V der Folgen mit Träger in $[\![1, 6]\!]$ über einem beliebigen Körper $(K, +, \cdot)$ gilt

$$U + W = \langle e_1, e_2, e_3, e_4, e_5, e_6 \rangle = V \quad \text{und} \quad U \cap W = \langle e_4 \rangle.$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U + W)}_{6} = \underbrace{\dim(U)}_{4} + \underbrace{\dim(W)}_{3} - \underbrace{\dim(U \cap W)}_{1}. \qquad \triangle$$

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 dem Fall schreiben wir auch $U \oplus W$. △

Beispiel 14.6 (direkte Summe von zwei Unterräumen)**.**
Von den Beispielen 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*) ⇒ Aussage (*ii*): $V = U \oplus W$ heißt insbesondere $V = U + W$. Für gegebenes $v \in V$ gibt es also Vektoren $u_1 \in U$ und $w_1 \in W$, sodass $v = u_1 + w_1$ gilt. Gilt nun ebenfalls $v = u_2 + w_2$ für $u_2 \in U$ und $w_2 \in W$, dann gilt

$$u_1 - u_2 = w_2 - w_1 \in U \cap W = \{0\}$$

nach Voraussetzung. Daher muss $u_1 = u_2$ und $w_1 = w_2$ sein.

Aussage (*ii*) ⇒ Aussage (*i*): Aus der Voraussetzung folgt sofort $V = U + W$. Zu zeigen ist $U \cap W = \{0\}$.

Für $v \in U \cap W$ folgt aus

$$\begin{aligned} v &= v + 0 && \text{mit } v \in U,\ 0 \in W \\ v &= 0 + v && \text{mit } 0 \in U,\ v \in W \end{aligned}$$

und der Eindeutigkeit der Zerlegung, dass $v = 0$ sein muss, also gilt tatsächlich $U \cap W = \{0\}$.

Aussage (*i*) ⇒ 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*) ⇒ Aussage (*i*): Es gilt

$$\begin{aligned} \dim(V) &= \dim(U) + \dim(W) && \text{nach Voraussetzung} \\ &= \dim(U + W) + \dim(U \cap W) && \text{nach Dimensionsformel (14.2)} \\ &= \dim(U + W) + 0 && \text{nach Voraussetzung.} \end{aligned}$$

$U + W$ ist also ein Unterraum von V maximaler Dimension und damit identisch zu V. Außerdem zeigt $\dim(U \cap W) = 0$, dass $U \cap W = \{0\}$ gilt, siehe Beispiel 13.16. □

Satz 14.8 (direkte Summe von zwei Unterräumen und disjunkte Zerlegung einer Basis)**.**
Es sei V ein Vektorraum. Dann gilt:

(*i*) Ist B eine Basismenge von V und bilden die Mengen B_1, B_2 eine disjunkte Zerlegung[39] von B in Teilmengen, dann gilt $V = \langle B_1\rangle \oplus \langle B_2\rangle$.

(*ii*) Sind U_1, U_2 Unterräume von V mit zugehörigen Basismengen B_1, B_2 und gilt $V = U_1 \oplus U_2$, so ist $B_1 \cup B_2$ eine Basismenge von V.

(*i*) Ist $B = (v_i)_{i\in I}$ eine Basisfamilie von V und bilden die Mengen I_1, I_2 eine disjunkte Zerlegung von I, dann gilt $V = \langle B_1\rangle \oplus \langle B_2\rangle$ für die Teilfamilien $B_1 := (v_i)_{i\in I_1}$ und $B_2 := (v_i)_{i\in I_2}$.

(*ii*) Sind U_1, U_2 Unterräume von V mit zugehörigen Basisfamilien B_1, B_2 und gilt $V = U_1 \oplus U_2$, so ist $B_1 \parallel B_2$ eine Basisfamilie on V.

Beweis. Wir führen den Beweis für Mengen.

Aussage (*i*): Wir zeigen zunächst $V = \langle B_1\rangle + \langle B_2\rangle$. Es gilt

$$\begin{aligned} V &= \langle B\rangle && B \text{ ist Basis von } V\\ &= \langle B_1 \cup B_2\rangle && \text{nach Voraussetzung}\\ &= \big\langle \langle B_1\rangle \cup \langle B_2\rangle\big\rangle && \text{nach Folgerung 11.18}\\ &= \langle B_1\rangle + \langle B_2\rangle && \text{nach Lemma 14.1}\\ &\subseteq V. \end{aligned}$$

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 $\widetilde{v} \in \langle B_1\rangle \cap \langle B_2\rangle$ an, d. h. es gilt

$$\widetilde{v} = \sum_{v\in B_{1,0}} \alpha_v\, v = \sum_{v\in B_{2,0}} \beta_v\, v$$

für geeignete endliche Teilmengen $B_{1,0} \subseteq B_1$ und $B_{2,0} \subseteq B_2$ und Koeffizienten α_v, β_v. Es folgt

$$0 = \sum_{v\in B_{1,0}} \alpha_v\, v + \sum_{v\in B_{2,0}} (-\beta_v)\, v.$$

Da $B = B_1 \cup B_2$ eine Basis ist, ist auch die Teilmenge $B_{1,0} \cup B_{2,0}$ linear unabhängig. Wegen $B_1 \cap B_2 = \emptyset$ gilt auch $B_{1,0} \cap B_{2,0} = \emptyset$, also sind die beteiligten Vektoren paarweise verschieden. Daraus folgt $\alpha_v = 0$ für alle $v \in B_{1,0}$ und $\beta_v = 0$ für alle $v \in B_{2,0}$. Das heißt aber $\widetilde{v} = 0$ und damit $\langle B_1\rangle \cap \langle B_2\rangle = \{0\}$.

Aussage (*ii*): Es seien nun U_1, U_2 Unterräume von V mit Basismengen 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

$$\begin{aligned} \langle B_1 \cup B_2\rangle &= \big\langle \langle B_1\rangle \cup \langle B_2\rangle\big\rangle && \text{nach Folgerung 11.18}\\ &= \langle U_1 \cup U_2\rangle && \text{da } B_1 \text{ Basis von } U_1 \text{ und } B_2 \text{ Basis von } U_2 \text{ ist}\\ &= U_1 + U_2 && \text{nach Lemma 14.1}\\ &= V && \text{nach Voraussetzung.} \end{aligned}$$

[39] Wir benutzen nicht das Wort „Partition“ (Definition 5.24), da $B_1 = \emptyset$ oder $B_2 = \emptyset$ erlaubt ist.

Um die lineare Unabhängigkeit von $B_1 \cup B_2$ zu zeigen, sei nun $B_0 \subseteq B_1 \cup B_2$ eine endliche Teilmenge. Wir können B_0 als disjunkte Zerlegung $B_0 = B_{1,0} \cup B_{2,0}$ schreiben, wobei $B_{1,0} \subseteq B_1$ und $B_{2,0} \subseteq B_2$ endliche Teilmengen sind. Wir betrachten nun die Linearkombination

$$\sum_{v \in B_{1,0}} \alpha_v v + \sum_{v \in B_{2,0}} \beta_v v = 0 \quad \text{bzw.} \quad u_1 := \sum_{v \in B_{1,0}} \alpha_v v = \sum_{v \in B_{2,0}} (-\beta_v) v =: u_2.$$

Dabei gehört u_1 zu U_1 und u_2 zu U_2. Wegen $U_1 \cap U_2 = \{0\}$ folgt $u_1 = u_2 = 0$, beide Linearkombinationen ergeben also den Nullvektor. Da aber B_1 und B_2 als Basen linear unbhängig sind, folgt weiter $\alpha_v = 0$ für alle $v \in B_{1,0}$ und $\beta_v = 0$ für alle $v \in B_{2,0}$. Damit ist gezeigt, dass $B_1 \cup B_2$ in der Tat linear unabhängig ist. □

Wir halten die Situation aus Satz 14.8, bei der zwei Unterräume in direkter Summe den ganzen Raum ergeben, in folgender Definition fest:

Definition 14.9 (komplementärer Unterraum, Kodimension)**.**
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. Im Fall $U = V$ jedoch ist der einzige zu U komplementäre Unterraum der Nullraum $\{0\}$, und im Fall $U = \{0\}$ ist der einzige zu U komplementäre Unterraum der Raum V selbst.

Beachte: Die Kodimension von U in V ist wohldefiniert$^{\text{AoC}}$, denn sind W_1 und W_2 zwei zu U komplementäre Unterräume von V, dann gibt es nach dem Basisexistenzsatz 13.6$^{\text{AoC}}$ zugehörige Basisfamilien B_0 von U bzw. B_1 von W_1 und B_2 von W_2, sodass die Konkatenation $B_0 \parallel B_1$ bzw. $B_0 \parallel B_2$ jeweils eine Basisfamilie von V ist (Satz 14.8). Da alle Basen von V gleichmächtig sind (Bemerkung 13.15$^{\text{AoC}}$), folgt, dass B_1 und B_2 gleichmächtig sind.

Folgerung 14.10 (Existenz eines komplementären Unterraumes$^{\text{AoC}}$)**.**
Es seien V ein Vektorraum und U ein Unterraum von V. Dann existiert ein weiterer Unterraum W von V, sodass $V = U \oplus W$ gilt. Es gilt[40]

$$\dim(V) = \dim(U) + \dim(W) = \dim(U) + \operatorname{codim}(U). \tag{14.3}$$

Beweis. Es sei $(v_i)_{i \in I_U}$ eine Basisfamilie von U. Aus dem Basisergänzungssatz 13.5 folgt die Existenz einer Oberfamilie $(v_i)_{i \in I_B}$, die eine Basis von V ist. Dann ist die Familie $(v_i)_{i \in I_B \setminus I_U}$ linear unabhängig, und $W := \langle B_W \rangle$ ist W nach Satz 14.8 ein Unterraum mit der gesuchten Eigenschaft.

Die Dimensionsformel (14.3) folgt direkt aus der Addition der Kardinalitäten der Indexmengen dieser Basen. □

[40] Hierbei gilt $\infty + k = k + \infty = \infty + \infty = \infty$ für $k \in \mathbb{N}_0$.

Folgende Konstellationen sind für komplementäre Unterräume $U \oplus W = V$ möglich:

$\dim(U)$	$\dim(W)$	$\dim(V)$
endlich	endlich	endlich
∞	endlich	∞
endlich	∞	∞
∞	∞	∞

In endlich-dimensionalen Räumen können wir eine Version von Folgerung 14.10 formulieren, deren Beweis ohne das Auswahlaxiom auskommt:

Folgerung 14.11 (Kodimension in endlich-dimensionalen Vektorräumen)**.**
Es seien V ein endlich-dimensionaler Vektorraum und U ein Unterraum von V. Dann existiert ein weiterer Unterraum W von V, sodass $V = U \oplus W$ gilt. Es gilt

$$\operatorname{codim}(U) = \dim(V) - \dim(U). \tag{14.4}$$

Beweis. Einen zu U komplementären Unterraum W können wir wie in Bemerkung 13.9 ohne Verwendung des Auswahlaxioms durch Ergänzung einer Basis von U zu einer Basis von V konstruieren. Nach Satz 14.7 gilt

$$\dim(V) = \dim(U) + \dim(W) = \dim(U) + \operatorname{codim}(U). \qquad \square$$

Beispiel 14.12 (komplementärer Unterraum)**.**

(*i*) In $\mathbb{R}^2$ ist jeder eindimensionale Unterraum W, der nicht identisch mit $U := \left\langle \binom{1}{1} \right\rangle$ ist, ein Komplement von U in $\mathbb{R}^2$.

(*ii*) Wir betrachten den Folgenraum $K^{\mathbb{N}}$ über einem Körper K und den Unterraum $U = (K^{\mathbb{N}})_{00}$ der endlich getragenen Folgen. Die zu U komplementären Unterräume haben keine einfache Beschreibung. (**Quizfrage 14.3:** Warum bilden — was man annehmen könnte — die nicht endlich getragenen Folgen plus die Nullfolge keinen solchen komplementären Unterraum?) $\triangle$

§ 14.2 Summen von Familien von Unterräumen

Wir beschäftigen uns abschließend in Erweiterung von § 14.1 noch mit Summen von einer beliebigen Anzahl von Unterräumen eines Vektorraumes.

Definition 14.13 (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

$$\sum_{i\in I} U_i := \left\langle \bigcup_{i\in I} U_i \right\rangle \tag{14.5}$$

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 (14.5) heißt **direkt** (englisch: direct sum), wenn gilt:

$$U_j \cap \sum_{i\in I\setminus\{j\}} U_i = \{0\} \quad \text{für alle } j \in I. \tag{14.6}$$

In dem Fall schreiben wir auch $\bigoplus_{i\in I} U_i$ und speziell im Fall $I = [\![1, n]\!]$ auch $U_1 \oplus \cdots \oplus U_n$ oder $\bigoplus_{i=1}^n U_i$. △

Beispiel 14.14 (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 13.2, gilt

$$K^n = \bigoplus_{i=1}^n \langle e_i \rangle.$$

(*ii*) Für den Raum der endlich getragenen Folgen $(K^{\mathbb{N}})_{00}$ über einem Körper K gilt

$$(K^{\mathbb{N}})_{00} = \bigoplus_{j\in\mathbb{N}} \langle e_j \rangle.$$ △

Bemerkung 14.15 (Summe einer Familie von Unterräumen)**.**

(*i*) Die Summe einer nichtleeren Familie $(U_i)_{i\in I}$ von Unterräumen hat die folgenden Darstellungen:

$$\sum_{i\in I} U_i = \bigcup \left\{ \sum_{i\in I_0} U_i \,\middle|\, I_0 \subseteq I \text{ ist eine endliche Teilmenge} \right\} \tag{14.7a}$$

$$= \left\{ \sum_{i\in I_0} u_i \,\middle|\, I_0 \subseteq I \text{ ist eine endliche Teilmenge und } u_i \in U_i \text{ für alle } i \in I_0 \right\}. \tag{14.7b}$$

Die Elemente von $\sum_{i\in I} U_i$ haben also jeweils eine Darstellung der Form $u_{i_1} + u_{i_2} + \cdots + u_{i_n}$ für $i_j \in I$, $j = 1, \ldots, n \in \mathbb{N}_0$. (**Quizfrage 14.4:** Ist klar, dass die rechte Seite von (14.7a) überhaupt ein Unterraum ist?)

(*ii*) Im Fall $\#I = 2$ stimmt die Bedingung (14.6) für die Direktheit der Summe einer Familie von Unterräumen überein mit Definition 14.5. Im Fall $\#I > 2$ reicht es jedoch für die Direktheit der Summe nicht aus, dass an Stelle von (14.6) nur paarweise $U_i \cap U_j = \{0\}$ für $i \neq j$ gefordert wird.

Betrachte zum Beispiel die Unterräume

$$U_1 = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle, \quad U_2 = \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle \quad \text{und} \quad U_3 = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle.$$

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 14.16 (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 Teilmenge $I_0 \subseteq I$ 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 der Übung. □

Satz 14.17 (direkte Summe von Unterräumen und disjunkte Zerlegung einer Basis, vgl. Satz 14.8)**.**

Es sei V ein Vektorraum. Dann gilt:

(*i*) Ist B eine Basismenge von V und bilden die Mengen B_i, $i \in I$, eine disjunkte Zerlegung von B in Teilmengen 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 Basismengen B_i, $i \in I$, und gilt $V = \bigoplus_{i\in I} U_i$, so ist $\bigcup_{i\in I} B_i$ eine Basismenge von V.

(*i*) Ist $B = (v_i)_{i\in I}$ eine Basisfamilie von V und bilden die Mengen I_j, $j \in J$, eine disjunkte Zerlegung von I mit nichtleerer Indexmenge J, dann gilt $V = \bigoplus_{j\in J}\langle B_j\rangle$ für die Teilfamilien $B_j := (v_i)_{i\in I_j}$.

(*ii*) Ist $(U_i)_{i\in I}$ eine nichtleere Familie von Unterräumen von V mit Basisfamilien B_i, $i \in I$, und gilt $V = \bigoplus_{i\in I} U_i$, so ist die Konkatenation $\Big\|_{i\in I} B_i$ der Familien B_i, $i \in I$, eine Basisfamilie von V.

Beweis. Der Beweis ist Gegenstand der Übung. □

Ende der Vorlesung 18

Ende der Woche 9

Kapitel 4 Matrizen und lineare Abbildungen

§ 15 Matrizen

Literatur: Fischer, Springborn, 2020, Kapitel 3.7; Bosch, 2014, Kapitel 3; Deiser, 2024b, Kapitel 3.3; Jänich, 2008, Kapitel 4.2 und 5.1–5.5

Matrizen sind ein universelles Mittel zur Darstellung verschiedener Sachverhalte, beispielsweise zur Beschreibung von Graphen, zur Erfassung von Rohstoffbedarfen in der Produktionsplanung, zur Darstellung chemischer Reaktionen und zur ersten Formulierung der Quantenmechanik in der Physik. Wir werden Matrizen in erster Linie zur Beschreibung linearer Abbildungen verwenden, das sind die Homomorphismen zwischen Vektorräumen.[1] Diese Bedeutung stellen wir aber bis § 19 zurück und betrachten Matrizen zunächst als eigenständiges Thema.

Definition 15.1 (Matrix)**.**
Es seien $(K, +, \cdot)$ ein Körper und $m, n \in \mathbb{N}_0$.

(*i*) Eine **Matrix** (englisch: matrix) **der Dimension** $n \times m$ (sprich: „n mal m“ oder „n Kreuz m“) oder eine $n \times m$**-Matrix** A **über dem Körper** K ist eine endliche, doppelt indizierte Familie in K mit der Indexmenge $[\![1, n]\!] \times [\![1, m]\!]$.[2] Wir schreiben sie in der Form[3]

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}. \tag{15.1}$$

Die Menge aller $n \times m$-Matrizen wird mit $K^{n \times m}$ bezeichnet.[4]

(*ii*) Die Indizes $(i, j) \in [\![1, n]\!] \times [\![1, m]\!]$ mit der Eigenschaft $j - i = k \in \mathbb{Z}$ bilden die k**-te Diagonale** (englisch: k-th diagonal) der Matrix. Die 0-te Diagonale heißt auch die **Hauptdiagonale** (englisch: main diagonal), die anderen Diagonalen heißen die **Nebendiagonalen** (englisch: off-diagonals) der Matrix.

(*iii*) Eine $n \times m$-Matrix heißt eine **Diagonalmatrix** (englisch: diagonal matrix), wenn alle Einträge außerhalb der Hauptdiagonale gleich 0 sind.[5]

[1] Obwohl nicht sofort offensichtlich, dienen Matrizen auch bei den genannten Sachverhalten zur Darstellung linearer Abbildungen.
[2] Wir können daher eine Matrix auch als eine Abbildung $[\![1, n]\!] \times [\![1, m]\!] \to K$ auffassen.
[3] Alternativ können statt der eckigen auch runde Klammern verwendet werden.
[4] Alternative Bezeichnungen sind $K^{n,m}$ oder $M_{n,m}(K)$.
[5] Man sagt auch, dass bei einer Diagonalmatrix die Nebendiagonalen „nicht besetzt“ sind, d. h., dass dort nur Nullen stehen.

(*iv*) Eine Matrix heißt **quadratisch** (englisch: square matrix, quadratic matrix), wenn $m = n$ gilt.

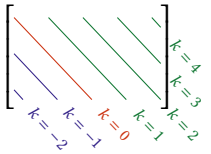
(*v*) Die quadratische $n \times n$-Diagonalmatrix

$$I_{n\times n} := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \tag{15.2}$$

heißt die $n \times n$-**Einheitsmatrix** (englisch: identity matrix). Wir bezeichnen sie auch mit I_n oder einfach mit I, wenn die Dimension klar oder unerheblich ist. △

Beachte: Wir lassen explizit zu, dass eine oder beide Dimensionen einer Matrix gleich 0 sind. Das ist aus vielerlei Gründen praktisch. Eine Matrix der Dimension $n \times 0$ oder $0 \times m$ hat keine Elemente, besitzt aber dennoch ihre spezifische Form. Es gibt nur eine einzige Matrix der Dimension $n \times 0$ bzw. der Dimension $0 \times m$.

Wir illustrieren die Lage der Hauptdiagonale, der oberen Nebendiagonalen ($k > 0$) sowie der unteren Nebendiagonalen ($k < 0$) am Beispiel einer 3×5-Matrix:



Matrizen werden häufig mit lateinischen Großbuchenstaben bezeichnet und ihre Elemente mit den zugehörigen Kleinbuchstaben, zum Beispiel

$$A = (a_{ij})_{i=1,\dots,n,\ j=1,\dots,m} \quad \text{oder} \quad A = (a_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m} \tag{15.3}$$

oder einfach $A = (a_{ij})$, wenn die Dimension klar ist.[6]

Der erste Index (häufig i) heißt der **Zeilenindex** (englisch: row index). Die i-te **Zeile** (englisch: row) von $A = (a_{ij}) \in K^{n\times m}$ ist die (einfach indizierte) Familie bzw. der Zeilenvektor

$$a_{i\bullet} := \begin{pmatrix} a_{i1}, a_{i2}, \dots, a_{im} \end{pmatrix} \in K_m, \tag{15.4}$$

vgl. Beispiel 11.3.

Der zweite Index (häufig j) heißt der **Spaltenindex** (englisch: column index). Die j-te **Spalte** (englisch: column) von $A = (a_{ij}) \in K^{n\times m}$ ist die (einfach indizierte) Familie bzw. der Spaltenvektor

$$a_{\bullet j} := \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} \in K^n, \tag{15.5}$$

[6] Aus Gründen der Verdeutlichung schreiben wir manchmal auch $a_{i,j}$ an Stelle von a_{ij}.

vgl. nochmals Beispiel 11.3. Wir werden $1 \times m$-Matrizen mit Zeilenvektoren und $n \times 1$-Matrizen mit Spaltenvektoren identifizieren.

Auf der Menge $K^{n\times m}$ der $n \times m$-Matrizen definieren wir komponentenweise die Addition und die S-Multiplikation wie folgt:

Definition 15.2 (Addition, S-Multiplikation von Matrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $m, n \in \mathbb{N}_0$. Auf der Menge der Matrizen $K^{n\times m}$ sind die innere Verknüpfung $+\colon K^{n\times m} \times K^{n\times m} \to K^{n\times m}$ (**Addition**[7]) und die äußere Verknüpfung $\cdot\colon K \times K^{n\times m} \to K^{n\times m}$ (**S-Multiplikation**[8]) durch

$$(A + B)_{ij} \coloneqq a_{ij} + b_{ij} \tag{15.6a}$$
$$(\alpha \cdot A)_{ij} \coloneqq \alpha \cdot a_{ij} \tag{15.6b}$$

für $A, B \in K^{n\times m}$ und $\alpha \in K$ erklärt. △

Wir werden das Zeichen $\cdot$ für die skalare Multiplikation in der Regel weglassen, vgl. Bemerkung 11.13.

Satz 15.3 ($(K^{n\times m}, +, \cdot)$ ist ein Vektorraum)**.**
Es seien $(K, +, \cdot)$ ein Körper und $m, n \in \mathbb{N}_0$. Dann bilden die $n \times m$-Matrizen mit den Verknüpfungen (15.6) einen K-Vektorraum. Dieser besitzt die Dimension $n\,m$, und die Matrizen

$$\{E_{11}, \dots, E_{nm}\} \text{ mit } E_{ij} \coloneqq \underbrace{\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{\uparrow j\text{-te Spalte}} \leftarrow i\text{-te Zeile} = (\delta_{ik}\,\delta_{j\ell})_{k=1,\dots,n,\ \ell=1,\dots,m} \tag{15.7}$$

bilden eine Basis, genannt die **Standardbasis** (englisch: standard basis) von $K^{n\times m}$.

Beweis. Die Eigenschaften eines Vektorraumes (Definition 11.1) sind leicht nachzurechnen:[9] $(K^{n\times m}, +)$ ist eine abelsche Gruppe, da $(K, +)$ eine abelsche Gruppe ist. Die Distributivgesetze der S-Multiplikation $\alpha\,(A + B) = \alpha\,A + \alpha\,B$ und $(\alpha + \beta)\,A = \alpha\,A + \beta\,A$ gelten wegen des Distributivgesetzes im Körper $(K, +, \cdot)$. Das gemischte Assoziativgesetz $(\alpha\,\beta)\,A = \alpha\,(\beta\,A)$ gilt wegen der Assoziativität der Multiplikation im Körper $(K, +, \cdot)$. Schließlich ist $1\,A = A$.

Die genannten Matrizen E_{ij} bilden nach Satz 13.3 eine Basis, da jede beliebige Matrix $A \in K^{n\times m}$ auf eindeutige Weise als Linearkombination darstellbar ist, nämlich als

$$A = \sum_{i=1}^{n} \sum_{j=1}^{m} \underbrace{a_{ij}}_{\text{Koeffizient}} E_{ij}. \tag{15.8}$$

Die Dimension von $K^{n\times m}$ ergibt sich aus der Anzahl $n\,m$ der Basiselemente E_{ij}. □

[7] Die Bezeichnung ist dieselbe wie die der „Addition“ im Körper K.
[8] Auch hier ist die Bezeichnung dieselbe wie die der „Multiplikation“ im Körper K.
[9] Wir könnten auch argumentieren, dass die Verknüpfungen (15.6) nichts anderes sind als die punktweise Addition und S-Multiplikation im Vektorraum der Abbildungen $[\![1, n]\!] \times [\![1, m]\!] \to K$, siehe Beispiel 11.3.

Bemerkung 15.4 (zum Vektorraum $K^{n\times m}$)**.**

(*i*) Das neutrale Element bzgl. der Addition ist die **Nullmatrix** (englisch: zero matrix)

$$\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \in K^{n\times m}.$$

(*ii*) Der Vektorraum der 1×1-Matrizen über K ist ein eindimensionaler K-Vektorraum. Dieser kann identifiziert werden mit K selbst.[10]

(*iii*) Die Vektorräume der $0\times m$- und der $n\times 0$-Matrizen sind nulldimensionale K-Vektorräume (Nullräume), da sie nur aus einem Element bestehen. △

§ 15.1 Matrix-Matrix-Multiplikation

Für Matrizen passender Dimensionen können wir eine Matrix-Matrix-Multiplikation einführen. Diese ist von zentraler Bedeutung im Umgang mit Matrizen.

Definition 15.5 (Matrix-Matrix-Multiplikation)**.**

Es seien K ein Körper und $m, n, \ell \in \mathbb{N}_0$. Für Matrizen passender Dimensionen ist die **Matrix-Matrix-Multiplikation** (englisch: matrix-matrix multiplication) oder kurz **Matrix-Multiplikation** (englisch: matrix multiplication) wie folgt definiert:

$$\cdot\colon K^{n\times m} \times K^{m\times \ell} \to K^{n\times \ell}. \tag{15.9a}$$

Dabei gilt für die Matrizen $A \in K^{n\times m}$, $B \in K^{m\times \ell}$ und ihr Matrix-Matrix-Produkt $C := A \cdot B \in K^{n\times \ell}$:

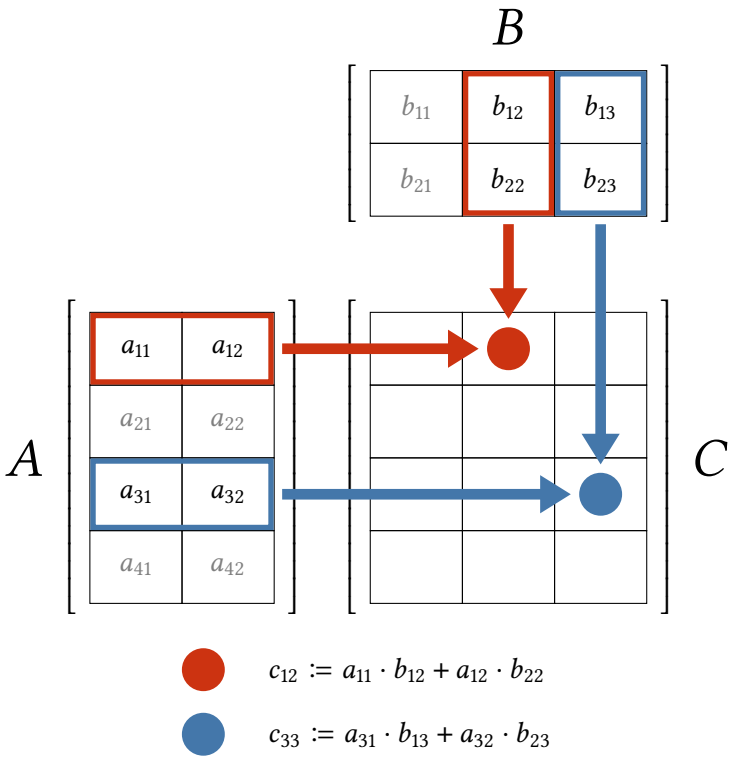
$$c_{ik} := \sum_{j=1}^{m} a_{ij} \cdot b_{jk} \quad \text{für } 1 \leqslant i \leqslant n \text{ und } 1 \leqslant k \leqslant \ell. \tag{15.9b}$$

△

Beachte: Die Summation verwendet die „Addition“ + aus dem Körper K, und jeder Summand ergibt sich aus der „Multiplikation“ $\cdot$ zweier Elemente von K. Im Fall $m = 0$ sind die Summen in (15.9b) alle leer, ergeben also das Nullelement des Körpers K. Daher ist das Produkt einer $n \times 0$- und einer $0 \times m$-Matrix die $n \times m$-Nullmatrix.

Den beispielhaften Fall der Matrix-Multiplikation einer 4×2-Matrix A mit einer 2×3-Matrix B können wir wie folgt grafisch darstellen:

[10] Mit Hilfe des Begriffs der Isomorphie von Vektorräumen (Definition 17.1) können wir das später präzisieren.



Beispiel 15.6 (Matrix-Multiplikation).
Wir multiplizieren eine 4×2-Matrix mit einer 2×3-Matrix über dem Körper $\mathbb{Q}$:[11]

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} \cdot \begin{bmatrix} 5 & 2 & -4 \\ 0 & -2 & 8 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \cdot 5 + (-3) \cdot 0 & 1 \cdot 2 + (-3) \cdot (-2) & 1 \cdot (-4) + (-3) \cdot 8 \\ 2 \cdot 5 + 4 \cdot 0 & 2 \cdot 2 + 4 \cdot (-2) & 2 \cdot (-4) + 4 \cdot 8 \\ 5 \cdot 5 + 0 \cdot 0 & 5 \cdot 2 + 0 \cdot (-2) & 5 \cdot (-4) + 0 \cdot 8 \\ (-3) \cdot 5 + (-6) \cdot 0 & (-3) \cdot 2 + (-6) \cdot (-2) & (-3) \cdot (-4) + (-6) \cdot 8 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 8 & -28 \\ 10 & -4 & 24 \\ 25 & 10 & -20 \\ -15 & 6 & -36 \end{bmatrix}.$$

△

Bemerkung 15.7 (Matrix-Multiplikation).

(*i*) Die Matrix-Matrix-Multiplikation (15.9) ist (außer im Fall $n = \ell = m$) keine innere Verknüpfung eines Vektorraumes von Matrizen, da die Dimensionen der beiden Faktoren und des Produkts verschieden sind.

[11] Wir würden dasselbe Ergebnis erhalten, wenn wir die Matrizen als Matrizen über $\mathbb{R}$ oder über $\mathbb{C}$ auffassen.

(*ii*) $A \cdot B$ ist genau dann definiert, wenn die Anzahl der Spalten des linken Faktors A übereinstimmt mit der Anzahl der Zeilen des rechten Faktors B.

(*iii*) Das Produkt $A \cdot B$ hat soviele Zeilen wie der linke Faktor A und soviele Spalten wie der rechte Faktor B. Die gemeinsame „mittlere Dimension“ ist nach der Bildung des Produkts $A \cdot B$ nicht mehr sichtbar.

(*iv*) Der Eintrag

$$c_{ik} = \sum_{j=1}^{m} a_{ij} \cdot b_{jk}$$

für Zeile i und Spalte k im Produkt $C = A \cdot B$ verwendet nur Informationen aus der i-ten Zeile $a_{i\bullet}$ des linken Faktors A und aus der k-ten Spalte $b_{\bullet k}$ des rechten Faktors B.

(*v*) Verantwortlich für die Position (i, k) im Ergebnis ist der Index i der Zeile des linken Faktors und der Index k der Spalte des rechten Faktors. △

Bei näherer Betrachtung ergibt sich zwei weitere Sichtweisen auf das Produkt $A \cdot B$:

(1) Die Spalten von $C = A \cdot B$ sind Linearkombinationen der Spalten des linken Faktors A. Beispielsweise ist die k-te Spalte von C gerade

$$c_{\bullet k} = \sum_{j=1}^{m} \underbrace{a_{\bullet j}}_{j\text{-te Spalte}} \cdot \underbrace{b_{jk}}_{\text{Koeffizient}}$$

Die Koeffizienten der Linearkombination stehen dabei in der k-ten Spalte von B.

In Beispiel 15.6 ist die erste Spalte des Ergebnisses gerade die Linearkombination „5 mal die erste Spalte von A plus 0 mal die zweite Spalte von A“:

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} \cdot \begin{bmatrix} 5 & 2 & -4 \\ 0 & -2 & 8 \end{bmatrix} = \begin{bmatrix} 5 & 8 & -28 \\ 10 & -4 & 24 \\ 25 & 10 & -20 \\ -15 & 6 & -36 \end{bmatrix}.$$

(2) Die Zeilen von $C = A \cdot B$ sind Linearkombinationen der Zeilen des rechten Faktors B. Beispielsweise ist die i-te Zeile von C gerade

$$c_{i\bullet} = \sum_{j=1}^{m} \underbrace{a_{ij}}_{\text{Koeffizient}} \cdot \underbrace{b_{j\bullet}}_{j\text{-te Zeile}}$$

Die Koeffizienten der Linearkombination stehen dabei in der i-ten Zeile von A.

In Beispiel 15.6 ist die zweite Zeile des Ergebnisses gerade die Linearkombination „2 mal die erste Zeile von B plus 4 mal die zweite Zeile von B“:

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} \cdot \begin{bmatrix} 5 & 2 & -4 \\ 0 & -2 & 8 \end{bmatrix} = \begin{bmatrix} 5 & 8 & -28 \\ 10 & -4 & 24 \\ 25 & 10 & -20 \\ -15 & 6 & -36 \end{bmatrix}.$$

Lemma 15.8 (Eigenschaften der Matrix-Multiplikation).
Es seien K ein Körper und $m, n, p, q \in \mathbb{N}_0$. Für Matrizen $A, A_1, A_2 \in K^{n\times m}$ und $B, B_1, B_2 \in K^{m\times p}$ sowie $C \in K^{p\times q}$ und Skalare $\alpha \in K$ gelten die folgenden Eigenschaften:

$$A \cdot (B_1 + B_2) = A \cdot B_1 + A \cdot B_2 \quad \textbf{Distributivgesetz}[12] \tag{15.10a}$$
$$(A_1 + A_2) \cdot B = A_1 \cdot B + A_2 \cdot B \quad \textbf{Distributivgesetz} \tag{15.10b}$$
$$(A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \textbf{Assoziativgesetz}[13] \tag{15.11}$$
$$A \cdot (\alpha \cdot B) = (\alpha \cdot A) \cdot B = \alpha \cdot (A \cdot B) \quad \text{„Skalare können überall stehen“} \tag{15.12}$$
$$I_n \cdot A = A \cdot I_m = A \quad \text{Neutralität der Einheitsmatrix.} \tag{15.13}$$

Beweis. Wir führen den Nachweis durch Vergleich der Einträge der Matrizen:

$$\begin{aligned}\big[A \cdot (B_1 + B_2)\big]_{ik} &= \sum_{j=1}^{m} a_{ij}\,(b_1 + b_2)_{jk} = \sum_{j=1}^{m} a_{ij}\,(b_1)_{jk} + \sum_{j=1}^{m} a_{ij}\,(b_2)_{jk} \\ &= \big[A \cdot B_1\big]_{ik} + \big[A \cdot B_2\big]_{ik} = \big[A \cdot B_1 + A \cdot B_2\big]_{ik}\end{aligned}$$

zeigt (15.10a). Analog folgt (15.10b). Die Rechnung

$$\begin{aligned}\big[(A \cdot B) \cdot C\big]_{i\ell} &= \sum_{j=1}^{p} (A \cdot B)_{ij}\, c_{j\ell} = \sum_{j=1}^{p} \sum_{k=1}^{m} (a_{ik}\, b_{kj})\, c_{j\ell} \\ &= \sum_{k=1}^{m} \sum_{j=1}^{p} a_{ik}\,(b_{kj}\, c_{j\ell}) = \sum_{k=1}^{m} a_{ik}\,\big[B \cdot C\big]_{k\ell} = \big[A \cdot (B \cdot C)\big]_{i\ell}\end{aligned}$$

zeigt (15.11). Weiter gilt

$$\begin{aligned}\big[A \cdot (\alpha \cdot B)\big]_{ik} &= \sum_{j=1}^{m} a_{ij}\,(\alpha \cdot B)_{jk} = \sum_{j=1}^{m} a_{ij}\,(\alpha\, b_{jk}) = \sum_{j=1}^{m} (\alpha\, a_{ij})\, b_{jk} = \big[(\alpha \cdot A) \cdot B\big]_{ik} \\ &= \alpha \sum_{j=1}^{m} a_{ij}\, b_{jk} = \alpha\,\big[A \cdot B\big]_{ik},\end{aligned}$$

also (15.12). Schließlich haben wir

$$\big[I_n \cdot A\big]_{ik} = \sum_{j=1}^{m} (I_n)_{ij}\, a_{jk} = \sum_{j=1}^{m} \delta_{ij}\, a_{jk} = a_{ik}$$
$$\text{und} \quad \big[A \cdot I_m\big]_{ik} = \sum_{j=1}^{m} a_{ij} (I_m)_{jk} = \sum_{j=1}^{m} a_{ij}\, \delta_{jk} = a_{ik},$$

also (15.13). □

[12] englisch: distributive law
[13] englisch: associative law

Auch bei der Matrix-Multiplikation werden wir in Zukunft das Multiplikationszeichen · in der Regel weglassen.

Bemerkung 15.9 (Matrix-Vektor-Multiplikation).
Ein wichtiger Spezialfall der Matrix-Matrix-Multiplikation ist die **Matrix-Vektor-Multiplikation** (englisch: matrix-vector multiplication) $A\,x$, wobei $A \in K^{n\times m}$ ist und der Spaltenvektor $x \in K^m$ als $m \times 1$-Matrix aufgefasst wird. Beispielsweise gilt über dem Körper $K = \mathbb{Q}$

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} \begin{pmatrix} 2 \\ -2 \end{pmatrix} = \begin{pmatrix} 8 \\ -4 \\ 10 \\ 6 \end{pmatrix}.$$

Ein zweiter Spezialfall ist die **Vektor-Matrix-Multiplikation** (englisch: vector-matrix multiplication) $y\,A$, wobei $A \in K^{n\times m}$ ist und der Zeilenvektor $y \in K_n$ als $1 \times n$-Matrix aufgefasst wird. Beispielsweise gilt

$$\begin{pmatrix} 2 & 0 & 1 & -1 \end{pmatrix} \begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} = \begin{pmatrix} 10 & 0 \end{pmatrix}. \qquad \triangle$$

Ende der Vorlesung 19

§ 15.2 Zeilen- und Spaltenraum

Definition 15.10 (Zeilen- und Spaltenraum, Zeilen- und Spaltenrang).
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in \mathbb{R}^{n\times m}$.

(*i*) Die lineare Hülle der Zeilenvektoren $a_{1\bullet}, \dots, a_{n\bullet} \in K_m$ heißt der **Zeilenraum** (englisch: row space) von A:

$$\mathrm{ZR}(A) := \langle a_{1\bullet}, \dots, a_{n\bullet} \rangle \subseteq K_m. \tag{15.14a}$$

Die Dimension von $\mathrm{ZR}(A)$ heißt der **Zeilenrang** von A (englisch: row rank), also

$$\mathrm{ZRang}(A) := \dim(\mathrm{ZR}(A)). \tag{15.14b}$$

(*ii*) Die lineare Hülle der Spaltenvektoren $a_{\bullet 1}, \dots, a_{\bullet m} \in K^n$ heißt der **Spaltenraum** (englisch: column space) von A:

$$\mathrm{SR}(A) := \langle a_{\bullet 1}, \dots, a_{\bullet m} \rangle \subseteq K^n. \tag{15.15a}$$

Die Dimension von $\mathrm{SR}(A)$ heißt der **Spaltenrang** von A (englisch: column rank), also

$$\mathrm{SRang}(A) := \dim(\mathrm{SR}(A)). \tag{15.15b}$$

$\triangle$

Lemma 15.11 (Zeilenrang und Spaltenrang)**.**
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Dann gilt:

(*i*) Der Zeilenrang $\mathrm{ZRang}(A)$ ist gleich der maximalen Anzahl linearer unabhängiger Zeilenvektoren von A.

(*ii*) Der Spaltenrang $\mathrm{SRang}(A)$ ist gleich der maximalen Anzahl linearer unabhängiger Spaltenvektoren von A.

Beweis. Aussage (*i*): Die Zeilenvektoren $a_{1\bullet}, \dots, a_{n\bullet}$ von A spannen den Zeilenraum $\mathrm{ZR}(A)$ auf. Nach dem Basisauswahlsatz (Folgerung 13.7) können wir aus den n Zeilenvektoren eine Basis von $\mathrm{ZR}(A)$ auswählen. Deren Anzahl entspricht dem Zeilenrang $\mathrm{ZRang}(A)$. Jede echte Obermenge ist nach Satz 13.3 linear abhängig. Daher ist $\mathrm{ZRang}(A)$ gleich der maximalen Anzahl linear unabhängiger Zeilenvektoren von A.

Ein analoges Argument für die Spaltenvektoren zeigt Aussage (*ii*). □

Beispiel 15.12 (Zeilen- und Spaltenraum, Zeilen- und Spaltenrang)**.**
Es sei

$$A = \begin{bmatrix} 2 & 3 & -1 \\ 7 & 4 & 0 \end{bmatrix} \in \mathbb{R}^{2\times 3}.$$

Dann gilt

$$\mathrm{ZR}(A) = \overbrace{\left\langle \begin{pmatrix} 2 & 3 & -1 \end{pmatrix}, \begin{pmatrix} 7 & 4 & 0 \end{pmatrix} \right\rangle}^{\text{linear unabhängig}} \quad \text{mit } \mathrm{ZRang}(A) = \dim(\mathrm{ZR}(A)) = 2$$

$$\text{und} \quad \mathrm{SR}(A) = \underbrace{\left\langle \begin{pmatrix} 2 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix} \right\rangle}_{\text{linear abhängig}} = \underbrace{\left\langle \begin{pmatrix} 2 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\rangle}_{\text{linear unabhängig}} \quad \text{mit } \mathrm{SRang}(A) = \dim(\mathrm{SR}(A)) = 2. \quad \triangle$$

Die in Beispiel 15.12 beobachtete Übereinstimmung von Zeilen- und Spaltenrang ist kein Zufall:

Satz 15.13 (Zeilenrang gleich Spaltenrang)**.**
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Dann gilt

$$0 \leqslant \mathrm{ZRang}(A) = \mathrm{SRang}(A) \leqslant \min\{m, n\}. \tag{15.16}$$

Beweis. Wir führen den Beweis in zwei Schritten.

Schritt 1: Wir zeigen $\mathrm{SRang}(A) \leqslant \mathrm{ZRang}(A)$.

Es sei $r := \mathrm{ZRang}(A) \in \mathbb{N}_0$ und $C \in K^{r\times m}$ eine Matrix, deren linear unabhängige Zeilen $c_{1\bullet}, \dots, c_{r\bullet} \in K_m$ eine Basis des Zeilenraumes $\mathrm{ZR}(A)$ bilden, also $\langle c_{1\bullet}, \dots, c_{r\bullet} \rangle = \mathrm{ZR}(A)$. Die i-te Zeile $a_{i\bullet}$ von A, die ja zu $\mathrm{ZR}(A)$ gehört, ist also eine Linearkombination der Zeilen von C, sagen wir

$$a_{i\bullet} = b_{i1}\, c_{1\bullet} + \cdots + b_{ir}\, c_{r\bullet}.$$

Da das Gesagte für jede Zeile $i = 1, \dots, n$ von A gilt, erhalten wir die Darstellung

$$A = BC = \begin{bmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & & \vdots \\ b_{i1} & \cdots & b_{ir} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nr} \end{bmatrix} \begin{bmatrix} \text{——} & c_{1\bullet} & \text{——} \\ & \vdots & \\ \text{——} & c_{r\bullet} & \text{——} \end{bmatrix}$$

mit einer Koeffizientenmatrix $B \in K^{n\times r}$.

Wegen $Ax = B(Cx)$ für alle $x \in K^m$ ist jede Linearkombination der Spalten von A auch eine Linearkombination der Spalten von B, es gilt also

$$\begin{aligned} & \operatorname{SR}(A) \subseteq \operatorname{SR}(B) \\ \Rightarrow\quad & \operatorname{SRang}(A) \leqslant \operatorname{SRang}(B) \leqslant r = \operatorname{ZRang}(A) \quad \text{nach Folgerung 13.17.} \end{aligned}$$

Schritt 2: Wir zeigen $\operatorname{ZRang}(A) \leqslant \operatorname{SRang}(A)$.

Es sei nun $s := \operatorname{SRang}(A) \in \mathbb{N}_0$ und $B \in K^{n\times s}$ eine Matrix, deren lineare unabhängige Spalten $b_{\bullet 1}, \dots b_{\bullet s} \in K^n$ eine Basis des Spaltenraumes $\operatorname{SR}(A)$ bilden, also $\langle b_{\bullet 1}, \dots b_{\bullet s}\rangle = \operatorname{SR}(A)$. Die j-te Spalte $a_{\bullet j}$ von A, die ja zu $\operatorname{SR}(A)$ gehört, ist also eine Linearkombination der Spalten von B, sagen wir

$$a_{\bullet j} = b_{\bullet 1} c_{1j} + \cdots + b_{\bullet s} c_{sj}.$$

Da das Gesagte für jede Spalte $j = 1, \dots, m$ von A gilt, erhalten wir die Darstellung

$$A = BC = \begin{bmatrix} | & & | \\ b_{\bullet 1} & \cdots & b_{\bullet s} \\ | & & | \end{bmatrix} \begin{bmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1m} \\ \vdots & & \vdots & & \\ c_{s1} & \cdots & c_{sj} & \cdots & c_{sm} \end{bmatrix}$$

mit einer Koeffizientenmatrix $C \in K^{s\times m}$.

Wegen $yA = (yB)C$ für alle $y \in K_n$ ist jede Linearkombination der Zeilen von A auch eine Linearkombination der Zeilen von C, es gilt also

$$\begin{aligned} & \operatorname{ZR}(A) \subseteq \operatorname{ZR}(C) \\ \Rightarrow\quad & \operatorname{ZRang}(A) \leqslant \operatorname{ZRang}(C) \leqslant s = \operatorname{SRang}(A) \quad \text{nach Folgerung 13.17.} \end{aligned}$$

Der Beweis bis hierher zeigt $0 \leqslant \operatorname{ZRang}(A) = \operatorname{SRang}(A)$ für beliebige Matrizen $A \in K^{n\times m}$. Wegen $\operatorname{ZRang}(A) \leqslant n$ und $\operatorname{SRang}(A) \leqslant m$ (Lemma 15.11) folgt die Behauptung (15.16). □

Da Zeilenrang und Spaltenrang übereinstimmen, sprechen wir ab sofort nur noch vom **Rang** einer Matrix:

Definition 15.14 (Rang einer Matrix)**.**
Es sei K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$.

(*i*) Dann ist der **Rang** (englisch: rank) von A definiert als

$$\operatorname{Rang}(A) := \operatorname{ZRang}(A) = \operatorname{SRang}(A).$$

(*ii*) Wir sagen, A habe **vollen Zeilenrang** (englisch: full row rank), wenn $\operatorname{Rang}(A) = n$ gilt, wenn also die Menge der Zeilenvektoren von A linear unabhängig ist.

(*iii*) Wir sagen, A habe **vollen Spaltenrang** (englisch: full column rank), wenn $\operatorname{Rang}(A) = m$ gilt, wenn also die Menge der Spaltenvektoren von A linear unabhängig ist.

