Lineare Algebra

Vorlesung 2012/2013

Universität Mannheim

gehalten von Ralf Kurbel

Inhaltsverzeichnis

Teil 1. Lineare Algebra I und IIa 1

Kapitel 0. Voraussetzungen und Grundlagen 3
0.1. Notationen 3
0.2. Mengen und Relationen 5
0.3. Zahlenmengen 9
0.4. Abbildungen 11
0.5. Vollständige Induktion 22

Kapitel 1. Grundlegende algebraische Strukturen 25
1.1. Algebraische Strukturen 25
1.2. Gruppen 44
1.3. Ringe und Körper 79

Kapitel 2. Vektorräume 103
2.1. Vektorräume und Moduln 103
2.2. Erzeugendensysteme und Basen 131

Kapitel 3. Matrizen 167
3.1. Matrizen 167
3.2. Der Gauß-Algorithmus 186
3.3. Determinanten 218
3.4. Matrizendarstellungen linearer Abbildungen 268

Kapitel 4. Euklidische Vektorräume 323
4.1. Euklidische Vektorräume 323

Anhang A. Lineare Algebra I und IIa Anh. 1
A.1. Allgemeines Assoziativ- und Kommutativgesetz Anh. 1
A.2. Potenzgesetze in Monoiden Anh. 4
A.3. Die symmetrische Gruppe S_n Anh. 7
A.4. Determinanten Anh. 13

Anhang. Literaturverzeichnis Lit. 1

Anhang. Index Ind. 1

Teil 1

Lineare Algebra I und IIa

KAPITEL 0

Voraussetzungen und Grundlagen

0.1. Notationen

Zuerst werden einige Schreibweisen und Symbole eingeführt, die im folgenden verwendet werden:

Bemerkung 0.1.1. *In diesem Skript werden numerierte und damit hervorgehobene Aussagen mit dem Symbol „□“ abgeschlossen (falls ein Beweis auf die Aussage folgt, am Ende des Beweises). Damit ist angedeutet, daß ein Sinnzusammenhang abgeschlossen ist.* □

Definition 0.1.2. *Wird in diesem Skript ein Objekt in einer Formel definiert, so ist dies durch das Symbol „ := “ kenntlich gemacht. Beispiele:*

$$f(x) := x^2 \qquad \rightsquigarrow \quad f \text{ wird definiert als die Funktion} \ldots$$
$$A := \{1, 2, 3\} \qquad \rightsquigarrow \quad A \text{ wird definiert als die Menge} \ldots \qquad \square$$

Diese Benutzung des Symbols „ := “ ist in der Mathematik nicht unüblich, wird aber nicht von allen Autoren konsequent genutzt. Viele verwenden auch bei Definitionen von Objekten das einfache Gleichheitszeichen (ohne den Doppelpunkt).
Die hier verwendete Notation ist eine Hilfe für den Leser: wenn etwas definiert wird, so gibt es nichts zu überlegen, sondern nur zu akzeptieren. Ein Gleichheitszeichen ist eine Aussage, über die nachzudenken ist:

$f(x) := g(x) \rightsquigarrow$ Die Funktion $f(x)$ wird eingeführt und $g(x)$ gleichgesetzt.

$f(x) = g(x) \rightsquigarrow$ Zwei (bekannte) Funktionen $f(x)$ und $g(x)$ sind gleich (wirklich?).

Würde in beiden Fällen nur das Gleichheitszeichen benutzt, so wäre ersteinmal nicht klar, ob der Autor die Funktion f definieren oder über ein schon bekanntes f eine Aussage treffen will.

Definition 0.1.3. *In der Mathematik werden aus Aussagen weitere gefolgert:*

„Wenn die Aussage A wahr ist, dann gilt auch Aussage B.“

Dies heißt Implikation (Folgerung) und wird mit dem Symbol „ $\Longrightarrow$ “ in Formeln geschrieben. Beispiel:

$$x = 7 \quad \Longrightarrow \quad x > 0$$

(wenn x den Wert sieben hat, dann ist x größer als Null).
Zwei Aussagen heißen äquivalent, wenn sie logisch gleichwertig sind:

„Die Aussage A gilt genau dann, wenn auch die Aussage B gilt.“

Dies wird mit dem Symbol „ $\Longleftrightarrow$ “ in Formeln notiert. Beispiel:

$$x \geq 0 \text{ und } x \leq 0 \quad \Longleftrightarrow \quad x = 0$$

(x ist genau dann sowohl größer gleich Null als auch kleiner gleich Null, wenn x gleich Null ist). □

Bemerkung 0.1.4. *Die obige Äquivalenz*

$$x \geq 0 \text{ und } x \leq 0 \quad \Longleftrightarrow \quad x = 0$$

ist natürlich so zu verstehen, daß es zwei äquivalente Aussagen A und B gibt mit

$$\begin{aligned} A &:= \text{„}x \geq 0 \text{ und } x \leq 0\text{“}. \\ B &:= \text{„}x = 0\text{“}. \end{aligned}$$

Strenggenommen sollte in der Formel die linke Seite geklammert werden, um kenntlich zu machen, daß „$x \geq 0$“ und „$x \leq 0$“ zusammen eine Aussage bilden, die äquivalent zur rechten Seite ist. Dies ist hier nur durch Abstände symbolisiert und wird in Zukunft auch so weitergeführt. Im folgenden ist also die Zeile

$$A \Longrightarrow B \qquad \Longleftrightarrow \qquad \neg B \Longrightarrow \neg A$$

zu lesen als:

$$(A \Longrightarrow B) \qquad \Longleftrightarrow \qquad (\neg B \Longrightarrow \neg A).$$ □

Für Implikationen und Äquivalenzen gelten folgende Regeln:

Lemma 0.1.5. *Sei für eine Aussage A mit $\neg A$ ihr logisches Gegenteil bezeichnet. Dann sind für Aussagen A und B folgende logische Beziehungen äquivalent und können jeweils untereinander ausgetauscht werden:*

$$\begin{aligned} A \Longrightarrow B \quad &\Longleftrightarrow \quad \neg B \Longrightarrow \neg A. \\ A \Longleftrightarrow B \quad &\Longleftrightarrow \quad A \Longrightarrow B \text{ und } B \Longrightarrow A. \\ A \Longleftrightarrow B \quad &\Longleftrightarrow \quad \neg A \Longleftrightarrow \neg B. \end{aligned}$$ □

Beim Beweis von Implikationen oder Äquivalenzen sind obige Umformulierungen oft von großem Nutzen.

Beispiel 0.1.6.

i.) Es seien die folgenden Aussagen gegeben:

$$\left.\begin{aligned} A &:= \text{„}x = 7\text{“}, \\ B &:= \text{„}x \geq 0\text{“} \end{aligned}\right\} \Longrightarrow \left\{\begin{aligned} \neg A &= \text{„}x \neq 7\text{“}, \\ \neg B &= \text{„}x < 0\text{“}. \end{aligned}\right.$$

Dann sind folgende Implikationen äquivalent:

$$x = 7 \Longrightarrow x \geq 0 \qquad \Longleftrightarrow \qquad x < 0 \Longrightarrow x \neq 7$$

ii.) Es seien die folgenden Aussagen gegeben:

$$\left.\begin{aligned} A &:= \text{„}x^2 = 1\text{“}, \\ B &:= \text{„}x \in \{\pm 1\}\text{“} \end{aligned}\right\} \Longrightarrow \left\{\begin{aligned} \neg A &= \text{„}x^2 \neq 1\text{“}, \\ \neg B &= \text{„}x \notin \{\pm 1\}\text{“}. \end{aligned}\right.$$

Dann gibt es folgende Äquivalenzen:

$$x^2 = 1 \Longleftrightarrow x \in \{\pm 1\} \qquad \Longleftrightarrow \qquad \left\{\begin{aligned} x^2 = 1 &\Longrightarrow x \in \{\pm 1\} \text{ und} \\ x \in \{\pm 1\} &\Longrightarrow x^2 = 1. \end{aligned}\right.$$

$$x^2 = 1 \Longleftrightarrow x \in \{\pm 1\} \qquad \Longleftrightarrow \qquad x^2 \neq 1 \Longleftrightarrow x \notin \{\pm 1\}.$$ □

0.2. Mengen und Relationen

In den *Mathematischen Annalen* gab 1895 Georg Cantor (03.03.1845—06.01.1918), der „Begründer“ der Mengenlehre, in seinem Aufsatz *Beiträge zur Begründung der transfiniten Mengenlehre* folgende Definition einer Menge [**MAC**]:

> Unter einer „Menge“ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die „Elemente“ von M genannt werden) zu einem Ganzen.
>
> In Zeichen drücken wir dies so aus:
>
> $$M = \{m\}.$$

Diese „freizügige“ Form der Mengenbildung führt zu Antinomien (Antinomie - logischer Widerspruch). Ein Beispiel ist durch die folgende Mengenbildung gegeben:

Sei M die Menge aller Mengen, die sich nicht selbst als Element enthalten.

Dann ergibt sich ein Widerspruch:

$$\begin{aligned} M \text{ ist Element von } M \quad &\Longrightarrow \quad M \text{ ist kein Element von } M. \\ M \text{ ist kein Element von } M \quad &\Longrightarrow \quad M \text{ ist ein Element von } M. \end{aligned}$$

Die „Zusammenfassung von Objekten unseres Denkens“ muß eingeschränkt werden, um obiges Problem zu vermeiden, und es gibt verschiedene Axiomensysteme zur Mengenlehre, die dies auf unterschiedliche, aber äquivalente Weise erreichen. Das kann hier nicht im Detail diskutiert werden. Alle in dieser Vorlesung gebildeten Mengen sind nach den Axiomensystemen „erlaubt“! Und wenn die „Objekte unseres Denkens“ aus einer schon existierenden Menge ausgewählt werden, so ergeben sich auch keine Widersprüche, wenn nach der Definition von Cantor eine Menge gebildet wird.

Definition 0.2.1. *(Saloppe Definition von Mengen)*
Eine Menge M ist eine Zusammenfassung von Objekten x (meist aus einer anderen Menge N gewählt), die eine Eigenschaft E besitzt. Notation:

$$M := \{\, x \mid x \text{ erfüllt } E \,\} \quad \text{oder} \quad M := \{\, x \in N \mid x \text{ erfüllt } E \,\}.$$

(Der senkrechte Strich „ | “ ist dabei zu lesen als: „für die gilt“.)
Eine Menge kann auch durch die explizite Aufzählung ihrer Elemente beschrieben werden: dabei müssen alle angegebenen Elemente paarweise verschieden sein.

$\{1,3,3,4\}$ *ist z.B. <u>keine</u> korrekte Mengenbeschreibung!* $\{1,3,4\}$ *schon.*

Die Objekte x heißen Elemente der Menge, und für ein beliebiges Objekt m wird bzgl. M notiert:

$$\begin{aligned} m \in M \quad &:= \quad m \text{ ist ein Element von } M. \\ m \notin M \quad &:= \quad m \text{ ist kein Element von } M. \end{aligned}$$

Eine Menge A heißt Teilmenge von M, wenn alle Elemente von A auch Elemente von M sind. Notation: $A \subseteq M$. Es gilt also:

$$A \subseteq M \qquad \Longleftrightarrow \qquad x \in A \Longrightarrow x \in M.$$

Zwei Mengen M, N sind gleich, wenn sie die gleichen Elemente enthalten:

$$M = N \quad \Longleftrightarrow \quad M \subseteq N \quad \text{und} \quad N \subseteq M \quad \Longleftrightarrow \quad x \in M \Longleftrightarrow x \in N.$$

Eine Teilmenge $A \subseteq M$ heißt echte Teilmenge, wenn es ein $x \in M$ gibt mit $x \notin A$. Dies wird notiert mit:

$$A \subsetneq M \quad \text{oder} \quad A \subset M.$$

Die Verwendung des Symbols „$\subset$“ ist in der Literatur nicht eindeutig: manche Autoren benutzen es einfach für „Teilmenge“ - echte oder nicht echte. Die Verwendung von „$\subseteq$“ für Teilmengen und „$\subsetneq$“ für echte Teilmengen ist unmißverständlich.
Die leere Menge, d.h. diejenige Menge, die keine Elemente enthält, wird mit „$\emptyset$“ (oder auch „$\{\}$“) bezeichnet. Sie ist definitionsgemäß Teilmenge einer jeden Menge.
Die Menge aller Teilmengen einer Menge M wird als die Potenzmenge von M bezeichnet und mit $\mathcal{P}(M)$ notiert und enthält definitionsgemäß immer $\emptyset$ und M als Elemente.
Häufig treten bei Aussagen über Mengen die folgenden beiden Formulierungen auf:

„Für alle $x \in M$ gilt:...“ und „Es gibt ein $x \in M$, für das gilt:...“

Dies wird in Formeln auch geschrieben als:

$$\forall x \in M : \ldots \qquad \text{und} \qquad \exists\, x \in M : \ldots$$

Dabei ist die Verwendung der Symbole „$\forall$“ und „$\exists$“ nur <u>vor</u> der Aussage erlaubt:

$\forall x \in M : x < 3.$	(*richtig*).
Es gilt $x < 3$ für alle $x \in M$.	(*richtig*).
Es gilt $x < 3$ $\forall x \in M$.	(*falsch!*).

Mit dem Symbol „$\exists$“ wird ausgedrückt, daß es mindestens ein Element gibt, welches eine Bedingung erfüllt. Gibt es genau eines, so wird dies mit „$\exists!$“ symbolisiert:

$$\exists!\, x \in \{1, 3, 4, 5\} : x \text{ ist gerade.} \qquad \square$$

Folgende Methoden erlauben die Konstruktion von Mengen aus gegebenen:

Definition 0.2.2. *Seien A und B Mengen. Dann sind folgende Mengen definiert:*

$A \cup B := \{\, x \mid x \in A \text{ oder } x \in B \,\}$,	*die Vereinigungsmenge von A und B.*
$A \cap B := \{\, x \mid x \in A \text{ und } x \in B \,\}$,	*die Schnittmenge von A und B.*
$A \setminus B := \{\, x \in A \mid x \notin B \,\}$,	*die Differenzmenge von A und B.*
$A \times B := \{(a, b) \mid a \in A \text{ und } b \in B \,\}$,	*das kartesische Produkt von A und B.*

Für $(a, b), (\tilde{a}, \tilde{b}) \in A \times B$ gilt dabei:

$$(a, b) = (\tilde{a}, \tilde{b}) \quad \Longleftrightarrow \quad a = \tilde{a} \text{ und } b = \tilde{b}.$$

Dies darf auch auf eine beliebige Menge von gegebenen Mengen verallgemeinert werden: Sei dazu I eine nicht-leere Indexmenge und A_i für jedes $i \in I$ eine Menge. Dann sind folgende Mengen definiert:

$\bigcup_{i \in I} A_i := \{\, x \mid x \in A_i \text{ für ein } i \in I \,\}$,	*die Vereinigungsmenge aller A_i.*
$\bigcap_{i \in I} A_i := \{\, x \mid x \in A_i \text{ für jedes } i \in I \,\}$,	*die Schnittmenge aller A_i.*

Sind alle A_i nicht-leere Mengen, so ist definiert:

$$\prod_{i\in I} A_i := \{\, (x_i)_{i\in I} \mid x_i \in A_i \text{ für jedes } i \in I \,\}, \quad \text{das kartesische Produkt aller } A_i.$$

Für $(x_i)_{i\in I}, (y_i)_{i\in I} \in \prod_{i\in I} A_i$ gilt dabei:

$$(x_i)_{i\in I} = (y_i)_{i\in I} \quad \Longleftrightarrow \quad x_i = y_i \text{ für alle } i \in I.$$

