Vorlesungsskript
Lineare Algebra

Wintersemester 2023

Roland Herzog*

2024-02-08

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

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

Änderungen gegenüber bereits veröffentlichten Versionen werden in dieser Farbe gekennzeichnet.

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

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

Inhaltsverzeichnis

Kapitel 1 Mathematische Grundlagen

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

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

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

§ 1 Aussagenlogik

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

Definition 1.1 (Aussage, Wahrheitswert)**.**
Eine **Aussage** (englisch: statement) ist ein Satz (einer Sprache), dem eindeutig entweder der **Wahrheitswert wahr** (kurz: W oder $\top$, englisch: true, T) oder der **Wahrheitswert falsch** (kurz: F oder $\bot$, 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 A, B usw.

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

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

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

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

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

(*v*) E: Es gibt unendlich viele Primzahlzwillinge.
Dieses ist 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 definieren einen Junktor über seine **Wahrheitswerttabelle** (auch: **Wahrheitstafel**, englisch: truth table).

Definition 1.3 (Junktoren)**.**

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

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

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

A	$\neg A$
W	F
F	W

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

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

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

[1] siehe Primzahlzwillingsvermutung
[2] lateinisch: coniungere: verbinden

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

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

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

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

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

A	B	$A \rightarrow B$
W	W	W
W	F	F
F	W	W
F	F	W

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

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

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

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

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

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

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

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

[3] lateinisch: disiungere: trennen, unterscheiden
[4] lateinisch: implicare: verwickeln
[5] lateinisch: conditio: Bedingung
[6] lateinisch: aequivalens: gleichwertig
[7] angelehnt an Beispiele aus Magnus u. a., 2023, Kapitel 5, genutzt unter der Lizenz CC-BY 4.0

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

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

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

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

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

- $E \wedge (\neg S)$

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

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

- $(\neg S_1) \wedge S_2$

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

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

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

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 A und B Aussagen.

(*i*) Die Aussagen

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

haben dieselben Wahrheitstafeln.

(*ii*) Die Aussagen

- $A \leftrightarrow B$
- $(A \to B) \wedge (B \to A)$

haben dieselben Wahrheitstafeln.

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

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

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

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

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

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

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

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

Wir berechnen jetzt die Wahrheitstafeln einiger zusammengesetzter Aussagen.

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

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

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

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

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

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

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

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

△

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

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

Es seien A und B Aussagen.

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

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

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

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

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

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

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

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

[8] altgriechisch: *ταυτο*: dasselbe

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

$\neg(\neg A)$	$\Leftrightarrow$	A	doppelte Verneinung[9]	(1.2)
A	$\Rightarrow$	$\top$	„Aus Beliebigem folgt Wahres.“[10]	(1.3a)
$\bot$	$\Rightarrow$	A	„Aus Falschem folgt Beliebiges.“[11]	(1.3b)
$A \wedge A$	$\Leftrightarrow$	A	**Idempotenz**[12]	(1.4a)
$A \vee A$	$\Leftrightarrow$	A	**Idempotenz**	(1.4b)
$A \wedge \top$	$\Leftrightarrow$	A	**Neutralität**[13]	(1.5a)
$A \vee \bot$	$\Leftrightarrow$	A	**Neutralität**	(1.5b)
$A \wedge \bot$	$\Leftrightarrow$	$\bot$	**Absorption**[14]	(1.6a)
$A \vee \top$	$\Leftrightarrow$	$\top$	**Absorption**	(1.6b)
$A \wedge \neg A$	$\Leftrightarrow$	$\bot$	**Komplementarität**[15]	(1.7a)
$A \vee \neg A$	$\Leftrightarrow$	$\top$	**Komplementarität**[16]	(1.7b)
$A \wedge B$	$\Leftrightarrow$	$B \wedge A$	**Kommutativität von $\wedge$**[17]	(1.8a)
$A \vee B$	$\Leftrightarrow$	$B \vee A$	**Kommutativität von $\vee$**	(1.8b)
$(A \vee B) \vee C$	$\Leftrightarrow$	$A \vee (B \vee C)$	**Assoziativität von $\vee$**[18]	(1.9a)
$(A \wedge B) \wedge C$	$\Leftrightarrow$	$A \wedge (B \wedge C)$	**Assoziativität von $\wedge$**	(1.9b)
$\neg(A \wedge B)$	$\Leftrightarrow$	$\neg A \vee \neg B$	**De Morgansches Gesetz**[19]	(1.10a)
$\neg(A \vee B)$	$\Leftrightarrow$	$\neg A \wedge \neg B$	**De Morgansches Gesetz**	(1.10b)
$A \wedge (B \vee C)$	$\Leftrightarrow$	$(A \wedge B) \vee (A \wedge C)$	**Distributivität**[20]	(1.11a)
$A \vee (B \wedge C)$	$\Leftrightarrow$	$(A \vee B) \wedge (A \vee C)$	**Distributivität**	(1.11b)

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

Ende der Vorlesung 1

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

§ 2 Prädikatenlogik

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

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

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

  Beispiele:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$\neg(\forall x\ A(x))$	$\Leftrightarrow$	$\exists x\ (\neg A(x))$	Negation des Allquantors	(2.1a)
$\neg(\exists x\ A(x))$	$\Leftrightarrow$	$\forall x\ (\neg A(x))$	Negation des Existenzquantors	(2.1b)
$\forall x\ \forall y\ C(x,y)$	$\Leftrightarrow$	$\forall y\ \forall x\ C(x,y)$	**Kommutativität gleicher Quantoren**	(2.2a)
$\exists x\ \exists y\ C(x,y)$	$\Leftrightarrow$	$\exists y\ \exists x\ C(x,y)$	**Kommutativität gleicher Quantoren**	(2.3a)
$\forall x\ (A(x) \wedge B(x))$	$\Leftrightarrow$	$\forall x\ A(x) \wedge \forall x\ B(x)$	**Distributivität**	(2.4a)
$\exists x\ (A(x) \vee B(x))$	$\Leftrightarrow$	$\exists x\ A(x) \vee \exists x\ B(x)$	**Distributivität**	(2.4b)
$(\forall x\ A(x)) \vee (\forall x\ B(x))$	$\Rightarrow$	$\forall x\ (A(x) \vee B(x))$		(2.5a)
$\exists x\ (A(x) \wedge B(x))$	$\Rightarrow$	$(\exists x\ A(x)) \wedge (\exists x\ B(x))$		(2.5b)
$\forall x\ (A(x) \to B(x))$	$\Rightarrow$	$(\forall x\ A(x)) \to (\forall x\ B(x))$		(2.6a)

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

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

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

§ 3 Beweismuster

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

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

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

$$(A \to B) \wedge A \quad \Rightarrow \quad B \qquad \textbf{modus ponendo ponens}, \tag{3.1a}$$
$$(A \to B) \wedge \neg B \quad \Rightarrow \quad \neg A \qquad \textbf{modus tollendo tollens}, \tag{3.1b}$$
$$(A \to \neg B) \wedge A \quad \Rightarrow \quad \neg B \qquad \textbf{modus ponendo tollens}[23], \tag{3.1c}$$
$$(\neg A \to B) \wedge \neg A \quad \Rightarrow \quad B \qquad \textbf{modus tollendo ponens}[24], \tag{3.1d}$$
$$(A \to B) \wedge (B \to C) \quad \Rightarrow \quad (A \to C) \qquad \textbf{Kettenschluss} \text{ (englisch: chain inference).} \tag{3.2}$$

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

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

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

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

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

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

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

Beispiel 3.1 (verschiedene Beweismuster)**.**

(1) **direkter Beweis**

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

Wir symbolisieren die zugehörigen Aussagen über zweistellige Aussageformen:

$$A(m,n) : m^2 < n^2$$
$$B(m,n) : m < n$$

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

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

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

	$m^2 < n^2$	nach Definition von A
$\Rightarrow$	$0 < n^2 - m^2$	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 A und B war für den Beweis auch nicht wesentlich, sodass wir im Folgenden darauf verzichten können.

(2) **Beweis durch Kontraposition**

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

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

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

(3) **Widerspruchsbeweis**[25]

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

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

[25] Dieses Beispiel ist Thiele, 1979 entnommen.

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

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

(4) **Beweis durch Fallunterscheidung**

Behauptung: Für jede ganze Zahl $n \in \mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ 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.

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

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

also wiederum eine gerade Zahl. △

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

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

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

Quizfrage 3.2: Wieviele Implikationen wären zu zeigen, wenn man die Äquivalenz der Aussagen A_i und A_j für $i, j = 1, \ldots, n$ 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 $A(n)$ für alle ganzen Zahlen $n \in \mathbb{Z}$ ab einem gewissen Startindex $n_0 \in \mathbb{Z}$ zeigen wollen, also für $n \geqslant n_0$. In diesem Fall zeigen wir am **Induktionsanfang** (englisch: base case) die Wahrheit der Aussage $A(n_0)$. Oft wird der Induktionsanfang bei $n_0 = 0$ oder $n_0 = 1$ gesetzt.

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

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

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

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

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

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

was $A(n+1)$ entspricht. △

Ende der Vorlesung 2

Ende der Woche 1

§ 4 Mengenlehre

Literatur: Deiser, 2022b, Kapitel 1.2, Jänich, 2008, Kapitel 1.1

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

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

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

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

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

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

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

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

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

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

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

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

$$Y := \{x \in X \,|\, A(x)\} \tag{4.1}$$

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

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

$$R := \{x \in X \,|\, x \notin x\}$$

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

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

[26] englisch: natural numbers
[27] englisch: integer numbers, lateinisch: integer: ganz, unversehrt
[28] englisch: rational numbers, lateinisch: ratio: Verhältnis
[29] englisch: real numbers
[30] englisch: complex numbers

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

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

Intervalle lassen sich beispielsweise über Mengenkomprehension definieren:

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

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

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

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

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

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

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

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

[34] englisch: closed interval

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

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

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

[38] englisch: unbounded above, closed interval

[39] englisch: unbounded above, open interval

[40] englisch: unbounded below, closed interval

[41] englisch: unbounded below, open interval

[42] englisch: unbounded above and below interval

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

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

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

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

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

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

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

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

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

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

$$\bigcap \mathcal{U} := \{x \mid \forall U \in \mathcal{U}\ (x \in U)\} \tag{4.2}$$

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

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

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

$$U_1 \cap U_2 := \{x \mid x \in U_1 \ \wedge\ x \in U_2\}. \tag{4.4}$$

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

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

$$\bigcup \mathcal{U} := \{x \mid \exists U \in \mathcal{U}\ (x \in U)\} \tag{4.5}$$

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

$$\bigcup_{i \in I} U_i := \{x \mid \exists i \in I\ (x \in U_i)\}. \tag{4.6}$$

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

$$U_1 \cup U_2 := \{x \mid x \in U_1 \ \vee\ x \in U_2\}. \tag{4.7}$$

[43] lateinisch: includere: einschließen

△

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Zur Vereinfachung der Notation vereinbaren wir auch hier wieder Bindungsregeln:

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

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

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

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

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

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

Beispiel 4.7 (Potenzmenge)**.**

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

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

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

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

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

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

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

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

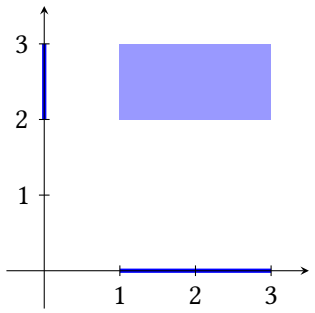
(*iii*) Wir schreiben $A^2 = A \times A$ und allgemeiner $A^n = \bigtimes_{i=1}^{n} A$ für das kartesische Produkt einer Menge A mit sich selbst. △

Beispiel 4.9 (kartesisches Produkt)**.**

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

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

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



△

Ende der Vorlesung 3

§ 5 Relationen

Literatur: Deiser, 2022b, Kapitel 1.3

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

Definition 5.1 (Relation)**.**

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

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

Beispiel 5.2 (Relation)**.**

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

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

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

[45] lateinisch: relatio: Verhältnis, Beziehung

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

(*iii*) Es sei $X = Y = \mathbb{R}$ und $R = \{(x, y) \in \mathbb{R}^2 \mid x \leqslant y\}$ 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 **Inklusionsrelation** (englisch: inclusion relation).

(*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) 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 (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

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

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

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

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

$$R^{-1} := \{(b, a) \in Y \times X \mid (a, b) \in R\} \subseteq Y \times X$$

definiert ist. △

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 5.1 Ordnungsrelationen

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis. Dieser Beweis ist Teil von Hausaufgabe 2.3. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Wir zeigen nun einige ausgewählte Eigenschaften.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 5.2 Äquivalenzrelation

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

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

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

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

Beispiel 5.14 (Äquivalenzrelationen)**.**

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

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

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

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

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

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

(*i*) Für $x \in X$ heißt die Menge

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

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

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

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

Beispiel 5.16 (Äquivalenzklasse, Repräsentant)**.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(*i*) Die Menge der Äquivalenzklassen

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

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

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

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

Beispiel 5.21 (wohldefinierte Aussageformen)**.**

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

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

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

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

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

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

Das führt uns zur Definition

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

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

Ende der Vorlesung 4

Ende der Woche 2

§ 6 Abbildungen

Literatur: Deiser, 2022b, Kapitel 1.3, Deiser, 2022b, Kapitel 1.4, 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 auch in der Form

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

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

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

für die Definition einer Funktion sind üblich.

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

Die Menge

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

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

Beispiel 6.3 (Abbildungen)**.**

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

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

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

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

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

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

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

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

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

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

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

(*i*) Für $A \subseteq X$ heißt

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

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

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

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

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

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

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

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

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

bei der gegenüber f nur die Zielmenge ersetzt wird.

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

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

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

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

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

[49] Wir sagen damit insbesondere, dass X und Y Mengen sind.
[50] Hierbei bedeutet $\frac{\pi}{2}\mathbb{Z}$ die Menge der ganzzahligen Vielfachen von $\frac{\pi}{2}$.

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

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

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

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

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

Dann ist

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

△

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:

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

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

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

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

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

Zum Beweis von (6.4a):

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

Zum Beweis von (6.4c):

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

□

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

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

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

$$f(A \cap B) = f(\emptyset) = \emptyset,$$
$$\text{aber} \quad f(A) \cap f(B) = \{0\} \cap \{0\} = \{0\}.$$ △

§ 6.1 Injektivität und Surjektivität

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

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

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

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

Äquivalent dazu ist

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

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

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

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

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

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

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 3.2. □

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

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

(*i*) Die Funktion
$$\mathbb{R} \ni x \mapsto x^2 \in \mathbb{R}$$
ist nicht surjektiv und nicht injektiv.

(*ii*) Die Funktion
$$\mathbb{R} \ni x \mapsto x^2 \in \mathbb{R}_{\geqslant 0}$$
ist surjektiv, aber nicht injektiv. Hierbei ist $\mathbb{R}_{\geqslant 0} = \{x \in \mathbb{R} \mid x \geqslant 0\}$ die Menge der nichtnegativen reellen Zahlen.

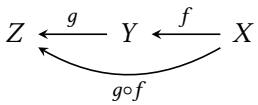
(*iii*) Die Funktion
$$\mathbb{R}_{\geqslant 0} \ni x \mapsto x^2 \in \mathbb{R}$$
ist injektiv, aber nicht surjektiv.

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

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

Definition 6.13 (Komposition von Funktionen)**.**
Es seien $f\colon X \to Y$ und $g\colon Y \to Z$ Funktionen. Die Funktion
$$X \ni x \mapsto h(x) \coloneqq g(f(x)) \in Z$$
heißt die **Komposition** (englisch: composition, lateinisch: componere: zusammenstellen), die **Hintereinanderausführung**, die **Verknüpfung** oder die **Verkettung** von f und g. Sie wird auch mit $h = g \circ f$ bezeichnet. Um die Reihenfolge klar zu benennen, sagt man auch „g **nach** f“. △

Wir können den Sachverhalt aus Definition 6.13 auch durch



illustrieren.

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

Beispiel 6.14 (Komposition von Funktionen)**.**
Es seien
$$\mathbb{R} \ni x \mapsto f(x) \coloneqq x^2 \in \mathbb{R},$$
$$\mathbb{R} \ni x \mapsto g(x) \coloneqq x + 1 \in \mathbb{R}.$$
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
$$\mathbb{R} \ni x \mapsto (g \circ f)(x) \coloneqq x^2 + 1 \in \mathbb{R},$$
$$\mathbb{R} \ni x \mapsto (f \circ g)(x) \coloneqq (x+1)^2 \in \mathbb{R}.$$
△

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

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f, \tag{6.5}$$
$$f|_A = f \circ i_{A\to X} \qquad \text{für } A \subseteq X, \tag{6.6}$$
$$f = (i_{Y\to B} \circ f)|^Y \qquad \text{für } B \supseteq Y. \tag{6.7}$$

△

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

Beweis. Für $x \in X$ gilt

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

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

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

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

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

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

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

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

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

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

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

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

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

Ende der Vorlesung 5

§ 6.2 Umkehrabbildung

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

(*i*) f ist bijektiv.

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

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

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

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

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

sowie

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

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

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

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

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

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

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

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

△

Satz 6.21 (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 die Umkehrfunktion ist gegeben durch

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

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

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

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

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

Lemma 6.22 (Charakterisierung der Injektivität)**.**

Es sei $f\colon X \to Y$ 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.

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

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

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

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. □

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

§ 6.3 Mächtigkeit von Mengen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Beweis. Es sei $n = \#(X \setminus \{x\}) \in \mathbb{N}_0$. Es gibt also eine bijektive Abbildung $\widehat{f}\colon \{1, \dots, n\} \to X \setminus \{x\}$. 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., $\#X = n + 1 = \#(X \setminus \{x\}) + 1$. □

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

Satz 6.27 (Funktionen auf endlichen Mengen)**.**

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

(*i*) f ist injektiv.

(*ii*) f ist surjektiv.

(*iii*) f ist bijektiv.

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

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

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

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

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

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

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

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

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

Wir haben jetzt Aussage (*i*) ⇔ Aussage (*ii*) bewiesen. Da die Bijektivität sich aus Surjektivität und Injektivität zusammensetzt, gilt auch Aussage (*i*) ⇔ Aussage (*ii*) ⇔ Aussage (*iii*). □

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

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

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

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

§ 6.4 Familien und Folgen

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

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

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

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

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

Bemerkung 6.30 (Familien und Mengen)**.**

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

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

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

Beispiel 6.31 (Folge)**.**
Die Abbildung

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

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

§ 6.5 Das Auswahlaxiom

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

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

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

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

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

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

△

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

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

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

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

$\mathbb{R}^{\mathbb{N}}$ die Menge aller Folgen mit Werten in $\mathbb{R}$,

$\{0,1\}^A$ die Menge aller $\{0,1\}$-wertigen (binären) Funktionen auf einer Menge A.

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

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

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

(*i*) Es gilt das Auswahlaxiom.

(*ii*) Ist I eine beliebige Menge und $(A_i)_{i\in I}$ eine Familie nichtleerer Mengen, so ist das kartesische Produkt $\bigtimes_{i\in I} A_i$ eine nichtleere Menge.

(*iii*) Jede Äquivalenzrelation besitzt ein vollständiges Repräsentantensystem.

(*iv*) Es sei $f\colon X \to Y$ eine beliebige Funktion. Dann sind äquivalent:

  (a) f ist surjektiv.

  (b) Es existiert eine Abbildung $h\colon Y \to X$ mit der Eigenschaft $f \circ h = \mathrm{id}_Y$. Eine solche Abbildung heißt eine **Rechtsinverse** (englisch: right inverse) von f. Sie ist notwendig injektiv.

(*v*) Es gilt das Lemma von Zorn 6.35.

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

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

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

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

Ende der Vorlesung 6

Ende der Woche 3

[56] englisch: Zorn's lemma
[57] X kann also nicht die leere Menge sein.

Kapitel 2 Algebraische Strukturen

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

§ 7 Halbgruppen und Gruppen

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

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

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

Beispiel 7.2 (Verknüpfung)**.**

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

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

Quizfrage 7.1: Wo kommen die Definitionen dieser Verknüpfungen her?

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

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

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

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

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

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

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

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

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

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

§ 7.1 Halbgruppen

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

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

△

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

Beispiel 7.4 (Halbgruppen)**.**
Beispiele für Halbgruppen sind:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$e_1 = e_1 \star e_2 = e_2. \qquad \square$$

Beispiel 7.8 (Halbgruppen mit und ohne neutrale Elemente)**.**

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

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

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

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

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

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

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

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

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

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

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

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

Beispiel 7.10 (Rechts- und Linkstranslation)**.**

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

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

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

während die Linkstranslation mit g gegeben ist durch

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

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

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

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

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

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

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

Beweis. Es gilt

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

□

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

Bemerkung 7.13 (abkürzende Schreibweisen)**.**

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

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

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

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

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

Es gilt

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

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

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

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

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

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

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

Es gilt

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

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

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

Beispiel 7.14 (invertierbare Elemente)**.**

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

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

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

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

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

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

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

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

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

Ende der Vorlesung 7

§ 7.2 Gruppen

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

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

Beispiel 7.16 (Gruppen und Gegenbeispiele)**.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

für $a, b_1, b_2 \in G$.

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

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

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

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

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

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

Beweis. Aussage (*i*):

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

Die Aussage (7.10b) folgt analog.

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

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

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

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

□

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

Lemma 7.18 (Gruppenkriterium mit Rechts- und Linkstranslationen („**Sudoku-Kriterium**“))**.**

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

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

Beweis. Dieser Beweis ist Teil von Hausaufgabe 4.3. □

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

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

gilt. △

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

Weitere Beispiele folgen in der Übung.

§ 7.3 Die symmetrische Gruppe

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

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

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

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

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

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

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

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

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

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

ist S_3 wie erwartet tatsächlich nicht kommutativ. △

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

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

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

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

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

Transpositionen sind also selbstinvers.

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

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

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

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

ist eine Komposition von $r = 0$ Transpositionen.

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

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

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

□

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

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

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

(*ii*) Die Zahl[4]

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

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

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

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

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

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

Die Permutation

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

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

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

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

△

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

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

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

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

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

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

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

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

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

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

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

Beweis. Wir führen den Beweis in drei Schritten.

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

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

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

gezeigt.

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

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

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

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

Schritt 3: Schließlich können wir den allgemeinen Fall zeigen.

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

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

$$\begin{aligned}
&\operatorname{sgn}\big(\sigma_1\circ\sigma_2\big)\\
&\quad= \operatorname{sgn}\big(\tau_1\circ\cdots\circ\tau_r\circ\sigma_2\big)\\
&\quad= (\operatorname{sgn}\tau_1)\cdot\operatorname{sgn}\big(\cdots\circ\tau_r\circ\sigma_2\big)\\
&\quad= \cdots\\
&\quad= (\operatorname{sgn}\tau_1)\cdots(\operatorname{sgn}\tau_r)(\operatorname{sgn}\sigma_2)\\
&\quad= \cdots\\
&\quad= \operatorname{sgn}\big(\tau_1\circ\cdots\circ\tau_r\big)\cdot\operatorname{sgn}(\sigma_2).
\end{aligned}$$

□

Folgerung 7.30 (zu Satz 7.29)**.**
Es sei $n \in \mathbb{N}$ und σ eine Permutation in S_n.

(*i*) Ist $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ dargestellt als Komposition[5] von $s \in \mathbb{N}_0$ Permutationen $\sigma_i \in S_n$, so gilt $\operatorname{sgn}\sigma = (\operatorname{sgn}\sigma_1)\cdots(\operatorname{sgn}\sigma_s)$.

(*ii*) Ist insbesondere $\sigma = \tau_1 \circ \cdots \circ \tau_r$ dargestellt als Komposition von $r \in \mathbb{N}$ Transpositionen in S_n, so gilt $\operatorname{sgn}\sigma = (-1)^r$.

(*iii*) Es gilt $\operatorname{sgn}\mathrm{id} = 1$.

(*iv*) Es gilt $\operatorname{sgn}\sigma = \operatorname{sgn}\sigma^{-1}$.

[5] Vereinbarungsgemäß ist die Verknüpfung von null Permutationen das neutrale Element in S_n, also die identische Abbildung id.

Beweis. Nach Satz 7.29 ist das Signum einer Komposition von zwei Permutationen gleich dem Produkt der Signa der beiden Faktoren. Wie im Beweis von Satz 7.29 können wir die Aussage leicht auf mehr als zwei Faktoren ausdehnen. Die Fälle $s = 0$ und $s = 1$ sind trivial. Das zeigt Aussage (i).

Das Signum einer Transposition ist nach Lemma 7.28 gleich -1. Aussage (ii) folgt damit aus Aussage (i).

Die identische Abbildung ist Produkt von null Transpositionen, also gilt $\operatorname{sgn} \mathrm{id} = (-1)^0 = 1$, also Aussage (iii).

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. Das zeigt Aussage (iv). □

Ende der Vorlesung 8

Ende der Woche 4

§ 7.4 Untergruppen

Definition 7.31 (Untergruppe)**.**
Es sei $(G, \star)$ eine Gruppe.

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

(ii) Eine bzgl. $\star$ abgeschlossene Teilmenge $U \subseteq G$ heißt eine **Untergruppe** (englisch: subgroup) von $(G, \star)$, wenn $(U, \star_U)$ selbst wieder eine Gruppe ist. Manchmal schreibt man dies als $(U, \star_U) \leqslant (G, \star)$.

(iii) Eine Untergruppe $(U, \star_U)$ von $(G, \star)$ heißt **echt** (englisch: proper subgroup), wenn $U \subsetneq G$ gilt. △

Beachte: Die Assoziativität wird von $\star$ auf $\star_U$ vererbt. Ist $(G, \star)$ abelsch, dann auch $(U, \star)$.

Lemma 7.32 (neutrale und inverse Elemente in einer Untergruppe)**.**
Es sei $(U, \star_U)$ eine Untergruppe der Gruppe $(G, \star)$. Dann ist das neutrale Element e_U von $(U, \star_U)$ gleich dem neutralen Element e von $(G, \star)$. Außerdem gilt für alle $a \in U$, dass das Inverse von a in U übereinstimmt mit dem Inversen von a in G.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 5.1. □

Aufgrund dieser Erkenntnis benötigen wir also keine neue Notation für das neutrale Element und die Inversen in einer Untergruppe. Außerdem schreiben wir ab jetzt einfach $\star$ statt $\star_U$.

Die Prüfung einer Teilmenge $U \subseteq G$ auf die Untergruppen-Eigenschaft lässt sich mit folgendem Kriterium abkürzen:

Satz 7.33 (Untergruppenkriterium)**.**
Es sei $(G, \star)$ eine Gruppe und $U \subseteq G$. Dann sind äquivalent:

(*i*) $(U, \star)$ ist eine Untergruppe von $(G, \star)$.

(*ii*) $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a \star b' \in U$.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $(U, \star)$ eine Untergruppe von $(G, \star)$. Dann enthält U notwendigerweise das neutrale Element e von $(G, \star)$, da es nach Lemma 7.32 auch das neutrale Element in $(U, \star)$ ist. Für $a, b \in U$ gilt $b' \in U$ nach Lemma 7.32. Da U bzgl. $\star$ abgeschlossen ist, folgt $a \star b' \in U$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*):

Schritt 1: U enthält das neutrale Element e von $(G, \star)$:

Da U nichtleer ist, existiert ein $a \in U$. Mit dem dazu inversen Element a' gilt aufgrund der Voraussetzung $a \star a' \in U$, also $e \in U$ für das neutrale Element e von $(G, \star)$.

Schritt 2: U enthält die Inversen seiner Elemente:

Es sei $a \in U$, dann gilt $a' = e \star a'$, und aufgrund der Voraussetzung liegt $a' \in U$.

Schritt 3: U ist abgeschlossen bzgl. $\star$:

Für $a, b \in U$ liegt auch $b' \in U$, also ist $a \star b = a \star (b')'$ aufgrund der Voraussetzung ebenfalls ein Element von U.

Zusammenfassend haben wir also gezeigt, dass U bzgl. $\star$ abgeschlossen ist (**Schritt** 3), also bildet $(U, \star)$ eine Halbgruppe. Weiter zeigt **Schritt** 1, dass $(U, \star)$ ein Monoid mit dem neutralen Element e von $(G, \star)$ ist. Schließlich zeigt **Schritt** 2, dass alle Elemente von U ein Inverses in U besitzen, also ist $(U, \star)$ eine Gruppe und wegen $U \subseteq$ eine Untergruppe von $(G, \star)$. □

Quizfrage 7.9: Könnte man an Stelle von Aussage (*ii*) in Satz 7.33 äquivalent auch $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a' \star b \in U$ fordern?

Beispiel 7.34 (Untergruppen)**.**

(*i*) Es sei $(G, \star)$ eine Gruppe mit neutralem Element e. Dann sind $(\{e\}, \star)$ und $(G, \star)$ Untergruppen von $(G, \star)$. Diese heißen die **trivialen Untergruppe** (englisch: trivial subgroups).

(*ii*) $(\mathbb{R}_{>0}, \cdot)$ ist eine Untergruppe von $(\mathbb{R}_{\neq 0}, \cdot)$.

(*iii*) Für jede Zahl $m \in \mathbb{N}$ ist $m\mathbb{Z} := \{m z \mid z \in \mathbb{Z}\}$ mit der Verknüpfung + eine Untergruppe der Gruppe $(\mathbb{Z}, +)$.

(*iv*) Für $n \geqslant 2$ ist

$$\begin{aligned} A_n &:= \{\sigma \in S_n \mid \sigma \text{ ist Komposition einer geraden Anzahl von Transpositionen}\} \\ &= \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\} \end{aligned} \tag{7.20}$$

eine Untergruppe von S_n, genannt die **alternierende Gruppe** (englisch: alternating group) vom Grad n. Sie hat $\frac{1}{2}n!$ Elemente.

(*v*) In S_3 besteht die alternierende Untergruppe A_3 in der Notation von Beispiel 7.22 gerade aus $\{\sigma_0, \sigma_1, \sigma_2\}$. Diese entsprechen bei Interpretation als Kongruenzabbildungen eines gleichseitigen Dreiecks auf sich selbst gerade den Drehungen. △

Quizfrage 7.10: Können Sie eine Gruppe finden, die außer den trivialen Untergruppen keine weiteren Untergruppen besitzt?

Beachte: Die Menge der Untergruppen einer Gruppe $(G, \star)$ sind bzgl. der Eigenschaft „ist Untergruppe von“ partiell geordnet.

Lemma 7.35 (Durchschnitt von Untergruppen)**.**
Es sei $(G, \star)$ eine Gruppe und $(U_i, \star)_{i \in I}$ eine Familie von Untergruppen mit der nichtleeren Indexmenge I. Dann ist auch $\bigcap_{i \in I} U_i$ mit $\star$ eine Untergruppe von $(G, \star)$.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 5.1. □

Definition 7.36 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe, Ordnung eines Elements)**.**
Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$.

(*i*) Dann heißt

$$\langle E \rangle := \bigcap \left\{ U \,\middle|\, (U, \star) \text{ ist Untergruppe von } (G, \star) \text{ und } E \subseteq U \right\} \tag{7.21}$$

die von E **erzeugte Untergruppe** (englisch: subgroup generated by E) in $(G, \star)$.

Beachte: Bezeichnen wir mit $\mathcal{R}$ die Menge auf rechten Seite von (7.21), über die der Durchschnitt gebildet wird, dann ist $\langle E \rangle$ das Minimum der Menge $\mathcal{R}$ bzgl. der Inklusionshalbordnung und sogar das Minimum der Menge $\mathcal{R}$ bzgl. der Halbordnung „ist Untergruppe von“.

Ist speziell $E = \{a\}$ für ein $a \in G$, so schreiben wir auch $\langle a \rangle$ statt $\langle \{a\} \rangle$ und nennen $\langle a \rangle$ die von a erzeugte **zyklische Untergruppe** (englisch: cyclic subgroup) von $(G, \star)$.

(*ii*) Gilt $\langle E \rangle = G$, dann heißt E ein **Erzeugendensystem** (englisch: generating set) von $(G, \star)$. Falls ein endliches Erzeugendensystem von G existiert, so heißt G **endlich erzeugt** (englisch: finitely generated).

(*iii*) Die Gruppe $(G, \star)$ heißt **zyklisch** (englisch: cyclic), wenn es ein $a \in G$ gibt, sodass gilt: $\langle a \rangle = G$. In diesem Fall heißt a ein **Erzeuger** (englisch: generator) von G.

(*iv*) Ein Element $a \in G$ heißt von **Ordnung** $n \in \mathbb{N}$ (englisch: order), wenn $n \in \mathbb{N}$ die kleinste Zahl ist, für die (in multiplikativer Notation) $a^n = 1$ gilt. Falls kein $n \in \mathbb{N}$ existiert, sodass $a^n = 1$ ist, so heißt a von **unendlicher Ordnung** (englisch: infinite order). Wir schreiben $\operatorname{ord}(a) = n$ bzw. $\operatorname{ord}(a) = \infty$. △

Satz 7.37 (Darstellung der erzeugten Untergruppe)**.**
Es sei $(G, \star)$ eine Gruppe und $E \subseteq G$. Dann gilt für die von E erzeugte Untergruppe:

$$\langle E \rangle = \left\{ a_1 \star \cdots \star a_n \,\middle|\, \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \; (a_i \in E \cup E') \right\}, \tag{7.22}$$

wobei E' die Menge der Inversen von E bezeichnet. (Im Fall $n = 0$ interpretieren wir wie üblich die Verknüpfung von null Elementen in der rechten Menge als das neutrale Element e. Insbesondere im Fall $E = \emptyset$ ist also $\langle E \rangle = \{e\}$.)

Beweis. Zur Abkürzung bezeichnen wir die Menge auf der rechten Seite von (7.22) mit M. Wir führen den Beweis in zwei Schritten.

Schritt 1: $\langle E\rangle \supseteq M$: Es sei U eine beliebige Untergruppe von G, die im Durchschnitt (7.21) vorkommt. U enthält also E als Teilmenge. Da U eine Untergruppe ist, enthält U auch E'. Da schließlich U abgeschlossen bzgl. $\star$ ist, enthält U auch alle Verknüpfungen endlich vieler Elemente aus $E \cup E'$. Also gilt $U \supseteq M$. Da dies für jede beliebige Untergruppe aus dem Durchschnitt in (7.21) gilt, gilt auch $\langle E\rangle \supseteq M$.

Schritt 2: $\langle E\rangle \subseteq M$: Wir zeigen zunächst, dass M selbst eine Untergruppe von G ist. Dazu überprüfen wir das Untergruppenkriterium (Satz 7.33). Offensichtlich ist $M \neq \emptyset$, denn M enthält mindestens e. Sind $a_1 \star \cdots \star a_n$ und $b_1 \star \cdots \star b_m$ zwei Elemente aus M, so ist auch $(a_1 \star \cdots \star a_n) \star (b_1 \star \cdots \star b_m)'$ ein Element aus M. Also ist M eine Untergruppe von G. Zusätzlich ist klar, dass $E \subseteq M$ gilt. (**Quizfrage 7.11:** Details?) Das heißt, M ist eine derjenigen Untergruppen von G, über die in der Definition von $\langle E\rangle$ der Durchschnitt gebildet wird. Folglich gilt $\langle E\rangle \subseteq M$. □

Beispiel 7.38 (erzeugte Untergruppe, Erzeugendensystem, zyklische Gruppe, Ordnung eines Elements)**.**

(*i*) In der Gruppe $(\mathbb{Z}, +)$ erzeugt das Element $m \in \mathbb{Z}$ die zyklische Untergruppe $\langle m\rangle = m\mathbb{Z}$.

(*ii*) Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch. Sie hat die Erzeuger 1 und -1, es gilt also $\langle 1\rangle = \langle -1\rangle = \mathbb{Z}$.

(*iii*) In S_3 gilt mit den Bezeichnungen aus Beispiel 7.22, also

$$\sigma_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad \sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad \sigma_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \qquad \text{(Drehungen)}$$

$$\sigma_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad \sigma_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \quad \sigma_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \qquad \text{(Spiegelungen)}$$

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 7.34. Wegen $\sigma_2^2 = \sigma_1$ und $\sigma_2^3 = \sigma_0$ gilt auch $\langle \sigma_2\rangle = A_3$. Wegen $\sigma_3^2 = \sigma_4^2 = \sigma_5^2 = \mathrm{id}_{\{1,2,3\}}$ gilt $\langle \sigma_3\rangle = \{\sigma_0, \sigma_3\}$, $\langle \sigma_4\rangle = \{\sigma_0, \sigma_4\}$ und $\langle \sigma_5\rangle = \{\sigma_0, \sigma_5\}$. Wollen wir ganz S_3 erzeugen, so müssen wir mindestens zwei Permutationen auswählen. Beispielsweise ist $\{\sigma_1, \sigma_3\}$ (eine Drehung, eine Spiegelung) ein Erzeugendensystem von S_3. △

Bemerkung 7.39 (abkürzende Schreibweisen)**.**
Es sei $(H, \star)$ eine Halbgruppe, $a \in H$ sowie $A, B \subseteq H$. Zur Abkürzung vereinbaren wir folgende Schreibweisen:

$$a \star B := \{a \star b \mid b \in B\}, \tag{7.23a}$$

$$B \star a := \{b \star a \mid b \in B\}, \tag{7.23b}$$

$$A \star B := \{a \star b \mid a \in A,\ b \in B\}, \tag{7.23c}$$

$$A' := \{a' \mid a \in A \text{ ist invertierbar}\}. \tag{7.23d}$$

Wenn A bzw. B die leere Menge ist, ist das Ergebnis in allen obigen Fällen die leere Menge. Mit Hilfe dieser Abkürzungen können wir z. B. das Untergruppenkriterium Satz 7.33 (*ii*) als $U \neq \emptyset$ und $U \star U' \subseteq U$ formulieren. △

Ende der Vorlesung 9

§ 7.5 Untergruppen induzieren Äquivalenzrelationen

Lemma 7.40 (von Untergruppe induzierte Äquivalenzrelationen)**.**
Es sei $(G, \star)$ eine Gruppe und $(U, \star)$ eine Untergruppe. Dann sind durch

$$a \sim^U b \quad \Leftrightarrow \quad b \in a \star U \quad \Leftrightarrow \quad a' \star b \in U \tag{7.24a}$$
$$a \,{}^U\!\sim b \quad \Leftrightarrow \quad a \in U \star b \quad \Leftrightarrow \quad a \star b' \in U \tag{7.24b}$$

für $a, b \in G$ zwei Äquivalenzrelationen auf G erklärt.[6] Für die Äquivalenzklassen gilt:

$$[a]_{\sim^U} = a \star U \tag{7.25a}$$
$$[a]_{U\sim} = U \star a. \tag{7.25b}$$

Jede der Äquivalenzklassen $[a]_{\sim^U}$ und $[a]_{U\sim}$ ist gleichmächtig zu U.

Beweis. Wir zeigen zunächst, dass die beiden angegebenen Bedingungen in (7.24) tatsächlich äquivalent sind. Wir haben

$$\begin{aligned}
& b \in a \star U \\
\Leftrightarrow \quad & \exists c \in U \ (b = a \star c) \\
\Leftrightarrow \quad & \exists c \in U \ (a' \star b = a' \star a \star c) \quad \text{„}\Leftarrow\text{“ folgt aus der Kürzungsregel (7.10a)} \\
\Leftrightarrow \quad & \exists c \in U \ (a' \star b = c) \\
\Leftrightarrow \quad & a' \star b \in U.
\end{aligned}$$

Wir weisen nun für $a \sim^U b$ die Eigenschaften einer Äquivalenzrelation nach. Das neutrale Element von U und G wird wieder mit e bezeichnet.

Schritt 1: $\sim^U$ ist reflexiv:

Es sei $a \in G$, dann ist $a' \star a = e \in U$, da U Untergruppe ist.

Schritt 2: $\sim^U$ ist symmetrisch:

Es gelte $a \sim^U b$, also $a' \star b \in U$. Dann ist auch das Inverse $(a' \star b)' \in U$, da U Untergruppe ist. Für das Inverse gilt nach Satz 7.17 *(iii)* und *(iv)*:

$$(a' \star b)' = b' \star (a')' = b' \star a \in U.$$

Das heißt aber $b \sim^U a$.

Schritt 3: $\sim^U$ ist transitiv:

Es gelte $a \sim^U b$ und $b \sim^U c$, also $a' \star b \in U$ und $b' \star c \in U$. Aufgrund der Untergruppeneigenschaft von U ist auch $a' \star b \star b' \star c = a' \star c \in U$. Das heißt aber $a \sim^U c$.

Die Darstellung der Äquivalenzklasse (7.25a) folgt sofort aus (7.24a).

Um zu zeigen, dass U und $[a]_{\sim^U} = a \star U$ gleichmächtig sind (Definition 6.23), betrachten wir die Abbildung $U \ni b \mapsto a \star b \in a \star U$. Diese Abbildung ist nach Definition von $a \star U$ surjektiv. Außerdem ist sie injektiv, denn aus $a \star b = a \star c$ folgt mit der Kürzungsregel (7.10a) $b = c$.

Der Beweis für (7.24b) und (7.25b) geht analog. □

[6] Für diese Relationen gibt es in der Literatur keine einheitliche Notation.

Die Äquivalenzklasse $[a]_{\sim^U} = a \star U$ heißt auch die **Linksnebenklasse** (englisch: left coset) von U nach a.[7] Weil $\sim^U$ eine Äquivalenzrelation ist, bilden die Linksnebenklassen der Untergruppe U eine Partition der Gruppe G (Satz 5.19). Man notiert die Quotientenmenge als $G / \sim^U$ oder auch als G / U.

Die Äquivalenzklasse $[a]_{{}^U\sim} = U \star a$ heißt auch die **Rechtsnebenklasse** (englisch: right coset) von U nach a. Weil auch ${}^U\sim$ eine Äquivalenzrelation ist, bilden auch die Rechtsnebenklassen der Untergruppe U eine Partition der Gruppe G. Man notiert die Quotientenmenge als $G / {}^U\sim$ oder auch als $U \backslash G$.

Folgerung 7.41 (zu Lemma 7.40)**.**

Es sei $(G, \star)$ eine abelsche Gruppe und $(U, \star)$ eine Untergruppe. Dann sind die Äquivalenzrelationen $a \sim^U b$ und $a \,{}^U\!\sim b$ identisch. Entsprechend gilt für die Nebenklassen $a \star U = U \star a$ für alle $a \in G$.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 5.3. □

Wann immer $a \sim^U b$ und $a \,{}^U\!\sim b$ identisch sind, schreiben wir auch einfach $a \overset{U}{\sim} b$ und sprechen von **Nebenklassen** (englisch: cosets) $[a]_{\overset{U}{\sim}} = U \star a = a \star U$ von U.

Beispiel 7.42 (Nebenklassen)**.**

(*i*) In der abelschen Gruppe $(\mathbb{Z}, +)$ erzeugt die Untergruppe $m\mathbb{Z}$ für $m \in \mathbb{N}$ gerade die Kongruenzrelation modulo m, d. h., $\overset{m\mathbb{Z}}{\sim}$ und $\overset{m}{\equiv}$ stimmen überein. Die Nebenklassen von $m\mathbb{Z}$ gilt (auch **Restklassen modulo** m genannt, vgl. Beispiel 5.16)

$$[a] = \{a + n\,m \mid n \in \mathbb{Z}\} = a + m\mathbb{Z}$$

partitionieren die ganzen Zahlen $\mathbb{Z}$ in m gleichmächtige Restklassen, $[0], [1], \ldots, [m-1]$.

(*ii*) Die Standardkonstruktion einer nicht messbaren Teilmenge von $\mathbb{R}$ (Satz von Vitali) verwendet die Nebenklassen von $\mathbb{Q}$ in der abelschen Gruppe $(\mathbb{R}, +)$, zusammen mit dem Auswahlaxiom. △

Aus Lemma 7.40 folgt der folgende wichtige **Satz von Lagrange** (englisch: Lagrange's theorem) der Gruppentheorie:

Satz 7.43 (Satz von Lagrange)**.**

Es sei $(G, \star)$ eine endliche Gruppe und $(U, \star)$ eine Untergruppe. Dann gilt $\#U \mid \#G$, d. h., die Kardinalität der Untergruppe ist ein Teiler der Kardinalität der Gruppe.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 5.3. □

[7] Merke: Bei den *Links*nebenklassen $a \star U$ steht der Repräsentant a *links* vom U. Im Relationszeichen $\sim^U$ steht die Tilde $\sim$ ebenfalls links vom U.

§ 8 Homomorphismen von Halbgruppen und Gruppen

Literatur: Beutelspacher, 2014, Kapitel 9.2.3, Fischer, Springborn, 2020, Kapitel 2.2

Homomorphismen (englisch: homomorphisms, altgriechisch: *ομος*: gemeinsam, altgriechisch: *μορφή*: Form) sind die **strukturverträglichen Abbildungen** (englisch: structurally compatible maps) zwischen algebraischen Strukturen. In diesem Abschnitt geht es speziell um Homomorphismen von Halbgruppen und Gruppen.

Definition 8.1 (Halbgruppenhomomorphismus)**.**
Es seien $(H_1, \star)$ und $(H_2, \square)$ zwei Halbgruppen.

(*i*) Eine Abbildung $f\colon H_1 \to H_2$ heißt **strukturverträglich** oder ein **(Halbgruppen-)Homomorphismus** (englisch: semigroup homomorphism) von $(H_1, \star)$ in $(H_2, \square)$, wenn gilt:

$$f(a \star b) = f(a) \square f(b) \quad \text{für alle } a, b \in H_1. \tag{8.1}$$

(*ii*) Im Fall $(H_1, \star) = (H_2, \square)$ sprechen wir auch von einem **(Halbgruppen-)Endomorphismus** (englisch: semigroup endomorphism, altgriechisch: *ένδον*: innen).

(*iii*) Ist $f\colon H_1 \to H_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Halbgruppen-)Isomorphismus** (englisch: semigroup isomorphism, altgriechisch: *ίσος*: gleich). In diesem Fall nennen wir $(H_1, \star)$ und $(H_2, \square)$ auch zueinander **isomorphe Halbgruppen** (englisch: isomorphic semigroups) und schreiben

$$(H_1, \star) \cong (H_2, \square).$$

(*iv*) Im Fall $(H_1, \star) = (H_2, \square)$ und $f\colon H_1 \to H_2$ bijektiv sprechen wir auch von einem **(Halbgruppen-)Automorphismus** (englisch: semigroup automorphism, altgriechisch: *αυτος*: selbst).[8] △

Quizfrage 8.1: Welche Art von Relation ist die Isomorphie auf der Klasse aller Halbgruppen?

Bemerkung 8.2 (Halbgruppenhomomorphismus als kommutatives Diagramm)**.**
Wir können den Sachverhalt, dass $f\colon (H_1, \star) \to (H_2, \square)$ ein Halbgruppenhomomorphismus ist, durch das folgende **kommutative Diagramm** (englisch: commutative diagram) ausdrücken:[9]

$$\begin{array}{ccc} H_1 \times H_1 & \xrightarrow{f \times f} & H_2 \times H_2 \\ \downarrow{\scriptstyle \star} & & \downarrow{\scriptstyle \square} \\ H_1 & \xrightarrow{f} & H_2 \end{array}$$

Ein solches Diagramm heißt **kommutativ** (englisch: commutative diagram), wenn alle Pfade mit demselben Ausgangs- und demselben Endpunkt dasselbe Ergebnis produzieren. △

[8] Ein Automorphismus ist somit ein bijektiver Endomorphismus oder auch ein Isomorphismus von einer Halbgruppe/Monoid/Gruppe auf sich selbst.
[9] Die Abbildung $f \times f$ ist dabei definiert durch $f \times f\colon H_1 \times H_1 \ni (a, b) \mapsto (f(a), f(b)) \in H_2 \times H_2$.

Wenn $(M_1, \star)$ und $(M_2, \square)$ beides Monoide sind, so können wir ganz analog zu Definition 8.1 die Begriffe **(Monoid-)Homomorphismus**, **-Endomorphismus**, **-Isomorphismus** und **-Automorphismus** (englisch: monoid homomorphism, endomorphism, isomorphism, automorphism) definieren. Zusätzlich zu (8.1) fordert man dabei aber noch, dass für die Einselemente gilt:

$$f(e_1) = e_2. \tag{8.2}$$

Die Monoide $(M_1, \star)$ und $(M_2, \square)$ heißen zueinander **isomorph**, wenn es zwischen ihnen einen Monoidisomorphismus gibt. Wir schreiben dann $(M_1, \star) \cong (M_2, \square)$.

Sind $(G_1, \star)$ und $(G_2, \square)$ beides Gruppen, so ergeben sich die Begriffe **(Gruppen-)Homomorphismus**, **-Endomorphismus**, **-Isomorphismus** und **-Automorphismus** (englisch: group homomorphism, endomorphism, isomorphism, automorphism). Hier wiederum muss man die Bedingung (8.2) nicht separat fordern, denn sie folgt aus (8.1); siehe Lemma 8.5. Die Gruppen $(G_1, \star)$ und $(G_2, \square)$ heißen zueinander **isomorph**, wenn es zwischen ihnen einen Gruppenisomorphismus gibt. Wir schreiben dann $(G_1, \star) \cong (G_2, \square)$.

Bemerkung 8.3 (zu Definition 8.1)**.**
Zwei zueinander isomorphe Halbgruppen/Monoide/Gruppen können und müssen, was ihre algebraischen Eigenschaften als Halbgruppen/Monoide/Gruppen angeht, nicht unterschieden werden. △

Beispiel 8.4 (Homomorphismen von Halbgruppen und Gruppen)**.**

(*i*) Es sei Σ eine nichtleere Menge und $(\Sigma^*, \circ)$ die Halbgruppe der Tupel über Σ mit der Konkatenation $\circ$, siehe Beispiel 7.4. Die Abbildung $\#\colon (\Sigma^*, \circ) \to (\mathbb{N}_0, +)$, die die Kardinalität eines Tupels angibt, ist ein Monoidhomomorphismus, denn es gilt

$$\#\big((x_1, \dots, x_n) \circ (y_1, \dots, y_m)\big) = \#(x_1, \dots, x_n) + \#(y_1, \dots, y_m) = n + m$$
$$\text{und} \quad \#() = 0.$$

Genau dann, wenn Σ einelementig ist, ist $\#$ auch bijektiv, also ein Monoidisomorphismus.

(*ii*) Für $a > 0$, $a \neq 1$ ist $\log_a\colon (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ ist wegen

$$\log_a(x \cdot y) = \log_a(x) + \log_a(y)$$

ein Gruppenhomomorphismus. Weiter ist $\log_a$ bijektiv, also sogar ein Gruppenisomorphismus.

(*iii*) Zwischen beliebigen Gruppen $(G_1, \star)$ und $(G_2, \square)$ gibt es immer den **trivialen Homomorphismus** (englisch: trivial homomorphism) $f\colon G_1 \ni a \mapsto f(a) \coloneqq e_2 \in G_2$. Für einige Paare von Gruppen ist das auch der einzig mögliche Homomorphismus.

(*iv*) Für festes $n \in \mathbb{Z}$ ist die Abbildung (vgl. (7.6))

$$G \ni a \mapsto a^n \in G$$

in einer *abelschen* Gruppe $(G, \cdot)$ ein Gruppenendomorphismus.

(*v*) Die sgn-Abbildung ist ein Gruppenhomomorphismus von der symmetrischen Gruppe S_n (für festes $n \in \mathbb{N}$) in die Gruppe $(\{\pm 1\}, \cdot)$, denn es gilt nach Satz 7.29

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

Genau für $n = 2$ ist sgn auch bijektiv, also ein Gruppenisomorphismus.

(*vi*) Die in Beispiel 7.22 vorgenommene „Identifikation“ der symmetrischen Gruppe S_3 mit der Gruppe der Kongruenzabbildungen eines gleichseitigen Dreiecks stellt einen Gruppenisomorphismus dar.

(*vii*) Die Abbildung

$$\mathbb{R} \ni f(x) := \exp(ix) = \cos(x) + i\sin(x) \in \mathbb{C}$$

ist ein Gruppenhomomorphismus $(\mathbb{R}, +) \to (\mathbb{C}, \cdot)$, 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 die **Additionstheoreme** für die Winkelsumme

$$\cos(x+y) = \cos(x) \cdot \cos(y) - \sin(x) \cdot \sin(y) \tag{8.3a}$$
$$\sin(x+y) = \sin(x) \cdot \cos(y) + \cos(x) \cdot \sin(y). \tag{8.3b}$$

△

Lemma 8.5 (Eigenschaften von Gruppenhomomorphismen)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt:

(*i*) $f(e_1) = e_2$.

(*ii*) $(f(a))' = f(a')$.

Beweis. Es gilt

$$\begin{aligned} f(e_1) \square e_2 &= f(e_1) && \text{da } e_2 \text{ neutrales Element in } (H_2, \square) \text{ ist} \\ &= f(e_1 \star e_1) && \text{da } e_1 \text{ neutrales Element in } (H_1, \star) \text{ ist} \\ &= f(e_1) \square f(e_1) && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Die Verknüpfung dieses Ausdrucks von links mit dem Inversen von $f(e_1)$, also die Anwendung der Kürzungsregel (7.10a), zeigt $e_2 = f(e_1)$, also Aussage (*i*).

Die Aussage (*ii*) folgt aus

$$\begin{aligned} f(a') \square f(a) &= f(a' \star a) && \text{da } f \text{ Homomorphismus ist} \\ &= f(e_1) && \text{da } e_1 \text{ neutrales Element in } (H_1, \star) \text{ ist} \\ &= e_2 && \text{wegen Aussage } (i). \end{aligned}$$

Aus (7.11b) folgt nun $f(a') = (f(a))'$. □

Beachte: Gruppenhomomorphismen bilden neutrale Elemente auf neutrale Element ab und inverse Elemente auf inverse Elemente. Das Lemma 8.5 gilt i. A. nicht, wenn $(G_2, \square)$ keine Gruppe, sondern nur ein Monoid ist!

Quizfrage 8.2: Kann $f\colon (\mathbb{Z}, +) \ni n \mapsto n+1 \in (\mathbb{Z}, +)$ ein Gruppenhomomorphismus sein?

Wir wollen nun Gruppenhomomorphismen genauer studieren.

Definition 8.6 (Bild und Kern eines Gruppenhomomorphismus)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus.

(*i*) Das **Bild** (englisch: image) von f ist definiert als

$$\text{Bild}(f) \coloneqq \left\{ f(x) \in G_2 \,\middle|\, x \in G_1 \right\} = f(G_1). \tag{8.4}$$

(*ii*) Der **Kern** (englisch: kernel) von f ist definiert als

$$\text{Kern}(f) \coloneqq \left\{ x \in G_1 \,\middle|\, f(x) = e_2 \right\} = f^{-1}(\{e_2\}). \tag{8.5}$$

△

Lemma 8.7 (Bild und Kern sind Untergruppen)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus.

(*i*) $\text{Bild}(f)$ ist eine Untergruppe von $(G_2, \square)$.

(*ii*) $\text{Kern}(f)$ ist eine Untergruppe von $(G_1, \star)$.

Beweis. Aussage (*i*): Wir überprüfen das Untergruppenkriterium (Satz 7.33). Es gilt $e_2 = f(e_1)$ nach Lemma 8.5, also $e_2 \in \text{Bild}(f)$ und $\text{Bild}(f) \neq \emptyset$. Weiter seien a_2, b_2 irgendwelche Elemente in $\text{Bild}(f)$. Wir müssen zeigen: $a_2 \square b_2' \in \text{Bild}(f)$.

Nach Definition von $\text{Bild}(f)$ gibt es $a_1, b_1 \in G_1$ mit $f(a_1) = a_2$ und $f(b_1) = b_2$. Daher ist

$$\begin{aligned} a_2 \square b_2' &= f(a_1) \square (f(b_1))' && \text{nach Voraussetzung} \\ &= f(a_1) \square f(b_1') && \text{nach Lemma 8.5} \\ &= f(a_1 \star b_1') && \text{da } f \text{ Homomorphismus ist} \end{aligned}$$

und damit $a_2 \square b_2' \in \text{Bild}(f)$.

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, b irgendwelche Elemente in $\text{Kern}(f)$. Wir müssen zeigen: $a \star b' \in \text{Kern}(f)$.

$$\begin{aligned} f(a \star b') &= f(a) \square f(b') && \text{da } f \text{ Homomorphismus ist} \\ &= f(a) \square (f(b))' && \text{nach Lemma 8.5} \\ &= e_2 \square e_2' && \text{da } a, b \in \text{Kern}(f) \text{ liegen} \\ &= e_2 && \text{da } e_2' = e_2 \text{ ist.} \end{aligned}$$

Damit ist $a \star b' \in \text{Kern}(f)$ gezeigt. □

Beispiel 8.8 (Bild und Kern sind Untergruppen)**.**

(*i*) Für die Abbildung $\#\colon (\Sigma^*, \circ) \to (\mathbb{N}_0, +)$ aus Beispiel 8.4 gilt:

$$\text{Bild}(\#) = \mathbb{N}_0 \quad \text{und} \quad \text{Kern}(\#) = \{()\},$$

wobei $()$ das leere Tupel kennzeichnet.

(*ii*) Für die Abbildung $\operatorname{sgn}\colon (S_n, \circ) \to (\{\pm 1\}, \cdot)$ aus Beispiel 8.4 gilt im Fall $n \geqslant 2$:

$$\operatorname{Bild}(\operatorname{sgn}) = \{\pm 1\} \quad \text{und} \quad \operatorname{Kern}(\operatorname{sgn}) = A_n,$$

die alternierende Gruppe, vgl. (7.20).

(*iii*) Für die Abbildung $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 (\mathbb{R}_{\neq 0}, \cdot)$ gilt

$$\operatorname{Bild}(f) = \mathbb{R}_{>0} \quad \text{und} \quad \operatorname{Kern}(f) = \{\pm 1\}. \qquad \triangle$$

Lemma 8.9 (Charakterisierung der Injektivität)**.**

Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann sind äquivalent:

(*i*) f ist injektiv.

(*ii*) $\operatorname{Kern}(f) = \{e_1\}$.

(*iii*) Die einzige Lösung der Gleichung $f(a) = e_2$ ist $a = e_1$.

Beachte: Um die Injektivität einer *beliebigen* Abbildung zu zeigen, müssen wir sicherstellen, dass niemals zwei verschiedene Elemente der Definitionsmenge auf dasselbe Element in der Zielmenge abgebildet werden (Definition 6.10). Wenn wir aber wissen, dass diese Abbildung ein Gruppenhomomorphismus ist, vereinfacht sich dieser Nachweis erheblich. Wir müssen dann nur noch zeigen, dass neben dem neutralen Element e_1 kein weiteres Element auf das neutrale Element e_2 abgebildet wird.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Nach Lemma 8.5 gilt $f(e_1) = e_2$. Ist f injektiv, dann wird kein weiteres Element von G_1 auf e_2 abgebildet, also gilt $\operatorname{Kern}(f) = \{e_1\}$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Umgekehrt gelte $\operatorname{Kern}(f) = \{e_1\}$. Es seien weiter $a, b \in G_1$ mit $f(a) = f(b)$. Dann folgt

$$\begin{aligned} f(a \star b') &= f(a) \square f(b') \\ &= f(a) \square (f(b))' \\ &= f(a) \square (f(a))' \\ &= e_2, \end{aligned}$$

also $a \star b' \in \operatorname{Kern}(f) = \{e_1\}$. Daher muss $a \star b' = e_1$ gelten, also wegen der Eindeutigkeit inverser Elemente $a = b$. Das zeigt die Injektivität von f.

Die Äquivalenz von Aussage (*ii*) und Aussage (*iii*) ist einfach zu sehen, weil $\operatorname{Kern}(f)$ gerade aus den Lösungen der Gleichung $f(a) = e_2$ besteht und nach Lemma 8.5 $f(e_1) = e_2$ gilt. $\square$

Ende der Vorlesung 10

Ende der Woche 5

§ 8.1 Normalteiler

Wir hatten in Lemma 7.40 gesehen, dass jede Untergruppe $(U, \star)$ einer Gruppe $(G, \star)$ zwei Äquivalenzrelationen ${}^{U}\!\sim$ und $\sim^{U}$ auf G induziert, deren Äquivalenzklassen durch $a \star U$ bzw. $U \star a$ gegeben und die i. A. verschieden sind.

Definition 8.10 (Normalteiler)**.**
Es sei $(G, \star)$ eine Gruppe. Eine Untergruppe $(N, \star)$ heißt eine **normale Untergruppe** (englisch: normal subgroup) oder **Normalteiler** von $(G, \star)$, wenn gilt:

$$a \star N = N \star a \quad \text{für alle } a \in G. \tag{8.6}$$

Manchmal schreibt man dies als $(N, \star) \trianglelefteq (G, \star)$. △

Anders ausgedrückt ist $(N, \star)$ genau dann eine normale Untergruppe, wenn die durch sie induzierten Äquivalenzrelationen ${}^{N}\!\sim$ und $\sim^{N}$ (siehe Lemma 7.40) übereinstimmen.

Beachte: Die Relation „ist Normalteiler von“ ist zwar reflexiv und antisymmetrisch, aber im Gegensatz zur Relation „ist Untergruppe von“ i. A. nicht transitiv!

Beispiel 8.11 (Normalteiler)**.**

(*i*) In jeder Gruppe $(G, \star)$ sind die trivialen Untergruppen $(\{e\}, \star)$ und $(G, \star)$ Normalteiler.

(*ii*) In einer abelschen Gruppe $(G, \star)$ ist jede Untergruppe ein Normalteiler (Folgerung 7.41). △

Lemma 8.12 (Kerne von Gruppenhomomorphismen sind Normalteiler)**.**
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen mit den neutralen Elementen e_1 bzw. e_2. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt:

(*i*) Für alle $a \in G_1$ gilt:
$$f^{-1}(\{f(a)\}) = a \star \operatorname{Kern}(f) = \operatorname{Kern}(f) \star a.$$

(*ii*) $\operatorname{Kern}(f)$ ist ein Normalteiler von G_1.