(*iv*) Wir sagen, A habe **vollen Rang** (englisch: full rank), wenn $\operatorname{Rang}(A) = \min\{m, n\}$ gilt. Andernfalls heißt die Matrix A **rang-defizitär** (englisch: rank-deficient). △

Beispiel 15.15 (Rang einer Matrix)**.**

(*i*) Die Matrix

$$A = \begin{bmatrix} 2 & 3 & -1 \\ 7 & 4 & 0 \end{bmatrix} \in \mathbb{R}^{2\times 3}$$

aus Beispiel 15.12 hat $\operatorname{Rang}(A) = 2$. A hat also vollen Rang, was hier vollen Zeilenrang bedeutet.

(*ii*) Die Matrix

$$A = \begin{bmatrix} 2 & 3 & -1 \\ 7 & \frac{21}{2} & -\frac{7}{2} \end{bmatrix} \in \mathbb{R}^{2\times 3}$$

hat dagegen nur $\operatorname{Rang}(A) = 1$. Sie ist rang-defizitär.

(*iii*) Der Rang einer Diagonalmatrix $D \in K^{n\times m}$ ist gleich der Anzahl der von Null verschiedenen Diagonaleinträge von D. △

Als direktes Resultat aus dem Beweis von Satz 15.13 halten wir fest:

Folgerung 15.16 (Rangfaktorisierung)**.**
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Ist $r = \operatorname{Rang}(A) \in \mathbb{N}_0$, dann existieren Matrizen $B_{\text{Rang}} \in K^{n\times r}$ und $C_{\text{Rang}} \in K^{r\times m}$, sodass gilt:

$$A = B_{\text{Rang}}\, C_{\text{Rang}} = \begin{bmatrix} | & & | \\ b_{\bullet 1} & \cdots & b_{\bullet r} \\ | & & | \end{bmatrix} \begin{bmatrix} — & & — \\ & c_{1\bullet} & \\ & \vdots & \\ & c_{r\bullet} & \\ — & & — \end{bmatrix}. \tag{15.17}$$

Die Spalten von B_{Rang} bilden eine Basis von $\operatorname{SR}(A)$. Die Zeilen von C_{Rang} bilden eine Basis von $\operatorname{ZR}(A)$.

Eine Faktorisierung der Matrix A wie in (15.17), bei der die inneren Dimensionen der Faktoren mit $\operatorname{Rang}(A)$ übereinstimmt, heißt eine **Rangfaktorisierung** (englisch: rank factorization) von A. Der Rang einer Matrix A ist ein Maß für deren „Informationsgehalt“.

Satz 15.17 (Rang des Produkts von Matrizen).
Es seien K ein Körper und $m, n, \ell \in \mathbb{N}_0$. Für Matrizen $A \in K^{n\times m}$ und $B \in K^{m\times \ell}$ gilt:

$$0 \leqslant \operatorname{Rang}(A\,B) \leqslant \min\{\operatorname{Rang}(A),\ \operatorname{Rang}(B)\} \leqslant \min\{\ell, m, n\}. \tag{15.18}$$

Beweis. Wir verwenden dieselbe Technik wie im Beweis von Satz 15.13: Jede Linearkombination der Spalten von $A\,B$, also $A\,B\,x = A\,(B\,x)$ mit Koeffizientenvektor $x \in K^{\ell}$, ist eine Linearkombination der Spalten von A. Also gilt $\operatorname{SR}(A\,B) \subseteq \operatorname{SR}(A)$ und somit $\operatorname{Rang}(A\,B) = \operatorname{SRang}(A\,B) \leqslant \operatorname{SRang}(A) = \operatorname{Rang}(A)$.

Außerdem ist jede Linearkombination der Zeilen von $A\,B$, also $y\,A\,B = (y\,A)\,B$ mit Koeffizientenvektor $y \in K_n$, eine Linearkombination der Zeilen von B. Also gilt $\operatorname{ZR}(A\,B) \subseteq \operatorname{ZR}(B)$ und somit $\operatorname{Rang}(A\,B) = \operatorname{ZRang}(A\,B) \leqslant \operatorname{ZRang}(B) = \operatorname{Rang}(B)$. Das zeigt die zweite Ungleichung in (15.18).

Die dritte Ungleichung folgt sofort aus $\operatorname{Rang}(A) \leqslant \min\{m, n\}$ und $\operatorname{Rang}(B) \leqslant \min\{\ell, m\}$, siehe Satz 15.13. □

§ 15.3 Zeilenstufenform

Wir geben in diesem Abschnitt eine konstruktive Möglichkeit an, eine Rangfaktorisierung (Folgerung 15.16) einer Matrix A und damit auch den $\operatorname{Rang}(A)$ zu bestimmen. Dazu bringen wir die Matrix A durch geschickte Umformungen auf eine Gestalt, aus der wir eine Basis von $\operatorname{ZR}(A)$ und damit die Dimension von $\operatorname{ZR}(A)$, also den Zeilenrang von A, ablesen können.

Definition 15.18 (elementare Zeilenumformungen, Elementarmatrizen).
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und

$$A = \begin{bmatrix} & a_{1\bullet} & \\ & \vdots & \\ & a_{i\bullet} & \\ & \vdots & \\ & a_{n\bullet} & \end{bmatrix} \in \mathbb{K}^{n\times m}.$$

Unter **elementaren Zeilenumformungen** (englisch: elementary row operations) versteht man die folgenden Operationen, angewendet auf die Matrix A:

Typ I: Multiplikation der i-ten Zeile mit einem Skalar $\alpha \in K \setminus \{0\}$, d. h., Multiplikation der Matrix A von links mit der $n \times n$-Diagonalmatrix

$$D_i(\alpha) := \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} = I + (\alpha - 1)\,E_{ii}. \tag{15.19}$$

Es gilt (nur die gegenüber A geänderten Zeilen werden hervorgehoben)

$$D_i(\alpha)\, A = \begin{bmatrix} & \vdots & \\ \cdots & \alpha\, a_{i\bullet} & \cdots \\ & \vdots & \end{bmatrix}.$$

Typ II: Addition des α-Fachen der j-ten Zeile zur i-ten Zeile ($i \neq j$) mit einem Skalar $\alpha \in K$, d. h., Multiplikation der Matrix A von links mit der $n \times n$-Matrix[14]

$$S_{i,j}(\alpha) := \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & \alpha & 1 & \\ & & & \ddots \\ & & & & 1 \end{bmatrix} = I + \alpha\, E_{ij}. \tag{15.20}$$

Es gilt

$$S_{i,j}(\alpha)\, A = \begin{bmatrix} & \vdots & \\ \cdots & a_{j\bullet} & \cdots \\ & \vdots & \\ \cdots & a_{i\bullet} + \alpha\, a_{j\bullet} & \cdots \\ & \vdots & \end{bmatrix}.$$

Typ III: Vertauschen der i-ten mit der j-ten Zeile ($i \neq j$), d. h. Multiplikation der Matrix A von links mit der $n \times n$-Matrix

$$T_{i,j} := \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & 1 & & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{bmatrix} = I - E_{ii} - E_{jj} + E_{ij} + E_{ji}. \tag{15.21}$$

Es gilt

$$T_{i,j}\, A = \begin{bmatrix} & \vdots & \\ \cdots & a_{j\bullet} & \cdots \\ & \vdots & \\ \cdots & a_{i\bullet} & \cdots \\ & \vdots & \end{bmatrix}.$$

[14] Die Illustration zeigt den Fall $i > j$.

Die Matrizen $D_i(\cdot)$, $S_{i,j}(\cdot)$ und $T_{i,j}$ heißen **Elementarmatrizen** (englisch: elementary matrices) vom Typ I, Typ II bzw. Typ III. Die Matrizen $T_{i,j}$ (Typ III) nennen wir auch **Transpositionsmatrizen** (englisch: transposition matrices).[15] △

Transpositionsmatrizen (Typ III) verwenden wir nur aus Bequemlichkeit. Sie werden eigentlich nicht benötigt, da wir jede Elementarmatrix vom Typ III als ein Produkt von Elementarmatrizen vom Typ I und Typ II schreiben können. (**Quizfrage 15.1:** Wie nämlich?)

Lemma 15.19 (elementare Zeilenumformungen ändern den Zeilenraum und den Zeilenrang nicht)**.**
Es seien K ein Körper und $m, n \in \mathbb{N}_0$. Entsteht die Matrix $C \in K^{n\times m}$ aus $A \in K^{n\times m}$ durch elementare Zeilenumformungen, dann gilt $\mathrm{ZR}(C) = \mathrm{ZR}(A)$, also auch $\mathrm{Rang}(C) = \mathrm{Rang}(A)$.

Beweis. Es reicht zu zeigen, dass sich durch eine einzelne elementare Zeilenumformung der Zeilenraum der Matrix nicht ändert.

Typ I: Für $\alpha \in K \setminus \{0\}$ gilt offensichtlich

$$\langle a_{1\bullet},\ \ldots,\ a_{n\bullet}\rangle = \langle a_{1\bullet},\ \ldots,\ a_{i-1\bullet},\ \alpha\, a_{i\bullet},\ a_{i+1\bullet},\ \ldots,\ a_{n\bullet}\rangle.$$

Typ II: Auch in diesem Fall haben wir

$$\langle a_{1\bullet},\ \ldots,\ a_{n\bullet}\rangle = \langle a_{1\bullet},\ \ldots,\ a_{i-1\bullet},\ a_{i\bullet} + \alpha\, a_{j\bullet},\ a_{i+1\bullet},\ \ldots,\ a_{n\bullet}\rangle.$$

Quizfrage 15.2: Wie rechnen sich die Koeffizienten einer Linearkombination der Vektoren um?

Typ III: Offenbar ändert die Reihenfolge der Vektoren nicht das Resultat von

$$\langle a_{1\bullet},\ \ldots,\ a_{n\bullet}\rangle.$$

□

Die gewünschte Gestalt, aus der man den Zeilenrang und eine Basis des Zeilenraumes einer Matrix gut ablesen kann, ist die folgende:

Definition 15.20 (Zeilenstufenform)**.**
Es seien K ein Körper und $m, n \in \mathbb{N}_0$. Eine Matrix $A \in K^{n\times m}$ heißt in **Zeilenstufenform** (englisch: row echelon form), wenn folgende Bedingungen erfüllt sind:

(*i*) Es gibt eine Zahl $r \in [\![0, n]\!]$, sodass die Zeilen $a_{1\bullet}, \ldots, a_{r\bullet}$ keine Nullzeilen sind und die Zeilen $a_{r+1\bullet}, \ldots, a_{n\bullet}$ sämtlich Nullzeilen sind.

(*ii*) Bezeichnet $j_i := \min\{j \in [\![1, m]\!] \mid a_{ij} \neq 0\}$ den niedrigsten Spaltenindex in Zeile $i \in [\![1, r]\!]$, in der ein Eintrag ungleich 0 steht, dann gilt die **Stufenbedingung** (englisch: echelon condition) $j_1 < j_2 < \cdots < j_r$.

Die Elemente $a_{1j_1}, \ldots, a_{rj_r}$ heißen die **Pivot-Elemente** (englisch: pivot elements) der Zeilenstufenform. △

[15] Die Bezeichnung der Typen I, II und III ist in der Literatur nicht einheitlich.

Bemerkung 15.21 (zur Zeilenstufenform)**.**

(*i*) Die Stufenbedingung bedeutet, dass sowohl links als auch unterhalb von Pivot-Elementen nur Nullen stehen können. Die Pivot-Elemente rücken von Zeile zu Zeile mindestens eine Spalte weiter nach rechts.

(*ii*) Die Lage der Pivot-Elemente in einer Zeilenstufenform einer Matrix ist durch die Ausgangsmatrix eindeutig festgelegt. Die gesamte Zeilenstufenform an sich ist aber i. A. nicht eindeutig, da wir Nicht-Nullzeilen mit Skalaren aus $K \setminus \{0\}$ multiplizieren können und wiederum eine Zeilenstufenform erhalten. Außerdem können wir zu einer Zeile ein Vielfaches einer weiter unten stehenden Zeile addieren, ohne die Zeilenstufenform zu stören.

(*iii*) Der Rang einer Matrix A in Zeilenstufenform ist wegen $r = \operatorname{Rang}(A)$ leicht abzulesen: Der Rang ist gleich der Anzahl der Nicht-Nullzeilen, also gleich der Anzahl der Pivot-Elemente. △

Beispiel 15.22 (Zeilenstufenform)**.**
Nachfolgend sind die Besetzungsmuster einiger 3×4-Matrizen in Zeilenstufenform zu sehen, wobei ? jeweils für einen Eintrag aus dem Körper K steht und $\star$ für einen Eintrag ungleich 0 (die Pivot-Elemente).

$$\begin{matrix} j_1 = 1 \to \\ j_2 = 2 \to \\ j_3 = 3 \to \end{matrix}\begin{bmatrix} \star & ? & ? & ? \\ 0 & \star & ? & ? \\ 0 & 0 & \star & ? \end{bmatrix} \qquad r = 3$$

$$\begin{matrix} j_1 = 1 \to \\ j_2 = 3 \to \end{matrix}\begin{bmatrix} \star & ? & ? & ? \\ 0 & 0 & \star & ? \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad r = 2$$

$$\begin{matrix} j_1 = 3 \to \\ j_2 = 4 \to \end{matrix}\begin{bmatrix} 0 & 0 & \star & ? \\ 0 & 0 & 0 & \star \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad r = 2$$

△

Wir geben nun einen Algorithmus an, der eine gegebene Matrix $A \in K^{n\times m}$ durch elementare Zeilenumformungen in eine Matrix $C \in K^{n\times m}$ in Zeilenstufenform überführt. Die Idee des Verfahrens ist folgende:

(1) Finde eines der am weitesten links stehenden Elemente in der Matrix. Dessen Spaltenindex sei j_1. Bringe das Element, sofern erforderlich, durch Zeilentausch (elementare Zeilenumformung vom Typ III) an die oberste Position $(1, j_1)$.

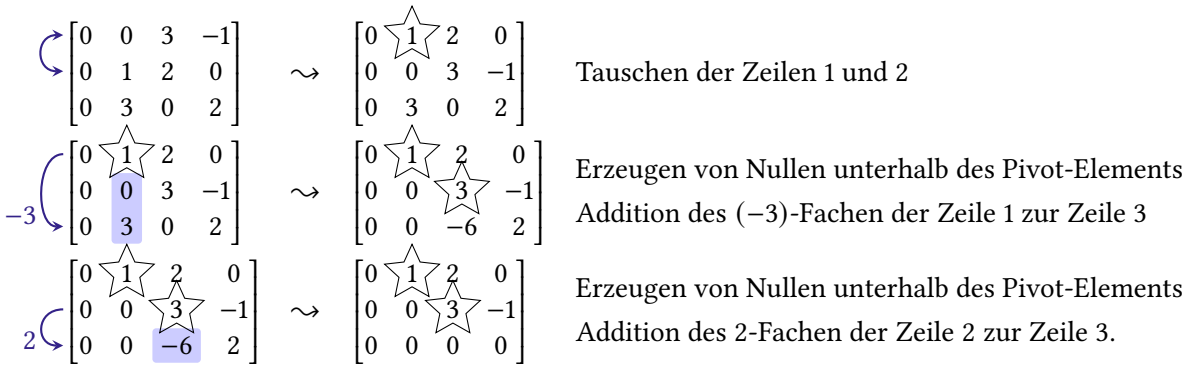
(2) Erzeuge in der Spalte j_1 unterhalb der Position $(1, j_1)$ Nullen durch Addition geeigneter Vielfacher der Zeile 1 zur entsprechenden Zeile 2 bis n (elementare Zeilenumformungen vom Typ II).

(3) Wiederhole die obigen Schritte mit der unteren rechten Teilmatrix ab Zeile 2 und ab Spalte $j_1 + 1$.

Ein vollständiges Verfahren wird in Algorithmus D.1 angegeben. Mit Hilfe von Algorithmus D.1 können wir folgenden Satz konstruktiv beweisen:

Satz 15.23 (Erreichbarkeit der Zeilenstufenform)**.**
Es seien K ein Körper und $n, m \in \mathbb{N}_0$. Jede Matrix $A \in K^{n\times m}$ lässt sich durch elementare Zeilenumformungen in eine Matrix $C \in K^{n\times m}$ in Zeilenstufenform überführen. Ist $r \in [\![0, n]\!]$ die Anzahl der Nicht-Nullzeilen in C, dann bilden die Zeilenvektoren $c_{1\bullet}, \ldots, c_{r\bullet}$ eine Basis von $\operatorname{ZR}(A) = \operatorname{ZR}(C)$, und es gilt $\operatorname{Rang}(A) = \operatorname{Rang}(C) = r$.

Beispiel 15.24 (Erreichbarkeit der Zeilenstufenform).
Wir betrachten ein Beispiel in $\mathbb{R}^{3\times 4}$:



Die ursprüngliche Matrix A wird also von links zunächst mit $T_{1,2}$ von links multipliziert, anschließend mit $S_{3,1}(-3)$ und schließlich mit $S_{3,2}(2)$. Da nun eine Zeilenstufenform erreicht ist, können wir aus dieser den Zeilenraum von A ablesen:

$$\mathrm{ZR}(A) = \left\langle \begin{pmatrix} 0 & 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 3 & -1 \end{pmatrix} \right\rangle,$$

und es gilt $\dim(\mathrm{ZR}(A)) = \mathrm{Rang}(A) = 2$. △

Bemerkung 15.25 (Berechnung einer Rangfaktorisierung).
Wir hatten eingangs des Abschnitts angekündigt, eine konstruktive Möglichkeit anzugeben, eine Rangfaktorisierung $A = B_{\mathrm{Rang}}\, C_{\mathrm{Rang}}$ einer Matrix $A \in K^{n\times m}$ zu bestimmen, sodass also $B_{\mathrm{Rang}} \in K^{n\times r}$, $C_{\mathrm{Rang}} \in K^{r\times m}$ und $r = \mathrm{Rang}(A)$ gilt. Tatsächlich erhalten wir aus der besprochenen Zeilenstufenform C den gesuchten rechten Faktor. Dazu müssen wir lediglich in C eventuell vorhandene Nullzeilen streichen, daraus ergibt sich die Matrix sei $C_{\mathrm{Rang}} \in K^{r\times m}$. Wie aber kommen wir an den linken Faktor B_{Rang}?

Die Zeilenstufenform entstand aus A durch Zeilenmanipulationen, also durch Multiplikation von A mit Elementarmatrizen $E_j \in K^{n\times n}$ von links:

$$E_k \cdots E_2\, E_1\, A = C. \tag{15.22}$$

Wenn es gelänge, die Multiplikationen durch geeignete Matrizen $E'_j \in K^{n\times n}$ rückgängig zu machen, wobei also $E'_j\, E_j = I_n$ gelten soll[16], dann bekämen wir die Darstellung

$$E_k\, E_{k-1} \cdots E_2\, E_1\, A = C \quad\Rightarrow\quad E_{k-1} \cdots E_2\, E_1\, A = E'_k\, C \quad\Rightarrow\quad \cdots \quad\Rightarrow\quad A = E'_1\, E'_2 \cdots E'_k\, C.$$

In der Tat ist das möglich, da Elementarmatrizen invertierbar sind (Übung). Setzen wir nun zur Abkürzung $B := E'_1\, E'_2 \cdots E'_k$, so erhalten wir eine Faktorisierung der Gestalt

$$A = \underset{n}{\Big[\underbrace{\overset{r}{B_{\mathrm{Rang}}} \;\Big|\; \overset{n-r}{*}}_{B}\Big]} \underbrace{\left[\begin{array}{c} \overset{m}{C_{\mathrm{Rang}}} \\ \hline 0 \end{array}\right]}_{C} \begin{matrix} r \\ n-r \end{matrix}$$

[16] Später (Definition 15.39, Lemma 15.43) werden wir solche Matrizen **invertierbar** nennen.

Da bei der Bildung des Matrix-Produkts $A = B\,C$ die letzten $n - r$ Spalten von B immer nur mit den Null-Koeffizienten aus den unteren Zeilen von C multipliziert werden, können wir, ohne das Ergebnis der Matrix-Multiplikation zu ändern, den rechten Faktor C durch seine oberen r Zeilen C_{Rang} und den linken Faktor B durch seine linken r Spalten B_{Rang} ersetzen. So erhalten wir die gewünschte Rangfaktorisierung

$$A = B_{\text{Rang}}\, C_{\text{Rang}}$$

mit $B_{\text{Rang}} \in K^{n\times r}$ und $C_{\text{Rang}} \in K^{r\times m}$. (**Quizfrage 15.3:** Wie müsste Algorithmus D.1 ergänzt werden, damit wir als Ergebnis auch den linken Faktor B der Faktorisierung $A = B\,C$ erhalten, aus der dann durch Streichen von Spalten bzw. Zeilen die Rangfaktorisierung $A = B_{\text{Rang}}\, C_{\text{Rang}}$ folgt? (Die Auflösung ergibt sich aus Algorithmus D.2.)) △

§ 15.4 Transposition von Matrizen

Definition 15.26 (Transposition)**.**
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Die Matrix $A^\mathsf{T} \in K^{m\times n}$, definiert durch $\left(A^\mathsf{T}\right)_{ij} = (A)_{ji}$ für $i \in [\![1, m]\!]$ und $j \in [\![1, n]\!]$, heißt die zu A **transponierte Matrix** (englisch: transposed matrix, lateinisch: transponere: umstellen) oder kurz die **Transponierte** (englisch: transpose) zu A. △

Die transponierte Matrix A^T entsteht aus A durch Spiegelung an der Hauptdiagonalen. Dadurch werden die Zeilen zu Spalten und die Spalten zu Zeilen. Die zu A transponierte Matrix hat die Darstellung

$$A^\mathsf{T} = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}. \tag{15.23}$$

Beispiel 15.27 (transponierte Matrix)**.**

$$A = \begin{bmatrix} 8 & -5 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ -1 & 7 & 4 & 4 \end{bmatrix} \quad\Rightarrow\quad A^\mathsf{T} = \begin{bmatrix} 8 & 0 & -1 \\ -5 & 2 & 7 \\ 2 & 3 & 4 \\ 0 & 0 & 4 \end{bmatrix}. \qquad \triangle$$

Lemma 15.28 (Rechenregeln für die Transposition)**.**
Es seien K ein Körper und $m, n, \ell \in \mathbb{N}_0$. Für Matrizen $A, B \in K^{n\times m}$ und $C \in K^{m\times \ell}$ und Skalare $\alpha \in K$ gelten die folgenden Eigenschaften:

$$(A^\mathsf{T})^\mathsf{T} = A \quad \text{Transposition ist } \textbf{involutorisch} \tag{15.24}$$
$$(A + B)^\mathsf{T} = A^\mathsf{T} + B^\mathsf{T} \quad \text{Transposition ist additiv} \tag{15.25a}$$
$$(\alpha\, A)^\mathsf{T} = \alpha\, A^\mathsf{T} \quad \text{Transposition ist homogen}^{17} \tag{15.25b}$$
$$(A\,C)^\mathsf{T} = C^\mathsf{T} A^\mathsf{T}. \tag{15.26}$$

Beweis. (15.24), (15.25a) und (15.25b) sind offensichtlich. Für (15.26) betrachten wir

$$[(AC)^\mathsf{T}]_{ik} = [AC]_{ki} = \sum_{j=1}^{m} a_{kj}\, c_{ji} = \sum_{j=1}^{m} c_{ji}\, a_{kj}$$
$$= \sum_{j=1}^{m} [C^\mathsf{T}]_{ij}\, [A^\mathsf{T}]_{jk} = [C^\mathsf{T} A^\mathsf{T}]_{ik}.$$ □

Lemma 15.29 (Rang der transponierten Matrix)**.**
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Dann gilt $\operatorname{Rang}(A) = \operatorname{Rang}(A^\mathsf{T})$.

Beweis. Es sei $A = BC$ eine Rangfaktorisierung (Folgerung 15.16) mit $B \in K^{n\times r}$, $C \in K^{r\times m}$ und $r = \operatorname{Rang}(A)$. Aufgrund von (15.26) gilt $A^\mathsf{T} = C^\mathsf{T} B^\mathsf{T}$. Aus Satz 15.17 und Satz 15.13 folgt $\operatorname{Rang}(A^\mathsf{T}) \leqslant \min\{\operatorname{Rang}(B^\mathsf{T}), \operatorname{Rang}(C^\mathsf{T})\} \leqslant \min\{m, n, r\} \leqslant r = \operatorname{Rang}(A)$.

Indem wir A durch A^T ersetzen, erhalten wir aus der bereits bewiesenen Aussage $\operatorname{Rang}(A^\mathsf{T}) \leqslant \operatorname{Rang}(A)$ auch die umgekehrte Ungleichung $\operatorname{Rang}(A) = \operatorname{Rang}((A^\mathsf{T})^\mathsf{T}) \leqslant \operatorname{Rang}(A^\mathsf{T})$. □

Definition 15.30 (symmetrische und antisymmetrische Matrizen)**.**
Es seien K ein Körper, $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$.

(*i*) A heißt **symmetrisch** (englisch: symmetric), wenn $A = A^\mathsf{T}$ gilt.

(*ii*) A heißt **antisymmetrisch** (englisch: antisymmetric) oder **schiefsymmetrisch** (englisch: skew-symmetric), wenn $A = -A^\mathsf{T}$ gilt.

Die Menge der symmetrischen bzw. schiefsymmetrischen $n \times n$-Matrizen bezeichnen wir mit $K^{n\times n}_{\text{sym}}$ bzw. $K^{n\times n}_{\text{skew}}$. △

Beispiel 15.31 (symmetrische und antisymmetrische Matrizen)**.**

(*i*) Die Matrix

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix} \in \mathbb{Q}^{3\times 3}$$

ist symmetrisch.

(*ii*) Die Matrix

$$B = \begin{bmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{bmatrix} \in \mathbb{Q}^{3\times 3}$$

ist antisymmetrisch.

[17] Additivität und Homogenität ergibt zusammen **Linearität**. Die Sprechweise, dass die Transposition eine lineare Abbildung sei, wird in § 17 klar werden.

(*iii*) Die Matrix

$$C = \begin{bmatrix} 0 & 1 & 2 \\ 4 & 0 & 3 \\ 3 & 2 & 0 \end{bmatrix} \in \mathbb{Z}_5^{3\times 3}$$

ist antisymmetrisch.

(*iv*) Die Matrix

$$D = \begin{bmatrix} 0 & -i & -2+i \\ i & 0 & 3 \\ 2-i & -3 & 0 \end{bmatrix} \in \mathbb{C}^{3\times 3}$$

ist antisymmetrisch. △

Lemma 15.32 (symmetrische und antisymmetrische Anteile quadratischer Matrizen)**.**
Es seien K ein Körper der Charakteristik $\operatorname{char}(K) \neq 2$ und $n \in \mathbb{N}_0$. Dann sind $K^{n\times n}_{\text{sym}}$ und $K^{n\times n}_{\text{skew}}$ Unterräume von $K^{n\times n}$ der Dimensionen

$$\dim(K^{n\times n}_{\text{sym}}) = \frac{1}{2} n\,(n+1), \tag{15.27a}$$

$$\dim(K^{n\times n}_{\text{skew}}) = \frac{1}{2} n\,(n-1), \tag{15.27b}$$

und gilt

$$K^{n\times n} = K^{n\times n}_{\text{sym}} \oplus K^{n\times n}_{\text{skew}}. \tag{15.28}$$

Quizfrage 15.4: Was gilt stattdessen im Körper $\mathbb{Z}_2$ der Charakteristik $\operatorname{char}(K) = 2$?

Beweis. Der Beweis ist Gegenstand der Übung. □

Ende der Vorlesung 20

§ 15.5 Der Ring quadratischer Matrizen

Die Menge der quadratischen Matrizen $K^{n\times n}$ über einem Körper $(K, +, \cdot)$ ist bzgl. der Matrix-Multiplikation $\cdot$ abgeschlossen.[18] Zusammen mit der Matrix-Addition ergibt sich eine Ringstruktur $(K^{n\times n}, +, \cdot)$:

Lemma 15.33 (quadratische Matrizen bilden einen nicht-kommutativen Ring mit Eins)**.**
Für $n \in \mathbb{N}_0$ bilden die quadratischen $n \times n$-Matrizen mit der Matrixaddition (15.6a) und der Matrix-Multiplikation (15.9) einen Ring mit dem Einselement I_n. Dieser Ring $(K^{n\times n}, +, \cdot)$ heißt **Matrixring** oder **Matrizenring** (englisch: matrix ring) der Größe $n \times n$ über dem Körper K. Im Fall $n \geqslant 2$ ist dieser Ring nicht kommutativ.

[18] Vorübergehend schreiben wir das Multiplikationszeichen $\cdot$ wieder.

Beweis. Wir prüfen die Definition 9.1 nach. $(K^{n\times n}, +)$ ist eine abelsche Gruppe, da $(K^{n\times n}, +, \cdot)$ (mit der S-Multiplikation $\cdot$) ein Vektorraum ist (Satz 15.3).[19] Mit der Matrix-Multiplikation $\cdot$ bildet $(K^{n\times n}, \cdot)$ eine Halbgruppe, da $\cdot$ nach Lemma 15.8 assoziativ ist. Die Distributivgesetze

$$A \cdot (B_1 + B_2) = A \cdot B_1 + A \cdot B_2$$
$$(A_1 + A_2) \cdot B = A_1 \cdot B + A_2 \cdot B$$

und die Neutralität der Einheitsmatrix I_n wurden ebenfalls in Lemma 15.8 gezeigt.

Die Nicht-Kommutativität für $n \geqslant 2$ sehen wir am Beispiel

$$E_{11} \cdot E_{12} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & & 0 \end{bmatrix} = E_{12}$$

$$E_{12} \cdot E_{11} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} = 0,$$

das für beliebige Körper K gültig ist. □

Der Ring der quadratischen Matrizen $K^{n\times n}$ enthält neben den Diagonalmatrizen noch einige weitere erwähnenswerte Teilmengen:

Definition 15.34 (obere und untere Dreiecksmatrix[20])**.**
Es seien K ein Körper und $n \in \mathbb{N}_0$. Eine Matrix $A \in K^{n\times n}$ heißt

(*i*) eine **obere Dreiecksmatrix** (englisch: upper triangular matrix), wenn $a_{ij} = 0$ für alle $1 \leqslant j < i \leqslant n$ gilt.

(*ii*) eine **strikte obere Dreiecksmatrix** (englisch: strictly upper triangular matrix), wenn $n \geqslant 1$ und $a_{ij} = 0$ für alle $1 \leqslant j \leqslant i \leqslant n$ gilt.

(*iii*) eine **untere Dreiecksmatrix** (englisch: lower triangular matrix), wenn $a_{ij} = 0$ für alle $1 \leqslant i < j \leqslant n$ gilt.

(*iv*) eine **strikte untere Dreiecksmatrix** (englisch: strictly lower triangular matrix), $n \geqslant 1$ und wenn $a_{ij} = 0$ für alle $1 \leqslant i \leqslant j \leqslant n$ gilt.

(*v*) **nilpotent** (englisch: nilpotent), wenn es ein $k \in \mathbb{N}_0$ gibt mit der Eigenschaft $A^k = 0$. △

[19] Dass wir sowohl die Matrix-Multiplikation als auch die S-Multiplikation einer Matrix mit einem Skalar mit demselben Symbol $\cdot$ bezeichnen, sollte nicht zu Verwirrung führen, da sich aus den verknüpften Objekten ergibt, welche Multiplikation gemeint ist. (**Quizfrage 15.5:** Wieso stimmt das auch im Fall $n = 1$?)

[20] Um Dreiecksmatrizen von strikten Dreiecksmatrizen unterscheiden zu können, schließen wir für die folgenden Resultate die 0×0-Matrizen aus.

Wir bezeichnen die Menge der Diagonalmatrizen der Dimension $n \times n$ auch mit dem Symbol $K^{n\times n}_{\diagdown}$ und die Menge der oberen bzw. unteren Dreiecksmatrizen mit $K^{n\times n}_{\diagup}$ bzw. $K^{n\times n}_{\diagdown}$. Es gilt

$$K^{n\times n}_{\diagdown} = K^{n\times n}_{\diagup} \cap K^{n\times n}_{\diagdown}.$$

Beispiel 15.35 (obere und untere Dreiecksmatrix)**.**

(*i*)
$$\begin{bmatrix} 1 & 3 & -3 \\ 0 & 7 & 4 \\ 0 & 0 & 5 \end{bmatrix} \in \mathbb{R}^{3\times 3}$$
ist eine obere Dreiecksmatrix, aber keine strikte obere Dreiecksmatrix.

(*ii*)
$$\begin{bmatrix} 0 & 0 & 0 \\ 7 & 0 & 0 \\ 2 & 1 & 0 \end{bmatrix} \in \mathbb{R}^{3\times 3}$$
ist eine strikte untere Dreicksmatrix.

(*iii*)
$$\begin{bmatrix} 2 & 2 & -2 \\ 5 & 1 & -3 \\ 1 & 5 & -3 \end{bmatrix} \in \mathbb{R}^{3\times 3}$$
ist eine nilpotente Matrix, denn es gilt

$$\begin{bmatrix} 2 & 2 & -2 \\ 5 & 1 & -3 \\ 1 & 5 & -3 \end{bmatrix}^3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \qquad \triangle$$

Lemma 15.36 (strikte Dreiecksmatrizen sind nilpotent)**.**
Es seien K ein Körper und $n \in \mathbb{N}$. Für jede strikte obere und jede strikte untere Dreiecksmatrix $A \in K^{n\times n}$ gilt $A^n = 0$.

Beweis. Der Beweis ist Gegenstand der Übung. □

Beispiel 15.37 (strikte Dreiecksmatrizen sind nilpotent)**.**
Für
$$A = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 0 & 0 & 4 & 5 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in \mathbb{R}^{4\times 4}$$
gilt
$$A^2 = \begin{bmatrix} 0 & 0 & 4 & 17 \\ 0 & 0 & 0 & 24 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{und} \quad A^3 = \begin{bmatrix} 0 & 0 & 0 & 24 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{und} \quad A^4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \qquad \triangle$$

Lemma 15.38 (obere und untere Dreiecksmatrizen bilden Unterringe)**.**
Es seien K ein Körper und $n \in \mathbb{N}_0$. Dann gilt:

(*i*) $K^{n\times n}_{\diagdown}$, $K^{n\times n}_{\triangledown}$ und $K^{n\times n}_{\triangle}$ bilden jeweils einen Unterring mit Eins (Definition 9.12) von $K^{n\times n}$. $K^{n\times n}_{\diagdown}$ ist sogar ein kommutativer Ring mit Eins.

(*ii*) Für $n \geqslant 1$ bilden die strikten oberen und strikten unteren Dreiecksmatrizen einen Unterring (aber keinen Unterring mit Eins) von $K^{n\times n}$. Im Fall $n = 1$ ist das ein Nullring.

(**Quizfrage 15.6:** Sind $K^{n\times n}_{\triangledown}$ und $K^{n\times n}_{\triangle}$ sogar Ideale?)

Beweis. Aussage (*i*): Nach Definition 9.12 ist zu zeigen, dass die jeweilige Teilmenge mit der Addition eine Untergruppe von $(K^{n\times n}, +)$ bildet, dass sie bzgl. der Matrix-Multiplikation abgeschlossen ist und das Einselement (die Einheitsmatrix I_n) enthält.

Wir führen den Beweis nur für den Fall $K^{n\times n}_{\triangledown}$ aus. Sind $A, B \in K^{n\times n}_{\triangledown}$, dann ist auch $-B \in K^{n\times n}_{\triangledown}$ und damit $A - B \in K^{n\times n}_{\triangledown}$. Aus dem Untergruppenkriterium (Satz 7.44) folgt, dass $(K^{n\times n}_{\triangledown}, +)$ eine Untergruppe von $(K^{n\times n}, +)$ ist. Da $I_n \in K^{n\times n}_{\triangledown}$ klar ist, bleibt nur zu zeigen, dass das Matrix-Produkt $A \cdot B$ von zwei Matrizen $A, B \in K^{n\times n}_{\triangledown}$ wieder in $K^{n\times n}_{\triangledown}$ liegt. Für Indizes $1 \leqslant k < i \leqslant n$ gilt

$$[A \cdot B]_{ik} = \sum_{j=1}^{n} \underbrace{a_{ij}}_{=0 \text{ für } j<i} \overbrace{b_{jk}}^{=0 \text{ für } j>k} = 0.$$

Da alle Summanden gleich Null sind, ist $A \cdot B$ tatsächlich wieder eine obere Dreiecksmatrix.

Aussage (*ii*): Der Beweis der Unterring-Eigenschaft geht genauso wie in Aussage (*i*). Da das Einselement I_n von $K^{n\times n}$ keine strikte Dreiecksmatrix ist, handelt es sich nicht um einen Unterring mit Eins[21] von $K^{n\times n}$. □

§ 15.6 Invertierbare Matrizen

Wir interessieren uns nun für die bzgl. der Matrix-Multiplikation invertierbaren Elemente im Ring der quadratischen Matrizen, also für die Einheitengruppe (Beispiel 7.22) des Monoids $(K^{n\times n}, \cdot)$.

Definition 15.39 (invertierbare Matrix)**.**
Es seien K ein Körper und $n \in \mathbb{N}_0$.

(*i*) Eine Matrix $A \in K^{n\times n}$ heißt **invertierbar** (englisch: invertible) oder **regulär** (englisch: non-singular), wenn sie ein invertierbares Element (Definition 7.14) des Monoids $(K^{n\times n}, \cdot)$ ist. Das heißt, es gibt eine Matrix $B \in K^{n\times n}$ mit der Eigenschaft

$$A\,B = I \quad \text{und} \quad B\,A = I. \tag{15.29}$$

[21] Im Fall $n = 1$ besteht der Unterring nur aus der Nullmatrix, ist also ein Nullring. Der Nullring hat zwar 0 als Einselement (Beispiel 9.2), dieses ist aber verschieden von der 1×1-Einheitsmatrix, daher handelt es sich auch in diesem Fall nicht um einen Unterring mit Eins im Sinne von Definition 9.12.

In diesem Fall heißt B die zu A **inverse Matrix** (englisch: inverse) oder kurz die **Inverse** (englisch: inverse) von A, in Symbolen: $B = A^{-1}$.

(*ii*) Andernfalls heißt A **nicht invertierbar** (englisch: non-invertible) oder **singulär** (englisch: singular).

(*iii*) Die Menge der invertierbaren Matrizen in $K^{n\times n}$, also die Einheitengruppe des Monoids $(K^{n\times n}, \cdot)$, heißt die **Gruppe der invertierbaren $n\times n$-Matrizen über K** (englisch: group of invertible matrices) oder die **allgemeine lineare Gruppe** (englisch: general linear group) **vom Grad n über dem Körper K**, in Symbolen

$$\mathrm{GL}(n, K) := \{A \in K^{n\times n} \mid A \text{ ist invertierbar}\}. \tag{15.30}$$

△

Bemerkung 15.40 (zu invertierbaren Matrizen)**.**

(*i*) B ist die Inverse von A genau dann, wenn A die Inverse von B ist. Wie in jedem Monoid ist das neutrale Element, also die Einheitsmatrix I, immer invertierbar und selbstinvers.

(*ii*) Die Bezeichnung **allgemeine lineare Gruppe** für die Einheitengruppe des Monoids $(K^{n\times n}, \cdot)$ leitet sich wie folgt ab: Jede Untergruppe des Monoids $(K^{n\times n}, \cdot)$, ist notwendigerweise eine Untergruppe der Einheitengruppe $\mathrm{GL}(n, K)$. Mit anderen Worten: $\mathrm{GL}(n, K)$ ist das Maximum der Menge aller Untergruppen von $(K^{n\times n}, \cdot)$ bzgl. der Untergruppen-Halbordnung, daher das Attribut **allgemeine Gruppe**. Das Attribut **linear** kommt daher, dass wir Matrizen über die Matrix-Vektor-Multiplikation $\mathbb{K}^n \ni x \mapsto Ax \in K^n$ als lineare Abbildungen (Endomorphismen) von K^n auffassen können (Beispiel 17.5). △

Beispiel 15.41 (invertierbare Matrix)**.**
Die Matrix

$$A = \begin{bmatrix} 1 & 0 & -7 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{bmatrix} \in \mathbb{Q}^{3\times 3}$$

ist invertierbar, denn es gilt

$$\begin{bmatrix} 1 & 0 & -7 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{bmatrix} \frac{1}{17} \begin{bmatrix} 3 & 7 & 0 \\ 1 & -9 & 17 \\ -2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{und} \quad \frac{1}{17} \begin{bmatrix} 3 & 7 & 0 \\ 1 & -9 & 17 \\ -2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & -7 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Die inverse Matrix ist also

$$A^{-1} = \frac{1}{17} \begin{bmatrix} 3 & 7 & 0 \\ 1 & -9 & 17 \\ -2 & 1 & 0 \end{bmatrix}.$$

△

Beachte: Wie wir die Invertierbarkeit einer Matrix überprüfen und ggf. die Inverse berechnen, wird gleich noch Thema sein.

Satz 15.42 (Rechenregeln für Inverse)**.**
Es seien K ein Körper und $n \in \mathbb{N}_0$ sowie $A, B, B_1, B_2 \in K^{n\times n}$.

(*i*) Ist A invertierbar, dann gelten die **Kürzungsregeln**

$$A\,B_1 = A\,B_2 \quad \Rightarrow \quad B_1 = B_2 \tag{15.31a}$$
$$B_1\,A = B_2\,A \quad \Rightarrow \quad B_1 = B_2. \tag{15.31b}$$

(*ii*) Die Invertierung ist **involutorisch**, d. h., für invertierbares A gilt

$$(A^{-1})^{-1} = A. \tag{15.32}$$

(*iii*) Sind A und B invertierbar, dann auch $A\,B$, und es gilt

$$(A\,B)^{-1} = B^{-1}A^{-1}. \tag{15.33}$$

(*iv*) Ist A invertierbar, dann auch A^T, und es gilt

$$(A^\mathsf{T})^{-1} = (A^{-1})^\mathsf{T}. \tag{15.34}$$

Beachte: Wegen (15.34) können wir statt $(A^\mathsf{T})^{-1}$ in Zukunft auch einfach $A^{-\mathsf{T}}$ schreiben.

Beweis. Die Aussagen (*i*) bis (*iii*) sind uns bereits aus allgemeinen Monoiden bekannt: Die Kürzungsregeln (15.31) wurden in Lemma 7.18 gezeigt. Die involutorische Eigenschaft der Invertierung (15.32) haben wir bereits in (7.5) festgestellt. Aussage (*iii*) und (15.33) für die Inverse eines Produkts invertierbarer Elemente eines Monoids finden sich in Lemma 7.16.

Es bleibt Aussage (*iv*) zu zeigen. Dazu sei A invertierbar, dann gilt nach (15.26) für die Transponierte eines Produkts

$$A^\mathsf{T}\,(A^{-1})^\mathsf{T} = (A^{-1}A)^\mathsf{T} = I^\mathsf{T} = I$$
$$\text{und} \quad (A^{-1})^\mathsf{T}\,A^\mathsf{T} = (A\,A^{-1})^\mathsf{T} = I^\mathsf{T} = I,$$

also ist $(A^{-1})^\mathsf{T}$ in der Tat die Inverse zu A^T, was (15.34) zeigt. □

Anhand der Definition 15.39 kann man die Invertierbarkeit oder Nicht-Invertierbarkeit einer Matrix schlecht erkennen. Stattdessen geben wir nun Kriterien für die Invertierbarkeit an. Dabei beginnen wir mit „einfachen“ Matrizen und verallgemeinern die Aussagen dann auf allgemeine Matrizen.

Das folgende Resultat haben wir in Bemerkung 15.25 bereits verwendet:

Lemma 15.43 (Elementarmatrizen sind invertierbar)**.**
Die Elementarmatrizen aus Definition 15.18 sind invertierbar. Die Inverse einer Elementarmatrix ist wiederum eine Elementarmatrix.

Beweis. Der Beweis ist Gegenstand der Übung. □

Lemma 15.44 (Invertierbarkeit von Diagonal- und Dreiecksmatrizen)**.**
Es seien K ein Körper und $n \in \mathbb{N}_0$.

(*i*) Es sei $A \in K^{n\times n}_{\diagdown}$ eine Diagonalmatrix. A ist genau dann invertierbar, wenn alle Diagonaleinträge von A ungleich Null sind. In dem Fall ist die Inverse von A wiederum eine Diagonalmatrix, bestehend aus den Inversen der Diagonaleinträge von A. Die invertierbaren Diagonalmatrizen bilden also eine Untergruppe der Gruppe der invertierbaren Matrizen $\mathrm{GL}(n, K)$.

(*ii*) Es sei $A \in K^{n\times n}_{\triangleleft}$ eine obere Dreiecksmatrix. A ist genau dann invertierbar, wenn alle Diagonaleinträge von A ungleich Null sind. In dem Fall ist die Inverse von A wiederum eine obere Dreiecksmatrix. Die invertierbaren oberen Dreiecksmatrizen bilden also eine Untergruppe der Gruppe der invertierbaren Matrizen $\mathrm{GL}(n, K)$.

(*iii*) Es sei $A \in K^{n\times n}_{\triangleright}$ eine untere Dreiecksmatrix. A ist genau dann invertierbar, wenn alle Diagonaleinträge von A ungleich Null sind. In dem Fall ist die Inverse von A wiederum eine untere Dreiecksmatrix. Die invertierbaren unteren Dreiecksmatrizen bilden also eine Untergruppe der Gruppe der invertierbaren Matrizen $\mathrm{GL}(n, K)$.

Beweis. Aussage (*i*): Es sei $A \in K^{n\times n}_{\diagdown}$ eine Diagonalmatrix. Wäre der Diagonaleintrag $a_{ii} = 0$ für ein $1 \leqslant i \leqslant n$, dann ist die i-te Zeile des Produkts AB für jede Matrix $B \in K^{n\times n}$ der Nullvektor. Damit kann AB nicht die Einheitsmatrix ergeben, d. h., A ist in diesem Fall nicht invertierbar. Es seien nun umgekehrt alle Diagonaleinträge von A ungleich Null. Dann ist

$$\begin{bmatrix} a_{11}^{-1} & & \\ & \ddots & \\ & & a_{nn}^{-1} \end{bmatrix} \begin{bmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{bmatrix} \begin{bmatrix} a_{11}^{-1} & & \\ & \ddots & \\ & & a_{nn}^{-1} \end{bmatrix} = I,$$

also ist wie behauptet die Diagonalmatrix bestehend aus den Inversen der Diagonaleinträge von A die Inverse von A.

Da das Produkt von Diagonalmatrizen wieder eine Diagonalmatrix ist (Lemma 15.38) und insbesondere die Einheitsmatrix eine invertierbare Diagonalmatrix ist, erfüllt die Menge der Diagonalmatrizen das Untergruppenkriterium (Satz 7.44) und ist damit eine Untergruppe von $\mathrm{GL}(n, K)$.

Aussage (*ii*): Es sei $A \in K^{n\times n}_{\triangleleft}$ eine obere Dreiecksmatrix. Im Fall $n = 0$ ist A auch eine Diagonalmatrix, und die Aussage folgt aus Aussage (*i*). Ist dagegen $n \in \mathbb{N}$, dann können wir A in der Form

$$A = D\,(I + N)$$

schreiben, wobei D die Diagonalmatrix mit den Diagonaleinträgen von A und N eine strikte obere Dreiecksmatrix ist. (**Quizfrage 15.7:** klar?) Wir rechnen nun nach, dass die Inverse von $I + N$ gegeben ist durch

$$(I + N)^{-1} = \sum_{k=0}^{n} (-N)^k. \tag{15.35}$$

Es gilt nämlich nach dem Distributiv- und dem Kommutativgesetz der Matrix-Addition und Matrix-Multiplikation

$$\begin{aligned}(I+N)\sum_{k=0}^{n}(-N)^k &= \sum_{k=0}^{n}(I+N)\,(-N)^k = \sum_{k=0}^{n}(-N)^k - \sum_{k=1}^{n+1}(-N)^k \\ &= (-N)^0 - (-N)^{n+1} = I - 0 = I.\end{aligned}$$

Die letzte Gleichheit gilt aufgrund von Lemma 15.36 (strikte Dreiecksmatrizen sind nilpotent). Ganz ähnlich können wir auch zeigen:

$$\begin{aligned}\left(\sum_{k=0}^{n}(-N)^k\right)(I+N) &= \sum_{k=0}^{n}(-N)^k\,(I+N) = \sum_{k=0}^{n}(-N)^k - \sum_{k=1}^{n+1}(-N)^k \\ &= (-N)^0 - (-N)^{n+1} = I - 0 = I.\end{aligned}$$

Tatsächlich ist also $I+N$ invertierbar und besitzt die in (15.35) angegebene Inverse. Diese ist aufgrund von Lemma 15.38 ebenfalls wieder eine obere Dreiecksmatrix.