Für eine ganze Zahl $n \geq 2$ und eine Menge A wird das n-fache kartesische Produkt mit sich selbst folgendermaßen notiert:

$$A^n := \prod_{i=1}^{n} A = \underbrace{A \times \cdots \times A}_{n\text{-mal}}. \qquad \square$$

Definition 0.2.3. *Mengen A_i für i aus einer nicht-leeren Indexmenge I heißen disjunkt, wenn jeweils zwei von ihnen kein gemeinsames Elemente besitzen, d.h. es gilt:*

$$\text{Die Mengen } A_i \text{ sind disjunkt} \quad \Longleftrightarrow \quad A_i \cap A_j = \emptyset \text{ für alle } i, j \in I \text{ mit } i \neq j.$$

Die Vereinigung disjunkter Mengen wird oft durch einen Punkt über dem Vereinigungszeichen kenntlich gemacht: z.B. $A \dot\cup B$ oder $\dot\bigcup_{i\in I} A_i$. $\square$

Nun zu einer Definition, die im weiteren Verlauf eine große Rolle spielen wird:

Definition 0.2.4. *Sei M eine nicht-leere Menge. Eine Relation auf M ist eine nicht-leere Teilmenge $R \subseteq M \times M$. Zwei Elemente $a, b \in M$ stehen in Relation zueinander (bzgl. der Relation R), falls $(a, b) \in R$ gilt. Notation:*

$$a \sim_R b \quad \text{für} \quad (a, b) \in R \qquad (\text{Kurznotation: } a \sim b).$$

Eine Relation R auf M heißt:

$$\begin{aligned} \text{reflexiv, falls gilt:} \quad & a \sim a \text{ für alle } a \in M, \\ \text{symmetrisch, falls gilt:} \quad & a \sim b \quad \Longrightarrow \quad b \sim a, \\ \text{transitiv, falls gilt:} \quad & a \sim b,\, b \sim c \quad \Longrightarrow \quad a \sim c. \end{aligned}$$

In der „Tupelschreibweise“ lauten die Definitionen für die Eigenschaften von R:

$$\begin{aligned} R \text{ ist reflexiv, falls gilt:} \quad & (a, a) \in R \text{ für alle } a \in M. \\ R \text{ ist symmetrisch, falls gilt:} \quad & (a, b) \in R \quad \Longrightarrow \quad (b, a) \in R. \\ R \text{ ist transitiv, falls gilt:} \quad & (a, b),\, (b, c) \in R \quad \Longrightarrow \quad (a, c) \in R. \end{aligned}$$

Eine reflexive, symmetrische und transitive Relation heißt Äquivalenzrelation.
Ist R eine Äquivalenzrelation auf M und $a \in M$, so ist seine Äquivalenzklasse $[a]_R$ (oder auch kurz $[a]$) definiert als

$$[a]_R := \{\, b \in M \mid a \sim b \,\},$$

und a heißt Repräsentant seiner Äquivalenzklasse $[a]_R$. $\square$

Bemerkung 0.2.5. *Es sei R eine Äquivalenzrelation auf M.*

i.) Die Relation R ist eine Teilmenge von $M \times M$. Für $a \in M$ ist die Äquivalenzklasse $[a]_R$ eine Teilmenge von M.
ii.) Für jedes $a \in M$ ist seine Äquivalenzklasse nicht leer, da nach Definition wegen der Reflexivität von R immer $a \in [a]_R$ gilt.
iii.) Für $x \in [a]$ gilt wegen der Symmetrie von R sowohl $a \sim x$ als auch $x \sim a$. □

Das wesentliche Ergebnis über Äquivalenzrelationen ist, daß ihre Äquivalenzklassen nicht nur irgendwelche Teilmengen der Ausgangsmenge sind, sondern diese sogar partitionieren, d.h. eine disjunkter Zerlegung liefern:

Satz 0.2.6. *Es sei eine Äquivalenzrelation auf M gegeben. Dann sind für $a, b \in M$ die Äquivalenzklassen $[a]$ und $[b]$ entweder gleich oder disjunkt, d.h. es gilt:*

$$[a] = [b] \quad \textit{oder} \quad [a] \cap [b] = \emptyset.$$

Insbesondere sind dann folgende Aussagen äquivalent:

$$a \in [b] \quad \Longleftrightarrow \quad [a] = [b] \quad \Longleftrightarrow \quad b \in [a].$$

Die Menge M läßt sich dann bzgl. eines geeigneten vollständigen Repräsentantensystems $S \subseteq M$ disjunkt in Äquivalenzklassen zerlegen:

$$M = \dot{\bigcup_{a \in S}} [a].$$

Beweis. Zum Beweis der ersten Aussage reicht es zu zeigen:

Ist $[a] \cap [b]$ nicht leer, so gilt schon $[a] = [b]$.

Sei also $x \in [a] \cap [b]$, d.h. $a \sim x$ und $x \sim a$ wegen $x \in [a]$ sowie $b \sim x$ und $x \sim b$ wegen $x \in [b]$. Dann liefert die Transitivität sofort $a \sim b$ und $b \sim a$.

$[a] \subseteq [b]$: Sei $y \in [a]$. Dann gilt $y \sim a$, und wegen $a \sim b$ auch $y \sim b$ und $y \in [b]$.
$[b] \subseteq [a]$: Sei $y \in [b]$. Dann gilt $y \sim b$, und wegen $b \sim a$ auch $y \sim a$ und $y \in [a]$.

Zu den äquivalenten Aussagen: Die Äquivalenzen ergeben sich sofort aus der vorherigen Aussage, denn z.B. für $a \in [b]$ sind wegen $a \in [a]$ die Äquivalenzklassen $[a]$ und $[b]$ nicht disjunkt und damit gleich.
Zur Partitionierung von M: Sei $\mathcal{F}$ die Menge aller Äquivalenzklassen. Nach obiger Aussage sind diese alle paarweise disjunkt. Jedes $a \in M$ liegt wegen $a \in [a]$ auch in einer Äquivalenzklasse, so daß gilt:

$$M = \dot{\bigcup_{K \in \mathcal{F}}} K.$$

Ein geeignetes vollständiges Repräsentantensystem $S \subseteq M$ kann dann gefunden werden, indem für jedes $K \in \mathcal{F}$ ein Repräsentant ausgewählt wird. □

Beispiel 0.2.7. *Sei M eine nicht-leere Menge.*

i.) $\Delta_M := \{\, (m,m) \mid m \in M \,\}$ *ist eine Äquivalenzrelation, deren Äquivalenzklassen gegeben sind durch die einelementigen Mengen* $[m] = \{m\}$ *für* $m \in M$.

ii.) $M \times M$ *ist eine Äquivalenzrelation auf* M, *deren einzige Äquivalenzklasse* M *selbst ist, d.h es gilt* $[m] = M$ *für jedes* $m \in M$.

iii.) *Für jede Äquivalenzrelation* R *auf* M *gilt:* $\Delta_M \subseteq R \subseteq M \times M$.

iv.) *Sei* $M := \dot{\bigcup_{i \in I}} A_i$ *eine Zerlegung von* M *in disjunkte nicht-leere Teilmengen* A_i *für* $i \in I$. *Weiter sei für* $a, b \in M$ *eine Relation definiert durch:*

$$a \sim b \quad := \quad a \text{ und } b \text{ liegen in der gleichen Teilmenge } A_i.$$

Dann definiert dies eine Äquivalenzrelation auf M *mit den Äquivalenzklassen* A_i *für* $i \in I$. *(Übung!)*

0.3. Zahlenmengen

Folgende Begriffe und Methoden werden aus der Schule als bekannt vorausgesetzt:

Definition 0.3.1. *Folgende Zahlenmengen sind definiert:*

$\mathbb{N} := \{1, 2, 3, \ldots\}$,	*natürliche Zahlen.*
$\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$.	
$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,	*ganze Zahlen.*
$\mathbb{Q} := \{\, \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N} \,\}$,	*rationale Zahlen, „Brüche“.*
$\mathbb{R} := \{$ *„Dezimalbrüche/Kommazahlen“* $\}$,	*reelle Zahlen.*

Auf diesen Zahlenmengen werden die Rechenoperationen „plus“, „minus“, „mal“ und „geteilt“ (Grundrechenarten) als bekannt vorausgesetzt, und es gelten folgende Inklusionsbedingungen:

$$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}. \qquad \square$$

Bemerkung 0.3.2.

i.) *Es ist in der Literatur nicht eindeutig geregelt, ob die Null in den natürlichen Zahlen liegt.*

ii.) *Die reellen Zahlen werden in jedem einführenden Buch zur Analysis eingehend studiert. In dieser Vorlesung reicht ein „naives“ Verständnis aus der Schule über sie aus, es muß nicht verstanden werden, was ein*

„vollständiger archimedisch angeordneter Körper“

ist. Ausführliches dazu findet sich z.B. in [**GMZ**] *oder* [**FAn1**].

Definition 0.3.3. *Auf den Zahlenmengen existiert eine natürliche Ordnung, d.h. für zwei Zahlen* a *und* b *kann immer entschieden werden, ob gilt:*

$$\begin{aligned} a < b \quad &\rightsquigarrow \quad a \text{ ist kleiner als } b, \\ a \leq b \quad &\rightsquigarrow \quad a \text{ ist kleiner oder gleich } b, \\ a > b \quad &\rightsquigarrow \quad a \text{ ist größer als } b, \\ a \geq b \quad &\rightsquigarrow \quad a \text{ ist größer oder gleich } b. \end{aligned}$$

Insbesondere gilt dabei:

$$a = b \qquad \Longleftrightarrow \qquad a \leq b \quad \textit{und} \quad a \geq b.$$

Es wird als bekannt vorausgesetzt, wie sich die Ordnung mit den Rechenorperationen verträgt. Für eine Zahl a wird mit $|a|$ der Betrag von a bezeichnet, und es gilt:

$$|a| = \begin{cases} a & \textit{für } a \geq 0, \\ -a & \textit{für } a < 0. \end{cases}$$

Das Signum einer Zahl a ist in Abhängigkeit seines Vorzeichens definiert als:

$$\operatorname{sign}(a) := \begin{cases} 1 & \textit{für } a > 0, \\ 0 & \textit{für } a = 0, \\ -1 & \textit{für } a < 0. \end{cases}$$

Insbesondere gelten dann folgende Beziehungen zwischen Signum und Betrag:

$$a = \operatorname{sign}(a) \cdot |a|, \quad |a| = \operatorname{sign}(a) \cdot a \quad \textit{und} \quad \operatorname{sign}(a)^2 = 1 \textit{ für } a \neq 0.$$

(Siehe dazu z.B. auch [**GMZ**] *oder* [**FAn1**]*.)* □

Folgende Aussage wird ebenso als bekannt vorausgesetzt:

Lemma 0.3.4. *Sei $M \subseteq \mathbb{N}_0$ eine nicht-leere Teilmenge. Dann besitzt M ein kleinstes Element. Dieses wird auch Minimum von M genannt und mit $\min(M)$ bezeichnet, d.h. es gilt:*

$$\min(M) \in M \quad \textit{und} \quad \min(M) \leq b \textit{ für alle } b \in M. \qquad \square$$

Nun läßt sich eine wesentliche Aussage über die ganzen Zahlen beweisen:

Satz 0.3.5. *(Division mit Rest in $\mathbb{Z}$)*
Seien a, b in $\mathbb{Z}$ mit $b \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit:

$$a = q \cdot b + r \quad \textit{und} \quad 0 \leq r < |b|.$$

Beweis.

Existenz von $q, r \in \mathbb{Z}$: Es sei folgende Menge betrachtet:

$$M := \{\, a - k \cdot b \mid k \in \mathbb{Z} \} \cap \mathbb{N}_0.$$

Offensichtlich gilt $M \subseteq \mathbb{N}_0$. Die Menge M ist nicht leer, denn es gilt:

$a \geq 0$: Mit $k := 0$ folgt sofort $a = a - k \cdot b \in M$.

$a < 0$: Es ist $(1 - |b|) \leq 0$, und wegen $a < 0$ folgt $a \cdot (1 - |b|) \geq 0$. Mit $k := a \cdot \operatorname{sign}(b)$ gilt dann:

$$a \cdot (1 - |b|) = a - a \cdot |b| = a - a \cdot \operatorname{sign}(b) \cdot b = a - k \cdot b \in M.$$

Da die Menge $M \subseteq \mathbb{N}_0$ nicht leer ist, besitzt sie nach Lemma 0.3.4 ein Minimum $r := \min(M)$, und so gibt es nach der Definition der Menge M ein $q \in \mathbb{Z}$ mit $r = a - q \cdot b$. Dabei gilt $r < |b|$, denn im Fall $r \geq |b|$ würde folgen:

$$0 \leq r - |b| = a - q \cdot b - |b| = a - \big(q + \operatorname{sign}(b)\big) \cdot b \quad \Longrightarrow \quad r - |b| \in M,$$

was wegen $0 \leq r - |b| < r$ der der Minimalität von r widerspräche.

Dann erfüllen q, r die gewünschten Eigenschaften, denn es gilt:

$$r = a - q \cdot b \quad \Longrightarrow \quad a = q \cdot b + r$$

und $0 \leq r < |b|$.

Eindeutigkeit von $q, r \in \mathbb{Z}$: Seien $\tilde{q}, \tilde{r} \in \mathbb{Z}$ ebenfalls Zahlen mit einer Darstellung

$$a = \tilde{q} \cdot b + \tilde{r} \quad \text{und} \quad 0 \leq \tilde{r} < |b|.$$

Wird o.B.d.A. angenommen, daß $r \geq \tilde{r}$ gilt, so folgt mit der Gleichsetzung beider Darstellungen von a:

$$\tilde{q} \cdot b + \tilde{r} = q \cdot b + r \quad \Longrightarrow \quad (\tilde{q} - q) \cdot b = r - \tilde{r} \geq 0.$$

Wegen $\tilde{r} \geq 0$ gilt $r - \tilde{r} \leq r$, und dies liefert mit der vorherigen Abschätzung:

$$0 \leq r - \tilde{r} = (\tilde{q} - q) \cdot b \leq r \quad \Longrightarrow \quad 0 \leq (\tilde{q} - q) \cdot b \leq r.$$

Auf die rechte Ungleichung kann der Betrag angewendet werden, und es folgt mit $k := (\tilde{q} - q)$:

$$0 \leq (\tilde{q} - q) \cdot b \leq r \quad \overset{|\cdot|}{\Longrightarrow} \quad |k| \cdot |b| \leq r$$

Wäre $k \neq 0$, so würde aus $|k| \cdot |b| \leq r$ die Ungleichung $|b| \leq |k| \cdot |b| \leq r$ folgen, im Widerspruch zu $r < |b|$. Also muß $k = 0$ und somit $\tilde{q} = q$ gelten, was dann sofort $\tilde{r} = r$ impliziert. □

Beispiel 0.3.6. *Division mit Rest in $\mathbb{Z}$:*

$$8 = 2 \cdot 3 + 2, \quad -8 = (-3) \cdot 3 + 1, \quad 8 = 4 \cdot 2 + 0.$$

0.4. Abbildungen

Definition 0.4.1. *Seien A und B nicht-leere Mengen. Eine Abbildung (oder auch: Funktion) f von A nach B ist eine Zuordnunsvorschrift, die jedem Element aus A genau ein Element aus B zuordnet. Notation:*

$$f \colon A \longrightarrow B \quad \text{mit} \quad a \mapsto \text{„Zuordnungsvorschrift für } a\text{“}$$
$$\text{(oder:} \quad f(a) := \text{„Zuordnungsvorschrift für } a\text{“).}$$