Beachte: Das Urbild eines Elements in der Bildmenge $f(G_1)$ ist also immer eine Nebenklasse von $\operatorname{Kern}(f)$.

Beweis. Wir zeigen zunächst die Aussage (*i*) in mehreren Schritten.

Schritt 1: $f^{-1}(\{f(a)\}) \subseteq \operatorname{Kern}(f) \star a$:

Es sei $b \in f^{-1}(\{f(a)\})$, also $f(b) = f(a)$. Dann gilt also

$$\begin{aligned} e_2 &= f(b) \square (f(a))' \\ &= f(b) \square f(a') && \text{nach Lemma 8.5} \\ &= f(b \star a') && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Das heißt aber, dass $b \star a' \in f^{-1}(\{e_2\}) = \operatorname{Kern}(f)$ liegt. Mit anderen Worten, $b \in \operatorname{Kern}(f) \star a$.

Schritt 2: $f^{-1}(\{f(a)\}) \subseteq a \star \mathrm{Kern}(f)$:

Ganz analog zu **Schritt** 1 gilt auch

$$\begin{aligned} e_2 &= (f(a))' \square f(b) \\ &= f(a') \square f(b) && \text{nach Lemma 8.5} \\ &= f(a' \star b) && \text{da } f \text{ Homomorphismus ist.} \end{aligned}$$

Das heißt aber $a' \star b \in f^{-1}(\{e_2\}) = \mathrm{Kern}(f)$ und daher $b \in a \star \mathrm{Kern}(f)$.

Schritt 3: $\mathrm{Kern}(f) \star a \subseteq f^{-1}(\{f(a)\})$:

Es sei $b \in \mathrm{Kern}(f)$. Wir müssen $b \star a \in f^{-1}(\{f(a)\})$ zeigen, also $f(b \star a) = f(a)$. Das folgt aber sofort aus

$$\begin{aligned} f(b \star a) &= f(b) \square f(a) && \text{da } f \text{ Homomorphismus ist} \\ &= e_2 \square f(a) && \text{da } b \in \mathrm{Kern}(f) \text{ ist} \\ &= f(a). \end{aligned}$$

Schritt 4: $a \star \mathrm{Kern}(f) \subseteq f^{-1}(\{f(a)\})$:

Es sei $b \in \mathrm{Kern}(f)$. Wir müssen $a \star b \in f^{-1}(\{f(a)\})$ zeigen, also $f(a \star b) = f(a)$. Das folgt aber sofort aus

$$\begin{aligned} f(a \star b) &= f(a) \square f(b) && \text{da } f \text{ Homomorphismus ist} \\ &= f(a) \square e_2 && \text{da } b \in \mathrm{Kern}(f) \text{ ist} \\ &= f(a). \end{aligned}$$

Aus Lemma 8.7 wissen wir, dass $\mathrm{Kern}(f)$ eine Untergruppe von G_1 ist. Aus Aussage (i) folgt $a \star \mathrm{Kern}(f) = \mathrm{Kern}(f) \star a$ für alle $a \in G_1$, also ist $\mathrm{Kern}(f)$ ein Normalteiler von G_1. Das zeigt Aussage (ii). □

Wenn $(N, \star)$ ein Normalteiler einer Gruppe $(G, \star)$ ist, dann können wir die Faktormenge $G / \overset{N}{\sim} = G / N$ mit einer Gruppenverknüpfung $\tilde{\star}$ ausstatten. Aus der Faktormenge wird damit die **Faktorgruppe** (englisch: factor group) oder **Quotientengruppe** (englisch: quotient group) von G nach N. Man sagt auch: „Aus der Gruppe $(G, \star)$ wird der Normalteiler N ausfaktorisiert."

Satz 8.13 (Faktorgruppe)**.**
Es sei $(G, \star)$ eine Gruppe mit neutralem Element e und $(N, \star)$ einer ihrer Normalteiler. Dann gilt:

(i) Auf der Faktormenge

$$G / N = \left\{ [a] = a \star N \,\middle|\, a \in G \right\}$$

ist $\tilde{\star}$, definiert als

$$[a] \,\tilde{\star}\, [b] := [a \star b] \quad \text{für } a, b \in G, \tag{8.7}$$

eine assoziative Verknüpfung, bzgl. der $(G / N, \tilde{\star})$ eine Gruppe bildet. Das neutrale Element ist $[e] = N$, und für die Inversen gilt $[a]' = [a']$.

(*ii*) Die Abbildung

$$\pi\colon \begin{cases} G \longrightarrow G/N \\ a \longmapsto [a], \end{cases} \tag{8.8}$$

die jedem Element $a \in G$ seine Nebenklasse $[a]$ zuordnet, ist ein surjektiver Gruppenhomomorphismus. Sie heißt die **kanonische Surjektion** (englisch: canonical surjection) von G auf G/N. Es gilt $\operatorname{Kern}(\pi) = N$.

(*iii*) Wenn $(G, \star)$ abelsch ist, dann auch $(G/N, \tilde{\star})$.

Beweis. Aussage (*i*): Wir müssen zunächst zeigen, dass $\tilde{\star}$ überhaupt eine Verknüpfung auf G/N darstellt, also dass (8.7) wohldefiniert ist, da wir dort ja Bezug auf konkrete Repräsentanten $a, b \in G$ nehmen. Es seien also $a_1, a_2, b_1, b_2 \in G$ gegeben, wobei $a_1 \overset{N}{\sim} a_2$ und $b_1 \overset{N}{\sim} b_2$ angenommen wird, d. h., $a_1 \star N = a_2 \star N$ und $b_1 \star N = b_2 \star N$. Dann gilt

$$\begin{aligned}
[a_2] \mathbin{\tilde{\star}} [b_2] &= [a_2 \star b_2] \\
&= (a_2 \star b_2) \star N && \text{nach (7.25)} \\
&= a_2 \star (b_2 \star N) && \text{da } \star \text{ assoziativ ist} \\
&= a_2 \star (N \star b_2) && \text{da } N \text{ Normalteiler ist} \\
&= a_2 \star N \star b_2 && \text{da } \star \text{ assoziativ ist} \\
&= a_2 \star N \star N \star b_2 && \text{da } N \text{ Untergruppe ist} \\
&= (a_2 \star N) \star (N \star b_2) && \text{da } \star \text{ assoziativ ist} \\
&= (a_1 \star N) \star (N \star b_1) && \text{da } a_1 \overset{N}{\sim} a_2 \text{ und } b_1 \overset{N}{\sim} b_2 \\
&= (a_1 \star N) \star (b_1 \star N) && \text{da } N \text{ Normalteiler ist} \\
&= [a_1] \mathbin{\tilde{\star}} [b_1].
\end{aligned}$$

Damit ist $\tilde{\star}$ als Verknüpfung auf G/N wohldefiniert. Die Assoziativität von $\tilde{\star}$ ergibt sich aus der Assoziativität von $\star$ und der Normalteilereigenschaft, denn es gilt:

$$\begin{aligned}
([a] \mathbin{\tilde{\star}} [b]) \mathbin{\tilde{\star}} [c] &= [a \star b] \mathbin{\tilde{\star}} [c] = (a \star b \star N) \star (c \star N) = (a \star b \star N) \star (N \star c) \\
&= a \star b \star N \star c = a \star b \star c \star N \\
[a] \mathbin{\tilde{\star}} ([b] \mathbin{\tilde{\star}} [c]) &= [a] \mathbin{\tilde{\star}} [b \star c] = (a \star N) \star (b \star c \star N) = (a \star N) \star (N \star b \star c) \\
&= a \star N \star b \star c = a \star b \star c \star N
\end{aligned}$$

Damit haben wir zunächst $(G/N, \tilde{\star})$ als Halbgruppe bestätigt.

Als nächstes zeigen wir, dass $[e] = e \star N = N$ das neutrale Element von $(G/N, \tilde{\star})$ ist. Dazu sei $a \in G$ beliebig. Dann gilt gemäß Definition (8.7)

$$[e] \mathbin{\tilde{\star}} [a] = [e \star a] = [a] \quad \text{sowie} \quad [a] \mathbin{\tilde{\star}} [e] = [a \star e] = [a].$$

Also ist $(G/N, \tilde{\star})$ ein Monoid mit neutralem Element $[e]$.

Nun zeigen wir, dass jedes $[a] \in G/N$ invertierbar ist mit Inverser $[a]' = [a']$:

$$[a] \mathbin{\tilde{\star}} [a'] = [a \star a'] = [e] \quad \text{sowie} \quad [a'] \mathbin{\tilde{\star}} [a] = [a' \star a] = [e].$$

Aussage (*ii*): Die Eigenschaft, ein Gruppenhomomorphismus zu sein, bedeutet $\pi(a \star b) = \pi(a) \mathbin{\tilde{\star}} \pi(b)$. Nach Definition von π heißt das aber gerade $[a \star b] = [a] \mathbin{\tilde{\star}} [b]$, was gerade die Definition von $\tilde{\star}$ war.

Die Surjektivität von π ist klar, denn ein beliebiges Element $[a]$ von G/N ist gerade das Bild von a unter π. Es gilt $\operatorname{Kern}(\pi) = \pi^{-1}([e]) = N$.

Aussage *(iii)*: Falls $(G, \star)$ abelsch ist, dann gilt

$$[a] \mathbin{\tilde{\star}} [b] = [a \star b] = [b \star a] = [b] \mathbin{\tilde{\star}} [a],$$

also ist auch $(G/N, \tilde{\star})$ abelsch. □

Bemerkung 8.14 (Faktorgruppe)**.**
Praktisch können wir die Faktorgruppe $(G/N, \tilde{\star})$ benutzen, um wie in der Gruppe $(G, \star)$ zu „rechnen“, wobei jedoch Elemente a, b in derselben Äquivalenzklasse (für die also $a \star b' \in N$ gilt) nicht mehr unterschieden werden. Die Faktorgruppe $(G/N, \tilde{\star})$ ist also eine „gröbere Version“ der Gruppe $(G, \star)$. △

Beispiel 8.15 (Faktorgruppe)**.**

(i) Es sei $(G, \star)$ eine beliebige Gruppe. Dann ist die triviale Untergruppe $\{e\}$ nach Beispiel 8.11 ein Normalteiler. Die zugehörige Faktorgruppe $(G/\{e\}, \tilde{\star})$ ist isomorph zur Ausgangsgruppe $(G, \star)$ selbst.

(ii) Es sei $(G, \star)$ eine beliebige Gruppe. Dann ist die triviale Untergruppe G nach Beispiel 8.11 ein Normalteiler. Die zugehörige Faktorgruppe $(G/G, \tilde{\star})$ ist isomorph zu $(\{e\}, \star)$.

(iii) In der abelschen Gruppe $(\mathbb{Z}, +)$ ist jede Untergruppe der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}$ ein Normalteiler. Die Elemente der Faktorgruppe $(\mathbb{Z}/m\mathbb{Z}, \tilde{+})$ sind die Nebenklassen von $m\mathbb{Z}$, also die Mengen der Form $[a] = a + m\mathbb{Z}$, vgl. Beispiel 7.42. Es gilt

$$[a] \mathbin{\tilde{+}} [b] = [a + b].$$

Die Faktorgruppe $(\mathbb{Z}/m\mathbb{Z}, \tilde{+})$ ist isomorph zu einer uns bereits bekannten Gruppe, nämlich zur additiven Gruppe modulo m $(\mathbb{Z}_m, +_m)$ aus Beispiel 7.16 mittels des Isomorphismus $[a] \mapsto$ natürlicher Repräsentant von a in $\mathbb{Z}_m$. Beispielsweise können wir für $m = 5$ wie folgt rechnen:

$$\begin{array}{lccccc} \text{in } (\mathbb{Z}/5\mathbb{Z}, \tilde{+}) & [-21] & \tilde{+} & [9] & = & [-12] \\ & \downarrow & & \downarrow & & \downarrow \\ \text{in } (\mathbb{Z}_5, +_5) & 4 & +_5 & 4 & = & 3 \end{array}$$

(iv) In der abelschen Gruppe $(\mathbb{R}_{\neq 0}, \cdot)$ ist die Untergruppe $(\{\pm 1\}, \cdot)$ ein Normalteiler. Die Elemente der Faktorgruppe sind die Nebenklassen

$$[a] = a \cdot \{\pm 1\} = \{a, -a\}$$

für $a \in \mathbb{R}_{\neq 0}$. Ein mögliches Repräsentantensystem ist $\mathbb{R}_{>0}$. △

Bemerkung 8.16 (Normalteiler sind genau die Kerne von Gruppenhomomorphismen)**.**
Es sei $(G_1, \star)$ eine Gruppe. Nach Lemma 8.12 ist für jeden beliebigen Gruppenhomomorphismus $f\colon G_1 \to G_2$ in irgendeine Gruppe $(G_2, \square)$ die Untergruppe $\operatorname{Kern}(f)$ immer ein Normalteiler von $(G_1, \star)$.

Umgekehrt kann man zeigen, dass jeder Normalteiler von dieser Form ist. Also gilt: Jeder Normalteiler von $(G_1, \star)$ ist der Kern eines geeignet gewählten Gruppenhomomorphismus von $(G_1, \star)$ in eine geeignet gewählte Gruppe $(G_2, \square)$. △

§ 8.2 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. Das geschieht zudem strukturverträglich. Dadurch ist das $\operatorname{Bild}(f)$ eines solchen Gruppenhomomorphismus bereits im Wesentlichen (d. h. bis auf Isomorphie) festgelegt ist durch $(G_1, \star)$ und die Untergruppe $\operatorname{Kern}(f)$.

Satz 8.17 (Homomorphiesatz für Gruppen[10]).
Es seien $(G_1, \star)$ und $(G_2, \square)$ Gruppen. Weiter sei $f\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt

$$G_1 / \operatorname{Kern}(f) \cong \operatorname{Bild}(f) \tag{8.9a}$$

mit dem Isomorphismus

$$I([a]) \coloneqq f(a) \quad \text{für } [a] = a \star \operatorname{Kern}(f) \in G_1 / \operatorname{Kern}(f). \tag{8.9b}$$

Beweis. Wir bezeichnen die neutralen Elemente von G_1 und G_2 mit e_1 bzw. e_2.

Wir definieren $I\colon G_1 / \operatorname{Kern}(f) \to \operatorname{Bild}(f)$ wie in (8.9).

Schritt 1: Wir müssen zunächst zeigen, dass I als Abbildung wohldefiniert ist, da wir in der Definition (8.9b) Bezug auf den konkreten Repräsentanten $a \in G_1$ nehmen.

Es seien dazu $a, b \in G_1$ gegeben mit $a \overset{\operatorname{Kern}(f)}{\sim} b$, d. h., $a \star \operatorname{Kern}(f) = b \star \operatorname{Kern}(f)$. Dann gilt

$$\begin{aligned} f(a \star \operatorname{Kern}(f)) &= f(a) \square f(\operatorname{Kern}(f)) && \text{da } f \text{ Homomorphismus ist} \\ &= \{f(a)\} && \text{da } f(\operatorname{Kern}(f)) = \{e_2\} \text{ gilt} \end{aligned}$$

und analog $f(b \star \operatorname{Kern}(f)) = \{f(b)\}$. Aus $a \star \operatorname{Kern}(f) = b \star \operatorname{Kern}(f)$ folgt also $f(a) = f(b)$. Außerdem ist nach Definition von I klar, dass I in $\operatorname{Bild}(f)$ abbildet. Damit ist I wohldefiniert.

Schritt 2: Als nächstes zeigen wir, dass I ein Homomorphismus ist. In der Tat gilt

$$\begin{aligned} I([a] \mathbin{\tilde\star} [b]) &= I([a \star b]) && \text{nach Definition (8.7) von } \tilde\star \\ &= f(a \star b) && \text{nach Definition von } I \\ &= f(a) \square f(b) && \text{da } f \text{ Homomorphismus ist} \\ &= I([a]) \square I([b]) && \text{nach Definition von } I. \end{aligned}$$

Schritt 3: Es bleibt zu zeigen, dass I surjektiv und injektiv ist. Wenn $a_2 \in \operatorname{Bild}(f)$ ist, dann existiert $a_1 \in G_1$ mit

$$a_2 = f(a_1) = I([a_1]).$$

Das zeigt die Surjektivität von I.

[10] englisch: fundamental theorem on group homomorphisms

Für die Injektivität genügt es nach Lemma 8.9 zu zeigen, dass $\operatorname{Kern}(I)$ nur aus dem neutralen Element des Definitionsbereiches $G_1 / \operatorname{Kern}(f)$ besteht, d. h., aus $[e_1] = \operatorname{Kern}(f)$, vgl. Satz 8.13. Es gilt

$$\begin{aligned}
\operatorname{Kern}(I) &= \big\{[a] \in G_1 / \operatorname{Kern}(f) \,\big|\, I([a]) = e_2\big\} && \text{nach Definition von } \operatorname{Kern}(I)\\
&= \big\{[a] \in G_1 / \operatorname{Kern}(f) \,\big|\, f(a) = e_2\big\} && \text{nach Definition von } I\\
&= \big\{[a] \in G_1 / \operatorname{Kern}(f) \,\big|\, a \in \operatorname{Kern}(f)\big\} && \text{nach Definition von } \operatorname{Kern}(f)\\
&= \big\{a \star \operatorname{Kern}(f) \,\big|\, a \in \operatorname{Kern}(f)\big\} && \text{wegen } [a] = a \star \operatorname{Kern}(f), \text{ siehe (7.25)}\\
&= \big\{\operatorname{Kern}(f)\big\} && \text{, denn } \operatorname{Kern}(f) \text{ ist Untergruppe von } (G_2, \square)\\
& && \text{nach Lemma 8.7.} \qquad \square
\end{aligned}$$

Beispiel 8.18 (Homomorphiesatz für Gruppen).

(*i*) Wir betrachten für festes $n \in \mathbb{N}$ die Abbildung $\operatorname{sgn}\colon S_n \to (\{\pm 1\}, \cdot)$, vgl. Beispiele 8.4 und 8.8. Es gilt $\operatorname{Kern}(\operatorname{sgn}) = A_n$. Für $n \geqslant 2$ sind die Elemente der Faktorgruppe $S_n / \operatorname{Kern}(\operatorname{sgn}) = S_n / A_n$ die beiden Nebenklassen

$$\begin{aligned}
[\mathrm{id}] &= \mathrm{id} \circ A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} && \text{(gerade Permutationen)},\\
[\tau] &= \tau \circ A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = -1\} && \text{(ungerade Permutationen)},
\end{aligned}$$

wobei τ irgendeine Transposition in S_n ist. Gemäß Homomorphiesatz 8.17 ist

$$S_n / \operatorname{Kern}(\operatorname{sgn}) = S_n / A_n \cong \operatorname{Bild}(\operatorname{sgn}) = \{\pm 1\}.$$

Es werden alle geraden Permutationen $A_n = \operatorname{Kern}(\operatorname{sgn})$ ausfaktorisiert.

Im Fall $n = 1$ gilt $A_1 = S_1$, daher gibt es nur die eine Nebenklasse

$$[\mathrm{id}] = \mathrm{id} \circ S_1 = \{\mathrm{id}\}.$$

Der Homomorphiesatz 8.17 besagt daher in diesem Fall

$$S_1 / \operatorname{Kern}(\operatorname{sgn}) = S_1 / A_1 \cong \operatorname{Bild}(\operatorname{sgn}) = \{1\}.$$

(*ii*) Für die Abbildung $f\colon (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 \in (\mathbb{R}_{\neq 0}, \cdot)$ aus Beispiel 8.8 und Beispiel 8.15 gilt

$$\mathbb{R}_{\neq 0} / \operatorname{Kern}(f) = \mathbb{R}_{\neq 0} / \{\pm 1\} \cong \operatorname{Bild}(f) = \mathbb{R}_{>0}.$$

Durch $\operatorname{Kern}(f) = \{\pm 1\}$ wird das Vorzeichen ausfaktorisiert. △

Ende der Vorlesung 11

§ 9 Ringe

Literatur: Bosch, 2014, Kapitel 5.1, Fischer, Springborn, 2020, Kapitel 2.3

Ein Ring ist eine algebraische Struktur mit zwei Verknüpfungen, die gewissen Gesetzmäßigkeiten folgen. In Anlehnung an die wichtigen Beispiele $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit den Verknüpfungen „Addition“ und „Multiplikation“ bezeichnen wir diese Verknüpfungen mit + und ·.

Definition 9.1 (Ring)**.**

Ein **Ring** (englisch: ring) $(R, +, \cdot)$ ist eine Menge R mit zwei (inneren) Verknüpfungen $+$ („Addition“) und $\cdot$ („Multiplikation“), die die folgenden Bedingungen erfüllen:

(*i*) $(R, +)$ ist eine abelsche Gruppe.

(*ii*) $(R, \cdot)$ ist eine Halbgruppe.

(*iii*) Es gelten die **Distributivgesetze** (englisch: distributive laws)

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{9.1a}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \tag{9.1b}$$

für alle $a, b, c \in R$.

Ein Ring $(R, +, \cdot)$ heißt **kommutativ** (englisch: commutative ring), wenn die Halbgruppe $(R, \cdot)$ kommutativ ist.[11] △

Wie üblich vereinbaren wir, dass $\cdot$ stärker bindet als $+$ („Punkt- vor Strichrechnung“), also könnten wir die rechte Seite in (9.1a) auch in der Form $a \cdot b + a \cdot c$ schreiben.

Wie in Gruppen in additiver Notation üblich (Bemerkung 7.13), bezeichnen wir das neutrale Element bzgl. $+$ als **Nullelement** (englisch: additive identity) und schreiben dafür zunächst „0_R“. Außerdem bezeichnen wir das bzgl. $+$ inverse Element von $a \in R$ mit $-a$. Die Bezeichnung $a - b$ steht für $a + (-b)$.

Falls $(R, \cdot)$ ein Monoid ist, so bezeichnen wir das neutrale Element bzgl. $\cdot$ als **Einselement** (englisch: multiplicative identity) und schreiben dafür zunächst „1_R“. In diesem Fall heißt $(R, +, \cdot)$ auch ein **Ring mit Eins** (englisch: ring with unity) oder ein **unitärer Ring** (englisch: unitary ring). Existiert dann zu $a \in R$ bzgl. $\cdot$ ein inverses Element, so bezeichnen wir dieses mit a^{-1}.

Wir vereinbaren, dass $\cdot$ stärker bindet als $+$ und $-$, sodass wir beispielsweise statt $(a \cdot b) + (a \cdot c)$ auch $a \cdot b + a \cdot c$ schreiben können. Außerdem können wir $-a \cdot b$ schreiben statt $-(a \cdot b)$.

Beispiel 9.2 (Ring)**.**

(*i*) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.

(*ii*) Der **Nullring** (englisch: zero ring) ist der (bis auf Isomorphie) eindeutig bestimmte Ring mit $R = \{0_R\}$ und den dadurch eindeutig bestimmten Verknüpfungen $0_R + 0_R = 0_R$ und $0_R \cdot 0_R = 0_R$. Da 0_R auch das neutrale Element bzgl. $\cdot$ ist, ist der Nullring ein Ring mit Eins, und es gilt $1_R = 0_R$. Er ist der einzige Ring, in dem das Nullelement und das Einselement identisch sind, siehe Lemma 9.3.

(*iii*) Für $m \in \mathbb{N}$ ist $(m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring. Im Fall $m \neq 1$ besitzt er kein Einselement. Im Fall $m = 1$ ist $1 \in \mathbb{Z}$ das Einselement.

(*iv*) Für $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit Einselement 1, denn nach Beispiel 7.16 ist $(\mathbb{Z}_m, +_m)$ eine abelsche Gruppe und $(\mathbb{Z}_m, \cdot_m)$ ein kommutatives Monoid. Er wird der **Ring von $\mathbb{Z}$ modulo m** (englisch: ring of $\mathbb{Z}$ modulo m) genannt. Im Fall $m = 1$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ der Nullring.

[11] In diesem Fall fallen die beiden Distributivgesetze (9.1a) und (9.1b) zusammen. Es reicht also, eines von beiden zu prüfen.

(*v*) Es sei $(G,+)$ eine abelsche Gruppe. Wir definieren

$$\mathrm{End}(G) \coloneqq \big\{ f \colon G \to G \,\big|\, f \text{ ist Endomorphismus} \big\} \tag{9.2}$$

und statten $\mathrm{End}(G)$ mit den Verknüpfungen

$$+ \colon \mathrm{End}(G) \times \mathrm{End}(G) \to \mathrm{End}(G) \quad \text{mit } (f,g) \mapsto f+g, \text{definiert durch } (f+g)(x) \coloneqq f(x)+g(x)$$
$$\circ \colon \mathrm{End}(G) \times \mathrm{End}(G) \to \mathrm{End}(G) \quad \text{mit } (f,g) \mapsto f\circ g, \text{definiert durch } (f\circ g)(x) \coloneqq f(g(x))$$

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 9.1: Warum definieren wir den Endomorphismenring nur für Endomorphismen auf abelschen Gruppen und nicht allgemeiner für Endomorphismen auf beliebigen Gruppen? △

Lemma 9.3 (Rechenregeln in Ringen)**.**
Es sei $(R,+,\cdot)$ ein Ring mit dem Nullelement 0_R. Für $a,b \in R$ gilt:

(*i*) $0_R \cdot a = 0_R = a \cdot 0_R$

(*ii*) $a \cdot (-b) = -a \cdot b = (-a) \cdot b$

(*iii*) $(-a) \cdot (-b) = a \cdot b$

(*iv*) Ist $(R,+,\cdot)$ ein Ring mit Einselement 1_R, aber nicht der Nullring, dann gilt $1_R \neq 0_R$.

Beachte: Hat R das Einselement 1_R, dann folgt aus Aussage (*ii*) insbesondere $-b = (-1_R)\cdot b$.

Beweis. Aussage (*i*): Es gilt

$$\begin{aligned} 0_R + 0_R \cdot a &= 0_R \cdot a && \text{da } 0_R \text{ das neutrale Element von } (R,+) \text{ ist} \\ &= (0_R + 0_R)\cdot a && \text{da } 0_R \text{ das neutrale Element von } (R,+) \text{ ist} \\ &= 0_R \cdot a + 0_R \cdot a && \text{wegen des Distributivgesetzes (9.1b).} \end{aligned}$$

Die Anwendung der Kürzungsregel (7.10a) in der Gruppe $(R,+)$, also die Addition von $-(0_R\cdot a)$ zu beiden Seiten der Gleichung, zeigt $0_R \cdot a = 0_R \cdot a$. Das zweite Resultat, $a \cdot 0_R = 0_R$, folgt analog.

Aussage (*ii*): Wir zeigen zunächst, dass $a\cdot(-b) = -a\cdot b$ gilt, also dass $a\cdot(-b)$ das Inverse zu $a\cdot b$ in der Gruppe $(R,+)$ ist. Gemäß (7.11) reicht dafür der Nachweis von $a\cdot(-b) + a\cdot b = 0_R$ aus, also der einseitige Test. In der Tat haben wir

$$\begin{aligned} a\cdot(-b) + a\cdot b &= a\cdot(-b+b) && \text{wegen des Distributivgesetzes (9.1a)} \\ &= a \cdot 0_R \\ &= 0_R && \text{nach Aussage (}i\text{).} \end{aligned}$$

Die Aussage $(-a)\cdot b = -a\cdot b$ folgt analog.

Aussage (*iii*): Wir haben

$$\begin{aligned} (-a)\cdot(-b) &= -(a\cdot(-b)) && \text{nach Aussage (}ii\text{)} \\ &= -(-a\cdot b) && \text{nach Aussage (}ii\text{)} \\ &= a\cdot b && \text{nach (7.12) (doppelte Invertierung).} \end{aligned}$$

Aussage (iv): Es sei R ein Ring mit Einselement 1_R. Wir führen den Beweis durch Kontraposition. Wir nehmen also $1_R = 0_R$ an. Nun sei $a \in R$ beliebig. Dann gilt

$$\begin{aligned} a &= a \cdot 1_R && \text{da } 1_R \text{ das neutrale Element von } (R, \cdot) \text{ ist} \\ &= a \cdot 0_R && \text{da } 1_R = 0_R \text{ angenommen wurde} \\ &= 0_R && \text{nach Aussage } (i). \end{aligned}$$

Der Ring R besteht also nur aus dem Nullelement 0_R, d. h., R ist der Nullring. □

Wir verwenden auch in Ringen $(R, +, \cdot)$ und insbesondere in der Gruppe $(R, +)$ die Schreibweise aus Bemerkung 7.13. Es gilt also für $n \in \mathbb{N}$

$$n\,a \coloneqq a + \cdots + a.$$

Besitzt $(R, +, \cdot)$ das Einselement 1_R, dann gilt nach Distributivgesetz weiter

$$n\,a = a + \cdots + a = 1_R \cdot a + \cdots + 1_R \cdot a = (1_R + \cdots + 1_R) \cdot a = (n\,1_R) \cdot a.$$

Weiter ist $(-n)\,a \coloneqq -(n\,a)$ und $0\,a \coloneqq 0_R$.

Definition 9.4 (Charakteristik eines Ringes)**.**
Es sei R ein Ring mit Einselement 1_R.

(i) Wenn es eine Zahl $n \in \mathbb{N}$ gibt, sodass $n\,1_R = 0_R$ gilt, so nennen wir die kleinste solche Zahl

$$\min\{n \in \mathbb{N} \mid n\,1_R = 0_R\}$$

die **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** (englisch: characteristic) 0 und schreiben $\operatorname{char}(R) = 0$. △

Beispiel 9.5 (Charakteristik eines Ringes)**.**

(i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ haben Charakteristik 0.

(ii) Der Nullring ist (bis auf Isomorphie) der einzige Ring mit Charakteristik 1, also der einzige Ring, in dem $1_R = 0_R$ gilt, vgl. Lemma 9.3.

(iii) Der Ring von $\mathbb{Z}$ modulo m $(\mathbb{Z}_m, +_m, \cdot_m)$ hat Charakteristik $m \in \mathbb{N}$.

(iv) Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ aus dem folgenden Beispiel 9.6 hat ebenfalls Charakteristik $m \in \mathbb{N}$. △

Beispiel 9.6 (Restklassenring modulo m)**.**
Es sei $m \in \mathbb{N}$. Wir erinnern an die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$ aus Beispiel 8.15 mit den Elementen $[a] = a + m\mathbb{Z}$ (für $a \in \mathbb{Z}$), der kommutativen Verknüpfung $[a] \tilde{+} [b] = [a + b]$ und dem neutralen Element $[0]$. $(\mathbb{Z}/m\mathbb{Z}, \tilde{+})$ bildet eine kommutative Gruppe.

Weiter bildet $(\mathbb{Z}/m\mathbb{Z}, \tilde{\cdot})$ mit der Verknüpfung $[a] \tilde{\cdot} [b] = [a \cdot b]$ ein kommutatives Monoid mit dem neutralen Element $[1]$, siehe auch Hausaufgabe 6.1.

Schließlich können wir zeigen, dass die Distributivgesetze (9.1a) und (9.1b) gelten, denn:

$$\begin{aligned}
[a] \mathbin{\tilde{\cdot}} ([b] \mathbin{\tilde{+}} [c]) &= [a] \mathbin{\tilde{\cdot}} [b+c] && \text{nach Definition von } \tilde{+} \\
&= [a \cdot (b+c)] && \text{nach Definition von } \tilde{\cdot} \\
&= [a \cdot b + a \cdot c] && \text{nach Distributivgesetz in } \mathbb{Z} \\
&= [a \cdot b] \mathbin{\tilde{+}} [a \cdot c] && \text{nach Definition von } \tilde{+} \\
&= [a] \mathbin{\tilde{\cdot}} [b] \mathbin{\tilde{+}} [a] \mathbin{\tilde{\cdot}} [c] && \text{nach Definition von } \tilde{\cdot}.
\end{aligned}$$

Das zweite Distributivgesetz (9.1b) ist wegen der Kommutativität der Halbgruppe $(\mathbb{Z}/m\mathbb{Z}, \tilde{\cdot})$ automatisch erfüllt. Daher bildet $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ einen kommutativen Ring mit Eins, genannt der **Restklassenring modulo** m. Im Fall $m = 1$ ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ der Nullring.

Die Verknüpfungstafeln für $\mathbb{Z}/m\mathbb{Z}$ für $m \in \{1, 2, 3, 4\}$ lauten:

$\tilde{+}$	$[0]$
$[0]$	$[0]$

$\tilde{\cdot}$	$[0]$
$[0]$	$[0]$

$\tilde{+}$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\tilde{\cdot}$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

$\tilde{+}$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\tilde{\cdot}$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

$\tilde{+}$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\tilde{\cdot}$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

△

Die für $m = 4$ in $\mathbb{Z}/m\mathbb{Z}$ erstmalig auftretende Situation $[2] \mathbin{\tilde{\cdot}} [2] = [0]$ wollen wir benennen:

Definition 9.7 (Nullteiler, Nullteilerfreiheit, Integritätsring)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(*i*) Das Element $a \in R$ heißt ein **Linksnullteiler** (englisch: left zero divisor), wenn es ein $b \in R \setminus \{0_R\}$ gibt, sodass $a \cdot b = 0_R$ gilt. Das Element b heißt ein **Rechtsnullteiler** (englisch: right zero divisor), wenn es ein $a \in R \setminus \{0_R\}$ gibt, sodass $a \cdot b = 0_R$ gilt.

(*ii*) Der Ring $(R, +, \cdot)$ heißt **nullteilerfrei** (englisch: ring with no zero divisors), wenn es außer dem Nullelement 0_R keine weiteren Links- oder Rechtsnullteiler gibt, wenn also gilt:

$$\forall a, b \in R \; (a \cdot b = 0_R \implies a = 0_R \text{ oder } b = 0_R). \tag{9.3}$$

(Anders gesagt: Aus $a \neq 0_R$ und $b \neq 0_R$ folgt $a \cdot b \neq 0_R$.)

(*iii*) Ein Ring $(R, +, \cdot)$ heißt **Integritätsring** oder **Integritätsbereich** (englisch: integral domain), wenn gilt: $(R, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit Eins ungleich dem Nullring. △

Quizfrage 9.2: Ist der Nullring nullteilerfrei?

Beispiel 9.8 (Integritätsringe und Gegenbeispiele)**.**

(*i*) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Integritätsringe.

(*ii*) Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist ein Integritätsring genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist; siehe Satz 9.9.

(*iii*) Es sei X eine Menge, $(R, +, \cdot)$ ein Ring und $R^X = \{f \mid f : X \to R\}$. Definieren wir ähnlich wie in Beispiel 7.2 die Verknüpfungen $+$ und $\cdot$ auf R^X als

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

dann ist $(R^X, +, \cdot)$ ein Ring. $(R^X, +, \cdot)$ ist kommutativ genau dann, wenn $(R, +, \cdot)$ kommutativ ist. $(R^X, +, \cdot)$ besitzt ein Einselement genau dann, $(R, +, \cdot)$ ein Einselement besitzt.

Beachte: Wenn $(R, +, \cdot)$ nicht der Nullring ist, dann ist $(R^X, +, \cdot)$ nicht nullteilerfrei, sobald X zwei oder mehr Elemente enthält! (**Quizfrage 9.3:** Wie sieht man das?) △

Satz 9.9 (Nullteilerfreiheit des Restklassenringes)**.**
Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist ein Integritätsring genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist.

Beweis. Für $m = 1$ ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ der Nullring und damit kein Integritätsring. Wir betrachten also im Weiteren nur den Fall $m \geqslant 2$, für den $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ein kommutativer Ring ungleich dem Nullring und mit dem Einselement $[1]$ ist. Die Frage, ob dieser Ring ein Integritätsring ist, hängt also genau an der Nullteilerfreiheit. Das Nullelement von $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist $[0]$.

Es sei $m \in \mathbb{N}$, $m \geqslant 4$, *keine* Primzahl, lässt sich also schreiben als $m = a \cdot b$ für Zahlen $a, b \in [\![2, m-1]\!]$. Die zugehörigen Restklassen $[a]$ und $[b]$ sind ungleich $[0]$ (**Quizfrage 9.4:** Warum?) Es gilt

$$\begin{aligned} [0] &= [m] && \text{da } 0 \overset{m}{\equiv} m \\ &= [a \cdot b] && \text{da } m = a \cdot b \\ &= [a] \,\tilde{\cdot}\, [b] && \text{nach Definition von } \tilde{\cdot}. \end{aligned}$$

Damit ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ *nicht* nullteilerfrei.

Es sei nun umgekehrt $m \in \mathbb{N}$, $m \geqslant 2$, eine Primzahl. Wir nehmen an, $[a]$ und $[b]$ seien Elemente aus $\mathbb{Z}/m\mathbb{Z}$ mit $[0] = [a] \,\tilde{\cdot}\, [b] = [a \cdot b]$. Das heißt aber, da 0 und $a \cdot b$ in derselben Restklasse modulo m liegen, dass $a \cdot b = m\,z$ gilt für irgendein $z \in \mathbb{Z}$. Da m eine Primzahl ist, kommt m in der (vorzeichenbehafteten) Primfaktorzerlegung von $a \cdot b$ vor. Das heißt, dass a oder b den Primfaktor m enthält, also gilt $m \mid a$ oder $m \mid b$, woraus $[a] = [0]$ oder $[b] = [0]$ folgt. Damit ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ nullteilerfrei. □

Definition 9.10 (Unterring, vgl. Definition 7.31 einer Untergruppe)**.**
Es sei $(R, +, \cdot)$ ein Ring.

(*i*) Eine Teilmenge $U \subseteq R$ heißt ein **Unterring** (englisch: subring) von $(R, +, \cdot)$, wenn U bzgl. **undefined** und bzgl. $\cdot$ abgeschlossen ist und wenn $(U, +, \cdot)$ selbst wieder ein Ring ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, +)$ eine Untergruppe von $(R, +)$ ist und wenn $(U, \cdot)$ bzgl. $\cdot$ abgeschlossen ist.

(*ii*) Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R, dann fordern wir für einen **Unterring mit Eins** (englisch: subring with unity) $(U, +, \cdot)$ zusätzlich zu Eigenschaft (*i*), dass $1_R \in U$ liegt.[12]

Beachte: Es reicht nicht aus, zu fordern, dass $(U, \cdot)$ *irgendein* neutrales Element besitzt.

(*iii*) Ein Unterring $(U, +, \cdot)$ von $(R, +, \cdot)$ heißt **echt** (englisch: proper subring), wenn $U \subsetneq R$ gilt. △

Definition 9.11 (Ringhomomorphismus, vgl. Definition 8.1 eines Halbgruppenhomomorphismus)**.**
Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ zwei Ringe.

(*i*) Eine Abbildung $f\colon R_1 \longrightarrow R_2$ heißt **strukturverträglich** oder ein **(Ring-)Homomorphismus** (englisch: ring homomorphism) von $(R_1, +_1, \cdot_1)$ in $(R_2, +_2, \cdot_2)$, wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in R_1, \tag{9.4a}$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in R_1. \tag{9.4b}$$

Besitzen beide Ringe ein Einselement 1_{R_1} bzw. 1_{R_2} und fordern wir zusätzlich

$$f(1_{R_1}) = 1_{R_2} \tag{9.4c}$$

dann nennen wir f genauer einen **Homomorphismus von Ringen mit Eins** (englisch: homomorphism of rings with unity).

(*ii*) Wie in Definition 8.1 sprechen wir im Fall $(R_1, +_1, \cdot_1) = (R_2, +_2, \cdot_2)$ von einem **(Ring-)Endomorphismus** (englisch: ring endomorphism) bzw. von einem **Endomorphismus eines Ringes mit Eins** (englisch: endomorphism of a ring with unity).

(*iii*) Ist $f\colon R_1 \longrightarrow R_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Ring-)Isomorphismus** (englisch: ring isomorphism) bzw. ein **Isomorphismus von Ringen mit Eins** (englisch: endomorphism of a ring with unity). In diesem Fall nennen wir $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ auch zueinander **isomorphe Ringe** (englisch: isomorphic rings) bzw. zueinander **isomorphe Ringe mit Eins** (englisch: isomorphic rings with unity) und schreiben

$$(R_1, +_1, \cdot_1) \cong (R_2, +_2, \cdot_2).$$

(*iv*) Im Fall $(R_1, +_1, \cdot_1) = (R_2, +_2, \cdot_2)$ und $f\colon R_1 \longrightarrow R_2$ bijektiv sprechen wir auch von einem **(Ring-)Automorphismus** (englisch: ring automorphism) bzw. von einem **Automorphismus eines Ringes mit Eins** (englisch: automorphism of a ring with unity).

(*v*) Das **Bild** (englisch: image) und der **Kern** eines Ringhomomorphismus $f\colon R_1 \longrightarrow R_2$ sind definiert als

$$\operatorname{Bild}(f) \coloneqq \left\{ f(x) \in R_2 \,\middle|\, x \in R_1 \right\} = f(R_1), \tag{9.5}$$
$$\operatorname{Kern}(f) \coloneqq \left\{ x \in R_1 \,\middle|\, f(x) = 0_{R_2} \right\} = f^{-1}(\{0_{R_2}\}). \qquad \triangle$$

[12] Dadurch ist der Unterring $(U, +, \cdot)$ dann natürlich selbst wieder ein Ring mit dem Einselement 1_R.

Die Beziehung (9.4a) besagt, dass $f\colon (R_1,+_1)\to(R_2,+_2)$ ein Gruppenhomomorphismus ist. Aus Lemma 8.5 folgt damit für die Nullelemente 0_{R_1} bzw. 0_{R_2} notwendigerweise

$$f(0_{R_1})=0_{R_2}. \tag{9.6}$$

Weiter bedeutet (9.4b), dass $f\colon (R_1,\cdot_1)\to(R_2,\cdot_2)$ ein Halbgruppenhomomorphismus ist. (9.4b) und (9.4c) zusammen bedeuten, dass $f\colon (R_1,\cdot_1)\to(R_2,\cdot_2)$ ein Monoidhomomorphismus ist.

Beispiel 9.12 (Ringhomomorphismen)**.**

(*i*) Die Abbildung

$$f\colon (\mathbb{Z},+,\cdot)\ni a\mapsto [a]=a+m\mathbb{Z}\in(\mathbb{Z}/m\mathbb{Z},\tilde{+},\tilde{\cdot})$$

ist ein surjektiver Ringhomomorphismus zwischen zwei kommutativen Ringen mit Eins, denn: f ist als kanonische Surjektion der Faktorgruppe nach Satz 8.13 und Beispiel 8.15 ein surjektiver Gruppenhomomorphismus $f\colon(\mathbb{Z},+)\to(\mathbb{Z}/m\mathbb{Z},\tilde{+})$, und außerdem ist $f\colon(\mathbb{Z},\cdot)\to(\mathbb{Z}/m\mathbb{Z},\tilde{\cdot})$ ein Monoidhomomorphismus, siehe Beispiel 9.6 und Hausaufgabe 6.1.

Es gilt

$$\begin{aligned}\operatorname{Bild}(f)&=\mathbb{Z}/m\mathbb{Z},\\ \operatorname{Kern}(f)&=f^{-1}([0])=m\mathbb{Z}.\end{aligned}$$

(*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 8.15 ein Gruppenisomorphismus $f\colon(\mathbb{Z}_m,+_m)\to(\mathbb{Z}/m\mathbb{Z},\tilde{+})$, und außerdem ist $f\colon(\mathbb{Z}_m,\cdot_m)\to(\mathbb{Z}/m\mathbb{Z},\tilde{\cdot})$ nach Hausaufgabe 6.1 ein Monoidisomorphismus.

Es gilt

$$\begin{aligned}\operatorname{Bild}(f)&=\mathbb{Z}/m\mathbb{Z},\\ \operatorname{Kern}(f)&=f^{-1}([0])=\{0\}.\end{aligned}$$

△

Ende der Vorlesung 12

Ende der Woche 6

§ 10 Körper

Literatur: Beutelspacher, 2014, Kapitel 2, Bosch, 2014, Kapitel 1.3, Fischer, Springborn, 2020, Kapitel 2.3, Deiser, 2022b, Kapitel 2.2

Ein Körper ist — wie ein Ring — eine algebraische Struktur mit zwei Verknüpfungen. In Anlehnung an die wichtigen Beispiele $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ mit den Verknüpfungen „Addition“ und „Multiplikation“ bezeichnen wir diese Verknüpfungen wieder mit + und ·.

Definition 10.1 (Körper)**.**
Ein **Körper** (englisch: field) $(K,+,\cdot)$ ist eine Menge K mit zwei (inneren) Verknüpfungen + („Addition“) und · („Multiplikation“), die die folgenden Bedingungen erfüllen:

(*i*) $(K, +)$ ist eine abelsche Gruppe. Das Nullelement bezeichnen wir mit 0_K.

(*ii*) $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe. Das Einselement bezeichnen wir mit 1_K.

(*iii*) Es gelten die **Distributivgesetze** (englisch: distributive laws)

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{10.1a}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \tag{10.1b}$$

für alle $a, b, c \in K$.[13] △

Oft wird $K \setminus \{0_K\}$ als K^* oder als $K^\times$ abgekürzt. Wir verwenden diese Bezeichnungen jedoch hier nicht.

Beispiel 10.2 (Körper und Gegenbeispiele)**.**

(*i*) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper mit dem Nullelement 0 und dem Einselement 1.

(*ii*) $(\mathbb{Z}_2, +_2, \cdot_2)$ aus Beispiel 7.16 mit den Verknüpfungstafeln aus Beispiel 7.2 ist ein Körper mit dem Nullelement 0 und dem Einselement 1.

(*iii*) Der Restklassenring $(\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ mit dem Nullelement $[0]$ und dem Einselement $[1]$ aus Beispiel 9.6 ist *kein* Körper, da $[2]$ nicht das Nullelement ist und $[2] \tilde{\cdot} [a] \neq [1]$ für alle $a \in \mathbb{Z}$ gilt und damit $[2]$ kein multiplikatives Inverses besitzt.

(*iv*) Es sei X eine Menge. Für die bisher besprochenen algebraischen Strukturen S (Halbgruppe, Monoid, Gruppe, Ring) galt, dass S^X, ausgestattet punktweise mit der oder den Verknüpfung(en) von S, die algebraische Struktur erbt, also ebenfalls Halbgruppe, Monoid, Gruppe oder Ring ist.

Wenn jedoch $(K, +, \cdot)$ ein Körper ist, dann ist $(K^X, +, \cdot)$ i. A. *kein* Körper, sondern nur ein kommutativer Ring mit Eins. (**Quizfrage 10.1:** Woran liegt das?) △

Lemma 10.3 (Eigenschaften eines Körpers)**.**

Es sei $(K, +, \cdot)$ ein Körper mit dem Nullelement 0_K und dem Einselement 1_K. Dann gilt:

(*i*) $0_K \neq 1_K$. Ein Körper hat also mindestens zwei Elemente.

(*ii*) $(K, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit dem Einselement 1_K ungleich dem Nullring, also ein Integritätsring.

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

$$a \cdot b_1 = a \cdot b_2 \quad \Rightarrow \quad b_1 = b_2 \tag{10.2a}$$
$$b_1 \cdot a = b_2 \cdot a \quad \Rightarrow \quad b_1 = b_2 \tag{10.2b}$$

für $a, b_1, b_2 \in K$ mit $a \neq 0_K$.

[13] Wie bereits in kommutativen Ringen fallen die beiden Distributivgesetze (10.1a) und (10.1b) zusammen. Es reicht also, eines von beiden zu prüfen.

Beweis. Aussage (i): Nach Definition 10.1 ist $K \setminus \{0_K\}$ eine Gruppe mit dem Einselement 1_K, also muss $0_K \neq 1_K$ gelten.

Aussage (ii): Nach Definition 10.1 ist $(K, +)$ eine abelsche Gruppe mit dem Nullelement 0_K. Wenn wir zeigen können, dass $(K, \cdot)$ ein abelsches Monoid mit dem Einselement 1_K ist, dann ist $(K, +, \cdot)$ per Definition 9.1 ein abelscher Ring mit dem Einselement 1_K. Dieser ist nach Aussage (i) nicht der Nullring. Wenn wir anschließend zeigen können, dass $(K, +, \cdot)$ nullteilerfrei ist, dann ist Aussage (ii) gezeigt.

Schritt 1: Wir zeigen: $0_K \cdot a = 0_K = a \cdot 0_K$ für alle $a \in K$.

Dieses Ergebnis folgt wie im Beweis von Lemma 9.3, Aussage (i): $0_K + 0_K \cdot a = 0_K \cdot a = (0_K + 0_K) \cdot a = 0_K \cdot a + 0_K \cdot a$ und daher $0_K \cdot a = 0_K$. Analog können wir $a \cdot 0_K = 0_K$ zeigen.

Schritt 2: Wir zeigen: $\cdot$ ist eine *assoziative* Verknüpfung auf ganz K:

Per Definition ist $\cdot$ eine Verknüpfung auf ganz K. Die Assoziativität $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ist klar, wenn nur Elemente $a, b, c \in K \setminus \{0_K\}$ verknüpft werden, da $(K \setminus \{0_K\}, \cdot)$ eine Gruppe ist. Wenn eines oder mehrere Elemente a, b, c aber das Nullelement 0_K sind, dann gilt wegen **Schritt** 1, dass sowohl $a \cdot (b \cdot c)$ als auch $(a \cdot b) \cdot c$ gleich 0_K sind. Die Assoziativität von $\cdot$ gilt also auf ganz K.

Schritt 3: Wir zeigen: $\cdot$ ist eine *kommutative* Verknüpfung auf ganz K:

Die Kommutativität $a \cdot b = b \cdot a$ ist klar, wenn nur Elemente $a, b \in K \setminus \{0_K\}$ verknüpft werden, da $(K \setminus \{0_K\}, \cdot)$ eine kommutative Gruppe ist. Wenn eines oder mehrere Element a, b aber das Nullelement 0_K sind, dann gilt wegen **Schritt** 1, dass sowohl $a \cdot b$ als auch $b \cdot a$ gleich 0_K sind. Die Kommutativität von $\cdot$ gilt also auf ganz K.

Schritt 4: Wir zeigen: 1_K ist neutrales Element bzgl. $\cdot$ auf ganz K:

Wir wissen bereits $1_K \cdot a = a \cdot 1_K$ für alle $a \in K \setminus \{0_K\}$. Ist nun $a = 0_K$, so gilt wegen **Schritt** 1 $1_K \cdot a = a \cdot 1_K = 0_K$. Damit ist 1_K neutrales Element bzgl. $\cdot$ auf ganz K.

Damit haben wir bisher gezeigt, dass $(K, \cdot)$ ein abelsches Monoid mit dem Einselement 1_K ist, also ist $(K, +, \cdot)$ per Definition 9.1 ein abelscher Ring mit dem Einselement 1_K, der Aussage (i) nicht der Nullring ist.

Schritt 5: Wir zeigen: Der Ring $(K, +, \cdot)$ ist nullteilerfrei.

Wenn $a, b \in K \setminus \{0_K\}$ sind, dann ist auch $a \cdot b \in K \setminus \{0_K\}$, da per Definition $(K \setminus \{0\}, \cdot)$ eine Gruppe und damit insbesondere $K \setminus \{0\}$ abgeschlossen bzgl. $\cdot$ ist. Das heißt, $(K, +, \cdot)$ ist nullteilerfrei.

Aussage (iii): Für $a, b_1, b_2 \in K \setminus \{0\}$ sind die Kürzungsregeln (10.2) nichts anderes als die Kürzungsregeln (7.10) in der Gruppe $(K \setminus \{0\}, \cdot)$. Wir zeigen (10.2a) in den verbleibenden Fällen. Ist $b_1 = 0_K$, dann folgt aus Aussage (i) und der Voraussetzung $0_K = a \cdot b_1 = a \cdot b_2$. Wegen der Nullteilerfreiheit und $a \neq 0_K$ folgt weiter $b_2 = 0_K$, also $b_1 = b_2$. Ist andererseits $b_2 = 0_K$, dann folgt aus Aussage (i) und der Voraussetzung $0_K = a \cdot b_2 = a \cdot b_1$. Wegen der Nullteilerfreiheit und $a \neq 0_K$ folgt weiter $b_1 = 0_K$, also wiederum $b_1 = b_2$.

Die Aussage (10.2b) können wir analog beweisen. □

Beachte: Die Rechenregeln in Ringen aus Lemma 9.3 gelten also auch in Körpern.

Die Definition 9.4 der Charakteristik eines Ringes wird auch auf Körper angewendet. Für Körper ist die Charakteristik entweder 0 oder eine Primzahl.

Satz 10.4 (Wann ist ein Ring ein Körper?)**.**
Es sei K eine Menge mit zwei (inneren) Verknüpfungen + und $\cdot$. Dann sind die folgenden Aussagen äquivalent:

(*i*) $(K, +, \cdot)$ ist ein Körper, dessen Nullelement mit 0_K und dessen Einselement mit 1_K bezeichnet werden.

(*ii*) $(K, +, \cdot)$ ist ein kommutativer Ring mit dem Einselement 1_K und dem Nullelement $0_K \neq 1_K$, wobei zu jedem $a \in K \setminus \{0_K\}$ ein Inverses bzgl. $\cdot$ in K existiert.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Nach Lemma 10.3 ist $(K, +, \cdot)$ ein kommutativer Ring mit dem Einselement 1_K und dem Nullelement $0_K \neq 1_K$. Da $(K \setminus \{0_K\}, \cdot)$ eine Gruppe ist, existiert zu jedem $a \in K \setminus \{0_K\}$ ein Inverses bzgl. $\cdot$.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Nach Voraussetzung ist $(K, +)$ eine abelsche Gruppe mit dem Nullelement 0_K. Weiter gelten die Distributivgesetze (10.1) nach Voraussetzung. Es bleibt zu zeigen, dass $(K \setminus \{0_K\}, \cdot)$ eine abelsche Gruppe mit dem Einselement 1_K ist.

Nach Voraussetzung ist $(K, \cdot)$ ein abelsches Monoid mit neutralem Element 1_K. Aus der Eigenschaft $\forall a \in K \setminus \{0\}\ \exists a^{-1} \in K\ (a \cdot a^{-1} = a^{-1} \cdot a = 1_K)$ folgt die Nullteilerfreiheit:

$$a \cdot b = 0_K \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_K = 0_K.$$

Also ist $K \setminus \{0_K\}$ bzgl. $\cdot$ abgeschlossen. Damit erbt $(K \setminus \{0_K\}, \cdot)$ die Eigenschaft, ein abelsches Monoid mit dem Einselement 1_K zu sein, von $(K, \cdot)$. Da jedes Element $a \in K \setminus \{0_K\}$ nach Voraussetzung ein Inverses a^{-1} bzgl. $\cdot$ mit $a^{-1} \in K$ besitzt und a^{-1} wegen $a \cdot 0_K = 0_K \neq 1_K$ sogar in $K \setminus \{0_K\}$ liegen muss, ist $(K \setminus \{0_K\}, \cdot)$ als abelsche Gruppe bestätigt. Das heißt, $(K, +, \cdot)$ ist ein Körper. □

Satz 10.5 (endliche Integritätsringe sind Körper)**.**
Es sei $(R, +, \cdot)$ ein Integritätsring mit endlich vielen Elementen. Dann ist $(R, +, \cdot)$ ein Körper.

Beweis. Es sei $(R, +, \cdot)$ ein Integritätsring, also ein kommutativer, nullteilerfreier Ring mit dem Einselement 1_R ungleich dem Nullring. Wir wissen also bereits: $(R, +)$ ist eine abelsche Gruppe mit dem Nullelement 0_R, und $(R, \cdot)$ ist eine abelsche Halbgruppe mit dem Einselement $1_R \neq 0_R$ (Lemma 9.3). Aus der Nullteilerfreiheit folgt, dass $R \setminus \{0_R\}$ bzgl. $\cdot$ abgeschlossen ist, also ist auch $(R \setminus \{0_R\}, \cdot)$ ein abelsches Monoid mit dem Einselement 1_R.

Es bleibt zu zeigen, dass $(R \setminus \{0_R\}, \cdot)$ sogar eine Gruppe ist. Dazu nutzen wir das Gruppenkriterium Lemma 7.18. Zu beliebigem $a \in R \setminus \{0\}$ betrachten wir die Rechtstranslation $\cdot_a$ auf dem Monoid $R \setminus \{0\}$. Diese ist injektiv, denn nach Distributivgesetz (9.1b) gilt

$$b \cdot a = c \cdot a \quad \Rightarrow \quad b \cdot a - c \cdot a = 0_R \quad \Rightarrow \quad (b - c) \cdot a = 0_R,$$

und da R nullteilerfrei und $a \neq 0_R$ ist, folgt $b = c$. Da nun R und damit $R \setminus \{0\}$ eine endliche Menge ist, gilt nach Satz 6.27, dass $\cdot_a$ auch surjektiv.

Ein analoges Argument zeigt, dass auch alle Linkstranslationen auf $R \setminus \{0\}$ surjektiv sind. Aus dem Gruppenkriterium Lemma 7.18 folgt nun, dass $(R \setminus \{0\}, \cdot)$ eine Gruppe ist. □

Folgerung 10.6 (Körpereigenschaft des Restklassenringes und des Ringes von $\mathbb{Z}$ modulo m, vgl. Satz 9.9)**.**
Der Restklassenring modulo m $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ sowie der zu ihm isomorphe Ring (Beispiel 9.12) von $\mathbb{Z}$ modulo m $(\mathbb{Z}_m, +_m, \cdot_m)$ sind Körper genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist. In diesem Fall nennen wir sie auch **Restklassenkörper modulo** m oder **Körper von** $\mathbb{Z}$ **modulo** m (englisch: field of $\mathbb{Z}$ modulo m).

Beweis. In Satz 9.9 haben wir gezeigt, dass $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ genau dann ein Integritätsbereich ist, wenn $m \in \mathbb{N}$ eine Primzahl ist. Da aber $\mathbb{Z}/m\mathbb{Z}$ nur endlich viele (nämlich m) Elemente hat, ist Integritätsbereich zu sein gleichbedeutend mit der Körpereigenschaft.

Nach Beispiel 9.12 sind $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ und $(\mathbb{Z}_m, +_m, \cdot_m)$ als Ringe isomorph, also gelten dieselben Eigenschaften auch für $(\mathbb{Z}_m, +_m, \cdot_m)$. □

Definition 10.7 (Unterkörper, vgl. Definition 9.10 eines Unterringes)**.**
Es sei $(K, +, \cdot)$ ein Körper.

(*i*) Eine Teilmenge $U \subseteq K$ heißt ein **Teilkörper** oder **Unterkörper** (englisch: subfield) von $(K, +, \cdot)$, wenn U bzgl. $+$ und bzgl. $\cdot$ abgeschlossen ist und wenn $(U, +, \cdot)$ selbst wieder ein Körper ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, +)$ eine Untergruppe von $(K, +)$ ist und wenn $(U \setminus \{0\}, \cdot)$ eine Untergruppe von $(K \setminus \{0\}, \cdot)$ ist.

(*ii*) Ein Unterkörper $(U, +, \cdot)$ von $(K, +, \cdot)$ heißt **echt** (englisch: proper subfield), wenn $U \subsetneq K$ gilt. △

Beispiel 10.8 (Unterkörper)**.**

(*i*) $(\mathbb{Q}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{R}, +, \cdot)$.

(*ii*) $(\mathbb{R}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{C}, +, \cdot)$. △

Definition 10.9 (Körperhomomorphismus, vgl. Definition 9.11 eines Ringhomomorphismus)**.**
Es seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ zwei Körper.

(*i*) Eine Abbildung $f\colon K_1 \to K_2$ heißt **strukturverträglich** oder ein **(Körper-)Homomorphismus** (englisch: field homomorphism) von $(K_1, +_1, \cdot_1)$ in $(K_2, +_2, \cdot_2)$, wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in K_1, \tag{10.3a}$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in K_1, \tag{10.3b}$$
$$f(1_{K_1}) = 1_{K_2}. \tag{10.3c}$$

(*ii*) Wie in Definition 8.1 sprechen wir im Fall $(K_1, +_1, \cdot_1) = (K_2, +_2, \cdot_2)$ von einem **(Körper-)Endomorphismus** (englisch: field endomorphism).