Sind nun alle Diagonaleinträge von A ungleich Null, dann ist die Digonalmatrix D von A nach Aussage (i) invertierbar. Damit ist $A = D\,(I+N)$ invertierbar, und die Inverse

$$A^{-1} = (I+N)^{-1}\,D^{-1} = \sum_{k=0}^{n}(-N)^k\,D^{-1}$$

ist eine Summe oberer Dreiecksmatrizen, also in der Tat selbst eine obere Dreiecksmatrix. Ist umgekehrt die Diagonalmatrix D von A nicht invertierbar, dann zeigt

$$A\,(I+N)^{-1} = D,$$

dass auch A nicht invertierbar sein kann.

Da das Produkt von oberen Dreiecksmatrizen wieder eine obere Dreiecksmatrix ist (Lemma 15.38) und insbesondere die Einheitsmatrix eine invertierbare obere Dreiecksmatrix ist, erfüllt die Menge der oberen Dreiecksmatrizen das Untergruppenkriterium (Satz 7.44) und ist damit eine Untergruppe von $\mathrm{GL}(n,K)$.

Aussage (iii): Ist $A \in K^{n\times n}$ eine untere Dreiecksmatrix, dann ist A^T eine obere Dreiecksmatrix mit denselben Diagonaleinträgen. Nach Satz 15.42 ist A genau dann invertierbar, wenn A^T invertierbar ist, und in dem Fall gilt für die Inverse nach (15.34)

$$A^{-1} = \left((A^{-1})^\mathsf{T}\right)^\mathsf{T} = \underbrace{\left((A^\mathsf{T})^{-1}\right)}_{\text{obere Dreiecksmatrix nach Aussage } (ii)}{}^\mathsf{T},$$

A^{-1} ist also eine untere Dreiecksmatrix. □

Wir können nun ein Invertierbarkeitskriterium für allgemeine Matrizen angeben. Dieses basiert auf der Beobachtung, dass die Umformung einer Matrix in Zeilenstufenform ihre Invertierbarkeit nicht ändert. Für Matrizen in Zeilenstufenform ist aber die Invertierbarkeit leicht zu erkennen:

Satz 15.45 (Invertierbarkeit von Matrizen erkennen durch Zeilenstufenform)**.**
Es seien K ein Körper, $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$. Weiter sei C eine zu A gehörige Matrix in Zeilenstufenform (Satz 15.23). Dann sind äquivalent:

(*i*) A ist invertierbar.
(*ii*) Es gilt $\text{Rang}(A) = n$.
(*iii*) C ist invertierbar.
(*iv*) Es gilt $\text{Rang}(C) = n$.
(*v*) C hat keine Nullzeilen und keine Nullspalten.

Beachte: Eine quadratische Matrix ist also genau dann invertierbar, wenn sie vollen Rang (Definition 15.14) besitzt. Das ist genau dann der Fall, wenn die Menge der Zeilenvektoren linear unabhängig ist, und auch genau dann, wenn die Menge der Spaltenvektoren linear unabhängig ist.

Beweis. Es sei C eine zu A gehörige Matrix in Zeilenstufenform. C ist also aus A durch Multiplikation von links mit Elementarmatrizen E_i hervorgegangen:

$$C = E_k \cdots E_2 \, E_1 \, A.$$

Aussage (*i*) $\Leftrightarrow$ Aussage (*iii*): Da die Elementarmatrizen nach Lemma 15.43 invertierbar sind, ist A genau dann invertierbar, wenn C invertierbar ist. (**Quizfrage 15.8:** Klar?)

Aussage (*ii*) $\Leftrightarrow$ Aussage (*iv*): Wie in Lemma 15.19 gezeigt wurde, ändern elementare Zeilenumformungen den Zeilenraum und insbesondere den Rang nicht. Es gilt also $\text{Rang}(A) = \text{Rang}(C)$.

Aussage (*iv*) $\Rightarrow$ Aussage (*iii*): Im Fall $n = 0$ ist die einzig mögliche Matrix C die leere Matrix, diese hat $\text{Rang}(C) = 0$ und ist selbstinvers. Für den Rest des Beweisschrittes betrachten wir nun $n \in \mathbb{N}$. $\text{Rang}(C) = n$ bedeutet, dass die Zeilenstufenform von C die Gestalt

$$\begin{bmatrix} \star & ? & ? \\ 0 & & ? \\ 0 & 0 & \star \end{bmatrix}$$

besitzt, vgl. Beispiel 15.22. Dabei sind die Pivot-Elemente $\star \in K \setminus \{0\}$. Nach Lemma 15.44 ist C also invertierbar.

Aussage (*iv*) $\Leftrightarrow$ Aussage (*v*): Wir wissen: $\text{Rang}(C)$ ist die Anzahl der Pivot-Elemente von C. Da C eine $n \times n$-Matrix ist, gilt:

$$\begin{aligned} & \text{Rang}(C) = n \\ \Leftrightarrow\ & C \text{ hat } n \text{ Pivot-Elemente} \\ \Leftrightarrow\ & \text{die Hauptdiagonale von } C \text{ hat keine Nullen} \\ \Leftrightarrow\ & C \text{ hat keine Nullzeilen und keine Nullspalten.} \end{aligned}$$

Aussage (iii) $\Rightarrow$ Aussage (v): Wir argumentieren mit einem Beweis durch Kontraposition. Angenommen, C habe eine Nullzeile. Dann hat $C\,X$ für jede Matrix $X \in K^{n\times n}$ ebenfalls eine Nullzeile, kann also nicht die Einheitsmatrix I_n sein. Also ist C nicht invertierbar.

Angenommen, C habe eine Nullspalte. Dann hat $X\,C$ für jede Matrix $X \in K^{n\times n}$ ebenfalls eine Nullspalte, kann also nicht die Einheitsmatrix I_n sein. Also ist C nicht invertierbar. □

Folgerung 15.46 (Multiplikation mit invertierbaren Matrizen ändert den Rang nicht)**.**
Es seien K ein Körper und $m, n \in \mathbb{N}_0$. Für beliebige Matrizen $A \in K^{n\times m}$ und invertierbare Matrizen $B \in K^{n\times n}$, $C \in K^{m\times m}$ gilt:

$$\operatorname{Rang}(B\,A\,C) = \operatorname{Rang}(A). \tag{15.36}$$

Beweis. Der Beweis ist Gegenstand der Übung. □

Abschließend zeigen wir, dass es für den Nachweis, dass zwei $n \times n$-Matrizen A und B Inverse voneinander sind, ausreichend ist, $A\,B = I$ *oder* $B\,A = I$ nachzuweisen.[22] Mit anderen Worten, jede **Rechtsinverse** einer quadratischen Matrix ist auch eine **Linksinverse** (und damit die eindeutige Inverse) und umgekehrt. Das ist eine durchaus bemerkenswerte Eigenschaft des Matrix-Monoids $(K^{n\times n}, \cdot)$, die in allgemeinen Monoiden nicht gilt (Übung).

Satz 15.47 (Rechtsinverse quadratischer Matrizen sind Linksinverse und umgekehrt)**.**
Es seien K ein Körper, $n \in \mathbb{N}_0$ und $A, B \in K^{n\times n}$. Dann sind äquivalent:

(i) B ist eine Rechtsinverse von A, d. h., es gilt $A\,B = I_n$.

(ii) B ist eine Linksinverse von A, d. h., es gilt $B\,A = I_n$.

(iii) B ist die Inverse von A, d. h., es gilt $A\,B = B\,A = I_n$.

Beweis. Aussage (i) $\Rightarrow$ Aussage (iii): Es sei $A\,B = I_n$. Dann gilt

$n = \operatorname{Rang}(I_n)$	nach Satz 15.45 (I_n ist invertierbar und hat daher vollen Rang)
$= \operatorname{Rang}(A\,B)$	$I_n = A\,B$ nach Voraussetzung
$\leqslant \min\{\operatorname{Rang}(A),\ \operatorname{Rang}(B)\}$	nach Satz 15.17 (Rang des Produkts von Matrizen)
$\leqslant n$	nach Satz 15.13 (Rang ist beschränkt durch die Dimensionen).

Es muss also überall Gleichheit gelten, insbesondere ist $\operatorname{Rang}(A) = \operatorname{Rang}(B) = n$, und nach Satz 15.45 sind A und B invertierbar. Wir müssen noch nachweisen, dass B tatsächlich die Inverse von A ist. Es gilt nämlich $A\,A^{-1} = I$, aber nach Voraussetzung auch $A\,B = I_n$. Nach Kürzungsregel (15.31a) muss $A^{-1} = B$ sein.

Der Beweis von Aussage (ii) $\Rightarrow$ Aussage (iii) geht analog.

Aussage (iii) $\Rightarrow$ Aussage (i) und Aussage (iii) $\Rightarrow$ Aussage (ii) sind klar. □

Ende der Vorlesung 21

Ende der Woche 10

[22] Wenn wir bereits wüssten, dass A oder B invertierbar ist, dann wäre das wegen Lemma 7.19 klar.

§ 16 Lineare Gleichungssysteme

Literatur: Fischer, Springborn, 2020, Kapitel 1.4 und 3.3; Bosch, 2014, Kapitel 3.5; Beutelspacher, 2014, Kapitel 4.1; Deiser, 2024b, Kapitel 3.3; Jänich, 2008, Kapitel 7

Sehr viele Aufgabenstellungen in den quantitativen Wissenschaften führen früher oder später auf lineare Gleichungssysteme.

Definition 16.1 (lineares Gleichungssystem)**.**
Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$.

(*i*) Eine Gleichung der Form $Ax = b$ mit dem unbekannten Koeffizientenvektor $x \in K^m$ heißt ein **lineares Gleichungssystem** (englisch: linear system of equations) oder kurz **LGS**. A heißt die **Koeffizientenmatrix** (englisch: coefficient matrix) und $b \in K^n$ der **Vektor der rechten Seite** (englisch: right-hand side vector) oder kurz die **rechte Seite** (englisch: right-hand side) des LGS. Der unbekannte Koeffizientenvektor x heißt auch die **Variable** (englisch: variable) des LGS.

(*ii*) Die Matrix $[A, b] \in K^{n\times(m+1)}$ heißt die **erweiterte Koeffizientenmatrix** (englisch: augmented coefficient matrix) zum LGS $Ax = b$.

(*iii*) Das LGS $Ax = b$ heißt **homogen** (englisch: homogeneous), wenn $b = 0 \in K^m$ ist, andernfalls **nichthomogen** (englisch: non-homogeneous) oder **inhomogen** (englisch: inhomogeneous).

(*iv*) Das LGS $Ax = b$ heißt **lösbar** (englisch: solvable), wenn es ein $x_0 \in K^m$ gibt, das $Ax_0 = b$ erfüllt, andernfalls **unlösbar** oder **nicht lösbar** (englisch: unsolvable). △

Beispiel 16.2 (lineares Gleichungssystem)**.**

(*i*) Wir betrachten folgendes Beispiel mit $m = 3$ (Anzahl der Gleichungen) und $n = 3$ (Anzahl der unbekannten Koeffizienten) über dem Körper $\mathbb{R}$:

$$\left.\begin{array}{rcrcrcr} 6x_1 & + & 1x_2 & + & 1x_3 & = & 11 \\ 3x_1 & + & 3x_2 & + & 1x_3 & = & 5 \\ -6x_1 & - & 6x_2 & - & 3x_3 & = & -9 \end{array}\right\} \quad \Leftrightarrow \quad \underbrace{\begin{bmatrix} 6 & 1 & 1 \\ 3 & 3 & 1 \\ -6 & -6 & -3 \end{bmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}_{x} = \underbrace{\begin{pmatrix} 11 \\ 5 \\ -9 \end{pmatrix}}_{b}.$$

(*ii*) Wie in Beispiel 11.9 bemerkt, führt die Bestimmung der unbekannten Koeffizienten in einer Linearkombination ebenfalls auf ein lineares Gleichungssystem. Wollen wir etwa den Vektor $\binom{3}{-7}$ im $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ als Linearkombination der Vektoren $\left\{\binom{2}{-1}, \binom{4}{1}\right\}$ darstellen, so müssen die gesuchten Koeffizienten $x_1, x_2 \in \mathbb{R}$ das LGS

$$\underbrace{\begin{bmatrix} 2 & 4 \\ -1 & 1 \end{bmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}}_{x} = \underbrace{\begin{pmatrix} 3 \\ -7 \end{pmatrix}}_{b}$$

erfüllen. △

Beachte: Jede Spalte der Matrix gehört zu einer der Variablen $x_1, \dots, x_m$. Jede Zeile der Matrix gehört zu einer Gleichung. Die Matrix $A \in \mathbb{R}^{n\times m}$, die rechte Seite $b \in K^n$ und die Variable $x \in K^m$ sind alles Objekte über demselben Körper K.

Unser Ziel ist es, *alle* Lösungen von $A\,x = b$ zu bestimmen, also die gesamte **Lösungsmenge** (englisch: solution set)

$$\mathcal{L}(A, b) \coloneqq \{x \in K^m \mid A\,x = b\}. \tag{16.1}$$

Dabei spielt die Zeilenstufenform der Koeffizientenmatrix A bzw. der erweiterten Koeffizientenmatrix $[A, b]$ eine entscheidende Rolle, wie wir am Beweis des folgenden Satzes und auch anschließend beim Lösungsverfahren sehen werden.

Satz 16.3 (Struktur der Lösungsmenge, Lösbarkeit)**.**

Es seien K ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$ und $b \in K^n$.

(*i*) $\mathcal{L}(A, 0)$ ist ein Unterraum von K^m der Dimension $m - \operatorname{Rang}(A)$.

(*ii*) Ist $x_0 \in K^m$ irgendeine („**partikuläre**“) **Lösung** (englisch: particular solution) von $A\,x = b$, dann gilt

$$\mathcal{L}(A, b) = x_0 + \mathcal{L}(A, 0). \tag{16.2}$$

Beachte: Die Lösungsmenge eines allgemeinen Systems $A\,x = b$ ergibt sich aus einer partikulären Lösung plus der Lösungsmenge des zugehörigen homogenen Systems.

(*iii*) Die folgenden Aussagen sind äquivalent:

(a) $A\,x = b$ ist lösbar.
(b) $b \in \operatorname{SR}(A)$.
(c) $\operatorname{Rang}(A) = \operatorname{Rang}([A, b])$.

(*iv*) Die folgenden Aussagen sind äquivalent:

(a) $A\,x = b$ ist eindeutig lösbar.
(b) $\operatorname{Rang}(A) = \operatorname{Rang}([A, b]) = m$.

(*v*) Ist A quadratisch, gilt also $m = n$, dann sind die folgenden Aussagen äquivalent:

(a) $A\,x = b$ ist eindeutig lösbar.
(b) $A\,x = c$ ist für jedes $c \in K^n$ eindeutig lösbar.
(c) A ist invertierbar.

In diesem Fall ist die eindeutige Lösung von $A\,x = b$ gegeben durch $x = A^{-1}b$.

Beweis. Wir zerlegen den Beweis von Aussage (*i*) in mehrere Schritte.

Schritt 1: $\mathcal{L}(A, 0)$ ist ein Unterraum von K^m:

Das folgt aus dem Unterraumkriterium (Satz 11.11), denn: Gehören die Vektoren $x, y \in K^m$ zu $\mathcal{L}(A, 0)$, erfüllen also die Bedingungen $A\,x = 0$ und $A\,y = 0$, und sind $\alpha, \beta \in K$, dann gehört auch $\alpha\,x + \beta\,y$ zu $\mathcal{L}(A, 0)$, denn es gilt

$$A\,(\alpha\,x + \beta\,y) = A\,(\alpha\,x) + A\,(\beta\,y) = \alpha\,A\,x + \beta\,A\,y = 0.$$

Schritt 2: Wir bringen A in Zeilenstufenform C ohne Nullzeilen und zeigen $\mathcal{L}(A,0) = \mathcal{L}(C,0)$:

Es sei dazu $\widehat{C} = E_k \cdots E_2 E_1 A$ eine zu A gehörige Zeilenstufenform. Da die Elementarmatrizen E_i invertierbar sind, gilt $Ax = 0 \Leftrightarrow \widehat{C}x = E_k \cdots E_2 E_1 x = 0$, also $\mathcal{L}(A,0) = \mathcal{L}(\widehat{C},0)$. Zur Abkürzung setzen wir $r := \operatorname{Rang}(A) = \operatorname{Rang}(\widehat{C})$, $0 \leqslant r \leqslant \min\{m,n\}$. Eventuell in $\widehat{C}$ auftretende Nullzeilen können wir streichen und erhalten die Matrix $C \in K^{r\times m}$ in Zeilenstufenform ohne Nullzeilen. Es gilt weiterhin $\mathcal{L}(A,0) = \mathcal{L}(\widehat{C},0) = \mathcal{L}(C,0)$.

Schritt 3: Wir bestätigen $\dim(\mathcal{L}(C,0)) = m - r$, indem wir eine Basis dieses Unterraumes angeben:

Wir bezeichnen mit $\mathcal{A} := (j_1,\ldots,j_r)$ die Familie der Pivot-Spalten (in aufsteigender Reihenfolge) und mit $\mathcal{I}$ die komplementäre Familie der Nicht-Pivot-Spalten $\mathcal{I} := (k_1,\ldots,k_{m-r})$. Wir können jeden Vektor $x \in K^m$ in zwei Teilvektoren $x_\mathcal{A} \in K^r$ und $x_\mathcal{I} \in K^{m-r}$ zerlegen. Dies geschieht durch Einführung der beiden Matrizen

$$\Pi_\mathcal{A} := [e_{j_i}^\mathsf{T}]_{i\in[\![1,r]\!]} \in K^{r\times m} \quad \text{und} \quad \Pi_\mathcal{I} :=\in K^{(m-r)\times m}[e_{k_i}^\mathsf{T}]_{i\in[\![1,m-r]\!]},$$

die aus komplementären Zeilen der $m\times m$-Einheitsmatrix bestehen. (**Quizfrage 16.1:** Können Sie sich davon überzeugen, dass die nachfolgenden Ausführungen auch in den Grenzfällen $r = 0$ und $r = m$ Sinn ergeben?) Dann gilt

$$x_\mathcal{A} = \Pi_\mathcal{A} x \quad \text{und} \quad x_\mathcal{I} = \Pi_\mathcal{I} x \quad \text{sowie} \quad x = \Pi_\mathcal{A}^\mathsf{T} x_\mathcal{A} + \Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I}.$$

Die wesentliche Erkenntnis hierbei ist, dass wir

$$Cx = C\Pi_\mathcal{A}^\mathsf{T} x_\mathcal{A} + C\Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I}$$

schreiben können, wobei die Matrix $C\Pi_\mathcal{A}^\mathsf{T} = [c_{\bullet j_1},\ldots,c_{\bullet j_r}]$ aus den Pivot-Spalten von C besteht und damit eine invertierbare obere Dreiecksmatrix (Satz 15.45) der Dimension $r\times r$ darstellt. Wir können also $Cx = 0$ nach der Teilvariablen $x_\mathcal{A}$ auflösen:

$$\begin{aligned} & Cx = 0 \\ \Leftrightarrow\quad & C\Pi_\mathcal{A}^\mathsf{T} x_\mathcal{A} + C\Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I} = 0 \\ \Leftrightarrow\quad & C\Pi_\mathcal{A}^\mathsf{T} x_\mathcal{A} = -C\Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I} \\ \Leftrightarrow\quad & x_\mathcal{A} = -\left(C\Pi_\mathcal{A}^\mathsf{T}\right)^{-1} C\Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I}, \end{aligned}$$

wobei $x_\mathcal{I} \in K^{m-r}$ frei gewählt werden kann. Setzen wir diese Darstellung in $x = \Pi_\mathcal{A}^\mathsf{T} x_\mathcal{A} + \Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I}$ ein, so erhalten wir durch

$$x = -\Pi_\mathcal{A}^\mathsf{T}\left(C\Pi_\mathcal{A}^\mathsf{T}\right)^{-1} C\Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I} + \Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I} = \left[I_m - \Pi_\mathcal{A}^\mathsf{T}\left(C\Pi_\mathcal{A}^\mathsf{T}\right)^{-1} C\right]\Pi_\mathcal{I}^\mathsf{T} x_\mathcal{I} \tag{16.3}$$

mit beliebigem $x_\mathcal{I} \in K^{m-r}$ genau die Lösungen von $Cx = 0$.

Wir zeigen nun, dass die Spalten der Matrix

$$\left[I_m - \Pi_\mathcal{A}^\mathsf{T}\left(C\Pi_\mathcal{A}^\mathsf{T}\right)^{-1} C\right]\Pi_\mathcal{I}^\mathsf{T} \in K^{n\times(m-r)} \tag{16.4}$$

linear unabhängig sind und damit eine Basis von $\mathcal{L}(C,0) = \mathcal{L}(A,0)$ bilden. Eine solche Spalte ergibt sich durch Multiplikation der Matrix aus (16.4) mit einem der

Standardbasisvektoren e_i von K^{m-r}. Die lineare Unabhängigkeit der Spalten folgt aus

$$\begin{aligned}
&\sum_{i=1}^{m-r} \alpha_i \left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}} \left(C \Pi_{\mathcal{A}}^{\mathsf{T}} \right)^{-1} C \right] \Pi_{\mathcal{I}}^{\mathsf{T}} e_i = 0 \\
\Rightarrow \quad & \Pi_{\mathcal{I}} \sum_{i=1}^{m-r} \alpha_i \left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}} \left(C \Pi_{\mathcal{A}}^{\mathsf{T}} \right)^{-1} C \right] \Pi_{\mathcal{I}}^{\mathsf{T}} e_i = 0 \\
\Rightarrow \quad & \sum_{i=1}^{m-r} \alpha_i \Pi_{\mathcal{I}} \left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}} \left(C \Pi_{\mathcal{A}}^{\mathsf{T}} \right)^{-1} C \right] \Pi_{\mathcal{I}}^{\mathsf{T}} e_i = 0 \\
\Rightarrow \quad & \sum_{i=1}^{m-r} \alpha_i \Big[\underbrace{\Pi_{\mathcal{I}} \Pi_{\mathcal{I}}^{\mathsf{T}}}_{=I_{m-r}} - \underbrace{\Pi_{\mathcal{I}} \Pi_{\mathcal{A}}^{\mathsf{T}} \left(C \Pi_{\mathcal{A}}^{\mathsf{T}} \right)^{-1} C \Pi_{\mathcal{I}}^{\mathsf{T}}}_{=0} \Big] e_i = 0 \\
\Rightarrow \quad & \sum_{i=1}^{m-r} \alpha_i \, e_i = 0.
\end{aligned}$$

Da die Menge der Standardbasisvektoren e_i von K^{m-r} linear unabhängig ist, folgt $\alpha_i = 0$ für alle $i \in [\![1, m-r]\!]$.

Damit haben wir gezeigt, dass die Spalten der Matrix (16.4) eine Basis der Kardinalität $m - r$ von $\mathcal{L}(C, 0) = \mathcal{L}(A, 0)$ bilden.

Aussage *(ii)*: Es sei $x_0 \in K^m$ mit $A\,x_0 = b$ gegeben. Dann gilt

$$\begin{aligned}
& x \in \mathcal{L}(A, b) \\
\Leftrightarrow \quad & A\,x = b \\
\Leftrightarrow \quad & A\,(x - x_0) = 0 \\
\Leftrightarrow \quad & x - x_0 \in \mathcal{L}(A, 0) \\
\Leftrightarrow \quad & x \in x_0 + \mathcal{L}(A, 0).
\end{aligned}$$

Nun zu Aussage *(iii)*:

Aussage (a) $\Leftrightarrow$ Aussage (b): $A\,x = b$ ist lösbar genau dann, wenn b als Linearkombination der Spalten von A darstellbar ist, also genau dann, wenn $b \in \mathrm{SR}(A)$ liegt.

Aussage (b) $\Leftrightarrow$ Aussage (c): Die Hinzunahme des Spaltenvektors b zu einer Matrix A erhöht genau dann den $\mathrm{Rang}(A) = \mathrm{SRang}(A) = \dim(\mathrm{SR}(A))$ nicht, wenn b bereits in $\mathrm{SR}(A)$ enthalten ist.

Wir beweisen Aussage *(iv)*:

Aussage (a) $\Rightarrow$ Aussage (b): Es besitze $A\,x = b$ eine eindeutige Lösung x_0. Aufgrund der Lösbarkeit folgt aus Aussage *(iii)* $\mathrm{Rang}(A) = \mathrm{Rang}([A, b])$. Aufgrund der Eindeutigkeit der Lösung und der Darstellung (16.2) $\mathcal{L}(A, b) = x_0 + \mathcal{L}(A, 0)$ muss $\mathcal{L}(A, 0) = \{0\}$, also $\dim(\mathcal{L}(A, 0)) = 0$ sein. Das bedeutet nach Aussage *(i)* aber gerade $m = \mathrm{Rang}(A)$.

Aussage (b) $\Rightarrow$ Aussage (a): Es gelte $\mathrm{Rang}(A) = \mathrm{Rang}([A, b]) = m$. Dann ist aufgrund von Aussage *(iii)* $A\,x = b$ lösbar. Aufgrund der Darstellung (16.5) und $\dim(\mathcal{L}(A, 0)) = m - \mathrm{Rang}(A) = 0$ folgt, dass die Lösung eindeutig ist.

Schließlich Aussage (v): Es sei nun A quadratisch, also $m = n$.

Aussage (a) $\Rightarrow$ Aussage (c): Es sei $Ax = b$ eindeutig lösbar. Nach Aussage (iv) folgt, dass $\operatorname{Rang}(A) = \operatorname{Rang}([A, b]) = n$ gilt. $\operatorname{Rang}(A) = n$ impliziert nach Satz 15.45 aber, dass A invertierbar ist.

Aussage (c) $\Rightarrow$ Aussage (b): Wenn A invertierbar ist, dann ist $Ax = c$ äquivalent zu $A^{-1}Ax = x = A^{-1}c$. Also ist $Ax = c$ für jedes $c \in K^n$ eindeutig lösbar.

Aussage (b) $\Rightarrow$ Aussage (a): Das ist offensichtlich. □

Bemerkung 16.4 (zu Satz 16.3 über die Struktur der Lösungsmenge eines linearen Gleichungssystems)**.**

(i) Wir illustrieren den Beweis von Aussage (i) aus Satz 16.3 anhand eines Beispiels (vgl. Beispiel 15.22). Die Zeilenstufenform von A habe die Gestalt

$$\widehat{C} = \begin{bmatrix} \star & ? & ? & ? \\ 0 & 0 & \star & ? \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{und nach Streichen von Nullenzeilen} \quad C = \begin{bmatrix} \star & ? & ? & ? \\ 0 & 0 & \star & ? \end{bmatrix}.$$

Hieraus lesen wir ab:

- Anzahl der Variablen $m = 4$
- Rang der Matrix $\operatorname{Rang}(A) = r = 2$
- Familie der Pivot-Spalten $\mathcal{A} = (1, 3)$
- Familie der Nicht-Pivot-Spalten $\mathcal{I} = (2, 4)$

Die Auswahlmatrizen $\Pi_{\mathcal{A}}$ und $\Pi_{\mathcal{I}}$ haben also die Form

$$\Pi_{\mathcal{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{und} \quad \Pi_{\mathcal{I}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Es gilt

$$x_{\mathcal{A}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_3 \end{pmatrix} \quad \text{und} \quad x_{\mathcal{I}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_4 \end{pmatrix}$$

sowie

$$\begin{aligned} x &= \Pi_{\mathcal{A}}^{\mathsf{T}} \; x_{\mathcal{A}} + \Pi_{\mathcal{I}}^{\mathsf{T}} \; x_{\mathcal{I}} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_3 \end{pmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} x_2 \\ x_4 \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} x_1 \\ 0 \\ x_3 \\ 0 \end{pmatrix}}_{\text{abhängige Variablen}} + \underbrace{\begin{pmatrix} 0 \\ x_2 \\ 0 \\ x_4 \end{pmatrix}}_{\text{unabhängige Variablen}} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}. \end{aligned}$$

Wir nennen die Variablen x_2 und x_4 auch die **unabhängigen Variablen** (englisch: independent variables), während x_1 und x_3 als die **abhängigen Variablen** (englisch: dependent variables) bezeichnet werden.

Die Teilmatrix $C\,\Pi_{\mathcal{A}}^{\mathsf{T}}$ (Auswahl der $\mathcal{A}$-Spalten von C) hat die Gestalt

$$\begin{bmatrix} \boxed{\begin{matrix} \star & ? \\ 0 & \star \end{matrix}} \end{bmatrix}$$

einer invertierbaren oberen $r \times r$-Dreiecksmatrix.

Wir halten fest, dass die kompliziert aussehende Darstellung

$$\left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}} \left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\right)^{-1} C\right] \Pi_{\mathcal{I}}^{\mathsf{T}} \in K^{n\times(m-r)} \tag{16.5}$$

einer spaltenweisen Basis von $\mathcal{L}(A,0)$ praktisch Folgendes bedeutet: Wir setzen genau eine der unabhängigen Variablen x_i auf den Wert 1 und die anderen unabhängigen Variablen auf den Wert 0. (Das entspricht einer Spalte von $\Pi_{\mathcal{I}}^{\mathsf{T}}$.) Dann rechnen wir die Werte der abhängigen Variablen $x_{\mathcal{A}}$ mit Hilfe der Gleichung

$$\left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\right) x_{\mathcal{A}} = -\underbrace{C\,\Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}}}_{\text{genau eine der } \mathcal{I}\text{-Spalten von } C} \tag{16.6}$$

aus. Weil $C\,\Pi_{\mathcal{A}}^{\mathsf{T}}$ eine obere Dreiecksmatrix ist, können wir die Werte der abhängigen Variablen $x_{\mathcal{A}}$ von hinten nach vorne bestimmen und an der richtigen Stelle in den Lösungsvektor einsortieren ($\Pi_{\mathcal{A}}^{\mathsf{T}} x_{\mathcal{A}}$). Ein Beispiel folgt in Beispiel 16.10.

(*ii*) Die Dimension des Lösungsraumes $\dim(\mathcal{L}(A,0)) = m - \operatorname{Rang}(A)$ sollten wir uns merken in der Form „Anzahl der Variablen (m) minus Anzahl der wesentlichen (sprich: linear unabhängigen) Gleichungen ($\operatorname{Rang}(A)$) im System $A\,x = b$“.

(*iii*) Bei einem linearen Gleichungssystem $A\,x = b$ können drei mögliche Fälle auftreten:

(1) Das System ist eindeutig lösbar.

(2) Das System ist lösbar, aber nicht eindeutig lösbar. In diesem Fall hat die Lösungsmenge die Struktur (16.2), also irgendeine beliebige, aber feste Lösung x_0 von $A\,x = b$, plus den Unterraum $\mathcal{L}(A,0)$ der Dimension $m - \operatorname{Rang}(A) \geqslant 1$.[23]

(3) Das System ist nicht lösbar. △

Wie berechnet man nun praktisch die Lösungsmenge eines linearen Gleichungssystems $A\,x = b$ bzw. stellt fest, dass das System nicht lösbar ist? Dazu gehen wir wie folgt vor:

(1) Wir bringen die erweiterte Koeffizientenmatrix $[A,b]$ zunächst in Zeilenstufenform. An ihr können wir bereits die Lösbarkeit und ggf. die Dimension des Lösungsraumes ablesen.

(2) Wenn das System lösbar ist, so überführen wir die erweiterte Koeffizientenmatrix in die sogenannte **reduzierte Zeilenstufenform**, aus der wir die Lösungsmenge ablesen können.[24]

[23] Die Lösungsmenge $\mathcal{L}(A,b)$ ist dann also eine unendliche Menge, falls der Körper K eine unendliche Menge ist. Ist dagegen der Körper K endlich, dann gilt $\#\mathcal{L}(A,b) = (\#K)^{m-\operatorname{Rang}(A)}$.

[24] Der zusätzliche Aufwand für die Überführung in die reduzierte Zeilenstufenform ist gerechtfertigt, weil dann die $\mathcal{A}$-Spalten $C\,\Pi_{\mathcal{A}}^{\mathsf{T}}$, aus denen sich — siehe (16.6) — die Werte der abhängigen Variablen ergeben, nicht nur eine obere Dreiecksmatrix, sondern die Einheitsmatrix ist, sodass wir die Werte direkt ablesen können.

Dieses Verfahren heißt **Gaußsches Eliminationsverfahren** (englisch: Gaussian elimination method).[25]

Definition 16.5 (reduzierte Zeilenstufenform, vgl. Definition 15.20)**.**
Es seien K ein Körper und $m, n \in \mathbb{N}_0$. Eine Matrix $A \in K^{n\times m}$ heißt in **reduzierter Zeilenstufenform** (englisch: reduced row echelon form), wenn sie in Zeilenstufenform ist (Definition 15.20) und zusätzlich gilt:

(*i*) Alle Pivot-Elemente sind gleich 1.

(*ii*) Elemente, die in einer Spalte oberhalb eines Pivot-Elements stehen, sind gleich 0. △

Beachte: Die reduzierte Zeilenstufenform einer Matrix ist eindeutig. Eine Matrix ist genau dann invertierbar, wenn ihre reduzierte Zeilenstufenform die Einheitsmatrix ist (Beweis in Folgerung 16.8).

Beispiel 16.6 (reduzierte Zeilenstufenform, vgl. Beispiel 15.22 zur Zeilenstufenform)**.**
Nachfolgend sind die Besetzungsmuster einiger 3×4-Matrizen in reduzierter Zeilenstufenform zu sehen, wobei ? jeweils für einen Eintrag aus dem Körper K steht. Die Zahl r gibt wieder den Rang der Matrix an.

$$\begin{matrix} j_1 = 1 \to \\ j_2 = 2 \to \\ j_3 = 3 \to \end{matrix}\begin{bmatrix} \boxed{1} & 0 & 0 & ? \\ 0 & \boxed{1} & 0 & ? \\ 0 & 0 & \boxed{1} & ? \end{bmatrix} \qquad r = 3$$

$$\begin{matrix} j_1 = 1 \to \\ j_2 = 3 \to \end{matrix}\begin{bmatrix} \boxed{1} & ? & 0 & ? \\ 0 & 0 & \boxed{1} & ? \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad r = 2$$

$$\begin{matrix} j_1 = 3 \to \\ j_2 = 4 \to \end{matrix}\begin{bmatrix} 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 0 & \boxed{1} \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad r = 2$$

△

Wir können Algorithmus D.1 erweitern, um die reduzierte Zeilenstufenform einer Matrix zu berechnen, siehe Algorithmus D.3. Mit desen Hilfe können wir analog zu Satz 15.23 beweisen:

Satz 16.7 (Erreichbarkeit der reduzierten Zeilenstufenform, vgl. Satz 15.23)**.**
Es seien K ein Körper und $n, m \in \mathbb{N}_0$. Jede Matrix $A \in K^{n\times m}$ lässt sich durch elementare Zeilenumformungen in eine Matrix $C \in K^{n\times m}$ in reduzierter Zeilenstufenform überführen. Ist $r \in [\![0, n]\!]$ die Anzahl der Nicht-Nullzeilen in C, dann bilden die Zeilenvektoren $c_{1\bullet}, \ldots, c_{r\bullet}$ eine Basis von $\mathrm{ZR}(A) = \mathrm{ZR}(C)$, und es gilt $\mathrm{Rang}(A) = \mathrm{Rang}(C) = r$.

Folgerung 16.8 (invertierbare Matrizen sind Produkte von Elementarmatrizen)**.**
Es seien K ein Körper, $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$. Dann sind äquivalent:

(*i*) Die Matrix A ist invertierbar.

(*ii*) Die reduzierte Zeilenstufenform von A ist die Einheitsmatrix I_n.

(*iii*) Es gibt Elementarmatrizen $E_1, \ldots, E_k \in K^{n\times n}$, $k \in \mathbb{N}_0$, so dass gilt:

$$A = E_1 E_2 \cdots E_k.$$

[25] Das Wort „Elimination“ bezieht sich darauf, dass durch die Überführung in Zeilenstufenform Variablen aus den Gleichungen derart eliminiert wurden (erkennbar an Null-Koeffizienten), dass zwischen benachbarten Zeilen von unten nach oben immer nur eine Variable (Pivot-Spalte) hinzukommt, nach der diese Zeile (Gleichung) aufgelöst werden kann.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Ist A invertierbar, dann gilt nach Satz 15.45 $\operatorname{Rang}(A) = n$. Nach Satz 16.7 besitzt auch die reduzierte Zeilenstufenform von A den Rang n, ist also die Einheitsmatrix I_n.

Aussage (ii) $\Rightarrow$ Aussage (iii): Es sei $C \in K^{n\times n}$ die reduzierte Zeilenstufenform von A. Diese ist aus A durch elementare Zeilenumformungen entstanden, also gibt es Elementarmatrizen $G_1, \dots, G_k \in K^{n\times n}$, $k \in \mathbb{N}_0$, so dass gilt:

$$C = I_n = G_k \cdots G_2\, G_1\, A.$$

Da Elementarmatrizen invertierbar sind (Lemma 15.43), folgt

$$A = G_1^{-1}\, G_2^{-1} \cdots G_k^{-1}.$$

Da die Inversen $E_i := G_i^{-1}$, $i = 1, \dots, k$, ebenfalls Elementarmatrizen sind (Lemma 15.43), folgt die gewünschte Darstellung.

Aussage (iii) $\Rightarrow$ Aussage (i): A ist als Produkt invertierbarer Elementarmatrizen wieder invertierbar (Satz 15.42). □

Bemerkung 16.9 (Erzeugendensystem der allgemeinen linearen Gruppe)**.**

(i) Die Folgerung 16.8 besagt, dass die Elementarmatrizen ein Erzeugendensystem der allgemeinen linearen Gruppe $\mathrm{GL}(n, K)$ der invertierbaren Matrizen bilden.

(ii) Da Elementarmatrizen vom Typ III ihrerseits als Produkte von Elementarmatrizen vom Typ I und Typ II dargestellt werden können, folgt, dass bereits die Elementarmatrizen vom Typ I und Typ II ein Erzeugendensystem von $\mathrm{GL}(n, K)$ bilden. △

(**Quizfrage 16.2:** Welche Untergruppe wird alleine von den Elementarmatrizen vom Typ I erzeugt? Welche von den Elementarmatrizen vom Typ II?)

Wir geben nun anhand von Beispielen die Bestimmung der reduzierten Zeilenstufenform für eine erweiterte Koeffizientenmatrizen $[A, b]$ an und wie wir daraus die Lösungsmenge des linearen Gleichungssystems $A\,x = b$ ablesen können. Dabei kommen alle drei Fälle (eindeutige Lösbarkeit, nicht-eindeutige Lösbarkeit und Nicht-Lösbarkeit) vor.

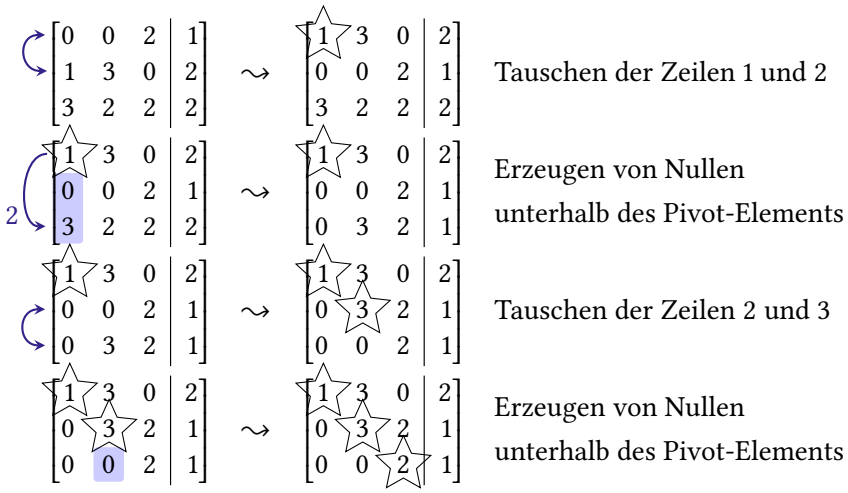
Beispiel 16.10 (Gaußsches Eliminationsverfahren)**.**
Wir betrachten drei lineare Gleichungssysteme über dem endlichen Körper $(\mathbb{Z}_5, +_5, \cdot_5)$, vgl. Folgerung 10.4. Der Einfachheit halber schreiben wir die Verknüpfungen als + und · (statt $+_5$ und $\cdot_5$) und wiederholen sie hier:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

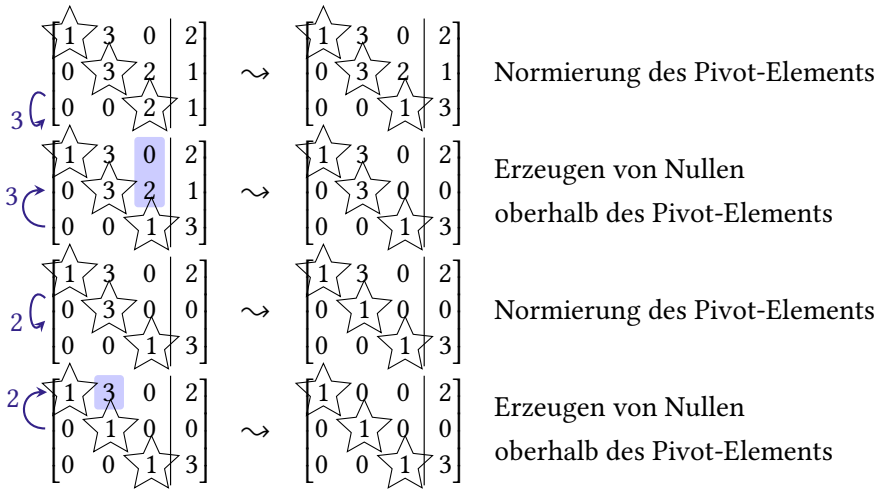
·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

In allen Fällen werden wir $m = 3$ Variablen und $n = 3$ Gleichungen verwenden.

(i) Wir betrachten das lineare Gleichungssystem



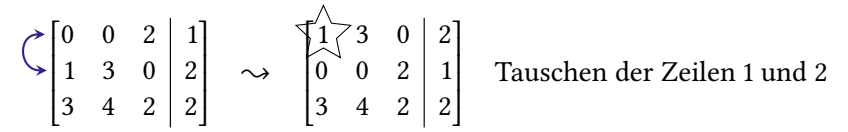
An dieser Stelle ist eine Zeilenstufenform hergestellt. Wir erkennen $\operatorname{Rang}(A) = 3 = m$, also ist die Matrix invertierb und das System für jede rechte Seite eindeutig lösbar. Wir gehen weiter zur reduzierten Zeilenstufenform:

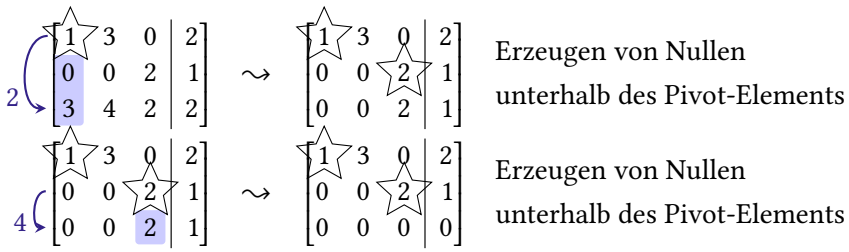


Wir haben in diesem Fall also die abhängigen Indizes $\mathcal{A} = (1, 2, 3)$ und keinen unabhängigen Index, also die leere Familie $\mathcal{I} = ()$. Hier können wir nun die eindeutige Lösung ablesen, nämlich $x = (2, 0, 3)^\mathsf{T}$. Wir führen die Probe durch:

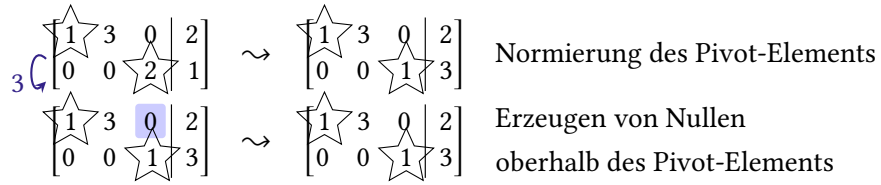
$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 3 & 0 \\ 3 & 2 & 2 \end{bmatrix} \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}.$$

(ii) Wir betrachten das lineare Gleichungssystem





An dieser Stelle ist eine Zeilenstufenform hergestellt. Wir erkennen $\operatorname{Rang}(A) = \operatorname{Rang}([A,b]) = 2 = m-1$, also ist das System lösbar, und die Lösungsmenge des homogenen Systems hat $\dim(\mathcal{L}(A,0)) = 1$. Wir gehen weiter zur reduzierten Zeilenstufenform:



Wir haben in diesem Fall also die abhängigen Indizes $\mathcal{A} = (1,3)$ und einen einzelnen unabhängigen Index $\mathcal{I} = (2)$.