A ist der Definitionsbereich der Funktion f und B ihr Wertebereich.
Für $a \in A$ heißt das Element $b \in B$ mit $a \mapsto b$ bzw. $f(a) = b$ das Bild von a unter f.
Das Bild der Abbildung f ist diejenige Teilmenge von B, deren Elemente als Bild eines Elementes aus A unter f auftreten:

$$\operatorname{im}(f) := \{\, b \in B \mid \exists\, a \in A : f(a) = b \,\}.$$

Der Graph von f ist definiert als:

$$\operatorname{graph}(f) := \big\{\, \big(a, f(a)\big) \in A \times B \mid a \in A \,\big\}.$$ □

Bemerkung 0.4.2.

i.) *Sind A und B nicht-leere Mengen, so kann eine Abbildung f von A nach B formaler defniert werden als eine Teilmenge $f \subseteq A \times B$, welche folgende Zusatzbedingung erfüllt:*

$$\textit{Zu jedem } a \in A \textit{ gibt es genau ein Tupel } (a, b) \in f.$$

Damit wäre der vage Begriff der „Zuordnungsvorschrift“ in der Definition 0.4.1 vermieden, und es wäre dann $a \mapsto b$ (oder $f(a) := b$) für dasjenige b mit $(a, b) \in f$.
Diese Definition würde eine Abbildung zu einer Menge machen, und es würde sogar $f = \operatorname{graph}(f)$ gelten (tatsächlich gibt die Definition des Graphen von f ja schon einen Hinweis, daß eine Abbildung als Menge aufgefaßt werden kann).
Hier ist dieser formale Ansatz nicht gewählt, um dem Begriff der Abbildung etwas Dynamisches zu geben: Eine Menge hat etwas statisches, sie ist. Aber der Transport von Elementen aus einer Menge in eine andere, der durch eine Zuordnungsvorschrift suggeriert wird, vermittelt Bewegung.

ii.) *Für eine Abbildung geht sowohl aus der Defintion 0.4.1 als auch aus der obigen formaleren Variante hervor, daß Definitions- und Wertebereich Bestandteile ihrer Definition sind. Strenggenommen ist nach Definition 0.4.1 eine Abbildung ein Tripel*

$$\textit{(Definitionsbereich, Wertebereich, Zuordnungsvorschrift).}$$

Damit sind zwei Abbildungen f und g genau dann gleich ($f = g$), wenn sie den gleichen Definitionsbereich und Wertebereich haben und für alle x aus dem Definitionsbereich gilt: $f(x) = g(x)$. □

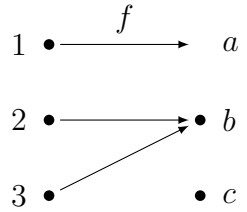
Beispiel 0.4.3. *Seien A und B nicht-leere Mengen.*

i.) *Eine Zuordnungsvorschrift muß nicht unbedingt durch eine Formel gegeben sein wie z.B. in $f(x) := x^2 - 2$. Ist die abzubildende Menge klein, so kann die Abbildung auch durch die direkte Auflistung aller Zuordnungen beschrieben werden:*

$$f\colon \{1, 2, 3\} \longrightarrow \{1, 2, 3\} \quad \textit{mit} \quad 1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2.$$

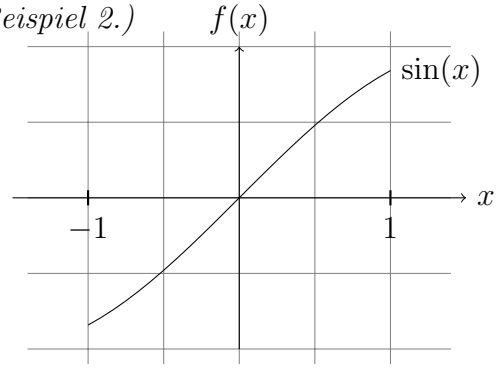
ii.) *Folgende Beispiele stellen Abbildungen dar:*

Beispiel 1.)



$A := \{1, 2, 3\} \quad B := \{a, b, c\}$

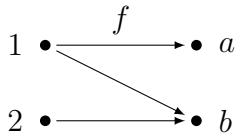
Beispiel 2.)



$A := [-1, 1] := B := [-1, 1] \subseteq \mathbb{R}$

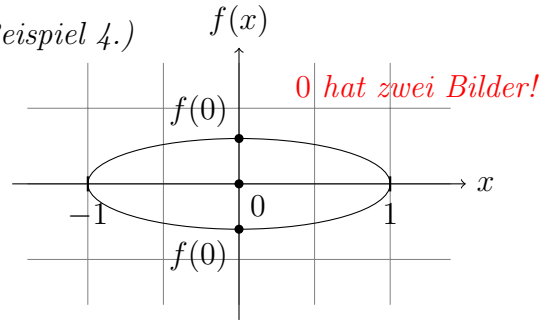
iii.) *Nach der Definition einer Abbildung darf einem a aus A nur <u>ein</u> Element aus B zugeordnet werden. Damit sind folgende Beispiele keine Abbildungen:*

Beispiel 3.) *1 hat zwei Bilder!*



$A := \{1, 2\} \quad B := \{a, b\}$

Beispiel 4.)



$A := [-1, 1] := B := [-1, 1] \subseteq \mathbb{R}$

iv.) $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ *mit* $f(x) := x^2$ *und* $g\colon \mathbb{Q} \longrightarrow \mathbb{R}$ *mit* $g(x) := x^2$ *sind verschiedene Abbilungen, da ihr Definitionsbereich nicht übereinstimmt.* □

Definition 0.4.4. *Sei $f\colon A \longrightarrow B$ eine Abbildung. Für eine Teilmenge $X \subseteq B$ ist das Urbild $f^{-1}(X)$ von X unter f die Menge aller $a \in A$, für die $f(a) \in X$ gilt:*

$$f^{-1}(X) := \{\, a \in A \mid f(a) \in X \,\}.$$

Für ein Element $b \in B$ ist das Urbild unter f definiert als das Urbild der Menge $\{b\} \subseteq B$. Das Urbild eines Elementes $b \in B$ wird auch als Faser von b unter f bezeichnet. Notation:

$$f^{-1}(b) := f^{-1}\big(\{b\}\big) := \{\, a \in A \mid f(a) = b \,\}.$$

Für ein b in $\operatorname{im}(f)$ heißt jedes $a \in f^{-1}(b)$ ein Urbild zu b unter f.
Die Fasern von f sind dann alle Teilmengen von A, die Faser eines $b \in B$ sind. □

Bemerkung 0.4.5.

i.) *Ist $f\colon A \longrightarrow B$ eine Abbildung, so muß für $b \in B$ bei der Benutzung des Begriffs „Urbild“ aufgepaßt werden: <u>das</u> Urbild von b ist die Menge $f^{-1}(b)$, und <u>ein</u> Urbild von b ist ein (nicht unbedingt eindeutiges) Element $a \in f^{-1}(b)$.*

ii.) *Ist $f\colon A \longrightarrow B$ eine Abbildung, so ist mit der Aussage*

$$\text{„}b \in B \text{ besitzt ein Urbild“}$$

gemeint, daß $f^{-1}(b)$ nicht leer ist und damit ein $a \in A$ existiert mit $f(a) = b$. Das Urbild (die Faser) von b existiert ja immer, ist aber evt. die leere Menge.

iii.) *Für eine Abbildung $f\colon A \longrightarrow B$ folgt aus Definition 0.4.4 insbesondere sofort für ein $b \in B$:*

$$f^{-1}(b) \neq \emptyset \qquad \Longleftrightarrow \qquad b \in \operatorname{im}(f).$$

iv.) *Sei $f\colon A \longrightarrow B$ eine Abbildung. Dann liefert folgende Definition für Elemente $x, y \in A$ eine Äquivalenzrelation auf A:*

$$x \sim y \quad := \quad f(x) = f(y).$$

Ist f eine surjektive Abbildung, so entsprechen deren Äquivalenzklassen genau den Fasern von f (Übung!).

v.) Das Studium von Fasern von Abbildungen ist eine wichtige Aufgabe der Mathematik. Sei zur Illustration dessen ein reelles Gleichungssystem gegeben:

$$\begin{aligned} 3xy^2 + 4x &= 7, \\ 3\sin(x)(2y - e^x)z &= 5. \end{aligned}$$

Wird dann folgende Abbildung betrachtet:

$$f\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad (x, y, z) \mapsto \big(3xy^2 + 4x,\ 3\sin(x)(2y - e^x)z\big),$$

dann entspricht die Lösungsmenge des Gleichungssystems der Faser des Punktes $(7, 5) \in \mathbb{R}^2$ unter der Abbildung f. Ein solches (allgemeines) Gleichungssystem ist, wenn überhaupt, nicht leicht zu lösen. Da f differenzierbar ist, kann versucht werden, eine Lösung mit Hilfsmittlen der Analysis zu finden.
Ist das Gleichungssystem von speziellerer Form, ein „lineares Gleichungssystem“ wie das folgende:

$$\begin{aligned} 3x + 4y + 5z &= 2, \\ 4x - 7z &= 1, \\ y - z &= 0, \end{aligned}$$

und die dazu passende Abbildung:

$$g\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \quad \textit{mit} \quad (x, y, z) \mapsto (3x + 4y + 5z,\ 4x - 7z,\ y - z),$$

so kann die Lösungsmenge des linearen Gleichungssystems und damit die Faser von $(2, 1, 0)$ unter der Abbildung g mit dem Gauß-Algorithmus berechnet werden. Die obige Abbildung g wird sich im Verlauf der Vorlesung als lineare Abbildung zwischen den Vektorräumen $\mathbb{R}^3$ und $\mathbb{R}^3$ herausstellen, und die Fasern solcher spezieller, nämlich linearer Abbildungen sind alle übersichtlich beschreibbar. □

Zu jeder Menge existiert eine besonders ausgezeichnete Abbildung:

Definition 0.4.6. *Sei M eine nicht-leere Menge. Dann ist die Identitätsabbildung auf M definiert durch:*

$$\mathrm{id}_M\colon M \longrightarrow M \quad \textit{mit} \quad x \mapsto x. \qquad \square$$

Folgende spezielle Eigenschaften von Abbildungen spielen eine große Rolle:

Definition 0.4.7. *Sei $f\colon A \longrightarrow B$ eine Abbildung. Sie heißt injektiv, falls für alle $x, y \in A$ gilt:*

$$f(x) = f(y) \quad \Longrightarrow \quad x = y.$$

Die Abbildung f heißt surjektiv, falls $\mathrm{im}(f) = B$ gilt, und sie heißt bijektiv, falls sie gleichzeitig injektiv und surjektiv ist. □

Bemerkung 0.4.8.
Sei $f\colon A \longrightarrow B$ eine Abbildung. Dann gilt nach den vorherigen Definitionen offensichtlich:

f injektiv: Folgende Aussagen sind äquivalent:
- *i.) f ist injektiv.*
- *ii.) Für alle $a, b \in A$ gilt: $f(a) = f(b) \quad \Longrightarrow \quad a = b$.*
- *iii.) Für alle $a, b \in A$ gilt: $a \neq b \quad \Longrightarrow \quad f(a) \neq f(b)$.*
- *iv.) Jede Faser von f enthält höchstens ein $a \in A$.*

v.) *Jedes $b \in B$ ist das Bild von höchstens einem $a \in A$.*
vi.) *Jedes $b \in B$ besitzt höchstens ein Urbild.*

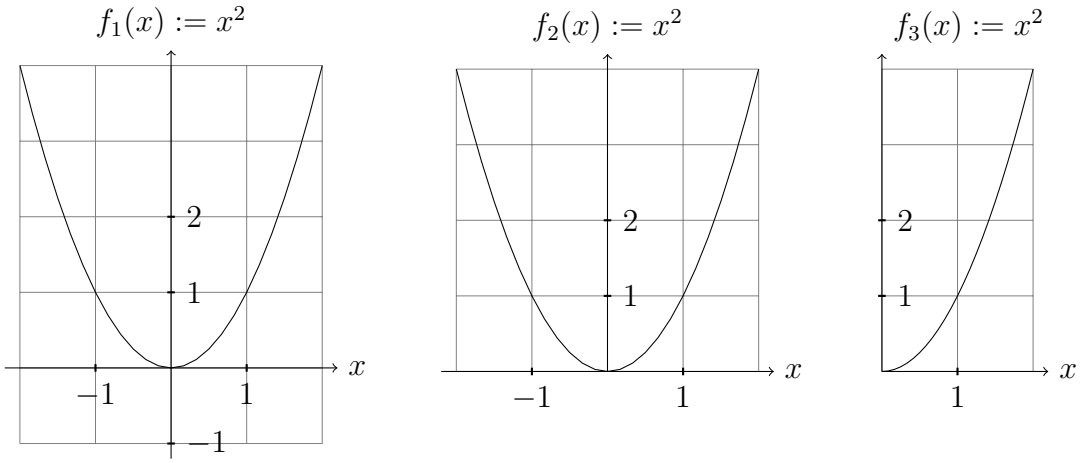
f surjektiv: Folgende Aussagen sind äquivalent:
i.) *f ist surjektiv.*
ii.) $\operatorname{im}(f) = B$.
iii.) *Jede Faser von f ist nicht leer.*
iv.) *Jedes $b \in B$ besitzt mindestens ein $a \in A$ mit $f(a) = b$.*
v.) *Jedes $b \in B$ besitzt mindestens ein Urbild.*

f bijektiv: Folgende Aussagen sind äquivalent:
i.) *f ist bijektiv.*
ii.) *Jede Faser von f ist einelementig.*
iii.) *Jedes $b \in B$ besitzt genau ein $a \in A$ mit $f(a) = b$.*
iv.) *Jedes $b \in B$ besitzt genau ein Urbild.* □

Beispiel 0.4.9.

i.) *Für jede nicht-leere Menge M ist id_M eine Bijektion.*
ii.) *In Beispiel 0.4.3 gilt: Die Abbildung aus Beispiel 1.) ist weder injektiv noch surjektiv, und die Abbildung aus Beispiel 2.) ist injektiv, aber nicht surjektiv.*
iii.) *Die Abbildung $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ mit $n \mapsto n+1$ ist injektiv, aber nicht surjektiv.*
iv.) *Es sei $\mathbb{R}_0^+ := \{\, x \in \mathbb{R} \mid x \geq 0 \,\}$. Dann gilt für folgende Abbildungen:*

$f_1\colon \mathbb{R} \longrightarrow \mathbb{R}$	*mit* $x \mapsto x^2$:	*f_1 ist weder injektiv noch surjektiv.*
$f_2\colon \mathbb{R} \longrightarrow \mathbb{R}_0^+$	*mit* $x \mapsto x^2$:	*f_2 ist nicht injektiv, aber surjektiv.*
$f_1\colon \mathbb{R}_0^+ \longrightarrow \mathbb{R}_0^+$	*mit* $x \mapsto x^2$:	*f_3 ist bijektiv.*



Die Abbildungen f_1, f_2 und f_3 sind alle verschieden, denn ihr Definitions- und Wertebereich stimmt nie bei zweien von ihnen überein. □

Nun zu einem wesentlichen Begriff für Abbildungen, deren Komposition:

Definition 0.4.10. *Seien $f\colon A \longrightarrow B$ und $g\colon B \longrightarrow C$ Abbildungen. Dann ist die Komposition von f und g (oder auch: g nach f) definiert durch:*

$$g \circ f\colon A \longrightarrow C \quad \textit{mit} \quad x \mapsto g\big(f(x)\big)$$

Reihenfolge in der Notation beachten: erst f, dann g ausführen! Anschauung:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

□

Die Komposition von Abbildungen verträgt sich folgendermaßen mit den Eigenschaften injektiv, surjektiv und bijektiv:

LEMMA 0.4.11. *Seien $f\colon A \longrightarrow B$ und $g\colon B \longrightarrow C$ Abbildungen. Dann gilt:*

$$\begin{aligned} f,\ g \text{ injektiv} \quad &\Longrightarrow \quad g \circ f \text{ injektiv.} \\ f,\ g \text{ surjektiv} \quad &\Longrightarrow \quad g \circ f \text{ surjektiv.} \\ f,\ g \text{ bijektiv} \quad &\Longrightarrow \quad g \circ f \text{ bijektiv.} \end{aligned}$$

BEWEIS.

f, g injektiv: Es ist für $x, y \in A$ zu zeigen:

$$(g \circ f)(x) = (g \circ f)(y) \quad \Longrightarrow \quad x = y.$$

Aus f und g injektiv folgt dazu sofort:

$$(g \circ f)(x) = (g \circ f)(y) \implies g\big(f(x)\big) = g\big(f(y)\big) \overset{g \text{ injektiv}}{\Longrightarrow} f(x) = f(y) \overset{f \text{ injektiv}}{\Longrightarrow} x = y.$$

f, g surjektiv: Es ist für $c \in C$ zu zeigen, daß es ein $a \in A$ gibt mit $(g \circ f)(a) = c$.

$$\left.\begin{aligned} g \text{ surjektiv} \quad &\Longrightarrow \quad \exists\, b \in B : g(b) = c, \\ f \text{ surjektiv} \quad &\Longrightarrow \quad \exists\, a \in A : f(a) = b \end{aligned}\right\} \quad \Longrightarrow \quad (g \circ f)(a) = g\big(f(a)\big) = g(b) = c.$$

f, g bijektiv: f, g sind beide injektiv und surjektiv, also ist nach den vorherigen Aussagen auch $g \circ f$ injektiv und surjektiv und damit bijektiv. □

Weitere wesentliche Eigenschaften der Komposition von Abbildungen beschreibt die folgende Aussage:

LEMMA 0.4.12. *Seien A, B, C und D nicht-leere Mengen und*

$$f\colon A \longrightarrow B, \quad g\colon B \longrightarrow C \quad \text{und} \quad h\colon C \longrightarrow D$$

Abbildungen. Dann gilt:

$$h \circ (g \circ f) = (h \circ g) \circ f \qquad \text{und} \qquad f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f.$$

BEWEIS.