(*iii*) Ist $f\colon K_1 \to K_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Körper-)Isomorphismus** (englisch: field isomorphism) In diesem Fall nennen wir $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ auch zueinander **isomorphe Körper** (englisch: isomorphic fields) und schreiben

$$(K_1, +_1, \cdot_1) \cong (K_2, +_2, \cdot_2).$$

(*iv*) Im Fall $(K_1, +_1, \cdot_1) = (K_2, +_2, \cdot_2)$ und $f\colon K_1 \to K_2$ bijektiv sprechen wir auch von einem **(Körper-)Automorphismus** (englisch: field automorphism). △

Da die Bedingungen (10.3) mit denen aus (9.4) übereinstimmen, ist ein Körperhomomorphismus nichts anderes als ein Ringhomomorphismus, der speziell zwischen Körpern eingesetzt wird. Insbesondere haben wir auch hier wie in (9.6) wieder

$$f(0_{K_1}) = 0_{K_2}. \tag{10.4}$$

Interessanterweise gilt weiter, dass Körperhomomorphismen automatisch injektiv sind, denn nehmen wir $a \neq b$, aber $f(a) = f(b)$ an, so ergibt sich der Widerspruch

$$\begin{aligned}
1_{K_2} &= f(1_{K_1}) && \text{wegen (10.3c)}\\
&= f\big((a -_1 b)^{-1} \cdot_1 (a -_1 b)\big) && \text{da } a -_1 b \neq 0_{K_1} \text{ vorausgesetzt wurde}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 f\big(a -_1 b\big) && \text{wegen (10.3a)}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 \big(f(a) -_2 f(b)\big) && \text{wegen (10.3b)}\\
&= f\big((a -_1 b)^{-1}\big) \cdot_2 0_{K_2} && \text{da } f(a) = f(b) \text{ vorausgesetzt wurde}\\
&= 0_{K_2} && \text{nach Lemma 9.3.}
\end{aligned}$$

§ 11 Polynome

Literatur: Beutelspacher, 2014, Kapitel 6, Bosch, 2014, Kapitel 5, Fischer, Springborn, 2020, Kapitel 2.3, Jänich, 2008, Kapitel 9.4

Definition 11.1 (Polynom)**.**
Es sei $(R, +, \cdot)$ ein kommutativer Ring.[14] Ein **Polynom** (englisch: polynomial, altgriechisch: *πολύ*: viel, altgriechisch: *όνομα*: Name) über R in der Variablen t ist ein formaler Ausdruck der Gestalt

$$a_n \cdot t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_1 \cdot t + a_0 \quad \text{oder auch} \quad \sum_{i=0}^{n} a_i \cdot t^i. \tag{11.1}$$

Dabei ist $n \in \mathbb{N}_0$. Die Zahlen $a_i \in R$ heißen die **Koeffizienten** (englisch: coefficients) des Polynoms. △

Bemerkung 11.2 (Polynom)**.**

(*i*) Die Variable t ist ein willkürlich gewähltes Symbol. Später werden wir für t geeignete Objekte einsetzen. Da zunächst unspezifiert ist, welche Objekte für die Variable t eingesetzt werden können, ist die Bedeutung der „Potenzen“ t^j, deren „Multiplikation“ mit den Koeffizienten $a_j \in R$ sowie die „Addition“ der daraus entstehenden Terme im Moment unklar. Daher verstehen wir (11.1) zunächst als formalen Ausdruck.

(*ii*) $a_1 \cdot t$ ist eine abkürzende Schreibweise für $a_1 \cdot t^1$, und a_0 ist eine abkürzende Schreibweise für $a_0 \cdot t^0$.

(*iii*) Die Reihenfolge der „Summanden“ in (11.1) ist unerheblich. Die Polynome $3 \cdot t^2 + 2 \cdot t$ und $2 \cdot t + 3 \cdot t^2$ werden also miteinander identifiziert.

(*iv*) Ist ein Koeffizient $a_i = 0_R \in R$, so lässt man häufig den entsprechenden „Summanden“ in der Darstellung (11.1) einfach weg. Die Polynome $3 \cdot t^2 + 0 \cdot t$ und $3 \cdot t^2$ werden also miteinander identifiziert.

[14] Tatsächlich ist R oft sogar ein Körper.

(*v*) Ist ein Koeffizient $a_i = 1_R$ in einem Ring mit dem Einselement 1_R, so lässt man den Koeffizienten 1_R in der Darstellung (11.1) manchmal weg, sofern es sich nicht um a_0 handelt. Die Polynome $1_R \cdot t^2$ und t^2 werden also miteinander identifiziert.

(*vi*) Die Menge aller Polynome über dem kommutativen Ring R in der Variablen t wird mit $R[t]$ bezeichnet.

(*vii*) Zwei Polynome sind gleich, wenn die entsprechenden Koeffizienten gleich sind.

(*viii*) Sind alle Koeffizienten gleich $0_R \in R$, so heißt das Polynom das **Nullpolynom** (englisch: zero polynomial), geschrieben 0_R.

(*ix*) Ist R ein Ring mit dem Einselement 1_R und sind alle Koeffizienten gleich $0_R \in R$ bis auf $a_0 = 1_R \in R$, so heißt das Polynom das **Einspolynom** (englisch: constant one polynomial), geschrieben 1_R.

(*x*) Ist R ein Ring mit dem Einselement 1_R, dann heißt ein Polynom der Form t^n das **Monom** (englisch: monomial) **vom Grad** $n \in \mathbb{N}_0$.[15]

(*xi*) Ein Polynom der Form $a_0 \in R \subseteq R[t]$ heißt ein **konstantes Polynom** (englisch: constant polynomial).

(*xii*) Ein Polynom der Form $a_0 + a_1 \cdot t \in R[t]$ mit $a_1 \neq 0_R$ heißt ein **lineares Polynom** (englisch: linear polynomial). △

Beispiel 11.3 (Polynome)**.**

(*i*) $p = \frac{3}{4} \cdot t^2 - 7 \cdot t + \frac{1}{2} = \frac{1}{2} + \frac{3}{4} \cdot t^2 - 7 \cdot t \in \mathbb{Q}[t]$ ist ein Polynom über dem Körper $\mathbb{Q}$.

(*ii*) $p = s^5 - \frac{\sqrt{2}}{3} \cdot s + \frac{2}{5} \in \mathbb{R}[s]$ ist ein Polynom über dem Körper $\mathbb{R}$.

(*iii*) $p = [1] \tilde{\cdot} X^3 \tilde{+} [3] \tilde{\cdot} X^2 \tilde{+} [2] \tilde{\cdot} X \in (\mathbb{Z}/4\mathbb{Z})[X]$ ist ein Polynom über dem Restklassenring $\mathbb{Z}/4\mathbb{Z}$. △

Wir definieren nun zwei Verknüpfungen + („Addition“) und · („Multiplikation“) auf der Menge $R[t]$ der Polynome über dem kommutativen Ring $(R, +, \cdot)$.[16] Es seien $p, q \in R[t]$ gegeben mit den Darstellungen

$$p = a_m \cdot t^m + \cdots + a_1 \cdot t + a_0 = \sum_{i=0}^{m} a_i \cdot t^i \tag{11.2a}$$

$$q = b_n \cdot t^n \ + \cdots + b_1 \cdot t + b_0 = \sum_{i=0}^{n} b_i \cdot t^i \tag{11.2b}$$

und $m, n \in \mathbb{N}_0$. Zur Abkürzung setzen wir außerdem $N := \max\{m, n\}$ und füllen in (11.2) nicht notierte Terme mit Nullkoeffizienten auf. Dann definieren wir die **Addition von Polynomen** (englisch: addition of polynomials)

$$p + q := (a_N + b_N) \cdot t^N + \cdots + (a_1 + b_1) \cdot t + (a_0 + b_0) = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) \cdot t^i \tag{11.3a}$$

[15] Der Begriff des Grades für beliebige Polynome wird in Definition 11.8 eingeführt.

[16] Es ist Absicht, dass die Verknüpfungen in $R[t]$ genauso benannt werden wie die Verknüpfungen im Koeffizientenring R. Dadurch wird $(R, +, \cdot)$ zu einem Unterring von $(R[t], +, \cdot)$, nämlich dem Unterring der konstanten Polynome.

sowie die **Multiplikation von Polynomen** (englisch: multiplication of polynomials)

$$p \cdot q \coloneqq c_{m+n} \cdot t^{m+n} + \cdots + c_1 \cdot t + c_0 \qquad = \sum_{k=0}^{m+n} c_k \cdot t^k, \tag{11.3b}$$

wobei c_k für $k \in \mathbb{N}_0$ als

$$c_k \coloneqq \sum_{i=0}^{k} a_i \cdot b_{k-i} = \sum_{\substack{i,j=0 \\ i+j=k}}^{k} a_i \cdot b_j \tag{11.3c}$$

gesetzt wird. Man nennt die aus (11.3c) entstehende Folge $(c_k)_{k\in\mathbb{N}_0}$, also

$$\begin{aligned} c_0 &= a_0 \cdot b_0 \\ c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0 \\ c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 \quad \text{usw.} \end{aligned}$$

die **Faltung** (englisch: convolution, lateinisch: convolvere: zusammenrollen) der Folgen $(a_i)_{i\in\mathbb{N}_0}$ und $(b_i)_{i\in\mathbb{N}_0}$.

Quizfrage 11.1: Wie kann man sich die Faltung der Koeffizientenfolgen $(a_i)_{i\in\mathbb{N}_0}$ und $(b_i)_{i\in\mathbb{N}_0}$ grafisch vorstellen?

Definition 11.4 (Polynomring)**.**
Es sei $(R, +, \cdot)$ ein kommutativer Ring. Mit den zwei Verknüpfungen (11.3) wird $(R[t], +, \cdot)$ zu einem kommutativen Ring, genannt der **Polynomring** (englisch: polynomial ring) **über** R in der Variablen t. R heißt der **Koeffizientenring** (englisch: coefficient ring, ring of coefficients) von $R[t]$. △

Das Nullelement von $R[t]$ ist das Nullpolynom 0_R. Besitzt R das Einselement 1_R, dann ist $(R[t], +, \cdot)$ ebenfalls ein Ring mit Einselement 1_R, dem Einspolynom. Das Symbol + aus (11.1) ist die gleichnamige Verknüpfung (11.3a) aus dem Polynomring. Das Symbol $\cdot$ aus (11.1) ist die gleichnamige Verknüpfung (11.3b) aus dem Polynomring, wobei ein Faktor ein Polynom der Form $a_i \in R$ ist und der andere Faktor ein Monom.

Bemerkung 11.5 (Polynomring als Erweiterung von $(R, +, \cdot)$)**.**
Wenn R ein Ring mit Eins, aber nicht der Nullring ist, so können wir den Polynomring $(R[t], +, \cdot)$ algebraisch auch verstehen als die (bis auf Ring-Isomorphie eindeutige) kleinstmögliche Erweiterung des kommutativen Ringes von $(R, +, \cdot)$ zu einem kommutativen Ring, der zusätzlich das freie Element $t \notin R$ enthält. Dadurch wird $(R, +, \cdot)$ zu ein Unterring von $(R[t], +, \cdot)$, dem Unterring der konstanten Polynome. △

Quizfrage 11.2: Wie sieht der Polynomring $R[t]$ aus, wenn R der Nullring ist?

Bemerkung 11.6 (Polynomring als Folgenring)**.**
Wir können ein Polynom identifizieren mit der Folge $\mathbb{N}_0 \to R$ (vgl. Definition 6.29) seiner in aufsteigender Reihenfolge der „Potenzen“ sortierten Koeffizienten, von denen nur endlich viele ungleich $0_R \in R$ sind. Man sagt, eine solche Folge habe **endlichen Träger**[17] (englisch: finite support). Diese Teilmenge von $R^{\mathbb{N}_0}$ notieren wir in dieser Lehrveranstaltung als $(R^{\mathbb{N}_0})_{00}$.

[17] Der **Träger einer Folge** (englisch: support of a sequence) mit Werten in einem Ring (oder allgemeiner mit Werten in einer additiven Gruppe) ist die Menge derjenigen Indizes, deren Folgenglieder ungleich dem Nullelement sind.

Beispielsweise kann das Polynom $t - t^2 + 3 \in \mathbb{Z}[t]$ identifiziert werden mit der endlich getragenen Folge $(3, 1, -1, 0, 0, \ldots)$ seiner Koeffizienten in $\mathbb{Z}$. Das Polynom p aus (11.2a) wird identifiziert mit der endlich getragenen Folge $(a_0, a_1, \ldots, a_m, 0, 0, \ldots)$. Statten wir dann $(R^{\mathbb{N}_0})_{00}$ mit der elementweisen Addition + der Folgenelemente und der Faltung als Multiplikation $c = a \cdot b$ wie in (11.3c) aus, so wird $((R^{\mathbb{N}_0})_{00}, +, \cdot)$ ebenfalls zu einem kommutativen Ring, der zu $R[t]$ isomorph ist. △

Ende der Vorlesung 13

Beispiel 11.7 (Addition und Multiplikation von Polynomen)**.**

(*i*) Für die Polynome

$$p = \frac{3}{4} \cdot t^2 - 7 \cdot t + \frac{1}{2}$$
$$q = -\frac{1}{2} \cdot t^3 - t + 1$$

über dem Körper $(\mathbb{Q}, +, \cdot)$ gilt

$$\begin{aligned} p + q &= \left(0 - \frac{1}{2}\right) \cdot t^3 + \left(\frac{3}{4} + 0\right) \cdot t^2 + \left(-7 + (-1)\right) \cdot t + \left(\frac{1}{2} + 1\right) \\ &= -\frac{1}{2} \cdot t^3 + \frac{3}{4} \cdot t^2 - 8 \cdot t + \frac{3}{2} \\ p \cdot q &= \left(0 + 0 + \frac{3}{4} \cdot \left(-\frac{1}{2}\right) + 0 + 0 + 0\right) \cdot t^5 + \left(0 + (-7) \cdot \left(-\frac{1}{2}\right) + 0 + 0 + 0\right) \cdot t^4 \\ &\quad + \left(\frac{1}{2} \cdot \left(-\frac{1}{2}\right) + 0 + \frac{3}{4} \cdot (-1) + 0\right) \cdot t^3 + \left(0 + (-7) \cdot (-1) + \frac{3}{4} \cdot 1\right) \cdot t^2 \\ &\quad + \left(\frac{1}{2} \cdot (-1) + (-7) \cdot 1\right) \cdot t + \left(\frac{1}{2} \cdot 1\right) \\ &= -\frac{3}{8} \cdot t^5 + \frac{7}{2} \cdot t^4 - t^3 + \frac{31}{4} \cdot t^2 - \frac{15}{2} \cdot t + \frac{1}{2}. \end{aligned}$$

Berechnung der Koeffizienten des Produkts $p \cdot q$ mittels Faltungstabelle:

	$\frac{1}{2}$	-7	$\frac{3}{4}$	0
1	$\frac{1}{2}$	-7	$\frac{3}{4}$	0
-1	$-\frac{1}{2}$	7	$-\frac{3}{4}$	0
0	0	0	0	0
$-\frac{1}{2}$	$-\frac{1}{4}$	$\frac{7}{2}$	$-\frac{3}{8}$	0

Die Summation entlang der Diagonalen ergibt wiederum die Koeffizienten

$$c_0 = \frac{1}{2}, \qquad c_1 = -\frac{1}{2} - 7 = -\frac{15}{2}, \qquad c_2 = 0 + 7 + \frac{3}{4} = \frac{31}{4},$$
$$c_3 = -\frac{1}{4} + 0 - \frac{3}{4} + 0 = -1, \qquad c_4 = \frac{7}{2} + 0 + 0 = \frac{7}{2}, \qquad c_5 = -\frac{3}{8} + 0 = -\frac{3}{8}.$$

(*ii*) Für die Polynome

$$p = [1] \tilde{\cdot} X^3 \tilde{+} [-3] \tilde{\cdot} X^2 \tilde{+} [2] \tilde{\cdot} X \qquad \text{oder auch } p = X^3 \tilde{+} X^2 \tilde{+} [2] \tilde{\cdot} X$$
$$q = [-1] \tilde{\cdot} X \tilde{+} [7] \qquad \text{oder auch } q = [3] \tilde{\cdot} X \tilde{+} [3]$$

über dem Restklassenring $\mathbb{Z}/4\mathbb{Z}$ gilt

$$\begin{aligned}(p \mathbin{\tilde{+}} q)(X) &= [1] \mathbin{\tilde{\cdot}} X^3 \mathbin{\tilde{+}} [1] \mathbin{\tilde{\cdot}} X^2 \mathbin{\tilde{+}} \big([2] \mathbin{\tilde{+}} [-1]\big) \mathbin{\tilde{\cdot}} X \mathbin{\tilde{+}} [7] \\ &= [1] \mathbin{\tilde{\cdot}} X^3 \mathbin{\tilde{+}} [1] \mathbin{\tilde{\cdot}} X^2 \mathbin{\tilde{+}} [1] \mathbin{\tilde{\cdot}} X \mathbin{\tilde{+}} [3],\end{aligned}$$

$$\begin{aligned}(p \mathbin{\tilde{\cdot}} q)(X) &= [1] \mathbin{\tilde{\cdot}} [-1] \mathbin{\tilde{\cdot}} X^4 \mathbin{\tilde{+}} \big([-3] \mathbin{\tilde{\cdot}} [-1] \mathbin{\tilde{+}} [1] \mathbin{\tilde{\cdot}} [7]\big) \mathbin{\tilde{\cdot}} X^3 \\ &\qquad \mathbin{\tilde{+}} \big([-3] \mathbin{\tilde{\cdot}} [7] \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} [-1]\big) \mathbin{\tilde{\cdot}} X^2 \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} [7] \mathbin{\tilde{\cdot}} X \\ &= [3] \mathbin{\tilde{\cdot}} X^4 \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} X^3 \mathbin{\tilde{+}} [1] \mathbin{\tilde{\cdot}} X^2 \mathbin{\tilde{+}} [2] \mathbin{\tilde{\cdot}} X.\end{aligned}$$

△

Zur Vereinfachung der Notation lassen wir in Zukunft das Multiplikationszeichen zwischen Koeffizient und Potenz einer Variable auch oft weg.

Definition 11.8 (Grad eines Polynoms, führender Koeffizient, monisches Polynom)**.**
Es sei p ein Polynom über dem kommutativen Ring R mit den Koeffizienten $a_j \in R$, $j \in \mathbb{N}_0$.

(*i*) Der **Grad** (englisch: degree) ist definiert als[18]

$$\deg(p) \coloneqq \begin{cases} -\infty, & \text{falls alle } a_j = 0_R \text{ sind, also } p = 0_R, \\ \max\{j \in \mathbb{N}_0 \mid a_j \neq 0_R\} & \text{sonst.} \end{cases} \tag{11.4}$$

Ein Polynom vom Grad 0 oder $-\infty$ heißt **konstant** (englisch: constant).

(*ii*) Wenn $p \neq 0_R$ (also nicht das Nullpolynom) ist, dann heißt $\ell(p) \coloneqq a_{\deg(p)}$ auch der **führende Koeffizient** (englisch: leading coefficient) oder der **Leitkoeffizient** von p. Für $p = 0_R$ definieren wir $\ell(0_R) = 0_R$.

(*iii*) Ist R ein Ring mit dem Einselement 1_R und gilt $\ell(p) = 1_R$, dann heißt das Polynom p **normiert** oder **monisch** (englisch: monic). △

Quizfrage 11.3: Was weiß man über das Produkt zweier monischer Polynome?

Beispiel 11.9 (Grad eines Polynoms, führender Koeffizient, monisches Polynom)**.**

(*i*) Das Polynom $p = \frac{3}{4}t^2 - 7t + \frac{1}{2} \in \mathbb{Q}[t]$ über dem Körper $\mathbb{Q}$ besitzt $\deg(p) = 2$. Das Polynom p ist nicht monisch, da $\ell(p) = \frac{3}{4} \neq 1 \in \mathbb{Q}$ ist.

(*ii*) Das Polynom $p = [-7]X^3 \mathbin{\tilde{+}} [-3]X^2 \mathbin{\tilde{+}} [2]X^2 \in (\mathbb{Z}/4\mathbb{Z})[X]$ über dem Restklassenring $\mathbb{Z}/4\mathbb{Z}$ besitzt $\deg(3)$. Das Polynom p ist monisch, da $\ell(p) = [-7] = [1] \in \mathbb{Z}/4\mathbb{Z}$ ist. △

Lemma 11.10 (Grad eines Polynoms)**.**
Es sei R ein kommutativer Ring und $p, q \in R[t]$ zwei Polynome. Dann gilt:

(*i*) $\deg(p+q) \leqslant \max\{\deg(p),\ \deg(q)\}$.

(*ii*) $\deg(p \cdot q) \leqslant \deg(p) + \deg(q)$.

(*iii*) Ist R nullteilerfrei, dann gilt sogar $\deg(p \cdot q) = \deg(p) + \deg(q)$.

Dabei sollen formal für $n \in \mathbb{N}_0$ die Beziehungen $\max\{n,\ (-\infty)\} = \max\{(-\infty), n\} = n$ gelten sowie $\max\{(-\infty),\ (-\infty)\} = -\infty$ und $n + (-\infty) = (-\infty) + n = (-\infty) + (-\infty) = -\infty$.

[18] Manchmal wird der Grad des Nullpolynoms abweichend auch als -1 definiert.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 7.3. □

Folgerung 11.11 (der Polynomring als Integritätsring)**.**
Es sei R ein Integritätsring. Dann ist auch $R[t]$ ein Integritätsring.

Beweis. Nach Definition ist R ein kommutativer, nullteilerfreier Ring mit Eins 1_R, und R ist ungleich dem Nullring. Folglich ist $R[t]$ ein kommutativer Ring mit Eins 1_R (Einspolynom) ungleich dem Nullring, da $1_R \neq 0_R$ (Nullpolynom) gilt. Es bleibt zu zeigen, dass $R[t]$ nullteilerfrei ist. Dazu seien $p, q \in R[t]$ beide nicht das Nullpolynom. Aus Lemma 11.10 Aussage *(iii)* folgt $\deg(p \cdot q) = \deg(p) + \deg(q) \geqslant 0$. Damit ist auch $p \cdot q$ nicht das Nullpolynom. □

§ 11.1 Polynomdivision

Lemma 11.12 (Polynomring ist kein Körper)**.**
Der Polynomring $R[t]$ ist niemals ein Körper.

Beweis. Wenn R der Nullring ist, dann ist auch $R[t]$ der Nullring, besitzt also nur ein Element und ist daher kein Körper (Lemma 10.3). Wir betrachten also im Weiteren nur den Fall, dass R nicht der Nullring ist. Wenn $R[t]$ ein Körper wäre, dann wäre 1_R das neutrale Element bzgl. der Multiplikation in $R[t]$ und damit auch in R. Daraus folgt, dass das Polynom $p = 0_R + 1_R \cdot t$ in $R[t]$ existiert. Dieses besitzt aber kein multiplikatives Inverses, denn: Wäre q das Inverse zu p, gälte also $p \cdot q = 1_R$, dann kann q nicht das Nullpolynom sein. Es müsste also $q = b_n\, t^n + \cdots + b_1\, t + b_0$ gelten für irgendwelche Koeffizienten $b_0, b_1, \ldots, b_n$, $n \in \mathbb{N}_0$. Der 0-te Koeffizient von $p \cdot q$ ist aber $0_R \cdot b_0 = 0_R$, und daher kann $p \cdot q$ nicht das Einspolynom sein. □

Als Ersatz für das Fehlen multiplikativer Inverser führen wir (wie bereits aus $\mathbb{Z}$ bekannt) eine **Division mit Rest** (englisch: division with remainder) von Polynomen ein. Wir arbeiten dabei für den Rest von § 11.1 mit einem Körper K für die Koeffizienten an Stelle eines kommutativen Ringes R.

Definition 11.13 (Teiler eines Polynoms)**.**
Es seien K ein Körper und $p_1, p_2 \in K[t]$ zwei Polynome. p_2 heißt ein **Teiler** (englisch: divisor) von p_1 (kurz: $p_2 \mid p_1$), wenn es ein weiteres Polynom $q \in K[t]$ gibt, sodass gilt:

$$p_1 = q \cdot p_2. \tag{11.5}$$

△

Satz 11.14 (Polynomdivision mit Rest)**.**
Es seien K ein Körper und $p_1, p_2 \in K[t]$ zwei Polynome. Ist $p_2 \neq 0_K$ (Nullpolynom), dann gibt es eindeutig bestimmte Polynome $q, r \in K[t]$, genannt der **Quotient** (englisch: quotient) und der **Rest** (englisch: remainder), sodass gilt:

$$p_1 = q \cdot p_2 + r \quad \text{und} \quad \deg(r) < \deg(p_2). \tag{11.6}$$

Beweis. Wir zeigen zunächst die Existenz der Zerlegung (11.6). Dazu sei $p_2 \in K[t]$ fest und $\deg(p_2) = m \in \mathbb{N}_0$. Wir verwenden vollständige Induktion nach $n := \deg(p_1) \in \mathbb{N}_0 \cup \{-\infty\}$.

Induktionsanfang: Für jedes $n \in \{-\infty\} \cup [\![0, m-1]\!]$ (also wenn $\deg(p_1) < \deg(p_2)$ gilt) setzen wir $q := 0_K$ und $r := p_1$.

Induktionsschritt: Es sei $n \geqslant m$ und die Behauptung für $n-1$ bereits bewiesen. Es sei nun $n = \deg(p_1) \geqslant \deg(p_2)$. Die Darstellungen von p und q seien

$$\begin{aligned} p_1 &= a_n\, t^n \ + a_{n-1}\, t^{n-1} \ + \cdots + a_1\, t + a_0, \\ p_2 &= b_m\, t^m + b_{m-1}\, t^{m-1} + \cdots + b_1\, t + b_0. \end{aligned}$$

Wir definieren $\widehat{p}_1 := p_1 - a_n\, b_m^{-1}\, t^{n-m} p_2$. Dann ist der Koeffizient von t^n in $\widehat{p}_1$ gleich 0_K. Damit gilt $\deg(\widehat{p}_1) < \deg(p_1)$. Nach Induktionsvoraussetzung existieren also $\widehat{q}, \widehat{r} \in K[t]$ mit der Eigenschaft $\widehat{p}_1 = \widehat{q}_1 \cdot p_2 + \widehat{r}$ und $\deg(\widehat{r}) < \deg(p_2) = m$. Es folgt nun

$$\begin{aligned} p_1 &= \widehat{p}_1 + a_n\, b_m^{-1}\, t^{n-m} p_2 && \text{nach Definition von } \widehat{p}_1 \\ &= \widehat{q}_1 \cdot p_2 + \widehat{r} + a_n\, b_m^{-1}\, t^{n-m} p_2 && \text{gemäß der Zerlegung von } \widehat{p}_1 \\ &= \underbrace{\left(\widehat{q}_1 + a_n\, b_m^{-1}\, t^{n-m}\right)}_{=:q} \cdot p_2 + \underbrace{\widehat{r}}_{=:r} && \text{wegen der Kommutativität und Distributivität im Ring } K[t]. \end{aligned}$$

Dabei gilt $\deg(r) = \deg(\widehat{r}) < \deg(p_2) = m$.

Es bleibt, die Eindeutigkeit der Zerlegung zu bestätigen. Angenommen, es gelte

$$p_1 = q \cdot p_2 + r = \widehat{q} \cdot p_2 + \widehat{r}$$

mit $\deg(r) < \deg(p_2)$ und $\deg(\widehat{r}) < \deg(p_2)$. Dann folgt $(q - \widehat{q}) \cdot p_2 = \widehat{r} - r$ und weiter

$$\begin{aligned} \deg(p_2) &> \deg(r - \widehat{r}) && \text{da } \deg(r - \widehat{r}) \leqslant \max\{\deg(r),\ \deg(-\widehat{r})\} \text{ nach Lemma 11.10} \\ &= \deg((q - \widehat{q}) \cdot p_2) \\ &= \deg(q - \widehat{q}) + \deg(p_2) && \text{nach Lemma 11.10, da } K \text{ als Körper nullteilerfrei ist.} \end{aligned}$$

Deshalb gilt $\deg(q - \widehat{q}) < 0$, woraus $q - \widehat{q} = 0_K$ folgt, also $q = \widehat{q}$. Aus $q \cdot p_2 + r = \widehat{q} \cdot p_2 + \widehat{r}$ folgt dann auch $r = \widehat{r}$. □

Folgerung 11.15 (Polynomdivision mit Rest)**.**
Unter den Voraussetzungen von Definition 11.13 ist q in (11.5) eindeutig bestimmt.

Beispiel 11.16 (Polynomdivision mit Rest)**.**
Die **Polynomdivision** (englisch: polynomial long division) ist ein Verfahren zur Berechnung der Zerlegung (11.6) für zwei gegebene Polynome $p_1, p_2 \in K[t]$. Man sortiert dazu p_1 und p_2 nach absteigenden Potenzen der Variablen und führt dieselben Schritte wie bei einer schriftlichen Division etwa in $\mathbb{Z}$ durch. Sobald der Grad des aktuellen Restes echt kleiner ist als der Grad von p_2, stoppt das Verfahren.

Für $p_1 = 3t^3 + 2t + 1$ und $p_2 = t^2 - 4t$ erhalten wir

$$\begin{array}{rl} 3t^3 & + 2t + 1 = (t^2 - 4t)(3t + 12) + 50t + 1 \\ \underline{-\,3t^3 + 12t^2} & \\ 12t^2 & + 2t \\ \underline{-\,12t^2 + 48t} & \\ & 50t + 1 \end{array}$$

Also gilt in diesem Beispiel

$$\underbrace{3t^3 + 2t + 1}_{p_1} = \underbrace{(3t + 12)}_{q} \cdot \underbrace{(t^2 - 4t)}_{p_2} + \underbrace{(50t + 1)}_{r}. \qquad \triangle$$

§ 11.2 Polynomfunktionen

Wir gehen nun der Frage nach, welche Objekte man für die Variable t in einem Polynom

$$p = a_n\, t^n + a_{n-1}\, t^{n-1} + \cdots + a_1\, t + a_0 \tag{11.7}$$

über einem kommutativen Ring $(R, +, \cdot)$ sinnvollerweise einsetzen kann. Die naheliegendste Wahl sind sicherlich Elemente aus R selbst, und nur diese lassen wir im Moment zu.

Genauer betrachtet induziert das Polynom p eine Funktion $\widetilde{p}\colon R \to R$, definiert durch

$$\widetilde{p}(r) := a_n\, r^n + a_{n-1}\, r^{n-1} + \cdots + a_1\, r + a_0. \tag{11.8}$$

Die Funktion $\widetilde{p}$ heißt die **Polynomfunktion** (englisch: polynomial function) zum Polynom p oder die vom Polynom p induzierte Polynomfunktion.

Bemerkung 11.17 (induzierte Polynomfunktion)**.**
Die Menge R^R der Funktionen $R \to R$, ausgestattet mit den punktweisen Verknüpfungen + und · aus R, bildet einen kommutativen Ring $(R^R, +, \cdot)$. Die Abbildung

$$\Phi\colon (R[t], +, \cdot) \ni p \mapsto \widetilde{p} \in (R^R, +, \cdot) \tag{11.9}$$

ist ein Ringhomomorphismus zwischen zwei kommutativen Ringen. Wenn R das Einselement 1_R besitzt, dann besitzt $R[t]$ das Einselement 1_R (das Einspolynom) und R^R das Einselement 1_R (die Einsabbildung $R \mapsto 1_R$), und es gilt $\Phi(1_R) = 1_R$.

Φ ist i. A. nicht injektiv. Verschiedene Polynome können also dieselbe Polynomfunktion induzieren. Wir betrachten als Beispiel den Körper $K = (\mathbb{Z}_2, +_2, \cdot_2)$ und das Polynom

$$p = t^2 + t.$$

Dann ist die zugehörige Polynomfunktion $K \to K$ gerade $\widetilde{p}(t) = t^2 +_2 t = t \cdot_2 t +_2 t$. Diese erfüllt $p(0) = 0 \cdot_2 0 +_2 0 = 0 +_2 0 = 0$ sowie $p(1) = 1 \cdot_2 1 +_2 1 = 1 +_2 1 = 0$. Es ist also $\widetilde{p}$ die Nullfunktion, obwohl p nicht das Nullpolynom ist. Da das Nullpolynom ebenfalls die Nullfunktion induziert, ist die Zuordnung $p \mapsto \widetilde{p}$ in der Tat nicht injektiv.

Φ ist i. A. auch nicht surjektiv. Bild(Φ) ist der Unterring der Polynomfunktionen des Ringes $(R^R, +, \cdot)$. $\triangle$

Definition 11.18 (Nullstelle eines Polynoms)**.**
Es sei R ein kommutativer Ring, $p \in R[t]$ ein Polynom und $\widetilde{p}\colon R \to R$ die zugehörige Polynomfunktion. $\lambda \in R$ heißt eine **Nullstelle** (englisch: zero) oder **Wurzel** (englisch: root) von p in R, wenn $\widetilde{p}(\lambda) = 0_R$ gilt. $\triangle$

Beispiel 11.19 (Nullstelle eines Polynoms)**.**

(*i*) Das Polynom $p = t^2 + 1 \in \mathbb{R}[t]$ besitzt keine Nullstelle in $\mathbb{R}$, weil für die zugehörige Polynomfunktion $\widetilde{p}\colon \mathbb{R} \to \mathbb{R}$ gilt: $\widetilde{p}(t) = t^2 + 1 \geqslant 1$ für alle $t \in \mathbb{R}$.

(*ii*) Das Polynom $p = t^2 + 1 \in \mathbb{C}[t]$ besitzt aber zwei Nullstellen in $\mathbb{C}$, und zwar i und $-i$.

(*iii*) Das Polynom $p = t^2 + 1 \in \mathbb{Z}_5[t]$ besitzt in $\mathbb{Z}_5$ genau die Nullstellen 2 und 3, da für die zugehörige Polynomfunktion $\widetilde{p}\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ gilt: $\widetilde{p}(t) = t \cdot_5 t +_5 1$ und damit

$$\begin{aligned}
\widetilde{p}(0) &= 0 \cdot_5 0 +_5 1 = 1,\\
\widetilde{p}(1) &= 1 \cdot_5 1 +_5 1 \ = 2,\\
\widetilde{p}(2) &= 2 \cdot_5 2 +_5 1 = 0,\\
\widetilde{p}(3) &= 3 \cdot_5 3 +_5 1 = 0,\\
\widetilde{p}(4) &= 4 \cdot_5 4 +_5 1 = 2.
\end{aligned}$$

(*iv*) Das Polynom $p = (t-0)\cdot(t-1)\cdot(t-2)\cdot(t-3)\cdot(t-4)+1$, besitzt in $\mathbb{Z}_5$ *keine* Nullstelle, denn es gilt $\widetilde{p}(t) = 1$ für alle $t \in \mathbb{Z}_5$. (Ein solches Polynom gibt es für jeden endlichen Körper.) △

Lemma 11.20 (Nullstellen und Teiler)**.**
Es seien K ein Körper und $p \in K[t]$ ein Polynom. Dann sind äquivalent:

(*i*) $\lambda \in K$ ist eine Nullstelle von p.

(*ii*) Das Polynom $t - \lambda \in K[t]$ ist ein Teiler von p.

In diesem Fall gilt für das eindeutig bestimmte Polynom $q \in K[t]$ mit $p = (t-\lambda)\cdot q$ die Eigenschaft $\deg(q) = \deg(p) - 1$.

Beweis. Aussage (*i*) ⇒ Aussage (*ii*): Es sei $\lambda \in K$ eine Nullstelle von p, also $\widetilde{p}(\lambda) = 0$. Nach Satz 11.14 gibt es (eindeutig bestimmte) Polynome $q, r \in K[t]$, sodass gilt: $p = q\cdot(t-\lambda) + r$ und $\deg(r) < \deg(t-\lambda) = 1$. Also ist r ein konstantes Polynom. Um es zu bestimmen, ist es ausreichend, den Wert der zugehörigen Polynomfunktion $\widetilde{r}$ an einer Stelle zu kennen. An der Stelle λ gilt

$$\widetilde{r}(\lambda) = \big(\widetilde{p} - \widetilde{q}\cdot(t-\lambda)\big)(\lambda) = \widetilde{p}(\lambda) - \widetilde{q}(\lambda)\cdot(\lambda-\lambda) = \widetilde{p}(\lambda) = 0_K$$

gilt. Also ist r das Nullpolynom, und es folgt $p = q\cdot(t-\lambda)$, d. h., $t-\lambda$ ist ein Teiler von p.

Aussage (*ii*) ⇒ Aussage (*i*): Es sei $t-\lambda$ ein Teiler von p, also existiert ein $q \in K[t]$ mit der Eigenschaft $p = q\cdot(t-\lambda)$. Das Einsetzen von λ liefert $\widetilde{p}(\lambda) = \widetilde{q}(\lambda)\cdot(\lambda-\lambda) = \widetilde{q}(\lambda)\cdot 0_K = 0_K$. Also ist λ eine Nullstelle von p.

Weiter gilt nach Lemma 11.10 (*iii*) $\deg(p) = \deg(q\cdot(t-\lambda)) = \deg(q) + 1$. □

Satz 11.21 (Zerlegung eines Polynoms)**.**
Es seien K ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0_K$. Dann gilt:

(*i*) Es existieren $s \in \mathbb{N}_0$, paarweise verschiedene Zahlen $\lambda_1, \ldots, \lambda_s \in K$ sowie Exponenten $n_1, \ldots, n_s \in \mathbb{N}$ und ein Polynom $q \in K[t]$ ohne Nullstelle in K, sodass gilt:

$$p = (t-\lambda_1)^{n_1}\cdot\cdots\cdot(t-\lambda_s)^{n_s}\cdot q. \tag{11.10}$$

Die Zahl $n_i \in \mathbb{N}$ heißt die **Vielfachheit** (englisch: multiplicity) der Nullstelle λ_i. Jedes Polynom $t-\lambda_i \in K[t]$ heißt ein **Linearfaktor** (englisch: linear factor) von p.

(*ii*) Die Nullstellen von p sind genau die Zahlen $\lambda_1, \dots, \lambda_s \in K$.

Beweis. Aussage (*i*): Wir führen eine Induktion nach $n := \deg(p)$ durch. Im Fall $n = 0$ (Induktionsanfang) ist p ein konstantes Polynom ungleich 0_K, das keine Nullstelle besitzt. Daher ist dann $s = 0$ und $q = p$.

Wir nehmen an, die Behauptung sei bereits gezeigt für Polynome vom Grad $n \in \mathbb{N}_0$. Es sei p nun ein Polynom vom Grad $n+1$. Wenn p keine Nullstelle besitzt, so gilt die Behauptung mit $s = 0$ und $q = p$. Andernfalls besitzt p eine Nullstelle $\lambda \in K$. Nach Lemma 11.20 ist also $t - \lambda \in K[T]$ ein Teiler von p, d. h., es gilt $p = (t-\lambda) \cdot \widehat{p}$. Aus Lemma 11.10 folgt $n+1 = \deg(p) = \deg(t-\lambda) + \deg(\widehat{p}) = 1 + \deg(\widehat{p})$, also gilt $\deg(\widehat{p}) = n$. Nach Induktionsvoraussetzung besitzt also $\widehat{p}$ eine Darstellung wie in (11.10), somit auch $p = (t-\lambda) \cdot \widehat{p}$.

Aussage (*ii*): Ist $\mu \in K$ eine Nullstelle von p, dann folgt

$$0 = \widetilde{p}(\mu) = (\mu - \lambda_1)^{n_1} \cdot \dots \cdot (\mu - \lambda_s)^{n_s} \cdot \widetilde{q}(\mu).$$

Da K als Körper nullteilerfrei ist, muss einer der Faktoren gleich 0_K sein. Da aber q nach Voraussetzung keine Nullstelle besitzt, muss es ein $i \in [\![1, s]\!]$ geben mit $\mu = \lambda_i$.

Umgekehrt ist nach Lemma 11.20 jedes λ_i, $i \in [\![1, s]\!]$, eine Nullstelle von p. □

Beachte: Man kann zeigen, dass die Darstellung (11.10) bis auf die Reihenfolge der Faktoren eindeutig ist.

Folgerung 11.22 (Zerlegung eines Polynoms)**.**
Es seien K ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0_K$. Dann gilt:

(*i*) p hat höchstens $\deg(p) \in \mathbb{N}_0$ viele paarweise verschiedene Nullstellen, also $s \leqslant \deg(p)$.

(*ii*) p hat höchstens $\deg(p) \in \mathbb{N}_0$ viele Nullstellen, wenn diese entsprechend ihrer Vielfachheit gezählt werden, also gilt $\sum_{i=1}^{s} n_i \leqslant \deg(p)$.

Beweis. Aussage (*i*): Es sei (11.10) die (i. W. eindeutige) Zerlegung von p mit $s \in \mathbb{N}_0$ paarweise verschiedenen Nullstellen von p. Dann gilt

$$\begin{aligned} \deg(p) &= \deg(q) + \sum_{i=0}^{s} n_i && \text{nach Lemma 11.10} \\ &\geqslant 0 + \sum_{i=0}^{s} 1 && q \neq 0_K \text{ und die Vielfachheit jeder Nullstelle ist} \geqslant 1 \\ &= s. \end{aligned}$$

Aussage (*ii*): Zählen wir die Nullstellen λ_i in (11.10) gemäß ihrer Vielfachheit n_i, so erhalten wir

$$\begin{aligned} \deg(p) &= \deg(q) + \sum_{i=0}^{s} n_i && \text{nach Lemma 11.10} \\ &\geqslant 0 + \sum_{i=1}^{s} n_i. \end{aligned}$$

□

In Bemerkung 11.17 hatten wir gesehen, dass die Abbildung Polynom $p \mapsto$ Polynomfunktion $\widetilde{p}$ i. A. nicht injektiv ist, weil auch Nicht-Nullpolynome auf die Nullfunktion abgebildet werden können. Das Beispiel dafür war ein Polynom über dem endlichen Körper $\mathbb{Z}_2$. Wie folgendes Ergebnis zeigt, ist die Endlichkeit des Körpers charakteristisch für die Nichtinjektivität von Φ.

Folgerung 11.23.
Es sei K ein unendlicher Körper. Dann ist die Abbildung $\Phi\colon K[t] \to K^K$ aus (11.9) injektiv.

Beweis. Es seien $p_1, p_2 \in K[t]$ Polynome und $\widetilde{p_1} = \widetilde{p_2}$ die zugehörigen Polynomfunktionen. Wir setzen $q := p_1 - p_2$. Wegen $\widetilde{q} = \widetilde{p_1} - \widetilde{p_2} = 0_K$ (**Quizfrage 11.4:** Warum gilt diese Gleichheit?) hat q unendlich viele Nullstellen, nämlich alle Elemente aus K. Das widerspricht Folgerung 11.22, es sei denn, q ist das Nullpolynom. Daher gilt $p_1 = p_2$, d. h., die Injektivität von Φ. □

Satz 11.24 (Fundamentalsatz der Algebra[19]).
Jedes Polynom $p \in \mathbb{C}[t]$ mit $\deg(p) > 0$ hat mindestens eine Nullstelle.

Ein Beweis dieses Satz wird i. d. R. in weiterführenden Veranstaltungen über *Funktionentheorie* oder *Algebra* vorgestellt.

Folgerung 11.25 (nicht-konstante Polynome über den komplexen Zahlen $\mathbb{C}$ zerfallen in Linearfaktoren)**.**

Jedes nicht-konstante Polynom $p \in \mathbb{C}[t]$ zerfällt vollständig in Linearfaktoren. In der Darstellung (11.10) gilt also $\deg(q) = 0$.

Beweis. Der Beweis gelingt mit vollständiger Induktion nach $n = \deg(p)$ und Anwendung des Fundamentalsatzes 11.24. □

Ende der Vorlesung 14

Ende der Woche 7

[19] englisch: fundamental theorem of algebra

Kapitel 3 Vektorräume

§ 12 Vektorräume

Literatur: Beutelspacher, 2014, Kapitel 3, Bosch, 2014, Kapitel 1, Fischer, Springborn, 2020, Kapitel 2.4–2.6, Jänich, 2008, Kapitel 2

Vektorräume sind die zentralen Strukturen in der *linearen* Algebra. Zu einem Vektorraum V gehört immer ein zugrundeliegender Körper, sagen wir $(K, +, \cdot)$. In Anlehnung an dessen Verknüpfungen bezeichnen wir die beiden Verknüpfungen im Vektorraum V mit $\oplus$ und $\odot$.

Definition 12.1 (Vektorraum)**.**
Es sei $(K, +, \cdot)$ ein Körper. Ein **Vektorraum** (englisch: vector space) oder **linearer Raum** (englisch: linear space) $(V, \oplus, \odot)$ **über** K (kurz: ein K-Vektorraum) ist eine Menge V mit einer inneren Verknüpfung $\oplus\colon V \times V \to V$ und einer **äußeren Verknüpfung** (englisch: (outer) operation) $\odot\colon K \times V \to V$, die die folgenden Bedingungen erfüllen:

(*i*) $(V, \oplus)$ ist eine abelsche Gruppe. Das Nullelement bezeichnen wir mit 0_V.

(*ii*) Für die Verknüpfung $\odot$, genannt **skalare Multiplikation** (englisch: scalar multiplication) oder **S-Multiplikation**, gelten die folgenden Gesetze für alle $\alpha, \beta \in K$ und $u, v \in V$: die **„gemischten" Distributivgesetze**[1] (englisch: „mixed" distributive laws)

$$\alpha \odot (u \oplus v) = (\alpha \odot u) \oplus (\alpha \odot v) \tag{12.1a}$$
$$(\alpha + \beta) \odot v = (\alpha \odot v) \oplus (\beta \odot v) \tag{12.1b}$$

sowie das **„gemischte" Assoziativgesetz** (englisch: „mixed" associative law)

$$(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v). \tag{12.1c}$$

Weiterhin ist das neutrale Element 1_K bzgl. $\cdot$ in K auch neutral bzgl. $\odot$:

$$1_K \odot v = v. \tag{12.1d}$$

(*iii*) In einem K-Vektorraum V heißen die Elemente von V auch **Vektoren** (englisch: vectors). Das Nullelement 0_V von $(V, \oplus)$ heißt auch der **Nullvektor** (englisch: zero vector). Die Elemente von K heißen **Skalare** (englisch: scalars), und K selbst heißt der **Skalarkörper** (englisch: scalar field) von V. △

Bemerkung 12.2 (abkürzende Schreibweisen)**.**

(*i*) Das Inverse zu $v \in V$ bzgl. $\oplus$ bezeichnen wir mit $\ominus v$. Die Bezeichnung $u \ominus v$ steht für $u \oplus (\ominus v)$.

[1] Wir bezeichnen die Gesetze hier als „gemischt", weil in ihnen Skalare $\alpha, \beta \in K$ mit Vektoren $u, v \in V$ gemischt auftauchen.

(*ii*) Wir vereinbaren, dass $\odot$ stärker bindet als $\oplus$, also könnten wir die rechte Seite in (12.1a) auch in der Form $\alpha \odot u \oplus \alpha \odot v$ schreiben.

(*iii*) Die Konvention, dass bei der skalaren Multiplikation $\odot\colon K \times V \to V$ die Skalare auf der linken Seite stehen, ist willkürlich. Wir können parallel auch $\boxdot\colon V \times K \to V$ definieren, und zwar durch $v \boxdot \alpha := \alpha \odot v$. Dann gelten auch dafür die Gesetze (12.1), wobei überall $\odot$ durch $\boxdot$ ersetzt wird und die beiden Argumente dieser Verknüpfung vertauscht werden. Aufgrund der Ähnlichkeit unterscheiden wir nicht zwischen der linken skalaren Multiplikation $\odot$ und der rechten skalaren Multiplikation $\boxdot$, sondern schreiben in Zukunft einfach $\odot$ für beide.

(*iv*) Wir behalten die unterschiedliche Notation der Verknüpfungen „+“ in K und „$\oplus$“ in V wie auch von „$\cdot$“ in K und „$\odot$“ in V zur Verdeutlichung zunächst bei. Später werden wir diese jedoch nur noch als „+“ bzw. „$\cdot$“ notieren, siehe Bemerkung 12.10.

(*v*) Wir werden im Folgenden statt von einem „Vektorraum $(V, \oplus, \odot)$ über dem Körper $(K, +, \cdot)$“ auch einfach von einem „Vektorraum $(V, \oplus, \odot)$“ sprechen, wenn der zugrundeliegende Körper aus dem Zusammenhang klar ist oder wenn wir uns nicht explizit auf ihn beziehen müssen. △

Beispiel 12.3 (Vektorraum)**.**

(*i*) Über jedem Körper $(K, +, \cdot)$ gibt es den (bis auf Isomorphie eindeutigen) Vektorraum $(V, \oplus, \odot)$ mit nur einem Element, nämlich $V = \{0_V\}$. Die Verknüpfungen $\oplus$ und $\odot$ sind dann eindeutig festgelegt. Dieser Raum heißt **Nullraum** (englisch: zero vector space) über K.

(*ii*) Jeder Körper $(K, +, \cdot)$, ausgestattet mit den Verknüpfungen $\oplus := +$ und $\odot := \cdot$, ist ein Vektorraum über sich selbst.

(*iii*) Allgemeiner sei $(K, +, \cdot)$ ein Körper und $(U, +, \cdot)$ ein Unterkörper. Dann ist $(K, +, \cdot)$ ein Vektorraum über U. Beispielsweise ist $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum, und $\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum und ein $\mathbb{Q}$-Vektorraum.

(*iv*) Es sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann ist die Menge

$$K_n := \big\{(x_1, \dots, x_n) \,\big|\, x_i \in K \text{ für } i = 1, \dots, n\big\} \tag{12.2}$$

der n-Tupel[2] über K, ausgestattet mit der **komponentenweisen Addition** (englisch: componentwise addition) und der **komponentenweisen skalaren Multiplikation** (englisch: componentwise scalar multiplication)

$$(x_1, \dots, x_n) \oplus (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n), \tag{12.3a}$$
$$\alpha \odot (x_1, \dots, x_n) := (\alpha \cdot x_1, \dots, \alpha \cdot y_n), \tag{12.3b}$$

ein Vektorraum über K, genannt der **Vektorraum der Zeilenvektoren** (englisch: row vector space) über K der Dimension n.[3] Der Nullvektor ist der Vektor $(0_K, \dots, 0_K) \in K_n$.

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 $()$. Es gilt $\alpha \odot () = ()$ für alle $\alpha \in K$.

[2] Gemäß Definition 4.8 müssten wir die n-Tupel eigentlich mit K^n bezeichnen. Es ist aber üblich, die Bezeichnung K^n für den Vektorraum der Spaltenvektoren zu verwenden.

[3] Der Begriff der Dimension für beliebige Vektorräume wird in Definition 13.16 eingeführt. Hier dient er zunächst zur Angabe der Anzahl der Einträge in einem Zeilenvektor.

(*v*) Es sei $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann ist die Menge

$$K^n := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| \, x_i \in K \text{ für } i = 1, \ldots, n \right\}, \tag{12.4}$$

ausgestattet mit der **komponentenweisen Addition** (englisch: componentwise addition) und der **komponentenweisen skalaren Multiplikation** (englisch: componentwise scalar multiplication)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \tag{12.5a}$$

$$\alpha \odot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \alpha \cdot x_1 \\ \vdots \\ \alpha \cdot x_n \end{pmatrix}, \tag{12.5b}$$

ein Vektorraum über K, genannt der **Vektorraum der Spaltenvektoren** (englisch: column vector space) oder auch der **Standardvektorraum** (englisch: standard vector space) oder der **Koordinatenraum** (englisch: coordinate space) über K der Dimension n.[4] Der Nullvektor ist der Vektor $\begin{pmatrix} 0_K \\ \vdots \\ 0_K \end{pmatrix}$ 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 $()$. Es gilt $\alpha \odot () = ()$ für alle $\alpha \in K$.

(*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 Vektorraum über K. Der Nullvektor ist die Nullfunktion.

Insbesondere ist die Menge der Folgen $K^{\mathbb{N}}$ mit Werten in K ein Vektorraum.

(*vii*) Es sei $(K, +, \cdot)$ ein Körper und $K[t]$ der Polynomring (Definition 11.4). In $K[t]$ ist die Addition $+$ gemäß (11.3a) erklärt.[5] Ergänzen wir die skalare Multiplikation[6]

$$\alpha \odot \left(a_n t^n + \cdots + a_1 t + a_0\right) := \alpha \cdot a_n t^n + \cdots + \alpha \cdot a_1 t + \alpha \cdot a_0, \tag{12.6}$$

so wird $K[t]$ zu einem Vektorraum über K, genannt der **Polynomraum** (englisch: vector space of polynomials) über K. △

Lemma 12.4 (Rechenregeln in Vektorräumen, vgl. Lemma 9.3)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein Vektorraum über K. Dann gilt für $\alpha \in K$ und $v \in V$:

[4] Der Begriff **Koordinatenraum** wird später in Satz 19.1 klar werden.
[5] Die zweite Verknüpfung in $K[t]$, also die Multiplikation $\cdot$ von Polynomen gemäß (11.3b), ignorieren wir hier.
[6] Die skalare Multiplikation stimmt überein mit der Multiplikation von Polynomen, wobei einer der Faktoren ein konstantes Polynom ist, das mit einem Element aus K identifiziert werden kann.

(*i*) $0_K \odot v = 0_V = v \odot 0_K$.

(*ii*) $\alpha \odot 0_V = 0_V$.

(*iii*) $\alpha \odot v = 0_V \quad \Rightarrow \quad \alpha = 0_K$ oder $v = 0_V$.

(*iv*) $\alpha \odot (\ominus v) = \ominus(\alpha \odot v) = (-\alpha) \odot v$ und insbesondere $\ominus v = (-1_K) \odot v$.

Beweis. Aussage (*i*):

$$\begin{aligned} 0_V \oplus 0_K \odot v &= 0_K \odot v && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= (0_K + 0_K) \odot v && \text{da } 0_K \text{ das neutrale Element von } (K, +) \text{ ist} \\ &= 0_K \odot v \oplus 0_K \odot v && \text{nach Distributivgesetz (12.1b).} \end{aligned}$$

Aus der Kürzungsregel (7.10b) in der Gruppe $(V, \oplus)$ folgt nun $0_V = 0_K \odot v$. Der Beweis der zweiten Gleichheit folgt sofort aus $0_K \odot v = v \odot 0_K$.

Aussage (*ii*): Für beliebiges $\alpha \in K$ gilt

$$\begin{aligned} \alpha \odot 0_V \oplus 0_V &= \alpha \odot 0_V && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= \alpha \odot (0_V \oplus 0_V) && \text{da } 0_V \text{ das neutrale Element von } (V, \oplus) \text{ ist} \\ &= \alpha \odot 0_V \oplus \alpha \odot 0_V && \text{nach Distributivgesetz (12.1a).} \end{aligned}$$

Aus der Kürzungsregel (7.10a) in der Gruppe $(V, \oplus)$ folgt nun $0_V = \alpha \odot 0_V$.

Aussage (*iii*): Es seien $\alpha \in K$ und $v \in V$ sowie $\alpha \odot v = 0_V$. Wir nehmen $\alpha \neq 0_K$ an. Dann gilt

$$\begin{aligned} v &= 1_K \odot v && \text{nach (12.1d)} \\ &= (\alpha \cdot \alpha^{-1}) \odot v && \text{da } \alpha \neq 0_K \text{ in der Gruppe } (K \setminus \{0\}, \cdot) \text{ das Inverse } \alpha^{-1} \text{ besitzt} \\ &= \alpha^{-1} \odot (\alpha \odot v) && \text{nach Assoziativgesetz (12.1c)} \\ &= \alpha^{-1} \odot 0_V && \text{nach Voraussetzung} \\ &= 0_V && \text{nach Aussage (ii).} \end{aligned}$$

Aussage (*iv*): Es seien $\alpha \in K$ und $v \in V$. Wir zeigen zunächst, dass $\alpha \odot v$ das Inverse zu $(-\alpha) \odot v$ in der Gruppe $(V, \oplus)$ ist:

$$\begin{aligned} \big[(-\alpha) \odot v\big] \oplus \big[\alpha \odot v\big] &= \big(-\alpha + \alpha\big) \odot v && \text{nach Distributivgesetz (12.1b)} \\ &= 0_K \odot v && \text{da } \alpha \text{ in der Gruppe } (K, +) \text{ das Inverse } -\alpha \text{ besitzt} \\ &= 0_V && \text{nach Aussage (i).} \end{aligned}$$

Das heißt, es gilt $\ominus(\alpha \odot v) = (-\alpha) \odot v$. Insbesondere für $\alpha = 1_K$ erhalten wir

$$\ominus v = \ominus(1_K \odot v) = (-1_K) \odot v. \tag{$*$}$$

Weiter haben wir

$$\begin{aligned} (-\alpha) \odot v &= \big[(-1_K) \cdot \alpha\big] \odot v && \text{nach Lemma 9.3} \\ &= \big[\alpha \cdot (-1_K)\big] \odot v && \text{da } (K, \cdot) \text{ kommutativ ist} \\ &= \alpha \odot \big((-1_K) \odot v\big) && \text{nach Assoziativgesetz (12.1c)} \\ &= \alpha \odot (\ominus v) && \text{nach } (*). \end{aligned}$$

□

Definition 12.5 (Linearkombination)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein Vektorraum über K.

(*i*) Es sei $E \subseteq V$. Ein Vektor der Form

$$\alpha_1 \odot v_1 \oplus \cdots \oplus \alpha_n \odot v_n \quad \text{oder kurz} \quad \sum_{j=1}^{n} \alpha_j \odot v_j \tag{12.7}$$

mit endlich vielen Skalaren $\alpha_j \in K$ und Vektoren $v_j \in E$ für $j = 1, \ldots, n$ und $n \in \mathbb{N}_0$ heißt eine **Linearkombination** (englisch: linear combination) **der Menge** E oder **Linearkombination von Vektoren der Menge** E. Falls $n = 0$ gilt, so interpretieren wir wie üblich die Addition von null Elementen in (12.7) als den Nullvektor 0_V.

(*ii*) Es sei $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V. Ein Vektor der Form

$$\alpha_1 \odot v_{i_1} \oplus \cdots \oplus \alpha_n \odot v_{i_n} \quad \text{oder kurz} \quad \sum_{j=1}^{n} \alpha_j \odot v_{i_j} \tag{12.8}$$

mit endlich vielen Indizes $i_j \in I$ und Skalaren $\alpha_j \in K$ für $j = 1, \ldots, n$ und $n \in \mathbb{N}_0$ heißt eine **Linearkombination der Familie** F oder **Linearkombination von Vektoren der Familie** F. Falls $n = 0$ gilt, so interpretieren wir auch hier die Addition von null Elementen in (12.8) als den Nullvektor 0_V.

In beiden Fällen heißen die Skalare α_j die **Koeffizienten** (englisch: coefficients) der Linearkombination. Die Linearkombination heißt **trivial** (englisch: trivial linear combination), wenn alle $\alpha_j = 0$ sind. Falls $n = 0$ gilt, so interpretieren wir wie üblich die Addition von null Elementen als den Nullvektor 0_V. △

Beachte: Linearkombinationen bestehen immer aus endlich vielen Termen!

Beispiel 12.6 (Linearkombination)**.**

(*i*) Der Vektor $\left(\begin{smallmatrix} 3 \\ -7 \end{smallmatrix}\right)$ ist eine Linearkombination der Menge der Vektoren $\left\{\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)\right\}$ im Standardvektorraum $\mathbb{R}^2$, nämlich

$$\begin{pmatrix} 3 \\ -7 \end{pmatrix} = 3 \odot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \oplus (-7) \odot \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(*ii*) Der Vektor $\left(\begin{smallmatrix} 3 \\ -7 \end{smallmatrix}\right)$ ist eine Linearkombination der Menge der Vektoren $\left\{\left(\begin{smallmatrix} 2 \\ -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 4 \\ 1 \end{smallmatrix}\right)\right\}$ im Standardvektorraum $\mathbb{R}^2$, nämlich

$$\begin{pmatrix} 3 \\ -7 \end{pmatrix} = \frac{31}{6} \odot \begin{pmatrix} 2 \\ -1 \end{pmatrix} \oplus \frac{-11}{6} \odot \begin{pmatrix} 4 \\ 1 \end{pmatrix}.$$

(Zur Bestimmung der Koeffizienten wurde ein lineares Gleichungssystem gelöst, siehe Kapitel 4.)

(*iii*) Die Funktion $[0, 2\pi] \ni x \mapsto \sin(x) \ominus \sqrt{2} \odot \cos(x) \in \mathbb{R}$ ist eine Linearkombination der Menge der Funktionen (Vektoren) $\{\sin, \cos\}$ im Vektorraum der Funktionen $\mathbb{R}^{[0,2\pi]}$.

(*iv*) Das Polynom $3\,t^2 \oplus 5$ im Vektorraum (Polynomraum) $\mathbb{Q}[t]$ ist eine Linearkombination der Menge der Polynome $\{t^2, t, 1\}$, wobei 1 das Einspolynom in $\mathbb{Q}[t]$ bezeichnet. Das Polynom t kommt in der Linearkombination $3\,t^2 \oplus 5$ mit dem Koeffizienten $0 \in \mathbb{Q}$ vor. △

Ende der Vorlesung 15

Definition 12.7 (Unterraum)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, \oplus, \odot)$ ein Vektorraum über K.

(*i*) Eine Teilmenge $U \subseteq V$ heißt ein **Untervektorraum** oder kurz: ein **(linearer) Unterraum** (englisch: vector subspace, linear subspace) von $(V, \oplus, \odot)$, wenn U bzgl. $\oplus$ und bzgl. der skalaren Multiplikation $\odot$ mit Elementen in K abgeschlossen ist und wenn $(U, \oplus, \odot)$ selbst wieder ein Vektorraum ist.

Beachte: Das ist genau dann erfüllt, wenn $(U, \oplus)$ eine Untergruppe von $(V, \oplus)$ ist und wenn U bzgl. der skalaren Multiplikation $\odot$ mit Elementen in K abgeschlossen ist, also $K \odot U \subseteq U$.

(*ii*) Ein Unterraum $(U, \oplus, \odot)$ von $(V, \oplus, \odot)$ heißt **echt** (englisch: proper subspace), wenn $U \subsetneq V$ gilt. △

Beachte: Da $(U, \oplus)$ eine Untergruppe von $(V, \oplus)$ ist, enthält ein Unterraum U immer den Nullvektor 0_V.

Die Prüfung einer Teilmenge $U \subseteq V$ auf die Unterraum-Eigenschaft lässt sich mit folgendem Kriterium bewerkstelligen:

Satz 12.8 (Unterraumkriterium)**.**
Es sei $(K, +, \cdot)$ ein Körper, $(V, \oplus, \odot)$ ein Vektorraum über K und $U \subseteq V$. Dann sind äquivalent:

(*i*) $(U, \oplus, \odot)$ ist ein Unterraum von $(V, \oplus, \odot)$.