Eine partikuläre Lösung erhalten wir, indem wir die unabhängige Variable $x_2 := 0$ setzen und die abhängigen Variablen mit Hilfe des Systems berechnen. Da wir die Pivot-Elemente auf 1 normiert haben, müssen wir dazu lediglich die rechte Seite ablesen und die Elemente an der richtigen Stelle (wie durch die Pivot-Spalten vorgegeben) in den Lösungsvektor eintragen. Wir erhalten so die partikuläre Lösung $x_0 = (2,0,3)^\mathsf{T}$. Wir führen die Probe durch:

$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 3 & 0 \\ 3 & 4 & 2 \end{bmatrix} \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}.$$

Eine Basis der Lösungsmenge des homogenen Systems

erhalten wir nach Bemerkung 16.4 dadurch, dass wir für die unabhängigen Variablen (hier nur x_2) einen der Standardbasisvektoren von K^{m-r} einsetzen (hier also nur die Zahl $x_2 := 1$) und die abhängigen Variablen von hinten nach vorne mit Hilfe der Gleichungen ausrechnen. Im vorliegenden Beispiel lesen wir aus der zweiten Gleichung

$$x_3 = 0$$

ab und anschließend aus der ersten Gleichung

$$x_1 + 3\,x_2 = 0 \quad \Leftrightarrow \quad x_1 = -3\,x_2 = 2\,x_2 = 2 \cdot 1 = 2.$$

Die Lösungsmenge des homogenen Systems besteht also gerade aus allen Vielfachen des Vektors $(2,1,0)^\mathsf{T}$. Wir führen auch hier die Probe durch:

$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 3 & 0 \\ 3 & 4 & 2 \end{bmatrix} \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Da wir es in unserem Beispiel mit dem endlichen Körper $\mathbb{Z}_5$ zu tun haben, können wir die Elemente des eindimensionalen Lösungsraumes sogar aufzählen. Es gilt

$$\begin{aligned}\mathcal{L}(A,b) &= \begin{pmatrix}2\\0\\3\end{pmatrix} + \left\{\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}2\\1\\0\end{pmatrix}, \begin{pmatrix}4\\2\\0\end{pmatrix}, \begin{pmatrix}1\\3\\0\end{pmatrix}, \begin{pmatrix}3\\4\\0\end{pmatrix}\right\} \\ &= \left\{\begin{pmatrix}2\\0\\3\end{pmatrix}, \begin{pmatrix}4\\1\\3\end{pmatrix}, \begin{pmatrix}1\\2\\3\end{pmatrix}, \begin{pmatrix}3\\3\\3\end{pmatrix}, \begin{pmatrix}0\\4\\3\end{pmatrix}\right\}.\end{aligned}$$

(*iii*) Wir betrachten das lineare Gleichungssystem

$$\left[\begin{array}{ccc|c}0&0&2&1\\1&3&0&2\\3&4&2&3\end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c}1&3&0&2\\0&0&2&1\\3&4&2&3\end{array}\right] \quad \text{Tauschen der Zeilen 1 und 2}$$

$$\left[\begin{array}{ccc|c}1&3&0&2\\0&0&2&1\\3&4&2&3\end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c}1&3&0&2\\0&0&2&1\\0&0&2&2\end{array}\right] \quad \begin{array}{l}\text{Erzeugen von Nullen}\\ \text{unterhalb des Pivot-Elements}\end{array}$$

$$\left[\begin{array}{ccc|c}1&3&0&2\\0&0&2&1\\0&0&2&2\end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c}1&3&0&2\\0&0&2&1\\0&0&0&1\end{array}\right] \quad \begin{array}{l}\text{Erzeugen von Nullen}\\ \text{unterhalb des Pivot-Elements}\end{array}$$

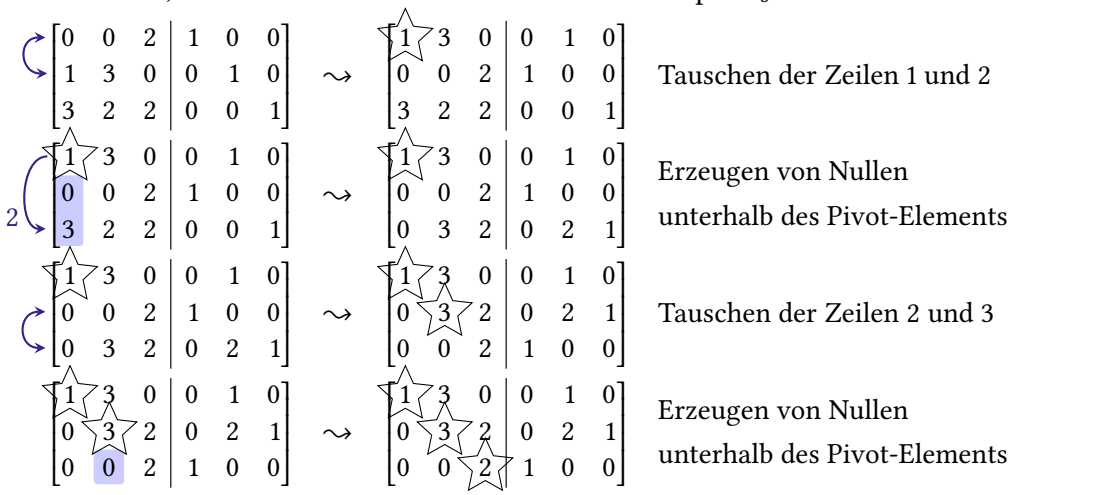
An dieser Stelle ist eine Zeilenstufenform hergestellt. Wir erkennen nun $\operatorname{Rang}(A) = 2$, aber $\operatorname{Rang}([A,b]) = 3$. Das heißt, das System ist nicht lösbar, vgl. Satz 16.3. Die reduzierte Zeilenstufenform muss daher nicht bestimmt werden. △

Abschließend bemerken wir, dass wir mit Hilfe der Transformation in reduzierte Zeilenstufenform nicht nur ein einzelnes lineares Gleichungssystem $Ax = b$ lösen können, sondern mehrere Systeme gleichzeitig, sofern diese sich nur in der rechten Seite unterscheiden. Haben wir $k \in \mathbb{N}_0$ rechte Seiten, so schreiben wir diese spaltenweise als $n \times k$-Matrix B. Das System für die k unbekannten Spaltenvektoren in der $n \times k$-Matrix X lautet dann $AX = B$. Die Transformation auf Zeilenstufenform geschieht einfach für alle Spalten der erweiterten Koeffizientenmatrix $[A, B]$ gleichzeitig. Wie gewohnt können wir an der Zeilenstufenform ablesen, für welche rechten Seiten das System lösbar ist. Die rechten Seiten, die zu unlösbaren Systemen führen, können wir vor der Herstellung der reduzierten Zeilenstufenform einfach herausstreichen (oder auch stehenlassen). Wir erhalten dann für jede rechte Seite, für die das System lösbar ist, eine partikuläre Lösung. Die Lösungsmenge des homogenen System ist für alle rechten Seite dieselbe, da das homogene System ja dasselbe ist.

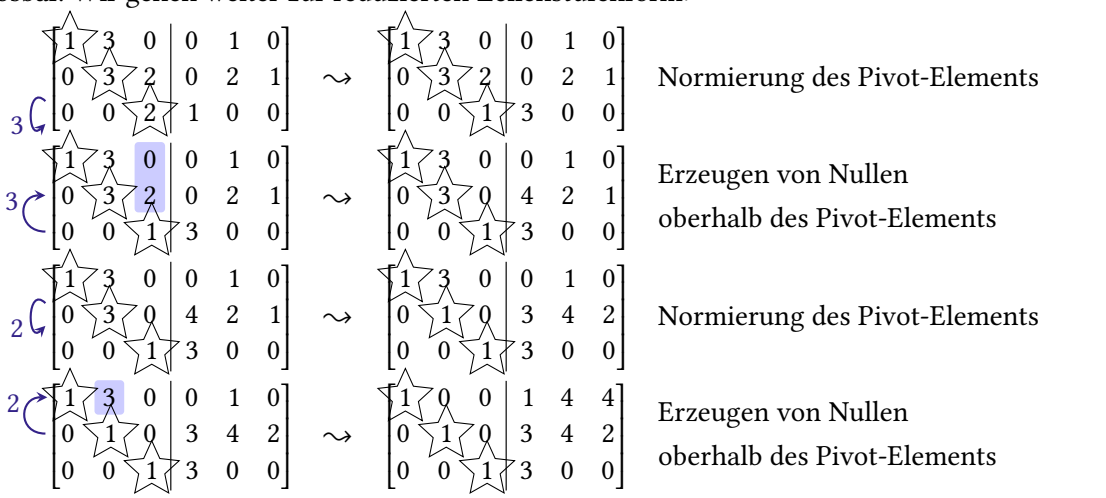
Ein wichtiger Anwendungsfall ist die Bestimmung der inversen Matrix einer quadratischen $n \times n$-Matrix A. Dies kann man durch die rechte Seite $B = I_n$ und Lösen des Systems $AX = I_n$ erreichen. An der Zeilenstufenform erkennt man, ob A invertierbar ist. Wenn ja, hat man am Ende rechts die inverse Matrix stehen.

Beispiel 16.11 (Berechnung der inversen Matrix, vgl. Beispiel 16.10)**.**

Wir führen die Berechnung der inversen Matrix für die erste Matrix aus Beispiel 16.10 vor. Wir erinnern daran, dass wir es hier mit Matrizen über dem Körper $\mathbb{Z}_5$ zu tun haben.



An dieser Stelle ist eine Zeilenstufenform hergestellt. Wir erkennen $\operatorname{Rang}(A) = \operatorname{Rang}([A, b]) = 3 = m$ für jede Spalte b der rechten Seite, also ist das System für jede der rechten Seiten eindeutig lösbar. Wir gehen weiter zur reduzierten Zeilenstufenform:



Die Matrix auf der rechten Seite ist die Inverse der Ausgangsmatrix.

Wir führen die Probe durch:

$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 3 & 0 \\ 3 & 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 4 & 4 \\ 3 & 4 & 2 \\ 3 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \qquad \triangle$$

Ende der Vorlesung 22

§ 17 Homomorphismen von Vektorräumen

Literatur: Fischer, Springborn, 2020, Kapitel 3.1–3.2; Bosch, 2014, Kapitel 2; Beutelspacher, 2014, Kapitel 5.1 und 5.3; Deiser, 2024b, Kapitel 3.3; Jänich, 2008, Kapitel 4

In diesem Abschnitt geht es um die Homomorphismen, also die strukturverträglichen Abbildungen zwischen Vektorräumen über demselben Körper.

Definition 17.1 (Vektorraumhomomorphismus, vgl. Definition 10.11 eines Körperhomomorphismus)**.**
Es seien $(V, +_1, \cdot_1)$, $(W, +_2, \cdot_2)$ Vektorräume über demselben Körper K.

(*i*) Eine Abbildung $f\colon V \to W$ heißt **strukturverträglich** oder ein **Homomorphismus von Vektorräumen** (englisch: vector space homomorphism) oder eine **lineare Abbildung** (englisch: linear map) von $(V, +_1, \cdot_1)$ in $(W, +_2, \cdot_2)$, wenn gilt:

$$f(u +_1 v) = f(u) +_2 f(v) \quad \text{für alle } u, v \in V, \tag{17.1a}$$
$$f(\alpha \cdot_1 u) = \alpha \cdot_2 f(u) \quad \text{für alle } u \in V \text{ und alle } \alpha \in K. \tag{17.1b}$$

Man bezeichnet die Eigenschaft (17.1a) auch als die **Additivität** (englisch: additivity) und die Eigenschaft (17.1b) als die **Homogenität** (englisch: homogeneity) der Abbildung f.

(*ii*) Ist $f\colon V \to W$ strukturverträglich und gilt $(V, +_1, \cdot_1) = (W, +_2, \cdot_2)$, so sprechen wir auch von einem **Endomorphismus eines Vektorraumes** (englisch: vector space endomorphism) oder einem **linearen Endomorphismus** (englisch: linear endomorphism)..

(*iii*) Ist $f\colon V \to W$ strukturverträglich und bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus von Vektorräumen** (englisch: vector space isomorphism) oder ein **linearer Isomorphismus** (englisch: linear isomorphism). In diesem Fall nennen wir $(V, +_1, \cdot_1)$ und $(W, +_2, \cdot_2)$ auch zueinander **isomorphe Vektorräume** (englisch: isomorphic vector spaces) und schreiben

$$(V, +_1, \cdot_1) \cong (W, +_2, \cdot_2).$$

(*iv*) Ist $f\colon V \to W$ strukturverträglich und bijektiv und gilt $(V, +_1, \cdot_1) = (W, +_2, \cdot_2)$, so sprechen wir auch von einem **Automorphismus eines Vektorraumes** (englisch: vector space automorphism) oder einem **linearen Automorphismus** (englisch: linear automorphism). △

Bemerkung 17.2 (zu Definition 17.1)**.**

(*i*) Die Vektorräume $(V, +_1, \cdot_1)$ und $(W, +_2, \cdot_2)$ sind insbesondere (abelsche) Gruppen $(V, +_1)$ und $(W, +_2)$. Aufgrund der Bedingung (17.1a) ist jeder Vektorraumhomomorphismus insbesondere ein Gruppenhomomorphismus. Wir können daher Ergebnisse aus § 8 verwenden.

(*ii*) Im Folgenden werden wir zulassen, die Vektorraumoperationen + und · in beiden Vektorräumen mit demselben Symbol (und demselben Symbol wie im zugrundeliegenden Körper) zu notieren. △

Satz 17.3 (Komposition von Vektorraumhomomorphismen, Inverse von Vektorraumisomorphismen, vgl. Satz 10.12 zu Körperhomomorphismen)**.**
Es seien U, V, W Vektorräume über demselben Körper K.

(*i*) Sind $f\colon U \to V$ und $g\colon V \to W$ lineare Abbildungen, dann ist auch $g \circ f\colon U \to W$ eine lineare Abbildung.

(*ii*) Ist $f\colon U \to V$ eine bijektive lineare Abbildung, dann ist auch $f^{-1}\colon V \to U$ eine bijektive lineare Abbildung.

Beweis. Der Beweis ist Gegenstand der Übung. □

Folgerung 17.4 (Isomorphie von Vektorräumen ist eine Äquivalenzrelation, vgl. Folgerung 10.13 zur Isomorphie von Körpern)**.**

Isomorphie ist eine Äquivalenzrelation auf der Klasse aller Vektorräume über demselben Körper K.

Beispiel 17.5 (Vektorraumhomomorphismus)**.**

(*i*) Die Vektorräume K_n und K^n über einem Körper K sind zueinander isomorph. Die Abbildung

$$\cdot^{\mathsf{T}}\colon K_n \ni x \mapsto x^{\mathsf{T}} \in K^n$$

ist ein linearer Isomorphismus, vgl. (15.25a) und (15.25b). (**Quizfrage 17.1:** Wie sieht der inverse Vektorraumisomorphismus aus? Gibt es weitere mögliche Vektorraumisomorphismen?)

(*ii*) Der Vektorraum der $n \times m$-Matrizen $K^{n\times m}$ über einem Körper K ist isomorph zum Vektorraum $K^{n\,m}$. Die **Vektorisierung** (englisch: vectorization)

$$\operatorname{vec}\colon K^{n\times m} \ni A \mapsto \operatorname{vec}(A) \in K^{n\,m},$$

definiert durch „Übereinanderstapeln“ der Spalten, also

$$\operatorname{vec}\left(\begin{bmatrix} | & & | \\ a_{\bullet 1} & \cdots & a_{\bullet m} \\ | & & | \end{bmatrix}\right) := \begin{pmatrix} a_{\bullet 1} \\ \vdots \\ a_{\bullet m} \end{pmatrix},$$

ist ein linearer Isomorphismus. (**Quizfrage 17.2:** Wie sieht der inverse Vektorraumisomorphismus aus?)

(*iii*) Im Standardvektorraum K^n über einem Körper K ist die **Projektion auf die i-te Koordinate** (englisch: projection onto the i-th coordinate), gegeben durch

$$\pi_i\colon K^n \ni x \mapsto x_i \in K \tag{17.2}$$

für $1 \leqslant i \leqslant n \in \mathbb{N}$, eine surjektive lineare Abbildung. (**Quizfrage 17.3:** Ist sie auch injektiv?)

(*iv*) Es seien K ein Körper und $n, m \in \mathbb{N}_0$. Für eine Matrix $A \in K^{n\times m}$ ist die Matrix-Vektor-Multiplikation mit A

$$f_A \colon K^m \ni x \mapsto f_A(x) \coloneqq A\,x \in K^n \tag{17.3}$$

eine lineare Abbildung. Sie wird die **von A induzierte lineare Abbildung** genannt (englisch: linear map induced by A). Ihre Eigenschaften untersuchen wir in § 17.2.

Wie wir in § 19 sehen werden, ist die Matrix-Vektor-Multiplikation der Prototyp einer linearen Abbildung zwischen endlich-dimensionalen Vektorräumen. Jede lineare Abbildung kann in Form von Matrix-Vektor-Multiplikation geschrieben werden. △

Expertenwissen: weitere lineare Abbildungen

Mit Kenntnissen aus Lehrveranstaltungen zur *Analysis* können wir zum Beispiel die Linearität der folgenden Abbildungen bestätigen:

(*i*) Die **Grenzwert-Abbildung**, definiert beispielsweise auf dem Vektorraum der konvergenten $\mathbb{R}$-wertigen Folgen $(\mathbb{R}^{\mathbb{N}})_c$ nach $\mathbb{R}$, also

$$\lim \colon (\mathbb{R}^{\mathbb{N}})_c \ni (y_n)_{n\in\mathbb{N}_0} \mapsto \lim_{n\to\infty}(y_n) \in \mathbb{R}$$

ist eine surjektive lineare Abbildung. (**Quizfrage 17.4:** Ist sie auch injektiv?)

(*ii*) Die **Ableitungsabbildung** (englisch: differentiation map), definiert beispielsweise auf dem Vektorraum der differenzierbaren Funktionen $(a, b) \to \mathbb{R}$ in den Vektorraum der Funktionen $(a, b) \to \mathbb{R}$, also

$$\cdot' \colon \left\{ f \in \mathbb{R}^{(a,b)} \,\middle|\, f \text{ ist differenzierbar} \right\} \ni f \mapsto f' \in \mathbb{R}^{(a,b)}$$

ist eine lineare Abbildung, die nicht surjektiv und nicht injektiv ist. (**Quizfrage 17.5:** Warum?)

Lemma 17.6 (Eigenschaften linearer Abbildungen)**.**
Es seien V, W Vektorräume über demselben Körper K. Weiter sei $f \colon V \to W$ eine lineare Abbildung. Dann gilt:

(*i*) $f(0) = 0$.

(*ii*) $f(-v) = -f(v)$ für alle $v \in V$.

(*iii*) $f\left(\sum_{i=1}^n \alpha_i\, v_i\right) = \sum_{i=1}^n \alpha_i\, f(v_i)$ für alle $n \in \mathbb{N}_0$, $\alpha_i \in K$ und $v_i \in V$.
(Das Bild einer Linearkombination von Vektoren ist also die Linearkombination der Bilder dieser Vektoren.)

(*iv*) Ist $E \subseteq V$, dann gilt $f\big(\langle E\rangle\big) = \big\langle f(E)\big\rangle$.
(Das Bild der linearen Hülle einer Menge ist die lineare Hülle des Bildes der Menge.)

(*v*) Ist $F = (v_i)_{i\in I}$ eine Familie von Vektoren in V, dann gilt $f\big(\langle F\rangle\big) = \big\langle f(F)\big\rangle$.
(Das Bild der linearen Hülle einer Familie ist die lineare Hülle des Bildes der Familie.)

(*vi*) Ist $U \subseteq V$ ein Unterraum, dann ist $f(U) \subseteq W$ ein Unterraum.
(Das Bild eines Unterraumes ist wieder ein Unterraum.)

(*vii*) Ist $Z \subseteq W$ ein Unterraum, dann ist $f^{-1}(Z) \subseteq V$ ein Unterraum.
(Das Urbild eines Unterraumes ist wieder ein Unterraum.)

(*viii*) Ist $M \subseteq V$ eine linear abhängige Menge von Vektoren, dann ist auch $f(M) \subseteq W$ eine linear abhängige Menge von Vektoren.
(Lineare Abhängigkeit kann durch eine lineare Abbildung nicht geheilt werden.)

(*ix*) Ist $F = (v_i)_{i\in I}$ eine linear abhängige Familie von Vektoren in V, dann ist auch $(f(v_i))_{i\in I}$ eine linear abhängige Familie von Vektoren.
(Lineare Abhängigkeit kann durch eine lineare Abbildung nicht geheilt werden.)

Beweis. Aussage (*i*) und Aussage (*ii*) folgen sofort aus Lemma 8.8.

Aussage (*iii*):

$$\begin{aligned} f\Big(\sum_{i=1}^{n} \alpha_i\, v_i\Big) &= \sum_{i=1}^{n} f(\alpha_i\, v_i) && \text{durch wiederholte Anwendung von (17.1a)} \\ &= \sum_{i=1}^{n} \alpha_i\, f(v_i) && \text{durch Anwendung von (17.1b) auf jeden Summanden} \end{aligned}$$

Aussage (*iv*): Nach Satz 11.16 besteht $\langle E\rangle$ gerade aus den Linearkombinationen von E, während $\big\langle f(E)\big\rangle$ aus den Linearkombinationen von $f(E)$ besteht. Nach Aussage (*iii*) sind das aber dieselben Mengen.

Aussage (*v*): Nach Satz 11.16 besteht $\langle F\rangle$ gerade aus den Linearkombinationen von F, während $\big\langle f(F)\big\rangle$ aus den Linearkombinationen von $(f(v_i))_{i\in I}$ besteht. Nach Aussage (*iii*) sind das aber dieselben Mengen.

Aussage (*vi*): Wir verwenden das Unterraumkriterium (Satz 11.11). Wegen $0 \in U$ und Aussage (*i*) ist $0 \in f(U)$, also ist $f(U) \neq \emptyset$. Sind weiter $w_1, w_2 \in f(U)$, dann gibt es $u_1, u_2 \in U$ mit $w_1 = f(u_1)$ und $w_2 = f(u_2)$. Für $\alpha_1, \alpha_2 \in K$ gilt

$$\alpha_1\, w_1 + \alpha_2\, w_2 = \alpha_1\, f(u_1) + \alpha_2\, f(u_2) = f(\alpha_1\, u_1 + \alpha_2\, u_2).$$

Wegen der Unterraumeigenschaft gehört $\alpha_1\, u_1 + \alpha_2\, u_2$ zu U, also gehört $\alpha_1\, w_1 + \alpha_2\, w_2$ zu $f(U)$.

Aussage (*vii*): Wir verwenden nochmal das Unterraumkriterium (Satz 11.11). Wegen $0 \in Z$ und Aussage (*i*) ist $0 \in f^{-1}(Z)$, also ist $f^{-1}(Z) \neq \emptyset$. Sind weiter $u_1, u_2 \in f^{-1}(Z)$, dann gibt es $w_1, w_2 \in Z$ mit $w_1 = f(u_1)$ und $w_2 = f(u_2)$. Für $\alpha_1, \alpha_2 \in K$ gilt

$$\alpha_1\, w_1 + \alpha_2\, w_2 = \alpha_1\, f(u_1) + \alpha_2\, f(u_2) = f(\alpha_1\, u_1 + \alpha_2\, u_2).$$

Wegen der Unterraumeigenschaft gehört $\alpha_1\, w_1 + \alpha_2\, w_2$ zu Z, also gehört $\alpha_1\, u_1 + \alpha_2\, u_2$ zu $f^{-1}(Z)$.

Aussage (*viii*): Es sei $M \subseteq V$ eine linear abhängige Menge, d. h., es gibt ein $n \in \mathbb{N}_0$ und paarweise verschiedene Vektoren $v_1, \ldots, v_n \in M$ sowie Koeffizienten $\alpha_1, \ldots, \alpha_n \in K$, die nicht alle gleich 0 sind, sodass gilt: $\sum_{i=1}^{n} \alpha_i\, v_i = 0$. Es folgt mit Aussage (*iii*) und Aussage (*i*)

$$\sum_{i=1}^{n} \alpha_i\, f(v_i) = f\Big(\sum_{i=1}^{n} \alpha_i\, v_i\Big) = f(0) = 0.$$

Das bedeutet aber gerade die lineare Abhängigkeit der Menge $f(M)$.

Aussage (ix): Es sei $F = (v_i)_{i\in I}$ eine linear abhängige Familie von Vektoren in V, d. h., es gibt ein $n \in \mathbb{N}_0$ und paarweise verschiedene Indizes $i_1, \dots, i_n \in I$ sowie Koeffizienten $\alpha_1, \dots, \alpha_n \in K$, die nicht alle gleich 0 sind, sodass gilt: $\sum_{\ell=1}^{n} \alpha_\ell v_{i_\ell} = 0$. Es folgt mit Aussage (iii) und Aussage (i)

$$\sum_{\ell=1}^{n} \alpha_\ell f(v_{i_\ell}) = f\Big(\sum_{\ell=1}^{n} \alpha_\ell v_{i_\ell}\Big) = f(0) = 0.$$

Das bedeutet aber gerade die lineare Abhängigkeit der Familie $(f(v_i))_{i\in I}$. □

Definition 17.7 (Bild und Kern einer linearen Abbildung, vgl. Definition 10.17 von Bild und Kern eines Körperhomomorphismus)**.**
Es seien V, W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ eine lineare Abbildung.

(i) Das **Bild** (englisch: image) von f ist definiert als

$$\mathrm{Bild}(f) \coloneqq \{f(u) \in W \mid u \in V\} = f(V). \tag{17.4}$$

(ii) Der **Kern** (englisch: kernel, null space[26]) von f ist definiert als

$$\mathrm{Kern}(f) \coloneqq \{u \in V \mid f(u) = 0_W\} = f^{-1}(\{0_W\}) \tag{17.5}$$

△

Lemma 17.8 (Kern und Bild linearer Abbildungen)**.**
Es seien V, W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ eine lineare Abbildung.

(i) $\mathrm{Bild}(f)$ ist ein Unterraum von W.

(ii) $\mathrm{Kern}(f)$ ist ein Unterraum von V.

Beweis. Aussage (i): V ist selbst ein Unterraum von V, daher ist $\mathrm{Bild}(f) = f(V)$ nach Lemma 17.6 (vi) ein Unterraum von W.

Aussage (ii): $\{0\}$ ist ein Unterraum von W, daher ist $\mathrm{Kern}(f) = f^{-1}(\{0\})$ nach Lemma 17.6 (vii) ein Unterraum von V. □

Lemma 17.9 (Charakterisierung der Injektivität linearer Abbildungen, vgl. Lemma 9.24 für Ringhomomorphismen)**.**
Es seien V, W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ eine lineare Abbildung. Dann sind äquivalent:

(i) f ist injektiv.

(ii) $\mathrm{Kern}(f) = \{0_V\}$.

[26] nicht zu verwechseln mit dem Begriff *zero vector space* (Nullraum) $\{0\}$, siehe Beispiel 11.3

(*iii*) Die einzige Lösung der Gleichung $f(a) = 0_W$ ist $a = 0_V$.

Beweis. Weder der Begriff der Injektivität noch die Definition von $\mathrm{Kern}(f) := \{u \in V \mid f(u) = 0\}$ ändern sich, wenn wir die lineare Abbildung $f\colon (V,+,\cdot) \to (W,+,\cdot)$ als Gruppenhomomorphismus $f\colon (V,+) \to (W,+)$ auffassen. Das Resultat folgt daher aus Lemma 8.13 (Charakterisierung der Injektivität für Gruppenhomomorphismen). □

§ 17.1 Konstruktion linearer Abbildungen

Wir zeigen nun, dass eine lineare Abbildung $V \to W$ durch die Bilder auf einer Basis von V bereits eindeutig festgelegt ist. Das gilt gleichermaßen für Basismengen wie für Basisfamilien (Definition 13.1). In Vorbereitung auf die spätere Darstellung linearer Abbildungen durch Matrizen (§ 19) bietet es sich aber bereits jetzt an, nur noch mit Basisfamilien zu arbeiten. Der Einfachheit halber werden wir diese ab sofort auch einfach als Basis bezeichnen.

Satz 17.10 (Existenz- und Eindeutigkeitssatz für Vektorraumhomomorphismen, vgl. Satz 8.14 für Gruppenhomomorphismen)**.**
Es seien V, W Vektorräume über demselben Körper K. Weiter sei $(v_i)_{i\in I}$ eine Familie von Vektoren in V und $(w_i)_{i\in I}$ eine Familie von Vektoren in W mit gleicher Indexmenge I.

(*i*) Ist $B := (v_i)_{i\in I}$ eine Basis von V, dann gibt es genau eine lineare Abbildung $f\colon V \to W$ mit der Eigenschaft $f(v_i) = w_i$ für alle $i \in I$.

Diese Abbildung hat außerdem folgende Eigenschaften:

(a) $\mathrm{Bild}(f) = \langle (w_i)_{i\in I} \rangle$.
(Die Bilder der Basisvektoren von V erzeugen den Bildraum $\mathrm{Bild}(f)$.)

(b) f ist surjektiv genau dann, wenn $\langle (w_i)_{i\in I} \rangle = W$ gilt.

(c) f ist injektiv genau dann, wenn $(w_i)_{i\in I}$ linear unabhängig ist.

(d) f ist bijektiv genau dann, wenn $(w_i)_{i\in I}$ eine Basis von W ist.

(*ii*) $^{\mathrm{AoC}}$ Ist $(v_i)_{i\in I}$ linear unabhängig, dann gibt es eine lineare Abbildung $f\colon V \to W$ mit der Eigenschaft $f(v_i) = w_i$ für alle $i \in I$.

Beweis. Wir beginnen mit Aussage (*i*).

Schritt 1: Wir konstruieren eine Abbildung $f\colon V \to W$ mit den gesuchten Eigenschaften.

Da $B = (v_i)_{i\in I}$ eine Basis von V ist, kann jedes $v \in V$ nach Satz 13.3 auf (bis auf Nullkoeffizienten) eindeutige Art und Weise als Linearkombination $v = \sum_{i\in I_0} \alpha_i v_i$ geschrieben werden. Daher ergibt die die Setzung

$$f(v) := \sum_{\ell=1}^{n} \alpha_\ell w_{i_\ell} \sum_{i\in I_0} \alpha_i w_i$$

eine wohldefinierte Funktion. (**Quizfrage 17.6:** Warum ist die Eindeutigkeit der Darstellung von v bis auf Nullkoeffizienten für die Wohldefiniertheit schon ausreichend?)

Wegen $v_i = 1\,v_i$ gilt

$$f(v_i) = f(1\,v_i) = 1\,w_i = w_i$$

erfüllt f wie gefordert die Bedingung $f(v_i) = w_i$.

Schritt 2: Wir zeigen: Die so definierte Abbildung $f\colon V \to W$ ist linear.

Sind $v = \sum_{i\in I_0} \alpha_i\, v_i$ und $w = \sum_{i\in I_1} \beta\, v_i$ zwei beliebige Vektoren aus V, dann können wir durch Hinzufügen von Nullkoeffizienten erreichen, dass beide Darstellungen dieselben endlich vielen Indizes aus $I_{01} \coloneqq I_0 \cup I_1$ verwenden, also $v = \sum_{i\in I_{01}} \alpha_i\, v_i$ und $w = \sum_{i\in I_{01}} \beta\, v_i$. Es gilt

$$\begin{aligned}
f(v+w) &= f\Big(\sum_{i\in I_{01}} \alpha_i\, v_i + \sum_{i\in I_{01}} \beta\, v_i\Big) && \text{nach Darstellung von } v \text{ und } w\\
&= f\Big(\sum_{i\in I_{01}} (\alpha_i + \beta_i)\, v_i\Big) && \text{nach Distributivgesetz (11.1c) und Kommutativität}\\
&= \sum_{i\in I_{01}} (\alpha_i + \beta_i)\, w_i && \text{nach Definition von } f\\
&= \sum_{i\in I_{01}} \alpha_i\, w_i + \sum_{i\in I_{01}} \beta_i\, w_i && \text{nach Distributivgesetz (11.1c)}\\
&= f(v) + f(w) && \text{nach Definition von } f
\end{aligned}$$

und außerdem für $\alpha \in K$

$$\begin{aligned}
f(\alpha\, v) &= f\Big(\alpha \sum_{i\in I_0} \alpha_i\, v_i\Big) && \text{nach Darstellung von } v\\
&= f\Big(\sum_{i\in I_0} (\alpha\,\alpha_i)\, v_i\Big) && \text{nach Distributivgesetz (11.1b)}\\
&= \sum_{i\in I_0} (\alpha\,\alpha_i)\, w_i && \text{nach Definition von } f\\
&= \alpha \sum_{i\in I_0} \alpha_i\, w_i && \text{nach Distributivgesetz (11.1b)}\\
&= \alpha\, f(v) && \text{nach Definition von } f.
\end{aligned}$$

Schritt 3: Wir zeigen die Eindeutigkeit von f.

Dazu sei $g\colon V \to W$ eine weitere lineare Abbildung mit der Eigenschaft $g(v_i) = w_i$. Ist $v \in V$ ein beliebiger Vektor mit der i. W. eindeutigen Darstellung $v = \sum_{i\in I_0} \alpha_i\, v_i$, dann gilt

$$\begin{aligned}
g(v) &= g\Big(\sum_{i\in I_0} \alpha_i\, v_i\Big) && \text{wegen der Darstellung von } v\\
&= \sum_{i\in I_0} \alpha_i\, g(v_i) && \text{wegen der Linearität von } g\\
&= \sum_{i\in I_0} \alpha_i\, w_i && \text{wegen der Eigenschaft } g(v_i) = w_i\\
&= f(v) && \text{nach Definition von } f.
\end{aligned}$$

Also muss g notwendig mit f übereinstimmen.

Wir kommen zu den weiteren Eigenschaften der Abbildung f.

Aussage (a): Es gilt

$$\begin{aligned}
\operatorname{Bild}(f) &= f(V) && \text{nach Definition von Bild}(f)\\
&= f\big(\langle (v_i)_{i\in I}\rangle\big) && \text{denn } (v_i)_{i\in I} \text{ ist eine Basis von } V\\
&= \big\langle (f(v_i))_{i\in I}\big\rangle && \text{nach Lemma 17.6 } (v)\\
&= \langle (w_i)_{i\in I}\rangle && \text{nach Definition von } f.
\end{aligned}$$

Aussage (b): $f\colon V \to W$ ist nach Definition surjektiv genau dann, wenn $\operatorname{Bild}(f) = W$ ist, also nach Aussage (a) genau dann, wenn $\langle (w_i)_{i\in I}\rangle = W$ gilt.

Aussage (c): Es sei zunächst die Familie $(w_i)_{i\in I}$ linear abhängig, d. h., es gibt eine endliche Teilmenge $I_0 \subseteq I$ und Koeffizienten $\alpha_i \in K$ mit $i \in I_0$, die nicht alle gleich 0 sind, sodass gilt: $\sum_{i\in I_0} \alpha_i w_i = 0$. Dann ist $v := \sum_{i\in I_0} \alpha_i v_i$ nicht der Nullvektor in V, da $(v_i)_{i\in I}$ eine Basis von V ist, jedoch gilt

$$f(v) = f\Big(\sum_{i\in I_0} \alpha_i v_i\Big) = \sum_{i\in I_0} \alpha_i w_i = 0.$$

Das bedeutet $f(v) = f(0) = 0$, also ist f nicht injektiv.

Nun sei umgekehrt $(w_i)_{i\in I}$ linear unabhängig und $v \in V$ ein Vektor mit $f(v) = 0$. Der Vektor v hat eine Darstellung $v = \sum_{i\in I_0} \alpha_i v_i$ mit einer endlichen Indexmenge $I_0 \subseteq I$, und es gilt

$$0 = f(v) = f\Big(\sum_{i\in I_0} \alpha_i v_i\Big) = \sum_{i\in I_0} \alpha_i w_i.$$

Aufgrund der linearen Unabhängigkeit der Familie $(w_i)_{i\in I}$ ist das nur möglich, wenn alle $\alpha_i = 0$ sind, also nur dann, wenn $v = 0$ ist. Mit anderen Worten, $\operatorname{Kern}(f) = \{0\}$, und nach Lemma 17.9 ist f injektiv.

Aussage (d) folgt sofort aus Aussage (b) und Aussage (c).

Nun kommen wir zur Aussage *(ii)*. Es sei also $(v_i)_{i\in I}$ linear unabhängig. Wir nutzen den Basisergänzungssatz 13.5 (der im Fall, dass V unendlich-dimensional ist, das Zornsche Lemma und damit das Auswahlaxiom verwendet[AoC]) und ergänzen die Menge zu einer Basis $(v_i)_{i\in\widehat{I}}$ von V. Wir wählen die fehlenden w_i für $\widehat{I} \setminus I$ als beliebige Vektoren in W (beispielsweise alle als den Nullvektor). Nach Aussage *(i)* gibt es dann eine (eindeutige) lineare Abbildung $f\colon V \to W$ mit der Eigenschaft $f(v_i) = w_i$ für alle $i \in \widehat{I}$, insbesondere für alle $i \in I$. □

Beispiel 17.11 (Konstruktion linearer Abbildungen)**.**

(i) Es sei V ein Vektorraum über dem Körper K. Dann ist eine lineare Abbildung $f\colon K \to V$ durch einen einzigen Funktionswert, etwa $f(1) \in V$, festgelegt.

(ii) Es sei K ein Körper und $(e_1, \dots, e_m)$ die Standardbasis im Vektorraum K^m, $m \in \mathbb{N}_0$. Eine lineare Abbildung $f\colon K^m \to K^n$ ist dadurch festgelegt, dass wir die Bilder $f(e_1), \dots, f(e_m)$

der m Basisvektoren angeben, also m Elemente von K^n. Tragen wir diese Bilder spaltenweise in eine Matrix

$$A \coloneqq \begin{bmatrix} | & & | \\ f(e_1) & \cdots & f(e_m) \\ | & & | \end{bmatrix}$$

ein, so gilt

$$f(x) = f\Big(\sum_{j=1}^{m} x_j\, e_j\Big) = \sum_{j=1}^{m} x_j\, f(e_j) = A\,x.$$

Jede lineare Abbildung $f\colon K^m \to K^n$ kann also durch Matrix-Vektor-Produkte $x \mapsto A\,x$ realisiert werden, wobei A spaltenweise die Bilder $f(e_j)$ der Standardbasisvektoren enthält.

(*iii*) Im Vektorraum $\mathbb{R}^2$ mit der Standardbasis $(e_1, e_2) = \left(\binom{1}{0}, \binom{0}{1}\right)$ legt

$$f(e_1) = \begin{pmatrix} \frac{1}{2}\sqrt{3} \\ \frac{1}{2} \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2}\sqrt{3} \end{pmatrix}$$

eine lineare Abbildung (einen Endomorphismus) fest, und zwar eine Drehung um den Winkel 30° im mathematisch positiven Sinn (gegen den Uhrzeigersinn) um den Ursprung. Allgemeiner beschreibt

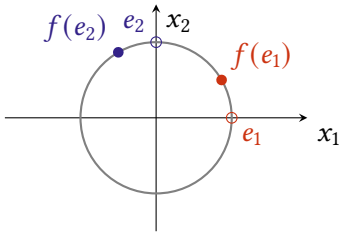
$$f(e_1) = \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix}$$

eine Drehung um den Winkel α. Da $(f(e_1),\ f(e_2))$ eine Basis von $\mathbb{R}^2$ bildet, ist die Drehabbildung nach Satz 17.10 (*ii*) bijektiv, also ein Isomorphismus $\mathbb{R}^2 \to \mathbb{R}^2$.

Die Drehabbildung kann also durch Matrix-Vektor-Produkte mit der Matrix

$$\begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \tag{17.6}$$

realisiert werden.



(*iv*) Im Vektorraum $\mathbb{R}^2$ mit der Standardbasis $(e_1, e_2) = \left(\binom{1}{0}, \binom{0}{1}\right)$ legt

$$f(e_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

eine lineare Abbildung (einen Endomorphismus) fest, und zwar eine Spiegelung an der x_1-Achse. Allgemeiner beschreibt

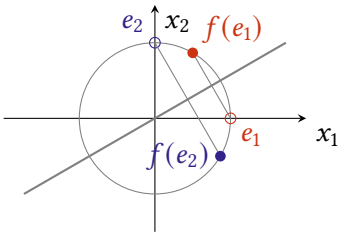
$$f(e_1) = \begin{pmatrix} \cos^2(\alpha) - \sin^2(\alpha) \\ 2\cos(\alpha)\ \sin(\alpha) \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} 2\cos(\alpha)\ \sin(\alpha) \\ \sin^2(\alpha) - \cos^2(\alpha) \end{pmatrix}$$

eine Spiegelung an derjenigen Achse durch den Ursprung, die den Winkel α gegen die x_1-Achse bildet. Da $(f(e_1), f(e_2))$ eine Basis von $\mathbb{R}^2$ bildet, ist die Spiegelungsabbildung nach Satz 17.10 bijektiv, also ein Isomorphismus $\mathbb{R}^2 \to \mathbb{R}^2$.

Die Spiegelungsabbildung kann also durch Matrix-Vektor-Produkte mit der Matrix

$$\begin{bmatrix} \cos^2(\alpha) - \sin^2(\alpha) & 2\cos(\alpha)\,\sin(\alpha) \\ 2\cos(\alpha)\,\sin(\alpha) & \sin^2(\alpha) - \cos^2(\alpha) \end{bmatrix} = \begin{bmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{bmatrix} \tag{17.7}$$

realisiert werden.[27] Das bedeutet, dass beide Basisvektoren e_1 und e_2 um den Winkel 2α rotiert werden, während der Basisvektor e_2 anschließend noch am Ursprung punktgespiegelt wird.



(*v*) Im Vektorraum $\mathbb{R}^2$ mit der Standardbasis $(e_1, e_2) = \left(\binom{1}{0}, \binom{0}{1}\right)$ legt

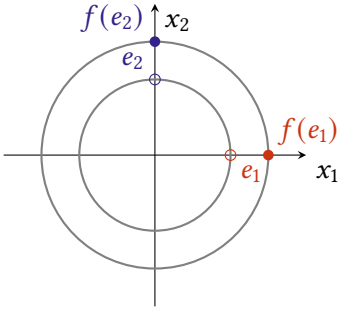
$$f(e_1) = \begin{pmatrix} \beta \\ 0 \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} 0 \\ \beta \end{pmatrix}$$

mit $\beta \in \mathbb{R}$ eine lineare Abbildung (einen Endomorphismus) fest, und zwar eine Streckung (im Fall $\beta > 0$) bzw. (im Fall $\beta < 0$) eine Streckung und Punktspiegelung am Ursprung. Da $(f(e_1), f(e_2))$ für $\beta \neq 0$ eine Basis von $\mathbb{R}^2$ bildet, ist die Streckungsabbildung nach Satz 17.10 (*ii*) in diesem Fall bijektiv, also ein Isomorphismus $\mathbb{R}^2 \to \mathbb{R}^2$.

Die Streckungsabbildung kann also durch Matrix-Vektor-Produkte mit der Matrix

$$\begin{bmatrix} \beta & 0 \\ 0 & \beta \end{bmatrix} \tag{17.8}$$

realisiert werden.



(*vi*) Im Vektorraum $(K^{\mathbb{N}})_{00}$ der endlich getragenen Folgen über einem Körper K mit der Standardbasis $(e_j)_{j\in\mathbb{N}}$, siehe Beispiel 13.2, legt

$$f(e_j) = e_{j+1} \quad \text{für } j \in \mathbb{N}$$

[27] Die Gleichheit in (17.7) folgt aus den Additionstheoremen (8.5).

eine lineare Abbildung (einen Endomorphismus) fest, eine sogenannte **Shift-Abbildung** (englisch: shift map). △

Ende der Vorlesung 23

Ende der Woche 11

§ 17.2 Die Matrix-Vektor-Multiplikation als lineare Abbildung

Die Matrix-Vektor-Multiplikation als Prototyp einer linearen Abbildung (Beispiele 17.5 und 17.11) ist von so zentraler Bedeutung, dass wir hier ihre Eigenschaften zusammenstellen. Kurz gesagt werden wir Folgendes sehen: Matrix-Vektor-Produkte sind die einzigen linearen Abbildungen $K^n \to K^m$, die es gibt; die Komposition linearer Abbildungen entspricht dem Produkt von Matrizen; und die inverse Abbildung entspricht der inversen Matrix.

Lemma 17.12 (Matrix-Vektor-Multiplikation als lineare Abbildung)**.**
Es sei K ein Körper und $n, m, k \in \mathbb{N}_0$.

(*i*) Ist $A \in K^{n\times m}$, dann ist

$$f_A \colon K^m \ni x \mapsto f_A(x) \coloneqq A\,x \in K^n \tag{17.9}$$

eine lineare Abbildung $K^m \to K^n$, genannt die **von A induzierte lineare Abbildung**.

(*ii*) Ist umgekehrt $f \colon K^m \to K^n$ eine lineare Abbildung, dann gibt es eine Matrix $A \in K^{n\times m}$, sodass $f = f_A$ gilt.

(*iii*) Sind $A \in K^{n\times m}$ und $B \in K^{m\times k}$, dann gilt

$$f_A \circ f_B = f_{A\,B}. \tag{17.10}$$

(„Die Komposition zweier linearer Abbildungen, die durch die Matrizen A und B induziert werden, entspricht derjenigen linearen Abbildung, die durch das Produkt der Matrizen A und B induziert wird.“)

(*iv*) $A \in K^{n\times n}$ ist genau dann invertierbar, wenn $f_A \colon K^n \to K^n$ invertierbar ist. In diesem Fall gilt

$$(f_A)^{-1} = f_{A^{-1}}. \tag{17.11}$$

(„Die Inverse einer linearen Abbildungen, die durch die Matrix A induziert ist, entspricht derjenigen linearen Abbildung, die durch die inverse Matrix A^{-1} induziert wird.“)

Beweis. Der Beweis ist Gegenstand der Übung. □

§ 17.3 Der Vektorraum der Vektorraumhomomorphismen

Definition 17.13 (Menge der Homomorphismen, Endomorphismen, Isomorphismen, Automorphismen von Vektorräumen)**.**
Es seien $(V,+,\cdot)$, $(W,+,\cdot)$ zwei Vektorräume über demselben Körper K.

(*i*) Wir führen folgende Bezeichnungen ein:

$$\begin{aligned}
\operatorname{Hom}(V,W) &:= \{f\colon V \to W \mid f \text{ ist Vektorraumhomomorphismus}\} && \text{(17.12a)}\\
\operatorname{End}(V) := \operatorname{Hom}(V,V) &= \{f\colon V \to V \mid f \text{ ist Vektorraumendomorphismus}\} && \text{(17.12b)}\\
\operatorname{Iso}(V,W) &:= \{f\colon V \to W \mid f \text{ ist Vektorraumisomorphismus}\} && \text{(17.12c)}\\
\operatorname{Aut}(V) := \operatorname{Iso}(V,V) &= \{f\colon V \to V \mid f \text{ ist Vektorraumautomorphismus}\}. && \text{(17.12d)}
\end{aligned}$$

(*ii*) Wollen wir den Skalarkörper betonen, so schreiben wir jeweils auch $\operatorname{Hom}_K(V,W)$, $\operatorname{End}_K(V)$, $\operatorname{Iso}_K(V,W)$ bzw. $\operatorname{Aut}_K(V)$. △

Satz 17.14 (die Homomorphismen zwischen Vektorräumen bilden einen Vektorraum)**.**
Es seien $(V,+,\cdot)$, $(W,+,\cdot)$ zwei Vektorräume über demselben Körper K. Die Menge $(\operatorname{Hom}(V,W),+,\cdot)$ mit der punktweisen Addition $+$ und der punktweisen S-Multiplikation $\cdot$

$$\begin{aligned}
+\colon \operatorname{Hom}(V,W)\times\operatorname{Hom}(V,W) &\to \operatorname{Hom}(V,W) && \text{mit } f+g \text{ def. durch } (f+g)(u) := f(u)+g(u)\\
\cdot\colon K\times\operatorname{Hom}(V,W) &\to \operatorname{Hom}(V,W) && \text{mit } \alpha\cdot f \text{ def. durch } (\alpha\cdot f)(u) := \alpha f(u)
\end{aligned}$$

bildet einen Vektorraum über K. Der Nullvektor in $(\operatorname{Hom}(V,W),+,\cdot)$ ist die **Nullabbildung** (englisch: zero map) $0\colon V \to W$, die jeden Vektor in V auf den Nullvektor $0 \in W$ abbildet.

Beweis. Wir prüfen die Bedingungen aus der Definition 11.1 nach. Wir wissen bereits, dass die Menge der Funktionen, die auf irgendeiner Menge definiert sind und die Werte in einer abelschen Gruppe haben, selbst eine abelsche Gruppe mit der punktweisen Gruppenoperation bildet (Beispiel 7.22). Insbesondere ist also $(\operatorname{Hom}(V,W),+)$ eine abelsche Gruppe, da $(W,+)$ eine abelsche Gruppe ist.

Weiter gelten die Distributivgesetze

$$\begin{aligned}
&\alpha\,(f+g) = \alpha f + \alpha g\\
\text{und}\quad &(\alpha+\beta)\,f = \alpha f + \beta f
\end{aligned}$$

für alle $\alpha,\beta \in K$ und $f,g \in \operatorname{Hom}(V,W)$, denn wir haben

$$\begin{aligned}
\big[\alpha\,(f+g)\big](u) &= \alpha\,\big[(f+g)(u)\big] = \alpha\,\big[f(u)+g(u)\big] = \alpha f(u) + \alpha g(u)\\
&= (\alpha f)(u) + (\alpha g)(u) = \big[\alpha f + \alpha g\big](u)\\
\text{und}\quad \big[(\alpha+\beta)\,f\big](u) &= (\alpha+\beta)\,f(u) = \alpha f(u) + \beta f(u)\\
&= \big[\alpha f + \beta f\big](u)
\end{aligned}$$

für alle $u \in V$.

Das Assoziativgesetz

$$(\alpha\,\beta)\,f = \alpha\,(\beta\,f)$$

gilt, denn wir haben

$$\big[(\alpha\,\beta)\,f\big](u) = (\alpha\,\beta)\,f(u) = \alpha\,(\beta\,f(u)) = \alpha\,([\beta\,f](u)) = [\alpha\,(\beta\,f)](u)$$

für alle $u \in V$.

Schließlich gilt $(1\,f)(u) = 1\,f(u) = f(u)$ für alle $u \in V$, d. h., $1 \in K$ ist auch neutrales Element der S-Multiplikation. □

Als Spezialfall von Satz 17.14 ergibt sich, dass insbesondere die Endomorphismen $(\mathrm{End}(V), +, \cdot)$ einen Vektorraum bilden. Betrachten wir an Stelle der S-Multiplikation als zweite Verknüpfung die Komposition $\circ$, so erhalten wir einen Ring wie schon beim Endomorphismenring einer abelschen Gruppe (vgl. Beispiel 9.2):

Satz 17.15 (die Endomorphismen eines Vektorraumes bilden einen Ring mit Eins, vgl. Beispiel 9.2)**.**

Es sei $(V, +, \cdot)$ ein Vektorraum. $(\mathrm{End}(V), +, \circ)$ mit der punktweisen Addition $+$ und der Komposition $\circ$

$$\begin{aligned} +\colon \mathrm{End}(V) \times \mathrm{End}(V) &\to \mathrm{End}(V) \quad \text{mit } f+g \text{ definiert durch} \quad (f+g)(u) \coloneqq f(u) + g(u), \\ \circ\colon \mathrm{End}(V) \times \mathrm{End}(V) &\to \mathrm{End}(V) \quad \text{mit } f\circ g \text{ definiert durch} \quad (f\circ g)(u) \coloneqq f(g(u)), \end{aligned}$$

bildet einen Ring mit dem Einselement id_V, genannt der **Endomorphismenring** (englisch: ring of endomorphisms) des Vektorraumes $(V, +, \cdot)$. Er ist i. A. nicht kommutativ.