$h \circ (g \circ f) = (h \circ g) \circ f$: Beide Abbildungen haben den Definitionsbereich A und den Wertebereich D, und sie stimmen auf dem Definitionsbereich überein, denn für $x \in A$ gilt:

$$\big(h \circ (g \circ f)\big)(x) = h\big((g \circ f)(x)\big) = h\Big(g\big(f(x)\big)\Big) = (h \circ g)\big(f(x)\big) = \big((h \circ g) \circ f\big)(x).$$

$f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$: Dies folgt sofort aus den Definitionen, denn alle drei Abbildungen haben den Definitionsbereich A und den Wertebereich B, und stimmen auf dem Definitionsbereich überein. □

Definition 0.4.13. *Sei $f\colon A \longrightarrow B$ eine Abbildung. Eine Abbildung $g\colon B \longrightarrow A$ heißt Umkehrabbildung oder auch inverse Abbildung (kurz: Inverse) zu f, falls gilt:*

$$f \circ g = \mathrm{id}_B \quad \textit{und} \quad g \circ f = \mathrm{id}_A\,. \qquad \square$$

Bemerkung 0.4.14. *Ist g eine Umkehrabbildung zu f, so ist offensichtlich auch f eine Umkehrabbildung zu g.* $\square$

Es läßt sich ein klares Kriterium herleiten, wann eine Abbildung eine Umkehrabbildung besitzt:

Satz 0.4.15. *Sei $f\colon A \longrightarrow B$ eine Abbildung. Dann sind äquivalent:*

$$f \textit{ besitzt eine Umkehrabbildung} \quad \Longleftrightarrow \quad f \textit{ ist bijektiv.}$$

Beweis.

$\Longrightarrow$: Sei g eine Umkehrabbildung zu f, d.h. es gilt $f \circ g = \mathrm{id}_B$ und $g \circ f = \mathrm{id}_A$. f ist injektiv, denn für $x, y \in A$ folgt:

$$\begin{aligned} f(x) = f(y) \quad &\Longrightarrow \quad g\big(f(x)\big) = g\big(f(y)\big) \quad &&\Longrightarrow \quad (g \circ f)(x) = (g \circ f)(y) \\ &\Longrightarrow \quad \mathrm{id}_A(x) = \mathrm{id}_A(y) &&\Longrightarrow \quad x = y. \end{aligned}$$

f ist surjektiv, denn für $b \in B$ folgt:

$$b = \mathrm{id}_B(b) = (f \circ g)(b) = f\big(g(b)\big),$$

so daß $a := g(b)$ dann wegen $f(a) = b$ ein Urbild von b ist.

$\Longleftarrow$: Bei bijektivem f sind alle Fasern einelementig (Bemerkung 0.4.8). Sei dann $\{a_b\} := f^{-1}(b)$ für $b \in B$. Die Vorschrift $g(b) := a_b$ liefert eine Abbildung $g\colon B \longrightarrow A$, und es reicht zu zeigen, daß die Gleichungen

$$f \circ g = \mathrm{id}_B \quad \text{und} \quad g \circ f = \mathrm{id}_A\,.$$

erfüllt sind, da dann g eine Umkehrabbildung von f ist. Dazu gilt Für alle $b \in B$:

$$(f \circ g)(b) = f\big(g(b)\big) = f(a_b) = b = \mathrm{id}_B(b) \quad \Longrightarrow \quad f \circ g = \mathrm{id}_B\,.$$

Die andere Gleichung ergibt sich daraus, daß für $f(a) \in B$ die einelementige Faser gleich $\{a\}$ sein muß und damit $g\big(f(a)\big) = a$. Für $a \in A$ folgt dann:

$$(g \circ f)(a) = g\big(f(a)\big) = a = \mathrm{id}_A(a) \quad \Longrightarrow \quad g \circ f = \mathrm{id}_A\,. \qquad \square$$

Bisher ist noch nicht geklärt, ob es zu einer Abbildung mehrere Umkehrabbildungen geben kann. Daß dies nicht der Fall ist, zeigt folgende Aussage:

Lemma 0.4.16. *Sei $f\colon A \longrightarrow B$ eine Abbildung. Existiert dann eine Umkehrabbildung g von f, so ist diese eindeutig bestimmt.*

Beweis. Sei $\tilde{g}\colon B \longrightarrow A$ eine weitere Umkehrabbildung von f. Dann gilt

$$f \circ g = \mathrm{id}_B, \quad g \circ f = \mathrm{id}_A \quad \text{und} \quad f \circ \tilde{g} = \mathrm{id}_B, \quad \tilde{g} \circ f = \mathrm{id}_A,$$

und mit Lemma 0.4.12 folgt:

$$\tilde{g} \overset{(0.4.12)}{=} \tilde{g} \circ \mathrm{id}_B = \tilde{g} \circ (f \circ g) \overset{(0.4.12)}{=} (\tilde{g} \circ f) \circ g = \mathrm{id}_A \circ g \overset{(0.4.12)}{=} g. \qquad \square$$

Damit ist nun folgende Definition möglich:

Definition 0.4.17. *Sei $f\colon A \longrightarrow B$ eine Abbildung. Wenn f eine Umkehrabbildung besizt (und diese ist dann eindeutig nach Lemma 0.4.16), so wird sie mit f^{-1} bezeichnet.* □

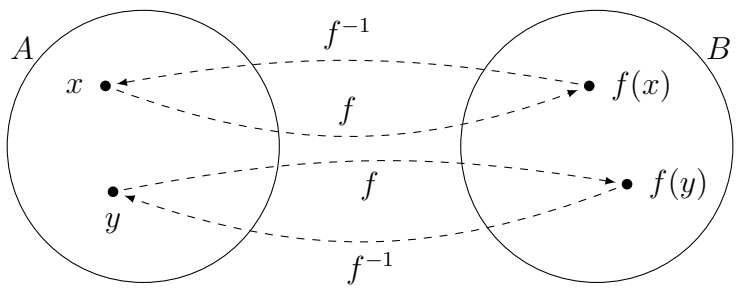
Bemerkung 0.4.18. *Ist $f\colon A \longrightarrow B$ eine Abbildung, so ist der Ausdruck $f^{-1}(b)$ für ein $b \in B$ mehrdeutig:*

i.) $f^{-1}(b)$ kann die Faser von b bzgl. f bedeuten (0.4.4) und ist dann eine Teilmenge von A. Dies ist für jede Abbildung definiert.

ii.) $f^{-1}(b)$ kann das Bild von b unter der Umkehrabbildung f^{-1} von f bedeuten und ist dann ein Element von A. Dies ist jedoch nur bei bijektivem f möglich, da nur dann eine Umkehrabbildung existiert.

Es ist fast immer aus dem Kontext klar, was gemeint ist. Ansonsten muß es genauer kommentiert werden. □

Ist $f\colon A \longrightarrow B$ eine Bijektion, so liefert sie eine Eins-zu-Eins-Zuordnung von Elementen aus A und B, wie z.B. der Beweis der Existenz einer Umkehrabbildung in Satz 0.4.15 illustriert oder die folgende Skizze:



Dies liefert eine Definition, wann zwei Mengen als „gleichgroß“ anzusehen sind: wenn es eine Eins-zu-Eins-Zuordnung ihrer Elemente zueinander gibt. Für endliche Mengen kann offensichtlich auch mit der Anzahl ihrer Elemente argumentiert werden, und „gleichgroß„ mit „gleicher Anzahl von Elementen“ beschrieben werden kann. Aber bei unendlich großen Mengen ist dies nicht möglich.

Definition 0.4.19. *Zwei nicht-leere Mengen A und B haben die gleiche Mächtigkeit, falls es eine Bijekion zwischen ihnen gibt. Notation:*

$$A \text{ und } B \text{ gleichmächtig:} \quad |A| = |B|.$$

Eine nicht-leere Menge M heißt endlich, wennn es ein $n \in \mathbb{N}$ gibt, so daß M die gleiche Mächtigkeit hat wie die Menge $\{1, \ldots, n\}$. Dann heißt M auch Menge der Ordnung (oder Mächtigkeit) n und es wird notiert: $|M| = n$. Ist M keine endliche Menge, so heißt sie unendlich, und es wird notiert: $|M| = \infty$.
Ist ein Menge endlich oder gleichmächtig zu $\mathbb{N}$, so heißt sie abzählbar, ansonsten wird sie als überabzählbar bezeichnet. □

Bemerkung 0.4.20.

i.) Für die beiden Mengen $A := \{a_1, \ldots, a_n\}$ und $B := \{b_1, \ldots, b_n\}$ gilt

$$|A| = |B| = n,$$

und damit folgt für jede Abbildung $f\colon A \longrightarrow B$ offensichtlich:

$$f \text{ injektiv} \quad \Longleftrightarrow \quad f \text{ surjektiv} \quad \Longleftrightarrow \quad f \text{ bijektiv.}$$

Daß sich eine solche Aussage nicht auf unendliche Mengen übertragen läßt, zeigt die Abbildung $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ mit $f(n) := n+1$, die injektiv, aber nicht surjektiv und damit auch nicht bijektiv ist.

ii.) *Die obige spezielle Eigenschaft von Abbildungen zwischen endlichen Mengen gleicher Ordnung kann sogar zu einer Definition von endlichen und unendlichen Mengen genutzt werden:*

Die Menge M heißt endlich, falls für jede Abbildung $f\colon M \longrightarrow M$ gilt:

$$f \text{ injektiv} \quad \Longleftrightarrow \quad f \text{ surjektiv} \quad \Longleftrightarrow \quad f \text{ bijektiv.}$$

Die Menge M heißt unendlich, wenn es eine Abbildung $f\colon M \longrightarrow M$ gibt, für die gilt:

$$f \text{ ist injektiv, aber nicht surjekiv.}$$

Eine unendliche Menge könnte auch definiert werden durch die Forderung der Existenz einer Abbildung $f\colon M \longrightarrow M$ mit:

$$f \text{ ist surjektiv, aber nicht injektiv.}$$

Die Definitionen sind äquivalent zu denen in Definition 0.4.19.

iii.) *Folgende Teilmengen sind jeweils echt in der nächsten enthalten:*

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

Trotzdem existieren zwischen allen diesen Mengen Bijektionen, und sie haben damit alle die gleiche Mächtikkeit und sind abzählbar. Ein Beispiel für eine solche Bijektion ist die Abbildung:

$$f\colon \mathbb{N}_0 \longrightarrow \mathbb{N} \quad \text{mit} \quad f(n) := n+1.$$

Die weiteren Bijektionen zu finden, ist eine kleine Übung, wobei eine Bijektion zwischen $\mathbb{N}$ und $\mathbb{Q}$ mittels des ersten Cantorschen Diagonalverfahrens konstruiert werden kann (siehe z.B. [**WAn1**, Seite 40-41]*).* □

Es sollen noch kurz spezielle Abbildungsmengen eingeführt werden, die im weiteren Verlauf immer wieder auftauchen:

Definition 0.4.21. *Seien A und B nicht-leere Mengen. Dann wird die Menge aller Abbildungen von A nach B mit $\mathrm{Abb}(A,B)$ oder auch B^A bezeichnet:*

$$\mathrm{Abb}(A,B) := \{\, f\colon A \longrightarrow B \mid f \text{ Abbildung} \,\}.$$

Sei M eine nicht-leere Menge und $f \in \mathrm{Abb}(M,M)$. Ein $x \in M$ mit $f(x) = x$ heißt Fixpunkt von f, und eine Teilmenge $X \subseteq M$ mit $f(X) \subseteq X$ invariant unter f.
Die Menge aller Bijektionen von M in sich selbst wird mit $S(M)$ bezeichnet, und die Elemente von $S(M)$ heißen Permutationen von M:

$$S(M) := \{\, f\colon M \longrightarrow M \mid f \text{ ist eine Bijektion} \,\}.$$

Ist $n \in \mathbb{N}$, so wird für die spezielle Menge $M := \{1,\ldots,n\}$ die Menge $S(M)$ auch kurz mit S_n bezeichnet:

$$S_n := S\big(\{1,\ldots,n\}\big) := \big\{ f\colon \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\} \mid f \text{ ist eine Bijektion} \big\}.$$

(Die Menge S_n heißt auch die Symmetrische Gruppe und ihre Elemente einfach Permutationen. Die Gruppenstruktur auf dieser Menge wird später betrachtet.) □

Bemerkung 0.4.22. *Sei M eine nicht-leere Menge.*

i.) *Es gilt:* $S(M) \subseteq \mathrm{Abb}(M, M)$.

ii.) *Die Menge $S(M)$ ist nicht leer, denn es gilt* $\mathrm{id}_M \in S(M)$.

iii.) *Ist $f \in S(M)$, so ist f bijektiv, besitzt eine Umkehrabbildung f^{-1}, und es gilt auch $f^{-1} \in S(M)$ (0.4.15).*

iv.) *Sind $f, g \in S(M)$, so gilt nach Lemma 0.4.11 auch $f \circ g, g \circ f \in S(M)$.* □

Definition 0.4.23. *Sei $f\colon A \longrightarrow B$ eine Abbildung und $X \subseteq A$ eine nicht-leere Teilmenge. Dann wird mit $f_{|X}$ die Einschränkung von f auf X bezeichnet und ist diejenige Abbildung von X nach B, für die gilt:*

$$f_{|X}(a) = f(a) \quad \text{für alle} \quad a \in X.$$

Gilt $A = B$ und ist $X \subseteq A$ eine f-invariante Teilmenge, so wird die Einschränkung $f_{|X}$ auch als Abbildung von X nach X aufgefaßt, also sowohl der Definitionsbereich als auch der Wertebereich eingeschränkt. □