(*ii*) $U \neq \emptyset$, und für alle $u, v \in U$ und $\alpha \in K$ gilt $u \oplus v \in U$ und $\alpha \odot u \in U$.
(Mit anderen Worten: $U \neq \emptyset$, und es gilt $U \oplus U \subseteq U$ sowie $K \odot U \subseteq U$.)

(*iii*) $U \neq \emptyset$, und für alle $u, v \in U$ und $\alpha, \beta \in K$ gilt $\alpha \odot u \oplus \beta \odot v \in U$.
(Mit anderen Worten: $U \neq \emptyset$, und es gilt $K \odot U \oplus K \odot U \subseteq U$.)

Beweis. Aussage (*i*) ⇒ Aussage (*ii*): Es sei $(U, \oplus, \odot)$ ein Unterraum von $(V, \oplus, \odot)$. Dann ist per Definition 12.7 und Definition 12.1 $(U, \oplus)$ eine Gruppe, also eine Untergruppe von $(V, \oplus)$. Insbesondere gilt $0_V \in U$, also $U \neq \emptyset$. Weiter ist U als Unterraum abgeschlossen bzgl. $\oplus$ und bzgl. der skalaren Multiplikation $\odot$ mit Elementen von K.

Aussage (*ii*) ⇒ Aussage (*i*): Wir müssen zeigen, dass $(U, \oplus, \odot)$ unter der Annahme von Aussage (*ii*) wieder ein Vektorraum ist. Diese Annahme zeigt insbesondere, dass $\oplus\colon U \times U \to U$ und $\odot\colon K \times U \to U$ eingeschränkt werden können. Die Eigenschaften aus (12.1) bleiben bei dieser Einschränkung erhalten. Es bleibt also nur zu zeigen, dass $(U, \oplus)$ eine abelsche Gruppe ist, also eine Untergruppe von $(V, \oplus)$. Dazu wenden wir das Untergruppenkriterium (Satz 7.33) an. Es gilt nach Voraussetzung $U \neq \emptyset$. Wegen $\ominus u = (-1_K) \odot u$ für $u \in U$ und der Annahme $K \odot U \subseteq U$ gilt $\ominus U \subseteq U$. Aus der Annahme $U \oplus U \subseteq U$ folgt daher weiter $U \oplus (\ominus U) \subseteq U$. Nach dem Untergruppenkriterium ist $(U, \oplus)$ damit eine Untergruppe von $(V, \oplus)$.

Aussage (*ii*) ⇒ 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 12.9 (Unterräume)**.**

(*i*) Es sei $(V, \oplus, \odot)$ ein Vektorraum. Dann sind $(\{0_V\}, \oplus, \odot)$ und $(V, \oplus, \odot)$ Unterräume von $(V, \oplus, \odot)$. Diese heißen die **trivialen Unterräume** (englisch: trivial subspaces). Speziell $(\{0_V\}, \oplus, \odot)$ ist der **Nullraum** (englisch: zero vector space) von V.

(*ii*) Wir betrachten den Standardvektorraum $V = \mathbb{R}^2$ über dem Körper $\mathbb{R}$.

(a) Die Menge

$$U_1 := \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \middle| \, x_1 - 2\,x_2 = 0 \right\}$$

ist ein Unterraum von $V = \mathbb{R}^2$, denn die Aussage (*ii*) des Unterraumkriteriums Satz 12.8 ist erfüllt: Zunächst gilt $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) \in U_1$, also ist $U_1 \neq \emptyset$. Weiter gilt für alle $\alpha \in \mathbb{R}$ und $u = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in U_1$ sowie $v = \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right) \in U_1$:

$$u \oplus v = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix} \in U_1, \quad \text{denn } (x_1 + y_1) - 2\,(x_2 + y_2) = (x_1 - 2\,x_2) + (y_1 - 2\,y_2) = 0$$

$$\alpha \odot u = \begin{pmatrix} \alpha\,x_1 \\ \alpha\,x_2 \end{pmatrix} \in U_1, \quad \text{denn } \alpha\,x_1 - 2\,(\alpha\,x_2) = \alpha\,(x_1 - 2\,x_2) = 0.$$

(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 $\left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$, was aber eine notwendige Bedingung für einen Unterraum darstellt, wie wir im Anschluss an Definition 12.7 bereits gesehen haben.

(c) Die Menge

$$U_3 := \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \middle| \, x_1 \geqslant 0,\ x_2 \geqslant 0 \right\}$$

ist kein Unterraum von $V = \mathbb{R}^2$, denn sie erfüllt das Unterraumkriterium nicht. Beispielsweise ist $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \in U_3$, aber $(-1) \odot \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 \\ -1 \end{smallmatrix}\right)$ nicht.

(*iii*) Es sei $(K, +, \cdot)$ ein Körper und $(K^{\mathbb{N}}, \oplus, \odot)$ der Vektorraum der Folgen mit Werten in K. Dann ist die Menge der Folgen mit endlichem Träger (siehe Bemerkung 11.6) und Werten in K

$$(K^{\mathbb{N}})_{00} := \left\{ (y_i)_{i \in \mathbb{N}} \middle| \, \{ i \in \mathbb{N} \mid y_i \neq 0_K \} \text{ ist endlich} \right\} \tag{12.9}$$

ein echter Unterraum von $(K^{\mathbb{N}}, \oplus, \odot)$.

(*iv*) Es sei $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ der Vektorraum der Folgen mit Werten in $\mathbb{R}$. Dann sind die Mengen

$$(\mathbb{R}^{\mathbb{N}})_b := \left\{ (y_i)_{i \in \mathbb{N}} \middle| \, \exists C \geqslant 0 \ \forall i \in \mathbb{N} \ (|y_i| \leqslant C) \right\} \quad \text{der } \textbf{beschränkten Folgen}^{7} \tag{12.10a}$$

$$(\mathbb{R}^{\mathbb{N}})_c := \left\{ (y_i)_{i \in \mathbb{N}} \middle| \, (y_i)_{i \in \mathbb{N}} \text{ ist konvergent} \right\} \quad \text{der } \textbf{konvergenten Folgen}^{8} \tag{12.10b}$$

$$(\mathbb{R}^{\mathbb{N}})_0 := \left\{ (y_i)_{i \in \mathbb{N}} \middle| \, (y_i)_{i \in \mathbb{N}} \text{ konvergiert gegen } 0 \right\} \quad \text{der } \textbf{Nullfolgen}^{9} \tag{12.10c}$$

$$(\mathbb{R}^{\mathbb{N}})_{00} := \left\{ (y_i)_{i \in \mathbb{N}} \middle| \, (y_i)_{i \in \mathbb{N}} \text{ hat endlichen Träger} \right\} \quad \text{der } \textbf{Folgen mit endlichem Träger}^{10} \tag{12.10d}$$

jeweils echte Unterräume von $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$. (**Quizfrage 12.1:** Gibt es auch Unterraumbeziehungen untereinander?)

[7] englisch: bounded sequences
[8] englisch: convergent sequences
[9] englisch: null sequences
[10] englisch: finitely supported sequences

(*v*) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Dann ist für jedes $n \in \mathbb{N}_0$ die Menge der **Polynome vom Höchstgrad** n (englisch: polynomials of maximum degree n)

$$K_n[t] := \left\{ a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 \,\middle|\, a_i \in K \text{ für } i = 0, \ldots, n \right\} \tag{12.11}$$

ein echter Unterraum von $(K[t], +, \cdot)$. (**Quizfrage 12.2:** Bilden auch die Polynome vom Mindestgrad $n \in \mathbb{N}$ einen Unterraum von $K[t]$?) (**Quizfrage 12.3:** Bilden die Polynome von geradem Grad $n \in 2\,\mathbb{N}_0$ einen Unterraum von $K[t]$?) △

Bemerkung 12.10 (Vereinfachung der Notation)**.**
Zur Vereinfachung der Notation werden wir in Zukunft für die Verknüpfungen $\oplus$ und $\odot$ in Vektorräumen einfach dieselbe Notation verwenden wie für die Verknüpfungen + und · des zugrundeliegenden Körpers. Aus dem Zusammenhang ist klar, ob die jeweilige Verknüpfung mit Skalaren oder mit Vektoren gemeint ist.

Das Zeichen für die Multiplikation · von Vektoren mit Elementen aus dem zugrundeliegenden Körper oder von Körperelementen untereinander wird sogar oft ganz weggelassen, solange sich dadurch keine Unklarheiten ergeben. Beispielsweise schreiben wir in Zukunft einfach $\sin -\sqrt{2} \cos$ an Stelle von $\sin \ominus \sqrt{2} \odot \cos$.

Wir werden außerdem das Nullelement von K einfach als 0 schreiben, das Einselement von K als 1 und den Nullvektor von V ebenfalls als 0. △

Wie bereits bei Untergruppen in § 7.4 beschäftigt uns nun die Frage, wie man Unterräume erzeugen kann.

Lemma 12.11 (Durchschnitt von Unterräumen)**.**
Es sei $(V, +, \cdot)$ ein Vektorraum und $(U_i, +, \cdot)$ eine Familie von Unterräumen mit der nichtleeren Indexmenge I. Dann ist auch $\bigcap_{i \in I} U_i$ mit + und · ein Unterraum von $(V, +, \cdot)$.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 8.3. □

Definition 12.12 (erzeugter Unterraum, lineare Hülle, Erzeugendensystem)**.**
Es sei $(V, +, \cdot)$ ein Vektorraum und $E \subseteq V$.

(*i*) Dann heißt

$$\langle E \rangle := \bigcap \left\{ U \,\middle|\, (U, +, \cdot) \text{ ist Unterraum von } (V, +, \cdot) \text{ und } E \subseteq U \right\} \tag{12.12}$$

der von E **erzeugte Unterraum** (englisch: subspace generated by E) oder die **lineare Hülle** (englisch: linear hull) $\mathrm{Lin}(E)$ von E oder auch der **Spann** (englisch: span) $\mathrm{Span}(E)$ von E in $(V, +, \cdot)$.

Beachte: Bezeichnen wir mit $\mathcal{R}$ die Menge auf rechten Seite von (12.12), über die der Durchschnitt gebildet wird, dann ist $\langle E \rangle$ das Minimum der Menge $\mathcal{R}$ bzgl. der Inklusionshalbordnung und sogar das Minimum der Menge $\mathcal{R}$ bzgl. der Halbordnung „ist Unterraum von“.

Ist speziell E die endliche Menge $E = \{v_1, \ldots, v_n\}$ für $v_i \in V$ und $n \in \mathbb{N}$, so schreiben wir auch $\langle v_1, \ldots, v_n \rangle$ oder $\mathrm{Lin}(v_1, \ldots v_n)$ 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 ein **Erzeugendensystem** (englisch: generating set) von $(V,+,\cdot)$. Falls ein endliches Erzeugendensystem von V existiert, so heißt V **endlich erzeugt** (englisch: finitely generated).

(*iii*) Wenn $F = (v_i)_{i\in I}$ eine Familie von Vektoren in V ist, definieren wir den von F **erzeugten Unterraum** in $(V,+,\cdot)$ bzw. die **lineare Hülle** $\langle F\rangle$ von F bzw. den **Spann** $\mathrm{Span}(F)$ von F in $(V,+,\cdot)$ als

$$\langle F\rangle := \bigcap \big\{U \,\big|\, (U,+,\cdot) \text{ ist Unterraum von } (V,+,\cdot) \text{ und } \{v_i \mid i\in I\} \subseteq U\big\}. \tag{12.13}$$

Wir nennen F ein **Erzeugendensystem** von $(V,+,\cdot)$, wenn $\langle F\rangle = V$ gilt. △

Satz 12.13 (Darstellung des erzeugten Unterraumes)**.**
Es sei $(K,+,\cdot)$ ein Körper, $(V,+,\cdot)$ ein Vektorraum über K und $E \subseteq V$. Dann gilt für den von E erzeugten Unterraum:

$$\langle E\rangle = \left\{ \sum_{i=1}^{n} \alpha_i v_i \,\middle|\, \exists n\in\mathbb{N}_0\ \forall i = 1,\dots,n\ (v_i \in E,\ \alpha_i \in K)\right\}. \tag{12.14}$$

(Zur Erinnerung: Im Fall $n = 0$ interpretieren wir die Linearkombination von null Elementen in der rechten Menge als den Nullvektor 0. Insbesondere im Fall $E = \emptyset$ ist also $\langle E\rangle = \langle\emptyset\rangle = \{0\}$.)

Ist $F = (v_i)_{i\in I}$ eine Familie von Vektoren in V, dann gilt für den von F erzeugten Unterraum:

$$\langle F\rangle = \left\{ \sum_{j=1}^{n} \alpha_j v_{i_j} \,\middle|\, \exists n\in\mathbb{N}_0\ \forall j = 1,\dots,n\ \exists i_j \in I\ (v_{i_j} \in F,\ \alpha_j \in K)\right\}. \tag{12.15}$$

Beachte: Der von einer Menge E (oder einer Familie F) erzeugte Unterraum stimmt also überein mit der Menge der Linearkombinationen von E (bzw. F).[11] Auf die Reihenfolge der Elemente in F kommt es offenbar nicht an.

Beweis. Zur Abkürzung bezeichnen wir die Menge auf der rechten Seite von (12.14) mit M. Wir führen den Beweis analog zu Satz 7.37 in zwei Schritten.

Schritt 1: $\langle E\rangle \supseteq M$: Es sei U ein beliebiger Unterraum von V, der im Durchschnitt (12.12) vorkommt. U enthält also E als Teilmenge. Da U ein Unterraum ist, enthält U auch alle Linearkombinationen von E. Also gilt $U \supseteq M$. Da dies für jeden beliebigen Unterraum aus dem Durchschnitt in (12.12) gilt, gilt auch $\langle E\rangle \supseteq M$.

Schritt 2: $\langle E\rangle \subseteq M$: Wir zeigen zunächst, dass M selbst ein Unterraum von V ist. Dazu überprüfen wir das Unterraumkriterium (Satz 12.8). Offensichtlich ist $M \neq \emptyset$, denn M enthält mindestens den Nullvektor 0. Sind $\sum_{i=1}^{n} \alpha_i v_i$ und $\sum_{j=1}^{m} \beta_j w_j$ zwei Elemente aus M, so ist auch $\sum_{i=1}^{n} \alpha_i v_i + \sum_{j=1}^{m} \beta_j w_j$ ein Element aus M. Zudem ist für jedes $\alpha \in K$ auch $\alpha \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \alpha\,\alpha_i v_i$ ein Element aus M. Also ist M ein Unterraum von V. Zusätzlich ist klar, dass $E \subseteq M$ gilt. (**Quizfrage 12.4:** Details?) Das heißt, M ist einer derjenigen Unterräume von V, über die in der Definition von $\langle E\rangle$ der Durchschnitt gebildet wird. Folglich gilt $\langle E\rangle \subseteq M$.

Der Beweis für den Fall (12.15) geht analog. □

Beispiel 12.14 (lineare Hülle)**.**

[11] In manchen Büchern wird daher (12.14) auch als Definition des erzeugten Unterraumes verwendet.

(*i*) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Die Menge aller Monome $E = \{1, t, t^2, \ldots\}$ bildet ein Erzeugendensystem von $K[t]$. Die Menge der Monome $E = \{1, t, \ldots, t^n\}$ bis zum Grad n bildet ein Erzeugendensystem von $K_n[t]$, dem Unterraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$.

(*ii*) In einem Vektorraum V heißt die lineare Hülle

$$\langle v \rangle = \{\alpha v \,|\, \alpha \in K\}$$

eines einzelnen Vektors $v \neq 0$ eine **Gerade** (englisch: line) durch 0 und v. Die lineare Hülle

$$\langle v, w \rangle = \{\alpha v + \beta w \,|\, \alpha, \beta \in K\}$$

von zwei Vektoren $v, w \neq 0$ mit $w \notin \langle v \rangle$ heißt eine **Ebene** (englisch: plane) durch 0, v und w. (**Quizfrage 12.5:** Was passiert im Fall $w \in \langle v \rangle$?) △

Folgerung 12.15 (zu Satz 12.13: lineare Hülle von Vereinigung und Schnitt)**.**
Es sei $(V, +, \cdot)$ ein Vektorraum und $E_1, E_2 \subseteq V$. Dann gilt:

(*i*)
$$\langle E_1 \cup E_2 \rangle = \big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle. \tag{12.16}$$

(*ii*)
$$\langle E_1 \cap E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cap \langle E_2 \rangle \big\rangle. \tag{12.17}$$

Beweis. Aussage (*i*): Die lineare Hülle ist ordnungserhaltend, d. h., es gilt $E_1 \subseteq \langle E_1 \rangle$ und $E_2 \subseteq \langle E_2 \rangle$. Daraus folgt $E_1 \cup E_2 \subseteq \langle E_1 \rangle \cup \langle E_2 \rangle$ und durch Bildung der linearen Hülle $\langle E_1 \cup E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle$.

Umgekehrt besteht $\langle E_1 \rangle$ nach Satz 12.13 gerade aus den Linearkombinationen von E_1, und $\langle E_2 \rangle$ besteht aus den Linearkombinationen von E_2. Das heißt, $\big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle$ besteht aus Linearkombinationen solcher Vektoren, die ihrerseits eine Linearkombination von E_1 oder eine Linearkombination von E_2 sind. Mit Hilfe des Assoziativgesetzes (12.1c) erhalten wir, dass wir jeden Vektor aus $\big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle$ als Linearkombination von $E_1 \cup E_2$ schreiben können, also $\big\langle \langle E_1 \rangle \cup \langle E_2 \rangle \big\rangle \subseteq \langle E_1 \cup E_2 \rangle$.

Aussage (*ii*) Wegen $E_1 \subseteq \langle E_1 \rangle$ und $E_2 \subseteq \langle E_2 \rangle$ gilt $E_1 \cap E_2 \subseteq \langle E_1 \rangle \cap \langle E_2 \rangle$. Durch Bildung der linearen Hülle ergibt sich $\langle E_1 \cap E_2 \rangle \subseteq \big\langle \langle E_1 \rangle \cap \langle E_2 \rangle \big\rangle$. □

Ende der Vorlesung 16

Ende der Woche 8

§ 13 Basis und Dimension

Literatur: Beutelspacher, 2014, Kapitel 3, Bosch, 2014, Kapitel 1, Fischer, Springborn, 2020, Kapitel 2.5, Jänich, 2008, Kapitel 3

In diesem Abschnitt beantworten wir die Frage, wie wir einen Vektorraum durch ein möglichst kleines Erzeugendensystem darstellen können und damit Redundanz in der Darstellung vermeiden.

Definition 13.1 (lineare (Un-)abhängigkeit)**.**
Es sei $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K.

(*i*) Eine Menge $E \subseteq V$ heißt **linear unabhängig** (englisch: linearly independent), wenn in jeder Linearkombination von $n \in \mathbb{N}$ paarweise verschiedenen Vektoren aus E, die den Nullvektor ergibt, notwendig alle Koeffizienten gleich 0 sind, wenn also für alle $n \in \mathbb{N}$ gilt:

$$v_1, \dots, v_n \in E, \quad v_i \neq v_j \text{ für } i \neq j \quad \text{und} \quad \sum_{\ell=1}^{n} \alpha_\ell v_\ell = 0 \quad \Rightarrow \quad \alpha_\ell = 0 \text{ für alle } \ell = 1, \dots, n. \tag{13.1}$$

(*ii*) Wenn dagegen eine Linearkombination von $n \in \mathbb{N}$ paarweise verschiedenen Vektoren aus E möglich ist, die den Nullvektor ergibt, wobei nicht alle Koeffizienten gleich 0 sind, dann heißt E **linear abhängig** (englisch: linearly dependent).

(*iii*) Eine Familie F von Vektoren in V heißt **linear unabhängig**, wenn in jeder Linearkombination von $n \in \mathbb{N}$ Vektoren aus F mit paarweise verschiedenen Indizes, die den Nullvektor ergibt, notwendig alle Koeffizienten gleich 0 sind, wenn also für alle $n \in \mathbb{N}$ gilt:

$$i_1, \dots, i_n \in I, \quad i_j \neq i_k \text{ für } j \neq k \quad \text{und} \quad \sum_{\ell=1}^{n} \alpha_\ell v_{i_\ell} = 0 \quad \Rightarrow \quad \alpha_\ell = 0 \text{ für alle } \ell = 1, \dots, n. \tag{13.2}$$

(*iv*) Wenn dagegen eine Linearkombination von $n \in \mathbb{N}$ Vektoren aus F zu paarweise verschiedenen Indizes möglich ist, die den Nullvektor ergibt, wobei nicht alle Koeffizienten gleich 0 sind, dann heißt F **linear abhängig**. △

Bemerkung 13.2 (lineare (Un-)abhängigkeit)**.**

(*i*) Die lineare (Un-)abhängigkeit ist eine Eigenschaft, die sich auf eine Menge oder eine Familie von Vektoren bezieht. Sprechweisen wie „Der Vektor v ist linear unabhängig von $\{v_1, v_2\}$." sind nicht korrekt. Man kann aber sagen, die Menge $\{v\} \cup \{v_1, v_2\}$ sei linear unabhängig.

(*ii*) Die Menge $\{v\}$ bestehend aus einem einzigen Vektor ist linear unabhängig, falls $v \neq 0$ ist, ansonsten linear abhängig. (Dasselbe gilt für eine einelementige Familie von Vektoren.)

(*iii*) Eine Menge oder Familie von Vektoren, die den Nullvektor enthält, ist stets linear abhängig.

(*iv*) Die leere Menge und die leere Familie von Vektoren sind per Definition linear unabhängig. △

Die lineare Abhängigkeit einer Menge bzw. einer Familie von Vektoren bedeutet, dass man einen Vektor als Linearkombination der anderen darstellen kann:

Lemma 13.3 (lineare Abhängigkeit ist äquivalent zur Kombinierbarkeit)**.**
Es sei V ein Vektorraum.

(*i*) Es sind äquivalent:

(a) $E \subseteq V$ ist eine linear abhängige Menge.

(b) Es gibt einen Vektor $v \in E$, der als Linearkombination von $E \setminus \{v\}$ darstellbar ist.

(*ii*) Es sind äquivalent:

(a) $F = (v_i)_{i \in I}$ ist eine linear abhängige Familie mit einer Indexmenge I.

(b) Es gibt es einen Vektor v_{i^*} aus der Familie, der als Linearkombination der Familie $(v_i)_{i \in I \setminus \{i^*\}}$ darstellbar ist.

Beweis. Dieser Beweis ist Gegenstand von Hausaufgabe 9.1. □

Lemma 13.4 (lineare (Un-)abhängigkeit von Teilmengen und Obermengen)**.**
Es sei V ein Vektorraum.

(*i*) Jede Teilmenge einer Menge linear unabhängiger Vektoren aus V ist ebenfalls linear unabhängig. Jede Teilfamilie einer Familie linear unabhängiger Vektoren aus V ist ebenfalls linear unabhängig.

(*ii*) Jede Obermenge einer Menge linear abhängiger Vektoren aus V ist ebenfalls linear abhängig. Jede Oberfamilie einer Familie linear abhängiger Vektoren aus V ist ebenfalls linear abhängig.

Beweis. Der Beweis ergibt sich unmittelbar aus der Definition 12.12. □

Beispiel 13.5 (lineare (Un-)abhängigkeit)**.**

(*i*) Die Teilmenge $\left\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\\sqrt{2}\end{pmatrix}, \begin{pmatrix}\sqrt{2}\\1\end{pmatrix}\right\}$ des Vektorraumes $\mathbb{R}^2$ über dem Körper $\mathbb{R}$ ist linear abhängig, denn es gilt

$$(1+\sqrt{2})\begin{pmatrix}1\\1\end{pmatrix} + (-1)\begin{pmatrix}1\\\sqrt{2}\end{pmatrix} + (-1)\begin{pmatrix}\sqrt{2}\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}.$$

(*ii*) Dieselbe Menge ist als Teilmenge des Vektorraumes $\mathbb{R}^2$ über dem Körper $\mathbb{Q}$ jedoch linear unabhängig, denn es gilt

$$\alpha_1\begin{pmatrix}1\\1\end{pmatrix} + \alpha_2\begin{pmatrix}1\\\sqrt{2}\end{pmatrix} + \alpha_3\begin{pmatrix}\sqrt{2}\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix} \quad \Rightarrow \quad \alpha_1 = \alpha_2 = \alpha_3 = 0.$$

(*iii*) Wir betrachten den K-Vektorraum K^X der Funktionen $X \to K$, wobei $(K, +, \cdot)$ ein Körper und X eine Menge ist; siehe Beispiel 12.3. Für $y \in X$ definieren wir die **charakteristische Funktion** (englisch: characteristic function) $e_y \colon X \to K$ durch[12]

$$x \mapsto e_y(x) := \delta_{xy} := \begin{cases} 1, & \text{falls } x = y, \\ 0, & \text{falls } x \neq y. \end{cases} \tag{13.3}$$

Dann ist die Menge $\{e_y \mid y \in X\}$ linear unabhängig.

(*iv*) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Dann ist die Menge der Monome $E = \{1, t, t^2, \ldots\}$ linear unabhängig. △

Die Bedeutung linear unabhängiger Mengen und Familien von Vektoren stellt folgendes Resultat klar.

Lemma 13.6 (lineare Unabhängigkeit und eindeutige Linearkombination)**.**
Es sei V ein Vektorraum und $(v_i)_{i\in I}$ eine Familie von Vektoren aus V. Dann sind äquivalent:

(*i*) $(v_i)_{i\in I}$ ist linear unabhängig.

(*ii*) Jeder Vektor $v \in \langle (v_i)_{i\in I}\rangle$ lässt sich in eindeutiger Weise (bis auf Summanden mit Nullkoeffizienten) aus paarweise verschiedenen Vektoren der Familie $(v_i)_{i\in I}$ linearkombinieren.

[12] 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 $x \notin A$.

Ein analoges Resultat gilt für Mengen von Vektoren aus V.

Beweis. 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 12.13 besteht $\langle (v_i)_{i\in I}\rangle$ gerade aus den Linearkombinationen von $(v_i)_{i\in I}$. Es gibt also eine endliche Teilmenge $I_0 \subseteq I$ und Skalare $\alpha_i \in K$, $i \in I_0$ mit der Eigenschaft

$$v = \sum_{i\in I_0} \alpha_i v_i. \tag{$*$}$$

Zu zeigen ist noch, dass diese Darstellung eindeutig ist. Wir nehmen dazu an, dass

$$v = \sum_{j\in I_1} \beta_j v_j \tag{$**$}$$

eine weitere Darstellung von v als Linearkombination von $(v_i)_{i\in I}$ ist mit endlicher Indexmenge I_1. Wir setzen $N := \{i \in I_0 \mid \alpha_i \neq 0\} \cup \{j \in I_1 \mid \beta_j \neq 0\}$. Dann ist N endlich. Wir haben

$$\begin{aligned}
0 &= v - v \\
&= \sum_{i\in I_0} \alpha_i v_i - \sum_{j\in I_1} \beta_j v_j \\
&= \sum_{i\in N} \alpha_i v_i - \sum_{j\in N} \beta_j v_j \quad \text{indem wir } \alpha_i = 0 \text{ für } i \in N \setminus I_0 \text{ und } \beta_j = 0 \text{ für } j \in N \setminus I_1 \text{ ergänzen} \\
&= \sum_{i\in N} (\alpha_i - \beta_i) v_i.
\end{aligned}$$

Da nach Voraussetzung $(v_i)_{i\in I}$ linear unabhängig ist, muss $\alpha_i - \beta_i = 0$ für alle $i \in N$ gelten, also $\alpha_i = \beta_i$. Die Darstellungen $(*)$ und $(**)$ unterscheiden sich also nur um eventuell auftauchende Terme mit Nullkoeffizienten.

Aussage (ii) $\Rightarrow$ Aussage (i): Es sei $I_0 \subseteq I$ eine beliebige endliche Teilmenge. Wir müssen zeigen, dass $(v_i)_{i\in I_0}$ linear unabhängig ist. Wir untersuchen also die Linearkombination

$$\sum_{i\in I_0} \alpha_i v_i = 0.$$

Diese wird erreicht durch die Wahl von $\alpha_i = 0$ für alle $i \in I_0$. Nach Voraussetzung ist das auch die einzig mögliche Wahl der Koeffizienten. Das heißt aber, dass $(v_i)_{i\in I_0}$ linear unabhängig ist. Da I_0 eine beliebige endliche Teilmenge von I war, ist die gesamte Familie $(v_i)_{i\in I}$ linear unabhängig.

Der Beweis für Mengen geht analog. □

Lemma 13.7 (lineare Abhängigkeit bedeutet Redundanz)**.**
Es sei V ein Vektorraum und $(v_i)_{i\in I}$ eine nichtleere Familie von Vektoren aus V. Dann sind äquivalent:

(i) $(v_i)_{i\in I}$ ist linear abhängig.

(ii) Es gibt ein $j \in I$, sodass gilt:
$$\langle (v_i)_{i\in I\setminus\{j\}}\rangle = \langle (v_i)_{i\in I}\rangle.$$

Ein analoges Resultat gilt für nichtleere Mengen von Vektoren aus V.

Beachte: Ist ein Erzeugendensystem eines Vektorraumes linear abhängig, so kann man mindestens ein Element aus dem Erzeugendensystem entfernen, ohne den erzeugten Raum zu verkleinern.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Es sei $(v_i)_{i\in I}$ linear abhängig, d. h., es gibt eine endliche Teilmenge $I_0 \subseteq I$ und Koeffizienten $\alpha_i \in K$, $i \in I_0$, die nicht alle gleich Null sind, sodass

$$\sum_{i\in I_0} \alpha_i v_i = 0$$

gilt. Es sei $j \in I_0$ ein Index, für den $\alpha_j \neq 0$ gilt. Dann ist

$$\alpha_j v_j = -\sum_{i\in I_0\setminus\{j\}} \alpha_i v_i,$$

also auch

$$v_j = -\alpha_j^{-1} \sum_{i\in I_0\setminus\{j\}} \alpha_i v_i = -\sum_{i\in I_0\setminus\{j\}} \alpha_j^{-1}\alpha_i v_i. \tag{$*$}$$

Das zeigt $v_j \in \langle (v_i)_{i\in I\setminus\{j\}}\rangle$.

Es sei nun $v \in \langle (v_i)_{i\in I}\rangle$ beliebig. Dann gibt es eine endliche Teilmenge $I_1 \subseteq I$ und Koeffizienten $\beta_i \in K$, $i \in I_1$, sodass

$$v = \sum_{i\in I_1} \beta_i v_i$$

gilt. Wir wollen zeigen, dass wir v auch ohne Verwendung von v_j linearkombinieren können. Falls $j \notin I_1$ liegt (also v_j ohnehin nicht verwendet wird), dann ist $\langle (v_i)_{i\in I\setminus\{j\}}\rangle$ klar. Falls jedoch $j \in I_1$ liegt, dann ersetze v_j durch ($*$):

$$\begin{aligned} v &= \sum_{i\in I_1} \beta_i v_i \\ &= \sum_{i\in I_1\setminus\{j\}} \beta_i v_i + \beta_j v_j \\ &= \sum_{i\in I_1\setminus\{j\}} \beta_i v_i - \sum_{i\in I_0\setminus\{j\}} \beta_j \alpha_j^{-1}\alpha_i v_i. \end{aligned}$$

Dies ist eine Darstellung von v als Linearkombination aus $(v_i)_{i\in I}$ ohne Verwendung von v_j. Insgesamt gilt also $v \in \langle (v_i)_{i\in I\setminus\{j\}}\rangle$ und damit Aussage (*ii*).

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Es sei $j \in I$ ein Index, sodass $\langle (v_i)_{i\in I\setminus\{j\}}\rangle = \langle (v_i)_{i\in I}\rangle$ gilt. Dann ist insbesondere $v_j \in \langle (v_i)_{i\in I\setminus\{j\}}\rangle$, d. h., es gibt eine endliche Teilmenge $I_0 \subseteq I\setminus\{j\}$ und Koeffizienten $\alpha_i \in K$, $i \in I_0$, sodass gilt:

$$v_j = \sum_{i\in I_0} \alpha_i v_i.$$

Das heißt aber auch

$$\sum_{i\in I_0} \alpha_i v_i - 1 v_j = 0,$$

d. h., $(v_i)_{i\in I}$ ist linear abhängig.

Der Beweis für Mengen geht analog. □

Im Folgenden interessieren wir uns vor allem für linear unabhängige Erzeugendensysteme, also solche ohne Redundanz.

Definition 13.8 (Basis)**.**
Es sei V ein Vektorraum.

(*i*) Eine Teilmenge $B \subseteq V$ heißt eine **Basis** (englisch: basis) von V, wenn B linear unabhängig ist und $\langle B \rangle = V$ gilt.

(*ii*) Eine Familie B von Vektoren aus V heißt eine **Basis** (englisch: basis) von V, wenn B linear unabhängig ist und $\langle B \rangle = V$ gilt. △

Beachte: Eine Basis ist also ein linear unabhängiges Erzeugendensystem.

Beispiel 13.9 (Basis)**.**

(*i*) $\emptyset$ ist die einzige Basis des Nullraumes $\{0\}$ über jedem Körper K.

(*ii*) Die Menge $E := \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}, \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \right\}$ ist ein Erzeugendensystem des $\mathbb{R}$-Vektorraumes $\mathbb{R}^2$, jedoch keine Basis, da sie linear abhängig ist; siehe Beispiel 13.5. Wenn wir ein beliebiges Element aus E entfernen, so erhalten wir eine Basis von $\mathbb{R}^2$.

(*iii*) Im Standardvektorraum K^n über einem Körper K (Beispiel 12.3) ist

$$\{e_1, \dots, e_n\} \text{ mit } e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{-ter Eintrag} \tag{13.4}$$

eine Basis, genannt die **kanonische Basis** (englisch: canonical basis), **Standardbasis** (englisch: standard basis) oder **Einheitsbasis** (englisch: unit basis) von K^n.

(*iv*) Es sei $(K, +, \cdot)$ ein Körper und $(K[t], +, \cdot)$ der Polynomraum über K; siehe Beispiel 12.3. Dann ist die Menge der Monome $E = \{1, t, t^2, \dots\}$ eine Basis von $K[t]$. Die Monome $E = \{1, t, \dots, t^n\}$ bilden eine Basis von $K_n[t]$, dem Unterraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$. △

Ende der Vorlesung 17

Satz 13.10 (Charakterisierung von Basen)**.**
Es sei V ein Vektorraum und $B \subseteq V$. Dann sind äquivalent:

(*i*) B ist eine Basis von V.

(*ii*) B ist eine maximale linear unabhängige Teilmenge von V.[13] Das heißt: B ist linear unabhängig, und jede echte Obermenge von B ist linear abhängig.

(*iii*) B ist ein minimales Erzeugendensystem von V.[14] Das heißt: B ist ein Erzeugendensystem, und jede echte Teilmenge von B ist kein Erzeugendensystem.

(*iv*) Jeder Vektor $v \in V$ lässt sich auf eindeutige Weise (bis auf Summanden mit Nullkoeffizienten) aus paarweise verschiedenen Elementen von B linearkombinieren.

[13] Genauer: B ist ein maximales Element bzgl. der Mengeninklusion (Definition 5.10) in der Menge der linear unabhängigen Teilmengen von V.

[14] Genauer: B ist ein minimales Element bzgl. der Mengeninklusion (Definition 5.10) in der Menge der Erzeugendensysteme von V.

Ein analoge Charakterisierung der Basiseigenschaft gilt für Familien B in V.

Beweis. Aussage (i) $\Rightarrow$ Aussage (ii): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B\rangle = V$. Für einen beliebigen Vektor $v \in V \setminus B$ gilt $\langle B \cup \{v\}\rangle = V$. Aus Lemma 13.7 („Redundanz bedeutet lineare Abhängigkeit“) folgt nun, dass $B \cup \{v\}$ linear abhängig ist.

Aussage (ii) $\Rightarrow$ Aussage (i): Es sei B eine maximale linear unabhängige Teilmenge von V. Zu zeigen ist, dass B ganz V erzeugt. Es sei dazu $v \in V$ beliebig. Nach Definition von $\langle B\rangle$ ist klar, dass $\langle B\rangle \supseteq B$ gilt. (**Quizfrage 13.1:** Warum?) Wenn also $v \in B$ ist, dann auch $v \in \langle B\rangle$, was zu zeigen war. Wir können also von $v \in V \setminus B$ ausgehen. Nach Voraussetzung ist $B \cup \{v\}$ als echte Obermenge von B linear abhängig. Es existieren also $n \in \mathbb{N}_0$, $v_i \in B$ und $\alpha_i \in K$, $i = 1, \dots, n$, sowie $\alpha \in K$, sodass gilt:

$$\sum_{i=1}^{n} \alpha_i v_i + \alpha v = 0.$$

Dabei ist $\alpha \neq 0$, denn sonst wäre bereits B linear abhängig, was der Voraussetzung widerspricht. Wir erhalten also

$$v = -\sum_{i=1}^{n} \alpha^{-1}\alpha_i v_i,$$

d. h., v lässt sich in der Tat aus Elementen von B linearkombinieren. Damit ist $\langle B\rangle = V$ gezeigt.

Aussage (i) $\Rightarrow$ Aussage (iii): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B\rangle = V$. Aus Lemma 13.7 („Redundanz bedeutet lineare Abhängigkeit“) folgt nun, dass B keine redundanten Elemente enthält, dass also für alle $v \in B$ gilt: $\langle B \setminus \{v\}\rangle \subsetneq V$.

Aussage (iii) $\Rightarrow$ Aussage (i): Nach Voraussetzung haben wir $\langle B\rangle = V$, und für alle $v \in B$ gilt: $\langle B \setminus \{v\}\rangle \subsetneq V$. Aus Lemma 13.7 („Redundanz bedeutet lineare Abhängigkeit“) folgt daher, dass B linear unabhängig ist, also eine Basis.

Aussage (i) $\Rightarrow$ Aussage (iv): Es sei B eine Basis von V, d. h., B ist linear unabhängig und $\langle B\rangle = V$. Aus Lemma 13.6 folgt, dass sich jedes $v \in \langle B\rangle = V$ in i. W. eindeutiger Weise aus Elementen von B linearkombinieren lässt.

Aussage (iv) $\Rightarrow$ Aussage (i): Nach Voraussetzung lässt sich jeder Vektor $v \in V$ auf eindeutige Weise (bis auf Summanden mit Nullkoeffizienten) aus paarweise verschiedenen Elementen von B linearkombinieren. Also ist $\langle B\rangle = V$, und aus Lemma 13.6 folgt, dass B linear unabhängig ist, also eine Basis von V. □

Folgerung.
Verschiedene Basen B_1 und B_2 eines Vektorraumes V sind bzgl. der Halbordnung „$\subseteq$“ nicht vergleichbar. D. h., es gilt weder $B_1 \subseteq B_2$ noch $B_2 \subseteq B_1$.

Beweis. 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 13.10. □

Wir geben nun einige wichtige Resultate zur Existenz von Basen an. Das Hauptresultat — der nachfolgende Basisergänzungssatz — besagt, dass zwischen einer linear unabhängigen, aber möglicherweise zu kleinen Menge (der erzeugte Raum ist nicht alles), und einem Erzeugendensystem, das aber möglicherweise zu groß (linear abhängig) ist, immer eine Basis liegt.

Satz 13.11 (Basisergänzungssatz[15]).
Es sei V ein Vektorraum.

(*i*) Es sei A eine linear unabhängige Menge von Vektoren aus V und E ein Erzeugendensystem von V mit der Eigenschaft $A \subseteq E$. Dann existiert eine Basis B von V mit $A \subseteq B \subseteq E$.

(*ii*) Es sei $A = (v_i)_{i \in I_A}$ eine linear unabhängige Familie von Vektoren aus V und $E = (v_i)_{i \in I_E}$ ein Erzeugendensystem von V mit der Eigenschaft $I_A \subseteq I_E$. Dann existiert eine Basis $B = (v_i)_{i \in I_B}$ von V mit $I_A \subseteq I_B \subseteq I_E$.

Beweis. Wir führen den Beweis für Mengen, also den Beweis von Aussage (*i*).

Wir betrachten die Menge aller linear unabhängigen Teilmengen zwischen A und E, also

$$\mathcal{D} := \{D \subseteq V \mid A \subseteq D \subseteq E, \text{ sodass } D \text{ linear unabhängig ist}\} \subseteq \mathcal{P}(E) \subseteq \mathcal{P}(V).$$

$\mathcal{D}$ ist mit der Mengeninklusion eine halbgeordnete Menge. Wegen $A \in \mathcal{D}$ ist $\mathcal{D} \neq \emptyset$. Ziel ist die Anwendung des Lemmas von Zorn 6.35.

Schritt 1: Jede totalgeordnete Teilmenge $\mathcal{C} \subseteq \mathcal{D}$ besitzt eine obere Schranke S in $\mathcal{D}$:

Wir zeigen, dass $S := \bigcup_{C \in \mathcal{C}} C$ eine obere Schranke (Definition 5.10) der Teilmenge $\mathcal{C}$ in $\mathcal{D}$ ist.

Dazu zeigen wir zunächst, dass S überhaupt Element von $\mathcal{D}$ ist:

(a) Für alle $C \in \mathcal{C} \subseteq \mathcal{D}$ gilt $A \subseteq C \subseteq E$, also auch $A \subseteq \bigcup_{C \in \mathcal{C}} C = S \subseteq E$.

(b) Weiter ist S linear unabhängig, denn: Es sei $\{c_1, \ldots, c_n\} \subseteq S$ 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 13.4 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.

Schritt 2: Das Lemma von Zorn 6.35 zeigt nun, dass ein maximales Element B von $\mathcal{D}$ existiert. Das heißt definitionsgemäß: B ist linear unabhängig und erfüllt $A \subseteq B \subseteq E$. Es bleibt zu zeigen, dass B tatsächlich ganz V erzeugt.

Falls $B = E$ gilt, so ist $V = \langle E \rangle = \langle B \rangle$ und der Beweis erbracht. Andernfalls gibt es ein $a \in E \setminus B$, also gilt $B \cup \{a\} \supsetneq B$. B ist aber ein maximales Element von $\mathcal{D}$, also kann $B \cup \{a\}$ nicht zu $\mathcal{D}$ gehören. Wegen $A \subseteq B \cup \{a\} \subseteq E$ muss das daran liegen, dass $B \cup \{a\}$ linear abhängig ist. Aus Lemma 13.7 folgt also $\langle B \cup \{a\} \rangle = \langle B \rangle$ und insbesondere $a \in \langle B \rangle$. Da dieses Argument für jedes $a \in E \setminus B$ gilt, folgt $E \setminus B \subseteq \langle B \rangle$, und natürlich gilt auch $B \subseteq \langle B \rangle$. Es folgt $E \subseteq \langle B \rangle$. Der Übergang zur linearen Hülle zeigt $V = \langle E \rangle \subseteq \big\langle \langle B \rangle \big\rangle = \langle B \rangle$, aber natürlich gilt auch $\langle B \rangle \subseteq V$, also $\langle B \rangle = V$. □

Es folgen drei unmittelbare Folgerungen als Spezialfälle des Basisergänzungssatzes 13.11, formuliert nur in der Version für Mengen:

[15] englisch: basis extension theorem

Folgerung 13.12 (Basisexistenzsatz: $A = \emptyset$ und $E = V$)**.**
Jeder Vektorraum V besitzt eine Basis.

Folgerung 13.13 (Basisauswahlsatz: $A = \emptyset$)**.**
Aus jedem Erzeugendensystem E eines Vektorraumes V lässt sich eine Basis auswählen.

Folgerung 13.14 (Basisergänzungssatz: $E = V$)**.**
Jede linear unabhängige Menge A eines Vektorraumes V kann zu einer Basis erweitert werden.

Bemerkung 13.15 (zum Basisergänzungssatzes 13.11)**.**
Der Beweis des Basisergänzungssatzes 13.11 und seiner Folgerungen 13.12 bis 13.14 ist nicht konstruktiv, d. h., wir können ihn nicht zur Grundlage eines Verfahrens machen, um eine Basis zu konstruieren. Beispielsweise können wir keine Basis von $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum (Beispiel 12.3) angeben.

Wenn der Vektorraum V jedoch endlich erzeugt ist, wenn es also ein endliches Erzeugendensystem gibt, dann lässt sich der Basisergänzungssatz 13.11 konstruktiv und ohne Verwendung des Zornschen Lemmas beweisen, indem man die linear unabhängige Menge A Schritt für Schritt durch einzelne Elemente von E ergänzt oder alternativ Schritt für Schritt einzelne Elemente von $E \setminus A$ entfernt. △

Wir kommen nun zum wichtigen Begriff der Dimension, der in gewissem Sinne die „Größe“ eines Vektorraumes beschreibt. Aus Gründen der Übersichtlichkeit formulieren wir die Definition nur für Basen, die Mengen sind, nicht für Familien.

Definition 13.16 (Dimension eines Vektorraumes)**.**
Es sei V ein Vektorraum.

(*i*) Wenn V eine Basis B der endlichen Kardinalität $n \in \mathbb{N}_0$ besitzt, so sagen wir, V habe **endliche Dimension** (englisch: finite dimension), genauer: die **Dimension** (englisch: dimension) n, in Symbolen: $\dim(V) = n$.

(*ii*) Wenn V keine Basis endlicher Kardinalität besitzt, so sagen wir, V habe **unendliche Dimension** (englisch: infinite dimension), in Symbolen: $\dim(V) = \infty$.

Zur Verdeutlichung, welcher Körper K verwendet wird, schreiben wir manchmal auch $\dim_K(V)$. △

Bevor wir mit dem Begriff der Dimension arbeiten, muss noch sichergestellt werden, dass dieser wohldefiniert ist, denn ein Vektorraum besitzt i. A. viele verschiedene Basen. Wir werden dazu beweisen, dass in dem Fall, dass ein Vektorraum eine Basis endlicher Kardinalität besitzt, alle seine Basen endliche Kardinalität haben, und zwar alle dieselbe.

Lemma 13.17 (Austauschlemma)**.**
Es sei V ein Vektorraum über dem Körper K und die endliche Menge $B = \{v_1, \dots, v_n\}$ eine Basis von V mit $n \in \mathbb{N}$. Ist $w = \sum_{i=1}^{n} \alpha_i v_i$ mit Koeffizienten $\alpha_i \in K$ und gilt $\alpha_j \neq 0$ für ein gewisses $j \in [\![1, n]\!]$, dann ist auch $B_0 := \{v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_n\}$ eine Basis von V.

Ein analoges Resultat gilt, wenn die endliche Familie B eine Basis von V ist.

Beweis. Da es bei einer Basis auf die Reihenfolge der Elemente nicht ankommt, nehmen wir aus Bequemlichkeit und o. B. d. A. an, dass $j = 1$ ist. Aus $w = \sum_{i=1}^{n} \alpha_i v_i$ folgt

$$v_1 = \alpha_1^{-1}\Big(w - \sum_{i=2}^{n} \alpha_i v_i\Big). \tag{$*$}$$

Schritt 1: Wir zeigen: $\langle B_0 \rangle = V$.

Es sei dazu $v \in V$. Da B eine Basis ist, gibt es Koeffizienten $\beta_1, \ldots, \beta_n \in K$, sodass $v = \sum_{i=1}^{n} \beta_i v_i$ gilt. Durch Einsetzen von ($*$) folgt

$$\begin{aligned} v &= \beta_1 \alpha_1^{-1}\Big(w - \sum_{i=2}^{n} \alpha_i v_i\Big) + \sum_{i=2}^{n} \beta_i v_i \\ &= \beta_1 \alpha_1^{-1} w - \beta_1 \alpha_1^{-1} \sum_{i=2}^{n} \alpha_i v_i + \sum_{i=2}^{n} \beta_i v_i \quad \text{nach Distributivgesetz (10.1a) in } K \\ &= \beta_1 \alpha_1^{-1} w + \sum_{i=2}^{n} \big(\beta_i - \beta_1 \alpha_1^{-1} \alpha_i\big) v_i \qquad \text{nach Kommutativ- und Distributivgesetz (10.1b).} \end{aligned}$$

Damit ist gezeigt, dass in der Tat $\langle B_0 \rangle = \langle w, v_2, \ldots, v_n \rangle = V$ 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 $B = \{v_1, \ldots, v_n\}$ linear unabhängig ist, ist das nur möglich, wenn alle Koeffizienten gleich Null sind, also

$$\beta_1 \alpha_1 = 0 \quad \text{und} \quad \beta_1 \alpha_i + \beta_i = 0 \text{ für } i = 2, \ldots, n.$$

Wegen $\alpha_1 \neq 0$ muss $\beta = 0$ sein, woraus dann weiter $\beta_2 = \ldots = \beta_n = 0$ folgt. Das heißt aber, dass $B_0 = \{w, v_2, \ldots, v_n\}$ linear unabhängig ist. □

Satz 13.18 (Austauschsatz von Steinitz[16]).

Es sei V ein Vektorraum und die endliche Menge $B = \{v_1, \ldots, v_n\}$ eine Basis von V mit $\#B = n \in \mathbb{N}_0$. Ist $A = \{a_1, \ldots, a_m\}$ eine linear unabhängige Menge in V mit $\#A = m \in \mathbb{N}_0$, dann gilt:

(*i*) $m \leqslant n$.

(*ii*) Es gibt eine $(n - m)$-elementige Teilmenge D von B, sodass $B_0 := A \cup D$ ebenfalls eine Basis von V ist. Es gilt $\#B_0 = n$.

[16] englisch: Steinitz exchange theorem

Beweis. Wir führen einen Induktionsbeweis nach der Mächtigkeit $m = \#A$. Den Induktionsanfang setzen wir bei $m = 0$. Dann ist $A = \emptyset$, und Aussage (i) gilt wegen $m = 0 \leqslant n$, und Aussage (ii) gilt mit $D = B$.

Es sei nun $m \geqslant 1$, und es gelten Aussagen (i) und (ii) bereits für $m-1$. Da $\{a_1, \dots, a_m\}$ linear unabhängig ist, ist auch $\{a_1, \dots, a_{m-1}\}$ linear unabhängig. Nach Induktionsannahme gilt $m - 1 \leqslant n$, und es existiert $D = \{v_{i_m}, \dots, v_{i_n}\} \subseteq B$, sodass $B_1 \coloneqq \{a_1, \dots, a_{m-1}, v_{i_m}, \dots v_{i_n}\}$ eine Basis von V ist.

Falls nun $m - 1 = n$ wäre, also $D = \emptyset$, dann wäre bereits $\{a_1, \dots a_{m-1}\}$ eine Basis von V. Nach dem Satz 13.10 über die Charakterisierung von Basen hieße das aber, dass $\{a_1, \dots a_m\}$ linear abhängig wäre, im Widerspruch zur Voraussetzung. Es gilt also $m - 1 < n$, also $m \leqslant n$. Damit ist der Induktionsschritt für Aussage (i) gezeigt. Da B_1 eine Basis von V ist, können wir jeden Vektor, insbesondere a_m, durch die Basiselemente linearkombinieren. Es gibt also Skalare α_j, $j = 1, \dots n$, sodass gilt:

$$a_m = \sum_{j=1}^{m-1} \alpha_j \, a_j + \sum_{j=m}^{n} \alpha_j \, v_{i_j}.$$

Wären alle $\alpha_m = \alpha_{m+1} = \dots \alpha_n = 0$, so würde das die lineare Abhängigkeit von $A = \{a_1, \dots, a_m\}$ zeigen, im Widerspruch zur Voraussetzung. Demzufolge gibt es einen Index $j \in [\![m, n]\!]$ mit $\alpha_j \neq 0$. Nach dem Austauschlemma 13.17 ist $B_0 = B_1 \setminus \{v_{i_j}\} \cup \{a_m\}$ eine Basis von V. Die Kardinalität von B_0 ist $\#B_0 \leqslant \#B_1 - 1 + 1 \leqslant n$. Wäre $a_m \in B_1 \setminus \{v_{i_j}\}$, dann würde aus

$$0 = \sum_{j=1}^{m-1} \alpha_j \, a_j + \sum_{j=m}^{n} \alpha_j \, v_{i_j} - a_m$$

folgen, das B_1 linear abhängig ist, im Widerspruch zur Basiseigenschaft von B_1. Somit folgt $\#B_0 = n$, was den Induktionsschritt für Aussage (ii) zeigt. □

Folgerung 13.19 (endliche Basen sind gleichmächtig)**.**
Es sei V ein Vektorraum.

- (i) Wenn V endlich erzeugt ist, dann ist jede Basis von V endlich, und alle Basen haben dieselbe Mächtigkeit.
- (ii) Wenn V nicht endlich erzeugt ist, dann ist jede Basis von V unendlich.

Beweis. Wir führen den Beweis für Mengen.

Aussage (i): Wenn V endlich erzeugt ist, dann gibt es ein endliches Erzeugendensystem und nach Basisergänzungssatz 13.11 damit auch eine endliche Basis B von V, sagen wir mit Mächtigkeit $\#B = n \in \mathbb{N}_0$. Es sei B_0 eine weitere (möglicherweise unendliche) Basis von V. Insbesondere jede endliche Teilmenge $B_1 \subseteq B_0$ ist dann ebenfalls linear unabhängig, und nach Satz 13.18 ist $\#B_1 \leqslant n$. Damit muss B_0 selbst endlich sein mit $\#B_0 \leqslant n = \#B$. Durch Tausch der Rollen von B und B_0 folgt auch $\#B \leqslant \#B_0$, also zusammen $\#B = \#B_0$.

Aussage (ii): Wäre B eine endliche Basis, dann wäre B auch ein endliches Erzeugendensystem, und V wäre endlich erzeugt, im Widerspruch zur Voraussetzung. □

Bemerkung 13.20 (Dimensionsbegriff für Vektorräume)**.**

- (i) Folgerung 13.19 zeigt, dass der Dimensionsbegriff aus Definition 13.16 wohldefiniert ist.

(*ii*) Der Beweis von Folgerung 13.19 verwendet den Basisergänzungssatz 13.11, jedoch nur die Version für endlich-dimensionale (endlich erzeugte) Vektorräume, die ohne das Zornsche Lemma und damit ohne das Auswahlaxiom auskommt. △

Beispiel 13.21 (Dimension eines Vektorraumes)**.**

(*i*) Der „Standardvektorraum K^n der Dimension n" über einem Körper K (Beispiel 12.3) hat tatsächlich die Dimension $n \in \mathbb{N}_0$.

(*ii*) Es gilt $\dim_{\mathbb{R}}(\mathbb{R}) = 1$ und $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$.

(*iii*) Es gilt $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ und $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. Eine Basis für $\dim_{\mathbb{R}}(\mathbb{C})$ ist $\{1, i\}$.

(*iv*) Der Nullraum $\{0\}$ ist über jedem Körper der einzige Vektorraum der Dimension 0.

(*v*) Der Polynomraum $(K[t], +, \cdot)$ über einem Körper $(K, +, \cdot)$ hat unendliche Dimension, da $B = \{1, t, t^2, \ldots\}$ eine (abzählbar) unendliche Basis von $K[t]$ ist. Die Monome $B = \{1, t, \ldots, t^n\}$ bilden eine Basis von $K_n[t]$, dem Unterraum der Polynome vom Höchstgrad $n \in \mathbb{N}_0$. Also gilt $\dim(K_n[t]) = n + 1$. △

Folgerung 13.22 (Dimension, Unterräume und lineare Unabhängigkeit)**.**
Es sei V ein Vektorraum der Dimension $n \in \mathbb{N}_0$.

(*i*) Ist $A \subseteq V$ eine linear unabhängige Teilmenge, dann gilt $\#A \leqslant n$.

(*ii*) $A \subseteq V$ ist genau dann eine Basis von V, wenn A linear unabhängig ist und $\#A = n$ gilt.

(*iii*) Für jeden Unterraum U von V gilt: $0 \leqslant \dim(U) \leqslant \dim(V)$.

(*iv*) Für jeden Unterraum U von V gilt $U = V$ genau dann, wenn $\dim(U) = \dim(V)$ ist.

Beweis. Aussage (*i*): Nach Basisergänzungssatz 13.11 existiert eine Basis B von V mit $A \subseteq B$. Nach Folgerung 13.19 ist $\#B = n$ und daher $\#A \leqslant n$.

Aussage (*ii*): Ist A eine Basis von V, dann ist A definitionsgemäß linear unabhängig, und nach Folgerung 13.19 gilt $\#A = \dim(V) = n$. Ist umgekehrt A linear unabhängig und gilt $\#A = n$, so gilt für jede Basis $B \supseteq A$ von V einerseits $\#B \geqslant \#A$, andererseite aber $\#B = \dim(V) = n$. Also muss $B = A$ sein, d. h., A ist bereits eine Basis.

Aussage (*iii*): Ist A eine Basis des Unterraumes U von V, dann ist A linear unabhängige Teilmenge von U und damit auch von V. Aus Aussage (*i*) folgt $\dim(U) = \#A \leqslant n = \dim(V)$.

Aussage (*iv*): Ist $U = V$, dann gilt $\dim(U) = \dim(V)$. Nun gelte andererseits $\dim(U) = \dim(V)$, und es sei A eine Basis von U. Dann ist A linear unabhängige Teilmenge von U und damit auch von V. Es gilt $\#A = \dim(U) = \dim(V) = n$. Aus Aussage (*ii*) folgt, dass A auch eine Basis von V ist, also gilt $U = \langle A \rangle = V$. □

Ende der Vorlesung 18

§ 14 Summen von Unterräumen

Literatur: Bosch, 2014, Kapitel 1, Fischer, Springborn, 2020, Kapitel 2.6

§ 14.1 Summen von zwei Unterräumen

Aus Lemma 12.11 wissen wir, dass der Durchschnitt $U \cap W$ zweier Unterräume U, W eines Vektorraumes V wieder ein Vektorraum ist. Die Vereinigung $U \cup W$ ist jedoch i. A. kein Unterraum von V.[17]

Es ist naheliegend, statt $U \cup W$ den kleinsten Unterraum von V zu betrachten, der $U \cup W$ enthält, also $\langle U \cup W \rangle$.

Lemma 14.1 (die lineare Hülle der Vereinigung zweier Unterräume ist die Summe.)**.**
Es sei V ein Vektorraum und U, W zwei Unterräume von V. Dann gilt

$$\langle U \cup W \rangle = U + W. \tag{14.1}$$

Wir bezeichnen den Unterraum $U + W$ als die **Summe der Unterräume** U und W (englisch: sum of two subspaces). (**Quizfrage 14.1:** Wie ist der Ausdruck $U + W$ zu verstehen?)

Beweis. Aus Satz 12.13 wissen wir, dass $\langle U \cup W \rangle$ übereinstimmt mit der Menge M aller Linearkombinationen von $U \cup W$. Wir zeigen nun, dass $M = U + W$ gilt. In der Tat sind die Elemente $u + w$ von $U + W$ auch Elemente von M, also $U + W \subseteq M$. Ist umgekehrt $v \in M$, dann hat v eine Darstellung der Form

$$v = \sum_{i=1}^{n} \alpha_i u_i + \sum_{j=1}^{m} \beta_j w_j$$

mit $n, m \in \mathbb{N}_0$, $\alpha_i, \beta_j \in K$ und $u_i \in U$ sowie $w_j \in W$. Da U und W Unterräume sind, ergibt die erste Summe wieder ein Element von U, und die zweite Summe ergibt ein Element von W. Das zeigt $M \subseteq U + W$, also insgesamt $M = U + W$. □

Bemerkung 14.2 (Ordnung auf der Menge aller Unterräume)**.**
Die Mengeninklusion ist eine Halbordnung auf der Menge aller Unterräume eines gegebenen (möglicherweise unendlich-dimensionalen) Vektorraumes V. Sie stimmt überein mit der Halbordnung „ist Unterraum von“. Für je zwei Unterräume U und W ist $U \cap W$ das Infimum von $\{U, W\}$ (Definition 5.10) und $U + W$ das Supremum von $\{U, W\}$. Genau dann, wenn $U \subseteq W$ oder $W \subseteq U$ gilt, ist das Infimum ein Minimum und das Supremum ein Maximum. △

Satz 14.3 (Dimension der Summe von zwei Unterräumen)**.**
Es seien V ein Vektorraum und U, W zwei endlich-dimensionale Unterräume von V. Dann gilt

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W). \tag{14.2}$$

Beweis. $U \cap W$ ist ebenfalls ein endlich-dimensionaler Unterraum von V, besitzt also eine endliche Basis $\{v_1, \dots, v_m\}$ mit $m = \dim(U \cap W) \in \mathbb{N}_0$. Nach dem Basisergänzungssatz 13.11 kann diese Basis zu einer Basis von U bzw. einer Basis von W ergänzt werden. Es gibt also $\{u_1, \dots, u_k\} \subseteq U$ und $\{w_1, \dots, w_\ell\} \subseteq W$ mit $k, \ell \in \mathbb{N}_0$, sodass

$$\begin{aligned} B_U &:= \{v_1, \dots, v_m,\ u_1, \dots, u_k\} && \text{Basis von } U \\ B_W &:= \{v_1, \dots, v_m,\ w_1, \dots, w_\ell\} && \text{Basis von } W \end{aligned}$$

[17] Tatsächlich gilt: $U \cup W$ ist genau dann ein Unterraum, wenn $U \subseteq W$ oder $W \subseteq U$ gilt (Hausaufgabe 8.3). Ein analoges Resultat gilt auch für Untergruppen (Hausaufgabe 5.1), Unterringe und Unterkörper.

ist. Wir zeigen nun, dass $B \coloneqq \{v_1, \ldots, v_m,\ u_1, \ldots, u_k,\ w_1, \ldots, w_\ell\}$ eine Basis von $U + W$ ist. Wegen $B = B_U \cup B_W$ ist B ein Erzeugendensystem von $U + W$. Die lineare Unabhängigkeit von B zeigen wir wie folgt: Wir setzen die Linearkombination

$$\sum_{i=1}^{m} \alpha_i v_i + \sum_{i=1}^{k} \beta_i u_i + \sum_{i=1}^{\ell} \gamma_i w_i = 0$$

an mit Koeffizienten $\alpha_i, \beta_i, \gamma_i \in K$. Definieren wir $u \coloneqq \sum_{i=1}^{m} \alpha_i v_i + \sum_{i=1}^{k} \beta_i u_i \in U$, so gilt

$$u = \sum_{i=1}^{\ell} (-\gamma_i)\, w_i \in W,$$

also $u \in U \cap W$. Wir haben also

$$\begin{aligned} \text{einerseits} \quad & u \in U \qquad = \langle v_1, \ldots, v_m,\ u_1, \ldots, u_k \rangle \\ \text{und andererseits} \quad & u \in U \cap W = \langle v_1, \ldots, v_m \rangle. \end{aligned}$$

Aus der Eindeutigkeit der Darstellung (Lemma 13.6) folgt $\beta_1 = \ldots = \beta_k = 0$. Es folgt also

$$\sum_{i=1}^{m} \alpha_i v_i + \sum_{i=1}^{\ell} \gamma_i w_i = 0,$$

und da $B_W = \{v_1, \ldots, v_m,\ w_1, \ldots, w_\ell\}$ eine Basis ist, folgt $\alpha_1 = \ldots = \alpha_m = 0$ und $\gamma_1 = \ldots = \gamma_\ell = 0$. Das zeigt die lineare Unabhängigkeit von B, also ist B tatsächlich eine Basis von $U + W$.