Beweis. Der Beweis ist derselbe wie für den Endomorphismenring der abelschen Gruppe $(V, +)$ aus Beispiel 9.2, siehe Übung. Wir wissen bereits aus Satz 17.14 und Satz 17.3, dass Summen und Kompositionen von Vektorraumendomorphismen wieder Vektorraumendomorphismen sind. □

Definition 17.16 (allgemeine lineare Gruppe)**.**
Die Menge der bijektiven Endomorphismen $\mathrm{Aut}(V)$ eines K-Vektorraumes V, also die Einheitengruppe des Monoids $(\mathrm{End}(V), \circ)$, heißt die **Automorphismengruppe** (englisch: automorphism group) oder die **allgemeine lineare Gruppe** (englisch: general linear group) von V. Sie wird mit $\mathrm{GL}(V, K)$ bezeichnet. △

Der Name „allgemeine lineare Gruppe“ kann dadurch motiviert werden, dass $\mathrm{GL}(V, K)$ die größte Untergruppe des Monoids $(\mathrm{End}(V), \circ)$ ist, die das neutrale Element id_V enthält. $\mathrm{GL}(V, K)$ ist also das Maximum der Menge

$$\{U \subseteq \mathrm{End}(V) \mid (U, \circ) \text{ ist Gruppe mit } \mathrm{id}_V \in U\}$$

bzgl. der Inklusionshalbordnung (und auch bzgl. der Untergruppen-Halbordnung). Alle weiteren Untergruppen von $(\mathrm{End}(V), \circ)$, die id_V enthalten, sind also Teilmengen (und sogar Untergruppen) von $\mathrm{GL}(V, K)$, vgl. Bemerkung 7.46. In diesem Sinne könnten wir also auch die Einheitengruppe eines Monoids als die „allgemeine Gruppe“ des Monoids bezeichnen, vgl. Bemerkung 7.46. Das Attribut „linear“ bezieht sich darauf, dass die Elemente von $\mathrm{GL}(V, K)$ lineare Abbildungen sind.

§ 17.4 Faktorräume

In § 8.1 hatten wir gesehen, dass bestimmte Untergruppen namens Normalteiler N aus einer Gruppe G ausfaktorisiert werden können, sodass die Faktormenge $G/N = \{[a] = a \star N \mid a \in G\}$ bestehend aus den Nebenklassen[28] von N wieder eine Gruppenstruktur trägt, die mit der Struktur der Gruppe verträglich ist. Die letzte Aussage bedeutete, dass die kanonische Surjektion $\pi\colon a \mapsto [a]$, also der Übergang von einem Gruppenelement zu seiner Nebenklasse, ein (surjektiver) Gruppenhomomorphismus ist, sodass also $[a \star b] = [a] \mathbin{\tilde{\star}} [b]$ gilt: „Erst verknüpfen, dann zur Nebenklasse übergehen ergibt dasselbe wie erst zur Nebenklasse übergehen und dann verknüpfen."

Die Einführung der Faktorgruppe $(G/N, \tilde{\star})$ — einer gröberen Version der Gruppe G — war wichtig für das Verständnis der Wirkungsweise von Gruppenhomomorphismen (Homomorphiesatz für Gruppen 8.25). Dieser Satz besagte, dass ein Gruppenhomomorphismus $f\colon G_1 \to G_2$ „nebenklassenweise" in der Faktorgruppe $G_1/\operatorname{Kern}(f)$ wirkt, also eine ganze Nebenklasse $[a] = a \star \operatorname{Kern}(f)$ auf ein Element in $\operatorname{Bild}(f)$ abbildet, und zwar verschiedene Nebenklassen auf verschiedene Bildelemente. Kurz gesagt: $G_1/\operatorname{Kern}(f) \cong \operatorname{Bild}(f)$.

Die gleiche Konstruktion könnten wir in einem Vektorraum $(V, +, \cdot)$ einsetzen, da ja $(V, +)$ eine abelsche Gruppe ist und daher sogar jede Untergruppe einen Normalteiler bildet. Allerdings zielen wir darauf ab, dass die Faktormenge nicht nur eine Gruppenstruktur trägt, sondern wieder zu einem Vektorraum wird. Diese zusätzliche Kompatibilität der Nebenklassenbildung mit der S-Multiplikation erhalten wir genau dann, wenn wir an Stelle beliebiger Normalteiler von $(V, +)$ nur Unterräume von $(V, +, \cdot)$ verwenden.

Aus der Faktormenge wird damit der **Faktorraum** (englisch: factor space) oder **Quotientenraum** (englisch: quotient space) **von V nach U**. Wir sagen auch: „Aus dem Vektorraum $(V, +, \cdot)$ wird der Unterraum U ausfaktorisiert." Jede additive Nebenklasse[29] $[v] = v + U$ wird ein **affiner Unterraum parallel zu U** (englisch: affine subspace parallel to U) genannt. Zwei Vektoren $v_1, v_2 \in V$ gehören zur selben Nebenklasse genau dann, wenn $v_1 + U = v_2 + U$ gilt, also genau dann, wenn $v_1 - v_2 \in U$ gilt. Man ordnet einem affinen Unterraum $v + U$ die **Dimension** (englisch: dimension) $\dim(v + U) := \dim(U)$ zu.

Satz 17.17 (Faktorraum, vgl. Satz 9.30 über Faktorringe)**.**

(*i*) Es seien $(K, +, \cdot)$ ein Körper, $(V, +, \cdot)$ ein Vektorraum über K und U ein Unterraum von V.

Dann gilt:

(a) Auf der Faktormenge

$$V/U = \{[v] = v + U \mid v \in V\}$$

sind $\tilde{+}$ und $\tilde{\cdot}$, definiert als

$$[v] \mathbin{\tilde{+}} [w] := [v + w] \quad \text{für } v, w \in V, \tag{17.13a}$$

$$\alpha \mathbin{\tilde{\cdot}} [v] := [\alpha \cdot v] \quad \text{für } \alpha \in K \text{ und } v \in V, \tag{17.13b}$$

[28] **Nebenklasse** war nur ein anderer Name für eine Äquivalenzklasse der durch einen Normalteiler N induzierten Äquivalenzrelation $a \overset{N}{\sim} b \Leftrightarrow a \star N = b \star N \Leftrightarrow a' \star b \in N$, siehe § 7.5.

[29] Das Attribut „additiv" sagen wir gelegentlich dazu, obwohl wir in Vektorräumen i. A. keine anderen Nebenklassen definieren können.

eine innere bzw. äußere Verknüpfung, bzgl. denen $(V/U, \tilde{+}, \tilde{\cdot})$ einen Vektorraum über K bildet. Das neutrale Element bzgl. $\tilde{+}$ ist $[0] = U$, und für die Inversen gilt $\tilde{-}[v] = [-v]$.

(b) Die Abbildung

$$\pi\colon \begin{cases} V \to V/U \\ v \mapsto [v], \end{cases} \tag{17.14}$$

die jedem Vektor $v \in V$ seine Nebenklasse $[v] = v + U$ zuordnet, ist ein surjektiver Vektorraumhomomorphismus. Sie heißt die **kanonische Surjektion** (englisch: canonical surjection) von V auf V/U. Es gilt $\operatorname{Kern}(\pi) = U$.

(*ii*) Es seien $(K, +, \cdot)$ ein Körper, $(V, +, \cdot)$ ein Vektorraum über K und $(U, +)$ irgendeine Untergruppe von $(V, +)$. Sind die Verknüpfungen (17.13) auf der Menge der Nebenklassen V/U wohldefiniert, dann ist U notwendigerweise ein Unterraum von V.

Beweis. Aussage (*i*): Wir zeigen zunächst die Aussage (a) und weisen die Bedingungen aus der Definition 11.1 eines Vektorraumes nach.

Nach Satz 8.21 ist $(V/U, \tilde{+})$ eine abelsche Gruppe, da $(U, +)$ eine Untergruppe und damit ein Normalteiler der abelschen Gruppe $(V, +)$ ist.

Schritt 1: Nun müssen wir uns zunächst davon überzeugen, dass die S-Multiplikation $\tilde{\cdot}$ überhaupt wohldefiniert ist. Es sei dazu $\alpha \in K$ und $v_1, v_2 \in V$ mit $[v_1] = [v_2]$, also $v_1 + U = v_2 + U$. Im Fall $\alpha \neq 0$ gilt $\alpha U = U$. (**Quizfrage 17.7:** Warum?) Damit folgt

$$\begin{aligned}
\alpha \mathbin{\tilde{\cdot}} [v_1] &= [\alpha v_1] && \text{nach Definition von } \tilde{\cdot} \\
&= \alpha v_1 + U && \text{nach Definition von } [\cdot] \\
&= \alpha (v_1 + U) && \text{da } \alpha U = U \text{ ist} \\
&= \alpha (v_2 + U) && \text{da } [v_1] = [v_2] \text{ vorausgesetzt wurde} \\
&= \alpha v_2 + U && \text{da } \alpha U = U \text{ ist} \\
&= [\alpha v_2] && \text{nach Definition von } [\cdot] \\
&= \alpha \mathbin{\tilde{\cdot}} [v_2] && \text{nach Definition von } \tilde{\cdot}.
\end{aligned}$$

Im Fall $\alpha = 0$ gilt

$$\begin{aligned}
\alpha \mathbin{\tilde{\cdot}} [v_1] &= [0 v_1] && \text{nach Definition von } \tilde{\cdot} \\
&= [0 v_2] && \text{da } 0 v_1 = 0 = 0 v_2 \text{ gilt} \\
&= \alpha \mathbin{\tilde{\cdot}} [v_2] && \text{nach Definition von } \tilde{\cdot}.
\end{aligned}$$

Schritt 2: Nun weisen wir das Assoziativgesetz (11.1a) nach:

$$\begin{aligned}
(\alpha \beta) \mathbin{\tilde{\cdot}} [v] &= [(\alpha \beta) v] && \text{nach Definition von } \tilde{\cdot} \\
&= [\alpha (\beta v)] && \text{aufgrund des Assoziativgesetzes (11.1a) in } (V, +, \cdot) \\
&= \alpha \mathbin{\tilde{\cdot}} [\beta v] && \text{nach Definition von } \tilde{\cdot} \\
&= \alpha \mathbin{\tilde{\cdot}} (\beta \mathbin{\tilde{\cdot}} [v]) && \text{nach Definition von } \tilde{\cdot}.
\end{aligned}$$

Schritt 3: Es folgen die Distributivgesetze (11.1b) und (11.1c) in $(V/U, \tilde{+}, \tilde{\cdot})$:

$$\begin{aligned}
\alpha \mathbin{\tilde{\cdot}} ([v_1] \mathbin{\tilde{+}} [v_2]) &= \alpha \mathbin{\tilde{\cdot}} [v_1 + v_2] && \text{nach Definition von } \tilde{+} \\
&= [\alpha\,(v_1 + v_2)] && \text{nach Definition von } \tilde{\cdot} \\
&= [\alpha\, v_1 + \alpha\, v_2] && \text{aufgrund des Distributivgesetzes (11.1b) in } (V, +, \cdot) \\
&= [\alpha\, v_1] \mathbin{\tilde{+}} [\alpha\, v_2] && \text{nach Definition von } \tilde{+} \\
&= \alpha \mathbin{\tilde{\cdot}} [v_1] \mathbin{\tilde{+}} \alpha \mathbin{\tilde{\cdot}} [v_2] && \text{nach Definition von } \tilde{\cdot}
\end{aligned}$$

und

$$\begin{aligned}
(\alpha + \beta) \mathbin{\tilde{\cdot}} [v] &= [(\alpha + \beta)\, v] && \text{nach Definition von } \tilde{\cdot} \\
&= [\alpha\, v + \beta\, v] && \text{aufgrund des Distributivgesetzes (11.1c) in } (V, +, \cdot) \\
&= [\alpha\, v] \mathbin{\tilde{+}} [\beta\, v] && \text{nach Definition von } \tilde{+} \\
&= \alpha \mathbin{\tilde{\cdot}} [v] \mathbin{\tilde{+}} \beta \mathbin{\tilde{\cdot}} [v] && \text{nach Definition von } \tilde{\cdot}.
\end{aligned}$$

Schritt 4: Und schließlich zeigen wir, dass $1 \in K$ neutrales Element bzgl. $\tilde{\cdot}$ ist:

$$\begin{aligned}
1 \mathbin{\tilde{\cdot}} [v] &= [1\, v] && \text{nach Definition von } \tilde{\cdot} \\
&= [v] && \text{da 1 neutrales Element bzgl. } \cdot \text{ in } (V, +, \cdot) \text{ ist.}
\end{aligned}$$

Damit ist $(V/U, \tilde{+}, \tilde{\cdot})$ als Vektorraum bestätigt. Die Aussagen über das neutrale Element $[0] = U$ und über die Inversen $\tilde{-}[v] = [-v]$ folgen bereits aus dem Satz 8.21 über die Eigenschaften der abelschen Gruppe $(V/U, \tilde{+})$.

Aussage (b): Wir wissen bereits aus Satz 8.21, dass π ein surjektiver Gruppenhomomorphismus $(V, +) \to (V/U, \tilde{+})$ mit $\operatorname{Kern}(\pi) = U$ ist. Die Strukturverträglichkeit mit der Multiplikation ist gerade die Aussage (17.13b).

Aussage *(ii)*: Die Eigenschaft, ein Vektorraumhomomorphismus zu sein, bedeutet

$$\begin{aligned}
\pi(v + w) &= \pi(v) \mathbin{\tilde{+}} \pi(v) \\
\text{und} \quad \pi(\alpha\, v) &= \alpha \mathbin{\tilde{\cdot}} \pi(v)
\end{aligned}$$

für alle $v, w \in V$ und $\alpha \in K$. Nach Definition von π heißt das aber

$$\begin{aligned}
[v + w] &= [v] \mathbin{\tilde{+}} [v] \\
\text{und} \quad [\alpha\, v] &= \alpha \mathbin{\tilde{\cdot}} [v],
\end{aligned}$$

was gerade die Definition von $\tilde{+}$ und $\tilde{\cdot}$ war. Die Surjektivität von π ist klar, denn ein beliebiges Element $[v]$ von V/U ist gerade das Bild von v unter π. Es gilt $\operatorname{Kern}(\pi) = \pi^{-1}([0]) = U$.

Aussage *(ii)*: Wir bemerken zunächst, dass die Addition (17.13a) unter den Voraussetzungen wohldefiniert ist, da $(U, +)$ ein Normalteiler der kommutativen Gruppe $(V, +)$ ist (Satz 8.21). Aus dem Unterraumkriterium (Satz 11.11) bleibt noch $\alpha\, U \subseteq U$ für beliebiges $\alpha \in K$ zu zeigen. In der Tat gilt für $v \in U$ die Beziehung $[v] = [0] = U$, da die additiven Nebenklassen von U eine Partition von V bilden. Aufgrund der Wohldefiniertheit von (17.13b) gilt für $\alpha \in K$ weiter

$$[\alpha\, v] = [\alpha\, 0] = [0],$$

also $\alpha\, v \in [0] = U$, was zu zeigen war. □

Bemerkung 17.18 (Faktorraum, vgl. Bemerkung 9.31 zu Faktorringen)**.**

Praktisch können wir den Faktorraum $(V / U, \tilde{+}, \tilde{\cdot})$ benutzen, um wie im Vektorraum $(V, +, \cdot)$ zu „rechnen“, wobei jedoch Vektoren v, w in derselben Äquivalenzklasse (für die also $v - w \in U$ gilt) nicht mehr unterschieden werden. Der Faktorraum $(V / U, \tilde{+}, \tilde{\cdot})$ ist also eine „gröbere Version“ des Vektorraumes $(V, +, \cdot)$.

Die Dimension von V / U werden wir später noch charakterisieren, siehe Satz 18.6. △

Beispiel 17.19 (Faktorraum, vgl. Beispiel 9.32 zu Faktorringen)**.**

(*i*) Es sei V ein beliebiger Vektorraum und $U = \{0\}$ der Nullraum, einer der beiden trivialen Unterräume von V. Der zugehörige Faktorraum $V / \{0\}$ ist isomorph zum Ausgangsraum V selbst.

(*ii*) Es sei V ein beliebiger Vektorraum und $U = V$ der andere triviale Unterraum von V. Der zugehörige Faktorraum V / V ist isomorph zum Nullraum $\{0\}$.

(*iii*) Es sei $(K, +, \cdot)$ ein Körper und $(K^{\mathbb{N}}, +, \cdot)$ der Folgenraum über K. Wählen wir U als den Unterraum derjenigen Folgen $(x_n)_{n \in \mathbb{N}}$, deren Einträge an allen ungeraden Indizes $n \in \mathbb{N}$ gleich 0 sind, dann besteht der Faktorraum $K^{\mathbb{N}} / U$ aus Äquivalenzklassen von Folgen, wobei zwei Folgen genau dann in derselben Äquivalenzklasse (Nebenklasse) liegen, wenn sie in allen ungeraden Einträgen übereinstimmen. Die geraden Einträge der Folgen spielen keine Rolle mehr. Die ungerade Einträge bestimmen die Äquivalenzklasse. △

Bemerkung 17.20 (Unterräume sind genau die Kerne von Vektorraumhomomorphismen, vgl. Bemerkung 9.33 zu Kernen von Ringhomomorphismen)**.**

Es sei $(V, +, \cdot)$ über dem Körper K.

(*i*) Nach Lemma 17.8 ist der Unterraum $\operatorname{Kern}(f)$ für jeden beliebigen Vektorraumhomomorphismus $f : V \to W$ in irgendeinen Vektorraum $(W, +, \cdot)$ über demselben Körper K immer ein Unterraum von $(V, +, \cdot)$.

(*ii*) Umgekehrt gilt auch, dass jeder Unterraum U von $(V, +, \cdot)$ der Kern eines Vektorraumhomomorphismus ist. Dazu wählen wir einfach $W := (V / U, \tilde{+}, \tilde{\cdot})$ als Zielraum und die kanonische Surjektion $\pi : V \to V / U$ als Vektorraumhomomorphismus. Dann gilt $\operatorname{Kern}(\pi) = U$. △

§ 17.5 Der Homomorphiesatz für Vektorräume

Mit Hilfe des Wissens über Faktorräume können wir nun die Struktur von Vektorraumhomomorphismen genauer analysieren. Der folgende Struktursatz besagt, dass ein Vektorraumhomomorphismus $f : V \to W$ „nebenklassenweise“ wirkt. Er bildet also eine gesamte additive Nebenklasse von $\operatorname{Kern}(f)$ — das ist ein affiner Unterraum parallel zu $\operatorname{Kern}(f)$ — auf ein- und dasselbe Element von W ab und verschiedene Nebenklassen auf verschiedene Elemente. Dadurch ist das $\operatorname{Bild}(f)$ eines solchen Vektorraumhomomorphismus bereits im Wesentlichen (d. h. bis auf Isomorphie) festgelegt durch V und den Unterraum $\operatorname{Kern}(f)$.

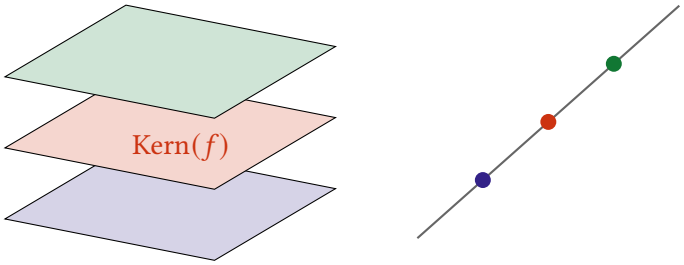


Abbildung 17.1.: Illustration des Homomorphiesatzes für Vektorraumhomomorphismen 17.21, vgl. Abbildung 8.2. Alle Elemente einer Nebenklasse des Unterraumes $\operatorname{Kern}(f)$ werden auf ein- und dasselbe Element von W abgebildet und verschiedene Nebenklassen auf verschiedene Elemente.

Satz 17.21 (**Homomorphiesatz für Vektorräume**[30], vgl. Homomorphiesatz für Ringe 9.38)**.**
Es seien V, W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ ein Homomorphismus. Dann gilt

$$V / \operatorname{Kern}(f) \cong \operatorname{Bild}(f) \tag{17.15a}$$

mit dem Isomorphismus

$$I([v]) \coloneqq f(v) \quad \text{für } [v] = v + \operatorname{Kern}(f) \in V / \operatorname{Kern}(f). \tag{17.15b}$$

Beweis. Der Vektorraumhomomorphismus ist insbesondere ein Gruppenhomomorphismus $f\colon (V,+) \to (W,+)$, und $\operatorname{Kern}(f) = \{u \in V \mid f(u) = 0\}$ hängt nicht davon ab, ob wir f als Homomorphismus von Gruppen oder von Vektorräumen betrachten. Aus dem Homomorphiesatz für Gruppen 8.25 folgt also sofort, dass $V / \operatorname{Kern}(f)$ und $\operatorname{Bild}(f)$ im Sinne von Gruppen isomorph sind, und zwar vermöge des Isomorphismus (17.15b).

Es bleibt nur zu zeigen, dass I tatsächlich auch ein Isomorphismus im Sinne von Vektorräumen ist. Dazu fehlt nur der Nachweis der Homogenität (17.1b), der aber einfach zu erbringen ist:

$$\begin{aligned} I(\alpha \cdot [v]) &= I([\alpha v]) && \text{nach Definition von } \cdot \\ &= f(\alpha v) && \text{nach Definition von } I \\ &= \alpha f(v) && \text{aufgrund der Homogenität von } f \\ &= \alpha I([v]) && \text{nach Definition von } I. \end{aligned}$$

□

Beispiel 17.22 (Homomorphiesatz für Vektorräume, vgl. Beispiel 8.27)**.**

(*i*) Es seien V, W Vektorräume über demselben Körper K. Wir betrachten den Nullhomomorphismus $f\colon V \to W$ mit $f(v) = 0$ für alle $v \in V$. Gemäß Homomorphiesatz für Vektorräume 17.21 ist

$$V / \operatorname{Kern}(f) = V / V \cong \{0\}.$$

[30] englisch: fundamental theorem on vector space homomorphisms

(*ii*) Es sei K^n der Standardvektorraum der Dimension $n \in \mathbb{N}$ über einem Körper K. Wir betrachten die Projektion auf die i-te Koordinate (Beispiel 17.5)

$$\pi_i \colon K^n \ni x \mapsto x_i \in K$$

für $1 \leqslant i \leqslant n \in \mathbb{N}$. Dann ist $\operatorname{Kern}(\pi_i) = \{x \in K^n \mid x_i = 0\}$, also besteht $K^n / \operatorname{Kern}(\pi_i)$ aus Äquivalenzklassen von Vektoren, die jeweils in der i-ten Koordinate übereinstimmen. Eine gesamte Äquivalenzklasse wird durch π_i auf ein- und dasselbe Element von K abgebildet.

Gemäß Homomorphiesatz für Vektorräume 17.21 gilt

$$K^n / \operatorname{Kern}(\pi_i) = K^n / \{x \in K^n \mid x_i = 0\} \;\cong\; \operatorname{Bild}(\pi_i) = K.$$

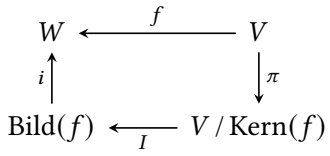
(*iii*) Es sei $K^{\mathbb{N}}$ der Folgenraum über einem Körper K. Wir betrachten auch hier die Projektion auf die i-Koordinate

$$\pi_i \colon K^{\mathbb{N}} \ni x \mapsto x_i \in K$$

für $i \in \mathbb{N}$, die eine Folge auf das i-te Folgenglied abbildet. Dann ist $\operatorname{Kern}(\pi_i) = \{(x_n)_{n\in\mathbb{N}} \mid x_i = 0\}$, also besteht $K^{\mathbb{N}} / \operatorname{Kern}(\pi_i)$ aus Äquivalenzklassen von Folgen, die jeweils im i-ten Folgenglied übereinstimmen. Eine gesamte Äquivalenzklasse wird auf ein- und dasselbe Element von K abgebildet. Gemäß Homomorphiesatz für Vektorräume 17.21 ist

$$K^{\mathbb{N}} / \operatorname{Kern}(\pi_i) = K^{\mathbb{N}} / \{x \in K^{\mathbb{N}} \mid x_i = 0\} \;\cong\; \operatorname{Bild}(\pi_i) = K. \qquad \triangle$$

Abschließend stellen wir den Homomorphiesatz für Vektorräume 17.21 nochmal schematisch mit Hilfe eines kommutativen Diagrammes dar. Dazu sei $i \colon \operatorname{Bild}(f) \ni w \mapsto w \in W$ der injektive Homomorphismus der kanonischen Einbettung.



$$f = \underbrace{i}_{\text{einbetten}} \circ \overbrace{I}^{\text{isomorph abbilden}} \circ \underbrace{\pi}_{\text{vergröbern}}.$$

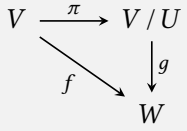
Expertenwissen: universelle Eigenschaft von Faktorräumen

Ähnlich wie Faktorgruppen (siehe Material im Anschluss an Satz 8.25) können auch Faktorräume durch eine universelle Eigenschaft charakterisiert werden:

Es seien V, W Vektorräume über demselben Körper K und $f \colon V \to W$ ein Homomorphismus. Weiter sei U ein Unterraum von V. Dann sind äquivalent:

(*i*) $U \subseteq \operatorname{Kern}(f)$, also $f(U) = \{0\}$.

(*ii*) Der Homomorphismus f **faktorisiert durch** die kanonische Surjektion $\pi \colon V \to V / U$, d. h., es gibt einen eindeutig bestimmten Homomorphismus $g \colon V / U \to W$ mit $f = g \circ \pi$.



Diese Eigenschaft nennt sich die **universelle Eigenschaft von Faktorräumen** (englisch: universal property of quotient spaces), denn sie charakterisiert Faktorräume bis auf Isomorphie eindeutig. Gilt also die obige Äquivalenzaussage mit irgendeinem K-Vektorraum Z an Stelle von V/U und einem surjektiven Vektorraumhomomorphismus $\pi\colon V \to Z$, dann ist Z isomorph zu V/U. Die universelle Eigenschaft ermöglicht es, Faktorräume (bis auf Isomorphie) zu definieren, ohne die konkrete Konstruktion über Nebenklassen zu verwenden.

Ende der Vorlesung 24

§ 18 Dimensionssätze

Literatur: Fischer, Springborn, 2020, Kapitel 3.2; Bosch, 2014, Kapitel 2; Beutelspacher, 2014, Kapitel 5.2

Wir wollen in diesem Abschnitt den Zusammenhang der Dimensionen der am Homomorphiesatz für Vektorräume 17.21 beteiligten Räume V, $\operatorname{Kern}(f)$ und $\operatorname{Bild}(f)$ untersuchen. Wir hatten am Beispiel 17.22 schon sehen können: Je höher die Dimension des ausfaktorisierten Unterraumes, desto geringer die verbleibende Dimension des Faktorraumes.

§ 18.1 Zusammenhang von Dimension und Isomorphie

Als Folgerungen aus dem Existenz- und Eindeutigkeitssatz für Vektorraumhomomorphismen 17.10 erhalten wir folgende bemerkenswerte Resultate:

Satz 18.1 (Vektorräume gleicher endlicher Dimension sind isomorph)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K. Dann sind äquivalent:

(*i*) V und W sind isomorphe Vektorräume.

(*ii*) $\dim(V) = \dim(W)$.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $f\colon V \to W$ ein Isomorphismus. Nach Folgerung 13.6 existiert eine Basis $(v_1, \dots, v_n)$ von V für ein $n \in \mathbb{N}_0$. Setze $w_i := f(v_i)$ für $i \in [\![1, n]\!]$. Dann ist nach Satz 17.10 $(w_1, \dots, w_n)$ eine Basis von W. Beide Basen sind gleichmächtig, also gilt $\dim(V) = \dim(W)$.

Aussage $(ii) \Rightarrow$ Aussage (i): Es gelte $\dim(V) = \dim(W) = n \in \mathbb{N}_0$. Es seien $(v_1, \ldots, v_n)$ eine beliebige Basis von V und $(w_1, \ldots, w_n)$ eine beliebige Basis von W. Nach Satz 17.10 gibt es genau eine lineare Abbildung $f\colon V \to W$ mit der Eigenschaft $f(v_i) = w_i$ für alle $i = 1, \ldots, n$. Nach Satz 17.10 ist dieses f bijektiv, also sind V und W zueinander isomorph. □

Satz 18.1 besagt, dass es bis auf Isomorphie nur einen einzigen K-Vektorraum der Dimension $n \in \mathbb{N}_0$ gibt! Anders gesagt: Alle K-Vektorräume V mit $\dim(V) = n \in \mathbb{N}_0$ sind zueinander isomorph. Die Dimension beschreibt also einen endlich-dimensionalen K-Vektorraum bereits vollständig. Das werden wir später in § 19 noch ausnutzen.

Es gilt sogar folgende Verallgemeinerung von Satz 18.1:

Satz 18.2 (Vektorräume mit gleichmächtigen Basen sind isomorph[AoC])**.**

Es seien V, W Vektorräume über demselben Körper K. Dann sind äquivalent:

(*i*) V und W sind isomorphe Vektorräume.

(*ii*) Es gibt eine Basis $(v_i)_{i \in I}$ von V und eine Basis $(w_j)_{j \in J}$ von W, die gleichmächtig sind.

Es gibt also nicht nur zu jeder endlichen Zahl, sondern sogar zu jeder Kardinalzahl eine Äquivalenzklasse isomorpher Vektorräume.[AoC] Wir können die Vektorräume K^n als natürliche Repräsentanten der Äquivalenzklasse der Vektorräume mit einer Basis der endlichen Mächtigkeit $n \in \mathbb{N}_0$ ansehen. Weiter ist der Folgenraum $K^{\mathbb{N}}$ der natürliche Repräsentant der Vektorräume mit abzählbar unendlicher Basis.

§ 18.2 Dimension von Faktorräumen

In diesem Abschnitt bestimmen wir die Dimension eines Faktorraumes V / U. Zur Vorbereitung benötigen wir folgendes Resultat.

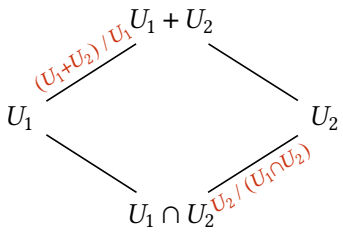
Satz 18.3 (Faktorraum einer Summe von Unterräumen)**.**

Es seien V ein Vektorraum und U_1, U_2 zwei Unterräume von V. Dann gilt:

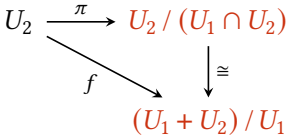
$$(U_1 + U_2) / U_1 \;\cong\; U_2 / (U_1 \cap U_2). \tag{18.1}$$

Beachte: Beide Seiten der Gleichung messen auf unterschiedliche Weise, „wieviel vom Unterraum U_2 nicht bereits im Unterraum U_1 liegt“, und kommen dabei zum selben Ergebnis (bis auf Isomorphie). Grafisch wird das Ergebnis manchmal durch das folgende Diagramm dargestellt, weshalb Satz 18.3 im Englischen auch als diamond theorem bezeichnet wird:[31]

[31] Ein anderer Name für Satz 18.3 ist **zweiter Isomorphiesatz** (englisch: second isomorphism theorem). Der **erste Isomorphiesatz** (englisch: first isomorphism theorem) ist der Homomorphiesatz für Vektorräume 17.21.



Beweis. Der Beweis basiert auf der Idee, einen surjektiven Homomorphismus $f\colon U_2 \to (U_1 + U_2)/U_1$ anzugeben mit $\operatorname{Kern}(f) = U_1 \cap U_2$. Aus dem Homomorphiesatz für Vektorräume 17.21 folgt dann $U_2/\operatorname{Kern}(f) = U_2/(U_1 \cap U_2) \cong \operatorname{Bild}(f) = (U_1 + U_2)/U_1$, also die Behauptung (18.1).



Wir definieren $f(u_2) \coloneqq [u_2] = u_2 + U_1$ für $u_2 \in U_2$. (Im gesamten Beweis bedeutet $[\cdot]$ immer eine Nebenklasse von U_1.)

Schritt 1: $f\colon U_2 \to (U_1 + U_2)/U_1$ ist ein Homomorphismus:

Zunächst stellen wir fest, dass $f(u_2) = u_2 + U_1$ in U_2/U_1 liegt, also erst recht in $(U_1 + U_2)/U_1$. Wir weisen die Linearität nach:

$$\begin{aligned} f(u_2 + v_2) &= [u_2 + v_2] && \text{nach Definition von } f \\ &= [u_2] \mathbin{\tilde{+}} [v_2] && \text{mit } \tilde{+} \text{ in } (U_1 + U_2)/U_1 \\ &= f(u_2) \mathbin{\tilde{+}} f(v_2) && \text{nach Definition von } f \end{aligned}$$

und

$$\begin{aligned} f(\alpha\, u_2) &= [\alpha\, u_2] && \text{nach Definition von } f \\ &= \alpha \mathbin{\tilde{\cdot}} [u_2] && \text{mit } \tilde{\cdot} \text{ in } (U_1 + U_2)/U_1 \\ &= \alpha \mathbin{\tilde{\cdot}} f(u_2) && \text{nach Definition von } f. \end{aligned}$$

Schritt 2: $\operatorname{Kern}(f) = U_1 \cap U_2$:

Es ist

$$\begin{aligned} \operatorname{Kern}(f) &= \{u_2 \in U_2 \mid f(u_2) = [0]\} && \text{nach Definition des Kerns und des} \\ &&& \text{neutralen Elements } [0] \text{ in } (U_1 + U_2)/U_1 \\ &= \{u_2 \in U_2 \mid [u_2] = [0]\} && \text{nach Definition von } f \\ &= \{u_2 \in U_2 \mid u_2 - 0 \in U_1\} && \text{nach Definition von } [\cdot] \\ &= U_1 \cap U_2. \end{aligned}$$

Schritt 3: f ist surjektiv, d. h., $\mathrm{Bild}(f) = (U_1 + U_2) / U_1$.

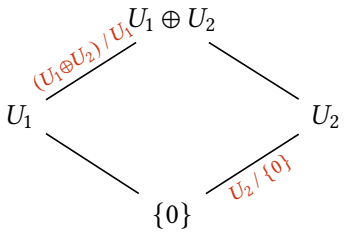
Es sei $[w] \in (U_1 + U_2) / U_1$. Wegen $w \in U_1 + U_2$ existieren $u_1 \in U_1$ und $u_2 \in U_2$ mit $w = u_1 + u_2$. Das heißt aber $[w] = u_1 + u_2 + U_1 = u_2 + U_1 = [u_2] = f(u_2)$. □

Für den Fall $U_1 \cap U_2 = \{0\}$ erhalten wir folgendes Korollar:

Folgerung 18.4 (Faktorraum einer direkten Summe von Unterräumen)**.**
Es seien V ein Vektorraum und U_1, U_2 zwei Unterräume von V. Wenn $U_1 \cap U_2 = \{0\}$ gilt, dann ist

$$(U_1 \oplus U_2) / U_1 \cong U_2. \tag{18.2}$$

Beachte: Folgerung 18.4 besagt insbesondere, dass jeder zu einem Unterraum U_1 eines Vektorraumes V komplementäre Unterraum U_2 isomorph zum Faktorraum V / U_1 ist. Analog zu oben können wir das Resultat von Folgerung 18.4 wie folgt illustrieren:



Beweis. Nach Satz 18.3 gilt

$$(U_1 + U_2) / U_1 \cong U_2 / (U_1 \cap U_2).$$

Die Voraussetzung $U_1 \cap U_2 = \{0\}$ bedeutet, dass die Summe $U_1 \oplus U_2$ direkt ist, also folgt

$$(U_1 \oplus U_2) / U_1 \cong U_2 / \{0\} = \big\{ [u_2] = u_2 + \{0\} \,\big|\, u_2 \in U_2 \big\} \cong U_2,$$

vgl. auch Beispiel 17.19. □

Beispiel 18.5 (Faktorraum einer Summe von Unterräumen)**.**
Wir betrachten ein Beispiel im Folgenraum $V = K^{\mathbb{N}}$ mit den Unterräumen

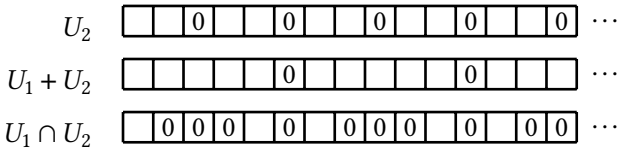
$$U_1 = \big\{ (x_n)_{n\in\mathbb{N}} \,\big|\, x_{2k} = 0 \text{ für alle } k \in \mathbb{N} \big\} \qquad \text{jedes zweite Folgenglied ist Null,}$$
$$U_2 = \big\{ (x_n)_{n\in\mathbb{N}} \,\big|\, x_{3k} = 0 \text{ für alle } k \in \mathbb{N} \big\} \qquad \text{jedes dritte Folgenglied ist Null.}$$

Dann gilt

$$U_1 + U_2 = \big\{ (x_n)_{n\in\mathbb{N}} \,\big|\, x_{6k} = 0 \text{ für alle } k \in \mathbb{N} \big\} \qquad \text{jedes sechste Folgenglied ist Null,}$$
$$U_1 \cap U_2 = \big\{ (x_n)_{n\in\mathbb{N}} \,\big|\, x_{2k} = x_{3k} = 0 \text{ für alle } k \in \mathbb{N} \big\} \qquad \text{jedes zweite und dritte Folgenglied ist Null.}$$

Wir illustrieren die Struktur der Folgen in diesen vier Unterräumen wie folgt:

U_1 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | ⋯



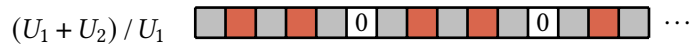
Wir betrachten nun die Faktorräume $(U_1 + U_2) / U_1$ und $U_2 / (U_1 \cap U_2)$:

- Jedes Element von $(U_1 + U_2) / U_1$ ist eine Äquivalenzklasse von Folgen. Zwei Folgen in $U_1 + U_2$ sind äquivalent, wenn ihre Differenz in U_1 liegt. Die Äquivalenzklasse einer Folge $(y_n)_{n\in\mathbb{N}} \in U_1 + U_2$ hat also die Gestalt

$$[(y_n)_{n\in\mathbb{N}}] = \left\{(x_n)_{n\in\mathbb{N}} \,\middle|\, x_{6k} = 0 \text{ und } x_{2k} = y_{2k} \text{ für alle } k \in \mathbb{N}\right\}.$$

  Eine solche Äquivalenzklasse ist also bereits durch die Werte y_{6k+2} und y_{6k+4} für alle $k \in \mathbb{N}_0$ eines Repräsentanten eindeutig bestimmt.

  Wir illustrieren die Struktur der Äquivalenzklassen in $(U_1 + U_2) / U_1$ wie folgt:



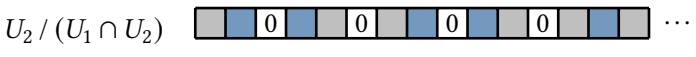
  Die mit ■ gekennzeichneten Einträge sind dabei für alle Elemente einer Äquivalenzklasse identisch. Diese Einträge legen die Äquivalenzklasse fest, bestimmen also das Element von $(U_1 + U_2) / U_1$. Verschiedene Repräsentanten einer Äquivalenzklasse unterscheiden sich nur in den mit ■ markierten Einträgen.

- Jedes Element von $U_2 / (U_1 \cap U_2)$ ist ebenfalls eine Äquivalenzklasse von Folgen. Zwei Folgen in U_2 sind äquivalent, wenn ihre Differenz in $U_1 \cap U_2$ liegt. Die Äquivalenzklasse einer Folge $(z_n)_{n\in\mathbb{N}} \in U_2$ hat also die Gestalt

$$[(z_n)_{n\in\mathbb{N}}] = \left\{(x_n)_{n\in\mathbb{N}} \,\middle|\, x_{3k} = 0 \text{ und } x_{2k} = z_{2k} \text{ und } x_{3k} = z_{3k} \text{ für alle } k \in \mathbb{N}\right\}.$$

  Eine solche Äquivalenzklasse ist also bereits durch die Werte z_{6k+2} und z_{6k+4} für alle $k \in \mathbb{N}_0$ eines Repräsentanten eindeutig bestimmt.

  Wir illustrieren die Struktur der Äquivalenzklassen in $U_2 / (U_1 \cap U_2)$ wie folgt:



  Die mit ■ gekennzeichneten Einträge sind dabei für alle Elemente einer Äquivalenzklasse identisch. Diese Einträge legen die Äquivalenzklasse fest, bestimmen also das Element von $U_2 / (U_1 \cap U_2)$. Verschiedene Repräsentanten einer Äquivalenzklasse unterscheiden sich nur in den mit ■ markierten Einträgen.

Offenbar ist die für $k \in \mathbb{N}_0$ durch

$$\begin{aligned} z_{6k+1} &:= 0 & z_{6k+3} &:= 0 & z_{6k+5} &:= 0 \\ z_{6k+2} &:= y_{6k+2} & z_{6k+4} &:= y_{6k+4} & z_{6k+6} &:= 0 \end{aligned}$$

definierte Zuordnung $[(y_n)_{n\in\mathbb{N}}] \mapsto [(z_n)_{n\in\mathbb{N}}]$ ein möglicher Isomorphismus zwischen den Faktorräumen $(U_1 + U_2) / U_1$ und $U_2 / (U_1 \cap U_2)$. △

Nun können wir die Dimension von Faktorräumen bestimmen:

Satz 18.6 (Dimension des Faktorraumes[32 AoC])**.**
Es seien V ein Vektorraum und U ein Unterraum von V. Dann gilt

(*i*) Ist W ein zu U komplementärer Unterraum von V, dann gilt

$$V / U \cong W \tag{18.3a}$$
$$\dim(V / U) = \operatorname{codim}(U) \tag{18.3b}$$
$$\dim(V) = \dim(V / U) + \dim(U). \tag{18.3c}$$

(*ii*) Ist V endlich-dimensional, dann gilt insbesondere

$$\dim(V / U) = \dim(V) - \dim(U). \tag{18.4}$$

Beweis. Aussage (*i*): Es sei W ein zu U komplementärer Unterraum von V. Dann gilt $V = U \oplus W$, und aus Folgerung 18.4 folgt

$$V / U = (U \oplus W) / U \cong W.$$

Aus Satz 18.2 folgt $\dim(V / U) = \dim(W) = \operatorname{codim}(U)$. Nach Folgerung 14.10 erhalten wir schließlich $\dim(V) = \dim(U) + \dim(W) = \dim(U) + \dim(V / U)$.

Aussage (*ii*): Ist V endlich-dimensional, dann gilt nach Folgerung 14.11 $\operatorname{codim}(U) = \dim(V) - \dim(U)$. □

§ 18.3 Dimensionen im Homomorphiesatz

Mit Hilfe von Satz 18.6 können wir nun die Dimensionen der Räume V, $\operatorname{Kern}(f)$ und $\operatorname{Bild}(f)$ im Homomorphiesatz für Vektorräume 17.21, also in der Aussage

$$V / \operatorname{Kern}(f) \cong \operatorname{Bild}(f),$$

untersuchen:

Satz 18.7 (Dimensionen der Räume im Homomorphiesatz für Vektorräume 17.21[33 AoC])**.**
Es seien V und W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ ein Homomorphismus. Dann gilt

$$\dim(\operatorname{Kern}(f)) + \dim(\operatorname{Bild}(f)) = \dim(V). \tag{18.5}$$

[32] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

[33] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

Beweis. Mit $U := \operatorname{Kern}(f)$ folgt

$$\dim(V) = \dim(\operatorname{Kern}(f)) + \dim(V / \operatorname{Kern} f)$$

aus (18.3). Da nach dem Homomorphiesatz für Vektorräume 17.21 $\operatorname{Bild}(f)$ und $V / \operatorname{Kern} f$ isomorph sind und nach Satz 18.2 isomorphe Vektorräume dieselbe Dimension besitzen, ist (18.5) gezeigt. □

Definition 18.8 (Rang und Defekt eines Homomorphismus)**.**
Es seien V und W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ ein Homomorphismus. Dann heißt

$$\operatorname{Rang}(f) := \dim(\operatorname{Bild}(f)) \tag{18.6}$$

der **Rang** (englisch: rank) der linearen Abbildung f, und

$$\operatorname{Defekt}(f) := \dim(\operatorname{Kern}(f)) \tag{18.7}$$

heißt der **Defekt** (englisch: defect) von f. △

Wir können also die Dimensionsformel (18.5) auch in der Form

$$\operatorname{Defekt}(f) + \operatorname{Rang}(f) = \dim(V) \tag{18.8}$$

schreiben.

Das folgende Resultat erleichtert der Nachweis der Bijektivität (also der Isomorphismus-Eigenschaft) einer linearen Abbildung erheblich.

Folgerung 18.9 (Charakterisierung der Bijektivität von Homomorphismen endlich-dimensionaler Vektorräume)**.**
Es seien V und W Vektorräume über demselben Körper K. Weiter sei $f\colon V \to W$ ein Homomorphismus.

(*i*) Haben V und W dieselbe endliche Dimension $\dim(V) = \dim(W)$, dann sind äquivalent:
  (a) f ist injektiv.
  (b) $\operatorname{Defekt}(f) = 0$.
  (c) f ist surjektiv.
  (d) $\operatorname{Rang}(f) = \dim(V)$.
  (e) f ist bijektiv.

(*ii*) Ist V endlich-dimensional und gilt $\dim(V) < \dim(W) \in \mathbb{N} \cup \{\infty\}$, dann kann f nicht surjektiv sein.

(*iii*) Ist W endlich-dimensional und gilt $\dim(W) < \dim(V) \in \mathbb{N} \cup \{\infty\}$, dann kann f nicht injektiv sein.

(*iv*) Es seien V oder W endlich-dimensional. Ein Isomorphismus $V \to W$ existiert genau dann, wenn der andere Vektorraum auch endlich-dimensional ist und $\dim(V) = \dim(W)$ gilt.

Beweis. Der Beweis ist Gegenstand der Übung. □

Beispiel 18.10 (Charakterisierung der Bijektivität von Homomorphismen endlich-dimensionaler Vektorräume)**.**

In diesem Beispiel illustrieren wir verschiedene Fälle aus Folgerung 18.9.

(*i*) Ein injektiver Homomorphismus $f\colon \mathbb{R} \to \mathbb{R}^2$, der nicht surjektiv ist:

$$f(x) \coloneqq \begin{bmatrix} 1 \\ 0 \end{bmatrix} x.$$

(*ii*) Ein surjektiver Homomorphismus $f\colon \mathbb{R}^2 \to \mathbb{R}$, der nicht injektiv ist:

$$f(x) \coloneqq \begin{bmatrix} 1 & 0 \end{bmatrix} x.$$

(*iii*) Sind V und W beide unendlich-dimensional, so können alle Kombinationen von Injektivität und Surjektivität auftreten. Wir betrachten dazu Endomorphismen des Vektorraumes $(K^{\mathbb{N}})_{00}$ der endlich getragenen Folgen über einem Körper K. Zur Definition dieser Endomorphismen geben wir (siehe Satz 17.10) jeweils die Bilder der Standardfolgen e_j an (Beispiel 11.17).