Bemerkung 0.4.24. *Bei der Einschränkung von Abbildungen auf Teilmengen des Definitionsbereiches wird oft stillschweigend der „passende“ Wertebereich angenommen, da meist aus dem Kontext klar ist, was gemeint ist. Im Zweifelsfall muß dies dann genauer kommentiert werden.*
Für $f\colon A \longrightarrow B$ und Teilmengen $X \subseteq A$ und $Y \subseteq B$ mit $f(X) \subseteq Y$ könnte eine Einschränkung des Definitionsbereichs auf X und des Wertebereichs auf Y z.B. mit $f_{|X,Y}$ oder $f_{|X \to Y}$ notiert werden. Dies ist im allgemeinen aber zu schwerfällig. □

Die folgende Definition spezieller Permutationen aus S_n und ihrer besonderen Zykeldarstellung führt später zu einer sehr nützlichen Zykeldarstellung von allgemeinen Permutationen aus S_n:

Definition 0.4.25. *Eine Permutation $\sigma \in S_n$ heißt zyklisch, falls es eine Teilmenge $T := \{a_1, \ldots, a_k\} \subseteq \{1, \ldots, n\}$ gibt mit $k \geq 2$, so daß gilt:*

$$\sigma_{|\{1,\ldots,n\}\setminus T} = \mathrm{id}_{|\{1,\ldots,n\}\setminus T}, \quad \text{und für } a_j \in T \text{ gilt:} \quad \sigma(a_j) = \begin{cases} a_{j+1} & \text{für } j \neq k, \\ a_1 & \text{für } j = k. \end{cases}$$

Dann ist $(a_1\, a_2\, \ldots\, a_k)$ eine Darstellung von σ als k-Zykel. T heißt der Träger von σ (bzw. des Zykels). □

Bemerkung 0.4.26.

i.) *Ist $\sigma \in S_n$ eine zyklische Permutation mit dem Träger $T := \{a_1, \ldots, a_k\}$ und einer Zykeldarstellung $(a_1\, a_2\, \ldots\, a_k)$, so ist daraus die Abbildungsvorschrift von σ folgendermaßen abzulesen: $i \notin T$ ist ein Fixpunkt von σ, und ein $i \in T$ wird von σ folgendermaßen abgebildet:*

$$\begin{tikzcd} a_1 \arrow[r, "\sigma"] & a_2 \arrow[r, "\sigma"] & a_3 \arrow[r, "\sigma"] & \ldots \arrow[r, "\sigma"] & a_k \arrow[llll, bend left, "\sigma"] \end{tikzcd}$$

Eine Zykeldarstellung von σ ist dabei nicht eindeutig: alle Rotationen des Zykels liefert wieder eine Zykeldarstellung, wie obige Skizze sofort klar macht. Dies sind

aber die einzigen Variationsmöglichkeiten in der Zykeldarstellung, und so hat σ genau die folgenden möglichen Zykeldarstellungen:

$$(a_1\, a_2\, \ldots\, a_k), \quad (a_k\, a_1\, a_2\, \ldots\, a_{k-1}), \quad \ldots \quad , \quad (a_2\, a_3\, \ldots\, a_{k-1}\, a_k\, a_1).$$

ii.) *Ist eine Teilmenge $T := \{a_1, \ldots, a_k\} \subseteq \{1, \ldots, n\}$ mit $k \geq 2$ gegeben, so existiert genau eine zyklische Permutation $\sigma \in S_n$, die eine Zykeldarstellung $(a_1\, a_2\, \ldots\, a_k)$ hat.*

iii.) *Wird bei der Definition von zyklischen Permutationen die Bedingung $k \geq 2$ weggelassen und damit $k = 1$ erlaubt, so vergrößert sich die Menge der zyklsichen Permutationen genau um die Identität* id. *In deren Fall kann als Trägermenge jede beliebige einelementige Menge $\{k\}$ mit $1 \leq k \leq n$ gewählt werden, und die resultierende Zykeldarstellung ist dann von der Form (k).*
Bei dieser Definitionsvariante (mit $k = 1$ erlaubt) wäre dann nur bei der zusätzlichen zyklischen Permutation id *die Zykeldarstellung nicht bis auf „Rotatin des Zykels“ eindeutig. Auch wäre bei ihr die Anschauung verletzt, daß eine zyklische Permutation außerhalb des Trägers nur Fixpunkte hat und innerhalb des Trägers alle Elemente „zyklisch“ bewegt: denn für* id *ist der einelementige Träger selbst ein Fixpunkt und wird eben nicht bewegt.*

iv.) *Es seien die beiden folgenden Permutationen gegeben:*

$$\sigma_1 \in S_2 \quad \textit{mit} \quad \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 1 \end{matrix} \qquad \textit{und} \qquad \sigma_2 \in S_3 \quad \textit{mit} \quad \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{matrix}.$$

Beide Permutationen haben eine Zykeldarstellung der Form $(1\,2)$, da der Fixpunkt 3 von σ_2 in einer Zykeldarstellung von σ_2 nicht notiert wird. Daher ist es falsch, $\sigma_1 = (12) = \sigma_2$ zu schreiben, denn die beiden Abbildungen σ_1 und σ_2 sind wegen unterschiedlicher Definitionsbereiche nicht gleich.
Einer Zykeldarstellung kann nicht der Definitonsbereich (und damit Wertebereich) der dargestellten Permutation angesehen werden.

v.) *Ist $\sigma \in S_n$ eine zyklische Permutation mit dem Träger T, so ist auch σ^{-1} eine zyklische Permutation mit dem Träger T: Die Abbildungsvorschrift auf dem Träger ist dann der umkehrte Zykeldurchlauf:*

$$\sigma: \qquad \begin{tikzcd} a_1 \arrow[r, "\sigma"] & a_2 \arrow[r, "\sigma"] & a_3 \arrow[r, "\sigma"] & \ldots \arrow[r, "\sigma"] & a_k \arrow[llll, bend left, "\sigma"] \end{tikzcd}$$

$$\sigma^{-1}: \qquad \begin{tikzcd} a_1 & a_2 \arrow[l, "\sigma^{-1}"'] & a_3 \arrow[l, "\sigma^{-1}"'] & \ldots \arrow[l, "\sigma^{-1}"'] & a_k \arrow[l, "\sigma^{-1}"'] \arrow[llll, bend left, "\sigma^{-1}"] \end{tikzcd}$$

Daraus folgt sofort für Zykeldarstellungen von σ und σ^{-1}:

Zykeldarstellung von σ: $\quad (a_1\, a_2\, \ldots\, a_k)$

Zykeldarstellung von σ^{-1}: $\quad (a_k\, a_{k-1}\, \ldots\, a_2\, a_1)$

vi.) *Haben zwei zyklische Permutationen $\sigma_1, \sigma_2 \in S_n$ disjunkte Träger, so gilt:*

$$\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1. \qquad \square$$

0.5. Vollständige Induktion

Es seien folgende Aussagen über die natürlichen Zahlen betrachtet (die im übrigen alle wahr sind):

A: Für alle $n \in \mathbb{N}$ gilt: $n + 1 \leq 2n$.

B: Die Summe der ersten n Zahlen ist gleich $\frac{n(n+1)}{2}$.

C: Die Summe der ersten n ungeraden Zahlen ist gleich n^2.

D: Für alle $n \in \mathbb{N}$ gilt: Hat die Menge M die Ordnung n, so hat ihre Potenzmenge die Ordnung 2^n.

E: Für alle $n \in \mathbb{N}$ gilt: $|S_n| = n!$ (mit $n! := 1 \cdot 2 \cdot \ldots \cdot n$).

Aussage A kann sofort in einer kurzen Zeile bewiesen werden, denn es gilt wegen $1 \leq n$ für alle $n \in \mathbb{N}$:

$$n + 1 \leq n + n = 2n.$$

Bei den weiteren Aussagen fällt es nicht so leicht, einen direkten Beweis für die jeweilige Aussage zu finden. Die Idee ist nun, *eine Aussage* über alle natürlichen Zahlen als eine *Menge von Aussagen* über jeweils eine einzelne natürliche Zahl aufzufassen:

Aussage B: Die Summe der ersten n Zahlen ist $\frac{n(n+1)}{2}$

wird zu der Menge von Aussagen:

Aussage B_1: Die Summe von 1 bis 1 ist gleich $\frac{1(1+1)}{2}$.
Aussage B_2: Die Summe von 1 bis 2 ist gleich $\frac{2(2+1)}{2}$.
Aussage B_3: Die Summe von 1 bis 3 ist gleich $\frac{3(3+1)}{2}$.
$\vdots$
Aussage B_k: Die Summe von 1 bis k ist gleich $\frac{k(k+1)}{2}$.
$\vdots$

Offensichtlich ist die Aussage B_1 wahr, und auch B_2 und B_3 können sofort verifiziert werden. Aber es können nicht alle Aussagen einzeln überprüft werden, da es unendlich viele sind. Hier hilft nun der folgende Trick:
Wenn nun die Aussage B_k wahr wäre, so würde folgen:

$$\underbrace{1 + 2 + \ldots + k}_{= \frac{k(k+1)}{2}, \text{ falls } B_k \text{ wahr}} + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2} = \frac{(k+1)\big((k+1)+1\big)}{2},$$

und die Aussage B_{k+1} wäre auch gültig.
Damit wäre es nun möglich, da k ja beliebig aus $\mathbb{N}$ gewählt war, von der wahren Aussage B_1 startend immer einen Schritt nach oben zu laufen: aus B_1 wahr folgt B_2 wahr, aus B_2 wahr folgt B_3 wahr usw.
Es scheint sofort klar, daß dann alle Aussagen gelten, aber es ist Vorsicht geboten: das „Nach-oben-Laufen“ ist ja ein nicht endender Prozeß...

Tatsächlich funktioniert die Methode trotzdem, wie der folgende Satz zeigt, und der Beweis basiert auf dem anschaulichen Lemma 0.3.4, daß jede Teilmenge der natürlichen Zahlen ein Minimum besitzt:

Satz 0.5.1. *(Vollständige Induktion I)*
Es sei eine über die natürlichen Zahlen indizierte Menge von Aussagen gegeben:

$$A_1, A_2, A_3, \ldots$$

Weiter seien die folgenden beiden Bedingungen erfüllt:

Induktionsanfang: *Die Aussage A_1 ist wahr.*

Induktionsschritt: *Wenn die Aussage A_n wahr ist, dann gilt auch die Aussage A_{n+1}.*

Dann sind alle Aussagen A_i wahr.

Beweis. Es sei folgende Teilmenge der natürlichen Zahlen betrachtet:

$$M := \{\, i \in \mathbb{N} \mid A_i \text{ ist falsch} \,\}.$$

Angenommen, die Menge M wäre nicht leer. Dann besäße M als nicht-leere Teilmenge von $\mathbb{N}_0$ nach Lemma 0.3.4 ein Minimum $k := \min(M)$. Weil die Induktionsannahme erfüllt ist, muß $k > 1$ gelten. Nach der Wahl von k ist dann A_{k-1} eine wahre Aussage. Da auch der Induktionsschritt gilt, folgt aus A_{k-1} wahr, daß A_k eine wahre Aussage ist, im Widerspruch zur Definition von k. Also muß die Menge M leer sein, und alle Aussagen sind damit wahr. □

Es ist oft einfacher, obigen „Induktionsschritt“ von A_n auf A_{n+1} durchzuführen, wenn angenommen werden darf, daß *alle* Aussaben A_k mit $k \leq n$ wahr sind, und nicht nur A_n. Auch diese Schlußweise ist erlaubt und liefert ein leicht modifiziertes Verfahren:

Satz 0.5.2. *(Vollständige Induktion II)*
Es sei eine über die natürlichen Zahlen indizierte Menge von Aussagen gegeben:

$$A_1, A_2, A_3, \ldots$$

Weiter seien die folgenden beiden Bedingungen erfüllt:

Induktionsanfang: *Die Aussage A_1 ist wahr.*

Induktionsschritt: *Wenn alle Aussagen A_k für $k \leq n$ wahr sind, dann gilt auch die Aussage A_{n+1}.*

Dann sind alle Aussagen A_i wahr.

Beweis. Es sei folgende Teilmenge der natürlichen Zahlen betrachtet:

$$M := \{\, i \in \mathbb{N} \mid A_i \text{ ist falsch} \,\}.$$

Angenommen, die Menge M wäre nicht leer. Dann besäße M als nicht-leere Teilmenge von $\mathbb{N}_0$ nach Lemma 0.3.4 ein Minimum $k := \min(M)$. Weil die Induktionsannahme erfüllt ist, muß $k > 1$ gelten. Nach der Wahl von k sind dann alle Aussagen A_m mit $1 \leq m < k$ bzw. $1 \leq m \leq k-1$ wahr.
Da auch der Induktionsschritt gilt, folgt aus A_m wahr für alle $m \leq k-1$, daß A_k eine wahre Aussage ist, im Widerspruch zur Definition von k. Also muß die Menge M leer sein, und alle Aussagen sind damit wahr. □

Bemerkung 0.5.3.

i.) *Häufig wird bei der vollständigen Induktion (in beiden Versionen) zusätzlich noch eine Induktionsannahme formuliert: in dieser wird die Aussage für ein n (oder für alle $k \leq n$) als wahr postuliert, um dann den Induktionsschritt auszuführen. Dies ist in den Sätzen 0.5.1 und 0.5.2 schon innerhalb des Induktionsschrittes formuliert.*

ii.) *Der Einfachheit halber wurden hier in beiden Versionen der vollständigen Induktion die Aussagen mit der Eins beginnend numeriert. Das Verfahren gilt natürlich für jeden beliebigen ganzzahligen Startwert.*
Manche Aussagenketten gelten ab $n := -3$, $n := 0$, oder erst ab $n := 7$ etc. $\square$

KAPITEL 1

Grundlegende algebraische Strukturen

1.1. Algebraische Strukturen

Wie schon im Grundlagen-Kapitel angedeutet, besteht ein wichtiger Teil der Mathematik in der Analyse und Klassifikation von Abbildungen, da sich meist ein „praktisches Problem“ durch solche formulieren läßt.
Es ist unmöglich, über alle Mengen und Abbildungen einen Überblick zu bekommen. Fast immer tragen aber die für ein jeweiliges Problem relevanten Mengen eine zusätzliche Struktur, die zur Analyse ausgenutzt werden kann: In Bemerkung 0.4.5 wurde ja schon bei der Umformulierung des Problems „Lösen eines Gleichungssystems“ in „Finden einer Faser“ darauf hingewiesen, daß die jeweiligen Funktionen zusätzliche Eigenschaften haben (differenzierbar und damit auch stetig bzw. lineare Abbildung sein), die bei der Analyse helfen. Diese Eigenschaften der Abbildungen sind nur formulierbar, wenn auf den zugehörigen Mengen (in der Bemerkung jeweils ein $\mathbb{R}^n$) passende Strukturen definiert werden.
Strukturen auf Mengen lassen sich (sehr grob) in drei Typen unterteilen: Ordnungsstrukturen, topologische Strukturen und algebraische Strukturen.

- Bei Ordnungsstrukturen lassen sich Elemente, zumindest teilweise, miteinander vergleichen und sortieren. Beispiele dazu wären die Zahlenmengen mit ihrer Ordnung nach „Größe“, oder die Teilmengen einer Menge mit der Ordnung „Inklusion“, d.h. für $A, B \subseteq M$ ist „A kleiner gleich B“, wenn $A \subseteq B$ gilt. Dieses Konzept einer Struktur ist leicht verständlich.
- Bei topologischen Strukturen ist die Abstraktion schon wesentlich höher, denn darin wird durch den Begriff von Umgebungen (offenen Mengen) das Konzept von „Nähe“ formalisiert. Damit lassen sich dann Aussagen über Approximation (Näherungen) und Konvergenz (Zustreben auf etwas...) formulieren.
- Algebraische Strukturen abstrahieren den Begriff des „Rechnens mit Zahlen“ durch „Verknüpfen von Elementen“ auf Mengen.