Die Behauptung (14.2) folgt nun aus

$$\underbrace{m + k + \ell}_{\dim(U+W)} = \underbrace{m + k}_{\dim(U)} + \underbrace{m + \ell}_{\dim(W)} - \underbrace{m}_{\dim(U \cap W)}.$$

□

Beispiel 14.4 (Summe von zwei Unterräumen)**.**

(*i*) Für die Unterräume

$$U = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle \quad \text{und} \quad W = \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle$$

von $\mathbb{R}^2$ gilt

$$U + W = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle = \mathbb{R}^2 \quad \text{und} \quad U \cap W = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}.$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U + W)}_{2} = \underbrace{\dim(U)}_{1} + \underbrace{\dim(W)}_{1} - \underbrace{\dim(U \cap W)}_{0}.$$

(*ii*) Für die Unterräume

$$U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle \quad \text{und} \quad W = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

von $\mathbb{R}^3$ gilt

$$U + W = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle = \mathbb{R}^3 \quad \text{und} \quad U \cap W = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U + W)}_{3} = \underbrace{\dim(U)}_{2} + \underbrace{\dim(W)}_{2} - \underbrace{\dim(U \cap W)}_{1}.$$

(*iii*) Für die Unterräume

$$U = \langle 1, t^2, t^3, t^5 \rangle \quad \text{und} \quad W = \langle t, t^3, t^4 \rangle$$

von $K_5[t]$ über einem beliebigen Körper $(K, +, \cdot)$ gilt

$$U + W = \langle 1, t, t^2, t^3, t^4, t^5 \rangle = K_5[t] \quad \text{und} \quad U \cap W = \langle t^3 \rangle .$$

Die Dimensionsformel (14.2) ergibt

$$\underbrace{\dim(U+W)}_{6} = \underbrace{\dim(U)}_{4} + \underbrace{\dim(W)}_{3} - \underbrace{\dim(U \cap W)}_{1} . \qquad \triangle$$

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 Symbolen: $U \oplus W$. $\triangle$

Beispiel 14.6 (direkte Summe von zwei Unterräumen)**.**
In Beispiel 14.4 ist nur

$$\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle \oplus \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle = \mathbb{R}^2$$

eine direkte Summe. (**Quizfrage 14.2:** Woran erkennt man das?) $\triangle$

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*) $\Rightarrow$ Aussage (*ii*): $V = U \oplus W$ impliziert $V = U + W$. Für gegebenes $v \in V$ gibt es also Vektoren $u \in U$ und $w \in W$, sodass $v = u + w$ gilt. Gilt nun ebenfalls $v = u' + w'$ für Vektoren $u' \in U$ und $w' \in W$, dann gilt

$$u - u' = w' - w \in U \cap W = \{0\}$$

nach Voraussetzung. Daher muss $u = u'$ und $w = w'$ sein.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Aus der Voraussetzung folgt sofort $V = U + W$. Zu zeigen ist $U \cap W = \{0\}$.

Für $v \in U \cap W$ zeigen

$$\begin{aligned} v &= v + 0 && \text{mit } v \in U,\ 0 \in W \\ v &= 0 + v && \text{mit } 0 \in U,\ v \in W \end{aligned}$$

und die Eindeutigkeit der Zerlegung, dass $v = 0$ sein muss, also gilt tatsächlich $U \cap W = \{0\}$.

Aussage (*i*) $\Rightarrow$ 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 $(iii) \Rightarrow$ Aussage (i): Unter den Voraussetzungen zeigt die Dimensionsformel (14.2):

$$\dim(V) = \dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W) = \dim(U + W).$$

$U + W$ ist also ein Unterraum von V maximaler Dimension und damit identisch zu V. Außerdem zeigt $\dim(U + W) = 0$, dass $U \cap W = \{0\}$ gilt. □

Satz 14.8 (direkte Summe von zwei Unterräumen und Partitionierung einer Basis)**.**
Es sei V ein Vektorraum. Dann gilt:

(i) Ist B eine Basis von V und $\{B_1, B_2\}$ eine Partition[18] von B, dann gilt $V = \langle B_1\rangle \oplus \langle B_2\rangle$.

(ii) Sind U_1, U_2 Unterräume von V mit Basen B_1, B_2 und gilt $V = U_1 \oplus U_2$, so ist $B_1 \cup B_2$ eine Basis von V.

Beweis. Aussage (i): Wir zeigen zunächst $V = \langle B_1\rangle + \langle B_2\rangle$. Es gilt

$$\begin{aligned}
V &= \langle B\rangle && B \text{ ist Basis von } V\\
&= \langle B_1 \cup B_2\rangle && \text{nach Voraussetzung}\\
&= \big\langle \langle B_1\rangle \cup \langle B_2\rangle \big\rangle && \text{nach Folgerung 12.15}\\
&= \langle B_1\rangle + \langle B_2\rangle && \text{nach Lemma 14.1 (lineare Hülle der Vereinigung zweier Unterräume)}\\
&\subseteq V.
\end{aligned}$$

Damit gilt überall Gleichheit und insbesondere $\langle B_1\rangle + \langle B_2\rangle = V$.

Es bleibt $\langle B_1\rangle \cap \langle B_2\rangle = \{0\}$ zu zeigen. Nehmen wir also $v \in \langle B_1\rangle \cap \langle B_2\rangle$ an, d. h.

$$v = \sum_{i=1}^{n} \alpha_i\, b_i^1 = \sum_{i=1}^{m} \beta_i\, b_i^2$$

für geeignete endliche Teilmengen $\{b_1^1, \ldots, b_n^1\} \subseteq B_1$ und $\{b_1^2, \ldots, b_m^2\} \subseteq B_2$ und Koeffizienten α_i, β_i. Es folgt

$$0 = \sum_{i=1}^{n} \alpha_i\, b_i^1 + \sum_{i=1}^{m} (-\beta_i)\, b_i^2.$$

Da $B = B_1 \cup B_2$ eine Basis ist, ist auch die Teilmenge $\{b_1^1, \ldots, b_n^1,\ b_1^2, \ldots, b_m^2\}$ linear unabhängig. Daraus folgt $\alpha_1 = \ldots = \alpha_n = \beta_1 = \ldots = \beta_m = 0$. Das heißt aber $v = 0$ und damit $\langle B_1\rangle \cap \langle B_2\rangle = \{0\}$.

Aussage (ii): Es seien nun U_1, U_2 Unterräume von V mit Basen B_1, B_2. Wir nehmen $V = U_1 \oplus U_2$ an. Wir müssen zeigen, dass $B_1 \cup B_2$ linear unabhängig ist und ganz V erzeugt. Letzteres folgt aus

$$\begin{aligned}
\langle B_1 \cup B_2\rangle &= \big\langle \langle B_1\rangle \cup \langle B_2\rangle \big\rangle && \text{nach Folgerung 12.15}\\
&= \langle U_1 \cup U_2\rangle && \text{da } B_1 \text{ Basis von } U_1 \text{ und } B_2 \text{ Basis von } U_2 \text{ ist}\\
&= U_1 + U_2 && \text{nach Lemma 14.1 (lineare Hülle der Vereinigung zweier Unterräume)}\\
&= V && \text{nach Voraussetzung.}
\end{aligned}$$

[18] Zur Erinnerung, das heißt $B_1, B_2 \neq \emptyset$, $B = B_1 \cup B_2$ und $B_1 \cap B_2 = \emptyset$, vgl. Definition 5.18. Hier wäre sogar $B_1 = \emptyset$ oder $B_2 = \emptyset$ erlaubt.

Es seien nun $\{b_1^1, \dots, b_n^1\} \subseteq B_1$ und $\{b_1^2, \dots, b_m^2\} \subseteq B_2$ endliche Teilmengen mit $n, m \in \mathbb{N}_0$. Wir betrachten die Linearkombination

$$\sum_{i=1}^{n} \alpha_i \, b_i^1 + \sum_{i=1}^{m} \beta_i \, b_i^2 = 0 \quad \text{bzw.} \quad \sum_{i=1}^{n} \alpha_i \, b_i^1 = \sum_{i=1}^{m} (-\beta_i) \, b_i^2.$$

Die erste Linearkombination gehört zu U_1, die zweite zu U_2. Wegen $U_1 \cap U_2 = \{0\}$ ist jede Linearkombination der Nullvektor. Da B_1 und B_2 Basen sind, gilt $\alpha_1 = \ldots = \alpha_n = \beta_1 = \ldots = \beta_m = 0$. Das heißt, dass $B_1 \cup B_2$ in der Tat linear unabhängig ist. □

Folgerung 14.9 (Existenz eines komplementären Unterraumes[19])**.**

Es seien V ein Vektorraum und U ein Unterraum von V. Dann existiert ein weiterer Unterraum W von V, sodass gilt: $V = U \oplus W$.

Beweis. Es sei B_U eine Basis von U. Aus dem Basisergänzungssatz 13.11 folgt die Existenz einer Basis B von V mit $B_U \subseteq B$. Setzen wir $B_W := B \setminus B_U$ und $W := \langle B_W \rangle$, so ist W nach Satz 14.8 (i) ein Unterraum mit der gesuchten Eigenschaft. □

Definition 14.10 (komplementärer Unterraum)**.**

Es seien V ein Vektorraum und U ein Unterraum von V.

(i) Ein Unterraum W von V heißt ein **zu U komplementärer Unterraum** (englisch: complementary subspace) oder ein **Komplement** (englisch: complement) von U in V, wenn $V = U \oplus W$ gilt.

(ii) Die Dimension $\dim(W)$ eines zu U komplementären Unterraumes W heißt die **Kodimension** (englisch: codimension) von U in V, kurz: $\operatorname{codim}(U)$. △

Beachte: Komplementäre Unterräume eines Vektorraumes sind i. A. nicht eindeutig. Im Fall $U = V$ 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.

Quizfrage 14.3: Was gilt für $\operatorname{codim}(U)$ in einem endlich-dimensionalen Vektorraum?

Beispiel 14.11 (komplementärer Unterraum)**.**

(i) Jeder eindimensionale Unterraum W, der nicht identisch mit $U = \left\langle \binom{1}{1} \right\rangle$ ist, ist ein Komplement von U in $\mathbb{R}^2$.

(ii) Die komplementären Unterräume des Unterraumes $(\mathbb{R}^{\mathbb{N}})_c$ der konvergenten Folgen im Vektorraum $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$, siehe Beispiel 12.9, haben keine einfache Darstellung. △

[19] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

§ 14.2 Summen von Familien von Unterräumen

Wir beschäftigen uns abschließend noch mit Summen von einer beliebigen Anzahl von Unterräumen eines Vektorraumes.

Definition 14.12 (Summe einer Familie von Unterräumen)**.**
Es seien V ein Vektorraum und $(U_i)_{i\in I}$ eine nichtleere Familie von Unterräumen von V.

(*i*) Der Unterraum

$$\sum_{i\in I} U_i := \left\langle \bigcup_{i\in I} U_i \right\rangle \tag{14.3}$$

heißt die **Summe der Familie von Unterräumen** $(U_i)_{i\in I}$ (englisch: sum of a family of subspaces). Im Fall $I = [\![1, n]\!]$ schreiben wir auch $U_1 + \cdots + U_n$ oder $\sum_{i=1}^n U_i$.

(*ii*) Die Summe heißt **direkt** (englisch: direct sum), wenn gilt:

$$U_j \cap \sum_{i\in I\setminus\{j\}} U_i = \{0\} \quad \text{für alle } j \in I. \tag{14.4}$$

Wir schreiben dann $\bigoplus_{i\in I} U_i$. Im Fall $I = [\![1, n]\!]$ schreiben wir auch $U_1 \oplus \cdots \oplus U_n$ oder $\bigoplus_{i=1}^n U_i$. △

Beispiel 14.13 (Summe einer Familie von Unterräumen)**.**

(*i*) Für den Standardvektorraum K^n über einem Körper K mit den Basisvektoren e_i, $i = 1, \ldots, n \in \mathbb{N}$, siehe Beispiel 13.9, gilt

$$K^n = \bigoplus_{i=1}^{n} \langle e_i \rangle.$$

(*ii*) Für den Polynomraum $(K[t], +, \cdot)$ über einem Körper K mit der Basis $B = \{1, t, t^2, \ldots\}$, siehe Beispiel 13.21, gilt

$$K[t] = \bigoplus_{i\in\mathbb{N}_0} \langle t^i \rangle.$$ △

Bemerkung 14.14 (Summe einer Familie von Unterräumen)**.**

(*i*) Die Elemente der Summe einer Familie $(U_i)_{i\in I}$ von Unterräumen haben die Darstellung

$$\begin{aligned}\sum_{i\in I} U_i &= \bigcup \left\{ \sum_{i\in I_0} U_i \,\middle|\, I_0 \subseteq I \text{ ist eine endliche Teilfamilie} \right\} \\ &= \left\{ \sum_{i\in I_0} u_i \,\middle|\, I_0 \subseteq I \text{ ist eine endliche Teilfamilie und } u_i \in U_i \text{ für alle } i \in I_0 \right\}. \end{aligned} \tag{14.5}$$

(*ii*) Im Fall $\#I = 2$ stimmt die Bedingung (14.4), dass die Summe einer Familie von Unterräumen eine direkte Summe ist, überein mit Definition 14.5. Im Fall $\#I > 2$ reicht es jedoch für die Direktheit der Summe nicht aus, dass an Stelle von (14.4) nur paarweise $U_i \cap U_j = \{0\}$ für $i \neq j$ gefordert wird.

Betrachte zum Beispiel die Unterräume

$$U_1 = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle, \quad U_2 = \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle \quad \text{und} \quad U_3 = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle.$$

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 14.15 (Charakterisierung direkter Summen von Familien von Unterräumen, vgl. Satz 14.7)**.**
Es seien V ein Vektorraum und $(U_i)_{i\in I}$ eine nichtleere Familie von Unterräumen von V. Dann sind äquivalent:

(*i*) $V = \bigoplus_{i\in I} U_i$.

(*ii*) Für alle $v \in V$ existiert eine endliche Teilfamilie $I_0 \subseteq I$ und Vektoren $u_i \in U_i$, sodass $v = \sum_{i\in I_0} u_i$ gilt, und diese Darstellung ist (bis auf die Summation von Nullvektoren) eindeutig.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 9.4. □

Satz 14.16 (direkte Summe von Unterräumen und Partitionierung einer Basis, vgl. Satz 14.8)**.**
Es sei V ein Vektorraum. Dann gilt:

(*i*) Ist B eine Basis von V und $(B_i)_{i\in I}$ eine Partition von B mit nichtleerer Indexmenge I, dann gilt $V = \bigoplus_{i\in I}\langle B_i\rangle$.

(*ii*) Ist $(U_i)_{i\in I}$ eine nichtleere Familie von Unterräumen von V mit Basen B_i, $i \in I$, und gilt $V = \bigoplus_{i\in I} U_i$, so ist $\bigcup_{i\in I} B_i$ eine Basis von V.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 9.4. □

Ende der Vorlesung 19

Ende der Woche 9

Kapitel 4 Matrizen und lineare Abbildungen

§ 15 Matrizen

Literatur: Fischer, Springborn, 2020, Kapitel 3.7, Bosch, 2014, Kapitel 3, Deiser, 2022b, Kapitel 3.3, Jänich, 2008, Kapitel 4.2 und 5.1–5.5

Matrizen sind ein universelles Mittel zur Darstellung verschiedener Sachverhalte, beispielsweise in den Wirtschaftswissenschaften, in der Graphentheorie und zur Beschreibung linearer Abbildungen, das sind die Homomorphismen zwischen Vektorräumen. Diese Bedeutung von Matrizen 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 der Dimension** $n \times m$ (englisch: matrix) oder eine $n \times m$**-Matrix** A **über dem Körper** K ist eine endliche, doppelt indizierte Familie von Elementen aus K mit Indexmenge $[\![1, n]\!] \times [\![1, m]\!]$. Wir schreiben sie in der Form[1]

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}. \tag{15.1}$$

Die Menge aller $n \times m$-Matrizen wird mit $K^{n\times m}$ bezeichnet.[2]

(*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.[3]

(*iv*) Eine Matrix heißt **quadratisch** (englisch: square matrix, quadratic matrix), wenn $m = n$ gilt.

(*v*) Die quadratische $n \times n$-Diagonalmatrix

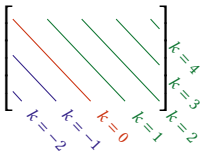
$$I_{n\times n} := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \tag{15.2}$$

[1] Alternativ können auch runde Klammern verwendet werden.
[2] Alternative Bezeichnungen sind $K^{n,m}$ oder $M_{n,m}(K)$.
[3] Man sagt auch, dass bei einer Diagonalmatrix die Nebendiagonalen „nicht besetzt“ sind, d. h., dass dort nur Nullen stehen.

heißt die $n \times n$-**Einheitsmatrix** (englisch: identity matrix).[4] Wir bezeichnen sie auch mit I_n oder einfach I, wenn die Dimension klar ist. △

Beachte: Wir lassen explizit zu, dass eine oder beide Dimensionen gleich 0 sind. Das ist aus vielerlei Gründen praktisch. Eine Matrix der Dimension $n \times 0$ oder $0 \times m$ hat keine Elemente, 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. 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

$$a_{i\bullet} := (a_{i1}, a_{i2}, \dots, a_{im}) \in K_m, \tag{15.4}$$

vgl. Beispiel 12.3. 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

$$a_{\bullet j} := \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} \in K^n, \tag{15.5}$$

vgl. nochmals Beispiel 12.3. 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 skalare Multiplikation (S-Multiplikation) wie folgt:

Definition 15.2 (Addition, skalare 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**[5], englisch: addition) und die äußere Verknüpfung $\cdot \colon K \times K^{n \times m} \to K^{n \times m}$ (**skalare Multiplikation**[6], englisch: scalar multiplication) erklärt:

$$(A + B)_{ij} := a_{ij} + b_{ij} \tag{15.6a}$$

$$(\alpha \cdot A)_{ij} := \alpha \cdot a_{ij} \tag{15.6b}$$

für $A, B \in K^{n \times m}$ und $\alpha \in K$. △

[4] Alternative Bezeichnungen sind I_n oder id_n.
[5] Die Bezeichnung ist dieselbe wie die der „Addition“ im Körper K.
[6] Auch hier ist die Bezeichnung dieselbe wie die der „Multiplikation“ im Körper K.

Wir werden das Zeichen · für die skalare Multiplikation in der Regel weglassen, vgl. Bemerkung 12.10.

Lemma 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 Vektorraum über K. Dieser besitzt die Dimension $n\,m$, und die Matrizen

$$\{E_{11}, \ldots, E_{nm}\} \text{ mit } E_{ij} \coloneqq \underbrace{\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{\uparrow j\text{-te Spalte}} \leftarrow i\text{-te Zeile} = \delta_{ij} \tag{15.7}$$

bilden eine Basis, genannt die **kanonische Basis** (englisch: canonical basis), **Standardbasis** (englisch: standard basis) oder **Einheitsbasis** (englisch: unit basis) von $K^{n\times m}$.

Beweis. Die Eigenschaften eines Vektorraumes (Definition 12.1) sind leicht nachzurechnen: $(K^{n\times m}, +)$ 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 13.10 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 der Basiselemente. □

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 Vektorraum über K. Dieser kann identifiziert werden mit K selbst.

(*iii*) Die Vektorräume der $0 \times m$- und der $n \times 0$-Matrizen sind nulldimensionale Vektorräume über K. △

§ 15.1 Matrix-Matrix-Multiplikation

Für Matrizen passender Dimensionen können wir eine Matrix-Matrix-Multiplikation einführen. Diese ist von fundamentaler Bedeutung für den Umgang mit Matrizen.

Definition 15.5 (Matrix-Matrix-Multiplikation)**.**

Es seien $(K, +, \cdot)$ ein Körper und $m, n, \ell \in \mathbb{N}_0$. Für Matrizen ist die **Matrix-Matrix-Multiplikation** (englisch: matrix-matrix multiplication) oder kurz **Matrix-Multiplikation** (englisch: matrix multiplication) wie folgt definiert:

$$\cdot \colon K^{n\times m} \times K^{m\times \ell} \to K^{n\times \ell}, \tag{15.9a}$$

wobei für $A \in K^{n\times m}$, $B \in K^{m\times \ell}$ und $C := A \cdot B \in K^{n\times \ell}$ gilt:

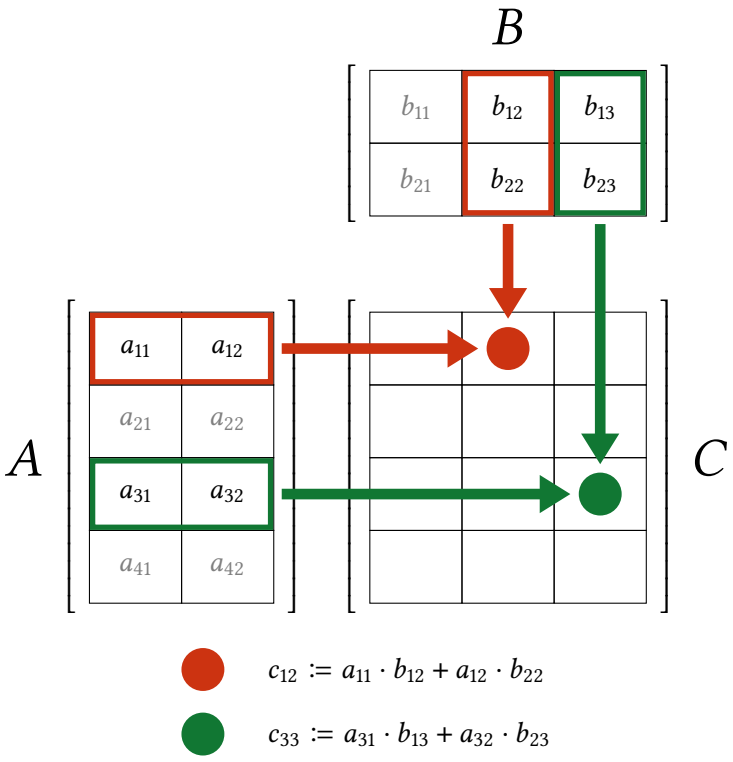
$$c_{ik} := \sum_{j=1}^{m} a_{ij} \cdot b_{jk} \quad \text{für } 1 \leqslant i \leqslant n \text{ und } 1 \leqslant k \leqslant \ell. \tag{15.9b}$$

△

Beachte: Die Summation verwendet die „Addition“ + aus dem Körper K, und in jedem Summanden kommt die „Multiplikation“ $\cdot$ aus K vor.

Beachte: Im Fall $m = 0$ sind die Summen in (15.9b) alle leer. Daher ist das Produkt einer $n \times 0$- und einer $0 \times m$-Matrix die $n \times m$-Nullmatrix.

Den Fall der Matrix-Multiplikation einer 4×2-Matrix A mit einer 2×3-Matrix B können wir wie folgt grafisch darstellen:



Beispiel 15.6 (Matrix-Multiplikation).

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} \cdot \begin{bmatrix} 5 & 2 & -4 \\ 0 & -2 & 8 \end{bmatrix}$$

$$= \begin{bmatrix} 1\cdot 5 + (-3)\cdot 0 & 1\cdot 2 + (-3)\cdot(-2) & 1\cdot(-4) + (-3)\cdot 8 \\ 2\cdot 5 + 4\cdot 0 & 2\cdot 2 + 4\cdot(-2) & 2\cdot(-4) + 4\cdot 8 \\ 5\cdot 5 + 0\cdot 0 & 5\cdot 2 + 0\cdot(-2) & 5\cdot(-4) + 0\cdot 8 \\ (-3)\cdot 5 + (-6)\cdot 0 & (-3)\cdot 2 + (-6)\cdot(-2) & (-3)\cdot(-4) + (-6)\cdot 8 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 8 & -28 \\ 10 & -4 & 24 \\ 25 & 10 & -20 \\ -15 & 6 & -36 \end{bmatrix}.$$

△

Bemerkung 15.7 (Matrix-Multiplikation).

(*i*) $A \cdot B$ ist genau dann definiert, wenn die Anzahl der Spalten des linken Faktors A übereinstimmt mit der Anzahl der Zeilen des rechten Faktors B.

(*ii*) Das Produkt $A \cdot B$ hat soviele Zeilen wie der linke Faktor A und soviele Spalten wie der rechte Faktor B. Die „mittlere Dimension“ ist nach der Bildung des Produkts $A \cdot B$ nicht mehr sichtbar.

(*iii*) 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.

(*iv*) 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 von 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.

Im Beispiel oben 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 von 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.

Im Beispiel oben 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 $(K, +, \cdot)$ ein Körper und $m, n, p, q \in \mathbb{N}_0$. Für Matrizen $A, A_1, A_2 \in K^{n\times m}$, $B, B_1, B_2 \in K^{m\times p}$, $C \in K^{p\times q}$ und Skalare $\alpha \in K$ gelten die folgenden Eigenschaften:

$$A \cdot (B_1 + B_2) = A \cdot B_1 + A \cdot B_2 \quad \textbf{Distributivgesetz}[7] \tag{15.10a}$$

$$(A_1 + A_2) \cdot B = A_1 \cdot B + A_2 \cdot B \quad \textbf{Distributivgesetz} \tag{15.10b}$$

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \textbf{Assoziativgesetz}[8] \tag{15.11}$$

$$A \cdot (\alpha \cdot B) = (\alpha \cdot A) \cdot B = \alpha \cdot (A \cdot B) \quad \text{Skalare können überall stehen} \tag{15.12}$$

$$I_n \cdot A = A \cdot I_m = A \quad \text{Neutralität der Einheitsmatrix} \tag{15.13}$$

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

$$\begin{aligned} \big[A \cdot (\alpha \cdot B)\big]_{ik} &= \sum_{j=1}^{m} a_{ij}\,(\alpha \cdot B)_{jk} = \sum_{j=1}^{m} a_{ij}\,(\alpha\, b_{jk}) = \sum_{j=1}^{m} (\alpha\, a_{ij})\, b_{jk} = \big[(\alpha \cdot A) \cdot B\big]_{ik} \\ &= \alpha \sum_{j=1}^{m} a_{ij}\, b_{jk} = \alpha\,\big[A \cdot B\big]_{ik}, \end{aligned}$$

[7] englisch: distributive law
[8] englisch: associative law

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). □

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 $A \in K^{n\times m}$ und $x \in K^m$ (aufgefasst als $m \times 1$-Matrix) ist. Beispielsweise ist

$$\begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} \begin{pmatrix} 2 \\ -2 \end{pmatrix} = \begin{pmatrix} 8 \\ -4 \\ 10 \\ 6 \end{pmatrix}.$$

Ein zweiter Spezialfall ist die **Vektor-Matrix-Multiplikation** (englisch: vector-matrix multiplication) $y\,A$, wobei $A \in K^{n\times m}$ und $y \in K_n$ (aufgefasst als $1 \times n$-Matrix) ist. Beispielsweise gilt

$$\begin{pmatrix} 2 & 0 & 1 & -1 \end{pmatrix} \begin{bmatrix} 1 & -3 \\ 2 & 4 \\ 5 & 0 \\ -3 & -6 \end{bmatrix} = \begin{pmatrix} 10 & 0 \end{pmatrix}.$$ △

Ende der Vorlesung 20

§ 15.2 Zeilen- und Spaltenraum

Definition 15.10 (Zeilen- und Spaltenraum, Zeilen- und Spaltenrang)**.**
Es seien $(K, +, \cdot)$ ein Körper, $m, n \in \mathbb{N}_0$ und $A \in \mathbb{R}^{n\times m}$.

(*i*) Die lineare Hülle der Zeilenvektoren $a_{1\bullet}, \ldots, a_{n\bullet} \in K_m$ heißt der **Zeilenraum** (englisch: row space) von A:

$$\mathrm{ZR}(A) \coloneqq \langle a_{1\bullet}, \ldots, a_{n\bullet} \rangle \subseteq K_m. \tag{15.14a}$$

Die Dimension von $\mathrm{ZR}(A)$ heißt der **Zeilenrang** von A (englisch: row rank), also

$$\mathrm{ZRang}(A) \coloneqq \dim(\mathrm{ZR}(A)). \tag{15.14b}$$

(*ii*) Die lineare Hülle der Spaltenvektoren $a_{\bullet 1}, \ldots, a_{\bullet m} \in K^n$ heißt der **Spaltenraum** (englisch: column space) von A:

$$\mathrm{SR}(A) \coloneqq \langle a_{\bullet 1}, \ldots, a_{\bullet m} \rangle \subseteq K^n. \tag{15.15a}$$

Die Dimension von $\mathrm{SR}(A)$ heißt der **Spaltenrang** von A (englisch: column rank), also

$$\mathrm{SRang}(A) \coloneqq \dim(\mathrm{SR}(A)). \tag{15.15b}$$

△

Beachte: Wir könnten äquivalent den Zeilenrang auch definieren als die maximale Anzahl linear unabhängiger Zeilen von A und den Spaltenrang als die maximale Anzahl linear unabhängiger Spalten von A. (**Quizfrage 15.1:** Warum gilt das?)

Beispiel 15.11 (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

$$\mathrm{ZR}(A) = \overbrace{\left\langle \begin{pmatrix} 2 & 3 & -1 \end{pmatrix}, \begin{pmatrix} 7 & 4 & 0 \end{pmatrix} \right\rangle}^{\text{linear unabhängig}} \qquad \text{mit } \mathrm{ZRang}(A) = \dim(\mathrm{ZR}(A)) = 2$$

$$\text{und} \quad \mathrm{SR}(A) = \underbrace{\left\langle \begin{pmatrix} 2 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix} \right\rangle}_{\text{linear abhängig}} = \underbrace{\left\langle \begin{pmatrix} 2 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\rangle}_{\text{linear unabhängig}} \quad \text{mit } \mathrm{SRang}(A) = \dim(\mathrm{SR}(A)) = 2.$$

△

Die hier beobachtete Übereinstimmung von Zeilen- und Spaltenrang ist kein Zufall:

Satz 15.12 (Zeilenrang gleich Spaltenrang)**.**
Es seien $(K, +, \cdot)$ 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. **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 $c_{1\bullet}, \ldots, c_{r\bullet} \in K_m$ eine Basis des Zeilenraumes $\mathrm{ZR}(A)$ bilden, also $\langle c_{1\bullet}, \ldots, c_{r\bullet} \rangle = \mathrm{ZR}(A)$. 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 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

$$\begin{aligned} & \mathrm{SR}(A) \subseteq \mathrm{SR}(B) \\ \Rightarrow \quad & \mathrm{SRang}(A) \leqslant \mathrm{SRang}(B) \leqslant r = \mathrm{ZRang}(A) \quad \text{nach Folgerung 13.22.} \end{aligned}$$

Schritt 2: Wir zeigen $\mathrm{ZRang}(A) \leqslant \mathrm{SRang}(A)$.

Es sei nun $s := \mathrm{SRang}(A) \in \mathbb{N}_0$ 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 $\mathrm{SR}(A)$ bilden, also $\langle b_{\bullet 1}, \dots b_{\bullet s}\rangle = \mathrm{SR}(A)$. Die j-te Spalte $a_{\bullet j}$ von A, die ja zu $\mathrm{SR}(A)$ gehört, ist also eine Linearkombination der Spalten von B, sagen wir

$$a_{\bullet j} = b_{\bullet 1}\, c_{1j} + \dots + b_{\bullet s}\, c_{sj}.$$

Da das Gesagte für jede Spalte von A gilt, erhalten wir die Darstellung

$$A = B\,C = \begin{bmatrix} | & & | \\ b_{\bullet 1} & \cdots & b_{\bullet s} \\ | & & | \end{bmatrix} \begin{bmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1m} \\ \vdots & & \vdots & & \\ c_{s1} & \cdots & c_{sj} & \cdots & c_{sm} \end{bmatrix}$$

mit einer Koeffizientenmatrix $C \in K^{s\times m}$.

Wegen $y\,A = (y\,B)\,C$ für alle $y \in K_n$ ist jede Linearkombination der Zeilen von A auch eine Linearkombination der Zeilen von C, es gilt also

$$\begin{aligned} & \mathrm{ZR}(A) \subseteq \mathrm{ZR}(C) \\ \Rightarrow\quad & \mathrm{ZRang}(A) \leqslant \mathrm{ZRang}(C) \leqslant s = \mathrm{SRang}(A) \quad \text{nach Folgerung 13.22.} \end{aligned}$$

Der Beweis bis hierher zeigt $0 \leqslant \mathrm{ZRang}(A) = \mathrm{SRang}(A)$ für beliebige Matrizen $A \in K^{n\times m}$. Wegen $\mathrm{ZRang}(A) \leqslant n$ und $\mathrm{SRang}(A) \leqslant m$ folgt die Behauptung (15.16). □

Da der Zeilenrang und Spaltenrang einer Matrix übereinstimmen, sprechen wir ab sofort nur noch vom **Rang** (englisch: rank), bezeichnet mit $\mathrm{Rang}(A)$. Als direktes Resultat aus dem Beweis von Satz 15.12 halten wir fest:

Folgerung 15.13 (Rangfaktorisierung)**.**

Es seien $(K, +, \cdot)$ ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Ist $r = \mathrm{Rang}(A) \in \mathbb{N}_0$, dann existieren Matrizen $B \in K^{n\times r}$ und $C \in K^{r\times m}$, sodass gilt:

$$A = B\,C. \tag{15.17}$$

Die Spalten von B bilden eine Basis von $\mathrm{SR}(A)$. Die Zeilen von C bilden eine Basis von $\mathrm{ZR}(A)$.

Eine solche Faktorisierung der Matrix A, bei der die inneren Dimensionen der Faktoren mit dem $\mathrm{Rang}(A)$ übereinstimmt, heißt eine **Rangfaktorisierung** (englisch: rank factorization) von A.

Satz 15.14 (Rang des Produkts von Matrizen)**.**

Es seien $(K, +, \cdot)$ 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:

$$0 \leqslant \mathrm{Rang}(A\,B) \leqslant \min\{\mathrm{Rang}(A),\ \mathrm{Rang}(B)\} \leqslant \min\{\ell, m, n\}. \tag{15.18}$$

Beweis. Wir verwenden dieselbe Technik wie im Beweis von Satz 15.12: 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 $\mathrm{SR}(A\,B) \subseteq \mathrm{SR}(A)$ und somit $\mathrm{Rang}(A\,B) = \mathrm{SRang}(A\,B) \leqslant \mathrm{SRang}(A) = \mathrm{Rang}(A)$.

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 $\mathrm{ZR}(A\,B) \subseteq \mathrm{ZR}(B)$ und somit $\mathrm{Rang}(A\,B) = \mathrm{ZRang}(A\,B) \leqslant \mathrm{ZRang}(B) = \mathrm{Rang}(B)$.

Die zweite Ungleichung folgt sofort aus $\mathrm{Rang}(A) \leqslant \min\{m, n\}$ und $\mathrm{Rang}(B) \leqslant \min\{\ell, m\}$, siehe Satz 15.12. □

§ 15.3 Zeilenstufenform

Wir geben in diesem Abschnitt eine konstruktive Möglichkeit an, eine Rangfaktorisierung einer Matrix A und damit auch den $\mathrm{Rang}(A)$ zu bestimmen. Dazu bringen wir die Matrix A durch geschickte Umformungen auf eine Gestalt, aus der wir eine Basis von $\mathrm{ZR}(A)$ und damit die Dimension von $\mathrm{ZR}(A)$, also den Zeilenrang von A, ablesen können.

Definition 15.15 (elementare Zeilenumformungen, Elementarmatrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper, $m, n \in \mathbb{N}_0$ und

$$A = \begin{bmatrix} & a_{1\bullet} & \\ & \vdots & \\ & a_{i\bullet} & \\ & \vdots & \\ & a_{n\bullet} & \end{bmatrix} \in \mathbb{R}^{n\times m}.$$

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

$$D := \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & \alpha & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} = I + (\alpha - 1)\,E_{ii}. \tag{15.19}$$

Es gilt (nur die Änderungen gegenüber A werden hervorgehoben)

$$D\,A = \begin{bmatrix} & \vdots & \\ & \alpha\,a_{i\bullet} & \\ & \vdots & \end{bmatrix}.$$

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[9]

$$S := \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & \alpha & 1 & \\ & & & \ddots \\ & & & & 1 \end{bmatrix} = I + \alpha E_{ij}. \tag{15.20}$$

Es gilt

$$SA = \begin{bmatrix} & \vdots & \\ \cdots & a_{j\bullet} & \cdots \\ & \vdots & \\ \cdots & a_{i\bullet} + \alpha a_{j\bullet} & \cdots \\ & \vdots & \end{bmatrix}.$$

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

$$T := \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & 1 & & 0 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{bmatrix} = I - E_{ii} - E_{jj} + E_{ij} + E_{ji}. \tag{15.21}$$

Es gilt

$$TA = \begin{bmatrix} & \vdots & \\ \cdots & a_{j\bullet} & \cdots \\ & \vdots & \\ \cdots & a_{i\bullet} & \cdots \\ & \vdots & \end{bmatrix}.$$

Die Matrizen D, S und T heißen **Elementarmatrizen** (englisch: elementary matrices) vom Typ I, Typ II bzw. Typ III. Die Matrizen T (Typ III) heißen genauer auch **Transpositionsmatrizen** (englisch: transposition matrices) △

Lemma 15.16 (elementare Zeilenumformungen ändern den Zeilenraum und den Zeilenrang nicht)**.** Es seien $(K, +, \cdot)$ 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 $\mathrm{Rang}(C) = \mathrm{Rang}(A)$.

[9] Die Illustration zeigt den Fall $i > j$.

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 15.17 (Zeilenstufenform)**.**
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. △

Bemerkung 15.18 (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 weiter nach rechts und können dabei auch Spalten überspringen.

(*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 $K \setminus \{0\}$ durchmultiplizieren können. Außerdem können wir zu einer Zeile ein Vielfaches einer weiter unten stehenden Zeile addieren, ohne die Zeilenstufenform zu stören. △

Beispiel 15.19 (Zeilenstufenform)**.**
Hier sind die Besetzungsmuster einiger 3×4-Matrizen in Zeilenstufenform, wobei $\star$ jeweils für einen Eintrag ungleich 0 steht (die Pivot-Elemente) und ? für einen beliebigen Eintrag aus dem Körper K.

$$\begin{matrix} j_1 = 1 \to \\ j_2 = 2 \to \\ j_3 = 3 \to \end{matrix}\begin{bmatrix} \star & ? & ? & ? \\ 0 & \star & ? & ? \\ 0 & 0 & \star & ? \end{bmatrix} \qquad r = 3$$

$$\begin{matrix} j_1 = 1 \to \\ j_2 = 3 \to \end{matrix}\begin{bmatrix} \star & ? & ? & ? \\ 0 & 0 & \star & ? \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad r = 2$$

$$\begin{matrix} j_1 = 3 \to \\ j_2 = 4 \to \end{matrix}\begin{bmatrix} 0 & 0 & \star & ? \\ 0 & 0 & 0 & \star \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad r = 2$$

△

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. Der Spaltenindex sei j_1. Bringe es durch Zeilentausch (elementare Zeilenumformung vom Typ III) an die 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 $j_1 + 1$.

Das vollständige Verfahren kann wie folgt angegeben werden:

Algorithmus 15.20 (Erzeugen der Zeilenstufenform).
Eingabe: Matrix $A \in K^{n\times m}$
Ausgabe: Matrix $C \in K^{n\times m}$ in Zeilenstufenform mit $\mathrm{ZR}(A) = \mathrm{ZR}(C)$ // Die ersten r Zeilen von C bilden eine Basis von $\mathrm{ZR}(A)$.
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 $j \leftarrow \min\left\{j_r + 1 \leqslant j \leqslant m \,\middle|\, (C)_{r+1\leqslant i\leqslant n,\ j}\right\}$ // erste Nicht-Nullspalte der Restmatrix
  Setze $i \leftarrow \min\left\{r + 1 \leqslant i \leqslant n \,\middle|\, c_{ij} \neq 0\right\}$ // 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
  Tausche in der Matrix C die Zeilen i und r // Pivot-Element kommt nach oben (Typ III)
  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 unterhalb des Pivot-Elements (r, j) (Typ II)
  end for
end while
return C und r // C ist eine Zeilenstufenform von A und $r = \mathrm{Rang}(A)$

Mit Hilfe von Algorithmus 15.20 können wir folgenden Satz konstruktiv beweisen:

Satz 15.21 (Erreichbarkeit der Zeilenstufenform).
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. Es sei $r \in [\![0, m]\!]$ die Anzahl der Nicht-Nullzeilen in C. Dann bilden die Zeilenvektoren $c_{1\bullet}, \ldots, c_{r\bullet}$ eine Basis von $\mathrm{ZR}(A) = \mathrm{ZR}(C)$. Für den Rang gilt $\mathrm{Rang}(A) = \mathrm{Rang}(C) = r$.

Beispiel 15.22 (Erreichbarkeit der Zeilenstufenform).
Wir betrachten ein Beispiel in $\mathbb{R}^{3\times 4}$:

$$\begin{bmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 3 & 0 & 2 \end{bmatrix}$$

Tauschen der Zeilen 1 und 2

$$\begin{bmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 3 & 0 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & -6 & 2 \end{bmatrix}$$

Erzeugen von Nullen unterhalb des Pivot-Elements
Addition des (-3)-Fachen der Zeile 1 zur Zeile 3

$$\begin{bmatrix} 0 & \boxed{1} & 2 & 0 \\ 0 & 0 & \boxed{3} & -1 \\ 0 & 0 & \boxed{-6} & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 0 & \boxed{1} & 2 & 0 \\ 0 & 0 & \boxed{3} & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

2 ↷

Erzeugen von Nullen unterhalb des Pivot-Elements
Addition des 2-Fachen der Zeile 2 zur Zeile 3.

Die Zeilenstufenform ist erreicht. Der Zeilenraum von A ist also

$$\mathrm{ZR}(A) = \left\langle \begin{pmatrix} 0 & 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 3 & -1 \end{pmatrix} \right\rangle \quad \text{mit } \dim(\mathrm{ZR}(A)) = \mathrm{Rang}(A) = 2. \qquad \triangle$$

Bemerkung 15.23 (Berechnung einer Rangfaktorisierung)**.**
Wir hatten eingangs des Abschnitts angekündigt, eine konstruktive Möglichkeit anzugeben, eine Rangfaktorisierung $A = BC$ einer Matrix $A \in K^{n\times m}$ zu bestimmen, sodass also $B \in K^{n\times r}$, $C \in K^{r\times m}$ 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; die resultierende Matrix sei $\overline{C} \in K^{r\times m}$. Wie aber kommen wir an den linken Faktor B?

Die Zeilenstufenform entstand durch Multiplikation mit Elementarmatrizen $E_j \in K^{n\times n}$:

$$E_k \cdots E_2 E_1 A = C. \tag{15.22}$$

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[10], 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 (Hausaufgabe 10.3). Setzen wir nun zur Abkürzung $B := E'_1 E'_2 \cdots E'_k$, so erhalten wir die Faktorisierung

$$A = \underbrace{\begin{array}{c} \overset{r}{\overline{B}} \end{array}}_{B} \underbrace{\begin{array}{c} \overset{m}{\overline{C}} \\ \hline 0 \end{array}}_{C} \begin{matrix} \\ r \\ n-r \end{matrix}$$

Da bei der Bildung des Matrix-Produkts $A = BC$ die letzten $n - r$ Spalten von B immer nur mit Null-Koeffizienten multipliziert werden, können wir, ohne das Ergebnis zu ändern, den rechten Faktor C durch seine oberen r Zeilen $\overline{C}$ und den linken Faktor B durch seine linken r Spalten $\overline{B}$ ersetzen. So erhalten wir die gewünschte Rangfaktorisierung

$$A = \overline{B}\,\overline{C}$$

mit $\overline{B} \in K^{n\times r}$ und $\overline{C} \in K^{r\times m}$. (**Quizfrage 15.3:** Wie müsste Algorithmus 15.20 ergänzt werden, damit wir als Ergebnis die Faktorisierung $A = BC$ erhalten, aus der dann durch Streichen von Spalten bzw. Zeilen die Rangfaktorisierung $A = \overline{B}\,\overline{C}$ folgt?) $\triangle$

§ 15.4 Transposition von Matrizen

Definition 15.24 (Transposition)**.**
Es seien $(K, +, \cdot)$ ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$. Die Matrix $A^\intercal \in K^{m\times n}$, definiert durch $(A^\intercal)_{ij} = (A)_{ji}$ für $i \in [\![1, m]\!]$ und $j \in [\![1, n]\!]$, heißt die zu A **transponierte Matrix** (englisch: transposed matrix) oder kurz die **Transponierte** zu A. $\triangle$

[10] Später (Definition 15.36) werden wir solche Matrizen **invertierbar** nennen.

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 15.25 (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 15.26 (Rechenregeln für Transponierte)**.**
Es seien $(K, +, \cdot)$ 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:

$$(A^\mathsf{T})^\mathsf{T} = A \quad \text{Transposition ist } \textbf{involutorisch} \tag{15.24}$$
$$(A+B)^\mathsf{T} = A^\mathsf{T} + B^\mathsf{T} \quad \text{Transposition ist linear}^{11} \tag{15.25a}$$
$$(\alpha A)^\mathsf{T} = \alpha A^\mathsf{T} \quad \text{Transposition ist linear} \tag{15.25b}$$
$$(AC)^\mathsf{T} = C^\mathsf{T} A^\mathsf{T} \tag{15.26}$$

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 15.27 (Rang der transponierten Matrix)**.**
Es seien $(K, +, \cdot)$ 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 15.13), also gilt $B \in K^{n\times r}$ und $C \in K^{r\times m}$ mit $r = \operatorname{Rang}(A)$. Aufgrund von (15.26) gilt $A^\mathsf{T} = C^\mathsf{T} B^\mathsf{T}$. Aus Satz 15.14 und Satz 15.12 folgt $\operatorname{Rang}(A^\mathsf{T}) \leqslant \min\{\operatorname{Rang}(B^\mathsf{T}), \operatorname{Rang}(C^\mathsf{T})\} \leqslant \min\{m, n, r\} \leqslant r = \operatorname{Rang}(A)$.

Führen wir dasselbe Argument nochmal mit einer Rangfaktorisierung $A^\mathsf{T} = \widehat{B}\widehat{C}$ mit $\widehat{B} \in K^{m\times s}$ und $C \in K^{s\times n}$ und $s = \operatorname{Rang}(A^\mathsf{T})$ durch, so ergibt sich unter Beachtung von (15.24) genauso auch $\operatorname{Rang}(A) \leqslant \min\{m, n, s\} \leqslant s = \operatorname{Rang}(A^\mathsf{T})$, zusammen also $\operatorname{Rang}(A) = \operatorname{Rang}(A^\mathsf{T})$. □

Definition 15.28 (symmetrische und antisymmetrische Matrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper, $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$.

(*i*) A heißt **symmetrisch** (englisch: symmetric matrix), wenn $A = A^\mathsf{T}$ gilt.

[11] Die Sprechweise, dass die Transposition eine lineare Abbildung sei, wird in § 17 klar werden.

(*ii*) A heißt **antisymmetrisch** (englisch: antisymmetric matrix) oder **schiefsymmetrisch** (englisch: skew-symmetric matrix), 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. $K^{n\times n}_{\text{skew}}$. △

Lemma 15.29 (symmetrische und antisymmetrische Anteile quadratischer Matrizen)**.**
Es seien $(K, +, \cdot)$ 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

$$\dim(K^{n\times n}_{\text{sym}}) = \frac{1}{2} n\,(n+1) \tag{15.27a}$$

$$\dim(K^{n\times n}_{\text{skew}}) = \frac{1}{2} n\,(n-1). \tag{15.27b}$$

Es 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 im Körper $\mathbb{Z}_2$ der Charakteristik $\operatorname{char}(K) = 2$?

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 10.4. □

Ende der Vorlesung 21

Ende der Woche 10

§ 15.5 Der Ring quadratischer Matrizen

Die Menge der quadratischen Matrizen $K^{n\times n}$ ist bzgl. der Matrix-Multiplikation abgeschlossen. Zusammen mit der Matrix-Addition ergibt sich eine Ringstruktur $(K^{n\times n}, +, \cdot)$:

Lemma 15.30 (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.

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 (Lemma 15.3). 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

$$E_{11} \cdot E_{12} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & & & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & & & 0 \end{bmatrix} = E_{12}$$

$$E_{12} \cdot E_{11} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & & & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} = 0,$$

das für beliebige Körper K gültig ist. □

Der Ring der quadratischen Matrizen $K^{n\times n}$ enthält neben den Diagonalmatrizen noch einige erwähnenswerte Teilmengen. Um Dreiecksmatrizen von strikten Dreiecksmatrizen unterscheiden zu können, schließen wir für die folgenden Resultate die 0×0-Matrizen aus.

Definition 15.31 (obere und untere Dreiecksmatrix)**.**
Es seien $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Eine Matrix $A \in K^{n\times n}$ heißt

(*i*) eine **obere Dreiecksmatrix** (englisch: upper triangular matrix), wenn $a_{ij} = 0$ für alle $i > j$ gilt.

(*ii*) eine **strikte obere Dreiecksmatrix** (englisch: strictly upper triangular matrix), wenn $a_{ij} = 0$ für alle $i \geqslant j$ gilt.

(*iii*) eine **untere Dreiecksmatrix** (englisch: lower triangular matrix), wenn $a_{ij} = 0$ für alle $i < j$ gilt.

(*iv*) eine **strikte untere Dreiecksmatrix** (englisch: strictly lower triangular matrix), wenn $a_{ij} = 0$ für alle $i \leqslant j$ gilt.

(*v*) **nilpotent** (englisch: nilpotent), wenn es ein $k \in \mathbb{N}_0$ gibt mit der Eigenschaft $A^k = 0$.

Hier gilt für die Indizes jeweils $1 \leqslant i, j \leqslant n$. △

Wir bezeichnen die Menge der Diagonalmatrizen der Dimension $n \times n$ auch mit $K^{n\times n}_{\diagdown}$ und die Menge der oberen bzw. unteren Dreiecksmatrizen mit $K^{n\times n}_{\diagdown\!\!\!\!\blacktriangleleft}$ bzw. $K^{n\times n}_{\diagdown\!\!\!\!\blacktriangleright}$. Es gilt

$$K^{n\times n}_{\diagdown} = K^{n\times n}_{\diagdown\!\!\!\!\blacktriangleleft} \cap K^{n\times n}_{\diagdown\!\!\!\!\blacktriangleright}.$$

Beispiel 15.32 (obere und untere Dreiecksmatrix)**.**

(*i*)
$$\begin{bmatrix} 1 & 3 & -3 \\ 0 & 7 & 4 \\ 0 & 0 & 5 \end{bmatrix}$$
ist eine obere Dreiecksmatrix, aber keine strikte obere Dreiecksmatrix.

(*ii*)
$$\begin{bmatrix} 0 & 0 & 0 \\ 7 & 0 & 0 \\ 2 & 1 & 0 \end{bmatrix}$$
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,[12] denn es gilt

$$\begin{bmatrix} 2 & 2 & -2 \\ 5 & 1 & -3 \\ 1 & 5 & -3 \end{bmatrix}^3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

△

Lemma 15.33 (strikte Dreiecksmatrizen sind nilpotent)**.**

Es seien $(K, +, \cdot)$ 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 von Hausaufgabe 11.1. □

Beispiel 15.34 (strikte Dreiecksmatrizen sind nilpotent)**.**

Für

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 0 & 0 & 4 & 5 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

gilt

$$A^2 = \begin{bmatrix} 0 & 0 & 4 & 17 \\ 0 & 0 & 0 & 24 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{und} \quad A^3 = \begin{bmatrix} 0 & 0 & 0 & 24 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{und} \quad A^4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

△

Lemma 15.35 (obere und untere Dreiecksmatrizen bilden Unterringe)**.**

Es seien $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}$. Dann gilt:

(*i*) $K_{\diagdown}^{n\times n}$, $K_{\diagup}^{n\times n}$ und $K_{\triangle}^{n\times n}$ bilden jeweils einen Unterring mit Eins (Definition 9.10) von $K^{n\times n}$. $K_{\diagdown}^{n\times n}$ ist sogar kommutativ für alle $n \in \mathbb{N}$.

(*ii*) Die strikten oberen und strikten unteren Dreiecksmatrizen bilden einen Unterring (aber keinen Unterring mit Eins) von $K^{n\times n}$. Im Fall $n = 1$ ist das der Nullring.

Beweis. Aussage (*i*): Nach Definition 9.10 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 $K_{\diagup}^{n\times n}$ aus. Sind $A, B \in K_{\diagup}^{n\times n}$, dann ist auch $-B \in K_{\diagup}^{n\times n}$ und damit $A - B \in K_{\diagup}^{n\times n}$. Aus dem Untergruppenkriterium (Satz 7.33) folgt, dass $(K_{\diagup}^{n\times n}, +)$ eine Untergruppe

[12] Quelle: https://en.wikipedia.org/wiki/Nilpotent_matrix#Example_5, genutzt unter der Lizenz CC-BY-SA 4.0

von $(K^{n\times n}, +)$ ist. Da $I_n \in (K^{n\times n}_{\triangleleft}, +)$ klar ist, bleibt nur zu zeigen, dass das Matrix-Produkt $A \cdot B$ von zwei Matrizen $A, B \in K^{n\times n}_{\triangleleft}$ wieder in $K^{n\times n}_{\triangleleft}$ liegt. Für Indizes $1 \leqslant k < i \leqslant n$ gilt

$$\big[A \cdot B\big]_{ik} = \sum_{j=1}^{n} \underbrace{a_{ij}}_{=0 \text{ für } j<i} \overbrace{b_{jk}}^{=0 \text{ für } j>k} = 0,$$

da alle Summanden gleich Null sind, also ist tatsächlich $A \cdot B$ wieder eine obere Dreiecksmatrix.

Aussage (ii): Der Beweis der Unterring-Eigenschaft geht genauso wie in Aussage (i). Da I_n keine strikte Dreiecksmatrix ist, handelt es sich nicht um einen Unterring mit Eins[13] 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 7.16) des Monoids $(K^{n\times n}, \cdot)$.

Definition 15.36 (invertierbare Matrix)**.**
Es seien $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}_0$.

(i) Eine Matrix $A \in K^{n\times n}$ heißt **invertierbar** (englisch: invertible matrix) oder **regulär** (englisch: non-singular matrix), wenn sie ein invertierbares Element (Definition 7.11) des Monoids $(K^{n\times n}, \cdot)$ ist. Das heißt, es gibt eine Matrix $B \in K^{n\times n}$ mit der Eigenschaft

$$A\,B = I \quad \text{und} \quad B\,A = I. \tag{15.29}$$

In diesem Fall heißt B die zu A **inverse Matrix** (englisch: inverse matrix) oder kurz die **Inverse** (englisch: inverse) von A, in Symbolen: $B = A^{-1}$.

(ii) Andernfalls heißt A **nicht invertierbar** (englisch: non-invertible matrix) oder **singulär** (englisch: singular matrix).

(iii) Die Menge der invertierbaren Matrizen in $K^{n\times n}$, also die Einheitengruppe des Monoids $(K^{n\times n}, \cdot)$, heißt die **allgemeine lineare Gruppe** (englisch: general linear group) **vom Grad n über dem Körper K**, in Symbolen

$$\mathrm{GL}(n, K) \coloneqq \big\{A \in K^{n\times n} \,\big|\, A \text{ ist invertierbar}\big\}. \tag{15.30}$$

△

Beachte: B ist Inverse von A genau dann, wenn A Inverse von B ist. Wie in jedem Monoid ist das neutrale Element, also die Einheitsmatrix I, immer invertierbar und selbstinvers.

Beispiel 15.37 (invertierbare Matrix)**.**
Die Matrix

$$A = \begin{bmatrix} 1 & 0 & -7 \\ 2 & 0 & 3 \\ 1 & 1 & 2 \end{bmatrix} \in \mathbb{R}^{3\times 3}$$

[13] Im Fall $n = 1$ besteht der Unterring nur aus der Nullmatrix, ist also der 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 9.10.

ist invertierbar, denn es gilt

$$\begin{bmatrix}1&0&-7\\2&0&3\\1&1&2\end{bmatrix}\frac{1}{17}\begin{bmatrix}3&7&0\\1&-9&17\\-2&1&0\end{bmatrix}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\quad\text{und}\quad\frac{1}{17}\begin{bmatrix}3&7&0\\1&-9&17\\-2&1&0\end{bmatrix}\begin{bmatrix}1&0&-7\\2&0&3\\1&1&2\end{bmatrix}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}.\quad\triangle$$

Satz 15.38 (Rechenregeln für Inverse, vgl. Satz 7.17)**.**
Es seien $(K,+,\cdot)$ 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

$$(A^\mathsf{T})^{-1}=(A^{-1})^\mathsf{T}. \tag{15.34}$$

Aus diesem Grund können wir statt $(A^\mathsf{T})^{-1}$ auch einfach $A^{-\mathsf{T}}$ schreiben.

Beweis. Der Beweis der Eigenschaften Aussagen (*i*) bis (*iii*) geht so wie in Satz 7.17.

Aussage (*iv*): Es sei A invertierbar. Dann gilt

$$A^\mathsf{T}\,(A^{-1})^\mathsf{T}=(A^{-1}A)^\mathsf{T}=\mathrm{id}^\mathsf{T}=\mathrm{id},$$
$$(A^{-1})^\mathsf{T}\,A^\mathsf{T}=(A\,A^{-1})^\mathsf{T}=\mathrm{id}^\mathsf{T}=\mathrm{id},$$

also ist $(A^{-1})^\mathsf{T}$ in der Tat die Inverse zu A^T. □

Anhand der Definition 15.36 kann man die Invertierbarkeit oder Nicht-Invertierbarkeit einer Matrix schlecht erkennen. Stattdessen geben wir nun Kriterien für die Invertierbarkeit an.

Lemma 15.39 (Elementarmatrizen sind invertierbar)**.**
Die Elementarmatrizen aus Definition 15.15 sind invertierbar.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 10.3. □

Für Matrizen in Zeilenstufenform ist die Invertierbarkeit leicht zu erkennen:

Satz 15.40 (Invertierbarkeit von Matrizen durch Zeilenstufenform)**.**
Es seien $(K,+,\cdot)$ 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 15.21). Dann sind äquivalent:

(*i*) A ist invertierbar.

(*ii*) Es gilt $\operatorname{Rang}(A) = n$.

(*iii*) C ist invertierbar.

(*iv*) Es gilt $\operatorname{Rang}(C) = n$.

(*v*) C hat keine Nullzeilen und keine Nullspalten.

Beachte: Eine quadratische Matrix ist also genau dann invertierbar, wenn sie maximalen Rang („**vollen Rang**“) besitzt. Das ist genau dann der Fall, wenn die Menge der Zeilenvektoren linear unabhängig ist und 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*) ⇔ Aussage (*iii*): Da die Elementarmatrizen nach Lemma 15.39 invertierbar sind, ist A genau dann invertierbar, wenn C invertierbar ist. (**Quizfrage 15.5:** Klar?)

Aussage (*ii*) ⇔ Aussage (*iv*): Wie in Lemma 15.16 gezeigt wurde, ändern elementare Zeilenumformungen den Zeilenraum und insbesondere den Rang nicht. Es gilt also $\operatorname{Rang}(A) = \operatorname{Rang}(C)$.

Aussage (*iv*) ⇒ Aussage (*iii*): Im Fall $n = 0$ ist die einzig mögliche Matrix C die leere Matrix, diese hat $\operatorname{Rang}(C) = 0$ und ist selbstinvers.

Für den Rest des Beweisschrittes betrachten wir nun $n \in \mathbb{N}$. $\operatorname{Rang}(C) = n$ bedeutet, dass die Zeilenstufenform von C die Gestalt

$$\begin{bmatrix} \star & ? & ? \\ 0 & & ? \\ 0 & 0 & \star \end{bmatrix}$$

besitzt, vgl. Beispiel 15.19. Dabei sind die Pivot-Elemente $\star \in K \setminus \{0\}$. Durch die Multiplikation $\widehat{C} := D\,C$ mit der Diagonalmatrix D bestehend aus den multiplikativen Inversen der Pivot-Elemente können wir erreichen, dass die Pivot-Elemente in $\widehat{C}$ alle gleich 1 sind.