- Die Shift-Abbildung nach links, gegeben durch $f(e_j) = e_{j-1}$ für $j \geqslant 2$ und $f(e_1) = 0$ (Nullfolge), ist surjektiv, aber nicht injektiv.
- Die Shift-Abbildung nach rechts, gegeben durch $f(e_j) = e_{j+1}$ für $j \in \mathbb{N}$, ist injektiv, aber nicht surjektiv.
- Die identische Abbildung, gegeben durch $f(e_j) = e_j$ für $j \in \mathbb{N}$, ist bijektiv.
- Die Nullabbildung, gegeben durch $f(e_j) = 0$ für $j \in \mathbb{N}$, ist weder injektiv noch surjektiv. △

Ende der Vorlesung 25

Ende der Woche 12

§ 19 Darstellungsmatrizen von Homomorphismen

Literatur: Fischer, Springborn, 2020, Kapitel 3.4–3.6 und 5.1, 5.3; Bosch, 2014, Kapitel 3.4 und 6.1; Beutelspacher, 2014, Kapitel 5.2 und 8.1–8.2; Jänich, 2008, Kapitel 9.1 und 11.1–11.2

Im gesamten § 19 sind alle Vektorräume endlich-dimensional. Wir erinnern an Satz 18.1, der besagt, dass alle K-Vektorräume der gemeinsamen Dimension $n \in \mathbb{N}_0$ zueinander isomorph sind. Es ist daher möglich und praktisch, für jeden n-dimensionalen K-Vektorraum V eine Art gemeinsame Standarddarstellung zu finden. Dafür bietet sich der Standardvektorraum K^n an.

§ 19.1 Koordinatendarstellung in endlich-dimensionalen Vektorräumen

Es sei V ein Vektorraum über dem Körper K mit $\dim(V) = n \in \mathbb{N}_0$. Der folgende Satz gibt an, wie wir mit Hilfe einer Basis von V jeden beliebigen Vektor in V mit Hilfe seines Koordinatenvektors in K^n bzgl. dieser Basis darstellen können.

Satz 19.1 (Koordinatenvektor, Syntheseabbildung, Analyseabbildung)**.**
Es sei V ein Vektorraum über dem Körper K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter sei die Familie $B = (v_1, \dots, v_n)$ eine Basis von V.

(*i*) Die Abbildung

$$\Phi_B \colon K^n \ni \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i v_i \in V \tag{19.1}$$

ist ein linearer Isomorphismus $K^n \to V$. Diese erzeugt aus einem **Koordinatenvektor**[34] (englisch: coordinate vector) $x \in K^n$ die zugehörige Linearkombination der Basisvektoren v_i. Wir bezeichnen die Abbildung Φ_B daher auch als die **Syntheseabbildung** (englisch: synthesis map) bzgl. der Basis B.

(*ii*) Der zu Φ_B inverse Isomorphismus ist die Abbildung

$$\Phi_B^{-1} \colon V \ni v \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n, \tag{19.2}$$

die jedem Vektor $v \in V$ seinen eindeutigen **Koordinatenvektor** $x \in K^n$ bzgl. der Basis B zuordnet. Wir nennen daher Φ_B^{-1} auch die **Koordinatenabbildung** (englisch: coordinate map) oder die **Analyseabbildung** (englisch: analysis map) bzgl. der Basis B. Der Eintrag $x_i \in K$ heißt die i-te **Koordinate** (englisch: coordinate) des Vektors $v \in V$ bzgl. der Basis B.

Beweis. Φ_B ist linear und bildet die Basis $(e_1, \dots, e_n)$ in K^n auf die Basis $(v_1, \dots, v_n)$ ab. Damit ist Φ_B nach Satz 17.10 bijektiv, also ein linearer Isomorphismus, und die Inverse Φ_B^{-1} ebenfalls (Satz 17.3). □

Wir werden Koordinatenvektoren typischerweise mit x bezeichnen.

Beispiel 19.2 (Koordinatendarstellung)**.**

(*i*) Im Vektorraum $\mathbb{R}^{(-\frac{\pi}{2}, \frac{\pi}{2})}$ der Funktionen $(-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ hat der Vektor

$$5 \sin - 3 \cos + 7 \tan$$

bzgl. der Basis $B = (\sin, \cos, \tan)$ den Koeffizientenvektor $\begin{pmatrix} 5 \\ -3 \\ 7 \end{pmatrix}$, denn es gilt

$$5 \sin - 3 \cos + 7 \tan = 5 \sin + (-3) \cos + 7 \tan.$$

[34] Hier zeigt sich der Grund, warum wir den Standardvektorraum K^n, der in Beispiel 11.3 eingeführt wurde, auch als **Koordinatenraum** bezeichnen. Statt **Koordinaten** kann man auch von den **Komponenten** (englisch: components) bzgl. der Basis B sprechen.

(*ii*) Um dieselbe Funktion $5\sin - 3\cos + 7\tan$ in der Basis $B = (\tan - \cos + \sin,\ \tan + 3\sin,\ \cos + \sin)$ darzustellen, schreiben wir sie als Linearkombination der Basisvektoren mit unbekanntem Koeffizientenvektor $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ auf:

$$5\sin + (-3)\cos + 7\tan = x_1(\tan - \cos + \sin) + x_2(\tan + 3\sin) + x_3(\cos + \sin).$$

Ein Koeffizientenvergleich ergibt das lineare Gleichungssystem

$$\begin{matrix} \text{Vergleich der sin-Terme} \rightarrow \\ \text{Vergleich der cos-Terme} \rightarrow \\ \text{Vergleich der tan-Terme} \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ -3 \\ 7 \end{pmatrix}$$

mit der eindeutigen Lösung $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 13 \\ -6 \\ 10 \end{pmatrix}$. (**Quizfrage 19.1:** Warum muss sich hier zwingend eine eindeutige Lösung ergeben?)

Wir führen die Probe durch:

$$\begin{aligned} &13(\tan - \cos + \sin) + (-6)(\tan + 3\sin) + 10(\cos + \sin) \\ &\quad = (13 - 6)\tan + (-13 + 10)\cos + (13 - 18 + 10)\sin \\ &\quad = 7\tan - 3\cos + 5\sin. \end{aligned}$$ △

Beachte: Zur Bestimmung des Koordinatenvektors $\Phi_B^{-1}(v)$ eines Vektors $v \in V$ bzgl. einer Basis B muss i. A. ein lineares Gleichungssystem gelöst werden!

§ 19.2 Darstellung linearer Abbildungen durch Matrizen

Aus Satz 17.10 wissen wir, dass eine lineare Abbildung bereits durch die Bilder der Vektoren einer Basis eindeutig festgelegt ist. Die wesentliche Idee bei der Darstellung einer linearen Abbildung $V \to W$ mit Hilfe einer Matrix ist nun,

- Vektoren in V durch ihre Koordinatenvektoren bzgl. einer Basis B_V darzustellen,
- ebenso Vektoren in W durch ihre Koordinatenvektoren bzgl. einer Basis B_W darzustellen
- und nur noch mit den Koordinatenvektoren zu rechnen, für die die lineare Abbildung notwendigerweise die Form von Matrix-Vektor-Produkten hat (Lemma 17.12).

Als Konsequenz können wir jede lineare Abbildung zwischen beliebigen endlich-dimensionalen Vektorräumen immer in der gleichen, einfachen und konkreten Form von Matrix-Vektor-Produkten auf der Ebene von Koordinatenvektoren darstellen.

Satz 19.3 (Darstellungssatz für lineare Abbildungen)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \ldots, v_m)$ und $B_W = (w_1, \ldots, w_n)$ Basen von V bzw. von W. Dann gibt es zu jeder linearen Abbildung $f\colon V \to W$ eine eindeutig definierte Matrix $A \in K^{n\times m}$ mit der Eigenschaft

$$f(v_j) = \sum_{i=1}^{n} a_{ij}\, w_i \quad \text{für alle } j = 1, \ldots, m. \tag{19.3}$$

Diese Matrix A heißt die **Darstellungsmatrix der linearen Abbildung f bzgl. der Basen B_V und B_W** (englisch: representation matrix), in Symbolen: $A = \mathcal{M}_{B_W \leftarrow B_V}(f)$.

Beweis. f ist durch die Bilder $f(v_j)$ der Basisvektoren v_j, $j = 1, \dots, m$, nach Satz 17.10 eindeutig festgelegt. Für jeden Vektor $f(v_j) \in W$ ist wiederum sein Koordinatenvektor bzgl. der Basis $B_W = (w_1, \dots, w_n)$ eindeutig festgelegt. Dieser Koordinatenvektor $\Phi_{B_W}^{-1}(f(v_j))$ bildet aber gerade die j-Spalte von A, die damit eindeutig festgelegt ist. □

Die Darstellung (19.3) definiert das Bild des j-ten Basisvektors v_j im Definitionsraum V als Linearkombination in der Basis des Zielraumes W. Die j-te Spalte $a_{\bullet j}$ der Darstellungsmatrix A enthält die Koordinaten von $f(v_j) \in W$ bzgl. der Basis B_W. Unsere Konvention beim Symbol der Darstellungsmatrix ist $\mathcal{M}_{\text{nach} \leftarrow \text{von}}$.

Beispiel 19.4 (Darstellungsmatrizen von Homomorphismen)**.**

(*i*) Es seien K ein Körper, $V = K^m$ und $W = K^n$ und die lineare Abbildung $f_A \colon K^m \to K^n$ durch Matrix-Vektor-Multiplikation mit einer Matrix A (Lemma 17.12) gegeben, also $f_A(x) = A\,x$. Wählen wir als Standardbasen $B_V = (e_1, \dots, e_m)$ und $B_W = (e_1, \dots, e_n)$ in K^m und K^n, dann ist A selbst die Darstellungsmatrix $\mathcal{M}_{B_W \leftarrow B_V}(f_A)$.

Inbesondere hat beispielsweise die Drehabbildung aus Beispiel 17.11 als Abbildung $\mathbb{R}^2 \to \mathbb{R}^2$ bzgl. der Standardbasis (e_1, e_2) (in beiden Räumen) die Darstellungsmatrix

$$\begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{bmatrix},$$

siehe (17.6).

(*ii*) Im Vektorraum $V = K^{[\![1,5]\!]}$ der endlichen Folgen (hier der Länge 5) über einem Körper K ist die **Shift-Abbildung** (englisch: shift map)

$$f \colon V \ni (y_1, y_2, y_3, y_4, y_5) \mapsto (0, y_1, y_2, y_3, y_4) \in W = V$$

definiert durch Einfügen einer Null am Anfang der Folge. Die **zyklische Shift-Abbildung** (englisch: cyclic shift map) ist definiert durch

$$g \colon V \ni (y_1, y_2, y_3, y_4, y_5) \mapsto (y_5, y_1, y_2, y_3, y_4) \in W = V.$$

Bzgl. der Standardbasen $B_V = B_W = \big((1,0,0,0,0), \dots, (0,0,0,0,1)\big)$ haben diese Endomorphismen die folgende Darstellung:

$$\mathcal{M}_{B_W \leftarrow B_V}(f) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{bzw.} \quad \mathcal{M}_{B_W \leftarrow B_V}(g) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

(**Quizfrage 19.2:** Können Sie die Form der Darstellungsmatrizen erklären?)

(*iii*) Auf dem Vektorraum $\mathbb{R}^{\mathbb{R}}$ der Funktionen $\mathbb{R} \to \mathbb{R}$ betrachten wir den vierdimensionalen Unterraum V der Funktionen, der von der Basis $B_V = (t \mapsto 1,\ t \mapsto t,\ t \mapsto t^2,\ t \mapsto t^3)$ aufgespannt wird. (**Quizfrage 19.3:** Warum ist das eine linear unabängige Familie?) Jede Funktionsauswertung eines Elements von V an einem festen Punkt ist eine lineare Abbildung $V \to \mathbb{R}$. (**Quizfrage 19.4:** Klar?) Wir betrachten diejenige lineare Abbildung $f\colon V \to W = \mathbb{R}^3$, die durch die drei Punktauswertungen an den Stellen -2, 0 und 2 gegeben ist, und wählen im Zielraum $W = \mathbb{R}^3$ die Standardbasis $B_W = (e_1, e_2, e_3)$. Dann hat die lineare Abbildung f die Darstellungsmatrix

$$\mathcal{M}_{B_W \leftarrow B_V}(f) = \begin{bmatrix} 1 & -2 & 4 & -8 \\ 1 & 0 & 0 & 0 \\ 1 & 2 & 4 & 8 \end{bmatrix} \begin{matrix} \leftarrow \text{Auswertung bei } t = -2 \\ \leftarrow \text{Auswertung bei } t = 0 \\ \leftarrow \text{Auswertung bei } t = 2. \end{matrix}$$

(*iv*) Wir betrachten den zweidimensionalen Vektorraum $V = \mathbb{C}$ über dem Körper $\mathbb{R}$ mit der Basis $B_V = (1, i)$ sowie den eindimensionalen Vektorraum $W = \mathbb{R}$ über dem Körper $\mathbb{R}$ mit der Standardbasis $B_W = (1)$. Die lineare Abbildung $\mathrm{Re}\colon \mathbb{C} \to \mathbb{R}$ (Realteil) hat dann die Darstellungsmatrix

$$\mathcal{M}_{B_W \leftarrow B_V}(\mathrm{Re}) = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

während die lineare Abbildung $\mathrm{Im}\colon \mathbb{C} \to \mathbb{R}$ (Imaginärteil) die Darstellungsmatrix

$$\mathcal{M}_{B_W \leftarrow B_V}(\mathrm{Im}) = \begin{bmatrix} 0 & 1 \end{bmatrix} \tag{19.4}$$

besitzt.

(*v*) Im Fall $V = W$ und für eine beliebige Wahl $B_V = B_W$ der Basis hat die Identitätsabbildung $\mathrm{id}_V\colon V \to V$ die Darstellungsmatrix

$$\mathcal{M}_{B_V \leftarrow B_V}(\mathrm{id}_V) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix},$$

also die Einheitsmatrix der passenden Dimension. △

Das folgende Resultat zeigt, dass durch eine geschickte Wahl der Basen B_V und B_W eine möglichst einfache Form der Darstellungsmatrix einer linearen Abbildung $V \to W$ erreicht werden kann.

Lemma 19.5 (möglichst einfache Darstellungsmatrizen für lineare Abbildungen)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter sei $f\colon V \to W$ ein Homomorphismus mit $r = \mathrm{Rang}(f)$ und $\mathrm{Defekt}(f) = \dim(\mathrm{Kern}(f)) = m - r$ nach Dimensionsformel (18.5). Wir können Basen B_V, B_W so wählen, dass gilt

$$B_W = (\underbrace{w_1, \ldots, w_r}_{\text{Basis von Bild}(f)}, \underbrace{w_{r+1}, \ldots, w_n}_{\text{Ergänzung zu einer Basis von } W})$$

und

$$B_V = (\underbrace{v_1, \dots, v_r}_{v_j \in f^{-1}(\{w_j\})}, \underbrace{v_{r+1}, \dots, v_m}_{\text{Basis von Kern}(f)}).$$

Die Darstellungsmatrix $\mathcal{M}_{B_W \leftarrow B_V}(f)$ von f bzgl. dieser Basen hat die Gestalt

$$\mathcal{M}_{B_W \leftarrow B_V}(f) = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \in K^{n \times m}. \tag{19.5}$$

Beweis. □

Wir gehen nun der Frage nach, welche Eigenschaften die Zuordnung eines Homomorphismus zu seiner Darstellungsmatrix bzgl. fest gewählter Basen hat:

Satz 19.6 (die Zuordnung zur Darstellungsmatrix ist ein Vektorraumisomorphismus)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \dots, v_m)$ und $B_W = (w_1, \dots, w_n)$ Basen von V bzw. von W. Die Zuordnung

$$\mathcal{M}_{B_W \leftarrow B_V} : \operatorname{Hom}(V, W) \ni f \mapsto \mathcal{M}_{B_W \leftarrow B_V}(f) \in K^{n \times m} \tag{19.6}$$

eines Homomorphismus zu seiner Darstellungsmatrix ist ein Isomorphismus von Vektorräumen.

Beachte: Dieses Resultat besagt, dass — wenn es um Vektorraumeigenschaften geht — unerheblich ist, ob wir Homomorphismen oder deren Darstellungsmatrizen betrachten.

Beweis. Wir zerlegen den Beweis in mehrere Schritte:

Schritt 1: Wir zeigen zunächst die Linearität von $\mathcal{M}_{B_W \leftarrow B_V}$.

Es seien dazu $f, g \in \operatorname{Hom}(V, W)$, $A := \mathcal{M}_{B_W \leftarrow B_V}(f)$ und $B := \mathcal{M}_{B_W \leftarrow B_V}(g)$. Dann gilt

$$\begin{aligned}(f+g)(v_j) &= f(v_j) + g(v_j) \\ &= \sum_{i=1}^{n} a_{ij}\, w_i + \sum_{i=1}^{n} b_{ij}\, w_i \\ &= \sum_{i=1}^{n} (a_{ij} + b_{ij})\, w_i\end{aligned}$$

für alle $j = 1, \dots, m$. Das heißt $\mathcal{M}_{B_W \leftarrow B_V}(f+g) = \mathcal{M}_{B_W \leftarrow B_V}(f) + \mathcal{M}_{B_W \leftarrow B_V}(g)$. Weiter gilt für $\alpha \in K$

$$\begin{aligned}(\alpha f)(v_j) &= \alpha\, f(v_j) \\ &= \alpha \sum_{i=1}^{n} a_{ij}\, w_i \\ &= \sum_{i=1}^{n} (\alpha\, a_{ij})\, w_i\end{aligned}$$

für alle $j = 1, \dots, m$. Das heißt $\mathcal{M}_{B_W \leftarrow B_V}(\alpha f) = \alpha\, \mathcal{M}_{B_W \leftarrow B_V}(f)$.

Schritt 2: Wir zeigen: $\mathcal{M}_{B_W \leftarrow B_V}$ ist injektiv.

Es sei dazu $f \in \mathrm{Hom}(V, W)$ so, dass $\mathcal{M}_{B_W \leftarrow B_V}(f) = 0 \in K^{n \times m}$ (die Nullmatrix) ergibt. Das heißt,

$$f(v_j) = \sum_{i=1}^{n} 0\, w_i = 0$$

für alle $j = 1, \ldots, m$. Damit ist $f\colon V \to W$ der Nullhomomorphismus, also der Nullvektor von $\mathrm{Hom}(V, W)$. Daher gilt $\mathrm{Kern}(\mathcal{M}_{B_W \leftarrow B_V}) = \{0\}$, und nach Lemma 17.8 ist $\mathcal{M}_{B_W \leftarrow B_V}$ injektiv.

Schritt 3: Wir zeigen: $\mathcal{M}_{B_W \leftarrow B_V}$ ist surjektiv.

Es sei dazu $A \in K^{n \times m}$. Nach Satz 17.10 gibt es (genau) einen Homomorphismus $f\colon V \to W$, der $f(v_j) = \sum_{i=1}^{n} a_{ij}\, w_i$ als Bilder und damit A als Darstellungsmatrix hat. □

Quizfrage 19.5: Warum haben wir, um die Bijektivität von $\mathcal{M}_{B_W \leftarrow B_V}$ zu zeigen, nicht die Charakterisierung der Bijektivität von Homomorphismen (bijektiv ⇔ injektiv ⇔ surjektiv) nach Folgerung 18.9 genutzt?

Folgerung 19.7 (Dimension des Vektorraumes der Homomorphismen)**.**

Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Dann gilt

$$\dim(\mathrm{Hom}(V, W)) = n\, m. \tag{19.7}$$

Beweis. Das Resultat folgt aus $\dim(K^{n \times m}) = n\, m$ (Satz 15.3) und der Isomorphie $\mathrm{Hom}(V, W) \cong K^{n \times m}$, aufgrund derer beide Räume $K^{n \times m}$ und $\mathrm{Hom}(V, W)$ dieselbe Dimension haben (Satz 18.1). □

Die Darstellungsmatrix $A \in K^{n \times m}$ einer linearen Abbildung $f\colon V \to W$ bzgl. fest gewählter Basen B_V und B_W induziert eine lineare Abbildung $f_A\colon K^m \to K^n$ (Lemma 17.12) auf Koeffizientenvektoren. Das folgende Resultat stellt den Zusammenhang zwischen diesen beiden linearen Abbildungen her.

Satz 19.8 (Zusammenhang zwischen einem Homomorphismus und dem durch seine Darstellungsmatrix induzierten Homomorphismus)**.**

Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \ldots, v_m)$ und $B_W = (w_1, \ldots, w_n)$ Basen von V bzw. von W und $f\colon V \to W$ ein Homomorphismus. Dann gilt für die Darstellungsmatrix $A := \mathcal{M}_{B_W \leftarrow B_V}(f)$ und die durch A induzierte lineare Abbildung f_A der Zusammenhang

$$f_A = \underbrace{\Phi_{B_W}^{-1}}_{\text{Koordinaten} \mapsto \text{Vektor}} \circ f \circ \underbrace{\Phi_{B_V}}_{\text{Vektor} \mapsto \text{Koordinaten}} : K^m \to K^n \tag{19.8a}$$

$$f = \underbrace{\Phi_{B_W}}_{\text{Vektor} \hookleftarrow \text{Koordinaten}} \circ f_A \circ \underbrace{\Phi_{B_V}^{-1}}_{\text{Koordinaten} \hookleftarrow \text{Vektor}} : V \to W. \tag{19.8b}$$

Mit anderen Worten, das folgende Diagramm kommutiert:

$$\begin{array}{ccc} W & \xleftarrow{\ f\ } & V \\ {\scriptstyle \Phi_{B_W}}\uparrow & & \downarrow{\scriptstyle \Phi_{B_V}^{-1}} \\ K^n & \xleftarrow[\ f_A\ ]{} & K^m \end{array}$$

Beachte: (19.8a) besagt, dass Matrix-Vektor-Produkte $f_A(x) = A\,x$ wie folgt wirken: Der Koordinatenvektor $x \in K^m$ wird durch Linearkombinationen der Basisvektoren in B_V zum Vektor $\Phi_{B_V}(x) \in V$ synthetisiert, auf diesen wirkt dann die Abbildung f, und schließlich wird das Ergebnis durch $\Phi_{B_W}^{-1}$ als Koordinatenvektor bzgl. der Basis B_W angegeben. (**Quizfrage 19.6:** Wie lässt sich (19.8b) interpretieren?)

Beweis. Wir zeigen, dass die Abbildungen $\Phi_{B_W} \circ f_A \in \mathrm{Hom}(K^m, W)$ und $f \circ \Phi_{B_V} \in \mathrm{Hom}(K^m, W)$ übereinstimmen. Dazu reicht es nach Satz 17.10 aus, zu zeigen, dass ihre Bilder auf einer Basis gleich sind. Wir wählen dazu die Standardbasis $(e_1, \dots, e_m)$ von K^m. Es gilt einerseits

$$\begin{aligned} (\Phi_{B_W} \circ f_A)(e_j) &= \Phi_{B_W}(f_A(e_j)) && \text{nach Definition 6.14 der Komposition } \circ \\ &= \Phi_{B_W}(A\,e_j) && \text{nach Definition der von } A \text{ induzierten Abbildung } f_A \\ &= \Phi_{B_W}(a_{\bullet j}) && \text{nach Definition des Matrix-Vektor-Produkts} \\ &= \sum_{i=1}^{n} a_{ij}\, w_i && \text{nach Definition (19.1) von } \Phi_{B_W} \end{aligned}$$

und andererseits

$$\begin{aligned} (f \circ \Phi_{B_V})(e_j) &= f(\Phi_{B_V}(e_j)) && \text{nach Definition 6.14 der Komposition } \circ \\ &= f(v_j) && \text{nach Definition (19.1) von } \Phi_{B_V} \\ &= \sum_{i=1}^{n} a_{ij}\, w_i && \text{nach Definition (19.3) der Darstellungsmatrix } A. \end{aligned}$$

Aus $\Phi_{B_W} \circ f_A \in \mathrm{Hom}(K^m, W) = f \circ \Phi_{B_V}$ können wir nun (19.8a) und (19.8b) leicht durch Auflösen herleiten, weil Φ_{B_V} und Φ_{B_W} bijektiv sind. □

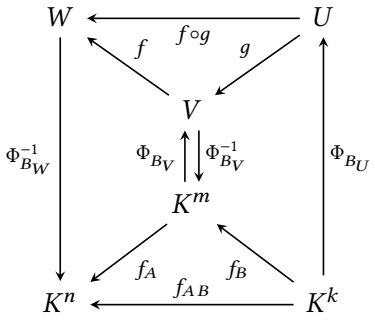
Wir zeigen abschließend in diesem Abschnitt nun noch, dass die Komposition linearer Abbildungen durch das Matrix-Matrix-Produkt ihrer Darstellungsmatrizen dargestellt wird.

Satz 19.9 (Darstellungsmatrix der Komposition von Homomorphismen)**.**
Es seien U, V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(U) = k \in \mathbb{N}_0$, $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_U = (u_1, \dots, u_k)$, $B_V = (v_1, \dots, v_m)$ und $B_W = (w_1, \dots, w_n)$ Basen von U bzw. von V bzw. von W und $g\colon U \to V$ sowie $f\colon V \to W$ Homomorphismen. Dann gilt für die Darstellungsmatrizen der Zusammenhang

$$\mathcal{M}_{B_W \leftarrow B_U}(f \circ g) = \mathcal{M}_{B_W \leftarrow B_V}(f)\, \mathcal{M}_{B_V \leftarrow B_U}(g). \tag{19.9}$$

Beachte: Im mittleren Raum V muss für die Darstellung der ankommenden Abbildung g und für die Darstellung der ausgehenden Abbildung f dieselbe Basis B_V verwendet werden.

Beweis. Wir führen den Beweis mit Hilfe eines Diagrammes:



Zur Abkürzung setzen wir $A \coloneqq \mathcal{M}_{B_W \leftarrow B_V}(f)$ und $B \coloneqq \mathcal{M}_{B_V \leftarrow B_U}(g)$. Das rechte und das linke Trapez sind kommutativ nach Satz 19.8, d. h., es gilt

$$f_A = \Phi_{B_W}^{-1} \circ f \circ \Phi_{B_V} \quad \text{und} \quad f_B = \Phi_{B_V}^{-1} \circ g \circ \Phi_{B_U}.$$

Das obere Dreieck ist kommutativ aufgrund der Definition von $f \circ g$. Das untere Dreieck ist kommutativ wegen $f_A \circ f_B = f_{AB}$, siehe Lemma 17.12. Damit folgt

$$\begin{aligned} f_{AB} &= f_A \circ f_B \\ &= \Phi_{B_W}^{-1} \circ f \circ \Phi_{B_V} \circ \Phi_{B_V}^{-1} \circ g \circ \Phi_{B_U} \\ &= \Phi_{B_W}^{-1} \circ f \circ g \circ \Phi_{B_U} \\ &= \Phi_{B_W}^{-1} \circ (f \circ g) \circ \Phi_{B_U}. \end{aligned}$$

Das heißt aber, AB ist die Darstellungsmatrix $\mathcal{M}_{B_W \leftarrow B_U}(f \circ g)$, was zu beweisen war. □

Ende der Vorlesung 26

§ 19.3 Eigenschaften linearer Abbildungen und ihrer Darstellungsmatrizen

Der isomorphe Zusammenhang zwischen linearen Abbildungen und ihren Darstellungsmatrizen (bzgl. beliebiger, aber fester Basen) erlaubt es, Eigenschaften linearer Abbildungen an ihren Darstellungsmatrizen abzulesen und umgekehrt. Um die bisher für Matrizen bzw. lineare Abbildungen schon bekannten Begriffe einmal zu rekapitulieren und fehlendes Vokabular zu ergänzen, geben wir folgende Tabelle an. Dabei ist K ein Körper, und V und W sind endlich-dimensionale Vektorräume über K.

Matrix $A \in K^{n\times m}$		lineare Abbildung $f\colon V \to W$	
Begriff	siehe	Begriff	siehe
$\mathrm{Bild}(A) \coloneqq \mathrm{SR}(A)$	(15.15a)	$\mathrm{Bild}(f) = \{f(u) \in W \mid u \in V\} = f(V)$	(17.4)
$\mathrm{SRang}(A) = \dim(\mathrm{SR}(A))$	(15.15b)	$\mathrm{Rang}(f) = \dim(\mathrm{Bild}(f))$	(18.6)
A ist surjektiv: $\mathrm{Bild}(A) = K^n$		f ist surjektiv: $\mathrm{Bild}(f) = W$	
$\mathrm{Kern}(A) \coloneqq \{x \in K^m \mid Ax = 0\}$		$\mathrm{Kern}(f) = \{u \in V \mid f(u) = 0\} = f^{-1}(\{0\})$	(17.5)
$\mathrm{Defekt}(A) \coloneqq \dim(\mathrm{Kern}(A))$		$\mathrm{Defekt}(f) = \dim(\mathrm{Kern}(f))$	(18.7)
A ist injektiv: $\mathrm{Kern}(A) = \{0\}$		f ist injektiv: $\mathrm{Kern}(f) = \{0\}$	

Beachte: Die Eigenschaften, die man der Matrix A zuspricht, sind gleichzeitig auch die Eigenschaften der von der Matrix induzierten linearen Abbildung f_A, also z. B. $\mathrm{Bild}(A) = \mathrm{Bild}(f_A)$ und $\mathrm{Kern}(A) = \mathrm{Kern}(f_A)$.

Wir können nun bestätigen, wie die oben genannten Begriffe für lineare Abbildungen zwischen endlich-dimensionalen Vektorräumen und ihren Darstellungsmatrizen zusammenhängen:

Satz 19.10 (Eigenschaften linearer Abbildungen und ihrer Darstellungsmatrizen)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \dots, v_m)$ und $B_W = (w_1, \dots, w_n)$ Basen von V bzw. von W und $f\colon V \to W$ ein Homomorphismus. Schließlich sei $A \coloneqq \mathcal{M}_{B_W \leftarrow B_V}(f) \in K^{n\times m}$ die Darstellungsmatrix von f bzgl. dieser Basen. Dann gilt:

(*i*) $\mathrm{Bild}(f) = \Phi_{B_W}\big(\mathrm{Bild}(A)\big)$.

(*ii*) $\mathrm{Rang}(f) = \mathrm{SRang}(A) = \mathrm{Rang}(A)$.
Insbesondere ist f surjektiv genau dann, wenn die Zeilen von A linear unabhängig sind.

(*iii*) $\mathrm{Kern}(f) = \Phi_{B_V}\big(\mathrm{Kern}(A)\big)$.

(*iv*) $\mathrm{Defekt}(f) = \mathrm{Defekt}(A)$.
Insbesondere ist f injektiv genau dann, wenn die Spalten von A linear unabhängig sind.

Beweis. Aussage (*i*): Es gilt

$$
\begin{aligned}
& w \in \mathrm{Bild}(f) \\
\Leftrightarrow\ & w \in \mathrm{Bild}(\Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}) && \text{wegen } f = \Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}, \text{ siehe (19.8b)} \\
\Leftrightarrow\ & w \in \Phi_{B_W}\big(\mathrm{Bild}(f_A \circ \Phi_{B_V}^{-1})\big) && \text{nach Definition von Bild} \\
\Leftrightarrow\ & w \in \Phi_{B_W}\big(\mathrm{Bild}(f_A)\big) && \text{wegen der Bijektivität von } \Phi_{B_V}^{-1} \\
\Leftrightarrow\ & w \in \Phi_{B_W}\big(\mathrm{Bild}(A)\big) && \text{wegen } f_A(x) = Ax.
\end{aligned}
$$

Aussage (*ii*): $\mathrm{Bild}(f)$ und $\mathrm{Kern}(A)$ sind nach Aussage (*i*) zueinander isomorphe Unterräume von W bzw. von K^n. Nach Satz 18.1 haben sie also dieselbe Dimension.

Weiter gilt

$$f \text{ ist surjektiv}$$

$\Leftrightarrow$	$\text{Bild}(f) = W$	nach Definition der Surjektivität
$\Leftrightarrow$	$\dim(\text{Bild}(f)) = n$	nach Folgerung 13.17
$\Leftrightarrow$	$\text{Rang}(f) = n$	nach Definition 18.8 von $\text{Rang}(f)$
$\Leftrightarrow$	$\text{Rang}(A) = n$	wie gerade gezeigt
$\Leftrightarrow$	die Zeilen von A sind linear unabhängig	nach Lemma 15.11 und Satz 15.13.

Aussage *(iii)*: Es gilt

	$v \in \text{Kern}(f)$	
$\Leftrightarrow$	$v \in \text{Kern}(\Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1})$	wegen $f = \Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}$, siehe (19.8b)
$\Leftrightarrow$	$v \in \Phi_{B_V}\big(\text{Kern}(\Phi_{B_W} \circ f_A)\big)$	wegen der Bijektivität von $\Phi_{B_V}^{-1}$
$\Leftrightarrow$	$v \in \Phi_{B_V}\big(\text{Kern}(f_A)\big)$	wegen der Bijektivität von Φ_{B_W}
$\Leftrightarrow$	$v \in \Phi_{B_V}\big(\text{Kern}(A)\big)$	wegen $f_A(x) = A\,x$.

Aussage *(iv)*: $\text{Kern}(f)$ und $\text{Bild}(A)$ sind nach Aussage *(iii)* zueinander isomorphe Unterräume von V bzw. von K^m. Nach Satz 18.1 haben sie also dieselbe Dimension.

Weiter gilt

	f ist injektiv	
$\Leftrightarrow$	$\text{Kern}(f) = \{0\}$	nach Lemma 17.9
$\Leftrightarrow$	$\dim(\text{Kern}(f)) = 0$	nach Beispiel 13.16
$\Leftrightarrow$	$\text{Defekt}(f) = 0$	nach Definition 18.8 von $\text{Defekt}(f)$
$\Leftrightarrow$	$\text{Rang}(f) = m$	nach Dimensionsformel (18.8)
$\Leftrightarrow$	$\text{SRang}(A) = \text{Rang}(A) = m$	nach Aussage *(ii)*
$\Leftrightarrow$	die Spalten von A sind linear unabhängig	nach Lemma 15.11. □

Satz 19.10 erlaubt es uns also, das Bild und den Kern einer beliebigen linearen Abbildung f zwischen beliebigen endlich-dimensionalen Vektorräumen auf eine standardisierte Weise zu berechnen. Dazu wählen wir irgendwelche Basen B_V und B_W und bestimmen die Darstellungsmatrix $A = \mathcal{M}_{B_W \leftarrow B_V}(f)$. Anschließend berechnen wir eine Basis des Unterraumes $\text{Bild}(A) \subseteq \mathbb{R}^n$ bzw. des Unterraumes $\text{Kern}(A) \subseteq \mathbb{R}^m$ (dazu gleich mehr). Um daraus dann eine Basis von $\text{Bild}(f) \subseteq W$ zu erhalten, müssen wir laut Satz 19.10 lediglich die Basisvektoren von $\text{Bild}(A)$ als Koordinatenvektoren bzgl. der Basis B_W interpretieren. Analog: Um eine Basis von $\text{Kern}(f) \subseteq V$ zu erhalten, interpretieren wir die Basisvektoren von $\text{Kern}(A)$ als Koordinatenvektoren bzgl. der Basis B_V. (**Quizfrage 19.7:** Warum können wir sicher sein, wieder eine Basis zu erhalten?)

Wie können wir nun für eine gegebene Matrix $A \in K^{n\times m}$ eine Basis von $\text{Bild}(A) \subseteq K^n$ bzw. eine Basis von $\text{Kern}(A) \subseteq K^m$ berechnen?

Bemerkung 19.11 (zur Bestimmung von Bild und Kern einer Matrix)**.**

(i) Für $\text{Bild}(A)$ haben wir folgende Möglichkeiten:

(1) Wir bestimmen mit Hilfe von Algorithmus D.2, wie in Bemerkung 15.25 beschrieben, eine Rangfaktorisierung $A = B_{\text{Rang}} C_{\text{Rang}}$ mit $B_{\text{Rang}} \in K^{n\times r}$ und $C_{\text{Rang}} \in K^{r\times m}$ (in Zeilenstufenform) und $r = \text{Rang}(A)$. Dann bilden die Spalten von B_{Rang} eine Basis von $\text{Bild}(A) = \text{SR}(A)$.

(2) Wir nutzen die Beziehung $\text{Bild}(A) = \text{SR}(A) = [\text{ZR}(A^\mathsf{T})]^\mathsf{T}$, bringen A^T in Zeilenstufenform (Algorithmus D.1) und erhalten somit eine Basis von $\text{ZR}(A^\mathsf{T})$. Durch Transposition der Basisvektoren von $\text{ZR}(A^\mathsf{T})$ bekommen wir die gesuchte Basis von $\text{Bild}(A)$.

Für die Rechnung per Hand erscheint die zweite Möglichkeit günstiger, weil wir den linken Faktor „B“ nicht mitführen müssen.

(*ii*) Die Bestimmung von $\text{Kern}(A) = \mathcal{L}(A, 0)$ haben wir in § 16 bei der Lösung linearer Gleichungssysteme bereits durchgeführt. Zur Erinnerung: Wir bringen die erweiterte Koeffizientenmatrix $[A, 0]$ zunächst in Zeilenstufenform. Daran können wir bereits $\text{Rang}(A)$ und damit auch $\dim(\text{Kern}(A)) = m - \text{Rang}(A)$ ablesen. Wenn $\dim(\text{Kern}(A)) = 0$ gilt, dann ist $\text{Kern}(A) = \{0\}$ und die einzige Basis von $\text{Kern}(A)$ ist die leere Menge. Wenn $\dim(\text{Kern}(A)) > 0$ gilt, dann überführen wir das System weiter in die reduzierte Zeilenstufenform. Anschließend können wir nacheinander Basisvektoren von $\text{Kern}(A)$ bestimmen, indem wir eine der unabhängigen Variablen x_i auf den Wert 1 und die anderen unabhängigen Variablen auf den Wert 0 setzen und die Werte der abhängigen Variablen von hinten nach vorne aus den Gleichungen ausrechnen (Bemerkung 16.4 und Beispiel 16.10). △

Beispiel 19.12 (zur Bestimmung von Bild und Kern einer Matrix)**.**

Wir betrachten wie in Beispiel 19.4 den vierdimensionalen Unterraum V der Funktionen $\mathbb{R} \to \mathbb{R}$, der von der Basis $B_V = (t \mapsto 1,\ t \mapsto t,\ t \mapsto t^2,\ t \mapsto t^3)$ aufgespannt wird, und darauf die lineare Abbildung $f : V \to W = \mathbb{R}^3$, die durch die drei Punktauswertungen an den Stellen -2, 0 und 2 gegeben ist. Bezüglich der Standardbasis $B_W = (e_1, e_2, e_3)$ hat f die Darstellungsmatrix

$$A = \begin{bmatrix} 1 & -2 & 4 & -8 \\ 1 & 0 & 0 & 0 \\ 1 & 2 & 4 & 8 \end{bmatrix}.$$

Eine Zeilenstufenform von A^T ist gegeben durch

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 4 \\ 0 & 0 & 8 \\ 0 & 0 & 0 \end{bmatrix}.$$

Es gilt also $\text{Rang}(A^\mathsf{T}) = \text{Rang}(A) = 3$. Die ersten drei Zeilen bilden eine Basis von $\text{ZR}(A^\mathsf{T})$. Ihre Transponierten bilden also eine Basis von $\text{SR}(A) = \text{Bild}(A)$, d. h., wir haben

$$\text{Bild}(A) = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 8 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle.$$

Da $\text{Bild}(A)$ aber maximale Dimension in $\mathbb{R}^3$ hat, also $\text{Bild}(A) = \mathbb{R}^3$ gilt, können wir auch jede andere Basis von $\mathbb{R}^3$ (z. B. die Standardbasis) als Basis von $\text{Bild}(A)$ verwenden.

Um $\mathrm{Kern}(A)$ zu bestimmen, bringen wir $[A, 0]$ zunächst in Zeilenstufenform

$$\left[\begin{array}{cccc|c} 1 & -2 & 4 & -8 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 8 & 0 \end{array}\right] \quad \rightsquigarrow \quad \left[\begin{array}{cccc|c} 1 & -2 & 4 & -8 & 0 \\ 0 & 2 & -4 & 8 & 0 \\ 0 & 0 & 8 & 0 & 0 \end{array}\right],$$

wo wir wiederum $\mathrm{Rang}(A) = 3$ und damit $\mathrm{Defekt}(A) = \dim(\mathrm{Kern}(A)) = 4 - 3 = 1$ ablesen können. Wir gehen weiter zu reduzierten Zeilenstufenform

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right],$$

an der wir ablesen:[35]

$$\mathrm{Kern}(A) = \left\langle \begin{pmatrix} 0 \\ -4 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

Übersetzen wir $\mathrm{Kern}(A)$ zurück in den Vektorraum V, so bedeutet das nach Satz 19.10 Aussage *(iii)*, dass wir $\begin{pmatrix} 0 \\ -4 \\ 0 \\ 1 \end{pmatrix}$ als Koordinatenvektor bzgl. der gewählten Basis $B_V = (t \mapsto 1,\ t \mapsto t,\ t \mapsto t^2,\ t \mapsto t^3)$ interpretieren müssen. Es sind also genau die Vielfachen der Funktion

$$t \mapsto p(t) \coloneqq 0\,1 - 4\,t + 0\,t^2 + 1\,t^3 = -4\,t + t^3,$$

die in $\mathrm{Kern}(f)$ liegen, die also die Eigenschaft besitzen, dass alle drei Punktauswertungen Null ergeben. In der Tat gilt

$$\begin{aligned} p(-2) &= -4 \cdot (-2) + (-2)^3 = 0 \\ p(0) &= -4 \cdot 0 + 0^3 = 0 \\ p(2) &= -4 \cdot 2 + 2^3 = 0. \end{aligned}$$

Wir haben also

$$\mathrm{Kern}(f) = \langle t \mapsto -4\,t + t^3 \rangle \subseteq V.$$

Für $\mathrm{Bild}(A)$ ist in unserem Beispiel keine solche Übersetzung zurück erforderlich, denn wegen der Wahl der Standardbasis in $\mathbb{R}^3$ gilt $\mathrm{Bild}(A) = \mathrm{Bild}(f)$. (**Quizfrage 19.8:** Wie äußert sich das in Aussage *(i)* von Satz 19.10?) △

Neben den Zusammenhängen in Satz 19.10 können wir auch die Invertierbarkeit einer linearen Abbildung in Verbindung bringen mit der Invertierbarkeit ihrer Darstellungsmatrix. Wie wir aus Folgerung 18.9 wissen, müssen dazu notwendigerweise beide endlich-dimensionalen Vektorräume dieselbe Dimension besitzen (und gleichbedeutend damit die Darstellungsmatrix quadratisch sein).

[35] Noch geschickter wäre folgendes Vorgehen gewesen: Wir bestimmen eine (reduzierte) Zeilenstufenform von A, um damit $\mathrm{Rang}(A)$, eine Basis von $\mathrm{Kern}(A)$ und $\dim(\mathrm{Kern}(A))$ zu bestimmen. Falls wie hier im Beispiel $\mathrm{Rang}(A) = n$ gilt, können wir uns die Berechnung einer Basis von $\mathrm{Bild}(A)$ sparen, da $\mathrm{Bild}(A)$ den ganzen K^n ausfüllt.

Satz 19.13 (Invertierbarkeit linearer Abbildungen und ihrer Darstellungsmatrizen)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K gleicher Dimension $\dim(V) = \dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \dots, v_n)$ und $B_W = (w_1, \dots, w_n)$ Basen von V bzw. von W und $f\colon V \to W$ ein Homomorphismus. Schließlich sei $A := \mathcal{M}_{B_W \leftarrow B_V}(f) \in K^{n\times n}$ die Darstellungsmatrix von f bzgl. dieser Basen. Dann sind äquivalent:

(*i*) f ist bijektiv.
(*ii*) $\mathrm{Rang}(f) = n$.
(*iii*) $\mathrm{Defekt}(f) = 0$.
(*iv*) A ist invertierbar.
(*v*) $\mathrm{Rang}(A) = n$.
(*vi*) $\mathrm{Defekt}(A) = 0$.

Ist f bijektiv, dann gilt für die Darstellungsmatrix der Inversen $f^{-1}\colon W \to V$

$$\mathcal{M}_{B_V \leftarrow B_W}(f^{-1}) = A^{-1}. \tag{19.10}$$

Beweis. Die Äquivalenz der Aussagen (*i*) bis (*iii*) wurde in Folgerung 18.9 gezeigt. Die Äquivalenz der Aussagen (*iv*) und (*v*) wurde in Satz 15.45 gezeigt. Nach Satz 19.10 gilt $\mathrm{Rang}(f) = \mathrm{Rang}(A)$, also sind auch Aussagen (*ii*) und (*v*) äquivalent. Ebenfalls nach Satz 19.10 gilt $\mathrm{Defekt}(f) = \mathrm{Defekt}(A)$, also sind auch Aussagen (*iii*) und (*vi*) äquivalent.

Ist f bijektiv, dann gilt

$$\begin{aligned}
& f^{-1} \circ f = \mathrm{id}_V \\
\Rightarrow\quad & \mathcal{M}_{B_V \leftarrow B_V}(f^{-1} \circ f) = \mathcal{M}_{B_V \leftarrow B_V}(\mathrm{id}_V) \\
\Rightarrow\quad & \mathcal{M}_{B_V \leftarrow B_W}(f^{-1})\, \mathcal{M}_{B_W \leftarrow B_V}(f) = I_n \qquad \text{nach Satz 19.9 und Beispiel 19.4} \\
\Rightarrow\quad & \mathcal{M}_{B_V \leftarrow B_W}(f^{-1}) \qquad A \qquad = I_n.
\end{aligned}$$

Das ist nach Satz 15.47 (Rechtsinverse quadratischer Matrizen sind Linksinverse und umgekehrt) bereits ausreichend, um (19.10) zu bestätigen. □

Wir können außerdem eine Variante von Satz 19.13 angeben, die die Links- bzw. Rechtsinvertierbarkeit linearer Abbildungen und ihrer Darstellungsmatrizen betrifft:[36]

Satz 19.14 (Links- bzw. Rechtsinvertierbarkeit linearer Abbildungen und ihrer Darstellungsmatrizen)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K mit $\dim(V) = m \in \mathbb{N}_0$ und $\dim(W) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \dots, v_m)$ und $B_W = (w_1, \dots, w_n)$ Basen von V bzw. von W und $f\colon V \to W$ ein Homomorphismus. Schließlich sei $A := \mathcal{M}_{B_W \leftarrow B_V}(f) \in K^{n\times m}$ die Darstellungsmatrix von f bzgl. dieser Basen.

(*i*) Es sind äquivalent:

[36] Aufgrund der vorausgesetzen endlichen Dimension der Vektorräume und der Linearität der Abbildung benötigen wir hier im Unterschied zu Satz 6.44 das Auswahlaxiom nicht.

(a) f ist surjektiv, also $\text{Rang}(f) = n$.

(b) Es existiert eine Rechtsinverse von f, also eine lineare Abbildung $f_r \colon K^n \to K^m$, sodass $f \circ f_r = \text{id}_{K^n}$ gilt. f_r ist notwendig injektiv.

(c) A besitzt vollen Zeilenrang, also $\text{Rang}(A) = n$.

(d) Es existiert eine Rechtsinverse von A, also eine Matrix $R \in K^{m \times n}$ mit $A\,R = I_n$ gilt. R besitzt notwendig vollen Spaltenrang.

(*ii*) Es sind äquivalent:

(a) f ist injektiv, also $\text{Defekt}(f) = 0$, d. h. $\text{Rang}(f) = m$.

(b) Es existiert eine Linksinverse von f, also eine lineare Abbildung $f_l \colon K^n \to K^m$, sodass $f_l \circ f = \text{id}_{K^m}$ gilt. f_l ist notwendig surjektiv. Ihre Einschränkung $f_l|_{f(V)}$ auf das Bild von f ist eindeutig.

(c) A besitzt vollen Spaltenrang, also $\text{Rang}(A) = m$.

(d) Es existiert eine Linksinverse von A, also eine Matrix $L \in K^{n \times m}$ mit $L\,A = I_m$ gilt. L besitzt notwendig vollen Zeilenrang.

Beweis. □

Aufgrund von Satz 19.14 wird manchmal auch die Sprechweise verwendet, eine **Matrix** A sei **surjektiv** oder **injektiv**. Gemeint ist immer die Aussage, dass jede durch A repräsentierte lineare Abbildung (z. B. $x \mapsto A\,x$) surjektiv bzw. injektiv ist.

§ 19.4 Transformationsmatrizen des Basiswechsels

Die Darstellung eines Vektors v eines endlich-dimensionalen Vektorraumes V mit Hilfe seines Koordinatenvektors $x = \Phi_{B_V}^{-1}(v) \in K^n$ hängt von der Wahl der Basis B_V ab. Ebenso hängt die Beschreibung von Homomorphismen über Darstellungsmatrizen von der Wahl der Basen im Definitions- und Zielraum ab. Es stellen sich daher folgende Fragen:

(1) Wie transformiert sich ein Koordinatenvektor beim Wechsel der Basis?