Auf gegebenen Strukturen werden dann immer nur Abbildungen betrachtet, die mit dem jeweiligen Strukurtyp „verträglich“ sind.

- Bei Ordnungsstrukturen wird dann Verträglichkeit im allgemeinen so formuliert sein, daß für „a kleiner b“ auch „$f(a)$ kleiner $f(b)$“ ist.
- Verträglichkeit einer Abbildung mit einer topologischen Struktur ist mit Stetigkeit bezeichnet und bedeutet im wesentlichen Konvergenzerhaltung.
- Bei algebraischen Strukturen ist das Grundprinzip der Strukturverträglichkeit, daß „Rechnen“ und Abbilden vertauscht werden kann:

  das Bild einer Verknüpfung ist gleich der Verknüpfung der Bilder,

  oder auch:

  erst verknüpfen, dann abbilden = erst abbilden, dann verknüpfen.

Definitionen und elementare Eigenschaften.

Definition 1.1.1. *Sei M eine nicht-leere Menge. Eine Abbildung*

$$*\colon M \times M \longrightarrow M$$

heißt innere Verknüpfung auf M. Dabei wird auch folgende Notation genutzt:

$$a * b := *(a, b) \qquad \text{für } a, b \in M.$$

Wird im folgenden $(M, *)$ als algebraische Struktur bezeichnet, so ist damit eine nicht-leere Menge M zusammen mit einer inneren Verknüpfung „$*$“ gemeint.
Gilt für $U \subseteq M$ die Bedingung $*(U \times U) \subseteq U$, so heißt U abgeschlossen bzgl. der Verknüpfung „$*$“, und die Abbildung „$*$“ kann dann auf $U \times U$ eingeschränkt werden. Diese Einschränkung definiert eine innere Verknüpfung auf U und wird ebenfalls mit dem gleichen Symbol „$*$“ bezeichnet (statt „$*|_{U\times U}$“). Ein solches $(U, *)$ heißt dann algebraische Unterstruktur von $(M, *)$. □

Bemerkung 1.1.2. *Der Begriff der algebraischen Struktur ist in diesem Skript kein fest definierter Begriff.*
Es ist zunächst nur eine *nicht-leere Menge zusammen mit* einer *inneren Verknüpfung damit gemeint. Dies wird später ausgebaut, indem auf einer Menge zwei innere Verknüpfungen betrachtet werden, und auch dies fällt dann unter den Sammelbegriff der algebraischen Struktur.*
Im nächsten Kapitel treten dann Vektorräume, die Hauptobjekte dieser Vorlesung, auf, und diese sind Strukturen, die aus zwei Mengen mit insgesamt vier Verknüpfungen bestehen: inneren und (noch zu definierenden) äußeren Verknüpfungen.
Es ließe sich nun sehr allgemein definieren, daß eine algebraische Strukture aus einer oder mehreren Mengen zusammen mit einer oder mehreren inneren Verknüpfungen pro Menge und mehreren äußeren Verknüpfungen zwischen den einzelnen Mengen besteht.
Dies ist jedoch so allgmein und unübersichtlich, daß die Definition nutzlos ist, und so bleibt der Begriff der algebraischen Struktur hier im Ungefähren und wird nur als Sammelbegriff für mehrere konkret nach dem gleichen oben beschriebenen Schema definierte Objekte verwendet. □

Beispiel 1.1.3.

i.) *Auf den Mengen $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sind die Rechenoperationen „$+$“ und „$\cdot$“ jeweils innere Verknüpfungen. Damit ist jede dieser Mengen zusammen mit einer der Verknüpfungen eine algebraische Struktur.*
Wegen der Abgeschlossenheit jeder Menge unter beiden Verknüpfungen ist pro Verknüpfung auch jede Struktur eine Unterstruktur bzgl. einer Obermenge: also ist z.B. $(\mathbb{N}, +)$ eine Unterstruktur von $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$ usw.

ii.) *Die Rechenoperation „$-$“ ist auf $\mathbb{N}$ keine innere Verknüpfung.*

iii.) *Für eine nicht-leere Menge M ist auf $\mathrm{Abb}(M, M)$ die Komposition von Abbildungen eine innere Verknüpfung (Definition 0.4.10). Nach Lemma 0.4.11 ist die Menge $S(M)$ abgeschlossen unter der Komposition und damit $\big(S(M), \circ\big)$ eine Unterstruktur von $\big(\mathrm{Abb}(M, M), \circ\big)$.*

iv.) *Auf der Menge $\mathbb{N}$ ist auch folgendes Beispiel eine innere Verknüpfung:*

$$\hat{}\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad \text{mit} \quad a\,\hat{}\,b := a^b \quad \text{(Potenzieren).}$$ □

Es werden nun einige spezielle Eigenschaften von inneren Verknüpfungen eingeführt und betrachtet:

Definition 1.1.4. *Sei $(M, *)$ eine algebraische Struktur.*
$(M, *)$ erfüllt das Assoziativgesetz, falls für alle $a, b, c \in M$ gilt:

$$(a * b) * c = a * (b * c).$$

$(M, *)$ erfüllt das Kommutativgesetz, falls für alle $a, b \in M$ gilt:

$$a * b = b * a.$$

Dann heißt $(M, *)$ auch assoziative bzw. kommutative algebraische Struktur, und die innere Verknüpfung „$*$“ wird als assoziativ bzw. kommutativ bezeichnet. □

Beispiel 1.1.5.

i.) *Die Mengen $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ sind bzgl. der Rechenoperatoren „$+$“ und „$\cdot$“ assoziative und kommutative algebraische Strukturen.*

ii.) *Auf der Menge $\mathbb{Z}$ ist die Rechenoperation „$-$“ eine innere Verknüpfung, die aber weder assoziativ noch kommutativ ist:*

$$(1-2)-3 = (-1)-3 = -4 \neq 0 = 1-(-1) = 1-(2-3) \quad \textit{und} \quad 1-2 \neq 2-1.$$

iii.) *Für eine nicht-leere Menge M ist auf $\mathrm{Abb}(M, M)$ und damit auch auf $S(M)$ die Komposition von Abbildungen eine assoziative innere Verknüpfung (Beispiel 1.1.3 und Lemma 0.4.12).*
Für $|M| \geq 2$ ist $\big(\mathrm{Abb}(M, M), \circ\big)$ keine kommutative algebraische Struktur, und ebenso für $|M| \geq 3$ auch $\big(S(M), \circ\big)$ nicht. (Übung!).

iv.) *Die algebraische Struktur $(\mathbb{N}, \hat{\ })$ aus Beispiel 1.1.3 erfüllt weder das Assoziativgesetz noch das Kommutativgesetz:*

$$3\hat{\ }(3\hat{\ }3) = 3\hat{\ }27 = 3^{27} = 7625597484987 \neq 19683 = 27^3 = 27\hat{\ }3 = (3\hat{\ }3)\hat{\ }3.$$

Dabei ist $3\hat{\ }(3\hat{\ }3) \neq (3\hat{\ }3)\hat{\ }3$ ein Gegenbeispiel für beide Fälle. □

Bemerkung 1.1.6. *Eine innere Verknüpfung auf einer Menge ist für genau* zwei *Elemente definert: der Ausdruck $3+4+5$ in der algebraischen Struktur $(\mathbb{N}, +)$ macht ersteinmal keinen Sinn. Die Zahlen müssen „Stück für Stück“ addiert werden, was durch Klammern zum Ausdruck gebracht werden kann: $(3+4)+5$ oder $3+(4+5)$. Da in $(\mathbb{N}, +)$ das Assoziativgesetz gilt, sind beide Ausdrücke gleich, und die Klammern werden meist eingespart.*
Tatsächlich werden sogar bei der Addition von beliebig vielen (jedoch endlich vielen!) natürlichen Zahlen keine Klammern gesetzt: dazu muß jedoch ersteinmal per Induktion gezeigt werden, daß das Assoziativgesetz auch bei z.B. 31415 Summanden gilt und bei jeder möglichen Klammerung der Summe das gleiche Ergebnis liefert.
Wie in Beispiel 1.1.3 gezeigt, gilt das Assoziativgesetz nicht in $(\mathbb{N}, \hat{\ })$, so daß in diesem Fall z.B. der Ausdruck $3\hat{\ }3\hat{\ }3$ überhaupt nicht definiert ist. □

Zuersteinmal wird nun das Produkt von n Elementen in einer algebraischen Struktur durch explizite Angabe einer Klammerungsreihenfolge wie folgt definiert:

Definition 1.1.7. *Sei $(M,*)$ eine algebraische Struktur. Dann wird für n Elemente $a_1,\dots,a_n \in M$ deren Verknüpfung definiert durch:*

$$\prod_{i=1}^{n} a_i := \begin{cases} a_1 & \text{für } n=1, \\ \left(\prod_{i=1}^{n-1} a_i\right) * a_n & \text{für } n>1. \end{cases}$$

Bei Verwendung des Verknüpfungssymbols „+ “ wird die Verknüpfung von $a_1,\dots,a_n$ mit $\sum_{i=1}^{n} a_i$ notiert.

Warnung: Es ist nur eine Verknüpfung von endlich vielen Elementen definiert! □

Somit ist festgelegt, daß n Elemente „von links nach rechts“ verknüpft werden sollen:

$$\prod_{i=1}^{n} a_i := \Big(\big((a_1 * a_2) * a_3\big) * \cdots\Big) * a_n.$$

Dies ist nur eine von mehreren Möglichkeiten, ein Produkt von n Elementen zu definieren. Eine andere Klammerung bei der Verknüpfung von n Elementen gibt in nicht-assoziativen algebraischen Strukturen evt. ein anderes Ergebnis. Falls jedoch das Assoziativgesetz gilt, kann ein „allgemeines Assoziativgesetz“ bewiesen werden, bei dem jedwede Klammerung von n Elementen das gleiche Ergebnis liefert, so daß die konkrete Vorgabe in obiger Definition keine Rolle mehr spielt.
Dies allgemein zu diskutieren, erfordert einigen formalen Aufwand für ein doch anschauliches Ergebnis, so daß eine ausführliche Konstruktion auf den Anhang A.1 verschoben ist und hier nur das Endergebnis formuliert ist:

Satz 1.1.8. *(Allgemeines Assoziativgesetz)*
Sei $(M,*)$ eine assoziative algebraische Struktur. Weiter seien $a_1,\dots,a_n \in M$. Dann gilt für alle $i,j \in \mathbb{N}$ mit $i+j=n$:

$$\prod_{t=1}^{n} a_t = \Big(\prod_{t=1}^{i} a_t\Big) * \Big(\prod_{t=1}^{j} a_{t+i}\Big).$$

Insbesondere folgt daraus rekursiv: Alle möglichen Klammerungen bei der Verknüpfung der Elemente $a_1,\dots,a_n$ liefern das gleiche Ergebnis und können somit weggelassen werden.

Beweis.
Siehe Anhang A.1, insbesondere Lemma A.1.3. □

Bemerkung 1.1.9. *Ist $(M,*)$ eine assoziative algebraische Struktur, so kann wegen der Gültigkeit des allgemeinen Assoziativgesetzes bei der Verknüpfung von n Elementen $a_1,\dots,a_n \in M$ auf eine explizite Klammerung verzichtet werden, und es wird salopp geschrieben:*

$$a_1 * a_2 * \cdots * a_n := \prod_{i=1}^{n} a_i.$$ □

Gelten in einer algebraischen Struktur das Assoziativ- und Kommutativgesetz, so läßt sich das Kommutativgesetz ebenfalls auf eine Verknüpfung von mehreren Elementen verallgemeinern. Auch in diesem Fall wird hier nur das Ergebnis zitiert, welches im Anhang A.1 ausführlich hergeleitet ist:

Satz 1.1.10. *(Allgemeines Kommutativgesetz)*
Sei $(M, *)$ eine kommutative und assoziative algebraische Struktur. Weiter seien $a_1, \ldots, a_n \in M$. Dann gilt für alle $f \in S_n$:

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{f(i)}.$$

Beweis.
Siehe Anhang A.1, insbesondere Satz A.1.7. □

Es werden nun zwei spezielle Typen von Elementen in algebraischen Strukturen definiert und betrachtet: neutrale und inverse Elemente.

Definition 1.1.11. *Sei $(M, *)$ eine algebraische Struktur. Sie besitzt ein neutrales Element, falls es ein $e \in M$ gibt mit:*

$$e * m = m * e = m \text{ für alle } m \in M.$$ □

Lemma 1.1.12. *Sei $(M, *)$ eine algebraische Struktur. Besitzt sie ein neutrales Element, so ist dieses eindeutig bestimmt, so daß von dem neutralen Element gesprochen werden kann.*

Beweis. Seien $e, f \in M$ neutrale Elemente. Dann gilt:

$$e \overset{(f \text{ neutral})}{=} e * f \overset{(e \text{ neutral})}{=} f.$$ □

Definition 1.1.13. *Es sei eine algebraische Struktur mit einem neutralen Element gegeben. Ist die innere Verknüpfung mit dem Symbol „+“ notiert, so wird das neutrale Element mit 0 bezeichnet und als Null genannt. Falls die innere Verknüpfung mit dem Symbol „$\cdot$“ notiert ist, wird das neutrale Element mit dem Symbol 1 bezeichnet und als Eins genannt.* □

Beispiel 1.1.14.

i.) $(\mathbb{N}, +)$ *besitzt kein neutrales Element.*
ii.) *Die Mengen $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ besitzen bzgl. der Rechenoperation „+“ das neutrale Element 0.*
iii.) *Die Mengen $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ besitzen bzgl. der Rechenoperation „$\cdot$“ das neutrale Element 1.*
iv.) *Für eine nicht-leere Menge M besizten $\big(\mathrm{Abb}(M, M), \circ\big)$ und $\big(S(M), \circ\big)$ das neutrale Element id_M (Lemma 0.4.12 und Bemerkung 0.4.22).* □

Definition 1.1.15. *Sei $(M, *)$ eine algebraische Struktur mit dem neutralen Element e. Ein Element $a \in M$ heißt invertierbar, falls es ein $b \in M$ gibt mit:*

$$a * b = b * a = e.$$

Dann heißt b inverses Element bzw. Inverses zu a. □

Bemerkung 1.1.16.

i.) *Sei $(M, *)$ eine algebraische Struktur und $a \in M$ invertierbar mit einem Inversen $b \in M$. Dann folgt aus Definition 1.1.15 sofort, daß auch b invertierbar ist und a ein Inverses zu b.*

ii.) *Ist e ein neutrales Element der algebraischen Struktur $(M, *)$, so ist e wegen $e * e = e$ invertierbar und invers zu sich selbst.* □

Lemma 1.1.17. *Sei $(M, *)$ eine assoziative algebraische Struktur mit einem neutralen Element. Besitzt $a \in M$ ein inverses Element, so ist dieses eindeutig bestimmt, und es kann von dem inversen Element zu a gesprochen werden.*

Beweis. Sei e das neutrale Element in M, und seien $b, c \in M$ inverse Elemente zu a. Dann folgt:

$$b = b * e = b * (a * c) \overset{(\text{Ass})}{=} (b * a) * c = e * c = c. \qquad \square$$

Bemerkung 1.1.18.

i.) *Ist die algebraische Struktur $(M, *)$ nicht assoziativ, kann es zu einem Element mehrere Inverse geben. Ein Beispiel dazu ist:*
Sei in $(\mathbb{N}_0, *)$ die innere Verknüpfung definiert durch:

$$n * m := \begin{cases} 0 & \text{für } n, m \in \mathbb{N}, \\ n + m & \text{sonst.} \end{cases}$$