$\widehat{C}$ ist also nun von der Form $\widehat{C} = I + N$ mit einer strikten oberen Dreiecksmatrix N. Wir rechnen nach, dass die Inverse von $\widehat{C}$ gegeben ist durch

$$\widehat{C}^{-1} = \sum_{k=0}^{n} (-N)^k.$$

Es gilt nämlich

$$\begin{aligned} \widehat{C} \sum_{k=0}^{n} (-N)^k = \sum_{k=0}^{n} \widehat{C}\,(-N)^k = \sum_{k=0}^{n} (I+N)\,(-N)^k = \sum_{k=0}^{n} (-N)^k - \sum_{k=1}^{n+1} (-N)^k \\ = (-N)^0 - (-N)^{n+1} = I - 0 = I. \end{aligned}$$

Die letzte Gleichheit gilt aufgrund von Lemma 15.33. Ganz ähnlich können wir auch zeigen:

$$\begin{aligned}\Big(\sum_{k=0}^{n}(-N)^k\Big)\,\widehat{C} &= \sum_{k=0}^{n}(-N)^k\,\widehat{C} = \sum_{k=0}^{n}(-N)^k\,(I+N) = \sum_{k=0}^{n}(-N)^k - \sum_{k=1}^{n+1}(-N)^k \\ &= (-N)^0 - (-N)^{n+1} = I - 0 = I.\end{aligned}$$

Tatsächlich ist also $\widehat{C}$ invertierbar und besitzt die angegebene Inverse. Damit ist auch $C = D^{-1}\widehat{C}$ invertierbar.

Aussage (iv) $\Leftrightarrow$ Aussage (v): Wir wissen: $\operatorname{Rang}(C)$ ist die Anzahl der Pivot-Elemente von C. Da C eine $n \times n$-Matrix ist, gilt:

$$\begin{aligned}&\operatorname{Rang}(C) = n \\ \Leftrightarrow\quad &C \text{ hat } n \text{ Pivot-Elemente} \\ \Leftrightarrow\quad &\text{die Hauptdiagonale von } C \text{ hat keine Nullen} \\ \Leftrightarrow\quad &C \text{ hat keine Nullzeilen und keine Nullspalten.}\end{aligned}$$

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 15.41 (Multiplikation mit invertierbaren Matrizen ändert den Rang nicht)**.**
Es seien $(K, +, \cdot)$ 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:

$$\operatorname{Rang}(B\,A\,C) = \operatorname{Rang}(A). \tag{15.35}$$

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 11.1. □

Abschließend zeigen wir, dass es für den Nachweis, dass zwei $n \times n$-Matrizen Inverse voneinander sind, ausreichend ist, diese in einer der beiden Reihenfolgen miteinander zu multiplizieren. Mit anderen Worten, jede Rechtsinverse einer quadratischen Matrix ist auch eine Linksinverse (und damit die eindeutige Inverse) und umgekehrt. In einer *Gruppe* kennen wir diese Eigenschaft bereits aus Satz 7.17 Aussage (ii). Allerdings bildet ja $(K^{n\times n}, \cdot)$ i. A. lediglich eine (nicht-kommutative) Halbgruppe, und dort gilt diese Eigenschaft i. A. nicht (Hausaufgabe 4.2). Es ist also bemerkenswert, dass die (für $n \geqslant 2$ nicht-kommutative) Halbgruppe $(K^{n\times n}, \cdot)$ die Eigenschaft „Rechtsinverse sind Linksinverse und umgekehrt“ besitzt.

Satz 15.42 (Rechtsinverse quadratischer Matrizen sind Linksinverse und umgekehrt)**.**
Es seien $(K, +, \cdot)$ 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

$n = \operatorname{Rang}(I_n)$	denn I_n ist invertierbar und hat daher vollen Rang nach Satz 15.40
$= \operatorname{Rang}(A\,B)$	$I_n = A\,B$ nach Voraussetzung
$\leqslant \min\{\operatorname{Rang}(A),\ \operatorname{Rang}(B)\}$	nach Satz 15.14 (Rang des Produkts von Matrizen)
$\leqslant n$	nach Satz 15.12 (Rang ist beschränkt durch die Dimensionen).

Es muss also überall Gleichheit gelten, insbesondere ist $\operatorname{Rang}(A) = \operatorname{Rang}(B) = n$, und nach Satz 15.40 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 22

§ 16 Lineare Gleichungssysteme

Literatur: Fischer, Springborn, 2020, Kapitel 1.4 und 3.3, Bosch, 2014, Kapitel 3.5, Beutelspacher, 2014, Kapitel 4.1, Deiser, 2022b, 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 $(K, +, \cdot)$ ein Körper, $m, n \in \mathbb{N}_0$ und $A \in K^{n\times m}$.

(i) Eine Gleichung der Form $A\,x = b$ mit dem unbekannten Koeffizientenvektor $x \in \mathbb{K}^m$ heißt ein **lineares Gleichungssystem** (englisch: linear system of equations). 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).

(ii) Die Matrix $[A, b] \in K^{n\times(m+1)}$ heißt die **erweiterte Koeffizientenmatrix** (englisch: augmented coefficient matrix).

(iii) Das lineare Gleichungssystem $A\,x = b$ heißt **homogen** (englisch: homogeneous), wenn $b = 0 \in K^m$ ist, andernfalls **nichthomogen** (englisch: non-homogeneous) oder **inhomogen** (englisch: inhomogeneous).

(iv) Das lineare Gleichungssystem $A\,x = b$ heißt **lösbar** (englisch: solvable), wenn es ein $x_0 \in K^m$ gibt, das $A\,x_0 = b$ 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):

$$\left.\begin{array}{rcrcrcr} 6x_1 & + & 1x_2 & + & 1x_3 & = & 11 \\ 3x_1 & + & 3x_2 & + & 1x_3 & = & 5 \\ -6x_1 & - & 6x_2 & - & 3x_3 & = & -9 \end{array}\right\} \quad \Leftrightarrow \quad \underbrace{\begin{bmatrix} 6 & 1 & 1 \\ 3 & 3 & 1 \\ -6 & -6 & -3 \end{bmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}_{x} = \underbrace{\begin{pmatrix} 11 \\ 5 \\ -9 \end{pmatrix}}_{b}.$$

(*ii*) Gesucht ist ein Polynom $p = c_0 + c_1 t + c_2 t^2 \in \mathbb{Z}_5[t]$, dessen zugehörige Polynomfunktion $\widetilde{p}$ folgende Bedingungen erfüllt:

$$\widetilde{p}(0) = 3, \quad \widetilde{p}(1) = 7, \quad \widetilde{p}(3) = 4$$

Das ist ein Beispiel einer **Interpolationsaufgabe**[14] (englisch: interpolation problem). Durch Einsetzen der drei **Interpolationsbedingungen** in die Polynomfunktion erhalten wir das lineare Gleichungssystem

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 3 & 4 \end{bmatrix}}_{A} \underbrace{\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix}}_{c} = \underbrace{\begin{pmatrix} 3 \\ 7 \\ 4 \end{pmatrix}}_{b}$$

für den gesuchten Koeffizientenvektor $c = (c_0, c_1, c_2)^\mathsf{T}$. △

Beachte: Jede Spalte der Matrix gehört zu einer der Variablen $x_1, \ldots, x_m$. Jede Zeile der Matrix gehört zu einer Gleichung.

Unser Ziel ist es, *alle* Lösungen von $Ax = b$ zu bestimmen, also die gesamte **Lösungsmenge** (englisch: solution set)

$$\mathcal{L}(A, b) := \{x \in K^m \mid Ax = b\}. \tag{16.1}$$

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 $(K, +, \cdot)$ 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**“) (englisch: particular solution) **Lösung** von $Ax = b$, dann gilt

$$\mathcal{L}(A, b) = x_0 + \mathcal{L}(A, 0). \tag{16.2}$$

Beachte: Die Lösungsmenge eines allgemeinen Systems $Ax = b$ ergibt sich aus einer partikulären Lösung plus der Lösungsmenge des zugehörigen homogenen Systems.

(*iii*) Die folgenden Aussagen sind äquivalent:

(a) $Ax = b$ ist lösbar.
(b) $b \in \operatorname{SR}(A)$.
(c) $\operatorname{Rang}(A) = \operatorname{Rang}([A, b])$.

[14] lateinisch: interpolare: neu herrichten, auffrischen

(*iv*) Die folgenden Aussagen sind äquivalent:

(a) $A\,x = b$ ist eindeutig lösbar.
(b) $\mathrm{Rang}(A) = \mathrm{Rang}([A, b]) = m$.

(*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. Aussage (*i*): Das Unterraumkriterium (Satz 12.8) zeigt, dass $\mathcal{L}(A, 0)$ ein Unterraum von K^m ist, 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

$$A\,(\alpha\,x + \beta\,y) = A\,(\alpha\,x) + A\,(\beta\,y) = \alpha\,A\,x + \beta\,A\,y = 0.$$

Wir bestätigen nun $\dim(\mathcal{L}(A, 0)) = m - \mathrm{Rang}(A)$, indem wir eine Basis dieses Unterraumes angeben. 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 $A\,x = 0 \Leftrightarrow \widehat{C}\,x = E_k \cdots E_2\,E_1\,0 = 0$, also $\mathcal{L}(A, 0) = \mathcal{L}(\widehat{C}, 0)$. Zur Abkürzung setzen wir $r := \mathrm{Rang}(A) = \mathrm{Rang}(\widehat{C})$, $0 \leqslant r \leqslant \min\{m, n\}$. 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 $\mathcal{L}(A, 0) = \mathcal{L}(\widehat{C}, 0) = \mathcal{L}(C, 0)$.

Wir bezeichnen mit $\mathcal{A} := (j_1, \ldots, j_r)$ die Familie der Pivot-Spalten und mit $\mathcal{I}$ die komplementäre Familie der Nicht-Pivot-Spalten mit $\#\mathcal{I} = m - r$. Wir können jeden Vektor $x \in K^m$ in zwei Teilvektoren $x_{\mathcal{A}} \in K^r$ und $x_{\mathcal{I}} \in K^{m-r}$ partitionieren. Dies geschieht durch Einführung der beiden Matrizen

$$\Pi_{\mathcal{A}} := (e_j^{\mathsf{T}})_{j\in\mathcal{A}} \quad \text{und} \quad \Pi_{\mathcal{I}} := (e_j^{\mathsf{T}})_{j\in\mathcal{I}},$$

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

$$C\,x = C\,\Pi_{\mathcal{A}}^{\mathsf{T}} x_{\mathcal{A}} + C\,\Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}}$$

schreiben können, wobei die Matrix $C\,\Pi_{\mathcal{A}}^{\mathsf{T}} = [a_{\bullet j_1}, \ldots, a_{\bullet j_r}]$ aus den Pivot-Spalten von C besteht und damit eine invertierbare obere Dreiecksmatrix (Satz 15.40) der Dimension $r \times r$ darstellt. Wir können also jede Lösung von $C\,x = 0$ in der Form

$$x_{\mathcal{A}} = -\big(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\big)^{-1} C\,\Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}}$$

schreiben, 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 mit

$$x = -\Pi_{\mathcal{A}}^{\mathsf{T}}\big(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\big)^{-1} C\,\Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}} + \Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}} = \big[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}}\big(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\big)^{-1} C\big]\,\Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}}$$

mit beliebigem $x_I \in K^{m-r}$ genau die Lösungen von $C\,x = 0$. Da die Spalten der Einheitsmatrix I_{m-r} eine Basis von K^{m-r} bilden, sind die Spalten der Matrix

$$\left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}}\left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\right)^{-1}C\right]\Pi_I^{\mathsf{T}} \in K^{n\times(m-r)}$$

eine Basis von $\mathcal{L}(C,0) = \mathcal{L}(A,0)$, und die Kardinalität der Basis ist $m-r$. In der Tat können wir auch

$$C\left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}}\left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\right)^{-1}C\right]\Pi_I^{\mathsf{T}} = \left[C - C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\right)^{-1}C\right]\Pi_I^{\mathsf{T}} = 0 \in K^{r\times(m-r)}$$

hier nochmal bestätigen.

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 (16.3) 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 $A\,x = b$ eindeutig lösbar. Nach Aussage (iv) folgt, dass $\mathrm{Rang}(A) = \mathrm{Rang}([A,b]) = n$ gilt. $\mathrm{Rang}(A) = n$ impliziert nach Satz 15.40 aber, dass A invertierbar ist.

Aussage (c) $\Rightarrow$ Aussage (b): Wenn A invertierbar ist, dann ist $A\,x = c$ äquivalent zu $A^{-1}A\,x = x = A^{-1}c$. Also ist $A\,x = c$ 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 15.19). Die Zeilenstufenform von A habe die Gestalt

$$\widehat{C} = \begin{bmatrix} \boxed{\star} & ? & ? & ? \\ 0 & 0 & \boxed{\star} & ? \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{und nach Streichen von Nullenzeilen} \quad C = \begin{bmatrix} \boxed{\star} & ? & ? & ? \\ 0 & 0 & \boxed{\star} & ? \end{bmatrix}.$$

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

$$\begin{aligned} x &= \Pi_{\mathcal{A}}^{\mathsf{T}} \, x_{\mathcal{A}} + \Pi_{\mathcal{I}}^{\mathsf{T}} \, x_{\mathcal{I}} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_3 \end{pmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} x_2 \\ x_4 \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} x_1 \\ 0 \\ x_3 \\ 0 \end{pmatrix}}_{\text{abhängige Variable}} + \underbrace{\begin{pmatrix} 0 \\ x_2 \\ 0 \\ x_4 \end{pmatrix}}_{\text{unabhängige Variable}} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}. \end{aligned}$$

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

$$\begin{bmatrix} \boxed{\star} & ? \\ 0 & \boxed{\star} \end{bmatrix}$$

einer invertierbaren oberen $r \times r$-Dreiecksmatrix.

Wir halten fest, dass die kompliziert aussehende Darstellung

$$\left[I_m - \Pi_{\mathcal{A}}^{\mathsf{T}} \left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}} \right)^{-1} C \right] \Pi_{\mathcal{I}}^{\mathsf{T}} \in K^{n \times (m-r)} \tag{16.3}$$

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 mit Hilfe der Gleichung

$$\left(C\,\Pi_{\mathcal{A}}^{\mathsf{T}}\right) x_{\mathcal{A}} = \underbrace{-\,C\,\Pi_{\mathcal{I}}^{\mathsf{T}} x_{\mathcal{I}}}_{\text{genau eine der } \mathcal{I}\text{-Spalten von } C} \tag{16.4}$$

aus. Weil $C\,\Pi_{\mathcal{A}}^{\mathsf{T}}$ eine obere Dreiecksmatrix ist, können wir die Werte der abhängigen Variablen 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 16.7.

(*ii*) Die Dimension des Lösungsraumes $\dim(\mathcal{L}(A, 0)) = m - \mathrm{Rang}(A)$ sollten wir uns merken in der Form „Anzahl der Variablen (m) minus Anzahl der wesentlichen (sprich: linear unabhängigen) Gleichungen ($\mathrm{Rang}(A)$) 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 $m - \mathrm{Rang}(A) \geqslant 1$.[15]
(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? Das Vorgehen ist wie folgt:

(1) Wir bringen die erweiterte Koeffizientenmatrix $[A, b]$ zunächst in Zeilenstufenform. Hier 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.[16]

Definition 16.5 (reduzierte Zeilenstufenform, vgl. Definition 15.17)**.**

Eine Matrix $A \in K^{n\times m}$ heißt in **reduzierter Zeilenstufenform** (englisch: reduced row echelon form), wenn sie in Zeilenstufenform ist (Definition 15.17) 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.

[15] 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 $\#\mathcal{L}(A, b) = (\#K)^{m-\mathrm{Rang}(A)}$.

[16] 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 (16.4) — die Werte der abhängigen Variablen ergeben, nicht nur eine obere Dreiecksmatrix, sondern die Einheitsmatrix ist, sodass wir die Werte direkt ablesen können.

Beispiel 16.6 (reduzierte Zeilenstufenform, vgl. Beispiel 15.19)**.**
Hier sind die Besetzungsmuster einiger 3×4-Matrizen in reduzierter Zeilenstufenform, wobei ? für einen beliebigen Eintrag aus dem Körper K steht. Die Zahl r gibt wieder den Rang der Matrix an.

$$\begin{array}{l} j_1 = 1 \to \\ j_2 = 2 \to \\ j_3 = 3 \to \end{array}\begin{bmatrix} 1 & 0 & 0 & ? \\ 0 & 1 & 0 & ? \\ 0 & 0 & 1 & ? \end{bmatrix} \quad \begin{array}{l} j_1 = 1 \to \\ j_2 = 3 \to \end{array}\begin{bmatrix} 1 & ? & 0 & ? \\ 0 & 0 & 1 & ? \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{array}{l} j_1 = 3 \to \\ j_2 = 4 \to \end{array}\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$
$$r = 3 \qquad r = 2 \qquad r = 2$$

△

Wir geben nun anhand von Beispielen die Bestimmung der reduzierten Zeilenstufenform erweiterter Koeffizientenmatrizen $[A, b]$ an und wie wir daraus die Lösungsmenge des linearen Gleichungssystems $Ax = b$ ablesen können. Dabei kommen alle drei Fälle (eindeutige Lösbarkeit, nicht-eindeutige Lösbarkeit und Nicht-Lösbarkeit) vor.

Beispiel 16.7 (Lösungsverfahren für lineare Gleichungssysteme)**.**
Wir betrachten drei lineare Gleichungssysteme über dem endlichen Körper $(\mathbb{Z}_5, +_5, \cdot_5)$, vgl. Folgerung 10.6. 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

$$\left[\begin{array}{cccc} 0 & 0 & 2 & 1 \\ 1 & 3 & 0 & 2 \\ 3 & 2 & 2 & 2 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{array}\right]$$ Tauschen der Zeilen 1 und 2

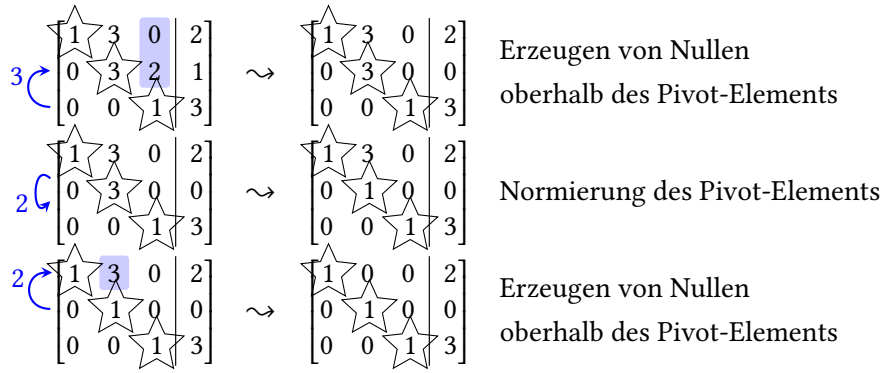
$$\left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 3 & 2 & 2 & 2 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 3 & 2 & 1 \end{array}\right]$$ Erzeugen von Nullen unterhalb des Pivot-Elements

$$\left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 3 & 2 & 1 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 \end{array}\right]$$ Tauschen der Zeilen 2 und 3

$$\left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 \end{array}\right]$$ Erzeugen von Nullen unterhalb des Pivot-Elements

An dieser Stelle ist eine Zeilenstufenform hergestellt. Wir erkennen $\mathrm{Rang}(A) = \mathrm{Rang}([A, b]) = 3 = m$, also ist das System eindeutig lösbar. Wir gehen weiter zur reduzierten Zeilenstufenform:

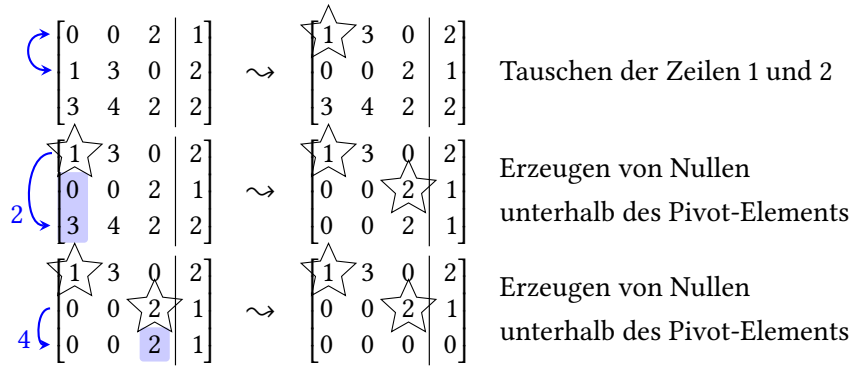
$$\left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 2 & 1 \end{array}\right] \rightsquigarrow \left[\begin{array}{cccc} 1 & 3 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 0 & 0 & 1 & 3 \end{array}\right]$$ Normierung des Pivot-Elements



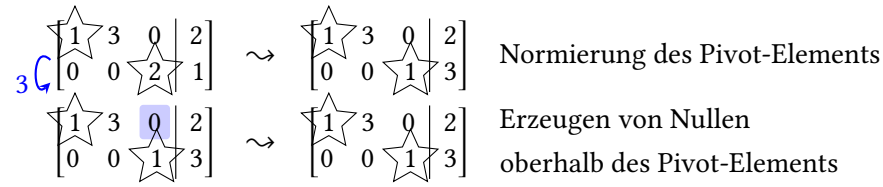
Wir haben in diesem Fall also die abhängigen Indizes $\mathcal{A} = (1, 2, 3)$ und keinen unabhängigen Index, also die leere Familie $\mathcal{I} = ()$. Hier können wir nun die eindeutige Lösung ablesen, nämlich $x = (2, 0, 3)^\mathsf{T}$. Wir führen die Probe durch:

$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 3 & 0 \\ 3 & 2 & 2 \end{bmatrix} \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}.$$

(*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

$$\left[\begin{array}{ccc|c} 1 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

erhalten wir nach Bemerkung 16.4 dadurch, dass wir für die unabhängigen Variablen (hier nur x_2) einen der Einheitsvektoren 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

$$\left[\begin{array}{ccc|c} 0 & 0 & 2 & 1 \\ 1 & 3 & 0 & 2 \\ 3 & 4 & 2 & 3 \end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 3 & 4 & 2 & 3 \end{array}\right] \quad \text{Tauschen der Zeilen 1 und 2}$$

$$\left[\begin{array}{ccc|c} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 3 & 4 & 2 & 3 \end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 2 & 2 \end{array}\right] \quad \begin{array}{l} \text{Erzeugen von Nullen} \\ \text{unterhalb des Pivot-Elements} \end{array}$$

$$\left[\begin{array}{ccc|c} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 2 & 2 \end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c} 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right] \quad \begin{array}{l} \text{Erzeugen von Nullen} \\ \text{unterhalb des Pivot-Elements} \end{array}$$

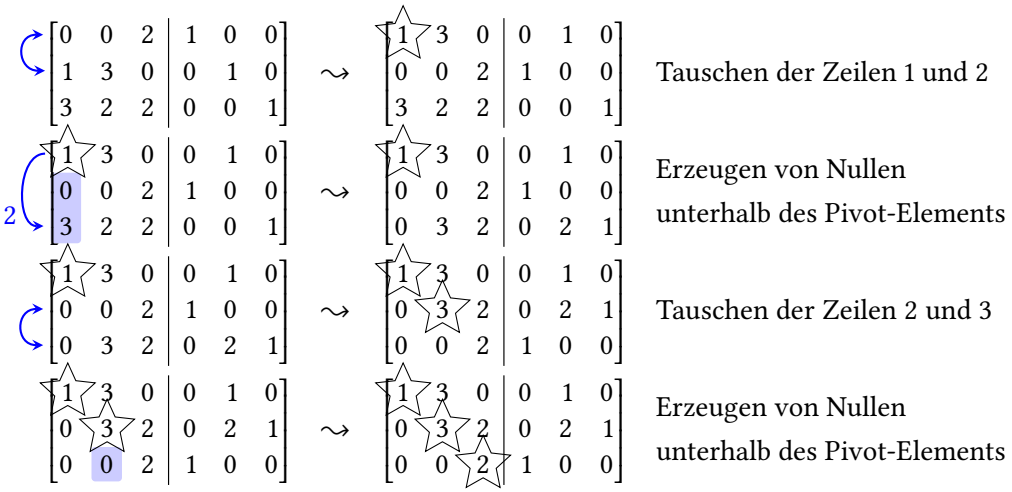
An dieser Stelle ist eine Zeilenstufenform hergestellt. Wir erkennen nun $\mathrm{Rang}(A) = 2$, aber $\mathrm{Rang}([A, b]) = 3$. Das heißt, das System ist nicht lösbar, vgl. Satz 16.3. △

Abschließend bemerken wir, dass wir mit Hilfe der Transformation in reduzierte Zeilenstufenform nicht nur ein einzelnes lineares Gleichungssystem $A\,x = b$ lösen können, sondern mehrere Systeme gleichzeitig, solange diese sich nur in der rechten Seite unterscheiden. Haben wir $k \in \mathbb{N}_0$ rechte

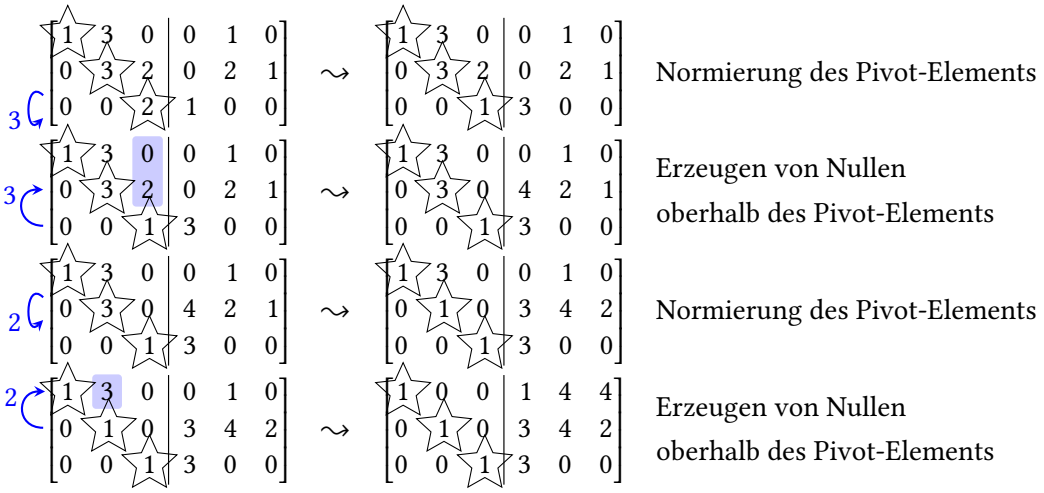
Seiten, so schreiben wir diese spaltenweise als $n \times k$-Matrix B. Das System für die k unbekannten Spaltenvektoren in der $n \times k$-Matrix X lautet dann $AX = B$. Die Transformation auf Zeilenstufenform geschieht einfach für alle Spalten der erweiterten Koeffizientenmatrix $[A, B]$ gleichzeitig. 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 16.8 (Berechnung der inversen Matrix)**.**
Wir führen die Berechnung der inversen Matrix für die erste Matrix aus Beispiel 16.7 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 $\mathrm{Rang}(A) = \mathrm{Rang}([A, b]) = 3 = m$ 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 23

Ende der Woche 11

§ 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, 2022b, 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 8.1 eines Halbgruppenhomomorphismus)**.**

Es seien $(K, +, \cdot)$ ein Körper und $(V, +_1, \cdot_1)$, $(W, +_2, \cdot_2)$ zwei Vektorräume über K.

(*i*) Eine Abbildung $f\colon V \to W$ heißt **strukturverträglich** oder ein **(Vektorraum-)Homomorphismus** (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*) Wie in Definition 8.1 sprechen wir im Fall $(V, +_1, \cdot_1) = (W, +_2, \cdot_2)$ von einem **(Vektorraum-)Endomorphismus** (englisch: vector space endomorphism) oder einem **linearen Endomorphismus** (englisch: linear endomorphism).

(*iii*) Ist $f\colon V \to W$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **(Vektorraum-)Isomorphismus** (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*) Im Fall $(V, +_1, \cdot_1) = (W, +_2, \cdot_2)$ und $f\colon V \to W$ bijektiv sprechen wir auch von einem **(Vektorraum-)Automorphismus** (englisch: vector space automorphism) oder einem **linearen Automorphismus** (englisch: linear automorphism).

(*v*) Das **Bild** (englisch: image) und der **Kern** (englisch: kernel, null space[17]) eines Vektorraumhomomorphismus $f\colon V \to W$ sind definiert als

$$\operatorname{Bild}(f) := \left\{ f(u) \in W \,\middle|\, u \in V \right\} = f(V), \tag{17.2}$$

$$\operatorname{Kern}(f) := \left\{ u \in V \,\middle|\, f(u) = 0_W \right\} = f^{-1}(\{0_W\}). \tag{17.3}$$

△

Bemerkung 17.2 (zu Definition 17.1)**.**

(*i*) Die Vektorräume $(V, +_1)$ und $(W, +_2)$ sind insbesondere (abelsche) Gruppen. 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 zu notieren. △

Beispiel 17.3 (Vektorraumhomomorphismus)**.**

(*i*) Die Vektorräume K_n und K^n über einem Körper K sind zueinander isomorph. Die Abbildung

$$\cdot^{\mathsf{T}}\colon K_n \ni x \mapsto u^{\mathsf{T}} \in K^n$$

ist ein linearer Isomorphismus, vgl. (15.25a) und (15.25b). (**Quizfrage 17.1:** Wie sieht der inverse Vektorraumisomorphismus aus?)

(*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

$$\pi_i\colon K^n \ni x \mapsto x_i \in K \tag{17.4}$$

für $1 \leqslant i \leqslant n \in \mathbb{N}$, eine surjektive lineare Abbildung. (**Quizfrage 17.3:** Ist sie auch injektiv?)

(*iv*) Die Grenzwert-Abbildung, definiert beispielsweise auf dem Vektorraum der konvergenten $\mathbb{R}$-wertigen Folgen $(\mathbb{R}^{\mathbb{N}})_c$ (siehe Beispiel 12.9) nach $\mathbb{R}$, also

$$\lim\colon (\mathbb{R}^{\mathbb{N}})_c \ni (y_i)_{i\in\mathbb{N}_0} \mapsto \lim_{i\to\infty}(y_i) \in \mathbb{R}$$

ist eine surjektive lineare Abbildung. (**Quizfrage 17.4:** Ist sie auch injektiv?)

[17] nicht zu verwechseln mit dem Begriff *zero vector space* (Nullraum) $\{0\}$, siehe Beispiel 12.3

(v) 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?)

(vi) Für eine Matrix $A \in K^{n \times m}$ über einem Körper K ist die Matrix-Vektor-Multiplikation mit A

$$f_A \colon K^m \ni x \mapsto f_A(x) \coloneqq A\,x \in K^n \tag{17.5}$$

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. △

Lemma 17.4 (Komposition linearer Abbildungen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(U, +, \cdot)$, $(V, +, \cdot)$, $(W, +, \cdot)$ Vektorräume über K. Sind $f \colon V \to W$ und $g \colon U \to V$ lineare Abbildungen, dann ist auch $f \circ g \colon U \to W$ eine lineare Abbildung.

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 12.1. □

Als Folgerung ergibt sich (wie auch bereits bei Halbgruppen, Monoiden, Gruppen, Ringen und Körpern), dass Isomorphie eine Äquivalenzrelation auf der Klasse aller Vektorräume über demselben Körper K ist.

Lemma 17.5 (Eigenschaften linearer Abbildungen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K. Weiter sei $f \colon V \to W$ eine lineare Abbildung.

(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 $v_i \in V$.

(iv) Ist $E \subseteq V$, dann gilt $f\big(\langle E \rangle\big) = \big\langle f(E) \big\rangle$.

(v) Ist $F = (v_i)_{i \in I}$ eine Familie von Vektoren in V, dann gilt $f\big(\langle F \rangle\big) = \big\langle f(F) \big\rangle$.

(vi) Ist $U \subseteq V$ ein Unterraum, dann ist $f(U) \subseteq W$ ein Unterraum.

(vii) Ist $Z \subseteq W$ ein Unterraum, dann ist $f^{-1}(Z) \subseteq V$ 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.

(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.

Beweis. Aussage (*i*) und Aussage (*ii*) folgen sofort aus Lemma 8.5.

Aussage (*iii*):

$$f\Big(\sum_{i=1}^{n} \alpha_i\, v_i\Big) = \sum_{i=1}^{n} f(\alpha_i\, v_i) \quad \text{durch wiederholte Anwendung von (17.1a)}$$
$$= \sum_{i=1}^{n} \alpha_i\, f(v_i) \quad \text{durch Anwendung von (17.1b) auf jeden Summanden}$$

Aussage (*iv*): Nach Satz 12.13 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 12.13 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 12.8). 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 12.8). 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 $v_1, \dots, v_n \in M$ sowie Koeffizienten $\alpha_1, \dots, \alpha_n \in K$, 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 $(f(v_i))_{i\in I}$. □

Lemma 17.6 (Kern und Bild linearer Abbildungen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K sowie $f\colon V \to W$ eine lineare Abbildung.

(*i*) Bild(f) ist ein Unterraum von W.

(*ii*) f ist surjektiv genau dann, wenn Bild(f) = W gilt.

(*iii*) Kern(f) ist ein Unterraum von V.

(*iv*) f ist injektiv genau dann, wenn Kern(f) = $\{0\}$ gilt.

Beweis. Aussage (*i*): V ist selbst ein Unterraum von V, daher ist Bild(f) = $f(V)$ nach Lemma 17.5 (*vi*) ein Unterraum von W.

Aussage (*ii*): Die Aussage folgt sofort aus der Definition von Bild(f) = $f(V)$.

Aussage (*iii*): $\{0\}$ ist ein Unterraum von W, daher ist Kern(f) = $f^{-1}(\{0\})$ nach Lemma 17.5 (*vii*) ein Unterraum von V.

Aussage (*iv*): Weder der Begriff der Injektivität noch die Definition von 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. Die Aussage (*iv*) folgt daher aus Lemma 8.9. □

§ 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. Zu diesem Zweck bietet es sich an, mit **indizierten Basen** (englisch: indexed basis) zu arbeiten, um eine „Nummerierung“ der Basisvektoren zu erhalten. Das heißt, dass wir von nun an bevorzugt mit Basen in Form von *Familien* von Vektoren (Definition 6.29) arbeiten anstatt mit Mengen von Vektoren. Ist die Indexmenge I dabei eine Teilmenge von $\mathbb{N}_0$, so sprechen wir auch von einer **geordneten Basis** (englisch: ordered basis).

Satz 17.7 (Existenz- und Eindeutigkeitssatz für Vektorraumhomomorphismen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über 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 $(v_i)_{i\in I}$ linear unabhängig, dann gibt es eine lineare Abbildung $f\colon V \to W$ mit der Eigenschaft $f(v_i) = w_i$ für alle $i \in I$.[18]

(*ii*) 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) Bild(f) = $\langle (w_i)_{i\in I} \rangle$.

(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.

Beweis. Wir beweisen zunächst die Aussage (*ii*).

[18] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

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 13.10 auf (bis auf Nullkoeffizienten) eindeutige Art und Weise als Linearkombination $v = \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}$ geschrieben werden. Daher ist die Setzung

$$f(v) \coloneqq \sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell}$$

wohldefiniert. (**Quizfrage 17.6:** Warum ist die Eindeutigkeit der Darstellung von v bis auf Nullkoeffizienten für die Wohldefiniertheit schon ausreichend?)

Wegen $v_i = 1 \cdot v_i$ gilt

$$f(v_i) = f(1 \cdot v_i) = 1\, w_i = w_i$$

erfüllt f die Bedingung $f(v_i) = w_i$.

Schritt 2: Wir zeigen: Die so definierte Abbildung $f\colon V \to W$ ist linear.

Sind $v = \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}$ und $u = \sum_{k=1}^{m} \beta_k\, v_{j_k}$ zwei beliebige Vektoren aus V, dann können wir durch Hinzufügen von Nullkoeffizienten erreichen, dass beide Darstellungen dieselben endlich vielen Indizes aus I verwenden, also $v = \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}$ und $u = \sum_{\ell=1}^{n} \beta_\ell\, v_{i_\ell}$. Es gilt

$$\begin{aligned}
f(v+u) &= f\Big(\sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell} + \sum_{\ell=1}^{n} \beta_\ell\, v_{i_\ell}\Big) && \text{nach Darstellung von } v \text{ und } u \\
&= f\Big(\sum_{\ell=1}^{n} (\alpha_\ell + \beta_\ell)\, v_{i_\ell}\Big) && \text{nach Distributivgesetz (12.1b) und Kommutativität} \\
&= \sum_{\ell=1}^{n} (\alpha_\ell + \beta_\ell)\, w_{i_\ell} && \text{nach Definition von } f \\
&= \sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell} + \sum_{\ell=1}^{n} \beta_\ell\, w_{i_\ell} && \text{nach Distributivgesetz (12.1b)} \\
&= f(v) + f(u) && \text{nach Definition von } f
\end{aligned}$$

und außerdem für $\alpha \in K$

$$\begin{aligned}
f(\alpha\, v) &= f\Big(\alpha \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}\Big) && \text{nach Darstellung von } v \\
&= f\Big(\sum_{\ell=1}^{n} (\alpha\, \alpha_\ell)\, v_{i_\ell}\Big) && \text{nach Distributivgesetz (12.1a)} \\
&= \sum_{\ell=1}^{n} (\alpha\, \alpha_\ell)\, w_{i_\ell} && \text{nach Definition von } f \\
&= \alpha \sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell} && \text{nach Distributivgesetz (12.1a)} \\
&= \alpha\, f(v) && \text{nach Definition von } f.
\end{aligned}$$

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 $v = \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}$, dann gilt

$$\begin{aligned} g(v) &= g\Big(\sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}\Big) && \text{wegen der Darstellung von } v \\ &= \sum_{\ell=1}^{n} \alpha_\ell\, g(v_{i_\ell}) && \text{wegen der Linearität von } g \\ &= \sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell} && \text{wegen der Eigenschaft } g(v_i) = w_i \\ &= f(v) && \text{nach Definition von } f. \end{aligned}$$

Also muss g notwendig mit f übereinstimmen.

Wir kommen zu den weiteren Eigenschaften der Abbildung f.

Aussage (a): Es gilt

$$\begin{aligned} \operatorname{Bild}(f) &= f(V) && \text{nach Definition von Bild}(f) \\ &= f\big(\langle (v_i)_{i\in I}\rangle\big) && \text{denn } (v_i)_{i\in I} \text{ ist eine Basis von } V \\ &= \big\langle (f(v_i))_{i\in I}\big\rangle && \text{nach Lemma 17.5 } (v) \\ &= \langle (w_i)_{i\in I}\rangle. \end{aligned}$$

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 $(w_i)_{i\in I}$ linear abhängig, 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: $\sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell} = 0$ gilt. Dann ist $v := \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}$ nicht der Nullvektor in V, da $(v_i)_{i\in I}$ eine Basis von V ist, jedoch gilt

$$f(v) = f\Big(\sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}\Big) = \sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell} = 0.$$

Das bedeutet, dass v und der Nullvektor durch f beide auf den Nullvektor in W abgebildet werden, 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 $v = \sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}$, und es gilt

$$0 = f(v) = f\Big(\sum_{\ell=1}^{n} \alpha_\ell\, v_{i_\ell}\Big) = \sum_{\ell=1}^{n} \alpha_\ell\, w_{i_\ell}.$$

Aufgrund der lineare Unabhängigkeit der Familie $(w_i)_{i\in I}$ ist das nur möglich, wenn alle $\alpha_\ell = 0$ sind, also nur dann, wenn $v = 0$ ist. Mit anderen Worten, $\operatorname{Kern}(f) = \{0\}$, und nach Lemma 17.6 (iv) ist f injektiv.

Aussage (d) folgt sofort aus Aussage (b) und Aussage (c).

Nun kommen wir zur Aussage (i). Es sei also $(v_i)_{i\in I}$ linear unabhängig. Wir nutzen den Basisergänzungssatz 13.11 (der im Fall, dass V unendlich-dimensional ist, das Zornsche Lemma und damit das Auswahlaxiom verwendet) und ergänzen die Menge zu einer Basis $(v_i)_{i\in \widehat{I}}$ von V. Wir wählen die

fehlenden $(w_i)_{\widehat{I}\setminus I}$ 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 17.8 (Konstruktion linearer Abbildungen)**.**

(i) Es sei K ein Körper und V ein Vektorraum über 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. 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

$$A := \begin{bmatrix} | & & | \\ f(e_1) & \cdots & f(e_m) \\ | & & | \end{bmatrix}$$

ein, so gilt

$$f(x) = f\Big(\sum_{j=1}^{m} x_j\, e_j\Big) = \sum_{j=1}^{m} x_j f(e_j) = A\,x.$$

Eine lineare Abbildung $K^m \to K^n$ kann also durch Matrix-Vektor-Produkte $x \mapsto A\,x$ realisiert werden.

(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 fest, und zwar eine Drehung um den Winkel 30° im mathematisch positiven Sinn (gegen den Uhrzeigersinn) um den Ursprung. Allgemeiner beschreibt

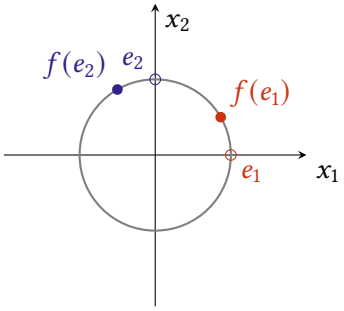
$$f(e_1) = \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix}$$

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 17.7 (ii) bijektiv, also ein Isomorphismus $\mathbb{R}^2 \to \mathbb{R}^2$.

Die Drehabbildung kann 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 fest, und zwar eine Spiegelung an der x_1-Achse. Allgemeiner beschreibt

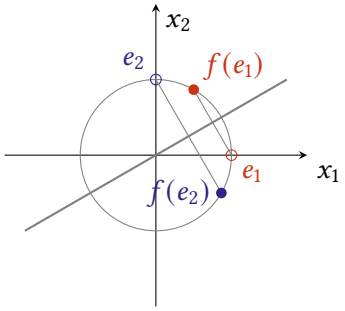
$$f(e_1) = \begin{pmatrix} \cos^2(\alpha) - \sin^2(\alpha) \\ 2\cos(\alpha)\ \sin(\alpha) \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} 2\cos(\alpha)\ \sin(\alpha) \\ \sin^2(\alpha) - \cos^2(\alpha) \end{pmatrix}$$

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 17.7 (*ii*) bijektiv, also ein Isomorphismus $\mathbb{R}^2 \to \mathbb{R}^2$.

Die Spiegelungsabbildung kann 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. 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

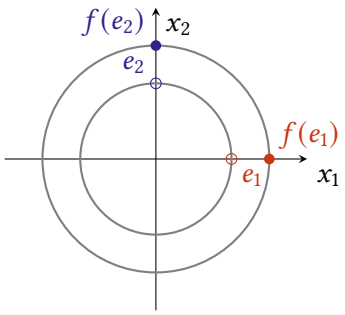
$$f(e_1) = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} \quad \text{und} \quad f(e_2) = \begin{pmatrix} 0 \\ \alpha \end{pmatrix}$$

mit $\alpha \in \mathbb{R}$ eine lineare Abbildung fest, und zwar eine Streckung bzw. (wenn $\alpha < 0$ ist) eine Streckung und Punktspiegelung am Ursprung. Da $(f(e_1), f(e_2))$ für $\alpha \neq 0$ eine Basis von $\mathbb{R}^2$ bildet, ist die Streckungsabbildung nach Satz 17.7 (*ii*) in diesem Fall bijektiv, also ein Isomorphismus $\mathbb{R}^2 \to \mathbb{R}^2$.

Die Streckungsabbildung kann durch Matrix-Vektor-Produkte mit der Matrix

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} \tag{17.8}$$

realisiert werden.



(*vi*) Es sei K ein Körper und $K[t]$ der Polynomraum über K (Beispiel 12.3). Die **Ableitungsabbildung** $f\colon K[t] \to K[t]$ ist ein linearer Endomorphismus, der durch die Festlegung

$$f(t^n) \coloneqq \begin{cases} n\,t^{n-1} & \text{für } n \in \mathbb{N} \\ 0 & \text{für } n = 0 \end{cases}$$

einndeutig bestimmt ist, da die Monome $(t^n)_{n\in\mathbb{N}_0}$ eine Basis von $K[t]$ bilden (Beispiel 13.9). △

Ende der Vorlesung 24

§ 17.2 Die Matrix-Vektor-Multiplikation als lineare Abbildung

Die Matrix-Vektor-Multiplikation als Prototyp einer linearen Abbildung (Beispiel 17.3) ist von so zentraler Bedeutung, dass wir hier ihre Eigenschaften zusammenstellen. Kurz gesagt: 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 17.9 (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 definiert die **von A induzierte lineare Abbildung**

$$f_A\colon K^m \ni x \mapsto f_A(x) \coloneqq A\,x \in K^n \tag{17.9}$$

eine lineare Abbildung $K^m \to K^n$.

(*ii*) Ist $f\colon K^m \to K^n$ 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

$$f_A \circ f_B = f_{A\,B}. \tag{17.10}$$

(*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

$$(f_A)^{-1} = f_{A^{-1}}. \tag{17.11}$$

Beweis. Der Beweis ist Gegenstand von Hausaufgabe 12.3. □

§ 17.3 Der Vektorraum der Vektorraumhomomorphismen

Definition 17.10 (Menge der Homomorphismen, Endomorphismen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K.

(*i*) Wir bezeichnen die Menge der linearen Abbildungen (Homomorphismen) $V \to W$ mit

$$\operatorname{Hom}(V, W) \coloneqq \big\{ f\colon V \to W \,\big|\, f \text{ ist Vektorraumhomomorphismus} \big\}. \tag{17.12}$$

Wollen wir den Skalarkörper betonen, so schreiben wir auch $\operatorname{Hom}_K(V, W)$.

(*ii*) Wir bezeichnen die Menge der Endomorphismen $V \to V$ mit

$$\mathrm{End}(V) \coloneqq \mathrm{Hom}(V,V) = \big\{ f \colon V \to V \,\big|\, f \text{ ist Vektorraumendomorphismus} \big\}. \tag{17.13}$$

Wollen wir den Skalarkörper betonen, so schreiben wir auch hier $\mathrm{End}_K(V)$. △

Satz 17.11 (die Homomorphismen zwischen Vektorräumen bilden einen Vektorraum)**.**
Es seien $(K,+,\cdot)$ ein Körper und $(V,+,\cdot)$, $(W,+,\cdot)$ zwei Vektorräume über K. $(\mathrm{Hom}(V,W),+,\cdot)$ mit der punktweisen Addition $+$ und der punktweisen S-Multiplikation $\cdot$

$$\begin{aligned} +\colon \mathrm{Hom}(V,W) \times \mathrm{Hom}(V,W) &\to \mathrm{Hom}(V,W) && \text{mit } f+g \text{ definiert durch } (f+g)(u) \coloneqq f(u)+g(u) \\ \cdot\colon K \times \mathrm{Hom}(V,W) &\to \mathrm{Hom}(V,W) && \text{mit } \alpha \cdot f \text{ definiert durch } (\alpha \cdot f)(u) \coloneqq \alpha\, f(u) \end{aligned}$$

bildet einen Vektorraum über K. Der Nullvektor in $(\mathrm{Hom}(V,W),+,\cdot)$ 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 12.1 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 10.2). Insbesondere ist also $(\mathrm{Hom}(V,W),+)$ 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 $f, g \in \mathrm{Hom}(V,W)$, denn wir haben

$$\begin{aligned} [\alpha\,(f+g)](u) &= \alpha\,[(f+g)(u)] = \alpha\,[f(u)+g(u)] = \alpha\, f(u) + \alpha\, g(u) \\ &= (\alpha\, f)(u) + (\alpha\, g)(u) = [\alpha\, f + \alpha\, g](u) \\ \text{und} \quad [(\alpha+\beta)\, f](u) &= (\alpha+\beta)\, f(u) = \alpha\, f(u) + \beta\, f(u) \\ &= [\alpha\, f + \beta\, f](u) \end{aligned}$$

für alle $u \in V$.

Das Assoziativgesetz

$$(\alpha\,\beta)\, f = \alpha\,(\beta\, f)$$

gilt, denn wir haben

$$[(\alpha\,\beta)\, f](u) = (\alpha\,\beta)\, f(u) = \alpha\,(\beta\, f(u)) = \alpha\,([\beta\, f](u)) = [\alpha\,(\beta\, f)](u)$$

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 17.11 ergibt sich, dass insbesondere die Endomorphismen $(\mathrm{End}(V),+,\cdot)$ einen Vektorraum bilden. Ersetzen wir die S-Multiplikation durch die Komposition $\circ$, so erhalten wir einen Ring wie schon beim Endomorphismenring einer abelschen Gruppe (vgl. Beispiel 9.2):

Satz 17.12 (die Endomorphismen eines Vektorraumes bilden einen Ring)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K. $(\mathrm{End}(V), +, \circ)$ mit der punktweisen Addition $+$ und der Komposition $\circ$

$$\begin{aligned} +\colon\ & \mathrm{End}(V) \times \mathrm{End}(V) \to \mathrm{End}(V) \quad \text{mit } f+g \text{ definiert durch } (f+g)(u) \coloneqq f(u)+g(u) \\ \circ\colon\ & \mathrm{End}(V) \times \mathrm{End}(V) \to \mathrm{End}(V) \quad \text{mit } f\circ g \text{ definiert durch } (f\circ g)(u) \coloneqq f(g(u)) \end{aligned}$$

bildet einen Ring mit dem Einselement id_V, genannt der **Endomorphismenring** (englisch: ring of endomorphisms) des Vektorraumes $(V, +, \cdot)$, vgl. Beispiel 9.2. Er ist i. A. nicht kommutativ.

Beweis. Der Beweis ist derselbe wie für den Endomorphismenring der abelschen Gruppe $(V, +)$ aus Beispiel 9.2, siehe Hausaufgabe 6.3. Die Vektorraumstruktur von V spielt hier überhaupt keine Rolle. □

§ 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[19] 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 Übergang zur Nebenklasse ergibt dasselbe wie erst Übergang zur Nebenklasse und dann verknüpfen."

Dieser Übergang zur Faktorgruppe $(G/N, \tilde{\star})$ — einer gröberen Version der Gruppe G — war wichtig für das Verständnis der Wirkungsweise von Gruppenhomomorphismen (Homomorphiesatz für Gruppen 8.17). Dieser Satz besagte, dass ein Gruppenhomomorphismus $f\colon G_1 \to G_2$ „nebenklassenweise" in der Faktorgruppe $G_1/\mathrm{Kern}(f)$ wirkt, also eine ganze Nebenklasse $[a] = a \star \mathrm{Kern}(f)$ auf ein Element in $\mathrm{Bild}(f)$ abbildet, und zwar verschiedene Nebenklassen auf verschiedene Bildelemente. Kurz gesagt: $G_1/\mathrm{Kern}(f) \cong \mathrm{Bild}(f)$.

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 als Normalteiler nicht beliebige Untergruppen verwenden, sondern Unterräume von V.

Aus der Faktormenge wird damit der **Faktorraum** (englisch: factor space) oder **Quotientenraum** (englisch: quotient space) von V nach U. Man sagt auch: „Aus dem Vektorraum $(V, +, \cdot)$ wird der Unterraum U ausfaktorisiert." Jede Nebenklasse $[v] = v + U$ heißt auch ein **affiner Unterraum parallel zu** U (englisch: affine subspace parallel to U). 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) $\dim(v + U) \coloneqq \dim(U)$ zu.

Satz 17.13 (Faktorraum, vgl. Satz 8.13 über Faktorgruppen)**.**
Es seien $(K, +, \cdot)$ ein Körper, $(V, +, \cdot)$ ein Vektorraum über K und U ein Unterraum von V. Dann gilt:

[19] **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.

(*i*) Auf der Faktormenge

$$V/U = \big\{[v] = v + U \,\big|\, v \in V\big\}$$

sind $\tilde{+}$ und $\tilde{\cdot}$, definiert als

$$[v] \mathbin{\tilde{+}} [w] := [v + w] \quad \text{für } v, w \in V, \tag{17.14a}$$

$$\alpha \mathbin{\tilde{\cdot}} [v] := [\alpha \cdot v] \quad \text{für } \alpha \in K \text{ und } v \in V, \tag{17.14b}$$

eine innere bzw. äußere Verknüpfung, bzgl. der $(V/U, \tilde{+}, \tilde{\cdot})$ einen Vektorraum über K bildet. Das neutrale Element bzgl. $\tilde{+}$ ist $[0] = U$, und für die Inversen gilt $\tilde{-}[v] = [-v]$.

(*ii*) Die Abbildung

$$\pi\colon \begin{cases} V \to V/U \\ v \mapsto [v], \end{cases} \tag{17.15}$$

die jedem Vektor $v \in V$ seine Nebenklasse $[v]$ zuordnet, ist ein surjektiver Vektorraumhomomorphismus. Sie heißt die **kanonische Surjektion** (englisch: canonical surjection) von V auf V/U. Es gilt $\operatorname{Kern}(\pi) = U$.

Beweis. Aussage (*i*): Wir weisen die Bedingungen aus der Definition 12.1 eines Vektorraumes nach.

Nach Satz 8.13 ist $(V/U, \tilde{+})$ eine abelsche Gruppe, da $(U, +)$ insbesondere eine Untergruppe und damit ein Normalteiler der abelschen Gruppe $(V, +)$ ist.

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

$$\begin{aligned}
\alpha \mathbin{\tilde{\cdot}} [v_1] &= [0\, v_1] && \text{nach Definition von } \tilde{\cdot} \\
&= [0\, v_2] && \text{da } 0\, v_1 = 0 = 0\, v_2 \text{ gilt} \\
&= \alpha \mathbin{\tilde{\cdot}} [v_2] && \text{nach Definition von } \tilde{\cdot}.
\end{aligned}$$

Nun weisen wir die Distributivgesetze (12.1a) und (12.1b) in $(V/U, \tilde{+}, \tilde{\cdot})$ nach:

$$\begin{aligned}
\alpha \mathbin{\tilde{\cdot}} ([v_1] \mathbin{\tilde{+}} [v_2]) &= \alpha \mathbin{\tilde{\cdot}} [v_1 + v_2] && \text{nach Definition von } \tilde{+} \\
&= [\alpha\,(v_1 + v_2)] && \text{nach Definition von } \tilde{\cdot} \\
&= [\alpha\, v_1 + \alpha\, v_2] && \text{aufgrund des Distributivgesetzes (12.1a) in } (V, +, \cdot) \\
&= [\alpha\, v_1] \mathbin{\tilde{+}} [\alpha\, v_2] && \text{nach Definition von } \tilde{+} \\
&= \alpha \mathbin{\tilde{\cdot}} [v_1] \mathbin{\tilde{+}} \alpha \mathbin{\tilde{\cdot}} [v_2] && \text{nach Definition von } \tilde{\cdot}
\end{aligned}$$

und

$$\begin{aligned}(\alpha+\beta)\mathbin{\tilde{\cdot}}[v] &= [(\alpha+\beta)\,v] && \text{nach Definition von } \tilde{\cdot}\\ &= [\alpha\,v+\beta\,v] && \text{aufgrund des Distributivgesetzes (12.1b) in } (V,+,\cdot)\\ &= [\alpha\,v]\mathbin{\tilde{+}}[\beta\,v] && \text{nach Definition von } \tilde{+}\\ &= \alpha\mathbin{\tilde{\cdot}}[v]\mathbin{\tilde{+}}\beta\mathbin{\tilde{\cdot}}[v] && \text{nach Definition von } \tilde{\cdot}.\end{aligned}$$

Es folgt das Assoziativgesetz (12.1c):

$$\begin{aligned}(\alpha\,\beta)\mathbin{\tilde{\cdot}}[v] &= [(\alpha\,\beta)\,v] && \text{nach Definition von } \tilde{\cdot}\\ &= [\alpha\,(\beta\,v)] && \text{aufgrund des Assoziativgesetzes (12.1c) in } (V,+,\cdot)\\ &= \alpha\mathbin{\tilde{\cdot}}[\beta\,v] && \text{nach Definition von } \tilde{\cdot}\\ &= \alpha\mathbin{\tilde{\cdot}}(\beta\mathbin{\tilde{\cdot}}[v]) && \text{nach Definition von } \tilde{\cdot}.\end{aligned}$$

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 8.13 über die Eigenschaften der abelschen Gruppe $(V/U, \tilde{+})$.

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 gerade

$$\begin{aligned}[v+w] &= [v]\mathbin{\tilde{+}}[v]\\ \text{und}\quad [\alpha\,v] &= \alpha\mathbin{\tilde{\cdot}}[v],\end{aligned}$$

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 $\operatorname{Kern}(\pi) = \pi^{-1}([0]) = U$. □

Bemerkung 17.14 (Faktorraum, vgl. Bemerkung 8.14)**.**
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 18.5. △

Beispiel 17.15 (Faktorraum, vgl. Beispiel 8.15)**.**

(i) Es sei V ein beliebiger Vektorraum und $U = \{0\}$ der Nullraum, einer der beiden trivialen Unterräume von V. Der zugehörige Faktorraum V/U 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/U ist isomorph zum Nullraum $\{0\}$.

(*iii*) Es sei V der Polynomraum $K[t]$ über einem Körper K. Wählen wir $U = K_0[t]$ als den Unterraum der konstanten Polynome, dann besteht der Faktorraum V/U gerade aus Äquivalenzklassen von Polynomen, wobei zwei Polynome genau dann in derselben Äquivalenzklasse (Nebenklasse) liegen, wenn sie sich nur um eine additive Konstante unterscheiden. △

Bemerkung 17.16 (Unterräume sind genau die Kerne von Vektorraumhomomorphismen, vgl. Bemerkung 8.16)**.**
Es sei $(V, +, \cdot)$ über dem Körper K.

(*i*) Nach Lemma 17.6 ist $\operatorname{Kern}(f)$ für jeden beliebigen Vektorraumhomomorphismus $f\colon V \to W$ in jeden beliebigen Vektorraum $(W, +, \cdot)$ über demselben Körper K immer ein Unterraum von $(V, +, \cdot)$.

(*ii*) Umgekehrt ist jeder Unterraum U von V der Kern eines geeignet gewählten Vektorraumhomomorphismus: Wähle z. B. W als den Faktorraum $(V/U, \tilde{+}, \tilde{\cdot})$ und als Homomorphismus die kanonische Surjektion $V \to V/U$. △

§ 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 $f\colon V \to W$ „nebenklassenweise“ wirkt. Er bildet also eine gesamte 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 $(V, +, \cdot)$ und den Unterraum $\operatorname{Kern}(f)$.

Satz 17.17 (Homomorphiesatz für Vektorräume[20]**,** vgl. Homomorphiesatz für Gruppen 8.17**).**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K. Weiter sei $f\colon V \to W$ ein Homomorphismus. Dann gilt

$$V/\operatorname{Kern}(f) \cong \operatorname{Bild}(f) \tag{17.16a}$$

mit dem Isomorphismus

$$I([v]) \coloneqq f(v) \quad \text{für } [v] = v + \operatorname{Kern}(f) \in V/\operatorname{Kern}(f). \tag{17.16b}$$

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 8.17 folgt also sofort, dass $V/\operatorname{Kern}(f)$ und $\operatorname{Bild}(f)$ im Sinne von Gruppen isomorph sind, und zwar durch den Isomorphismus (17.16b).

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:

$$\begin{aligned} I(\alpha \mathbin{\tilde{\cdot}} [v]) &= I([\alpha v]) && \text{nach Definition von } \tilde{\cdot} \\ &= f(\alpha v) && \text{nach Definition von } I \\ &= \alpha f(v) && \text{aufgrund der Homogenität von } f \\ &= \alpha I([v]) && \text{nach Definition von } I. \end{aligned}$$

□

[20] englisch: fundamental theorem on vector space homomorphisms

Beispiel 17.18 (Homomorphiesatz für Vektorräume, vgl. Beispiel 8.18)**.**

(*i*) Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K. Wir betrachten den Nullhomomorphismus $f\colon V \to W$ mit $f(v) = 0$ für alle $v \in V$. Gemäß Homomorphiesatz für Vektorräume 17.17 ist

$$V / \operatorname{Kern}(f) = V / v \;\cong\; \{0\}.$$

(*ii*) Es seien K ein Körper und $V := K[t]$ der Polynomraum über K (Beispiel 12.3). Wir betrachten die Ableitungsabbildung $f\colon K[t] \to K[t]$ aus Beispiel 17.8, ein linearer Endomorphimus. Diese Abbildung ist surjektiv, aber nicht injektiv. Es gilt $\operatorname{Kern}(f) = K_0[t]$, der Unterraum der konstanten Polynome. Gemäß Homomorphiesatz für Vektorräume 17.17 ist

$$V / \operatorname{Kern}(f) = K[t] / K_0[t] \;\cong\; \operatorname{Bild}(f) = K[t].$$

In diesem Fall wird also das Bild trotz Ausfaktorisierung eines eindimensionalen Unterraumes nicht kleiner (geringer in der Dimension) als der Ursprungsraum $V = K[t]$. Das kann nur passieren, wenn $\dim(V) = \infty$ gilt.

Jede Äquivalenzklasse besteht aus denjenigen Polynomen, die sich nur um eine additive Konstante unterscheiden und daher durch die Ableitungsabbildung auf dasselbe Polynom abgebildet werden. Durch $\operatorname{Kern}(f)$ werden die konstante Polynom ausfaktorisiert.