(2) Wie transformiert sich die Darstellungsmatrix eines Homomorphismus, wenn wir eine oder beide Basen wechseln?

(3) In welchen Basen hat die Darstellungsmatrix eines Homomorphismus eine besonders einfache Gestalt?

Die Frage (3) ist mit Lemma 19.5 bereits beantwortet: Die Darstellung $\left[\begin{smallmatrix} I_r & 0 \\ 0 & 0 \end{smallmatrix}\right]$ ist möglich, und einfacher geht es nicht, weil alle Darstellungsmatrizen einer linearen Abbildung nach Satz 19.10 denselben Rang wie die Abbildung haben.

Die Beantwortung der ersten beiden Fragen gelingt im Folgenden mit Hilfe von **Transformationsmatrizen** für den Basiswechsel.

Definition 19.15 (Transformationsmatrix).
Es sei V ein Vektorraum über dem Körper K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \dots, v_n)$ und $\widehat{B}_V = (\widehat{v}_1, \dots, \widehat{v}_n)$ zwei Basen von V.[37] Dann heißt

$$\mathcal{T}_{B_V \leftarrow \widehat{B}_V} := \mathcal{M}_{B_V \leftarrow \widehat{B}_V}(\mathrm{id}_V) \in K^{n \times n} \tag{19.11}$$

die **Transformationsmatrix des Basiswechsels**, **Übergangsmatrix** oder **Basiswechselmatrix von $\widehat{B}_V$ nach B_V** (englisch: transformation matrix, transition matrix, change-of-basis matrix). △

Die Transformationsmatrix $\mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ ist also nichts anderes als die Darstellung der Identitätsabbildung bzgl. der „neuen“ Basis $\widehat{B}_V$ im Definitionsraum V und der „alten“ Basis B_V im Zielraum V. Die Einträge t_{ij} der Transformationsmatrix $T := \mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ bestimmen sich daher aus den Bedingungen

$$\underbrace{\mathrm{id}_V(\widehat{v}_j) = \widehat{v}_j}_{\text{Bild des Basisvektors } \widehat{v}_j \text{ im Definitionsraum unter der identischen Abbildung}} = \sum_{i=1}^{n} t_{ij}\, v_i \quad \text{für } j = 1, \dots, n. \tag{19.12}$$

Die j-te Spalte von $T = \mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ enthält also die Koeffizienten für die Darstellung des „neuen“ Basisvektors $\widehat{v}_j$ als Linearkombination der „alten“ Basis B_V.

Das folgende Resultat beantwortet nun die Frage (1) zur Transformation von Koordinatenvektoren bei einem Basiswechsel.

Lemma 19.16 (Eigenschaften von Transformationsmatrizen).
Es sei V ein Vektorraum über dem Körper K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter seien $B_V = (v_1, \dots, v_n)$ und $\widehat{B}_V = (\widehat{v}_1, \dots, \widehat{v}_n)$ zwei Basen von V. Dann gilt:

(*i*) Ist $\widehat{x} \in K^n$ der Koordinatenvektor eines Vektors $v \in V$ bzgl. der Basis $\widehat{B}_V$, dann ist $x = \mathcal{T}_{B_V \leftarrow \widehat{B}_V} \widehat{x}$ der Koordinatenvektor von v bzgl. der Basis B_V.[38]

(*ii*) Die Transformationsmatrix $\mathcal{T}_{B_V \leftarrow \widehat{B}_V} \in K^{n \times n}$ ist invertierbar.

(*iii*) $\left(\mathcal{T}_{B_V \leftarrow \widehat{B}_V}\right)^{-1} = \mathcal{T}_{\widehat{B}_V \leftarrow B_V}$.

(*iv*) Die von der Matrix $T := \mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ induzierte lineare Abbildung $f_T \colon K^n \to K^n$ ist $f_T = \Phi_{B_V}^{-1} \circ \Phi_{\widehat{B}_V} \in \mathrm{Aut}(K^n)$.

Beweis. Wir setzen zur Abkürzung $T := \mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ wie in (19.12).

Aussage (*i*): Es gilt

$$v = \sum_{j=1}^{n} \widehat{x}_j\, \widehat{v}_j \qquad \text{nach Voraussetzung}$$

[37] Wir verwenden die Konvention, dass wir die „alte“ Basis in blau und die „neue“ Basis in rot kennzeichnen. Warum wir in Definition 19.15 die Übergangsmatrix von „neu“ nach „alt“ in den Vordergrund stellen, wird später in Satz 19.20 noch deutlich.

[38] Beachte das Muster $x = \mathcal{T}_{B_V \leftarrow \widehat{B}_V} \widehat{x}$ mit „alter“ und „neuer“ Basis und zugehörigen Koordinatenvektoren.

$$= \sum_{j=1}^{n} \widehat{x}_j \sum_{i=1}^{n} t_{ij}\, v_i \qquad \text{nach (19.12)}$$

$$= \sum_{i=1}^{n} \underbrace{\sum_{j=1}^{n} (t_{ij}\, \widehat{x}_j)}_{\text{Koeffizient } x_i \text{ bzgl. der Basis } B_V = (v_1, \ldots, v_n)} v_i \qquad \text{wegen Distributivität und Kommutativität im Körper } K.$$

Nach Definition des Matrix-Vektor-Produkts (Bemerkung 15.9) gilt also $x = \mathcal{T}_{B_V \leftarrow \widehat{B}_V} \widehat{x}$.

Aussage (ii): Die Invertierbarkeit von $\mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ folgt aus Satz 19.13, da $\mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ eine Darstellungsmatrix des bijektiven Homomorphismus $\mathrm{id}_V \colon V \to V$ ist.

Aussage (iii): Es gilt

$$\begin{aligned} \mathcal{T}_{B_V \leftarrow \widehat{B}_V} \mathcal{T}_{\widehat{B}_V \leftarrow B_V} &= \mathcal{M}_{B_V \leftarrow \widehat{B}_V}(\mathrm{id}_V) \mathcal{M}_{\widehat{B}_V \leftarrow B_V}(\mathrm{id}_V) \\ &= \mathcal{M}_{B_V \leftarrow B_V}(\mathrm{id}_V \circ \mathrm{id}_V) && \text{nach Satz 19.9} \\ &= \mathcal{M}_{B_V \leftarrow B_V}(\mathrm{id}_V) \\ &= I_n && \text{nach Beispiel 19.4.} \end{aligned}$$

Aussage (iv): Nach Satz 19.8 und wegen $T = \mathcal{T}_{B_V \leftarrow \widehat{B}_V} = \mathcal{M}_{B_V \leftarrow \widehat{B}_V}(\mathrm{id}_V)$ gilt für die durch T induzierte Abbildung $K^n \to K^n$ die Gleichung

$$f_T = \Phi_{B_V}^{-1} \circ \mathrm{id}_V \circ \Phi_{\widehat{B}_V} = \underbrace{\Phi_{B_V}^{-1}}_{\text{„alte“ Koordinaten} \mapsto \text{Vektor in } V} \circ \underbrace{\Phi_{\widehat{B}_V}}_{\text{Vektor in } V \mapsto \text{„neue“ Koordinaten}}.$$

$$\begin{array}{ccc} V & \xleftarrow{\mathrm{id}_V} & V \\ {\scriptstyle \Phi_{B_V}^{-1}}\downarrow & & \uparrow{\scriptstyle \Phi_{\widehat{B}_V}} \\ K^n & \xleftarrow[f_T]{} & K^n \end{array}$$

□

Beispiel 19.17 (Transformationsmatrix).
Auf dem Vektorraum $\mathbb{R}^{\mathbb{R}}$ der Funktionen $\mathbb{R} \to \mathbb{R}$ betrachten wir den zweidimensionalen Unterraum V der Funktionen, der von der „alten“ Basis $B_V = (t \mapsto \mathrm{e}^t,\ t \mapsto \mathrm{e}^{-t})$ aufgespannt wird. Als „neue“ Basis verwenden wir $\widehat{B}_V = (\sinh, \cosh)$. Es gilt

$$\sinh(t) = \frac{\mathrm{e}^t - \mathrm{e}^{-t}}{2} \quad \text{und} \quad \cosh(t) = \frac{\mathrm{e}^t + \mathrm{e}^{-t}}{2} \quad \text{für alle } t \in \mathbb{R}.$$

Die Transformationsmatrix $\mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ ist also gegeben durch

$$\mathcal{T}_{B_V \leftarrow \widehat{B}_V} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{matrix} \mathrm{e}^t \\ \mathrm{e}^{-t} \end{matrix} \quad \text{mit inverser Matrix} \quad \mathcal{T}_{\widehat{B}_V \leftarrow B_V} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{matrix} \sinh \\ \cosh \end{matrix}.$$

Wollen wir beispielsweise die Funktion $7 \sinh - 3 \cosh$ mit dem „neuen“ Koordinatenvektor $\widehat{x} = \left(\begin{smallmatrix} 7 \\ -3 \end{smallmatrix}\right)$ bzgl. der „alten“ Basis darstellen, dann ist der zugehörige „alte“ Koordinatenvektor gegeben durch

$$x = \mathcal{T}_{B_V \leftarrow \widehat{B}_V} \widehat{x} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{pmatrix} 7 \\ -3 \end{pmatrix} = \begin{pmatrix} 2 \\ -5 \end{pmatrix},$$

also gilt $7\,\sinh(t) - 3\,\cosh(t) = 2\,\mathrm{e}^{t} - 5\,\mathrm{e}^{-t}$. Wollen wir umgekehrt beispielsweise die Funktion $t \mapsto \mathrm{e}^{t} + 4\,\mathrm{e}^{-t}$ mit dem „alten“ Koordinatenvektor $x = \binom{1}{4}$ bzgl. der „neuen“ Basis darstellen, dann ist der zugehörige „neue“ Koordinatenvektor gegeben durch

$$\widehat{x} = \mathcal{T}_{\widehat{B}_V \leftarrow B_V} x = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} 1 \\ 4 \end{pmatrix} = \begin{pmatrix} -3 \\ 5 \end{pmatrix},$$

also gilt $\mathrm{e}^{t} + 4\,\mathrm{e}^{-t} = -3\,\sinh(t) + 5\,\cosh(t)$. △

Bemerkung 19.18 (Eigenschaften von Transformationsmatrizen in K^n).
Im Fall $V = K^n$ stimmen Vektoren mit ihren Koordinatenvektoren bzgl. der Standardbasis $(e_1, \dots, e_n)$ überein. Ist $B_V = (v_1, \dots, v_n)$ eine Basis von $V = K^n$, so hat die Transformationsmatrix $\mathcal{T}_{(e_1,\dots,e_n)\leftarrow B_V}$ die einfache Gestalt

$$\mathcal{T}_{(e_1,\dots,e_n)\leftarrow B_V} = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}.$$

Um nun den Übergang von einer Basis $\widehat{B}_V$ zu einer anderen Basis B_V zu beschreiben, können wir daher wie folgt vorgehen:

$$\begin{aligned} \mathcal{T}_{B_V \leftarrow \widehat{B}_V} &= \mathcal{T}_{B_V \leftarrow (e_1,\dots,e_n)} \mathcal{T}_{(e_1,\dots,e_n)\leftarrow \widehat{B}_V} \\ &= \big(\mathcal{T}_{(e_1,\dots,e_n)\leftarrow B_V}\big)^{-1} \mathcal{T}_{(e_1,\dots,e_n)\leftarrow \widehat{B}_V} = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}^{-1} \begin{bmatrix} | & & | \\ \widehat{v}_1 & \cdots & \widehat{v}_n \\ | & & | \end{bmatrix}. \end{aligned} \tag{19.13}$$

△

Beispiel 19.19 (Transformationsmatrizen in K^n).
Wir wollen im Raum $V = \mathbb{Q}^2$ über dem Körper $\mathbb{Q}$ die Transformationsmatrix $\mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ von der Basis $\widehat{B}_V = \big(\binom{2}{-1}, \binom{1}{-1}\big)$ zur Basis $B_V = \big(\binom{-1}{1}, \binom{1}{1}\big)$ finden. Nach (19.13) gilt

$$\mathcal{T}_{B_V \leftarrow \widehat{B}_V} = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 2 & 1 \\ -1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} -3 & -2 \\ 1 & 0 \end{bmatrix}.$$

Wir führen noch die Probe durch. Die erste Spalte der Transformationsmatrix sollte die Koeffizienten für die Darstellung des ersten „neuen“ Basisvektors $\widehat{v}_1$ als Linearkombination der „alten“ Basisvektoren enthalten:

$$\frac{-3}{2} \begin{pmatrix} -1 \\ 1 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix} = \widehat{v}_1.$$

Analog gilt für den zweiten „neuen“ Basisvektor $\widehat{v}_2$:

$$\frac{-2}{2} \begin{pmatrix} -1 \\ 1 \end{pmatrix} + \frac{0}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \widehat{v}_2.$$

△

§ 19.5 Transformation der Darstellungsmatrizen von Homomorphismen

Wir kommen nun zur Frage (2), wie sich die Darstellungsmatrix einer linearen Abbildung bei einem Wechsel einer oder beider Basen transformiert.

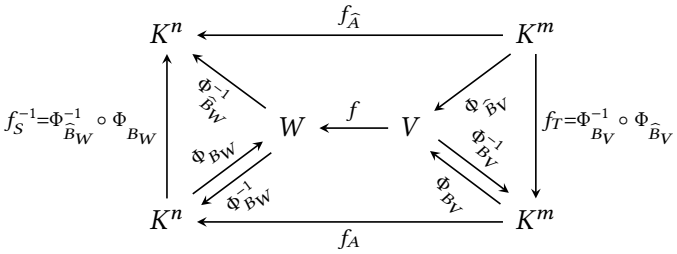
Satz 19.20 (Transformation der Darstellungsmatrix eines Homomorphismus beim Wechsel der Basen)**.**
Es seien V, W endlich-dimensionale Vektorräume über demselben Körper K. Weiter seien B_V und $\widehat{B}_V$ Basen von V sowie B_W und $\widehat{B}_W$ Basen von W. Dann gilt für die Darstellungsmatrix eines Homomorphismus $f\colon V \to W$:[39]

$$\mathcal{M}_{\widehat{B}_W \leftarrow \widehat{B}_V}(f) = \mathcal{T}_{\widehat{B}_W \leftarrow B_W}\, \mathcal{M}_{B_W \leftarrow B_V}(f)\, \mathcal{T}_{B_V \leftarrow \widehat{B}_V}. \tag{19.14}$$

Beweis. Wir setzen zur Abkürzung

$$\begin{aligned}
T &:= \mathcal{T}_{B_V \leftarrow \widehat{B}_V} && \text{Übergang von } \widehat{B}_V \text{ nach } B_V,\\
A &:= \mathcal{M}_{B_W \leftarrow B_V}(f) && \text{„alte“ Darstellungsmatrix von } f,\\
S &:= \mathcal{T}_{B_W \leftarrow \widehat{B}_W} && \text{Übergang von } \widehat{B}_W \text{ nach } B_W,\\
\text{also } S^{-1} &= \mathcal{T}_{\widehat{B}_W \leftarrow B_W} && \text{Übergang von } B_W \text{ nach } \widehat{B}_W,\\
\widehat{A} &:= \mathcal{M}_{\widehat{B}_W \leftarrow \widehat{B}_V}(f) && \text{„neue“ Darstellungsmatrix von } f.
\end{aligned}$$

Wir betrachten das Diagramm



Das obere und das untere Trapez sind kommutativ nach Satz 19.8. Das linke Dreieck und das rechte Dreieck sind kommutativ nach Lemma 19.16. Damit kommutiert auch das äußere Rechteck, d. h., es gilt

$$\begin{aligned}
f_{\widehat{A}} &= f_S^{-1} \circ f_A \circ f_T\\
&= f_{S^{-1}} \circ f_A \circ f_T && \text{nach Lemma 17.12}\\
&= f_{S^{-1}AT} && \text{nach Lemma 17.12.}
\end{aligned}$$

Aus Lemma 17.12 folgt dann auch

$$\widehat{A} = S^{-1}AT, \tag{19.15}$$

also die Behauptung (19.14). □

[39] Die Farben deuten wieder den Übergang von den „alten“ Basen zu den „neuen“ Basen an.

Beispiel 19.21 (Transformation der Darstellungsmatrix eines Homomorphismus beim Wechsel der Basen)**.**
Wir betrachten die Abbildung $f_A\colon \mathbb{R}^2 \to \mathbb{R}^3$, die durch die Matrix

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$$

induziert ist. Das heißt, A ist gleich der Darstellungsmatrix $\mathcal{M}_{(e_1,e_2,e_3)\leftarrow(e_1,e_2)}(f_A)$ bzgl. der Standardbasen in $\mathbb{R}^2$ und $\mathbb{R}^3$. Wir wollen die Darstellungsmatrix nun in die neuen Basen $\widehat{B}_V = \left(\begin{pmatrix}-1\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right)$ und $\widehat{B}_W = \left(\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}\right)$ umrechnen, also

$$\widehat{A} = \mathcal{M}_{\widehat{B}_W\leftarrow\widehat{B}_V}(f_A) = S^{-1}AT$$

bestimmen. Es gilt

$$T := \mathcal{T}_{(e_1,e_2)\leftarrow\widehat{B}_V} = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$$

und

$$S^{-1} := \mathcal{T}_{\widehat{B}_W\leftarrow(e_1,e_2,e_3)} = \left(\mathcal{T}_{(e_1,e_2,e_3)\leftarrow\widehat{B}_W}\right)^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}^{-1} = \frac{1}{2}\begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}.$$

Wir erhalten also die transfomierte Darstellungsmatrix bzgl. der neuen Basen gemäß (19.14)

$$\widehat{A} = S^{-1}AT = \frac{1}{2}\begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 7 \\ 1 & 15 \end{bmatrix}. \qquad \triangle$$

Definition 19.22 (Äquivalenztransformation, äquivalente Matrizen)**.**
Es seien K ein Körper und $n, m \in \mathbb{N}_0$. Zwei Matrizen $A, \widehat{A} \in K^{n\times m}$ heißen **äquivalent** (englisch: equivalent), wenn es invertierbare Matrizen $S \in K^{n\times n}$ und $T \in K^{m\times m}$ gibt, sodass gilt:

$$\widehat{A} = S^{-1}AT. \tag{19.16}$$

Der Übergang von A zu $S^{-1}AT$, also die Multiplikation von links und von rechts mit invertierbaren Matrizen, heißt auch eine **Äquivalenztransformation** (englisch: equivalence transformation) von A. $\triangle$

Beachte: Die Äquivalenz von Matrizen ist eine Äquivalenzrelation auf der Menge $K^{n\times m}$. Aufgrund von Folgerung 15.46 (Multiplikation mit invertierbaren Matrizen ändert den Rang nicht) besteht die Äquivalenzklasse von $A \in K^{n\times m}$ genau aus denjenigen $n\times m$-Matrizen, die denselben Rang wie A besitzen:

$$[A] = \left\{\widehat{A} \in K^{n\times m} \;\middle|\; \operatorname{Rang}(\widehat{A}) = \operatorname{Rang}(A)\right\}. \tag{19.17}$$

In der Äquivalenzklasse $[A]$ einer Matrix $A \in K^{n\times m}$ der ranggleichen Matrizen gibt es einen natürlichen Repräsentanten, der eine besonders einfache Gestalt besitzt und der die **Rang-Normalform** (englisch: rank normal form) genannt wird:

Lemma 19.23 (Rang-Normalform einer Matrix).
Es seien K ein Körper, $n, m \in \mathbb{N}_0$ und $A \in K^{n\times m}$ mit $\operatorname{Rang}(A) = r$. Dann existieren reguläre Matrizen $S \in K^{n\times n}$ und $T \in K^{m\times m}$, sodass gilt:

$$S^{-1}AT = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \in K^{n\times m}. \tag{19.18}$$

Beweis. A stimmt überein mit der Darstellungsmatrix der von A induzierten Abbildung $f_A\colon K^m \to K^n$ bzgl. der Standardbasen $B_{K^m} = (e_1, \dots, e_m)$ und $B_{K^n} = (e_1, \dots, e_n)$, siehe Beispiel 19.4, also

$$A = \mathcal{M}_{B_{K^n} \leftarrow B_{K^m}}(f_A).$$

Wählen wir jetzt weitere Basen $\widehat{B}_{K^m}$ von K^m und $\widehat{B}_{K^n}$ von K^n wie in Lemma 19.5, so gilt einerseits

$$\widehat{A} = \mathcal{M}_{\widehat{B}_{K^n} \leftarrow \widehat{B}_{K^m}}(f_A) = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \in K^{n\times m}.$$

Andererseits gilt aufgrund des Transformationssatzes 19.20

$$\widehat{A} = S^{-1}AT$$

mit den Transformationsmatrizen $T := \mathcal{T}_{B_{K^m} \leftarrow \widehat{B}_{K^m}}$ und $S := \mathcal{T}_{B_{K^n} \leftarrow \widehat{B}_{K^n}}$. □

Der folgende Satz fasst die Bedeutung äquivalenter Matrizen zusammen:

Satz 19.24 (über äquivalente Matrizen).
Es seien K ein Körper, $n, m \in \mathbb{N}_0$ und $A, \widehat{A} \in K^{n\times m}$. Dann sind äquivalent:

(*i*) A und $\widehat{A}$ sind äquivalente Matrizen.

(*ii*) Es gilt $\operatorname{Rang}(A) = \operatorname{Rang}(\widehat{A})$.

(*iii*) Sind V, W Vektorräume über K mit $\dim(V) = m$ und $\dim(W) = n$ und Basen B_V bzw. B_W, ist $f\colon V \to W$ ein Homomorphismus und gilt $A = \mathcal{M}_{B_W \leftarrow B_V}(f)$, dann gibt es Basen $\widehat{B}_V$ und $\widehat{B}_W$, sodass $\widehat{A} = \mathcal{M}_{\widehat{B}_W \leftarrow \widehat{B}_V}(f)$ gilt.

Beweis. Aussage (*i*) ⇒ Aussage (*ii*): Es sei $\widehat{A}$ äquivalent zu A, d. h., es existieren invertierbare Matrizen $S \in K^{n\times n}$ und $T \in K^{m\times m}$, sodass $\widehat{A} = S^{-1}AT$ gilt. Nach Folgerung 15.46 (Multiplikation mit invertierbaren Matrizen ändert den Rang nicht) gilt $\operatorname{Rang}(\widehat{A}) = \operatorname{Rang}(A)$.

Aussage (*ii*) ⇒ Aussage (*i*): Die Äquivalenzklassen der Äquivalenzrelation partitionieren die Menge $K^{n\times m}$. Die Matrizen A und $\widehat{A}$ gehören also zu jeweils genau einer der Äquivalenzklassen. Sie liegen aber wegen Folgerung 15.46 notwendigerweise in derselben Äquivalenzklasse.

Aussage (*i*) ⇒ Aussage (*iii*): Es sei $\widehat{A}$ äquivalent zu A, d. h., es existieren invertierbare Matrizen $S \in K^{n\times n}$ und $T \in K^{m\times m}$, sodass $\widehat{A} = S^{-1}AT$ gilt. Wir können T als Transformationsmatrix eines Basiswechsels $T = \mathcal{T}_{B_V \leftarrow \widehat{B}_V}$ auffassen, indem wir die „neue“ Basis von V durch

$$\widehat{v}_j = \sum_{i=1}^{m} t_{ij}\, v_i \quad \text{für } j = 1, \dots, m$$

definieren, vgl. (19.12). Ebenso können wir S als Transformationsmatrix eines Basiswechsels $S = \mathcal{T}_{B_W \leftarrow \widehat{B}_W}$ auffassen, indem wir die „neue“ Basis von W durch

$$\widehat{w}_j = \sum_{i=1}^{n} s_{ij}\, w_i \quad \text{für } j = 1, \dots, n$$

definieren. Wir sehen jetzt

$$\begin{aligned}
f_{\widehat{A}} &= f_{S^{-1}AT} && \text{nach Voraussetzung} \\
&= f_{S^{-1}} \circ f_A \circ f_T && \text{nach Lemma 17.12} \\
&= f_{S^{-1}} \circ \Phi_{B_W}^{-1} \circ f \circ \Phi_{B_V} \circ f_T && \text{nach Satz 19.8} \\
&= \Phi_{\widehat{B}_W}^{-1} \circ \Phi_{B_W} \circ \Phi_{B_W}^{-1} \circ f \circ \Phi_{B_V} \circ \Phi_{B_V}^{-1} \circ \Phi_{\widehat{B}_V} && \text{nach Lemma 19.16} \\
&= \Phi_{\widehat{B}_W}^{-1} \circ f \circ \Phi_{\widehat{B}_V}.
\end{aligned}$$

Das bedeutet wiederum nach Satz 19.8 aber, dass $\widehat{A}$ die Darstellungsmatrix von f bzgl. der „neuen“ Basen $\widehat{V}$ und $\widehat{W}$ ist.

Aussage $(iii) \Rightarrow$ Aussage (i): Das folgt sofort aus Satz 19.20. □

Bemerkung 19.25 (Matrizen stellen immer lineare Abbildungen dar)**.**
Matrizen stellen (immer) lineare Abbildungen zwischen Vektorräumen dar. Wir verwenden Matrizen also nicht zum „Selbstzweck“. Vielmehr sind sie ein praktisches Hilfsmittel, um lineare Abbildungen zwischen endlich-dimensionalen Vektorräumen zu untersuchen. Bisher haben wir beispielsweise den Rang, das Bild und den Kern von Abbildungen $f\colon V \to W$ mit Hilfe ihrer Darstellungsmatrizen bestimmt (Satz 19.10, Beispiel 19.12). △

Expertenwissen: über äquivalente Matrizen

Es seien K ein Körper sowie V und W zwei endlich-dimensionale Vektorräume über K mit $\dim(V) = m$ und $\dim(W) = n$ für $m, n \in \mathbb{N}_0$. Der Satz 19.24 bedeutet, dass folgendes Diagramm für jede feste Wahl von Basen B_V und B_W kommutiert:

$$\begin{array}{ccc}
\operatorname{Hom}(V,W) & \xrightarrow[\text{isomorph}]{\mathcal{M}_{B_W \leftarrow B_V}} & K^{n\times m} \\
\Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \widetilde{\pi}} \\
\operatorname{Hom}(V,W) \,/\sim_{\text{Rang}} & \xrightarrow[\mathcal{M}_{B_W \leftarrow B_V}]{\text{bijektiv}} & K^{n\times m} \,/\sim_{\text{Rang}}
\end{array}$$

Dabei ist auf der linken Seite des Diagramms $\sim_{\text{Rang}}$ die Äquivalenzrelation „gleicher Rang“ auf $\operatorname{Hom}(V,W)$ mit den Äquivalenzklassen

$$[f] := \big\{ g \in \operatorname{Hom}(V,W) \,\big|\, \operatorname{Rang}(g) = \operatorname{Rang}(f) \big\}.$$

Weiter ist $\operatorname{Hom}(V,W) / \sim_{\text{Rang}}$ die zugehörige Faktormenge (Menge aller Äquivalenzklassen) und π die kanonische Surjektion $f \mapsto [f]$. Übrigens gibt es wegen $0 \leqslant \operatorname{Rang}(f) \leqslant \min\{m,n\}$ höchstens $\min\{m,n\}+1$ dieser Äquivalenzklassen, und tatsächlich sind genau

$\min\{m, n\} + 1$ Äquivalenzklassen, da man leicht einen Homomorphismus des entsprechenden Ranges angeben kann.

Auf der rechten Seite des Diagramms steht das Symbol $\sim_{\text{Rang}}$ für die Äquivalenzrelation „gleicher Rang“ auf $K^{n,m}$ mit den Äquivalenzklassen

$$\begin{aligned}[A] &:= \left\{\widehat{A} \in K^{n\times m} \,\middle|\, \operatorname{Rang}(\widehat{A}) = \operatorname{Rang}(A)\right\} \\ &= \left\{\widehat{A} \in K^{n\times m} \,\middle|\, \widehat{A} \text{ ist äquivalent zu } A\right\} \\ &= \left\{S^{-1}AT \,\middle|\, S \in K^{n\times n} \text{ und } T \in K^{m\times m} \text{ sind invertierbar}\right\}.\end{aligned}$$

Weiter ist $K^{n\times m} / \sim_{\text{Rang}}$ die zugehörige Faktormenge und $\widetilde{\pi}$ die kanonische Surjektion $A \mapsto [A]$.

Nach Satz 19.24 bildet $\mathcal{M}_{B_W \leftarrow B_V}$ eine gesamte Äquivalenzklasse von $\operatorname{Hom}(V, W)$ auf eine Äquivalenzklasse von $K^{n\times m}$ ab und verschiedene Äquivalenzklassen von $\operatorname{Hom}(V, W)$ auf verschiedene Äquivalenzklassen von $K^{n\times n}$. Allerdings sind die Äquivalenzklassen hier (bis auf die für Rang 0) keine Unterräume; $[f] \mapsto [A]$ kann also keine lineare Zuordnung sein. Stattdessen ist jede Äquivalenzklasse $[f]$ von $\operatorname{Hom}(V, W)$ eine sogenannte **glatte Mannigfaltigkeit** (englisch: smooth manifold). Über solche Strukturen erfahren Sie mehr in Vorlesungen über Differentialgeometrie.

Ebenso ist jede Äquivalenzklasse $[A]$ von $K^{n\times m}$ eine glatte Mannigfaltigkeit, und die Abbildung $\mathcal{M}_{B_W \leftarrow B_V}$ ist ein **Diffeomorphismus** zwischen $[f]$ und $[A]$ mit $\operatorname{Rang}(f) = \operatorname{Rang}(A)$. Ein Diffeomorphismus ist eine (beliebig oft) differenzierbare Abbildung (hier: zwischen glatten Mannigfaltigkeiten), deren inverse Abbildung ebenfalls (beliebig oft) differenzierbar ist.

Ende der Vorlesung 27

Ende der Woche 13

Kapitel A Zur Konstruktion der Zahlen

Literatur: Goldrei, 1996, Chapters 2–3

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 $2x = 1$ 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 $\mathbb{C}$. Wir deuten in diesem Abschnitt kurz an, wie die die Zahlbereiche (4.1) von den natürlichen bis zu den komplexen Zahlen mitsamt ihren Verknüpfungen Addition und Multiplikation mathematisch fundiert konstruiert werden können.

Die natürlichen Zahlen

Die **natürlichen Zahlen** (englisch: natural numbers) können auf verschiedene Arten konstruiert werden, beispielsweise — unabhängig von den Axiomen der Zermelo-Fraenkel-Mengenlehre — mit Hilfe der Peano-Axiome. Alternativ können wir die natürlichen Zahlen $\mathbb{N}_0$ aber auch innerhalb der Zermelo-Fraenkel-Mengenlehre abbilden. Von Neumann setzt dazu

$$\begin{aligned} 0 &:= \emptyset \\ 1 &:= 0 \cup \{0\} = \{\emptyset\} \\ 2 &:= 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &:= 2 \cup \{2\} = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

usw. Gleichzeitig mit diesen „Zahlen“ wird die Funktion **Nachfolger** (englisch: successor) $S(n) := n \cup \{n\}$ definiert. Die Menge $\mathbb{N}_0$ ist dann der Durchschnitt aller Mengen, die die 0 (also $\emptyset$) enthalten und die die Eigenschaft haben, dass sie ihr Bild unter der Nachfolgerfunktion enthalten:

$$\mathbb{N}_0 := \bigcap \{M \text{ ist Menge} \mid \emptyset \in M \text{ und } S(M) \subseteq M\}.$$

Da jede natürliche Zahl in $\mathbb{N}_0$ entweder gleich 0 oder der Nachfolger einer natürlichen Zahl ist, kann die **Addition** (englisch: addition) rekursiv durch

$$\begin{aligned} m + 0 &:= m && \text{für } m \in \mathbb{N}_0 \\ m + S(n) &:= S(m + n) && \text{für } m, n \in \mathbb{N}_0 \end{aligned}$$

definiert werden. Es kann gezeigt werden, dass die Addition eine assioziative, kommutative Verknüpfung auf $\mathbb{N}_0$ mit neutralem Element 0 ist. Also ist $(\mathbb{N}_0, +)$ ein kommutatives Monoid. Beispielsweise gilt

$$\begin{aligned}
5+2 &= 5+S(1) = S(5+1) = S(5+S(0)) = S(S(5+0)) = S(S(5)) = S(6) = 7\\
2+5 &= 2+S(4) = S(2+4) = S(2+S(3)) = S(S(2+3)) = S(S(2+S(2))) = S(S(S(2+2)))\\
&= S(S(S(2+S(1)))) = S(S(S(S(2+1)))) = S(S(S(S(2+S(0))))) = S(S(S(S(2+0)))))\\
&= S(S(S(S(2))))) = S(S(S(S(3)))) = S(S(S(4))) = S(S(5)) = S(6) = 7.
\end{aligned}$$

Aufbauend auf der Addition kann dann die **Multiplikation** (englisch: multiplication) rekursiv durch

$$\begin{aligned}
m \cdot 0 &:= 0 && \text{für } m \in \mathbb{N}_0\\
m \cdot S(n) &:= (m \cdot n) + m && \text{für } m, n \in \mathbb{N}_0
\end{aligned}$$

definiert werden. Auch für die Multiplikation kann gezeigt werden, dass sie eine assioziative, kommutative Verknüpfung auf $\mathbb{N}_0$ ist, und zwar mit dem neutralen Element 1. Also ist auch $(\mathbb{N}_0, \cdot)$ ein kommutatives Monoid.

Nun kann noch das Distributivgesetz $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ für alle $a, b, c \in \mathbb{N}_0$ bestätigt werden.

Mit Hilfe der Addition kann die natürliche Totalordnung $\leqslant$ auf $\mathbb{N}_0$ definiert werden, und zwar durch

$$a \leqslant b \quad \Leftrightarrow \quad \exists n \in \mathbb{N}_0\, (b = a + n).$$

Für alle $b \in \mathbb{N}_0$ gilt $b \geqslant 0$. Wie leicht zu sehen ist, ist diese Ordnung kompatibel mit der Addition und Multiplikation, es gilt also $a \leqslant b \Rightarrow a+c \leqslant b+c$ und $a \leqslant b \Rightarrow a \cdot c \leqslant b \cdot c$ für alle $c \in \mathbb{N}_0$.

Durch Entfernen der 0 aus der Menge $\mathbb{N}_0$ erhalten wir die kommutative Halbgruppe $(\mathbb{N}, +)$ bzw. das kommutative Monoid $(\mathbb{N}, \cdot)$.

Die ganzen Zahlen

Die **ganzen Zahlen** (englisch: integer numbers) können wir aus den natürlichen Zahlen $\mathbb{N}_0$ konstruieren, beispielsweise durch

$$\widetilde{\mathbb{Z}} := \mathbb{N}_0 \times \mathbb{N}_0 \,/\sim$$

bzgl. der Äquivalenzrelation

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a + d = b + c$$

auf $\mathbb{N}_0 \times \mathbb{N}_0$. Wir führen auf $\widetilde{\mathbb{Z}}$ durch

$$[(a, b)] + [(c, d)] := [(a + c, b + d)]$$

die **Addition** ein. Für diese kann gezeigt werden, dass sie wohldefiniert, assoziativ und kommutativ ist und das neutrale Element $[(0,0)]$ besitzt. Damit ist $(\widetilde{\mathbb{Z}},+)$ ein kommutatives Monoid. Tatsächlich ist $(\widetilde{\mathbb{Z}},+)$ sogar eine abelsche Gruppe, denn $[(b,a)]$ ist wegen

$$[(a,b)]+[(b,a)]=[(a+b,b+a)]=[(a+b,a+b)]=[(0,0)]$$

das additive Inverse zu $[(a,b)]$.

Jede Äquivalenzklasse $[(a,b)]$ enthält entweder genau ein Element der Form $(c,0)$ mit $c\in\mathbb{N}$ oder genau ein Element der Form $(0,d)$ mit $d\in\mathbb{N}$ oder das Element $(0,0)$. Im ersten Fall bezeichnen wir die Äquivalenzklasse $[(c,0)]$ kurz mit c. Im zweiten Fall bezeichnen wir die Äquivalenzklasse $[(0,d)]$ kurz mit $-d$. Im dritten Fall bezeichnen wir die Äquivalenzklasse $[(0,0)]$ kurz mit 0. Durch diese bijektive Abbildung $\varphi\colon\widetilde{\mathbb{Z}}\to\mathbb{Z}:=\{0,1,-1,2,-2,\dots\}$ können wir auf der Repräsentantenmenge $\mathbb{Z}$ die Addition erklären, sodass $(\mathbb{Z},+)$ eine abelsche Gruppe mit dem neutralen Element 0 wird. Diese ist isomorph zu $\widetilde{\mathbb{Z}}$. Beispielsweise gilt

$$\begin{aligned}2+3&=[(2,0)]+[(3,0)]=[(5,0)]=5\\2+(-3)&=[(2,0)]+[(0,3)]=[(2,3)]=[(0,1)]=-1\\2-(-3)&=[(2,0)]-[(0,3)]=[(2,0)]+[(3,0)]=[(5,0)]=5.\end{aligned}$$

Die zuvor definierte Addition in $\mathbb{N}_0$ stimmt dann mit der Addition in $\mathbb{Z}$, eingeschränkt auf $\mathbb{N}_0$, überein. Formal wird das Monoid $(\mathbb{N}_0,+)$ mit Hilfe des injektiven Monoidhomomorphismus $\mathbb{N}_0\ni a\mapsto a\ni\mathbb{Z}$ in die Gruppe $(\mathbb{Z},+)$ eingebettet. So werden die natürlichen Zahlen zu einer Teilmenge der ganzen Zahlen und die Addition auf $\mathbb{Z}$ zu einer Fortsetzung der Addition auf $\mathbb{N}_0$.

Die **Multiplikation** kann nun ebenfalls zunächst wieder auf $\widetilde{\mathbb{Z}}$ definiert werden, und zwar (mit Hilfe der Addition und Multiplikation in $\mathbb{N}_0$) durch

$$[(a,b)]\cdot[(c,d)]:=[(a\cdot c+b\cdot d,a\cdot d+b\cdot c)].$$

Auch hier kann die Wohldefiniertheit, Assoziativität und Kommutativität gezeigt werden. Das neutrale Element ist $[(1,0)]$. Anschließend können wir wieder mit Hilfe der Bijektion $\varphi\colon\widetilde{\mathbb{Z}}\to\mathbb{Z}$ die Multiplikation auf $\mathbb{Z}$ erklären. Alternativ können wir die Multiplikation auch direkt nur auf $\mathbb{Z}$ definieren, indem wir für $a\cdot b$ eine Fallunterscheidung nach dem Vorzeichen von a und b vornehmen. (Damit ist die Fallunterscheidung $a\geqslant 0$ oder $a\leqslant 0$ bzw. $b\geqslant 0$ oder $b\leqslant 0$ bzgl. der gleich erläuterten Ordnung auf $\mathbb{Z}$ gemeint.) In jedem Fall ergibt sich, dass $(\mathbb{Z},\cdot)$ eine kommutative Halbgruppe mit neutralem Element 1 ist und dass $(\mathbb{N}_0,\cdot)$ in $(\mathbb{Z},\cdot)$ eingebettet ist.

Abschließend kann noch das Distributivgesetz $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ gezeigt werden, wodurch $(\mathbb{Z},+,\cdot)$ zu einem kommutativen Ring (Definition 9.1) mit dem Einselement 1 wird.

Die natürliche Totalordnung $\leqslant$ auf $\mathbb{N}_0$ kann auf $\mathbb{Z}$ fortgesetzt werden, und zwar wiederum durch

$$a\leqslant b\quad\Leftrightarrow\quad\exists n\in\mathbb{N}_0\,(b=a+n).$$

Es gilt $a\leqslant b\Rightarrow a+c\leqslant b+c$ für alle $c\in\mathbb{Z}$ sowie $a\leqslant b\Rightarrow a\cdot c\leqslant b\cdot c$ für alle $c\in\mathbb{N}_0$ und $a\leqslant b\Rightarrow a\cdot c\geqslant b\cdot c$ für alle $c\in-\mathbb{N}_0$.

Der **Betrag** $|a|$ einer ganzen Zahl a ist definiert als

$$|a|:=\begin{cases}a & \text{falls } a\geqslant 0,\\ -a & \text{falls } a<0.\end{cases}$$

Die rationalen Zahlen

Die **rationalen Zahlen** (englisch: rational numbers) können wir aus den ganzen Zahlen $\mathbb{Z}$ konstruieren durch

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$$

mit der Äquivalenzrelation

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a \cdot d = c \cdot b$$

auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Auf $\mathbb{Q}$ führen wir durch

$$[(a, b)] + [(c, d)] := [(a \cdot d + b \cdot c, b \cdot d)]$$

die **Addition** ein. Für diese kann gezeigt werden, dass sie wohldefiniert, assoziativ und kommutativ ist und das neutrale Element $[(0, 1)]$ besitzt. Damit ist $(\mathbb{Q}, +)$ ein kommutatives Monoid. Tatsächlich ist $(\mathbb{Q}, +)$ sogar eine abelsche Gruppe, denn $[(-a, b)]$ ist wegen

$$[(a, b)] + [(-a, b)] = [(a \cdot b + b \cdot (-a), b \cdot b)] = [(0, b \cdot b)] = [(0, 1)]$$

das additive Inverse zu $[(a, b)]$. Auch hier gilt, dass $\mathbb{Z}$ durch $a \mapsto [(a, 1)]$ in $\mathbb{Q}$ eingebettet ist und dass die Addition auf $\mathbb{Q}$, eingeschränkt auf $\mathbb{Z} \times \{1\}$, mit der Addition auf $\mathbb{Z}$ übereinstimmt.

Die **Multiplikation** auf $\mathbb{Q}$ wird definiert durch

$$[(a, b)] \cdot [(c, d)] := [(a \cdot c, b \cdot d)].$$

Auch diese ist wohldefiniert, assoziativ und kommutativ mit neutralem Element $[(1, 1)]$. Damit ist $(\mathbb{Q}, \cdot)$ ein kommutatives Monoid. Tatsächlich ist $(\mathbb{Q} \setminus \{[(0, 1)]\}, \cdot)$ sogar eine abelsche Gruppe, denn $[(b, a)]$ ist wegen

$$[(a, b)] \cdot [(b, a)] = [(a \cdot b, b \cdot a)] = [(a \cdot b, a \cdot b)] = [(1, 1)]$$

das multiplikative Inverse zu $[(a, b)]$. Insbesondere ist $[(1, a)]$ das multiplikative Inverse zu $[(a, 1)]$ für alle $a \in \mathbb{Z} \setminus \{0\}$. Auch hier wird durch $a \mapsto [(a, 1)]$ die Menge $\mathbb{Z}$ in $\mathbb{Q}$ eingebettet und die Multiplikation auf $\mathbb{Q}$, eingeschränkt auf $\mathbb{Z} \times \{1\}$, stimmt mit der Multiplikation auf $\mathbb{Z}$ überein.

Weiterhin kann das Distributivgesetz gezeigt werden, wodurch $(\mathbb{Q}, +, \cdot)$ zu einem Körper wird (Definition 10.1). Es ist üblich, die Äquivalenzklasse $[(a, b)]$ in der Gestalt eines „Bruches“ $\frac{a}{b}$ zu notieren, vgl. (5.18). Durch „Kürzen“ und „Erweitern“ können wir jederzeit den Repräsentanten einer Äquivalenzklasse wechseln. Insbesondere kann ein Bruch immer in der Form $\frac{a}{b}$ mit „Zähler“ $a \in \mathbb{Z}$ und „Nenner“ $b \in \mathbb{N}$ dargestellt werden.

Die natürliche Totalordnung $\leqslant$ auf $\mathbb{Z}$ kann auf $\mathbb{Q}$ fortgesetzt werden, und zwar für die Darstellungen mit $b, d \in \mathbb{N}$ durch

$$\frac{a}{b} \leqslant \frac{c}{d} \quad \Leftrightarrow \quad a \cdot d \leqslant c \cdot b \quad \text{(im Sinne der Totalordnung } \leqslant \text{ auf } \mathbb{Z}).$$

Es gilt $a \leqslant b \Rightarrow a + c \leqslant b + c$ für alle $c \in \mathbb{Q}$ sowie $a \geqslant 0,\ b \geqslant 0 \Rightarrow a \cdot b \geqslant 0$. Damit wird $(\mathbb{Q}, +, \cdot)$ zu einem geordneten Körper (Definition 10.19).

Der **Betrag** $\left|\frac{a}{b}\right|$ einer rationalen Zahl $\frac{a}{b}$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{Z} \setminus \{0\}$ ist definiert als

$$\left|\frac{a}{b}\right| := \begin{cases} \frac{a}{b} & \text{falls } \frac{a}{b} \geqslant 0, \\ -\frac{a}{b} & \text{falls } \frac{a}{b} < 0. \end{cases}$$

Die reellen Zahlen

Es gibt verschiedene Möglichkeiten, die **reellen Zahlen** (englisch: real numbers) aus den rationalen Zahlen $\mathbb{Q}$ zu konstruieren. Wir skizzieren hier die Konstruktion über Dedekindsche Schnitte. Ein **Dedekindscher Schnitt** (englisch: Dedekind cut) ist ein Paar (A, B) von Mengen $A, B \subseteq \mathbb{Q}$ mit den folgenden Eigenschaften:

(1) $\{A, B\}$ bildet eine Partition von $\mathbb{Q}$,

(2) $y \in A$ und $x \in \mathbb{Q}$, $x \leqslant y$ impliziert $x \in A$,
(A ist nach unten abgeschlossen.)

(3) für alle $x \in A$ existiert $y \in A$ mit $y > x$.
(A besitzt kein Maximum.)

Da A und B eine Partition von $\mathbb{Q}$ bilden, kann Eigenschaft (2) auch in der Form $a < b$ für alle $a \in A$ und alle $b \in B$ ausgedrückt werden. (**Quizfrage A.1:** Klar?)

Wir definieren nun die reellen Zahlen als

$$\mathbb{R} := \{A \subseteq \mathbb{Q} \mid (A, B) \text{ ist ein Dedekindscher Schnitt}\}.$$

Mit anderen Worten bestehen die reellen Zahlen also gerade aus den sogenannten **linken Abschnitten** A (englisch: Dedekind left sets) der Dedekindschen Schnitte (A, B).

Auf $\mathbb{R}$ führen wir durch

$$A_1 + A_2 := \{a_1 + a_2 \mid a_1 \in A_1,\ a_2 \in A_2\}$$

die **Addition** ein. Für diese kann gezeigt werden, dass sie wohldefiniert, assoziativ und kommutativ ist und das neutrale Element $\mathbb{Q}_{<0} := \{x \in \mathbb{Q} \mid x < 0\}$ („Null“) besitzt. Damit ist $(\mathbb{R}, +)$ ein kommutatives Monoid. Tatsächlich ist $(\mathbb{R}, +)$ sogar eine abelsche Gruppe, denn es kann gezeigt werden, dass

$$\begin{aligned} -A &= \mathbb{Q}_{<0} - (\mathbb{Q} \setminus A) \\ &= \{x - b \mid x \in \mathbb{Q}_{<0} \text{ und } b \in \mathbb{Q} \setminus A\} \\ &= \{y \in \mathbb{Q} \mid \exists b \in \mathbb{Q} \setminus A\,(y < -b)\} \end{aligned}$$

das additive Inverse zu A ist.

Bevor die Multiplikation auf $\mathbb{R}$ eingeführt werden kann, definieren wir die Ordnungsrelation $A_1 \leqslant A_2$ durch $A_1 \subseteq A_2$. Dadurch wird $\mathbb{R}$ zu einer totalgeordneten Menge. Ein Element $A \in \mathbb{R}$ heißt **negativ** (englisch: negative) im Fall $A \subsetneq \mathbb{Q}_{<0}$, **nicht-positiv** (englisch: non-positive) im Fall $A \subseteq \mathbb{Q}_{<0}$, **positiv** (englisch: positive) im Fall $\mathbb{Q}_{<0} \subsetneq A$ und **nicht-negativ** (englisch: non-negative) im Fall $\mathbb{Q}_{<0} \subseteq A$.