Die Verknüpfung ist nicht assoziativ wegen

$$1 * (2 * 3) = 1 \neq 3 = (1 * 2) * 3.$$

0 ist das neutrale Element, und zu jedem $n \in \mathbb{N}$ ist jedes $m \in \mathbb{N}$ ein Inverses.

ii.) *Das neutrale Element ist immer eindeutig (Lemma 1.1.12), ohne daß eine weitere Forderung an die Verknüpfung gestellt werden muß.* □

Definition 1.1.19. *Sei $(M, *)$ eine assoziative algebraische Struktur mit einem neutralen Element und $a \in M$. Existiert zu $a \in M$ ein Inverses, so ist dies eindeutig bestimmt und wird mit a^{-1} bezeichnet.*
Falls die innere Verknüpfung mit dem Symbol „$+$“ notiert ist, wird das Inverse zu a mit $-a$ bezeichnet. Dann wird auch abkürzend geschrieben: $a - b := a + (-b)$. □

Bemerkung 1.1.20. *Wie in Beispiel 1.1.5 gesehen, ist die Verknüpfung „$-$“ (Minus/Subtraktion) auf den ganzen Zahlen und damit allen deren Zahlenobermengen keine brauchbare, da nicht einmal assoziative Verknüpfung. Da aber in $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ jeweils (additive) Inverse zu allen Elementen existieren, kann mit der Definition 1.1.19 der Term $a - b$ als $a + (-b)$ aufgefaßt werden: damit wäre dann die eigentliche Verknüpfung „$+$“, und die Subtraktion von b nur die Addition des (additiv) Inversen von b.*
Analoges ist zu der Division auf den Zahlenmengen $\mathbb{Q} \setminus \{0\}$ und $\mathbb{R} \setminus \{0\}$ zu sagen: Darin besitzt jedes Element ein multiplikativ Inverses, d.h. zu a existiert ein a^{-1} mit $a \cdot a^{-1} = 1$. Die Division ist ebenfalls auf diesen Zahlenmengen keine brauchbare Verknüpfung (siehe auch Aufgabenblatt 3, Aufgabe 3), aber es kann $a \div b$ als $a \cdot b^{-1}$ interpretiert werden, so daß die eigentliche Verknüpfung die Multiplikation ist und wieder schöne Eigenschaften hat. □

Beispiel 1.1.21.

i.) *In* $(\mathbb{N},+)$ *besitzt kein Element ein Inverses.*
ii.) *In* $(\mathbb{N}_0,+)$ *ist nur* 0 *invertierbar.*
iii.) *In* $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ *und* $(\mathbb{R},+)$ *besitzt jedes Element ein Inverses.*
iv.) *In* $(\mathbb{Z},\cdot)$ *sind nur* -1 *und* 1 *invertierbar.*
v.) *In* $(\mathbb{Q},\cdot)$ *und* $(\mathbb{R},\cdot)$ *sind alle Elemente außer* 0 *invertierbar.*
vi.) *Für eine nicht-leere Menge* M *gilt nach Satz 0.4.15: Ein Element aus der algebraischen Struktur* $\big(\mathrm{Abb}(M,M),\circ\big)$ *besitzt genau dann ein Inverses, wenn es schon in* $S(M)$ *liegt.* □

Folgende algebraische Strukturen sind von besonderem Interesse:

Definition 1.1.22.

i.) *Eine algebraische Struktur* $(M,*)$ *heißt Halbgruppe, falls das Assoziativgesetz erfüllt ist.*
ii.) *Eine Halbgruppe heißt Monoid, falls darin ein neutrales Element existiert (dieses ist dann eindeutig nach Lemma 1.1.12).*
iii.) *Ein Monoid heißt Gruppe, falls jedes Element darin ein Inverses besitzt (dann ist jedes Inverse jeweils eindeutig nach Lemma 1.1.17).*

Diese Definitionen seien noch einmal schematisch dargestellt:

$(M,*)$ heißt:	falls erfüllt ist:
Halbgruppe	Assoziativgesetz
Monoid	Assoziativgesetz, Existenz neutr. El.
Gruppe	Assoziativgesetz, Existenz neutr. El., Existenz von Inversen

Falls für eine algebraische Struktur auch das Kommutativgesetz erfüllt ist, trägt sie zusätzlich das Attribut „kommutativ“.
Eine kommutative Gruppe wird üblicherweise als abelsche Gruppe bezeichnet (nach dem norwegischen Mathematiker Nils Henrik Abel, 05.08.1802—06.04.1829).
Ist $(U,*)$ *eine Unterstruktur von* $(M,*)$, *die eine der obigen Bedingungen erfüllt, heißt sie je nachdem Unterhalbgruppe, Untermonoid oder Untergruppe.* □

Bemerkung 1.1.23.

i.) *Offensichtlich gilt nach Definition 1.1.22:*

$$(M,*)\ \textit{Gruppe} \quad\Longrightarrow\quad (M,*)\ \textit{Monoid} \quad\Longrightarrow\quad (M,*)\ \textit{Halbgruppe.}$$

ii.) *Ist* $(M,*)$ *ein Monoid mit dem neutralen Element* e, *so kann für* $a,b\in M$ *aus der Gleichung* $a*b=e$ *nicht gefolgert werden, daß* a *und* b *invertierbar sind und* b *das Inverse zu* a *ist (oder* a *das Inverse zu* b*). Ein Gegenbeispiel findet sich z.B. im Monoid* $\big(\mathrm{Abb}(\mathbb{N},\mathbb{N}),\circ\big)$*: dort seien dazu folgende Abbildungen* f *und* g *betrachtet mit:*

$$f(n):=n+1 \qquad \textit{und} \qquad g(n):=\begin{cases}1 & \textit{für } n\in\{1,2\},\\ n-1 & \textit{für } n\geq 3.\end{cases}$$

Es gilt offensichtlich $g\circ f=\mathrm{id}_{\mathbb{N}}$, *aber weder* f *noch* g *sind bijektiv und besitzen daher nach Satz 0.4.15 beide keine Umkehrabbildung bzw. Inverse bzgl. der Verknüpfung „*$\circ$*“.*

Entscheidend ist hier, daß die Gleichung $f \circ g = \mathrm{id}_{\mathbb{N}}$ nicht gilt, und zur Definition von Inversen Elementen gehören eben „beide Richtungen“: Für $a, b \in M$ muß $a * b = e$ und $b * a = e$ gelten, damit beide Elemente zueinander invers sind.
Ist $(M, *)$ aber schon eine Gruppe, und damit bekannt, daß $a, b \in M$ Inverse a^{-1} und b^{-1} besitzen, so kann aus der Gleichung $a * b = e$ gefolgert werden, daß a und b zueinander invers sind:

$$a * b = e \quad \Longrightarrow \quad a^{-1} * (a * b) = a^{-1} * e \quad \Longrightarrow \quad b = a^{-1},$$

und analog:

$$a * b = e \quad \Longrightarrow \quad (a * b) * b^{-1} = e * b^{-1} \quad \Longrightarrow \quad a = b^{-1}. \qquad \square$$

Beispiel 1.1.24.

i.) Die Mengen $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ tragen bezüglich der Rechenoperationen „$+$“ und „$\cdot$“ folgende Struktur:

kommutative Halbgruppe:	$(\mathbb{N}, +)$
kommutativer Monoid:	$(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$
abelsche Gruppe:	$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$

Zusätzlich sind folgende Strukturen abelsche Gruppen:

$$\big(\mathbb{Q} \setminus \{0\}, \cdot\big) \quad \text{und} \quad \big(\mathbb{R} \setminus \{0\}, \cdot\big).$$

ii.) Ist M eine nicht-leere Menge, so ist $\big(\mathrm{Abb}(M, M), \circ\big)$ ein Monoid mit dem neutralen Element id_M, und $\big(S(M), \circ\big)$ eine Untergruppe mit dem gleichen neutralen Element (Beispiel 1.1.5, 1.1.14 und 1.1.21). $\square$

Rechenregeln in Monoiden.

Lemma 1.1.25. *Sei $(M, *)$ ein Monoid, und seien $a, b \in M$ invertierbar. Dann gilt:*

i.) a^{-1} ist invertierbar, und es gilt: $(a^{-1})^{-1} = a$.
ii.) $a * b$ ist invertierbar, und es gilt: $(a * b)^{-1} = b^{-1} * a^{-1}$.

Es sei $E(M)$ die Menge aller inverterbaren Elemente aus M:

$$E(M) := \{\, a \in M \mid a \text{ besitzt ein Inverses in } M \,\}.$$

Dann ist $\big(E(M), *\big)$ eine Untergruppe von $(M, *)$.

Beweis. Es sei e das neutrale Element vo M:

i.) In einem Monoid sind inverse Elemente eindeutig und das Inverse zu a wird mit a^{-1} bezeichnet. Damit ist die Aussage nur eine andere Formulierung von Bemerkung 1.1.16.

ii.) Es reicht, die nötigen Gleichungen für die Elemente $(a * b)$ und $(b^{-1} * a^{-1})$ zu verifizieren:

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e.$$
$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

Damit ist $a * b$ invertierbar und $(b^{-1} * a^{-1})$ das Inverse zu $a * b$.

$E(M)$ ist eine Untergruppe von $(M, *)$:

- $E(M)$ ist nach Aussage ii.) abgeschlossen unter der Verknüpfung „ $*$ “ und damit eine Halbgruppe.
- Da nach Bemerkung 1.1.16 das neutrale Element invertierbar ist, gilt $e \in E(M)$ und $E(M)$ ist ein Monoid.
- Weil nach i.) für $a \in E(M)$ auch $a^{-1} \in E(M)$ gilt, besitzt jedes Element in $E(M)$ ein Inverses und $E(M)$ ist sogar eine Gruppe. □

Beispiel 1.1.26.

$$\begin{aligned} (\mathbb{Z}, \cdot): &\quad E(\mathbb{Z}) = \{\pm 1\}. \\ (\mathbb{Z}, +): &\quad E(\mathbb{Z}) = \mathbb{Z}. \\ \big(\operatorname{Abb}(M, M), \circ\big): &\quad E\big(\operatorname{Abb}(M, M)\big) = S(M). \end{aligned}$$

Dabei ist im letzten Beispiel M eine beliebige nicht-leere Menge. □

Als nächstes sollen Potenzen in Monoiden definiert und Rechengesetze dazu hergeleitet werden:

Definition 1.1.27. *Sei $(M, *)$ ein Monoid mit dem neutralen Element e. Für $a \in M$ und $n \in \mathbb{N}_0$ sei die n-te Potenz definiert als:*

$$a^0 := e \quad \text{und} \quad a^n := \prod_{i=1}^{n} a \text{ für } n \in \mathbb{N}.$$

Ist a invertierbar, so sei für $n < 0$ definiert:

$$a^n := (a^{-1})^{|n|}.$$

Wird die Verknüpfung „ $+$ “ benutzt, so wird für $n \in \mathbb{N}_0$ (oder auch $n \in \mathbb{Z}$) die n-te Potenz von a als n-fache Verknüpfung von a mit sich selbst mit $n \bullet a$ geschrieben. □

Bemerkung 1.1.28.

i.) In den Gruppen $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ stimmt dann für $n \in \mathbb{Z}$ und a aus einer der Gruppen $n \bullet a$ mit dem Produkt $n \cdot a$, der „normalen“ Multiplikation mit n, überein. Allerdings muß dabei auf die Reihenfolge der „Faktoren“ geachtet werden, denn es ist zwar $3 \bullet \pi = \pi + \pi + \pi$ definiert, aber nicht $\pi \bullet 3$.
In $(\mathbb{Z}, +)$ gibt es gar keinen Unterschied zwischen „ $\bullet$ “ und „ $\cdot$ “. Es gilt für alle $a, b \in \mathbb{Z}$:

$$a \bullet b = b \bullet a = a \cdot b = b \cdot a.$$

ii.) Ist M eine nicht-leere Menge, so ist im Monoid $\big(\operatorname{Abb}(M, M), \circ\big)$ mit obiger Definition für jedes $f \in \operatorname{Abb}(M, M)$ dann $f^0 := \mathrm{id}_M$. □

Es folgen nun eine Reihe von Aussagen über Potenzen von Elementen in Monoiden und Rechenregeln dazu, insbesondere die Potenzgesetze (Satz 1.1.32). Alle Aussagen sind anschaulich klar, wenn das Potenzieren als mehrfaches Verknüpfen aufgefaßt wird. Formale Beweise sind leicht per Fallunterscheidungen und vollständige Induktion zu erstellen. Dies sollte zur Übung durchgeführt werden. Alle Aussagen sind mit Beweisen auch im Anhang A.2 zu finden.

LEMMA 1.1.29. *Sei $(M, *)$ ein Monoid mit dem neutralen Element e und $a \in M$ invertierbar. Dann gilt für $k \in \mathbb{Z}$:*

$$a^{-k} = (a^{-1})^k = (a^k)^{-1}.$$

Insbesondere gilt dann $a^k * a^{-k} = e$ für alle $k \in \mathbb{Z}$.

BEWEIS. Siehe Anhang A.2, Lemma A.2.3. □

DEFINITION 1.1.30. *Sei $(M, *)$ eine Halbgruppe. $a, b \in M$ kommutieren, falls gilt:*

$$a * b = b * a.$$ □

LEMMA 1.1.31. *Sei $(M, *)$ ein Monoid, und $a, b \in M$ kommutieren. Dann gilt für alle $n, m \in \mathbb{N}_0$:*

$$a^n * b^m = b^m * a^n.$$

Falls a und b invertierbar sind, gilt diese Aussage für alle $n, m \in \mathbb{Z}$.

BEWEIS. Siehe Anhang A.2, Lemma A.2.5. □

SATZ 1.1.32. *(Potenzgesetze) Sei $(M, *)$ ein Monoid.*

i.) Dann gilt für $a \in M$ und $n, m \in \mathbb{N}_0$:

$$a^n * a^m = a^{n+m}.$$

Ist a invertierbar, so gilt die Aussage für alle $n, m \in \mathbb{Z}$.

ii.) Falls $a, b \in M$ kommutieren, so folgt für alle $n, m \in \mathbb{N}_0$:

$$a^n * b^n = (a * b)^n.$$

Sind a und b beide invertierbar, so gilt die Aussage für alle $n, m \in \mathbb{Z}$.

iii.) Für $a \in M$ und $n, m \in \mathbb{N}_0$ gilt:

$$(a^n)^m = a^{n \cdot m}.$$

Ist a invertierbar, so gilt die Aussage für alle $n, m \in \mathbb{Z}$.

BEWEIS. Siehe Anhang A.2, Satz A.2.6. □

Struktur von Permutationen einer Menge.