(*iii*) Es seien $(K, +, \cdot)$ ein Körper und $V := (K^{\mathbb{N}}, +, \cdot)$ der Vektorraum aller K-wertigen Folgen. Wir betrachten den Homomorphismus $f\colon K^{\mathbb{N}} \to K$, der definiert ist durch

$$f((y_i)_{i\in\mathbb{N}}) := y_1 \in K,$$

der also die Folge auf das erste Folgenelement abbildet. Dann ist $\operatorname{Kern}(f) = \{(y_i)_{i\in\mathbb{N}} \mid y_1 = 0\}$, also besteht $K^{\mathbb{N}} / \operatorname{Kern}(f)$ aus Äquivalenzklassen von Folgen, die jeweils im ersten Folgenglied übereinstimmen. Eine gesamte Äquivalenzklasse wird auf ein- und dasselbe Element von K abgebildet. Gemäß Homomorphiesatz für Vektorräume 17.17 ist

$$V / \operatorname{Kern}(f) = K^{\mathbb{N}} / \operatorname{Kern}(f) \;\cong\; \operatorname{Bild}(f) = K. \qquad \triangle$$

Abschließend stellen wir den Homomorphiesatz für Vektorräume 17.17 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.

$$\begin{array}{ccc} W & \xleftarrow{\;f\;} & V \\ {\scriptstyle i}\uparrow & & \downarrow{\scriptstyle \pi} \\ \operatorname{Bild}(f) & \xleftarrow[\;I\;]{} & V / \operatorname{Kern}(f) \end{array}$$

Das Diagramm besagt:

$$f = \underbrace{i}_{\text{einbetten}} \circ \overbrace{I}^{\text{isomorph abbilden}} \circ \underbrace{\pi}_{\text{vergröbern}}.$$

Ende der Vorlesung 25

Ende der Woche 12

§ 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 17.17 beteiligten Räume V, $\mathrm{Kern}(f)$ und $\mathrm{Bild}(f)$ untersuchen.

§ 18.1 Zusammenhang von Dimension und Isomorphie

Als Folgerungen aus dem Existenz- und Eindeutigkeitssatz für Vektorraumhomomorphismen 17.7 erhalten wir folgende bemerkenswerte Resultate:

Folgerung 18.1 (isomorphe Vektorräume besitzen dieselbe Dimension[21])**.**

Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K. Sind V und W isomorph, dann gilt $\dim(V) = \dim(W)$.

Beweis. Es sei $f\colon V \to W$ ein Isomorphismus. Nach Folgerung 13.12 existiert eine Basis $(v_i)_{i\in I}$ von V. Setze $w_i := f(v_i)$ für $i \in I$. Dann ist nach Satz 17.7 *(ii)* (d) $(w_i)_{i\in I}$ eine Basis von W. Beide Basen sind gleichmächtig, also gilt $\dim(V) = \dim(W)$. □

Folgerung 18.2 (Vektorräume gleicher endlicher Dimension sind isomorph)**.**

Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K. Dann sind äquivalent:

(*i*) V und W sind isomorphe Vektorräume.

(*ii*) $\dim(V) = \dim(W)$.

Beweis. Aussage (*i*) ⇒ Aussage (*ii*) ist gerade die Aussage des Lemmas 18.2.

Aussage (*ii*) ⇒ Aussage (*i*): Es gelte $\dim(V) = \dim(W) = n \in \mathbb{N}_0$. Es seien $(v_1, \dots, v_n)$ eine beliebige Basis von V und $(w_1, \dots, w_n)$ eine beliebige Basis von W. Nach Satz 17.7 *(ii)* gibt es genau eine lineare Abbildung $f\colon V \to W$ mit der Eigenschaft $f(v_i) = w_i$ für alle $i = 1, \dots, n$. Nach Satz 17.7 *(ii)* (d) ist dieses f bijektiv, also sind V und W zueinander isomorph. □

Folgerung 18.2 besagt, dass es bis auf Isomorphie nur einen einzigen K-Vektorraum der Dimension $n \in \mathbb{N}_0$ gibt! Alle K-Vektorräume V mit $\dim(V) = n \in \mathbb{N}_0$ sind zueinander isomorph. Das werden wir später in § 19 noch ausnutzen.

[21] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

§ 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 (Isomorphiesatz)**.**
Es seien $(K,+,\cdot)$ ein Körper und $(V,+,\cdot)$ ein Vektorraum über K sowie U_1, U_2 zwei Unterräume von V. Dann gilt:

$$(U_1+U_2)/U_1 \cong U_2/(U_1\cap U_2). \tag{18.1}$$

Beweis. Die Beweisidee basiert darauf, 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 17.17 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

$$\begin{aligned} \operatorname{Kern}(f) &= \{u_2\in U_2 \mid f(u_2) = [0]\} && \text{nach Definition des Kerns}\\ &&& \text{und des neutralen Elements } [0] \text{ in } (U_1+U_2)/U_1\\ &= \{u_2\in U_2 \mid [u_2] = [0]\} && \text{nach Definition von } f\\ &= \{u_2\in U_2 \mid u_2 - 0 \in U_1\} && \text{nach Definition von } [\cdot]\\ &= U_1\cap U_2. \end{aligned}$$

Schritt 3: f ist surjektiv, d. h., $\operatorname{Bild}(f) = (U_1+U_2)/U_1$.

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 $[w] = u_1+u_2+U_1 = u_2+U_1 = [u_2] = f(u_2)$. □

Folgerung 18.4 (Isomorphiesatz)**.**
Es seien $(K,+,\cdot)$ ein Körper und $(V,+,\cdot)$ ein Vektorraum über K sowie U_1, U_2 zwei Unterräume von V. Wenn $U_1\cap U_2 = \{0\}$ gilt, dann ist

$$(U_1\oplus U_2)/U_1 \cong U_2. \tag{18.2}$$

Beweis. Nach Satz 18.3 gilt

$$(U_1 + U_2) / U_1 \cong U_2 / (U_1 \cap U_2).$$

Die Direktheit der Summe $U_1 \oplus U_2$ bedeutet $U_1 \cap U_2 = \{0\}$, also gilt

$$(U_1 + U_2) / U_1 \cong U_2 / \{0\} = \left\{ [u_2] = u_2 + \{0\} \,\middle|\, u_2 \in U_2 \right\} \cong U_2,$$

vgl. auch Beispiel 17.15. □

Nun können wir die Dimension von Faktorräumen bestimmen:

Satz 18.5 (Dimension des Faktorraumes[22])**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K sowie U ein Unterraum von V. Dann gilt

(*i*)
$$\dim(V) = \dim(U) + \dim(V / U) \tag{18.3}$$
Wenn $\dim(V) = \infty$ ist, dann hat also mindestens einer der Räume U und V / U ebenfalls unendliche Dimension.

(*ii*)
$$\dim(V / U) = \operatorname{codim}(U). \tag{18.4}$$

(*iii*) Ist V endlich-dimensional, dann gilt auch
$$\dim(V / U) = \dim(V) - \dim(U). \tag{18.5}$$

Beweis. Aussage (*i*) und Aussage (*ii*): Nach Folgerung 14.9 existiert ein zu U komplementärer Unterraum W, sodass also $V = U \oplus W$ gilt. Dieses Resultat haben wir, ausgehend von einer Basis B_U von U, mit Hilfe des Basisergänzungssatzes 13.11 durch Ergänzung zu einer Basis B von V bewiesen, wobei $B_W := B \setminus B_U$ eine Basis von B_W ergibt.

Es gilt also
$$\dim(V) = \dim(U) + \dim(W) \quad \text{und} \quad \dim(W) = \operatorname{codim}(U)$$
nach Definition 14.10 der Kodimension. Diese Gleichung gilt auch im Fall $\dim(V) = \infty$, wobei dann mindestens einer der Räume U und W ebenfalls unendliche Dimension besitzt. Nach Folgerung 18.4 ist $V / U = U \oplus W / U \cong W$. Da isomorphe Vektorräume dieselbe Dimension besitzen (Folgerung 18.1), folgen
$$\dim(V) = \dim(U) + \dim(V / U) \quad \text{und} \quad \dim(V / U) = \operatorname{codim}(U),$$
also (18.3) und (18.4).

Aussage (*iii*): Wenn $\dim(V)$ endlich ist, dann sind auch die Dimensionen der Unterräume $\dim(U)$ und $\dim(W) = \dim(V / U)$ endlich (Folgerung 13.22), und wir können (18.3) auflösen nach $\dim(V / U)$ auflösen, um (18.5) zu erhalten. □

[22] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

§ 18.3 Dimensionen im Homomorphiesatz

Mit Hilfe von Satz 18.5 können wir nun die Dimensionen der Räume V, $\operatorname{Kern}(f)$ und $\operatorname{Bild}(f)$ im Homomorphiesatz für Vektorräume 17.17 untersuchen:

Folgerung 18.6 (Dimensionen der Räume im Homomorphiesatz für Vektorräume 17.17[23])**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K. Weiter sei $f\colon V \to W$ ein Homomorphismus. Dann gilt

$$\dim(\operatorname{Kern}(f)) + \dim(\operatorname{Bild}(f)) = \dim(V). \tag{18.6}$$

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 17.17 $\operatorname{Bild}(f)$ und $V / \operatorname{Kern} f$ isomorph sind und nach Folgerung 18.1 isomorphe Vektorräume dieselbe Dimension besitzen, ist (18.6) gezeigt. □

Definition 18.7 (Rang und Defekt eines Homomorphismus)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K. Weiter sei $f\colon V \to W$ ein Homomorphismus. Dann heißt

$$\operatorname{Rang}(f) := \dim(\operatorname{Bild}(f)) \tag{18.7}$$

der **Rang** (englisch: rank) der linearen Abbildung f, und

$$\operatorname{Defekt}(f) := \dim(\operatorname{Kern}(f)) \tag{18.8}$$

heißt der **Defekt** (englisch: defect) von f. △

Wir können also die Dimensionsformel (18.6) auch in der Form

$$\operatorname{Defekt}(f) + \operatorname{Rang}(f) = \dim(V) \tag{18.9}$$

schreiben.

Das folgende Resultat erleichtert der Nachweis der Bijektivität (also der Isomorphismus-Eigenschaft) einer linearen Abbildung erheblich.

Folgerung 18.8 (Charakterisierung der Bijektivität von Homomorphismen endlich-dimensionaler Vektorräume)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei Vektorräume über K sowie $f\colon V \to W$ 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.

[23] Dieses Resultat hängt im Fall, dass V unendlich-dimensional ist, vom Zornschen Lemma und damit vom Auswahlaxiom ab.

(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 sei 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 von Hausaufgabe 13.2. □

Beispiel 18.9 (Charakterisierung der Bijektivität von Homomorphismen endlich-dimensionaler Vektorräume)**.**
In diesem Beispiel illustrieren wir verschiedene Fälle aus Folgerung 18.8.

(*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 Fälle auftreten:

- Die Ableitungsabbildung $f\colon K[t] \to K[t]$ ist surjektiv, aber nicht injektiv (Beispiel 17.18).
- Die Abbildung $f\colon K[t] \to K[t]$ definiert durch $f(p) = t \cdot p$ ist injektiv, aber nicht surjektiv.
- Die Abbildung $f\colon K[t] \to K[t]$ definiert durch $f(p) = -p$ ist bijektiv.
- Die Nullabbildung $f\colon K[t] \to K[t]$ definiert durch $f(p) = 0$ ist weder injektiv noch surjektiv. △

§ 19 Matrizen zur Darstellung linearer Abbildungen

Literatur: Fischer, Springborn, 2020, Kapitel 3.4–3.5, Beutelspacher, 2014, Kapitel 5.2

Im gesamten § 19 sind alle Vektorräume endlich-dimensional. Wir erinnern an Folgerung 18.2, die besagt, dass es bis auf Isomorphie nur einen einzigen K-Vektorraum der Dimension $n \in \mathbb{N}_0$ gibt! Alle K-Vektorräume V mit $\dim(V) = n \in \mathbb{N}_0$ sind also zueinander isomorph. 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 Die Koordinatendarstellung eines endlich-dimensionalen Vektorraumes

Der folgende Satz gibt an, wie wir mit Hilfe einer Basis von V einen Isomorphismus $K^n \longrightarrow V$ erhalten können.

Satz 19.1 (Koordinatendarstellung)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter sei die Familie $B = (v_1, \ldots, v_n)$ eine Basis von V. Dann ist die Abbildung

$$\Phi_B \colon K^n \ni \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i v_i \in V \tag{19.1}$$

ein linearer Isomorphismus $K^n \longrightarrow V$. 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** (englisch: coordinate vector) $x \in K^n$ bzgl. der Basis B zuordnet. Wir nennen daher Φ_B^{-1} auch die **Koordinatenabbildung** (englisch: coordinate map) bzgl. der Basis B.[24]

Beweis. Φ_B ist linear und bildet die Basis $(e_1, \ldots, e_n)$ in K^n auf die Basis $(v_1, \ldots, v_n)$ ab. Damit ist Φ_B nach Satz 17.7 (*ii*) (d) bijektiv, also ein linearer Isomorphismus, und die Inverse Φ_B^{-1} ebenfalls. □

Wir werden Koordinatenvektoren typischerweise mit x bezeichnen.

Beispiel 19.2 (Koordinatendarstellung)**.**

(*i*) Das Polynom $7t^2 - 3t + 5$ hat in der Monombasis $(1,\ t,\ t^2)$ von $\mathbb{R}_2[t]$ den Koeffizientenvektor $\begin{pmatrix} 5 \\ -3 \\ 7 \end{pmatrix}$, denn es gilt

$$7t^2 - 3t + 5 = 5 \cdot 1 + (-3) \cdot t + 7 \cdot t^2.$$

(*ii*) Um dasselbe Polynom $7t^2 - 3t + 5$ in der Basis $(t^2 - t + 1,\ t^2 + 3,\ t + 1)$ darzustellen, schreiben wir es als Linearkombination der Basisvektoren mit unbekanntem Koeffizientenvektor $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ auf:

$$7t^2 - 3t + 5 = x_1 (t^2 - t + 1) + x_2 (t^2 + 3) + x_3 (t + 1).$$

Ein Koeffizientenvergleich ergibt das lineare Gleichungssystem

$$\begin{bmatrix} 1 & 3 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ -3 \\ 7 \end{pmatrix}$$

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?)

[24] Hier zeigt sich der Grund, warum wir den Standardvektorraum K^n, der in Beispiel 12.3 eingeführt wurde, auch als **Koordinatenraum** bezeichnen.

Probe:

$$\begin{aligned} &13\,(t^2 - t + 1) + (-6)\,(t^2 + 3) + 10\,(t + 1) \\ &\quad = (13 - 6)\,t^2 + (-13 + 10)\,t + (13 - 18 + 10)\,1 \\ &\quad = 7\,t^2 - 3\,t + 5. \end{aligned}$$

△

Beachte: Zur Bestimmung des Koordinatenvektors $\Phi_B^{-1}(v)$ eines Vektors $v \in V$ muss man i. A. ein lineares Gleichungssystem lösen!

Ende der Vorlesung 26

§ 19.2 Darstellung linearer Abbildungen durch Matrizen

Aus Satz 17.7 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 $V \longrightarrow W$ mit Hilfe einer Matrix ist nun,

- alle Vektoren in V durch ihre Koordinatenvektoren bzgl. einer Basis darzustellen,
- ebenso alle Vektoren in W durch ihre Koordinatenvektoren bzgl. einer Basis darzustellen
- und nur noch mit den Koordinatenvektoren zu rechnen, für die die lineare Abbildung notwendigerweise die Form von Matrix-Vektor-Produkten hat.

Als Konsequenz können wir jede lineare Abbildung zwischen beliebigen endlich-dimensionalen Vektorräumen immer in der gleichen, einfachen und konkreten Form von Matrix-Vektor-Produkten darstellen.

Satz 19.3 (Darstellungssatz für lineare Abbildungen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K. 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 $f\colon V \longrightarrow W$ 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 auch die **Darstellungsmatrix der Abbildung f bzgl. der Basen B_V und B_W** (englisch: representation matrix), in Symbolen: $A = \mathcal{M}_{B_W}^{B_V}(f)$.

Beweis. f ist durch die Bilder $f(v_j)$ der Basisvektoren v_j, $j = 1, \ldots, m$, nach Satz 17.7 eindeutig festgelegt. Für jeden Vektor $f(v_j) \in W$ ist wiederum sein Koordinatenvektor bzgl. der Basis $(w_1, \ldots, w_n)$ 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 als Linearkombination in der Basis von 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 $\mathcal{M}_{\text{nach}}^{\text{von}}$, d. h., die Basis des Definitionsraumes („von“) der darzustellenden Abbildung steht oben, und die Basis des Zielraumes („nach“) steht unten.

Beispiel 19.4 (Darstellungsmatrizen von Homomorphismen)**.**

(*i*) Ist $V = K^m$ 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 17.9) gegeben, also $f_A(x) = A\,x$, dann ist A selbst die Darstellungsmatrix $\mathcal{M}_{B_W}^{B_V}(f)$, wenn $B_V = (e_1, \dots, e_m)$ und $B_W = (e_1, \dots, e_n)$ als die Standardbasen in K^m und K^n gewählt werden. Inbesondere hat beispielsweise die Drehabbildung aus Beispiel 17.8 als Abbildung $\mathbb{R}^2 \to \mathbb{R}^2$ bzgl. der Standardbasis 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 und die **zyklische Shift-Abbildung** (englisch: cyclic shift map) 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 Basen $B_V = B_W = \big((1,0,0,0,0), \dots, (0,0,0,0,1)\big)$ haben diese Endomorphismen die folgende Darstellung:

$$\mathcal{M}_{B_W}^{B_V}(f) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{bzw.} \quad \mathcal{M}_{B_W}^{B_V}(g) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

(*iii*) Auf dem Vektorraum $V = \mathbb{R}_3[t]$ der Polynome über $\mathbb{R}$ vom Höchstgrad 3 mit der Monombasis $(1,\ t,\ t^2\ t^3)$ betrachten wir die lineare Abbildung (drei Punktauswertungen der zugehörigen Polynomfunktion) mit Werten in $W = \mathbb{R}^3$

$$\mathbb{R}_3[t] \ni p \mapsto \begin{pmatrix} \widetilde{p}(-2) \\ \widetilde{p}(0) \\ \widetilde{p}(2) \end{pmatrix} \in \mathbb{R}^3.$$

Verwenden wir in $\mathbb{R}^3$ die Standardbasis, so besitzt diese Abbildung die Darstellungsmatrix

$$\begin{bmatrix} 1 & -2 & 4 & -8 \\ 1 & 0 & 0 & 0 \\ 1 & 2 & 4 & 8 \end{bmatrix}.$$

(*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 Basis $B_W = (1)$. Die lineare Abbildung $\mathrm{Re}\colon \mathbb{C} \to \mathbb{R}$ (Realteil) hat dann die Darstellungsmatrix

$$\mathcal{M}_{B_W}^{B_V}(\mathrm{Re}) = \begin{bmatrix} 1 & 0 \end{bmatrix},$$

während die lineare Abbildung $\mathrm{Im}\colon \mathbb{C} \to \mathbb{R}$ (Imaginärteil) die Darstellungsmatrix

$$\mathcal{M}_{B_W}^{B_V}(\mathrm{Im}) = \begin{bmatrix} 0 & 1 \end{bmatrix} \tag{19.4}$$

besitzt.

(*v*) Es seien $(K, +, \cdot)$ ein Körper und V und W Vektorräume über K. Es sei $\dim(V) = m$, $\dim(W) = n$ und $f\colon V \to W$ ein Homomorphismus mit $r = \operatorname{Rang}(f)$ und daher $\operatorname{Defekt}(f) = \dim(\operatorname{Kern}(f)) = m - r$ nach Dimensionsformel (18.6). Wir wählen die Basen so, 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

$$B_V = (\underbrace{v_1, \ldots, v_r}_{\text{siehe unten}}, \underbrace{v_{r+1}, \ldots, v_m}_{\text{Basis von Kern}(f)}).$$

Dabei sei $v_j \in f^{-1}(\{w_j\})$, sodass also $f(v_j) = w_j$ gilt für $j = 1, \ldots, r$. Bzgl. dieser angepassten Basen hat f die Darstellungsmatrix

$$\mathcal{M}_{B_W}^{B_V}(f) = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \in K^{n \times m}.$$

(*vi*) 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

$$\mathcal{M}_{B_V}^{B_V}(\mathrm{id}_V) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix},$$

also die Einheitsmatrix der passenden Dimension. △

Satz 19.5 (die Zuordnung zur Darstellungsmatrix ist ein Vektorraumisomorphismus)**.**

Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K. Weiter seien $B_V = (v_1, \ldots, v_m)$ und $B_W = (w_1, \ldots, w_n)$ Basen von V bzw. von W. Die Zuordnung

$$\mathcal{M}_{B_W}^{B_V}\colon \operatorname{Hom}(V, W) \ni f \mapsto \mathcal{M}_{B_W}^{B_V}(f) \in K^{n \times m} \tag{19.5}$$

eines Homomorphismus zu seiner Darstellungsmatrix ist ein Isomorphismus von Vektorräumen.

Beweis. **Schritt** 1: Wir zeigen zunächst die Linearität von $\mathcal{M}_{B_W}^{B_V}$.

Es seien dazu $f, g \in \operatorname{Hom}(V, W)$, $A := \mathcal{M}_{B_W}^{B_V}(f)$ und $B := \mathcal{M}_{B_W}^{B_V}(g)$. 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 $\mathcal{M}_{B_W}^{B_V}(f+g) = \mathcal{M}_{B_W}^{B_V}(f) + \mathcal{M}_{B_W}^{B_V}(g)$. Weiter gilt für $\alpha \in K$

$$\begin{aligned}(\alpha f)(v_j) &= \alpha f(v_j)\\ &= \alpha \sum_{i=1}^{n} a_{ij}\, w_i\\ &= \sum_{i=1}^{n} (\alpha\, a_{ij})\, w_i\end{aligned} \tag{19.6}$$

für alle $j = 1, \dots, m$. Das heißt $\mathcal{M}_{B_W}^{B_V}(\alpha f) = \alpha\, \mathcal{M}_{B_W}^{B_V}(f)$.

Schritt 2: Wir zeigen: $\mathcal{M}_{B_W}^{B_V}$ ist injektiv.

Es sei dazu $f \in \mathrm{Hom}(V, W)$ so, dass $\mathcal{M}_{B_W}^{B_V}(f) = 0 \in K^{n\times m}$ (die Nullmatrix) ergibt. Das heißt,

$$f(v_j) = \sum_{i=1}^{n} 0\, w_i = 0$$

für alle $j = 1, \dots, m$. Damit ist $f\colon V \to W$ der Nullhomomorphismus, also der Nullvektor von $\mathrm{Hom}(V, W)$. Daher gilt $\mathrm{Kern}(\mathcal{M}_{B_W}^{B_V}) = \{0\}$, und nach Lemma 17.6 ist $\mathcal{M}_{B_W}^{B_V}$ injektiv.

Schritt 3: Wir zeigen: $\mathcal{M}_{B_W}^{B_V}$ ist surjektiv.

Es sei dazu $A \in K^{n\times m}$. Nach Satz 17.7 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 19.2: Warum haben wir, um die Bijektivität von $\mathcal{M}_{B_W}^{B_V}$ zu zeigen, nicht die Charakterisierung der Bijektivität von Homomorphismen nach Folgerung 18.8 genutzt?

Folgerung 19.6 (Dimension des Vektorraumes der Homomorphismen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K mit $\dim(V) = m$ und $\dim(W) = n$ sowie $m, n \in \mathbb{N}_0$. Dann gilt

$$\dim(\mathrm{Hom}(V, W)) = n\, m. \tag{19.7}$$

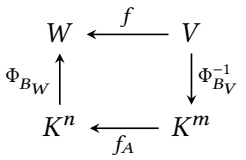
Beweis. Das Resultat folgt sofort aus $\dim(K^{n\times m}) = n\, m$ (Lemma 15.3) und der Isomorphie $\mathrm{Hom}(V, W) \cong K^{n\times m}$, aufgrund derer beide Räume dieselbe Dimension haben (Folgerung 18.2). □

Satz 19.7 (Zusammenhang zwischen einem Homomorphismus und seiner Darstellungsmatrix)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K. 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. Dann gilt für die Darstellungsmatrix $A := \mathcal{M}_{B_W}^{B_V}(f)$ und die durch A induzierte lineare Abbildung f_A der Zusammenhang

$$f_A = \underbrace{\Phi_{B_W}^{-1}}_{\text{Koordinaten} \mapsto \text{Vektor}} \circ f \circ \underbrace{\Phi_{B_V}}_{\text{Vektor} \mapsto \text{Koordinaten}} \colon K^m \to K^n \tag{19.8a}$$

$$f = \underbrace{\Phi_{B_W}}_{\text{Vektor} \mapsto \text{Koordinaten}} \circ f_A \circ \underbrace{\Phi_{B_V}^{-1}}_{\text{Koordinaten} \mapsto \text{Vektor}} \colon V \to W. \tag{19.8b}$$

Mit anderen Worten, folgendes Diagramm kommutiert:



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 in den Vektor $\Phi_{B_V}(x) \in V$ umgerechnet, dann wirkt f, und schließlich wird das Ergebnis durch $\Phi_{B_W}^{-1}$ als Koordinatenvektor bzgl. der Basis B_W angegeben. (**Quizfrage 19.3:** 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 17.7 aus, zu zeigen, dass ihre Bilder auf einer Basis gleich sind. Wir wählen dazu die Standardbasis $(e_1, \ldots, e_m)$ von K^m. Es gilt einerseits

$$\begin{aligned}
(\Phi_{B_W} \circ f_A)(e_j) &= \Phi_{B_W}(f_A(e_j)) && \text{nach Definition 6.13 der Komposition } \circ \\
&= \Phi_{B_W}(A\,e_j) && \text{nach Definition der von } A \text{ induzierten Abbildung } f_A \\
&= \Phi_{B_W}(a_{\bullet j}) && \text{nach Definition des Matrix-Vektor-Produkts} \\
&= \sum_{i=1}^{n} a_{ij}\,w_i && \text{nach Definition (19.1) von } \Phi_{B_W}
\end{aligned}$$

und andererseits

$$\begin{aligned}
(f \circ \Phi_{B_V})(e_j) &= f(\Phi_{B_V}(e_j)) && \text{nach Definition 6.13 der Komposition } \circ \\
&= f(v_j) && \text{nach Definition (19.1) von } \Phi_{B_V} \\
&= \sum_{i=1}^{n} a_{ij}\,w_i && \text{nach Definition (19.3) der Darstellungsmatrix } A.
\end{aligned}$$

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. □

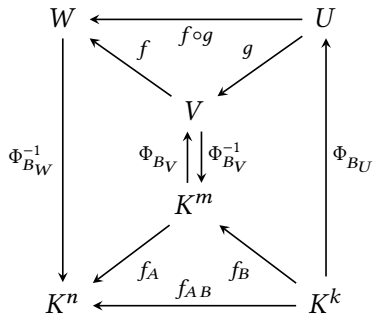
Wir zeigen nun noch, dass die Komposition linearer Abbildungen durch das Matrix-Matrix-Produkt ihrer Darstellungsmatrizen dargestellt wird.

Satz 19.8 (Darstellungsmatrix der Komposition von Homomorphismen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(U, +, \cdot)$, $(V, +, \cdot)$ und $(W, +, \cdot)$ endlich-dimensionale Vektorräume über K. Weiter seien $B_U = (u_1, \ldots, u_k)$, $B_V = (v_1, \ldots, v_m)$ und $B_W = (w_1, \ldots, w_n)$ 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

$$\mathcal{M}_{B_W}^{B_U}(f \circ g) = \mathcal{M}_{B_W}^{B_V}(f)\,\mathcal{M}_{B_V}^{B_U}(g). \tag{19.9}$$

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 $A := \mathcal{M}_{B_W}^{B_V}(f)$ und $B := \mathcal{M}_{B_V}^{B_U}(g)$. Das rechte und das linke Trapez sind kommutativ nach Satz 19.7, 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 17.9. 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 $\mathcal{M}_{B_W}^{B_U}(f \circ g)$, was zu beweisen war. □

§ 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, W sind Vektorräume über K.

Matrix $A \in K^{n\times m}$		lineare Abbildung $f\colon V \to W$	
Begriff	siehe	Begriff	siehe
$\text{Bild}(A) := \text{SR}(A)$	(15.15a)	$\text{Bild}(f) = \{f(u) \in W \mid u \in V\} = f(V)$	(17.2)
$\text{SRang}(A) = \dim(\text{SR}(A))$	(15.15b)	$\text{Rang}(f) = \dim(\text{Bild}(f))$	(18.7)
$\text{Kern}(A) := \{x \in K^m \mid Ax = 0\}$		$\text{Kern}(f) = \{u \in V \mid f(u) = 0\} = f^{-1}(\{0\})$	(17.3)
$\text{Defekt}(A) := \dim(\text{Kern}(A))$		$\text{Defekt}(f) = \dim(\text{Kern}(f))$	(18.8)

Beachte: Aus den Definitionen folgt sofort $\text{Bild}(A) = \text{Bild}(f_A)$ und $\text{Kern}(A) = \text{Kern}(f_A)$.

Wir können nun bestätigen, dass die oben genannten Eigenschaften für lineare Abbildungen zwischen endlich-dimensionalen Vektorräumen und ihren Darstellungsmatrizen übereinstimmen.

Satz 19.9 (Eigenschaften linearer Abbildungen und ihrer Darstellungsmatrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K mit $\dim(V) = m$ und $\dim(W) = n$. 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. Schließlich sei $A := \mathcal{M}_{B_W}^{B_V}(f) \in K^{n\times m}$ die Darstellungsmatrix von f. Dann gilt:

(*i*) $\mathrm{Bild}(f) = \Phi_{B_W}\big(\mathrm{Bild}(A)\big)$.

(*ii*) $\mathrm{Rang}(f) = \mathrm{SRang}(A) = \mathrm{Rang}(A)$.

(*iii*) $\mathrm{Kern}(f) = \Phi_{B_V}\big(\mathrm{Kern}(A)\big)$.

(*iv*) $\mathrm{Defekt}(f) = \mathrm{Defekt}(A)$.

Beweis. Aussage (*i*):

$$
\begin{aligned}
& w \in \mathrm{Bild}(f) \\
\Leftrightarrow\ & w \in \mathrm{Bild}(\Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}) && \text{wegen } f = \Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}, \text{ siehe (19.8b)} \\
\Leftrightarrow\ & w \in \Phi_{B_W}\big(\mathrm{Bild}(f_A \circ \Phi_{B_V}^{-1})\big) && \text{nach Definition von Bild} \\
\Leftrightarrow\ & w \in \Phi_{B_W}\big(\mathrm{Bild}(f_A)\big) && \text{wegen der Bijektivität von } \Phi_{B_V}^{-1} \\
\Leftrightarrow\ & w \in \Phi_{B_W}\big(\mathrm{Bild}(A)\big) && \text{wegen } f_A(x) = A\,x.
\end{aligned}
$$

Aussage (*ii*): $\mathrm{Bild}(f)$ und $\mathrm{Bild}(A)$ sind nach Aussage (*i*) zueinander isomorphe Unterräume von W bzw. von K^n. Nach Folgerung 18.8 haben sie also dieselbe Dimension.

Aussage (*iii*):

$$
\begin{aligned}
& v \in \mathrm{Kern}(f) \\
\Leftrightarrow\ & v \in \mathrm{Kern}(\Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}) && \text{wegen } f = \Phi_{B_W} \circ f_A \circ \Phi_{B_V}^{-1}, \text{ siehe (19.8b)} \\
\Leftrightarrow\ & v \in \Phi_{B_V}\big(\mathrm{Kern}(\Phi_{B_W} \circ f_A)\big) && \text{wegen der Bijektivität von } \Phi_{B_V}^{-1} \\
\Leftrightarrow\ & v \in \Phi_{B_V}\big(\mathrm{Kern}(f_A)\big) && \text{wegen der Bijektivität von } \Phi_{B_W} \\
\Leftrightarrow\ & v \in \Phi_{B_V}\big(\mathrm{Kern}(A)\big) && \text{wegen } f_A(x) = A\,x.
\end{aligned}
$$

Aussage (*iv*): $\mathrm{Kern}(f)$ und $\mathrm{Bild}(A)$ sind nach Aussage (*iii*) zueinander isomorphe Unterräume von V bzw. von K^m. Nach Folgerung 18.8 haben sie also dieselbe Dimension. □

Bemerkung 19.10 (zur Bestimmung von Bild und Kern einer Matrix)**.**
Wie können wir für eine gegebene Matrix $A \in K^{n\times m}$ eine Basis von $\mathrm{Bild}(A) \subseteq K^n$ und eine Basis von $\mathrm{Kern}(A) \subseteq K^m$ bestimmen?

(*i*) Für $\mathrm{Bild}(A)$ haben wir folgende Möglichkeiten:

(1) Wir bestimmen mit Hilfe einer Erweiterung von Algorithmus 15.20, wie in Bemerkung 15.23 beschrieben, eine Rangfaktorisierung $A = B\,C$ mit $B \in K^{n\times r}$ und $C \in K^{r\times m}$ (in Zeilenstufenform) und $r = \mathrm{Rang}(A)$. Dann bilden die Spalten von B eine Basis von $\mathrm{Bild}(A) = \mathrm{SR}(A)$.

(2) Wir nutzen die Beziehung $\mathrm{Bild}(A) = \mathrm{SR}(A) = [\mathrm{ZR}(A^\mathsf{T})]^\mathsf{T}$, bringen A^T in Zeilenstufenform (Algorithmus 15.20) und erhalten somit eine Basis von $\mathrm{ZR}(A^\mathsf{T})$. Durch Transposition der Basisvektoren von $\mathrm{ZR}(A^\mathsf{T})$ bekommen wir die gesuchte Basis von $\mathrm{Bild}(A)$.

Für die Rechnung per Hand erscheint die zweite Möglichkeit günstiger, weil wir den linken Faktor „B“ nicht mitführen müssen.

(*ii*) Die Bestimmung von $\mathrm{Kern}(A) = \mathcal{L}(A, 0)$ 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 $\mathrm{Rang}(A)$ und damit auch $\dim(\mathrm{Kern}(A)) = m - \mathrm{Rang}(A)$ ablesen. Nur wenn $\dim(\mathrm{Kern}(A)) > 0$ ist, überführen wir das System weiter in die reduzierte Zeilenstufenform. Anschließend können wir nacheinander Basisvektoren von $\mathrm{Kern}(A)$ 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 Gleichungsn ausrechnen (Bemerkung 16.4 und Beispiel 16.7).

Ist die Matrix A die Darstellungsmatrix einer linearen Abbildung f, also $A = \mathcal{M}_{B_W}^{B_V}(f)$, dann erhalten wir so auch eine Basis von $\mathrm{Bild}(f)$ und von $\mathrm{Kern}(f)$. Wir müssen lediglich die Basisvektoren von $\mathrm{Bild}(A)$ als Koeffizientenvektoren bzgl. der Basis B_W und die Basisvektoren von $\mathrm{Kern}(A)$ als Koeffizientenvektoren bzgl. der Basis B_V interpretieren. △

Beispiel 19.11 (zur Bestimmung von Bild und Kern einer Matrix)**.**
Wir betrachten die Punktauswertungsabbildung

$$f : \mathbb{R}_3[t] \ni p \mapsto \begin{pmatrix} \widetilde{p}(-2) \\ \widetilde{p}(0) \\ \widetilde{p}(2) \end{pmatrix} \in \mathbb{R}^3$$

aus Beispiel 19.4. Bzgl. der Monombasis $(1,\ t,\ t^2\ t^3)$ in $\mathbb{R}_3[t]$ und der Standardbasis (e_1, e_2, e_3) in $\mathbb{R}^3$ hat dieser Homomorphismus 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 $\mathrm{Rang}(A^\mathsf{T}) = \mathrm{Rang}(A) = 3$. Die ersten drei Zeilen bilden eine Basis von $\mathrm{ZR}(A^\mathsf{T})$. Ihre Transponierten bilden also eine Basis von $\mathrm{SR}(A) = \mathrm{Bild}(A)$, d. h., wir haben

$$\mathrm{Bild}(A) = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 8 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle.$$

Da $\mathrm{Bild}(A)$ aber maximale Dimension in $\mathbb{R}^3$ hat, also $\mathrm{Bild}(A) = \mathbb{R}^3$ gilt, können wir auch jede andere Basis von $\mathbb{R}^3$ (z. B. die Standardbasis) als Basis von $\mathrm{Bild}(A)$ verwenden.

Um $\mathrm{Kern}(A)$ zu bestimmen, bringen wir $[A, 0]$ zunächst in Zeilenstufenform

$$\left[\begin{array}{cccc|c} 1 & -2 & 4 & -8 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 4 & 8 & 0 \end{array}\right] \quad \rightsquigarrow \quad \left[\begin{array}{cccc|c} 1 & -2 & 4 & -8 & 0 \\ 0 & -2 & -4 & 8 & 0 \\ 0 & 0 & 8 & 0 & 0 \end{array}\right],$$

wo wir wiederum $\text{Rang}(A) = 3$ und damit $\text{Defekt}(A) = \dim(\text{Kern}(A)) = 4 - 3 = 1$ 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

$$\text{Kern}(A) = \left\langle \begin{pmatrix} 0 \\ -4 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

ablesen.[25]

Übersetzen wir $\text{Kern}(A)$ zurück in den Vektorraum $\mathbb{R}_3[t]$, so bedeutet das nach Satz 19.9 Aussage (iii), dass wir $\begin{pmatrix} 0 \\ -4 \\ 0 \\ 1 \end{pmatrix}$ als Koeffizientenvektor bzgl. der gewählten Basis $(1,\ t,\ t^2\ t^3)$ interpretieren müssen. Es sind also genau die Vielfachen des Polynoms

$$p = 0\,1 - 4\,t + 0\,t^2 + 1\,t^3 = -4\,t + t^3,$$

die in $\text{Kern}(f)$ liegen, also die Eigenschaft besitzen, dass alle drei Punktauswertungen Null ergeben. In der Tat gilt

$$\begin{aligned} \widetilde{p}(-2) &= -4 \cdot (-2) + (-2)^3 = 0 \\ \widetilde{p}(0) &= -4 \cdot 0 + 0^3 = 0 \\ \widetilde{p}(2) &= -4 \cdot 2 + 2^3 = 0. \end{aligned}$$

Wir haben also

$$\text{Kern}(f) = \langle -4\,t + t^3 \rangle \subseteq \mathbb{R}_3[t].$$

Für $\text{Bild}(A)$ ist in unserem Beispiel keine solche Übersetzung zurück erforderlich, denn wegen der Wahl der Standardbasis in $\mathbb{R}^3$ gilt $\text{Bild}(A) = \text{Bild}(f)$. (**Quizfrage 19.4:** Wie äußert sich das in Satz 19.9 Aussage (i)?) △

Neben den Zusammenhängen in Satz 19.9 können wir auch die Invertierbarkeit einer linearen Abbildung in Verbindung bringen mit der Invertierbarkeit ihrer Darstellungsmatrix. Wie wir aus Folgerung 18.8 wissen, müssen dazu notwendigerweise beide endlich-dimensionalen Vektorräume dieselbe Dimension besitzen (und gleichbedeutend damit die Darstellungsmatrix quadratisch sein).

Satz 19.12 (Invertierbarkeit linearer Abbildungen und ihrer Darstellungsmatrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K mit $\dim(V) = \dim(W) = n$ und $n \in \mathbb{N}$. Weiter seien $B_V = (v_1, \ldots, v_n)$ und $B_W = (w_1, \ldots, w_n)$ Basen von V bzw. von W und $f\colon V \to W$ ein Homomorphismus. Schließlich sei $A := \mathcal{M}_{B_W}^{B_V}(f) \in K^{n\times n}$ die Darstellungsmatrix von f. Dann sind äquivalent:

(i) f ist bijektiv.

(ii) $\text{Rang}(f) = n$.

(iii) $\text{Defekt}(f) = 0$.

[25] Noch geschickter wäre folgendes Vorgehen gewesen: Wir bestimmen eine (reduzierte) Zeilenstufenform von A, um damit $\text{Rang}(A)$, eine Basis von $\text{Kern}(A)$ und $\dim(\text{Kern}(A))$ zu bestimmen. Falls wie hier im Beispiel $\text{Rang}(A) = n$ gilt, können wir uns die Berechnung einer Basis von $\text{Bild}(A)$ sparen, da $\text{Bild}(A)$ den ganzen K^n ausfüllt.

(*iv*) A ist invertierbar.

(*v*) $\text{Rang}(A) = n$

(*vi*) $\text{Defekt}(A) = 0$

Ist f bijektiv, dann gilt für die Darstellungsmatrix der Inversen $f^{-1}\colon W \to V$

$$\mathcal{M}_{B_V}^{B_W}(f^{-1}) = A^{-1}. \tag{19.10}$$

Beweis. Die Äquivalenz der Aussagen (*i*) bis (*iii*) wurde in Folgerung 18.8 gezeigt. Die Äquivalenz der Aussagen (*iv*) und (*v*) wurde in Satz 15.40 gezeigt. Nach Satz 19.9 gilt $\text{Rang}(f) = \text{Rang}(A)$, also sind auch Aussagen (*ii*) und (*v*) äquivalent. Ebenfalls nach Satz 19.9 gilt $\text{Defekt}(f) = \text{Defekt}(A)$, also sind auch Aussagen (*iii*) und (*vi*) äquivalent.

Ist f bijektiv, dann gilt

$$\begin{aligned}
& f^{-1} \circ f = \text{id}_V \\
\Rightarrow\quad & \mathcal{M}_{B_V}^{B_V}(f^{-1} \circ f) = \mathcal{M}_{B_V}^{B_V}(\text{id}_V) \\
\Rightarrow\quad & \mathcal{M}_{B_V}^{B_W}(f^{-1})\, \mathcal{M}_{B_W}^{B_V}(f) = I_n \qquad \text{nach Satz 19.8 und Beispiel 19.4} \\
\Rightarrow\quad & \mathcal{M}_{B_V}^{B_W}(f^{-1})\, A = I_n.
\end{aligned}$$

Das ist nach Satz 15.42 bereits ausreichend, um

$$A^{-1} = \mathcal{M}_{B_V}^{B_W}(f^{-1}),$$

also (19.10) zu bestätigen. □

§ 19.4 Darstellungsmatrizen von Endomorphismen

Wir betrachten abschließend noch einmal die Endomorphismen eines endlich-dimensionalen Vektorraumes V über einem Körper K. $\text{End}(V, +, \cdot)$ bildet als Spezialfall von $(\text{Hom}(V, V), +, \cdot)$ natürlich einen Vektorraum (Satz 17.11). Endomorphismen können daher wie andere Homomorphismen auch mit Hilfe ihrer Darstellungsmatrix beschrieben werden. Dafür müssen wir eine Basis im Definitionsraum und eine Basis im Zielraum wählen. Obwohl Definitions- und Zielraum bei einem Endomorphismus identisch sind, heißt das nicht, dass wir dieselbe Basis wählen müssten. Es gibt aber einen guten Grund, das zu tun.

Wie wir in Satz 17.12 nachgewiesen haben, bildet $\text{End}(V, +, \circ)$ mit der Komposition $\circ$ einen Ring mit Einselement id_V. Insbesondere ist $\text{End}(V, \circ)$ eine (i. A. nicht-abelsche) Gruppe. Besitzen die Endomorphismen f und g die Darstellungsmatrizen A und B, so hätten wir gerne, dass $f \circ g$ durch die Matrix $A\,B$ dargestellt wird. Das gilt infolge von Satz 19.8 auch, allerdings nur unter der Voraussetzung, dass wir in beiden Kopien des Vektorraumes V (als Definitions- und als Zielraum) dieselbe Basis verwenden!

Unter dieser Voraussetzung gilt folgendes Resultat:

Satz 19.13 (Darstellungssatz für Endomorphismen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter sei $B_V = (v_1, \ldots, v_n)$ eine Basis von V. Dann gilt:

(*i*) Die Zuordnung

$$\mathcal{M}_{B_V}^{B_V} : (\mathrm{End}(V), +, \circ) \ni f \mapsto \mathcal{M}_{B_V}^{B_V}(f) \in (K^{n\times n}, +, \cdot) \tag{19.11}$$

eines Endomorphismus zu seiner Darstellungsmatrix ist ein Isomorphismus von Ringen mit Eins.

(*ii*) Die Abbildung

$$\mathcal{M}_{B_V}^{B_V} : (\mathrm{Aut}(V), \circ) \ni f \mapsto \mathcal{M}_{B_V}^{B_V}(f) \in (\mathrm{GL}(n, K), \cdot) \tag{19.12}$$

bildet außerdem die Untergruppe der Automorphismen von V, kurz: $\mathrm{Aut}(V)$, bijektiv auf die Untergruppe der invertierbaren $n \times n$-Matrizen, $\mathrm{GL}(n, K)$, ab.

Beweis. Aussage (*i*): Die additive Verträglichkeit von $\mathcal{M}_{B_V}^{B_V} : (\mathrm{End}(V), +, \circ) \to (K^{n\times n}, +, \cdot)$, also

$$\mathcal{M}_{B_V}^{B_V}(f + g) = \mathcal{M}_{B_V}^{B_V}(f) + \mathcal{M}_{B_V}^{B_V}(g) \quad \text{für alle } f, g \in \mathrm{End}(V),$$

folgt als Spezialfall von Satz 19.5. Die multiplikative Verträglichkeit, also

$$\mathcal{M}_{B_V}^{B_V}(f \circ g) = \mathcal{M}_{B_V}^{B_V}(f) \cdot \mathcal{M}_{B_V}^{B_V}(g) \quad \text{für alle } f, g \in \mathrm{End}(V),$$

folgt als Spezialfall von Satz 19.8. Schließlich gilt

$$\mathcal{M}_{B_V}^{B_V}(\mathrm{id}_V) = I_n,$$

siehe Beispiel 19.4.

Aussage (*ii*): Nach Satz 19.12 bildet $\mathcal{M}_{B_V}^{B_V}$ tatsächlich $(\mathrm{Aut}(V), \circ) \to (\mathrm{GL}(n, K), \cdot)$ bijektiv ab. □

Ende der Vorlesung 27

Ende der Woche 13

§ 20 Basiswechsel und Normalformen von Darstellungsmatrizen

Literatur: Fischer, Springborn, 2020, Kapitel 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

Die Darstellung eines Vektors v eines endlich-dimensional 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 und insbesondere Endomorphismen 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 die Basen wechseln?

(3) In welcher Basis hat die Darstellungsmatrix besonders einfache Gestalt, die weitergehende Struktureinsichten zulässt?

Die Beantwortung der ersten beiden Fragen gelingt mit Hilfe von **Transformationsmatrizen** für den Basiswechsel.

Definition 20.1 (Transformationsmatrix).
Es seien $(K,+,\cdot)$ ein Körper und $(V,+,\cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Es seien $B_V = (v_1,\dots,v_n)$ und $\widehat{B}_V = (\widehat{v}_1,\dots,\widehat{v}_n)$ zwei Basen von V.[26] Dann heißt

$$\mathcal{T}_{\widehat{B}_V}^{B_V} := \mathcal{M}_{\widehat{B}_V}^{B_V}(\mathrm{id}_V) \in K^{n\times n} \tag{20.1}$$

die **Transformationsmatrix des Basiswechsels**, **Übergangsmatrix** oder **Basiswechselmatrix von B_V nach $\widehat{B}_V$** (englisch: transformation matrix, transition matrix, change-of-basis matrix). △

Die Transformationsmatrix $\mathcal{T}_{\widehat{B}_V}^{B_V}$ ist also nichts anderes als die Darstellung der Identitätsabbildung bzgl. der „alten“ Basis B_V im Definitionsraum V und der „neuen“ Basis $\widehat{B}_V$ im Zielraum V. Die Einträge t_{ij} der Transformationsmatrix $\mathcal{T}_{\widehat{B}_V}^{B_V}$ bestimmen sich daher aus den Bedingungen

$$\underbrace{\mathrm{id}_V(v_j) = v_j}_{\text{Bild des „alten“ Basisvektors } v_j \text{ unter der } \mathrm{id}_V\text{-Abbildung}} = \sum_{i=1}^{n} t_{ij}\,\widehat{v}_i \quad \text{für } j = 1,\dots,n. \tag{20.2}$$

Beispiel 20.2 (Transformationsmatrix).
Wir betrachten den Vektorraum $V = \mathbb{R}_2[t]$ der Polynome vom Höchstgrad 2 über $\mathbb{R}$ mit der „alten“ Basis $B_V = (1,\ t,\ t^2)$ und der „neuen“ Basis $\widehat{B}_V = (t^2-t+1,\ t^2+3,\ t+1)$. Dann ist die Transformationsmatrix $\mathcal{T}_{\widehat{B}_V}^{B_V} = (t_{ij})$ gegeben durch die Bedingungen

$$\begin{aligned} 1 &= t_{11}(t^2-t+1) + t_{21}(t^2+3) + t_{31}(t+1),\\ t &= t_{12}(t^2-t+1) + t_{22}(t^2+3) + t_{32}(t+1),\\ t^2 &= t_{13}(t^2-t+1) + t_{23}(t^2+3) + t_{33}(t+1), \end{aligned}$$

was durch Koeffizientenvergleich als lineares Gleichungssystem mit drei rechten Seiten

$$\begin{bmatrix} 1 & 3 & 1\\ -1 & 0 & 1\\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} t_{11} & t_{12} & t_{13}\\ t_{21} & t_{22} & t_{23}\\ t_{31} & t_{32} & t_{33} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1 \end{bmatrix}$$

geschrieben werden kann. Dessen eindeutige Lösung ist

$$\mathcal{T}_{\widehat{B}_V}^{B_V} = \begin{bmatrix} -1 & 1 & 3\\ 1 & -1 & -2\\ -1 & 2 & 3 \end{bmatrix}.$$

Zur Probe rechnen wir Beispiel 19.2 nach, in dem wir das Polynom $7t^2 - 3t + 5$ mit dem bekannten Koeffizientenvektor $x = \begin{pmatrix} 5\\ -3\\ 7 \end{pmatrix}$ bzgl. der „alten“ Basis in der „neuen“ Basis dargestellt hatten. Für den „neuen“ Koeffizientenvektor gilt

$$\widehat{x} = \mathcal{T}_{\widehat{B}_V}^{B_V} x = \begin{bmatrix} -1 & 1 & 3\\ 1 & -1 & -2\\ -1 & 2 & 3 \end{bmatrix} \begin{pmatrix} 5\\ -3\\ 7 \end{pmatrix} = \begin{pmatrix} 13\\ -6\\ 10 \end{pmatrix},$$

vgl. Beispiel 19.2. △

[26] Wir verwenden die Konvention, dass wir zumindest anfänglich die „alte“ Basis in blau und die „neue“ Basis in rot kennzeichnen.

Das folgende Resultat beantwortet insbesondere die Frage (1).

Lemma 20.3 (Eigenschaften von Transformationsmatrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Es seien $B_V = (v_1, \ldots, v_n)$ und $\widehat{B}_V = (\widehat{v}_1, \ldots, \widehat{v}_n)$ zwei Basen von V. Dann gilt:

(*i*) Ist $x \in K^n$ der Koordinatenvektor eines Vektors $v \in V$ bzgl. der Basis B_V, dann ist $\widehat{x} = \mathcal{T}_{\widehat{B}_V}^{B_V} x$ der Koordinatenvektor von v bzgl. der Basis $\widehat{B}_V$.[27]

(*ii*) Die Transformationsmatrix $\mathcal{T}_{\widehat{B}_V}^{B_V} \in K^{n \times n}$ ist invertierbar.

(*iii*) $\left(\mathcal{T}_{\widehat{B}_V}^{B_V}\right)^{-1} = \mathcal{T}_{B_V}^{\widehat{B}_V}$.

(*iv*) Die von der Matrix $\mathcal{T}_{\widehat{B}_V}^{B_V}$ induzierte lineare Abbildung $K^n \to K^n$ ist $\Phi_{\widehat{B}_V}^{-1} \circ \Phi_{B_V} \in \mathrm{Aut}(K^n)$.

Beweis. Aussage (*i*): Es gilt

$$
\begin{aligned}
v &= \sum_{j=1}^{n} x_j v_j && \text{nach Voraussetzung} \\
&= \sum_{j=1}^{n} x_j \sum_{i=1}^{n} t_{ij} \widehat{v}_i && \text{nach (20.2)} \\
&= \sum_{i=1}^{n} \underbrace{\sum_{j=1}^{n} (t_{ij} x_j)}_{\text{Koeffizient } \widehat{x}_i \text{ bzgl. der Basis } \widehat{B}_V = (\widehat{v}_1, \ldots, \widehat{v}_n)} \widehat{v}_i && \text{wegen Distributivität und Kommutativität im Körper } K.
\end{aligned}
$$

Nach Definition des Matrix-Vektor-Produkts (Bemerkung 15.9) gilt also $\widehat{x} = \mathcal{T}_{\widehat{B}_V}^{B_V} x$.

Aussage (*ii*): Die Invertierbarkeit von $\mathcal{T}_{\widehat{B}_V}^{B_V}$ folgt aus Satz 19.12, da $\mathcal{T}_{\widehat{B}_V}^{B_V}$ die Darstellungsmatrix des bijektiven Homomorphismus $\mathrm{id}_V : V \to V$ ist.

Aussage (*iii*): Die Eigenschaft $\left(\mathcal{T}_{\widehat{B}_V}^{B_V}\right)^{-1} = \mathcal{T}_{B_V}^{\widehat{B}_V}$ folgt ebenfalls aus Satz 19.12, denn es gilt

$$
\begin{aligned}
\mathcal{T}_{B_V}^{\widehat{B}_V} &= \mathcal{M}_{B_V}^{\widehat{B}_V}(\mathrm{id}_V) && \text{nach Definition von Transformationsmatrizen} \\
&= \mathcal{M}_{B_V}^{\widehat{B}_V}((\mathrm{id}_V)^{-1}) && \mathrm{id}_V \text{ ist selbstinvers} \\
&= \left(\mathcal{M}_{\widehat{B}_V}^{B_V}(\mathrm{id}_V)\right)^{-1} && \text{nach Satz 19.12, (19.10)} \\
&= \left(\mathcal{T}_{\widehat{B}_V}^{B_V}\right)^{-1} && \text{nach Definition von Transformationsmatrizen.}
\end{aligned}
$$

Aussage (*iv*): Mit $A := \mathcal{T}_{\widehat{B}_V}^{B_V}$ ist folgendes Diagramm kommutativ (vgl. Satz 19.7):

[27] Beachte das Muster $\widehat{x} = \mathcal{T}_{\widehat{B}_V}^{B_V} x$ mit alter und neuer Basis und zugehörigen Koeffizientenvektoren.

$$\begin{array}{ccc} V & \xleftarrow{\mathrm{id}_V} & V \\ {\scriptstyle \Phi^{-1}_{\widehat{B}_V}}\downarrow & & \uparrow{\scriptstyle \Phi_{B_V}} \\ K^n & \xleftarrow[f_A]{} & K^n \end{array}$$

Also ist

$$f_A = \Phi^{-1}_{\widehat{B}_V} \circ \mathrm{id}_V \circ \Phi_{B_V} = \underbrace{\Phi^{-1}_{\widehat{B}_V}}_{\text{„neue“ Koordinaten} \mapsto \text{Vektor}} \circ \underbrace{\Phi_{B_V}}_{\text{Vektor} \mapsto \text{„alte“ Koordinaten}}$$

die von A induzierte Abbildung $K^n \to K^n$. □

Folgerung 20.4 (Eigenschaften von Transformationsmatrizen in K^n)**.**
Im Fall $V = K^n$ können wir die Basen $B_V = (v_1, \dots, v_n)$ und $\widehat{B}_V = (\widehat{v}_1, \dots, \widehat{v}_n)$ als Matrizen

$$B_V = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix} \quad \text{und} \quad \widehat{B}_V = \begin{bmatrix} | & & | \\ \widehat{v}_1 & \cdots & \widehat{v}_n \\ | & & | \end{bmatrix}$$

in $K^{n\times n}$ auffassen. Dann gilt

$$\mathcal{T}^{B_V}_{\widehat{B}_V} = \left(\widehat{B}_V\right)^{-1} B_V. \tag{20.3}$$

Ist insbesondere eine der Basen die Standardbasis $(e_1, \dots, e_n)$, so gilt

$$\mathcal{T}^{B_V}_{(e_1,\dots,e_n)} = B_V \quad \text{bzw.} \quad \mathcal{T}^{(e_1,\dots,e_n)}_{\widehat{B}_V} = \left(\widehat{B}_V\right)^{-1}. \tag{20.4}$$

Beweis. In diesem Fall gilt $f^{-1}_{B_V} = \Phi_{B_V}$ und $f^{-1}_{\widehat{B}_V} = \Phi_{\widehat{B}_V}$ (**Quizfrage 20.1:** Warum?), also können wir das Diagramm aus dem Beweis von Lemma 20.3 schreiben als

$$\begin{array}{ccc} K^n & \xleftarrow{\mathrm{id}_{K^n}} & K^n \\ {\scriptstyle \Phi^{-1}_{\widehat{B}_V} = f^{-1}_{\widehat{B}_V}}\downarrow & & \uparrow{\scriptstyle \Phi_{B_V} = f_{B_V}} \\ K^n & \xleftarrow[f_A]{} & K^n \end{array}$$

Wir erhalten

$$\begin{aligned} f_A &= \Phi^{-1}_{\widehat{B}_V} \circ \Phi_{B_V} && \text{nach Lemma 20.3 } (iv) \\ &= f^{-1}_{\widehat{B}_V} \circ f_{B_V} && \text{denn } f_{B_V} = \Phi_{B_V} \text{ und } f_{\widehat{B}_V} = \Phi_{\widehat{B}_V} \\ &= f_{(\widehat{B}_V)^{-1}} \circ f_{B_V} && \text{nach Lemma 17.9} \\ &= f_{(\widehat{B}_V)^{-1} B_V} && \text{nach Lemma 17.9.} \end{aligned}$$

Weil f_A die Matrix A eindeutig festlegt (nochmal Lemma 17.9), folgt $\mathcal{T}^{B_V}_{\widehat{B}_V} = A = (\widehat{B}_V)^{-1} B_V$, also (20.3).
Die Spezialfälle (20.4) gelten, weil die zur Standardbasis gehörige Matrix $\widehat{B}_V$ bzw. B_V die Einheitsmatrix ist. □

Beispiel 20.5 (Transformationsmatrizen in K^n).
Wir wollen im Raum $V = \mathbb{R}^2$ über dem Körper $\mathbb{R}$ die Transformationsmatrix $\mathcal{T}_{\widehat{B}_V}^{B_V}$ von der Basis $B_V = \left(\binom{-1}{1}, \binom{1}{1}\right)$ zur Basis $\widehat{B}_V = \left(\binom{2}{-1}, \binom{1}{-1}\right)$ finden. Nach (20.3) gilt

$$\mathcal{T}_{\widehat{B}_V}^{B_V} = \begin{bmatrix} 2 & 1 \\ -1 & -1 \end{bmatrix}^{-1} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & -2 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -1 & -3 \end{bmatrix}. \qquad \triangle$$

§ 20.1 Transformation der Darstellungsmatrizen von Homomorphismen

Wir kommen nun zur Frage (2).

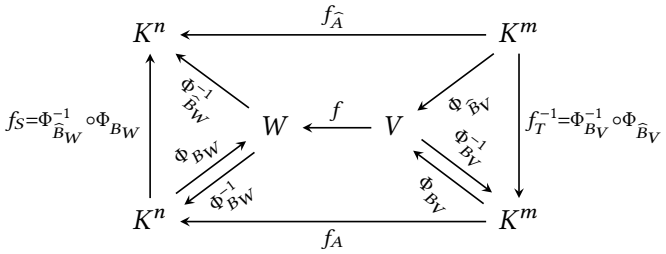
Satz 20.6 (Transformation der Darstellungsmatrix eines Homomorphismus beim Wechsel der Basen).
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K. Weiter seien B_V und $\widehat{B}_V$ Basen von V sowie B_W und $\widehat{B}_W$ Basen von W. Dann gilt für die Darstellungsmatrix eines Homomorphismus $f\colon V \to W$:[28]

$$\mathcal{M}_{\widehat{B}_W}^{\widehat{B}_V}(f) = \mathcal{T}_{\widehat{B}_W}^{B_W} \, \mathcal{M}_{B_W}^{B_V}(f) \, \mathcal{T}_{B_V}^{\widehat{B}_V}. \tag{20.5}$$

Beweis. Wir setzen zur Abkürzung

$$\begin{aligned} T &:= \mathcal{T}_{\widehat{B}_V}^{B_V} && \text{Übergang von } B_V \text{ nach } \widehat{B}_V, \\ \text{also } T^{-1} &= \mathcal{T}_{B_V}^{\widehat{B}_V} && \text{Übergang von } \widehat{B}_V \text{ nach } B_V, \\ A &:= \mathcal{M}_{B_W}^{B_V}(f) && \text{„alte“ Darstellungsmatrix von } f, \\ S &:= \mathcal{T}_{\widehat{B}_W}^{B_W} && \text{Übergang von } B_W \text{ nach } \widehat{B}_W, \\ \widehat{A} &:= \mathcal{M}_{\widehat{B}_W}^{\widehat{B}_V}(f) && \text{„neue“ Darstellungsmatrix von } f. \end{aligned}$$

Wir betrachten das Diagramm



Das obere und das untere Trapez sind kommutativ nach Satz 19.7. Das linke Dreieck und das rechte Dreieck sind kommutativ nach Lemma 20.3. Damit kommutiert auch das äußere Rechteck, d. h., es gilt

$$f_{\widehat{A}} = f_S \circ f_A \circ f_T^{-1} = f_S \circ f_A \circ f_{T^{-1}} = f_{S\,A\,T^{-1}}.$$

Das heißt nach Lemma 17.9 aber gerade

$$\widehat{A} = S\,A\,T^{-1}, \tag{20.6}$$

also die Behauptung (20.5). □

[28] Die Farben deuten wieder den Übergang von den „alten“ Basen zu den „neuen“ Basen an.