Die **Multiplikation** auf $\mathbb{R}$ wird nun fallweise definiert. Wenn A_1 und A_2 beide positiv sind, dann setzen wir

$$A_1 \cdot A_2 := \{a_1 \cdot a_2 \mid a_1 \geqslant 0,\ a_2 \geqslant 0,\ a_1 \in A_1,\ a_2 \in A_2\} \cup \mathbb{Q}_{<0}.$$

Ist A_1 negativ und A_2 positiv, dann setzen wir $A_1 \cdot A_2 := -((-A_1) \cdot A_2)$. Ist A_1 positiv und A_2 negativ, dann setzen wir $A_1 \cdot A_2 := -(A_1 \cdot (-A_2))$. Sind A_1 und A_2 beide negativ, dann setzen

wir $A_1 \cdot A_2 \coloneqq ((-A_1) \cdot (-A_2))$. Ist schließlich mindestens einer der beiden linken Abschnitte A_1 oder A_2 gleich $\mathbb{Q}_{<0}$ („Null“), dann setzen wir $A_1 \cdot A_2 \coloneqq \mathbb{Q}_{<0}$. Auch für die Multiplikation kann gezeigt werden, dass sie wohldefiniert, assoziativ und kommutativ ist und das neutrale Element $\{x \in \mathbb{Q} \mid x < 1\}$ besitzt. Damit ist $(\mathbb{R}, \cdot)$ ein kommutatives Monoid. Tatsächlich ist $(\mathbb{R} \setminus \mathbb{Q}_{<0}, \cdot)$ sogar eine abelsche Gruppe.

Weiterhin kann das Distributivgesetz gezeigt werden, wodurch $(\mathbb{R}, +, \cdot)$ zu einem Körper wird (Definition 10.1). Außerdem ist die oben definerte Totalordnung $\leqslant$ auf $\mathbb{R}$ kompatibel mit der Addition und Multiplikation, es gilt also $A_1 \leqslant A_2 \Rightarrow A_1 + A_3 \leqslant A_2 + A_3$ für alle $A_3 \in \mathbb{R}$, und für alle nicht-negativen A_1, A_2 ist auch $A_1 \cdot A_2$ nicht-negativ. Damit wird $(\mathbb{R}, +, \cdot)$ zu einem geordneten Körper (Definition 10.19).

Ist $\mathcal{A}$ eine nach oben beschränkte Teilmenge[1] von $\mathbb{R}$, so besitzt $\mathcal{A}$ ein Supremum in $\mathbb{R}$, und zwar $\sup \mathcal{A} = \bigcup_{A \in \mathcal{A}} A$. Ist $\mathcal{A}$ eine nach unten beschränkte Teilmenge von $\mathbb{R}$, so besitzt $\mathcal{A}$ ein Infimum in $\mathbb{R}$, und zwar $\inf \mathcal{A} = \bigcap_{A \in \mathcal{A}} A$. Die Existenz dieser Suprema und Infima ist der entscheidende Unterschied zwischen den rationalen und den reellen Zahlen.

Eine rationale Zahl $q \in \mathbb{Q}$ wird mit dem linken Abschnitt $A_q \coloneqq \{x \in \mathbb{Q} \mid x < q\}$ identifiziert. Man kann zeigen, dass diese Abbildung $q \mapsto A_q$ und verträglich mit der Addition und Multiplikation auf $\mathbb{Q}$ und $\mathbb{R}$ ist. Mit anderen Worten: Diese Abbildung ist ein Körperhomomorphismus von $(\mathbb{Q}, +, \cdot)$ nach $(\mathbb{R}, +, \cdot)$, durch den $\mathbb{Q}$ in $\mathbb{R}$ eingebettet wird. Dabei können wir ausnutzen, dass Körperhomomorphismen stets injektiv sind (Lemma 10.14).

Neben allen Elementen von $\mathbb{Q}$ besitzen auch bestimmte andere linke Abschnitte Kurzbezeichnungen, wie beispielsweise $\sqrt{2} \coloneqq \{x \in \mathbb{Q} \mid x \cdot x < 2 \text{ oder } x < 0\}$. Linke Abschnitte, die nicht von der Form $\{x \in \mathbb{Q} \mid x < q\}$ für $q \in \mathbb{Q}$ sind, heißen **irrationale Zahlen** (englisch: irrational numbers). Beispiele für (benannte) irrationale Zahlen sind $\sqrt{2}$, die Eulersche Zahl e und die Kreiszahl π.

An dieser Stelle halten wir einmal fest, dass die reellen Zahlen überlicherweise abstrakt als ein geordneter Körper mit der zusätzlichen Eigenschaft definiert werden, dass jede nach oben beschränkte Teilmenge ein Supremum besitzt. Letztere Eigenschaft nennt man auch die **Ordnungsvollständigkeit** (englisch: order completeness). Man kann dann zeigen, dass ein solcher Körper bis auf Isomorphie eindeutig ist. Insofern stellt die oben skizzierte Konstruktion der reellen Zahlen über Dedekindsche Schnitte ein mögliches Modell für die reellen Zahlen dar. Insbesondere zeigt es, dass eine algebraische Struktur mit den genannten Eigenschaften überhaupt existiert. In der Praxis arbeiten wir aber nur mit den abstrakten Eigenschaften des geordneten Körpers $\mathbb{R}$.

Die Ordnungsvollständigkeit der reellen Zahlen sorgt übrigens dafür, dass eine Wiederholung der Konstruktion durch Schnitte in $\mathbb{R}$, also $\{A \subseteq \mathbb{R} \mid (A, B) \text{ ist ein Dedekindscher Schnitt}\}$ wiederum auf einen Körper führt, der isomorph zu $\mathbb{R}$ ist.

Der **Betrag** $|a|$ einer reellen Zahl a ist definiert als

$$|a| \coloneqq \begin{cases} a & \text{falls } a \geqslant 0, \\ -a & \text{falls } a < 0. \end{cases}$$

[1] $\mathcal{A}$ ist also eine Menge linker Abschnitte, und es gibt einen linken Abschnitt A_0, sodass $A \subseteq A_0$ für alle $A \in \mathcal{A}$ gilt.

Schließlich können wir für $n \in \mathbb{N}$ die n-te Wurzel nicht-negativer reeller Zahlen $a \geqslant 0$ definieren:

$$\sqrt[n]{a} \coloneqq \{x \in \mathbb{Q} \mid \underbrace{x \cdot x \cdots x}_{n\text{-faches Produkt}} < a \text{ oder } x < 0\}.$$

Die **Exponentialfunktion** (englisch: exponential function)

$$\mathbb{R} \ni x \mapsto a^x \in \mathbb{R}_{>0}$$

zur Basis $a \in \mathbb{R}$, $a > 0$ können wir definieren, indem wir zunächst für rationale Exponenten $x = \frac{m}{n} \in \mathbb{Q}$ mit $m \in \mathbb{Z}$ und $n \in \mathbb{N}$

$$a^{\frac{m}{n}} \coloneqq \sqrt[n]{a^m} \in \mathbb{R}$$

und anschließend für beliebiges $x \in \mathbb{R}$

$$a^x \coloneqq \sup\left\{a^q \in \mathbb{R} \,\middle|\, q \in \mathbb{Q},\ q < x\right\}$$

setzen. Mit Mitteln der Analysis kann gezeigt werden, dass die Exponentialabbildung im Fall $a \neq 1$ bijektiv $\mathbb{R} \to \mathbb{R}_{>0}$ abbildet. Ihre Umkehrabbildung ist die **Logarithmusfunktion** (englisch: logarithm function) zur Basis a, notiert als $\log_a \colon \mathbb{R}_{>0} \to \mathbb{R}$. Häufig wird als Basis die **Eulersche Zahl** (englisch: Euler's number) verwendet, die als

$$\mathrm{e} \coloneqq \sup\left\{\left(1 + \frac{1}{n}\right)^n \,\middle|\, n \in \mathbb{N}\right\}$$

definiert werden kann. Die Exponentialfunktion $\mathbb{R} \ni x \mapsto \mathrm{e}^x \in \mathbb{R}_{>0}$ heißt auch die **natürliche Exponentialfunktion** (englisch: natural exponential function) und wird als exp notiert. Wir setzen also $\exp(x) \coloneqq \mathrm{e}^x$.

Die Definition trigonometrischer Funktionen wie der sin- und cos-Funktion erfolgt üblicherweise über Potenzreihen und wird ebenfalls in Lehrveranstaltungen zur *Analysis* behandelt.

Die komplexen Zahlen

Die **komplexen Zahlen** (englisch: complex numbers) können wir aus den rellen Zahlen $\mathbb{R}$ konstruieren durch

$$\mathbb{C} \coloneqq \mathbb{R} \times \mathbb{R}.$$

Auf $\mathbb{C}$ führen wir durch

$$(a, b) + (c, d) \coloneqq (a + c, b + d)$$

die **Addition** ein. Damit erbt $(\mathbb{C}, +)$ die Eigenschaften von $(\mathbb{R}, +)$ als Abelsche Gruppe und besitzt das neutrale Element $(0, 0)$.[2] Das zu (a, b) additive Inverse ist $(-a, -b)$.

Weiterhin führen wir durch

$$(a, b) \cdot (c, d) \coloneqq (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$$

[2] Diese Konstruktion heißt das **(äußere) direkte Produkt** (englisch: (outer) direct product) der Gruppe $(\mathbb{R}, +)$ mit sich selbst.

die **Multiplikation** auf $\mathbb{C}$ ein. Auch diese ist assoziativ und kommutativ mit neutralem Element $(1,0)$. Damit ist $(\mathbb{C},\cdot)$ ein kommutatives Monoid. Tatsächlich ist $(\mathbb{C}\setminus\{(0,0)\},\cdot)$ sogar eine abelsche Gruppe, denn $\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$ ist wegen $a^2+b^2>0$ und

$$(a,b)\cdot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=\left(\frac{a^2+b^2}{a^2+b^2},\frac{a\cdot(-b)+b\cdot a}{a^2+b^2}\right)=(1,0)$$

das multiplikative Inverse zu (a,b).

Weiterhin kann das Distributivgesetz gezeigt werden, wodurch $(\mathbb{C},+,\cdot)$ zu einem Körper wird (Definition 10.1). Es lässt sich jedoch keine Totalordnung auf $\mathbb{C}$ definieren, durch die $(\mathbb{C},+,\cdot)$ zu einem geordneten Körper wird.

Durch den Körperhomomorphismus $a\mapsto(a,0)$ in $(\mathbb{C},+,\cdot)$ wird der Körper $(\mathbb{R},+,\cdot)$ eingebettet.

Es ist üblich, das Element $(a,b)\in\mathbb{C}$ als $a+b\,i$ zu notieren, wobei $i:=(0,1)$ ist und die **imaginäre Einheit** (englisch: imaginary unit) genannt wird. In dieser Darstellung heißt $a=:\mathrm{Re}(z)\in\mathbb{R}$ der **Realteil** (englisch: real part) und $b=:\mathrm{Im}(z)\in\mathbb{R}$ der **Imaginärteil** (englisch: imaginary part). Weiter gilt für die Addition

$$(a+b\,i)+(c+d\,i):=(a+c)+(b+d)\,i$$

und für die Multiplikation

$$(a+b\,i)\cdot(c+d\,i):=(a\cdot c-b\cdot d)+(a\cdot d+b\cdot c)\,i.$$

Formal rechnen wir wie in den reellen Zahlen mit dem zusätzlichen Symbol i, für das $i^2=-1$ gilt.

Die Abbildung der **komplexen Konjugation** (englisch: complex conjugation

$$\mathbb{C}\ni z=a+b\,i\mapsto\overline{z}=a-b\,i\in\mathbb{C}$$

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).

Mit Hilfe der komplexen Konjugation können wir auch nochmals das multiplikative Inverse von $z=a+b\,i$ bestätigen:

$$\frac{1}{a+b\,i}=\frac{1}{a+b\,i}\cdot\frac{a-b\,i}{a-b\,i}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}\,i.$$

Es gilt weiterhin

$$\frac{z+\overline{z}}{2}=\frac{a+b\,i+a-b\,i}{2}=a=\mathrm{Re}(z),$$
$$\frac{z-\overline{z}}{2\,i}=\frac{a+b\,i-a+b\,i}{2\,i}=b=\mathrm{Im}(z).$$

Das Produkt $z \cdot \overline{z}$ einer komplexen Zahl $z = a + b\,i$ mit ihrer konjugiert komplexen Zahl ergibt

$$z \cdot \overline{z} = (a + b\,i) \cdot (a - b\,i) = a^2 + b^2 \in \mathbb{R}.$$

Der **Betrag** $|z|$ einer komplexen Zahl $z = a + b\,i$ ist definiert als

$$|z| := \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}.$$

Für die Beträge von $w, z \in \mathbb{C}$ gilt

$$|w \cdot z| = |w| \cdot |z|.$$

Die Exponentialfunktion $\mathbb{R} \ni x \mapsto \exp(x) \in \mathbb{R}_{>0}$ besitzt eine natürliche Fortsetzung auf die komplexen Zahlen. Ist $z = a + b\,i$ die Darstellung der komplexen Zahl z mit $a = \mathrm{Re}(z)$ und $b = \mathrm{Im}(z)$, so ist diese Fortsetzung gegeben durch

$$\mathbb{C} \ni z = a + b\,i \mapsto \exp(a + b\,i) := \underbrace{\exp(a)}_{\in \mathbb{R}_{>0}} \cdot \underbrace{(\cos(b) + i \cdot \sin(b))}_{\in \mathbb{C}}.$$

Insbesondere gilt die **Eulersche Formel** (englisch: Euler's formula)

$$\exp(ix) = \cos(x) + i \cdot \sin(x) \quad \text{für } x \in \mathbb{R},$$

deren Spezialfall $\exp(i\pi) = -1$ als **Eulersche Identität** (englisch: Euler's identity) bekannt ist.

Jede komplexe Zahl besitzt eine **Polardarstellung** (englisch: polar form) der Form

$$z = r \cdot (\cos(\varphi) + i \cdot \sin(\varphi)) = r \cdot \exp(i\varphi)$$

mit $r = |z| \in \mathbb{R}_{\geqslant 0}$ und einem Winkel $\varphi \in \mathbb{R}$, der auch das **Argument** (englisch: argument) von z genannt wird. Im Fall $r > 0$ ist das Argument bis auf ganzzahlige Vielfache von $2\,\pi$ eindeutig bestimmt.

Kapitel B Liste algebraischer Strukturen

In der folgenden Tabelle ist X irgendeine Menge. Die Abkürzungen „komm.“ und „neut. E.“ stehen für „kommutativ“ und „neutrales Element“. Bei Ringen und Körpern 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.	neut. E.	Referenz
Halbgruppen und Monoide ($m \in \mathbb{N}$)				
$(\mathbb{N}, +)$		✓	–	Beispiele 7.2, 7.4, 7.8, 7.17, 7.22
$(\mathbb{N}_0, +)$		✓	0	und 7.29
$(\mathbb{N}, \cdot)$		✓	1	
$(\mathbb{N}_0, \cdot)$		✓	1	
$(\mathbb{Z}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.17, 7.22
$(\mathbb{Q}, \cdot)$		✓	1	und 7.29
$(\mathbb{R}, \cdot)$		✓	1	
$(\mathbb{C}, \cdot)$		✓	1	
$(\mathbb{Z}_m, \cdot_m)$	multiplikatives Monoid $\mathbb{Z}$ modulo m	✓	1	Beispiele 7.17 und 7.22
$(H^X, +)$	Funktionen $X \to H$ in die Halbgruppe $(H, +)$	wie in $(H, +)$		
$(\mathbb{N}^X, +)$		✓	–	Beispiele 7.2, 7.4, 7.8 und 7.24
$(\mathbb{N}_0^X, +)$		✓	$x \mapsto 0$	
$(H^X, \cdot)$	Funktionen $X \to H$ in die Halbgruppe $(H, \cdot)$	wie in $(H, \cdot)$		
$(\mathbb{N}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{N}_0^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{Z}^X, \cdot)$		✓	$x \mapsto 1$	Beispiele 7.2, 7.4, 7.8 und 7.24
$(\mathbb{Q}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{R}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{C}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathcal{P}(X), \cap)$	Potenzmenge einer Menge X	✓	X	
$(\mathcal{P}(X), \cup)$		✓	$\emptyset$	Beispiele 7.4, 7.8 und 7.12
$(\mathcal{P}(X), \triangle)$		✓	$\emptyset$	
$(X^X, \circ)$		–	id_X	Beispiele 7.2, 7.4, 7.17, 7.22 und 7.24
$(\Sigma^*, \circ)$		–	$()$	Beispiele 7.4 und 7.8

Symbol	Beschreibung	komm.	neut. E.	Referenz
Gruppen	($m \in \mathbb{N}$)			
$(\mathbb{Z}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8, 7.17, 7.22 und 7.29
$(\mathbb{Q}, +)$		✓	0	
$(\mathbb{R}, +)$		✓	0	
$(\mathbb{C}, +)$		✓	0	
$(\mathbb{Q}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.17, 7.22 und 7.29
$(\mathbb{R}_{\neq 0}, \cdot)$		✓	1	
$(\mathbb{C}_{\neq 0}, \cdot)$		✓	1	
$(m\mathbb{Z}, +)$	ganzzahlige Vielfache von m	✓	1	Beispiele 7.45 und 7.51
$(\mathbb{Z}_m, +_m)$	additive Gruppe $\mathbb{Z}$ modulo m	✓	0	Beispiele 7.22 und 8.23
$(\mathbb{Z}/m\mathbb{Z}, \tilde{+})$	Faktorgruppe, isomorph zu $(\mathbb{Z}_m, +_m)$	✓	$[1]$	
$(G^X, +)$	Funktionen $X \to G$ in die Gruppe $(G, +)$	wie in $(G, +)$		Beispiele 7.2, 7.4, 7.8 und 7.22
$(\mathbb{Z}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{Q}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{R}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{C}^X, +)$		✓	$x \mapsto 0$	
$(G^X, \cdot)$	Funktionen $X \to G$ in die Gruppe $(G, \cdot)$	wie in $(G, \cdot)$		Beispiele 7.2, 7.4, 7.8 und 7.22
$(\mathbb{Q}_{\neq 0}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{R}_{\neq 0}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{C}_{\neq 0}^X, \cdot)$		✓	$x \mapsto 1$	
$(S_n, \circ)$	symmetrische Gruppe auf $[\![1, n]\!]$	–	$\mathrm{id}_{[\![1,n]\!]}$	Definition 7.30 und Beispiele 7.31 und 7.45
$(A_n, \circ)$	alternierende Gruppe auf $[\![1, n]\!]$	–	$\mathrm{id}_{[\![1,n]\!]}$	

Symbol	Beschreibung	komm.	neut. E.	Referenz
Ringe	($m \in \mathbb{N}$, $n \in \mathbb{N}_0$)			
$(\{0_R\}, +, \cdot)$	Nullring	✓	0_R	Beispiele 9.2 und 9.5
$(\mathbb{Z}, +, \cdot)$		✓	1	Beispiele 9.2, 9.5 und 9.9
$(m\,\mathbb{Z}, +, \cdot)$	ganzzahlige Vielfache von m	✓	—	Beispiel 9.2
$(\mathbb{Z}_m, +_m, \cdot_m)$	$\mathbb{Z}$ modulo m	✓	1	Beispiele 9.2, 9.5, 9.6, 9.23, 9.32
$(\mathbb{Z}/m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$	Restklassenring modulo m, isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$	✓	[1]	und 10.2
$(R^X, +, \cdot)$	Funktionen $X \to R$ in den Ring $(R, +, \cdot)$	wie in $(R, +, \cdot)$		
$(\mathbb{Z}^X, +, \cdot)$		✓	1	
$(\mathbb{Q}^X, +, \cdot)$		✓	1	Beispiele 9.2, 9.9 und 10.2
$(\mathbb{R}^X, +, \cdot)$		✓	1	
$(\mathbb{C}^X, +, \cdot)$		✓	1	
$(\mathcal{P}(X), \triangle, \cap)$		✓	X	Beispiele 9.2 und 9.9
$(\mathrm{End}(G), +, \circ)$	Endomorphismenring der abelschen Gruppe $(G, +)$	—	id_G	Beispiel 9.2 und Satz 17.15
$(\mathrm{End}(V), +, \circ)$	Endomorphismenring des Vektorraumes $(V, +, \cdot)$	—	id_V	
$(K^{n\times n}, +, \cdot)$	quadratische $n \times n$-Matrizen über einem Körper K	—	I_n	
$(K^{n\times n}_{\triangledown}, +, \cdot)$	Unterring der oberen Dreiecksmatrizen	—	I_n	Lemmata 15.33 und 15.38
$(K^{n\times n}_{\triangle}, +, \cdot)$	Unterring der unteren Dreiecksmatrizen	—	I_n	
$(K^{n\times n}_{\diagdown}, +, \cdot)$	Unterring der Diagonalmatrizen	✓	I_n	

Symbol	Beschreibung	komm.	neut. E.	Referenz
Körper	$(m \in \mathbb{N})$			
$(\mathbb{Q}, +, \cdot)$		✓	1	Beispiele 9.2, 9.5, 9.9, 10.2 und 10.21
$(\mathbb{R}, +, \cdot)$		✓	1	
$(\mathbb{C}, +, \cdot)$		✓	1	
$(\mathbb{Z}_m, +_m, \cdot_m)$	Körper von $\mathbb{Z}$ modulo m für Primzahlen m	✓	1	Beispiele 9.2, 10.2 und 10.8, Satz 9.11 und Folgerung 10.4
$(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$	Restklassenkörper mod. m für Primz. m, isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$	✓	[1]	

Symbol	Beschreibung	Referenz
Vektorräume	$(n, m \in \mathbb{N}_0)$	
$(K_n, +, \cdot)$	Zeilenvektoren über einem Körper $(K, +, \cdot)$	Beispiel 11.3
$(K^n, +, \cdot)$	Spaltenvektoren über einem Körper $(K, +, \cdot)$	
$(K^X, +, \cdot)$	Funktionen $X \to K$ in den Körper $(K, +, \cdot)$	Beispiele 11.3 und 11.12
$(K^{\mathbb{N}}, +, \cdot)$	Folgen mit Werten im Körper $(K, +, \cdot)$	
$(K^{\mathbb{N}}, +, \cdot)_{00}$	Folgen mit endlichem Träger und Werten im Körper $(K, +, \cdot)$	
$(V^X, +, \cdot)$	Funktionen $X \to V$ in den Vektorraum $(V, +, \cdot)$	
$(V^{\mathbb{N}}, +, \cdot)$	Folgen mit Werten im Vektorraum $(V, +, \cdot)$	
$(V^{\mathbb{N}}, +, \cdot)_{00}$	Folgen mit endlichem Träger und Werten im Vektorraum $(V, +, \cdot)$	
$(K^{n \times m}, +, \cdot)$	$n \times m$-Matrizen über einem Körper $(K, +, \cdot)$	Sätze 15.3 und 19.6
$(\mathrm{Hom}(V, W), +, \cdot)$	Homomorphismen $V \to W$ mit VR $(V, +, \cdot)$ und $(W, +, \cdot)$ über demselben Körper	Satz 17.14

Kapitel C Hüllenoperatoren

Wir haben im Verlauf der Vorlesung an verschiedenen Stellen die Bildung von *Hüllen* von Teilmengen gewisser Strukturen betrachtet. Diese sind in der untenstehenden Tabelle aufgeführt, ergänzt um einige weitere naheliegende Beispiele, die wir nicht explizit behandelt haben. Die Intention der Hüllenbildung war jeweils, eine gegebene Menge durch Vergrößerung mit einer gewünschten Zusatzeigenschaft auszustatten, die sie i. A. noch nicht besitzt. Beispielsweise können wir durch die Bildung der reflexiven Hülle von einer beliebigen zu einer reflexiven Relation übergehen.

Wir klären zunächst den Begriff des Hüllenoperators, der die Grundlage für alle Hüllenbegriffe bildet:

Definition C.1 (Hüllenoperator)**.**
Es sei X eine Menge. Ein **Hüllenoperator** auf X (englisch: closure operator) ist eine Abbildung $H\colon \mathcal{P}(X) \to \mathcal{P}(X)$ mit den folgenden Eigenschaften:

$$A \subseteq H(A) \qquad H \text{ ist } \textbf{extensiv}^{1} \tag{C.1a}$$

$$A \subseteq B \quad \Rightarrow \quad H(A) \subseteq H(B) \qquad H \text{ ist } \textbf{monoton}^{2} \tag{C.1b}$$

$$H(H(A)) = H(A) \qquad H \text{ ist } \textbf{idempotent}^{3} \tag{C.1c}$$

für alle $A, B \subseteq X$. △

Wir könnten jetzt für die in der unten stehenden Tabelle aufgeführten Hüllen jeweils zeigen, dass sie Hüllenoperatoren im Sinne der Definition C.1 sind. Beispielsweise ist die reflexive Hülle $H(R) \coloneqq R^{?} = \bigcap\{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\}$ ein Hüllenoperator auf $X \times X$, denn für jede Relation $R \subseteq X \times X$ gilt: R ist Teilmenge jeder Relation S, über die in der rechten Menge der Durchschnitt gebildet wird. Daher ist R auch Teilmenge des Durchschnitts $H(R)$, d. h., H ist extensiv. Bilden wir die reflexive Hülle von $H(R)$, so ist $H(R)$ Teilmenge jeder Relation S, über die in der rechten Menge der Durchschnitt gebildet wird. Daher ist $H(R)$ auch Teilmenge des Durchschnitts $H(H(R))$. Andererseits gilt wegen der Extensivität von H auch die umgekehrte Inklusion $H(R) \subseteq H(H(R))$, also ist H idempotent. Sind schließlich $R_1 \subseteq R_2$ zwei Relationen auf X, so ist jede Relation S, die in der rechten Menge der Durchschnittsbildung von $H(R_2)$ vorkommt, auch in der rechten Menge der Durchschnittsbildung von $H(R_1)$ enthalten. Daraus folgt $H(R_1) \subseteq H(R_2)$, d. h., H ist monoton.

Dieser Beweis würde für alle anderen Hüllenoperatoren in der Tabelle genau dieselben Argumente verwenden. Daher stellt sich die Frage nach einer Charakterisierung von Hüllenoperatoren.

[1] englisch: extensive
[2] englisch: monotone
[3] englisch: idempotent

Es stellt sich heraus, dass die entscheidende Eigenschaft ist, dass beispielsweise der Durchschnitt reflexiver Relationen wieder eine reflexive Relation ist. Diese Eigenschaft wird mit der folgenden Definition formalisiert:

Definition C.2 (Abschlusssystem)**.**
Es sei X eine Menge. Ein **Abschlusssystem** auf X (englisch: closure system) ist eine Teilmenge $\mathcal{A} \subseteq \mathcal{P}(X)$ mit der Eigenschaft, dass für jede nichtleere Menge $\mathcal{B} \subseteq \mathcal{A}$ gilt: $\bigcap \mathcal{B} \in \mathcal{A}$. △

Ein Abschlusssystem auf X ist also eine Menge von Teilmengen von X, die bezüglich der Durchschnittsbildung abgeschlossen ist. Beispielsweise ist die Menge $\mathcal{A}$ aller reflexiven Relationen auf einer Menge X ein Abschlusssystem auf $X \times X$, weil der Durchschnitt reflexiver Relationen wieder eine reflexive Relation ist (Lemma 5.13). Auch die Menge $\mathcal{A}$ aller Untergruppen einer Gruppe G bildet ein Abschlusssystem (auf G), weil der Durchschnitt von Untergruppen wieder eine Untergruppe ist (Lemma 7.47).

Der folgende Satz stellt nun klar, dass Hüllenoperatoren und Abschlusssysteme „dasselbe“ sind, genauer: dass diese bijektiv aufeinander abgebildet werden können.

Satz C.3 (Zusammenhang zwischen Hüllenoperatoren und Abschlusssystemen)**.**
Es sei X eine Menge.

(*i*) Es sei $H\colon \mathcal{P}(X) \to \mathcal{P}(X)$ ein Hüllenoperator auf X. Dann ist

$$\mathcal{A}_H \coloneqq \{A \subseteq X \mid H(A) = A\}$$

ein Abschlusssystem auf X.
(Wir sammeln alle Teilmengen, die durch Hüllenbildung nicht größer werden.)

(*ii*) Es sei $\mathcal{A} \subseteq \mathcal{P}(X)$ ein Abschlusssystem auf X. Dann ist die durch

$$H_{\mathcal{A}}(A) \coloneqq \bigcap \{B \in \mathcal{A} \mid A \subseteq B\}$$

definierte Abbildung $H_{\mathcal{A}}\colon \mathcal{P}(X) \to \mathcal{P}(X)$ ein Hüllenoperator auf X.
(Wir bilden den Durchschnitt über alle Obermengen im Abschlusssystem, die also die gewünschte Eigenschaft besitzen.)

(*iii*) Für jeden Hüllenoperator H auf X gilt: $H = H_{\mathcal{A}_H}$.

(*iv*) Für jedes Abschlusssystem $\mathcal{A}$ auf X gilt: $\mathcal{A} = \mathcal{A}_{H_{\mathcal{A}}}$.

Wir können nun auf einen Schlag und ohne weiteren Aufwand zeigen, dass alle in der Tabelle aufgeführten Begriffe tatsächlich Hüllenoperatoren im Sinne der Definition C.1 sind, denn: Wir wissen in jedem Fall bereits (oder können leicht zeigen), dass die jeweils relevante Menge $\mathcal{A}$ (z. B. die Menge aller reflexiven Relationen auf einer Menge X) ein Abschlusssystem ist. Im Einzelnen: Der Durchschnitt reflexiver Relationen ist wieder reflexiv, der Durchschnitt symmetrischer Relationen ist wieder symmetrisch usw. (Lemma 5.13). Der Durchschnitt von Unterhalbgruppen einer Halbgruppe ist wieder eine Unterhalbgruppe (leicht zu zeigen). Der Durchschnitt von Untergruppen einer Gruppe ist wieder eine Untergruppe (Lemma 7.47). Der Durchschnitt von Normalteilern einer Gruppe ist wieder ein Normalteiler (leicht zu zeigen). Der Durchschnitt

von Unterringen eines Ringes ist wieder eine Unterring (leicht zu zeigen). Der Durchschnitt von Idealen eines Ringes ist wieder ein Ideal (Lemma 9.34). Der Durchschnitt von Unterkörpern eines Körpers ist wieder ein Unterkörper (Lemma 10.10). Der Durchschnitt von Unterräumen eines Vektorraumes ist wieder ein Unterraum (Lemma 11.14).

Der Satz C.3 zeigt, dass wir für jede Eigenschaft, die unter Durchschnittsbildung abgeschlossen ist, einen zugehörigen Hüllenoperator definieren können. Die Hüllenbildung $H(A)$ wird zu einer Teilmenge $A \subseteq X$ genau dann nichts hinzufügen (also $H(A) = A$ liefern), wenn A die gewünschte Eigenschaft bereits besitzt.

Name	Definition	Referenz
homogene **Relation** R auf einer Menge X (Teilmenge R einer Menge $X \times X$)		
reflexive Hülle	$R^? := \bigcap\{S \subseteq X \times X \mid S \text{ ist reflexiv und } R \subseteq S\}$	Definition 5.9
symmetrische Hülle	$R^{\text{sym}} := \bigcap\{S \subseteq X \times X \mid S \text{ ist symmetrisch und } R \subseteq S\}$	
transitive Hülle	$R^+ := \bigcap\{S \subseteq X \times X \mid S \text{ ist transitiv und } R \subseteq S\}$	
reflexiv-transitive Hülle	$R^* := \bigcap\{S \subseteq X \times X \mid S \text{ ist reflexiv und transitiv und } R \subseteq S\}$	
reflexiv-symmetrisch-transitive Hülle	$R^\sim := \bigcap\{S \subseteq X \times X \mid S \text{ ist reflexiv, symmetrisch und transitiv und } R \subseteq S\}$	
Teilmenge E einer **Halbgruppe** H		
erzeugte Unterhalbgruppe	$\bigcap\{U \mid U \text{ ist Unterhalbgruppe von } H \text{ und } E \subseteq U\}$	—
Teilmenge E einer **Gruppe** G		
erzeugte Untergruppe	$\langle E\rangle := \bigcap\{U \mid U \text{ ist Untergruppe von } G \text{ und } E \subseteq U\}$	Definition 7.48
erzeugter Normalteiler	$\bigcap\{U \mid U \text{ ist normale Untergruppe von } G \text{ und } E \subseteq U\}$	—
Teilmenge E eines **Ringes** R		
erzeugter Unterring	$\bigcap\{U \mid U \text{ ist Unterring von } R \text{ und } E \subseteq U\}$	—
erzeugtes Ideal	$(E) := \bigcap\{J \mid J \text{ ist Ideal von } R \text{ und } E \subseteq J\}$	Definition 9.35
Teilmenge E eines **Körpers** K		
erzeugter Unterkörper	$\bigcap\{U \mid U \text{ ist Unterkörper von } R \text{ und } E \subseteq U\}$	—
Teilmenge E eines **Vektorraumes** V		
erzeugter Unterraum	$\langle E\rangle := \bigcap\{U \mid U \text{ ist Unterraum von } V \text{und } E \subseteq U\}$	Definition 11.10

Kapitel D Einige Algorithmen

Der folgende Algorithmus erzeugt aus einer Matrix $A \in K^{n\times m}$ eine Matrix in Zeilenstufenform $C \in K^{n\times m}$ (Definition 15.20) mit der Eigenschaft $\mathrm{ZR}(A) = \mathrm{ZR}(C)$ (Satz 15.23). Die Anzahl $r \in [\![0, n]\!]$ der Nicht-Nullzeilen von C ist der Rang von A. Diese Zeilen bilden eine Basis von $\mathrm{ZR}(A)$.

Algorithmus D.1 (Erzeugen einer Zeilenstufenform)**.**
Eingabe: Matrix $A \in K^{n\times m}$
Ausgabe: Matrix $C \in K^{n\times m}$ in Zeilenstufenform mit $\mathrm{ZR}(A) = \mathrm{ZR}(C)$
Ausgabe: $r = \mathrm{Rang}(A) = \mathrm{Rang}(C)$

Setze $C \leftarrow A$
Setze $r \leftarrow 0$ // bisher festgestellter Rang
Setze $j_0 \leftarrow 0$ // Spalte des letzten Pivot-Elements
while $r < n$ und $j_r < m$ und die Restmatrix $(C)_{r+1\leqslant i\leqslant n,\ j_r+1\leqslant j\leqslant m}$ ist nicht die Nullmatrix **do**
    Setze $j \leftarrow \min\{j_r + 1 \leqslant j \leqslant m \mid (C)_{r+1\leqslant i\leqslant n,\ j}\}$ // erste Nicht-Nullspalte der Restmatrix
    Setze $i \leftarrow \min\{r + 1 \leqslant i \leqslant n \mid c_{ij} \neq 0\}$ // erster Nicht-Nulleintrag in dieser Spalte
    Setze $r \leftarrow r + 1$ // festgestellter Rang erhöht sich
    Setze $j_r \leftarrow j$ // Spalte des neuen Pivot-Elements merken
    Tausche in der Matrix C die Zeilen i und r // Pivot-Element kommt nach oben (Typ III)
  // Erzeuge Nullen unterhalb des Pivot-Elements (r, j) durch Elementarmatrizen (Typ II):
    for $i = r + 1, \ldots, m$ **do**
        Setze $c_{i\bullet} \leftarrow c_{i\bullet} - \frac{c_{ij}}{c_{rj}} c_{r\bullet}$ // Erzeuge eine Null an der Stelle (i, j) durch $S_{i,r}(-\frac{c_{ij}}{c_{rj}})$
    end for
end while
return C und r

Der folgende Algorithmus ist eine Erweiterung von Algorithmus D.1. Dieser erzeugt aus einer Matrix $A \in K^{n\times m}$ eine Faktorisierung $A = BC$ mit invertierbarer Matrix $B \in K^{n\times n}$ und derselben Matrix $C \in K^{n\times m}$ in Zeilenstufenform C wie in Algorithmus D.1. Durch Beschränkung auf die ersten r Spalten von B (mit $B_{\text{Rang}} \in K^{n\times r}$ bezeichnet) und die ersten r Zeilen von C (mit $C_{\text{Rang}} \in K^{r\times m}$ bezeichnet) erhalten wir eine Rangfaktorisierung $A = BC = B_{\text{Rang}}\,C_{\text{Rang}}$ (Folgerung 15.16, Bemerkung 15.25) der Matrix A. Die Spalten von B_{Rang} bilden eine Basis von $\mathrm{SR}(A)$. Die Zeilen von C_{Rang} bilden eine Basis von $\mathrm{ZR}(A)$.

Algorithmus D.2 (Erzeugen einer Rangfaktorisierung $A = BC = B_{\text{Rang}}\,C_{\text{Rang}}$)**.**
Eingabe: Matrix $A \in K^{n\times m}$
Ausgabe: Matrix $B \in K^{n\times n}$ mit $\mathrm{SR}(A) = \mathrm{SR}(B)$
Ausgabe: Matrix $B_{\text{Rang}} \in K^{n\times r}$ mit $\mathrm{SR}(A) = \mathrm{SR}(B_{\text{Rang}})$
Ausgabe: Matrix $C \in K^{n\times m}$ in Zeilenstufenform mit $\mathrm{ZR}(A) = \mathrm{ZR}(C)$
Ausgabe: Matrix $C_{\text{Rang}} \in K^{r\times m}$ in Zeilenstufenform mit $\mathrm{ZR}(A) = \mathrm{ZR}(C_{\text{Rang}})$
Ausgabe: $r = \mathrm{Rang}(A) = \mathrm{Rang}(B) = \mathrm{Rang}(B_{\text{Rang}}) = \mathrm{Rang}(C) = \mathrm{Rang}(C_{\text{Rang}})$

1: Setze $B \leftarrow I_n$
2: Setze $C \leftarrow A$
3: Setze $r \leftarrow 0$ // bisher festgestellter Rang
4: Setze $j_0 \leftarrow 0$ // Spalte des letzten Pivot-Elements
5: **while** $r < n$ und $j_r < m$ und die Restmatrix $(C)_{r+1\leqslant i\leqslant n,\ j_r+1\leqslant j\leqslant m}$ ist nicht die Nullmatrix **do**
6: Setze $j \leftarrow \min\{j_r + 1 \leqslant j \leqslant m \mid (C)_{r+1\leqslant i\leqslant n,\ j} \}$ // erste Nicht-Nullspalte der Restmatrix
7: Setze $i \leftarrow \min\{r + 1 \leqslant i \leqslant n \mid c_{ij} \neq 0\}$ // erster Nicht-Nulleintrag in dieser Spalte
8: Setze $r \leftarrow r + 1$ // festgestellter Rang erhöht sich
9: Setze $j_r \leftarrow j$ // Spalte des neuen Pivot-Elements merken
10: Tausche in der Matrix C die Zeilen i und r // Pivot-Element kommt nach oben (Typ III)
11: Tausche in der Matrix B die Spalten i und r
// Erzeuge Nullen unterhalb des Pivot-Elements (r, j) durch Elementarmatrizen (Typ II):
12: **for** $i = r + 1, \ldots, m$ **do**
13: Setze $c_{i\bullet} \leftarrow c_{i\bullet} - \frac{c_{ij}}{c_{rj}} c_{r\bullet}$ // Erzeuge eine Null an der Stelle (i, j) durch $S_{i,r}(-\frac{c_{ij}}{c_{rj}})$
14: Setze $b_{\bullet r} \leftarrow b_{\bullet r} + \frac{c_{ij}}{c_{rj}} b_{\bullet i}$ // Gehe von $A = BC$ über zu $A = B\,S_{i,r}(-\frac{c_{ij}}{c_{rj}})^{-1} S_{i,r}(-\frac{c_{ij}}{c_{rj}})\,C$
15: **end for**
16: **end while**
17: Setze $B_{\text{Rang}} \leftarrow \begin{bmatrix} b_{\bullet 1} & \cdots & b_{\bullet r} \end{bmatrix}$
18: Setze $C_{\text{Rang}} \leftarrow \begin{bmatrix} c_{1\bullet} \\ \vdots \\ c_{r\bullet} \end{bmatrix}$
19: **return** B, B_{Rang}, C, C_{Rang} und r

Der folgende Algorithmus ist eine Erweiterung sowohl von Algorithmus D.1 als auch von Algorithmus D.2. Er erzeugt aus einer Matrix $A \in K^{n\times m}$ eine Faktorisierung $A = BC$ mit invertierbarer Matrix $B \in K^{n\times n}$ und Matrix in reduzierter Zeilenstufenform $C \in K^{n\times m}$ (Definition 16.5) mit der Eigenschaft $\mathrm{ZR}(A) = \mathrm{ZR}(C)$ (Satz 16.7). Durch Beschränkung auf die ersten r Spalten von B (mit $B_{\mathrm{Rang}} \in K^{n\times r}$ bezeichnet) und die ersten r Zeilen von C (mit $C_{\mathrm{Rang}} \in K^{r\times m}$ bezeichnet) erhalten wir eine Rangfaktorisierung $A = BC = B_{\mathrm{Rang}}\, C_{\mathrm{Rang}}$ (Folgerung 15.16, Bemerkung 15.25) der Matrix A. Die Spalten von B_{Rang} bilden eine Basis von $\mathrm{SR}(A)$. Die Zeilen von C_{Rang} bilden eine Basis von $\mathrm{ZR}(A)$.

Gilt $n = m$, dann ist A genau dann invertierbar, wenn $C = I_n$ gilt.

Algorithmus D.3 (Erzeugen einer Rangfaktorisierung $A = BC = B_{\mathrm{Rang}}\, C_{\mathrm{Rang}}$ mit reduzierter Zeilenstufenform)**.**

Eingabe: Matrix $A \in K^{n\times m}$
Ausgabe: Matrix $B \in K^{n\times n}$ mit $\mathrm{SR}(A) = \mathrm{SR}(B)$
Ausgabe: Matrix $B_{\mathrm{Rang}} \in K^{n\times r}$ mit $\mathrm{SR}(A) = \mathrm{SR}(B_{\mathrm{Rang}})$
Ausgabe: Matrix $C \in K^{n\times m}$ in reduzierter Zeilenstufenform mit $\mathrm{ZR}(A) = \mathrm{ZR}(C)$
Ausgabe: Matrix $C_{\mathrm{Rang}} \in K^{r\times m}$ in reduzierter Zeilenstufenform mit $\mathrm{ZR}(A) = \mathrm{ZR}(C_{\mathrm{Rang}})$
Ausgabe: $r = \mathrm{Rang}(A) = \mathrm{Rang}(B) = \mathrm{Rang}(B_{\mathrm{Rang}}) = \mathrm{Rang}(C) = \mathrm{Rang}(C_{\mathrm{Rang}})$

1: Setze $B \leftarrow I_n$
2: Setze $C \leftarrow A$
3: Setze $r \leftarrow 0$ // bisher festgestellter Rang
4: Setze $j_0 \leftarrow 0$ // Spalte des letzten Pivot-Elements
5: **while** $r < n$ und $j_r < m$ und die Restmatrix $(C)_{r+1\leqslant i\leqslant n,\ j_r+1\leqslant j\leqslant m}$ ist nicht die Nullmatrix **do**
6: Setze $j \leftarrow \min\{j_r + 1 \leqslant j \leqslant m \mid (C)_{r+1\leqslant i\leqslant n,\ j}\}$ // erste Nicht-Nullspalte der Restmatrix
7: Setze $i \leftarrow \min\{r + 1 \leqslant i \leqslant n \mid c_{ij} \neq 0\}$ // erster Nicht-Nulleintrag in dieser Spalte
8: Setze $r \leftarrow r + 1$ // festgestellter Rang erhöht sich
9: Setze $j_r \leftarrow j$ // Spalte des neuen Pivot-Elements merken
10: Tausche in der Matrix C die Zeilen i und r // Pivot-Element kommt nach oben (Typ III)
11: Tausche in der Matrix B die Spalten i und r
// Erzeuge Nullen unterhalb des Pivot-Elements (r, j) durch Elementarmatrizen (Typ II):
12: **for** $i = r + 1, \ldots, m$ **do**
13: Setze $c_{i\bullet} \leftarrow c_{i\bullet} - \frac{c_{ij}}{c_{rj}} c_{r\bullet}$ // Erzeuge eine Null an der Stelle (i, j) durch $S_{i,r}(-\frac{c_{ij}}{c_{rj}})$
14: Setze $b_{\bullet r} \leftarrow b_{\bullet r} + \frac{c_{ij}}{c_{rj}} b_{\bullet i}$ // Gehe von $A = BC$ über zu $A = B\, S_{i,r}(-\frac{c_{ij}}{c_{rj}})^{-1} S_{i,r}(-\frac{c_{ij}}{c_{rj}})\, C$
15: **end for**
16: **end while**
17: **for** $k = r, \ldots, 1$ **do**
18: Setze $j \leftarrow j_k$ // aktuelles Pivot-Element ist (k, j)
// Erzeuge Nullen oberhalb des Pivot-Elements (k, j) durch Elementarmatrizen (Typ II):
19: **for** $i = k - 1, \ldots, 1$ **do**
20: Setze $c_{i\bullet} \leftarrow c_{i\bullet} - \frac{c_{ij}}{c_{kj}} c_{k\bullet}$ // Erzeuge eine Null an der Stelle (i, j) durch $S_{i,k}(-\frac{c_{ij}}{c_{kj}})$
21: Setze $b_{\bullet k} \leftarrow b_{\bullet k} + \frac{c_{ij}}{c_{kj}} b_{\bullet i}$ // Gehe von $A = BC$ über zu $A = B\, S_{i,k}(-\frac{c_{ij}}{c_{kj}})^{-1} S_{i,k}(-\frac{c_{ij}}{c_{kj}})\, C$
22: **end for**
23: Setze $p \leftarrow c_{kj}$ // Hole das Pivot-Element
24: Setze $c_{k\bullet} \leftarrow \frac{1}{p} c_{k\bullet}$ // Mache das Pivot-Element (k, j) zu 1 durch $D_k(\frac{1}{p})$

Setze $b_{\bullet k} \leftarrow p\, b_{\bullet k}$ // Gehe von $A = B\,C$ über zu $A = B\,D_k(\frac{1}{p})^{-1} D_k(\frac{1}{p})\,C$

end for

Setze $B_{\text{Rang}} \leftarrow \begin{bmatrix} b_{\bullet 1} & \cdots & b_{\bullet r} \end{bmatrix}$

Setze $C_{\text{Rang}} \leftarrow \begin{bmatrix} c_{1\bullet} \\ \vdots \\ c_{r\bullet} \end{bmatrix}$

return B, B_{Rang}, C, C_{Rang} und r

Kapitel E Das griechische Alphabet

Kleinbuchstabe	Großbuchstabe	Name
α	A	alpha
β	B	beta
γ	Γ	gamma
δ	Δ	delta
ϵ, ε	E	epsilon
ζ	Z	zeta
η	H	eta
θ, ϑ	Θ	theta
ι	I	iota
κ, $\varkappa$	K	kappa
λ	Λ	lambda
μ	M	mu
ν	N	nu
ξ	Ξ	xi
o	O	omikron
π, ϖ	Π	pi
ρ, ϱ	P	rho
σ, ς	Σ	sigma
τ	T	tau
υ	Υ	ypsilon
ϕ, φ	Φ	phi
χ	X	chi
ψ	Ψ	psi
ω	Ω	omega

Kapitel F 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

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. (2022). *Einführung in die Mathematik 2.1. Elementare Zahlentheorie und Graphentheorie.* URL: https://www.aleph1.info/?call=Puc&permalink=ema21.

Deiser, O. (2024a). *Einführung in die Mengenlehre. Die Mengenlehre Georg Cantors und ihre Axiomatisierung durch Ernst Zermelo.* URL: https://www.aleph1.info/?call=Puc&permalink=mengenlehre1.

Deiser, O. (2024b). *Grundbegriffe der Mathematik. Sprache, Zahlen und erste Erkundungen.* 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.

Goldrei, D. (1996). *Classic Set Theory. For Guided Independent Study.* Chapman & Hall/CRC, Boca Raton, FL.

Jänich, K. (2008). *Lineare Algebra.* 11. Aufl. Springer Berlin Heidelberg. DOI: 10.1007/978-3-540-75502-9.

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.

Velleman, D. J. (2019). *How to Prove It. A Structured Approach.* 3. Aufl. Cambridge University Press, Cambridge. DOI: 10.1017/9781108539890.

Index