Beispiel 20.7 (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 die Darstellungsmatrix $\mathcal{M}_{(e_1,e_2,e_3)}^{(e_1,e_2)}(f_A)$ bzgl. der Standardbasen in $\mathbb{R}^2$ und $\mathbb{R}^3$. Wir wollen die Darstellungsmatrix 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

$$\widehat{A} = \mathcal{M}_{\widehat{B}_W}^{\widehat{B}_V}(f_A) = S\,A\,T^{-1}$$

bestimmen. Es gilt

$$T^{-1} \coloneqq \mathcal{T}_{(e_1,e_2)}^{\widehat{B}_V} = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$$

und

$$S \coloneqq \mathcal{T}_{\widehat{B}_W}^{(e_1,e_2,e_3)} = \left[\mathcal{T}_{(e_1,e_2,e_3)}^{\widehat{B}_W}\right]^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}^{-1} = \frac{1}{2}\begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}.$$

Wir erhalten also die transfomierte Darstellungsmatrix bzgl. der neuen Basen gemäß (20.5)

$$\widehat{A} = S\,A\,T^{-1} = \frac{1}{2}\begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}\begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 7 \\ 1 & 15 \end{bmatrix}. \qquad \triangle$$

Definition 20.8 (Äquivalenztransformation, äquivalente Matrizen)**.**
Es seien $(K, +, \cdot)$ 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:

$$\widehat{A} = S\,A\,T^{-1}. \tag{20.7}$$

Der Übergang von A zu $S\,A\,T^{-1}$, 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 $K^{n\times m}$.

Satz 20.9 (über äquivalente Matrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper, $n, m \in \mathbb{N}_0$ und $A, \widehat{A} \in K^{n\times m}$. Weiter seien V und W zwei Vektorräume über K mit $\dim(V) = m$ und $\dim(W) = n$ und B_V eine Basis von V, B_W eine Basis von W und $f\colon V \to W$ ein Homomorphismus und $A = \mathcal{M}_{B_W}^{B_V}(f)$.[29] Dann sind äquivalent:

(*i*) A und $\widehat{A}$ sind äquivalente Matrizen.

(*ii*) $\widehat{A}$ ist die Darstellungsmatrix von f bzgl. geeigneter Basen $\widehat{B}_V$ und $\widehat{B}_W$.

[29] Diese Voraussetzung ist nicht einschränkend. Zu einer gegebenen Matrix A können wir immer $V = K^m$, $W = K^n$, B_V und B_W als die Standardbasisen und $f = f_A$ wählen.

(*iii*) Es gilt $\operatorname{Rang}(A) = \operatorname{Rang}(\widehat{A})$.

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 $\widehat{A} = S\,A\,T^{-1}$ gilt. Wir können T^{-1} als Transformationsmatrix eines Basiswechsels $T^{-1} = \mathcal{T}_{B_V}^{\widehat{B}_V}$ auffassen, indem wir die „neue“ Basis von V durch

$$\widehat{v}_j = \sum_{i=1}^{m} [T^{-1}]_{ij}\, v_i \quad \text{für } j = 1, \dots, m$$

definieren, vgl. (20.2). Ebenso können wir S als Transformationsmatrix eines Basiswechsels $S = \mathcal{T}_{\widehat{B}_W}^{B_W}$ auffassen, indem wir die „neue“ Basis von W durch

$$\widehat{w}_j = \sum_{i=1}^{n} [S^{-1}]_{ij}\, w_i \quad \text{für } j = 1, \dots, n$$

definieren. Wir sehen jetzt

$$\begin{aligned}
f_{\widehat{A}} &= f_{S\,A\,T^{-1}} && \text{nach Voraussetzung}\\
&= f_S \circ f_A \circ f_{T^{-1}} && \text{nach Lemma 17.9}\\
&= f_S \circ \Phi_{B_W}^{-1} \circ f \circ \Phi_{B_V} \circ f_{T^{-1}} && \text{nach Satz 19.7}\\
&= \Phi_{\widehat{B}_W}^{-1} \circ \Phi_{B_W} \circ \Phi_{B_W}^{-1} \circ f \circ \Phi_{B_V} \circ \Phi_{B_V}^{-1} \circ \Phi_{\widehat{B}_V} && \text{nach Lemma 20.3}\\
&= \Phi_{\widehat{B}_W}^{-1} \circ f \circ \Phi_{\widehat{B}_V}.
\end{aligned}$$

Das bedeutet wiederum nach Satz 19.7 aber, dass $\widehat{A}$ die Darstellungsmatrix von f bzgl. der „neuen“ Basen $\widehat{V}$ und $\widehat{W}$ ist.

Aussage (*ii*) ⇒ Aussage (*i*): Das folgt sofort aus Satz 20.6.

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 $\widehat{A} = S\,A\,T^{-1}$ gilt. Nach Folgerung 15.41 gilt $\operatorname{Rang}(\widehat{A}) = \operatorname{Rang}(A)$.

Aussage (*iii*) ⇒ Aussage (*i*): Wir betrachten $f_A \colon K^m \to K^n$. Nach Satz 19.9 gilt $\operatorname{Rang}(f_A) = \operatorname{Rang}(A)$. Gemäß Beispiel 19.4 können wir eine Basis B von K^m und eine Basis C von K^n finden, sodass

$$\begin{aligned}
\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] &= \mathcal{M}_B^C(f_A)\\
&= \mathcal{T}_C^{(e_1,\dots,e_n)}\, \mathcal{M}_{(e_1,\dots,e_n)}^{(e_1,\dots,e_m)}(f_A)\, \mathcal{T}_{(e_1,\dots,e_m)}^{B}\\
&= \underbrace{\mathcal{T}_C^{(e_1,\dots,e_n)}}_{=:S}\, A\, \underbrace{\mathcal{T}_{(e_1,\dots,e_m)}^{B}}_{=:T^{-1}}\\
&= S\,A\,T^{-1}
\end{aligned}$$

mit invertierbaren Matrizen $S \in K^{n\times n}$ und $T \in K^{m\times m}$ gilt. Dasselbe Argument können wir für $f_{\widehat{A}}$ verwenden, um zu zeigen, dass es Matrizen $\widehat{S}$ und $\widehat{T}$ gibt, sodass

$$\left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] = \widehat{S}\,\widehat{A}\,\widehat{T}^{-1}$$

gilt. Zusammen also:

$$\widehat{A} = (\widehat{S}^{-1} S)\, A\, (T^{-1}\, \widehat{T}).$$

Da die Produkte $\widehat{S}^{-1}S$ und $T^{-1}\widehat{T}$ wieder invertierbare Matrizen sind, folgt die Äquivalenz von A und $\widehat{A}$. □

Bemerkung 20.10 (über äquivalente Matrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$, $(W, +, \cdot)$ zwei endlich-dimensionale Vektorräume über K mit $\dim(V) = m$ und $\dim(W) = n$. Der Satz 20.9 bedeutet, folgendes Diagramm kommutiert:

$$\begin{array}{ccc} \mathrm{Hom}(V,W) & \xrightarrow[\text{isomorph}]{\mathcal{M}_{B_W}^{B_V}} & K^{n\times m} \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi} \\ \mathrm{Hom}(V,W)\,/\sim_{\mathrm{Rang}} & \underset{\mathcal{M}_{B_W}^{B_V}}{\xrightarrow{\text{bijektiv}}} & K^{n\times m}\,/\sim_{\mathrm{Rang}} \end{array}$$

Dabei ist auf der linken Seite des Diagramms $\sim_{\mathrm{Rang}}$ die Äquivalenzrelation „gleicher Rang“ auf $\mathrm{Hom}(V, W)$ mit den Äquivalenzklassen

$$[f] := \big\{ g \in \mathrm{Hom}(V,W) \,\big|\, \mathrm{Rang}(g) = \mathrm{Rang}(f) \big\}.$$

Weiter ist $\mathrm{Hom}(V, W) / \sim_{\mathrm{Rang}}$ die zugehörige Faktormenge (Menge aller Äquivalenzklassen) und π die kanonische Surjektion $f \mapsto [f]$. (**Quizfrage 20.2:** Wieviele Äquivalenzklassen gibt es?)

Auf der rechten Seite des Diagramms ist $\sim_{\mathrm{Rang}}$ die Äquivalenzrelation „gleicher Rang“ auf $K^{n,m}$ mit den Äquivalenzklassen

$$\begin{aligned} [A] &:= \big\{ \widehat{A} \in K^{n\times m} \,\big|\, \mathrm{Rang}(\widehat{A}) = \mathrm{Rang}(A) \big\} \\ &= \big\{ \widehat{A} \in K^{n\times m} \,\big|\, \widehat{A} \text{ ist äquivalent zu } A \big\} \\ &= \big\{ S\,A\,T^{-1} \,\big|\, S \in K^{n\times n} \text{ und } T \in K^{m\times m} \text{ sind invertierbar} \big\}. \end{aligned}$$

Weiter ist $K^{n\times m} / \sim_{\mathrm{Rang}}$ die zugehörige Faktormenge und π die kanonische Surjektion $A \mapsto [A]$.

Nach Satz 20.9 bildet $\mathcal{M}_{B_W}^{B_V}$ eine gesamte Äquivalenzklasse von $\mathrm{Hom}(V, W)$ auf eine Äquivalenzklasse von $K^{n\times m}$ ab, und verschiedene Äquivalenzklassen von $\mathrm{Hom}(V, W)$ 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 $\mathrm{Hom}(V, W)$ eine sogenannte **glatte Mannigfaltigkeit** (englisch: smooth manifold).[30] Ebenso ist jede Äquivalenzklasse $[A]$ von $K^{n\times m}$ eine glatte Mannigfaltigkeit, und die Abbildung $\mathcal{M}_{B_W}^{B_V}$ ist ein **Diffeomorphismus** zwischen $[f]$ und $[A]$ mit $\mathrm{Rang}(f) = \mathrm{Rang}(A)$. △

Folgerung 20.11 (Normalform der Darstellungsmatrix eines Homomorphismus)**.**
Es seien $(K, +, \cdot)$ ein Körper, $n, m \in \mathbb{N}_0$ und $A \in K^{n\times m}$ mit $\mathrm{Rang}(A) = r$. Dann existieren reguläre Matrizen $S \in K^{n\times n}$ und $T \in K^{m\times m}$, sodass gilt:

$$S\,A\,T^{-1} = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right] \in K^{n\times m}. \tag{20.8}$$

[30] Über solche Strukturen erfahren Sie mehr in Vorlesungen über Differentialgeometrie.

Beweis. Dieses Resultat wurde beim Beweis von Satz 20.9 Aussage (*iii*) ⇒ Aussage (*i*) gezeigt; siehe auch Beispiel 19.4. □

Wir nennen die zu A äquivalente Matrix (20.8) die **Rang-Normalform** (englisch: rank normal form) von A. Sie ist eindeutig bestimmt. Eine Matrix in Rang-Normalform kann als natürlicher Repräsentant ihrer Äquivalenzklasse bzgl. der Äquivalenzrelation „gleicher Rang“ angesehen werden. Damit haben wir für allgemeine Homomorphismen auch die Frage (3) beantwortet.

Ende der Vorlesung 28

§ 20.2 Transformation der Darstellungsmatrizen von Endomorphismen

In § 19.4 hatten wir gesehen, dass es sinnvoll ist, bei der Darstellung von Endomorphismen $f\colon V \to V$ eines endlich-dimensionalen Vektorraumes V durch Darstellungsmatrizen im Definitions- und im Zielraum zweimal dieselbe Basis B_V zu verwenden. (**Quizfrage 20.3:** Was war nochmal der Grund dafür?)

Analog zum Transformationssatz für Darstellungsmatrizen von Homomorphismen 20.6 erhalten wir also als Sonderfall folgende Variante für Endomorphismen:

Satz 20.12 (Transformation der Darstellungsmatrix eines Endomorphismus beim Wechsel der Basis)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein endlich-dimensionaler Vektorraum über K. Weiter seien B_V und $\widehat{B}_V$ Basen von V. Dann gilt für die Darstellungsmatrix eines Endomorphismus $f\colon V \to V$:[31]

$$\mathcal{M}_{\widehat{B}_V}^{\widehat{B}_V}(f) = \mathcal{T}_{\widehat{B}_V}^{B_V}\, \mathcal{M}_{B_V}^{B_V}(f)\, \mathcal{T}_{B_V}^{\widehat{B}_V}. \tag{20.9}$$

Das bedeutet, dass wir mit der Notation aus § 20.1

$$\begin{aligned} T &:= \mathcal{T}_{\widehat{B}_V}^{B_V} && \text{Übergang von } B_V \text{ nach } \widehat{B}_V, \\ \text{also } T^{-1} &= \mathcal{T}_{B_V}^{\widehat{B}_V} && \text{Übergang von } \widehat{B}_V \text{ nach } B_V, \\ A &:= \mathcal{M}_{B_V}^{B_V}(f) && \text{„alte“ Darstellungsmatrix von } f, \\ \widehat{A} &:= \mathcal{M}_{\widehat{B}_V}^{\widehat{B}_V}(f) && \text{„neue“ Darstellungsmatrix von } f, \end{aligned}$$

die Beziehung

$$\widehat{A} = T\,A\,T^{-1} \tag{20.10}$$

erhalten.

Definition 20.13 (Ähnlichkeitstransformation, ähnliche Matrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}_0$. Zwei Matrizen $A, \widehat{A} \in K^{n\times n}$ heißen **ähnlich** (englisch: similar), wenn es eine invertierbare Matrix $T \in K^{n\times n}$ gibt, sodass gilt:

$$\widehat{A} = T\,A\,T^{-1}. \tag{20.11}$$

Der Übergang von A zu $T\,A\,T^{-1}$, also die Multiplikation von links und von rechts einmal mit einer invertierbaren Matrix und einmal mit ihrer Inversen, heißt auch eine **Ähnlichkeitstransformation** (englisch: similarity transformation) von A. △

[31] Die Farben deuten wieder den Übergang von der „alten“ Basis zur „neuen“ Basis an.

Beachte: Die Ähnlichkeit von Matrizen ist eine Äquivalenzrelation auf der Menge $K^{n\times n}$.

Analog zu Satz 20.9 halten wir fest:

Satz 20.14 (über ähnliche Matrizen)**.**
Es seien $(K,+,\cdot)$ ein Körper, $n \in \mathbb{N}_0$ und $A, \widehat{A} \in K^{n\times n}$. Weiter sei V ein Vektorraum über K mit $\dim(V) = n$ und B_V eine Basis von V, $f\colon V \to V$ ein Endomorphismus und $A = \mathcal{M}_{B_V}^{B_V}(f)$.[32] Dann sind äquivalent:

(*i*) A und $\widehat{A}$ sind ähnliche Matrizen.

(*ii*) $\widehat{A}$ ist die Darstellungsmatrix von f bzgl. einer geeigneten Basis $\widehat{B}_V$.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*): Der Beweis ist ein Spezialfall des entsprechenden Beweisschrittes von Satz 20.9.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Das folgt sofort aus Satz 20.12. □

Es stellt sich an dieser Stelle allerdings die Frage, ob wir nicht zusätzlich zu der relativ offensichtlichen Aussage von Satz 20.14 noch eine vergleichbar einfache Charakterisierung der Ähnlichkeit zweier Matrizen finden können, wie es mit der Ranggleichheit bei der Äquivalenz in Satz 20.9 der Fall war. Es stellt sich allerdings heraus, dass es bei der Ähnlichkeit von Matrizen auf sehr viel komplexere Struktur des dargestellten Endomorphismus ankommt, als das beim Rang einer Matrix bzw. dem Rang des dargestellten Homomorphismus der Fall war. Auch die Frage (3) nach einer geeigneten Basis, bzgl. der die Darstellungsmatrix eines Endomorphismus eine möglichst einfache Gestalt hat, also ein Analogon zu Folgerung 20.11, ist für uns noch offen. Da diese Frage eng mit der Charakterisierung der Ähnlichkeit zusammenhängt, ist auch hier die Beantwortung deutlich schwieriger als bei der Rang-Normalform von Homomorphismen. Ein weiterer Hinweis darauf wird durch die Tatsache gegeben, dass wir zur Herstellung einer wie auch immer gearteten einfachen Form der Darstellungsmatrix jetzt nur noch eine Basis, also nur noch eine Transformationsmatrix zur Verfügung haben, um $T\,A\,T^{-1}$ in möglichst einfache Form zu bringen.

Wir werden die gerade gestellten Fragen erst im zweiten Teil der Vorlesung vollständig beantworten können. Wir wollen hier jedoch schon einige Überlegungen dazu anstellen und können zumindest für eine Teilmenge von Matrizen bereits jetzt eine Charakterisierung der Ähnlichkeit erreichen. Dazu führen wir zunächst einen neuen Begriff ein.

Definition 20.15 (invarianter Unterraum eines Endomorphismus bzw. einer Matrix)**.**

(*i*) Es seien $(K,+,\cdot)$ ein Körper und $(V,+,\cdot)$ ein Vektorraum über K. Weiter sei $f\colon V \to V$ ein Endomorphismus. Ein Unterraum $U \subseteq V$ heißt ein **f-invarianter Unterraum** (englisch: f-invariant subspace), wenn gilt:

$$f(U) \subseteq U. \tag{20.12}$$

(*ii*) Es seien $(K,+,\cdot)$ ein Körper und $A \in K^{n\times n}$ eine Matrix mit $n \in \mathbb{N}_0$. Ein Unterraum $U \subseteq K^n$ heißt ein **A-invarianter Unterraum**, wenn gilt:[33]

$$f_A(U) \subseteq U. \tag{20.13}$$

△

[32] Diese Voraussetzung ist nicht einschränkend. Zu einer gegebenen Matrix A können wir immer $V = K^n$, B_V als die Standardbasis und $f = f_A$ wählen.

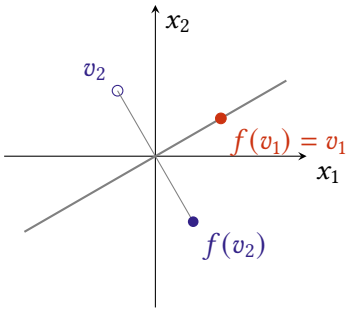
[33] Mit anderen Worten: $\{A\,x \mid x \in U\} \subseteq U$ oder kurz: $A \cdot U \subseteq U$.

Vektoren u in einem f-invarianten Unterraum U haben also die Eigenschaft, dass sie durch f wieder auf einen Vektor $f(u) \in U$ abgebildet werden (auch bei wiederholter Anwendung von f).

Beispiel 20.16 (invarianter Unterraum eines Endomorphismus)**.**

(*i*) In jedem Vektorraum V sind die trivialen Unterräume $\{0\}$ und V invariante Unterräume für jeden Endomorphismus $f\colon V \to V$.

(*ii*) Die Spiegelungsabbildung an einer Achse in $\mathbb{R}^2$ aus Beispiel 17.8 hat zwei verschiedene eindimensionale invariante Unterräume, wie wir uns grafisch überlegen können:



Der Vektor $v_1 = \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix}$ wird durch das Matrix-Vektor-Produkt mit der Darstellungsmatrix

$$\begin{aligned}
&\begin{bmatrix} \cos^2(\alpha) - \sin^2(\alpha) & 2\cos(\alpha)\,\sin(\alpha) \\ 2\cos(\alpha)\,\sin(\alpha) & \sin^2(\alpha) - \cos^2(\alpha) \end{bmatrix} \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} \\
&\quad = \begin{pmatrix} \cos^3(\alpha) - \sin^2(\alpha)\,\cos(\alpha) + 2\cos(\alpha)\,\sin^2(\alpha) \\ 2\cos^2(\alpha)\,\sin(\alpha) + \sin^3(\alpha) - \cos^2(\alpha)\,\sin(\alpha) \end{pmatrix} = \begin{pmatrix} \cos(\alpha)\big[\cos^2(\alpha) + \sin^2(\alpha)\big] \\ \sin(\alpha)\big[\cos^2(\alpha) + \sin^2(\alpha)\big] \end{pmatrix} \\
&\quad = \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix}
\end{aligned}$$

tatsächlich auf sich selbst abgebildet, während für das Bild des Vektors $v_2 = \begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix}$

$$\begin{aligned}
&\begin{bmatrix} \cos^2(\alpha) - \sin^2(\alpha) & 2\cos(\alpha)\,\sin(\alpha) \\ 2\cos(\alpha)\,\sin(\alpha) & \sin^2(\alpha) - \cos^2(\alpha) \end{bmatrix} \begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix} \\
&\quad = \begin{pmatrix} -\cos^2(\alpha)\,\sin(\alpha) + \sin^3(\alpha) + 2\cos^2(\alpha)\,\sin(\alpha) \\ -2\cos(\alpha)\,\sin^2(\alpha) + \sin^2(\alpha)\cos(\alpha) - \cos^3(\alpha) \end{pmatrix} = \begin{pmatrix} \sin(\alpha)\big[\cos^2(\alpha) + \sin^2(\alpha)\big] \\ \cos(\alpha)\big[\cos^2(\alpha) + \sin^2(\alpha)\big] \end{pmatrix} \\
&\quad = \begin{pmatrix} \sin(\alpha) \\ \cos(\alpha) \end{pmatrix}
\end{aligned}$$

gilt, d. h., $f(v_2) = -v_2$. Die Unterräume $U_1 = \langle v_1 \rangle$ und $U_2 = \langle v_2 \rangle$ sind also in der Tat zwei verschiedene eindimensionale invariante Unterräume der Spiegelungsabbildung (**Quizfrage 20.4:** klar?). Wegen $U_1 \cap U_2 = \{0\}$ gilt $\mathbb{R}^2 = U_1 \oplus U_2$. In diesem Beispiel kann also der gesamte Vektorraum als direkte Summe invarianter Unterräume des Endomorphismus „Spiegelung“ geschrieben werden.

(*iii*) Für die Ableitungsabbildung als Endomorphismus $f\colon K[t] \to K[t]$ (Beispiel 18.9) sind die invarianten Unterräume genau die Unterräume von der Form $\langle 1, t, t^2, \ldots, t^k \rangle = K_k[t]$ für $k \in \mathbb{N}_0$ bzw. der Nullraum. (**Quizfrage 20.5:** Warum?) Wenn wir die Ableitungsabbildung einschränken auf den Polynomraum vom Höchstgrad $n \in \mathbb{N}_0$, also $f\colon K_n[t] \to K_n[t]$, dann sind die invarianten Unterräume noch immer genau die Unterräume der Form $K_k[t]$ für $k \in \mathbb{N}_0$ bzw. der Nullraum. In diesem Beispiel ist also keine Zerlegung des Vektorraumes $K_n[t]$ in eine direkte Summe verschiedener invarianter Unterräume möglich. △

Wenn wir für den Moment annehmen, dass $f\colon V \to V$ ein Endomorphismus auf einem Vektorraum V mit $\dim(V) = n \geqslant 2$ ist und U ein nicht-trivialer f-invarianter Unterraum, d. h., $\dim(U) = k$ mit $1 \leqslant k \leqslant n-1$, dann können wir eine Basis der Form

$$B_V = (\underbrace{v_1, \dots, v_k}_{\text{Basis von } U}, \underbrace{v_{k+1}, \dots, v_n}_{\text{Basis eines zu } U \text{ komplementären Unterraumes } W})$$

verwenden, also $V = U \oplus W$ zerlegen. Bzgl. dieser Basis hat die Darstellungsmatrix von f die Gestalt

$$\mathcal{M}_{B_V}^{B_V}(f) = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline 0 & A_{22} \end{array}\right] \begin{matrix} k \\ n-k \end{matrix}$$

mit den angegebenen Dimensionen der Blöcke. An der Struktur der Matrix sieht man sehr schön, dass f auf dem Unterraum U „isoliert“ wirkt, dass also die Einschränkung $f|_U^U$ definiert ist.

Ist zusätzlich auch der zu U komplementäre Unterraum W ein f-invarianter Unterraum, gilt also $f(W) \subseteq W$, dann ist die Darstellungsmatrix von f eine **Blockdiagonalmatrix** (englisch: block diagonal matrix)

$$\mathcal{M}_{B_V}^{B_V}(f) = \left[\begin{array}{c|c} A_{11} & 0 \\ \hline 0 & A_{22} \end{array}\right] \begin{matrix} k \\ n-k \end{matrix}.$$

Hier wirkt also f nun in beiden Unterräumen „isoliert“, sodass auch die Einschränkung $f|_W^W$ definiert ist.

Diese Überlegungen gelten auch für Zerlegungen des Raumes V in direkte Summen von mehr als zwei Unterräumen. Es geht also bei der Aufgabe, eine möglichst einfache Gestalt der Darstellungsmatrix eines Endomorphismus $f\colon V \to V$ zu finden, darum, möglichst niedrig-dimensionale, paarweise verschiedene f-invariante Unterräume von V zu finden, deren direkte Summe den ganzen Raum V ergibt. Der triviale Fall, als einzigen f-invarianten Unterraum V selbst zu nutzen, ist immer möglich, manchmal nicht vermeidbar, bringt aber keine strukturelle Einsicht.

Satz 20.17 (Blockdiagonalgestalt der Darstellungsmatrix eines Endomorphismus)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter sei $f\colon V \to V$ ein Endomorphismus und $N \in \mathbb{N}_0$. Dann sind äquivalent:

(i) Es existieren f-invariante Unterräume $U_1, \dots, U_N$ der Dimensionen $\dim(U_j) = n_j \in \mathbb{N}_0$, sodass gilt:

$$V = U_1 \oplus \cdots \oplus U_L. \tag{20.14}$$

(ii) Es existiert eine Basis B_V von V, sodass die Darstellungsmatrix von f die Blockdiagonalgestalt

$$\mathcal{M}_{B_V}^{B_V}(f) = \begin{bmatrix} A_{11} & & & \\ & A_{22} & & \\ & & \ddots & \\ & & & A_{N_L N_L} \end{bmatrix} \begin{matrix} n_1 \\ n_2 \\ \vdots \\ n_L \end{matrix} \qquad \begin{matrix} n_1 & n_2 & \cdots & n_L \end{matrix} \tag{20.15}$$

besitzt, wobei für die Blöcke $A_{jj} \in K^{n_j \times n_j}$, $j = 1, \dots, N$ gilt.

Beachte: Wie gesagt, der Fall $L = 1$ mit $U_1 = V$ ist immer möglich, bringt aber keine strukturelle Einsicht, da der einzige Block A_{11} in (20.15) die gesamte Matrix ist.

Beweis. □

Beispiel 20.18 (Blockdiagonalgestalt der Darstellungsmatrix eines Endomorphismus)**.**
Das Beispiel der Spiegelungsabbildung aus Beispiel 20.16 in $V = \mathbb{R}^2$ zeigt, dass es Endomorphismen gibt, die die in Satz 20.17 beschriebene Darstellung in Form einer Blockdiagonalmatrix zulassen, die nicht nur aus einem großen Block besteht. Bezüglich der Basis $B_V = \left(\begin{pmatrix}\cos(\alpha)\\ \sin(\alpha)\end{pmatrix}, \begin{pmatrix}-\sin(\alpha)\\ \cos(\alpha)\end{pmatrix}\right)$ erhalten wir für die Spiegelungsabbildung die diagonale Darstellungsmatrix (mit Blöcken der minimalen Größe $n_1 = n_2 = 1$)

$$\mathcal{M}_{B_V}^{B_V}(f) = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}. \qquad \triangle$$

Wir gehen dem in Beispiel 20.18 beobachteten bestmöglichen Fall, in dem die Darstellung eines Endomorphismus in Form einer Diagonalmatrix möglich ist, weiter nach. Dieser Fall entspricht der Zerlegung von V in die direkte Summe von $L = N$ eindimensionalen Unterräumen, sodass die Blöcke in (20.15) alle die minimale Größe 1×1 haben. Was bedeutet diese Situation für die f-invarianten Unterräume U_j?

Da U_j eindimensional ist, gibt es einen Vektor $v_j \neq 0$, sodass $U_j = \langle v_j \rangle$ gilt. Da $f(U_j) \subseteq U_j$ gilt, muss $f(v_j)$ ein Vielfaches von v_j sein. Das führt uns zu folgender Definition:

Definition 20.19 (Eigenwert, Eigenvektor eines Endomorphismus bzw. einer Matrix)**.**

(*i*) Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K. Weiter sei $f\colon V \to V$ ein Endomorphismus. Ein Vektor $v \in V \setminus \{0\}$ heißt ein **Eigenvektor** (englisch: eigenvector) zum **Eigenwert** $\lambda \in K$ **des Endomorphismus** f (englisch: eigenvalue), wenn gilt:

$$f(v) = \lambda v. \tag{20.16}$$

In diesem Fall heißt $(\lambda, v) \in K \times (V \setminus \{0\})$ auch ein **Eigenpaar des Endomorphismus** f (englisch: eigenpair).

(*ii*) Es seien $(K, +, \cdot)$ ein Körper und $A \in K^{n\times n}$ eine Matrix mit $n \in \mathbb{N}_0$. Ein Vektor $x \in K^n \setminus \{0\}$ heißt ein **Eigenvektor** zum **Eigenwert** $\lambda \in K$ **der Matrix** A, wenn gilt:

$$A x = \lambda x. \tag{20.17}$$

In diesem Fall heißt $(\lambda, x) \in K \times (K^n \setminus \{0\})$ auch ein **Eigenpaar der Matrix** A. △

Beachte: Die Eigenpaare einer Matrix $A \in K^{n\times n}$ sind per Definition genau die Eigenpaare des von A induzierten Endomorphismus $f_A\colon K^n \to K^n$.

Beachte: Die Sprechweise „$\lambda \in K$ ist ein Eigenwert des Endomorphismus $f\colon V \to V$“ bedeutet, dass es ein $v \in V \setminus \{0\}$ gibt, sodass $f(v) = \lambda v$ gilt. Analog bedeutet „$\lambda \in K$ ist ein Eigenwert der Matrix $A \in K^{n\times n}$, dass es ein $x \in K^n \setminus \{0\}$ gibt, sodass $A x = \lambda v$ gilt.“

Lemma 20.20 (Eigenpaare von Endomorphismen und ihrer Darstellungsmatrizen)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter sei $f\colon V \to V$ ein Endomorphismus und $A = \mathcal{M}_{B_V}^{B_V}(f) \in K^{n\times n}$ seine Darstellungsmatrix bzgl. einer beliebigen Basis B_V von V. Dann sind äquivalent:

(*i*) $\lambda \in K$ ist ein Eigenwert von f.

(*ii*) $\lambda \in K$ ist ein Eigenwert von A.

Weiter gilt:

(*iii*) Ist $v \in V$ ein Eigenvektor zum Eigenwert λ von f, so ist $x = \Phi_{B_V}^{-1}(v)$ ein Eigenvektor zum Eigenwert λ von A.

(*iv*) Ist $x \in K^n$ ein Eigenvektor zum Eigenwert λ von A, so ist $v = \Phi_{B_V}(x)$ ein Eigenvektor zum Eigenwert λ von f.

Beweis. Aussage (*i*) $\Rightarrow$ Aussage (*ii*) und Aussage (*iii*): Es sei $(\lambda, v) \in K \times (V \setminus \{0\})$ ein Eigenpaar von f und $x = \Phi_{B_V}^{-1}(v)$, also auch $v = \Phi_{B_V}(x)$. Dann gilt

$$\begin{aligned}
A\,x &= f_A(x) && \text{nach Definition von } f_A \\
&= (\Phi_{B_V}^{-1} \circ f \circ \Phi_{B_V})(x) && \text{nach Satz 19.7} \\
&= \Phi_{B_V}^{-1}\big(f(\Phi_{B_V}(x))\big) && \text{nach Definition der Komposition} \\
&= \Phi_{B_V}^{-1}(f(v)) && \text{wegen } v = \Phi_{B_V}(x) \\
&= \Phi_{B_V}^{-1}(\lambda\, v) && \text{wegen } f(v) = \lambda\, v \\
&= \lambda\, \Phi_{B_V}^{-1}(v) && \text{wegen der Linearität von } \Phi_{B_V}^{-1} \\
&= \lambda\, x && \text{wegen } x = \Phi_{B_V}^{-1}(v).
\end{aligned}$$

Das zeigt: $(\lambda, x) \in K \times (K^n \setminus \{0\})$ ist ein Eigenpaar von A.

Aussage (*ii*) $\Rightarrow$ Aussage (*i*) und Aussage (*iv*): Es sei $(\lambda, x) \in K \times (K^n \setminus \{0\})$ ein Eigenpaar von A und $v = \Phi_{B_V}(x)$, also auch $x = \Phi_{B_V}^{-1}(v)$. Dann gilt

$$\begin{aligned}
f(v) &= (\Phi_{B_V} \circ f_A \circ \Phi_{B_V}^{-1})(v) && \text{nach Satz 19.7} \\
&= \Phi_{B_V}\big(f_A(\Phi_{B_V}^{-1}(v))\big) && \text{nach Definition der Komposition} \\
&= \Phi_{B_V}\big(f_A(x)\big) && \text{wegen } x = \Phi_{B_V}^{-1}(v) \\
&= \Phi_{B_V}(A\,x) && \text{nach Definition von } f_A \\
&= \Phi_{B_V}(\lambda\, x) && \text{wegen } A\,x = \lambda\, x \\
&= \lambda\, \Phi_{B_V}(x) && \text{wegen der Linearität von } \Phi_{B_V} \\
&= \lambda\, v && \text{wegen } v = \Phi_{B_V}(x).
\end{aligned}$$

Das zeigt: $(\lambda, v) \in K \times (V \setminus \{0\})$ ist ein Eigenpaar von f. □

Folgerung 20.21 (ähnliche Matrizen haben dieselben Eigenwerte)**.**
Es seien $(K, +, \cdot)$ ein Körper, $n \in \mathbb{N}_0$ und $A, \widehat{A} \in K^{n\times n}$. Wenn A und $\widehat{A}$ ähnlich sind, dann besitzen sie genau dieselben Eigenwerte.

Beweis. Nach Satz 20.14 können A und $\widehat{A}$ als Darstellungsmatrizen desselben Endomorphismus $f\colon V \to V$ in einem Vektorraum V mit $\dim(V) = n$ angesehen werden. Nach Lemma 20.20 sind daher die Eigenwerte von A und auch die Eigenwerte von $\widehat{A}$ identisch mit den Eigenwerten von f. □

Beachte: Die Umkehrung von Folgerung 20.21 gilt nicht! Zwei Matrizen $A, \widehat{A} \in K^{n\times n}$, die dieselben Eigenwerte besitzen, sind also nicht notwendigerweise ähnlich zueinander.

Beispiel 20.22 (nicht-ähnliche Matrizen mit gleichen Eigenwerten)**.**
Die Matrizen

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{und} \quad \widehat{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ in } \mathbb{R}^{2\times 2}$$

besitzen beide genau die Eigenwerte $\lambda_1 = 1$ und $\lambda_2 = 1$, sie sind aber nicht ähnlich zueinander, denn der Ansatz $\widehat{A} = T\,A\,T^{-1}$ bzw. $\widehat{A}\,T = T\,A$ mit einer Matrix T führt auf

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

oder ausgeschrieben

$$\begin{bmatrix} t_{11} + t_{21} & t_{12} + t_{22} \\ t_{21} & t_{22} \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{bmatrix},$$

was notwendigerweise $t_{21} = t_{22} = 0$ ergibt. Damit hat T aber eine Nullzeile und ist nicht invertierbar. △

Wir kommen zurück zu der in Beispiel 20.18 beobachteten Situation, in der zu einem Endomorphismus (der Spiegelungsabbildung auf $\mathbb{R}^2$) eine diagonale Darstellungsmatrix existierte.

Definition 20.23 (diagonalisierbarer Endomorphismus, diagonalisierbare Matrix)**.**
Es seien $(K, +, \cdot)$ ein Körper und $n \in \mathbb{N}_0$.

(*i*) Ein Endomorphismus $f\colon V \to V$ eines Vektorraumes über K mit $\dim(V) = n$ heißt **diagonalisierbar** (englisch: diagonalizable), wenn es f-invariante Unterräume $U_1, \ldots, U_n$ der Dimension 1 gibt, sodass $V = U_1 \oplus \cdots \oplus U_n$ gilt.

(*ii*) Eine Matrix $A \in K^{n\times n}$ heißt **diagonalisierbar** (englisch: diagonalizable), wenn sie zu einer Diagonalmatrix ähnlich ist. △

Den Zusammenhang zwischen der Diagonalisierbarkeit eines Endomorphismus und seinen Darstellungsmatrizen stellt der folgende Satz her:

Satz 20.24 (Diagonalisierbarkeit der Darstellungsmatrix eines Endomorphismus)**.**
Es seien $(K, +, \cdot)$ ein Körper und $(V, +, \cdot)$ ein Vektorraum über K mit $\dim(V) = n \in \mathbb{N}_0$. Weiter sei $f\colon V \to V$ ein Endomorphismus und $A = \mathcal{M}_{B_V}^{B_V}(f) \in K^{n\times n}$ seine Darstellungsmatrix bzgl. einer beliebigen Basis B_V von V. Dann sind äquivalent:

(*i*) f ist diagonalisierbar.

(*ii*) V besitzt eine Basis, die nur aus Eigenvektoren von f besteht.

(*iii*) A ist diagonalisierbar.

(*iv*) K^n besitzt eine Basis, die nur aus Eigenvektoren von A besteht.

Beweis. Aussage (*i*) ⇒ Aussage (*iii*): Es sei f diagonalisierbar, also gibt es eine Zerlegung $V = U_1 \oplus \cdots \oplus U_n$ mit f-invarianten Unterräumen. Nach Satz 20.17 gibt es also eine Basis $\widehat{B}_V$, sodass die Darstellungsmatrix $\widehat{A} = \mathcal{M}_{\widehat{B}_V}^{\widehat{B}_V}(f)$ eine Diagonalmatrix ist. Da A und $\widehat{A}$ denselben Endomorphismus f darstellen, ist A nach Satz 20.17 ähnlich zur Diagonalmatrix $\widehat{A}$, d. h., A ist diagonalisierbar.

Aussage (*iii*) $\Rightarrow$ Aussage (*iv*): Es sei A diagonalisierbar, also existiert eine invertierbare Matrix $T \in K^{n\times n}$, sodass $\widehat{A} = T\,A\,T^{-1}$ eine Diagonalmatrix ist. Es gilt also

$$\widehat{A} = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}.$$

Wir setzen $X := T^{-1}$ und schreiben $A = T^{-1}\,\widehat{A}\,T = X\,\widehat{A}\,X^{-1}$. Wir zeigen, dass die Spalten $x_{\bullet 1}, \dots, x_{\bullet n}$ von X Eigenvektoren zu den Eigenwerten $\lambda_1, \dots, \lambda_n$ von A sind, denn es gilt:

$$\begin{aligned} A\,x_{\bullet j} &= X\,\widehat{A}\,X^{-1}x_{\bullet j} \\ &= X\,\widehat{A}\,e_j && \text{mit dem Standardbasisvektor } e_j \in K^n \\ &= X\,\lambda_j\,e_j && \text{wegen der Diagonalstruktur von } \widehat{A} \\ &= \lambda_j\,Xe_j && \text{aufgrund des Assoziativgesetzes (15.12)} \\ &= \lambda_j\,x_{\bullet j} && \text{nach Definition der Matrix-Vektor-Multiplikation.} \end{aligned}$$

Da T invertierbar ist, ist auch $X = T^{-1}$ invertierbar. Die Spalten von X sind also linear unabhängig (Satz 15.40). Das heißt, K^n besitzt die Basis $x_{\bullet 1}, \dots, x_{\bullet n}$ aus Eigenvektoren von A. (Die Eigenwerte sind gerade die Diagonaleinträge von $\widehat{A}$.)

Aussage (*iv*) $\Rightarrow$ Aussage (*ii*): Es sei $(x_1, \dots, x_n)$ eine Basis von K^n aus Eigenvektoren der Matrix A zu den Eigenwerten $\lambda_1, \dots, \lambda_n \in K$. Nach Lemma 20.20 ist dann $v_j = \Phi_{B_V}(x_j)$ ein Eigenwert des Endomorphismus f zum Eigenwert λ_j für jedes $j = 1, \dots, n$. Da $\Phi_{B_V} : K^n \to V$ ein Isomorphismus ist, bilden die Vektoren $(v_1, \dots, v_n)$ eine Basis von V (Satz 17.7).

Aussage (*ii*) $\Rightarrow$ Aussage (*i*): Es sei $B_V = (v_1, \dots, v_n)$ eine Basis von V aus lauter Eigenvektoren von f, sagen wir $f(v_j) = \lambda_j\,v_j$ für den zugehörigen Eigenwert $\lambda_j \in K$. Wir definieren die eindimensionalen Unterräume $U_j := \langle v_j \rangle$, $j = 1, \dots, n$. Dann ist jedes U_j f-invariant, denn es gilt

$$\begin{aligned} f(U_j) &= f(\langle v_j \rangle) && \text{nach Definition von } U_j \\ &= \langle f(v_j) \rangle && \text{nach Lemma 17.5} \\ &= \langle \lambda_j\,v_j \rangle && \text{wegen } f(v_j) = \lambda_j\,v_j \\ &= \lambda_j\,\langle v_j \rangle && \text{wegen Satz 12.13 (lineare Hülle besteht aus Linearkombinationen)} \\ &= \lambda_j\,U_j && \text{nach Definition von } U_j \\ &\subseteq U_j. \end{aligned}$$

(**Quizfrage 20.6:** Warum steht hier $\subseteq$ und nicht $=$?) Weiter gilt nach Satz 14.16

$$V = \langle v_1 \rangle \oplus \cdots \langle v_n \rangle = U_1 \oplus \cdots \oplus U_n,$$

d. h., f ist diagonalisierbar. □

Wie der Beweis von Satz 20.24 zeigt, sind es genau die diagonalisierbaren Endomorphismen, die bei geeigneter Wahl der Basis (nämlich einer Basis aus lauter Eigenvektoren) die denkbar einfachste Form einer Darstellungsmatrix besitzen, nämlich eine Diagonalmatrix. Bei dieser sind die Diagonaleinträge gerade die Eigenwerte (die möglicherweise mehrfach auftreten). Zwei *diagonalisierbare* $n \times n$-Matrizen sind also genau dann ähnlich, wenn sie zur selben Diagonalmatrix ähnlich sind.

Wie bereits erwähnt, werden wir

- den allgemeineren Fall von Darstellungsmatrizen in Blockdiagonalgestalt, der eintritt, wenn V als direkte Summe f-invarianter Unterräume darstellbar ist (Satz 20.17),
- sowie den ganz allgemeinen Fall für beliebige Endomorphismen

erst im zweiten Teil der Vorlesung untersuchen können. Wir nehmen jedoch vorweg, dass auch dabei Eigenwerte und Eigenvektoren von f eine wesentliche Rolle spielen.

Ende der Vorlesung 29

Ende der Woche 14

Kapitel A Die komplexen Zahlen

Die natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \ldots\}$ oder $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ sind ausreichend, um Objekte zu zählen. Gleichungen wie $x + 2 = 1$ sind jedoch in $\mathbb{N}_0$ nicht lösbar. Dafür benötigen wir die Menge der ganzen Zahlen $\mathbb{Z}$. Gleichungen wie $2\,x = 1$ sind aber auch in $\mathbb{Z}$ nicht lösbar. Dafür benötigen wir die Menge der rationalen Zahlen $\mathbb{Q}$. Gleichungen wie $x^2 = 2$ sind aber auch in $\mathbb{Q}$ nicht lösbar. Dafür benötigen wir die Menge der reellen Zahlen $\mathbb{R}$. Gleichungen wie $x^2 = -1$ sind aber auch in $\mathbb{R}$ nicht lösbar. Dafür benötigen wir die Menge der komplexen Zahlen $\mathbb{C}$.

Die **komplexen Zahlen** lassen sich aus den reellen Zahlen $\mathbb{R}$ aufbauen. Die Menge $\mathbb{C}$ der komplexen Zahlen besteht aus allen Ausdrücken der Form

$$a + b\,i,$$

wobei $a, b \in \mathbb{R}$ sind und i ein Symbol ist, das nicht in $\mathbb{R}$ enthalten ist.

Die **Addition** (englisch: addition) mit dem Symbol + ist definiert durch

$$(a + b\,i) + (c + d\,i) \coloneqq (a + c) + (b + d)\,i.$$

Aufgrund der Kommutativität von + in $\mathbb{R}$ bildet $(\mathbb{C}, +)$ eine kommutative Halbgruppe. Wir prüfen leicht nach, dass $0 + 0\,i$ neutrales Element in $(\mathbb{C}, +)$ ist und dass $a + b\,i$ und $-a - b\,i \coloneqq (-a) + (-b)\,i$ additive Inverse zueinander sind. Wir schreiben daher auch $-(a + b\,i)$ für $(-a) + (-b)\,i$. Wir haben damit gezeigt: $(\mathbb{C}, +)$ ist eine abelsche Gruppe.

Wir definieren weiter die **Multiplikation** (englisch: multiplication) mit dem Symbol $\cdot$ durch[1]

$$(a + b\,i) \cdot (c + d\,i) \coloneqq (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)\,i.$$

Motiviert ist diese Definition durch das formale Distributivgesetz $(a + b\,i) \cdot (c + d\,i) = a \cdot c + (b\,i) \cdot c + a \cdot (d\,i) + (b\,i) \cdot (d\,i)$, wobei die Kommutativitäts-Regeln $(b\,i) \cdot c = (b \cdot c)\,i$ und $a \cdot (d\,i) = (a \cdot d)\,i$ und $(b\,i) \cdot (d\,i) = (b \cdot d)\,i^2$ gelten sollen sowie $i^2 = -1$. Aufgrund der Kommutativität von $\cdot$ in $\mathbb{R}$ bildet $(\mathbb{C}, \cdot)$ eine kommutative Halbgruppe. Wir prüfen leicht nach, dass $1 + 0\,i$ neutrales Element in $(\mathbb{C}, \cdot)$ ist und dass $a + b\,i$ und $a/(a^2 + b^2) - b/(a^2 + b^2)\,i$ multiplikative Inverse zueinander sind, solange $a + b\,i \neq 0 + 0\,i$ gilt. Wir schreiben daher auch $(a + b\,i)^{-1}$ für $a/(a^2 + b^2) - b/(a^2 + b^2)\,i$. Wir haben damit gezeigt: $(\mathbb{C} \setminus \{0 + 0\,i\}, \cdot)$ eine abelsche Gruppe.

Weiterhin können wir die (wegen der Kommutativität von $\cdot$ zusammenfallenden) Distributivgesetze

$$\begin{aligned}(a + b\,i) \cdot \big((c + d\,i) + (e + f\,i)\big) &= (a + b\,i) \cdot (c + d\,i) + (a + b\,i) \cdot (e + f\,i)\\ \big((a + b\,i) + (c + d\,i)\big) \cdot (e + f\,i) &= (a + b\,i) \cdot (e + f\,i) + (c + d\,i) \cdot (e + f\,i)\end{aligned}$$

nachprüfen. Nach Definition 10.1 ist damit $(\mathbb{C}, +, \cdot)$ ein Körper.

[1] Die Einführung von $\mathbb{C}$ als formale Ausdrücke der Form $a + b\,i$ ist der Einführung von Polynomen in Definition 11.1 nicht unähnlich. Die Besonderheit hier ist aber die Festlegung $i^2 = -1$, die es ermöglicht, jede komplexe Zahl als „Polynom maximal ersten Grades“ in i zu schreiben.

Die Abbildung

$$\mathbb{C} \ni z = a + b\,i \mapsto \overline{z} = a - b\,i \in \mathbb{C}$$

ist ein Körperautomorphismus $(\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$. Es gilt also insbesondere

$$\overline{z + w} = \overline{z} + \overline{w} \quad \text{und} \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

für alle $z, w \in \mathbb{C}$. Dabei heißt $\overline{z}$ die zu z **konjugiert komplexe Zahl** (englisch: complex conjugate).

Das Produkt $z \cdot \overline{z}$ einer komplexen Zahl $z = a + b\,i$ mit ihrer konjugiert komplexen Zahl ergibt

$$z \cdot \overline{z} = (a + b\,i) \cdot (a - b\,i) = a^2 + b^2.$$

Mit Hilfe der komplexen Konjugation können wir die oben eingeführte Darstellung der multiplikativen Inversen motivieren, denn es gilt

$$\frac{1}{a + b\,i} = \frac{1}{a + b\,i} \cdot \frac{a - b\,i}{a - b\,i} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\,i.$$

In der Darstellung einer komplexen Zahl $z = a + b\,i$ heißt $a =: \operatorname{Re}(z) \in \mathbb{R}$ der **Realteil** (englisch: real part) und $b =: \operatorname{Im}(z) \in \mathbb{R}$ der **Imaginärteil** (englisch: imaginary part). Es gilt

$$\frac{z + \overline{z}}{2} = \frac{a + b\,i + a - b\,i}{2} = a = \operatorname{Re}(z)$$
$$\frac{z - \overline{z}}{2\,i} = \frac{a + b\,i - a + b\,i}{2\,i} = b = \operatorname{Im}(z).$$

Beachte: $\operatorname{Re}\colon (\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$ und $\operatorname{Im}\colon (\mathbb{C}, +, \cdot) \to (\mathbb{C}, +, \cdot)$ sind keine Körperhomomorphismen! (**Beachte:** Warum nicht?)

Schließlich halten wir fest, dass $\mathbb{R}$ mittels der Identifikation $a = a + 0\,i$ zu einem Teilkörper von $\mathbb{C}$ wird.

Kapitel B Liste algebraischer Strukturen

In der folgenden Tabelle ist X irgendeine Menge. Die Abkürzungen „komm.“ und „n. E.“ stehen für „kommutativ“ und „neutrales Element“. Bei Ringen bezieht sich die Kommutativität und die Angabe des neutrale Elements auf die zweite Verknüpfung. Die angegebenen Eigenschaften können in Einzelfällen abweichen, vor allem im Fall $m = 1$ oder wenn X die leere Menge oder eine einelementige Menge ist.

Symbol	Beschreibung	komm.	n. E.	Referenz
Halbgruppen und Monoide ($m \in \mathbb{N}$)				
$(\mathbb{N}, +)$		✓	–	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{N}_0, +)$		✓	0	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{N}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.14 und 7.20
$(\mathbb{N}_0, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{Z}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.14 Beispiele 7.16 und 7.20
$(\mathbb{Q}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{R}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8, 7.14 und 7.20
$(\mathbb{C}, \cdot)$		✓	1	Beispiele 7.2, 7.4, 7.8 und 7.20
$(\mathbb{Z}_m, \cdot_m)$	multiplikatives Monoid $\mathbb{Z}$ modulo m	✓	1	Beispiele 7.2, 7.8, 7.14 und 7.16
$(H^X, +)$	Halbgruppe der Funktionen $X \to H$ in die Halbgruppe $(H, +)$	wie in $(H, +)$		Beispiel 10.2
$(\mathbb{N}^X, +)$		✓	–	
$(\mathbb{N}_0^X, +)$		✓	$x \mapsto 0$	
$(H^X, \cdot)$	Halbgruppe der Funktionen $X \to H$ in die Halbgruppe $(H, \cdot)$	wie in $(H, \cdot)$		Beispiel 10.2
$(\mathbb{N}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{N}_0^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{Z}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{Q}^X, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{R}^X, \cdot)$		✓	$x \mapsto 1$	Beispiele 7.2, 7.4 und 7.16
$(\mathbb{C}^X, \cdot)$		✓	$x \mapsto 1$	
$(X^X, \circ)$		–	id_X	Beispiele 7.2, 7.4, 7.14 und 7.16
$(\mathcal{P}(X), \cap)$		✓	X	Beispiele 7.4 und 7.8
$(\mathcal{P}(X), \cup)$		✓	$\emptyset$	Beispiele 7.4 und 7.8
$(\mathcal{P}(X), \triangle)$		✓	$\emptyset$	Beispiele 7.4 und 7.8
$(\Sigma^*, \circ)$		–	$()$	Beispiele 7.4 und 7.8

Symbol	Beschreibung	komm.	n. E.	Referenz
Gruppen	$(m \in \mathbb{N})$			
$(\mathbb{Z}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8 und 7.14 Beispiele 7.16, 7.20 und 7.38
$(\mathbb{Q}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8 und 7.14 Beispiele 7.16 und 7.20
$(\mathbb{R}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8 und 7.14 Beispiele 7.16 und 7.20
$(\mathbb{C}, +)$		✓	0	Beispiele 7.2, 7.4, 7.8 und 7.14 Beispiele 7.16 und 7.20
$(\mathbb{Q}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.14 und 7.16
$(\mathbb{R}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.14 und 7.16
$(\mathbb{C}_{\neq 0}, \cdot)$		✓	1	Beispiele 7.14 und 7.16
$(m\,\mathbb{Z}, +)$	ganzzahlige Vielfache von m	✓	1	Beispiele 7.34 und 7.38
$(\mathbb{Z}_m, +_m)$	additive Gruppe $\mathbb{Z}$ modulo m	✓	0	Beispiele 7.2, 7.8, 7.14 und 7.16
$(\mathbb{Z}\,/\,m\,\mathbb{Z}, \tilde{+})$	Faktorgruppe, isomorph zu $(\mathbb{Z}_m, +_m)$	✓	$[1]$	Beispiel 8.15
$(G^X, +)$	Gruppe der Funktionen $X \to G$ in die Gruppe $(G, +)$	wie in $(G, +)$		Beispiel 10.2
$(\mathbb{Z}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{Q}^X, +)$		✓	$x \mapsto 0$	
$(\mathbb{R}^X, +)$		✓	$x \mapsto 0$	Beispiele 7.2, 7.4 und 7.16
$(\mathbb{C}^X, +)$		✓	$x \mapsto 0$	
$(G^X, \cdot)$	Gruppe der Funktionen $X \to G$ in die Gruppe $(G, \cdot)$	wie in $(G, \cdot)$		Beispiel 10.2
$(\mathbb{Q}^X_{\neq 0}, \cdot)$		✓	$x \mapsto 1$	
$(\mathbb{R}^X_{\neq 0}, \cdot)$		✓	$x \mapsto 1$	Beispiel 7.16
$(\mathbb{C}^X_{\neq 0}, \cdot)$		✓	$x \mapsto 1$	
$(S_n, \circ)$	symmetrische Gruppe auf $[\![1, n]\!]$	–	$\mathrm{id}_{[\![1,n]\!]}$	Definition 7.21
$(A_n, \circ)$	alternierende Gruppe auf $[\![1, n]\!]$	–	$\mathrm{id}_{[\![1,n]\!]}$	Beispiel 7.34

Symbol	Beschreibung	komm.	n. E.	Referenz
Ringe	$(m \in \mathbb{N})$			
$(\{0_R\}, +, \cdot)$	Nullring	✓	0_R	Beispiel 9.2
$(\mathbb{Z}, +, \cdot)$		✓	1	Beispiel 9.2
$(m\,\mathbb{Z}, +, \cdot)$	ganzzahlige Vielfache von m	✓	—	Beispiel 9.2
$(\mathbb{Z}_m, +_m, \cdot_m)$	$\mathbb{Z}$ modulo m	✓	1	Beispiel 9.2
$(\mathbb{Z}/m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$	Restklassenring modulo m, isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$	✓	[1]	Beispiel 9.2
$(R^X, +, \cdot)$	Funktionen $X \to R$ in den Ring $(R, +, \cdot)$	wie in $(R, +, \cdot)$		Beispiele 9.8 und 10.2
$(\mathbb{Z}^X, +, \cdot)$		✓	1	
$(\mathbb{Q}^X, +, \cdot)$		✓	1	
$(\mathbb{R}^X, +, \cdot)$		✓	1	
$(\mathbb{C}^X, +, \cdot)$		✓	1	
$(R[t], +, \cdot)$	Polynomring über dem kommutativen Ring $(R, +, \cdot)$	✓	1	Definition 11.4
$(R^R, +, \cdot)$	Funktionen $R \to R$ in den Ring $(R, +, \cdot)$	wie in $(R, +, \cdot)$		Bemerkung 11.17
$(\mathrm{End}(G), +, \circ)$	Endomorphismenring der abelschen Gruppe G	—	id_G	Beispiel 9.2
$K^{n\times n}$	quadratische $n \times n$-Matrizen über einem Körper K	—	I_n	Lemma 15.30
$(\mathrm{End}(V), +, \circ)$	Endomorphismen eines VRes $(V, +, \cdot)$ über einem Körper $(K, +, \cdot)$	—	id_V	Satz 17.12
Körper	$(m \in \mathbb{N})$			
$(\mathbb{Q}, +, \cdot)$		✓	1	Beispiele 9.2 und 10.2
$(\mathbb{R}, +, \cdot)$		✓	1	Beispiele 9.2 und 10.2
$(\mathbb{C}, +, \cdot)$		✓	1	Beispiele 9.2 und 10.2
$(\mathbb{Z}_m, +_m, \cdot_m)$	Körper von $\mathbb{Z}$ modulo m für Primzahlen m	✓	1	Beispiel 9.2
$(\mathbb{Z}/m\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$	Restklassenkörper mod. m für Primz. m, isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$	✓	[1]	Beispiel 9.2

Symbol	Beschreibung	komm.	n. E.	Referenz
Vektorräume	$(n, m \in \mathbb{N}_0)$			
K_n	Zeilenvektoren über einem Körper $(K, +, \cdot)$			Beispiel 12.3
K^n	Spaltenvektoren über einem Körper $(K, +, \cdot)$			Beispiel 12.3
$(K^X, +, \cdot)$	Funktionen $X \to K$ in den Körper $(K, +, \cdot)$			Beispiel 12.3
$(V^X, +, \cdot)$	Funktionen $X \to V$ in den Vektorraum $(V, +, \cdot)$ über dem Körper $(K, +, \cdot)$			
$(K[t], +, \cdot)$	Polynome über dem Körper $(K, +, \cdot)$			Beispiel 12.3
$(K_n[t], +, \cdot)$	Polynome vom Höchstgrad $n \in \mathbb{N}_0$ über dem Körper $(K, +, \cdot)$			Beispiel 12.9
$(K^{\mathbb{N}}, +, \cdot)$	Folgen mit Werten im Körper $(K, +, \cdot)$			Beispiel 12.9
$(K^{\mathbb{N}}, +, \cdot)_{00}$	Folgen mit endlichem Träger und Werten im Körper $(K, +, \cdot)$			Beispiel 12.9
$(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$	Folgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			
$(\mathbb{Q}^{\mathbb{N}}, +, \cdot)_b$	beschränkte Folgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			
$(\mathbb{Q}^{\mathbb{N}}, +, \cdot)_c$	konvergente Folgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			
$(\mathbb{Q}^{\mathbb{N}}, +, \cdot)_0$	Nullfolgen mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			
$(\mathbb{Q}^{\mathbb{N}}, +, \cdot)_{00}$	Folgen mit endlichem Träger mit Werten im Körper $(\mathbb{Q}, +, \cdot)$			
$(\mathbb{R}^{\mathbb{N}}, +, \cdot)$	Folgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^{\mathbb{N}}, +, \cdot)_b$	beschränkte Folgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^{\mathbb{N}}, +, \cdot)_c$	konvergente Folgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^{\mathbb{N}}, +, \cdot)_0$	Nullfolgen mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{R}^{\mathbb{N}}, +, \cdot)_{00}$	Folgen mit endlichem Träger mit Werten im Körper $(\mathbb{R}, +, \cdot)$			Beispiel 12.9
$(\mathbb{C}^{\mathbb{N}}, +, \cdot)$	Folgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			
$(\mathbb{C}^{\mathbb{N}}, +, \cdot)_b$	beschränkte Folgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			
$(\mathbb{C}^{\mathbb{N}}, +, \cdot)_c$	konvergente Folgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			
$(\mathbb{C}^{\mathbb{N}}, +, \cdot)_0$	Nullfolgen mit Werten im Körper $(\mathbb{C}, +, \cdot)$			
$(\mathbb{C}^{\mathbb{N}}, +, \cdot)_{00}$	Folgen mit endlichem Träger mit Werten im Körper $(\mathbb{C}, +, \cdot)$			
$K^{n \times m}$	$n \times m$-Matrizen über einem Körper K			Definition 15.2
$(\mathrm{Hom}(V, W), +, \cdot)$	Homomorphismen $V \to W$ mit VR $(V, +, \cdot)$ und $(W, +, \cdot)$ über demselben Körper $(K, +, \cdot)$			Satz 17.11

Kapitel C 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 D Abkürzungen

Abkürzung	Bedeutung
bzgl.	bezüglich
d. h.	das heißt
etc.	et cetera
i. A.	im Allgemeinen
i. d. R.	in der Regel
i. W.	im Wesentlichen
o. B. d. A.	ohne Beschränkung der Allgemeinheit
o. ä.	oder ähnlich
usw.	und so weiter
vgl.	vergleiche

Index

Literatur

Beutelspacher, A. (2014). *Lineare Algebra. Eine Einführung in die Wissenschaft der Vektoren, Abbildungen und Matrizen*. 8. Aufl. Springer Fachmedien Wiesbaden. DOI: 10.1007/978-3-658-02413-0.

Bosch, S. (2014). *Lineare Algebra*. 5. Aufl. Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-55260-1.

Deiser, O. (2022a). *Einführung in die Mengenlehre*. URL: https://www.aleph1.info/?call=Puc&permalink=mengenlehre1.

– (2022b). *Grundbegriffe der Mathematik*. URL: https://www.aleph1.info/?call=Puc&permalink=grundbegriffe.

Fischer, G.; B. Springborn (2020). *Lineare Algebra*. 19. Aufl. Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-61645-1.

Jänich, K. (2008). *Lineare Algebra*. 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.