Mit Hilfe der Potenzgesetze kann in der Gruppe $S(M)$ nun leicht folgende Aussage bewiesen werden, die einen Einblick in das Verhalten von Permutationen auf einer Menge gibt und im Spezialfall zu einer Zykeldarstellung der Elemente von S_n führt:

LEMMA 1.1.33. *Sei M eine nicht-leere Menge und $f \in S(M)$. Dann ist auf M eine Äquivalenzrelation definiert durch:*

$$x \sim y \quad := \quad \exists i \in \mathbb{Z} : y = f^i(x).$$

Sei T eine Äquivalenzklasse dieser Relation. Dann ist T invariant unter den Abbildungen f und f^{-1}, und beide Abbildungen eingeschränkt auf T sind zueinander inverse Bijektionen:

$$f_{|T}, (f^{-1})_{|T} \in S(T) \quad \text{und} \quad (f_{|T})^{-1} = (f^{-1})_{|T}.$$

Weiter gilt für eine Äquivalenzklasse T:

$$|T| > 1 \qquad \Longleftrightarrow \qquad f_{|T} \text{ hat keinen Fixpunkt.}$$

BEWEIS.
Zu der Äquivalenzrelation:

reflexiv: Für $i := 0$ ist $f^i = \mathrm{id}_M$ (Bemerkung 1.1.28) und es folgt:

$$x = \mathrm{id}_M(x) = f^0(x) \qquad \Longrightarrow \qquad x \sim x.$$

symmetrisch: Sei $x \sim y$ mit $y = f^i(x)$ und $i \in \mathbb{Z}$. Dann gilt:

$$x = \mathrm{id}_M(x) = f^0(x) = f^{-i+i}(x) = f^{-i}\big(f^i(x)\big) = f^{-i}(y) \qquad \Longrightarrow \qquad y \sim x.$$

transitiv: Sei $x \sim y$ mit $y = f^i(x)$ und $y \sim z$ mit $z = f^j(y)$ mit $i, j \in \mathbb{Z}$. Es folgt:

$$z = f^j(y) = f^j\big(f^i(x)\big) = f^{i+j}(x) \qquad \Longrightarrow \qquad x \sim z.$$

Zum Beweis der Invarianz von T unter f und f^{-1}:

$f(T) \subseteq T$: Nach der Definition der Äquivalenzrelation gilt wegen $f(x) = f^1(x)$ die Relation $x \sim f(x)$ und damit $f(x) \in [x]$ für jedes $x \in M$. Daraus folgt sofort mit Satz 0.2.6:

$$x \in T \quad \overset{0.2.6}{\Longrightarrow} \quad \left.\begin{array}{r} [x] = T, \\ x \sim f(x) \end{array}\right\} \quad \Longrightarrow \quad f(x) \in [x] = T.$$

$f^{-1}(T) \subseteq T$: Für $x \in T$ folgt wegen $f \circ f^{-1} = \mathrm{id}_M$ und vorherigen Argumenten:

$$x = f\big(f^{-1}(x)\big) \Longrightarrow f^{-1}(x) \sim x \Longrightarrow x \sim f^{-1}(x) \Longrightarrow f^{-1}(x) \in [x] \overset{\text{(s.o.)}}{=} T.$$

Aus der Invarianz von T unter f und f^{-1} folgt mit $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_M$ sofort:

$$f_{|T} \circ (f^{-1})_{|T} = (f^{-1})_{|T} \circ f_{|T} = \mathrm{id}_T\,.$$

Dann sind $f_{|T}$ und $(f^{-1})_{|T}$ zueinander invers und nach Satz 0.4.15 Bijektionen.
Zum Beweis der letzten Behauptung wird die folgende dazu äquivalente Aussage gezeigt:

$$|T| = 1 \qquad \Longleftrightarrow \qquad f_{|T} \text{ hat einen Fixpunkt.}$$

$\Longrightarrow$: Ist $|T| = 1$ und $T = \{x\}$, so folgt wegen $f(x) \in T$ sofort $f(x) = x$, und x ist ein Fixpunkt von $f_{|T}$.

$\Longleftarrow$: Sei $x \in T$ ein Fixpunkt von $f_{|T}$. Dann gilt $f(x) = f_{|T}(x) = x$ und damit auch $f^{-1}(x) = x$, und es folgt sogar für alle $i \in \mathbb{Z}$ die Gleichung $f^i(x) = x$. Die Äquivalenzklasse von x hat dann die Form $[x] = \{x\}$. Da mit $x \in T$ schon $T = [x]$ gilt, ist für einen Fixpunkt x letztendlich $T = [x] = \{x\}$ und $|T| = 1$. $\square$

Somit liefert Lemma 1.1.33 folgende Anschauung für das Verhalten einer Permutation $f \in S(M)$: Die Menge M zerlegt sich in disjunkte und f-invariante Äquivalenzklassen T_i, in denen f alle Elemente bewegt, falls die Äquivalenzklasse mehr als ein Element (und damit keinen Fixpunkt) enthält:

$$M = \dot{\bigcup_{i \in I}} T_i \quad \text{und} \quad f(T_i) = T_i.$$

Wenn es nur endlich viele Äquivalenzklassen $T_1, \ldots, T_k$ gibt, die mehr als einen Punkt enthalten, so läßt sich f in ein Produkt von Permutationen $f = f_1 \circ \cdots \circ f_k$ zerlegen, bei denen f_i nur die Äquivalenzklasse T_i bewegt: Seien dazu für $1 \leq i \leq k$ folgende Abbildungen definiert:

$$f_i \in S(M) \text{ mit: } \quad f_{i|_{T_i}} := f_{|_{T_i}} \quad \text{und} \quad f_{i|_{M \setminus T_i}} := \mathrm{id}_{M \setminus T_i}.$$

Dann verhält sich f_i auf der Äquivalenzklasse T_i wie f, und außerhalb davon wie die Identität. Offensichtlich gilt dann, da die T_i paarweise disjunkt sind:

$$f = f_1 \circ \cdots \circ f_k.$$

Auch läßt sich leicht überlegen, wie sich f auf einer Äquivalenzklase T verhält: Ein $x \in T$ ist ein Repräsentant der Klasse, d.h. es gilt $T = [x]$. Nach der Definition der Äquivalenzrelation gilt für jedes $y \in T$ dann $y = f^i(x)$ für ein $i \in \mathbb{Z}$ (für $y \neq x$ ist $i \neq 0$).
Dies bedeutet für $i > 0$, daß y durch wiederholtes Abbilden mit f in einer Abbildungskette erreicht wird:

$$\overset{T}{\boxed{x \xrightarrow{f} f(x) \xrightarrow{f} f^2(x) \xrightarrow{f} \ldots \xrightarrow{f} f^{i-1}(x) \xrightarrow{f} f^i(x) = y}}$$

Für $i < 0$ wird y dann wegen $f^i = (f^{-1})^{|i|}$ durch wiederholtes Abbilden mit f^{-1} in einer Abbildungskette erreicht.

$$\overset{T}{\boxed{x \xrightarrow{f^{-1}} f^{-1}(x) \xrightarrow{f^{-1}} f^{-2}(x) \xrightarrow{f^{-1}} \ldots \xrightarrow{f^{-1}} f^{i+1}(x) \xrightarrow{f^{-1}} f^i(x) = y}}$$

Zusammengefaßt bedeutet dies, daß alle Elemente von T von x startend durch wiederholtes Abbilden entweder mit f oder mit f^{-1} erreicht werden können und damit T die folgende Gestalt hat:

$$\overset{T}{\boxed{\ldots \xleftarrow{f^{-1}} f^{-2}(x) \xleftarrow{f^{-1}} f^{-1}(x) \xleftarrow{f^{-1}} x \xrightarrow{f} f(x) \xrightarrow{f} f^2(x) \xrightarrow{f} \ldots}}$$

Ist die f-invariante Äquivalenzklasse T endlich, so muß bei der Abbildungskette

$$x \xrightarrow{f} f(x) \xrightarrow{f} f^2(x) \xrightarrow{f} \ldots$$

irgendwann ein Element getroffen werden, welches in der Kette schon einmal vorkam. Sei dabei $i \in \mathbb{N}$ der erste Index, bei dem dies geschieht, d.h. es sind

$$x, f(x), f^2(x), \dots f^{i-1}(x) \text{ paarweise verschieden} \quad \text{und} \quad f^i(x) \in \{x, \dots, f^{i-1}(x)\}.$$

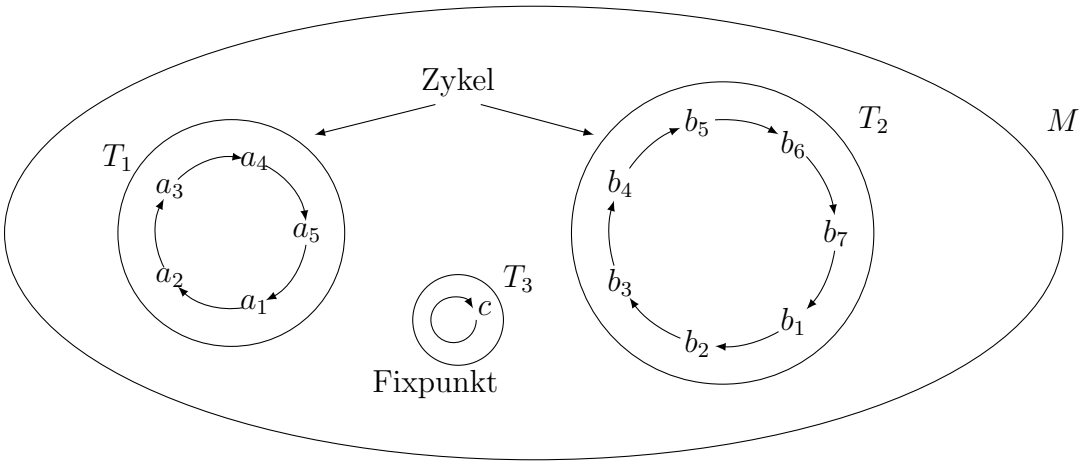
Wegen der Bijektivität von f muß dann $f^i(x) = x$ gelten, da sonst für $f^i(x) = f^j(x)$ mit $1 \leq j < i$ das Element $f^j(x)$ das Bild von $f^{j-1}(x)$ und $f^{i-1}(x)$ wäre, die nach Voraussetzung verschieden sind:

$$\begin{tikzcd}
x \arrow[r, "f"] & f(x) \arrow[r, "f"] & \dots \arrow[r, "f"] & f^{j-1}(x) \arrow[r, "f"] & f^j(x) \arrow[r, "f"] & \dots \arrow[r, "f"] & f^{i-1}(x) \arrow[llll, bend left, "f"] \\
& & & \text{nicht injektiv!} \arrow[ur] & & & \text{falsch!}
\end{tikzcd}$$

$$\begin{tikzcd}
x \arrow[r, "f"] & f(x) \arrow[r, "f"] & \dots \arrow[r, "f"] & f^{i-1}(x) \arrow[llll, bend left, "f"] \\
& & & \text{richtig!}
\end{tikzcd}$$

Die Frage ist nun noch, ob der obige Zykel schon alle Elemente aus T enthält: ist $y \in T$ und $y = f^j(x)$ mit $j \geq 0$, so muß y schon in dem Zykel enthalten sein. Für $j < 0$ kann wegen $y = f^j(x) = (f^{-1})^{|j|}(x)$ in dem Zykel dann $|j|$-mal rückwärts gelaufen werden, um zu y zu gelangen, und auch dann liegt y schon in dem Zykel. Also ist für eine endliche Klasse T die Abbildung $f|_T$ zyklisch mit dem Träger T.

Ist die Menge M endlich, so fallen beide oben beschriebenen Phänomene zusammen, denn in diesem Fall kann es nur endlich viele Äquivalenzklassen geben, und jede einzelne kann nur endlich groß sein. Dann zerlegt sich M nach obigen Beschreibungen in Klassen mit jeweils Fixpunkten von f und in Klassen von „Zykeln“ (natürlich mit disjunkten Trägern):



Insbesondere für den Fall der Permutationen der Menge $\{1, \dots, n\}$, also für die Elemente der symmetrischen Gruppe S_n liefert dies:

SATZ 1.1.34. *Es sei $M := \{1, \ldots, n\}$, $\sigma \in S_n$ und $\sigma \neq \mathrm{id}_M$. Dann existieren eindeutig bestimmte zyklische Permutationen $\sigma_1, \ldots, \sigma_k \in S_n$ mit paarweise disjunkten Trägermengen $T_1, \ldots, T_k \subseteq M$, so daß sich σ als Produkt der σ_i schreiben läßt:*

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_k.$$

Da zyklische Permutationen mit disjunkten Trägern kommutieren (siehe Bemerkung 0.4.26), ist dieses Produkt nur bis auf die Reihenfolge der σ_i eindeutig.
Wird bzgl. σ die Äquivalenzrelation aus Lemma 1.1.33 betrachtet, so entsprechen die Trägermengen T_i denjenigen Äquivalenzklassen, die keinen Fixpunkt von σ enthalten.

BEWEIS. Der Beweis ist im wesentlichen vor dem Satz skizziert. Ein formaler Beweis findet sich im Anhang A.3, Satz A.3.1. □

BEMERKUNG 1.1.35.

i.) *Für die zyklischen Permutationen der S_n wurde in Bemerkung 0.4.26 eine kompakte Darstellungsform mit Hilfe einer Zykeldarstellung vorgestellt, und diese kann nun auf alle Permutationen der S_n (bis auf die Identität) ausgedehnt werden: Hat $\sigma \in S_n$ eine Zerlegung in zyklische Permutationen $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$ mit disjunkten Trägern, und besitzt σ_i eine Zykeldarstellung*

$$\sigma_i : (a_{i,1}\, a_{i,2}\, \ldots\, a_{i,t_i}) \quad \textit{bzgl. des Trägers} \quad \{a_{i,1}, \ldots, a_{i,t_i}\},$$

so kann σ nun folgendermaßen beschrieben werden:

$$\sigma : \underbrace{(a_{1,1}\, a_{1,2}\, \ldots\, a_{1,t_1})}_{\textit{Zykeldarstellung von } \sigma_1} \underbrace{(a_{2,1}\, a_{2,2}\, \ldots\, a_{2,t_2})}_{\textit{Zykeldarstellung von } \sigma_2} \ldots \underbrace{(a_{k,1}\, a_{k,2}\, \ldots\, a_{k,t_k})}_{\textit{Zykeldarstellung von } \sigma_k}.$$

Dabei wird üblicherweise zwischen den einzelnen Zykeldarstellungen auf das Verknüpfungssymbol „$\circ$“ verzichtet.

ii.) *Hat z.B. $\sigma \in S_4$ eine Zykeldarstellung $\sigma : (1\,2)(3\,4)$, so können daraus weitere Zykeldarstellung gewonnen werden, in dem die einzelnen Zykel rotiert , oder die Zykel in ihrer Reihenfolge vertauscht werden. Dies sind jedoch nach Satz 1.1.34 und Bemerkung 0.4.26 die einzigen Variationsmöglichkeiten, so daß σ genau die folgenden acht verschiedenen Zykeldarstellungen besitzt:*

$$\begin{array}{llll} (1\,2)(3\,4), & (1\,2)(4\,3), & (2\,1)(3\,4), & (2\,1)(4\,3), \\ (3\,4)(1\,2), & (3\,4)(2\,1), & (4\,3)(1\,2), & (4\,3)(2\,1). \end{array}$$

iii.) *Ist eine Permutation $\sigma \in S_n$ durch irgendeine Abbildungsvorschrift gegeben, so kann daraus leicht eine Zykeldarstellung mit paarweise disjunkten Trägern gewonnen werden, indem für alle $x \in \{1, \ldots, n\}$ die Äquivalenzklassen bzgl. der Relation aus Lemma 1.1.33 aufgebaut werden, wie in der späteren Analyse beschrieben wurde: Für ein gewähltes x wird einfach die Abbildungskette*

$$x,\ \sigma(x),\ \sigma^2(x),\ \ldots$$

gebildet, bis zum erstenmal wieder das Element x erreicht wird (hier sei dies bei der Potenz $i \in \mathbb{N}$ erfüllt: $\sigma^i(x) = x$). Im Falle $i = 1$ ist $\sigma(x) = x$ und x ein Fixpunkt, und dieser kann in der Beschreibung durch Zykel ignoriert werden. Im Falle $i \geq 2$ ist

$$\big(x\, \sigma(x)\, \sigma^2(x)\, \ldots\, \sigma^{i-1}(x)\big)$$

ein Zykel der Zykeldarstellung mit dem Träger $\{x, \sigma(x), \ldots, \sigma^{i-1}(x)\}$.

Dieses Verfahren wird für alle Elemente des Definitionsbereichs $\{1, \ldots, n\}$ *solange durchgeführt, bis jedes entweder als Fixpunkt identifiziert ist oder in einem Träger (bzw. Zykel) vorkommt.*

iv.) Das „Zykelprodukt“ $(1\,2\,3)(2\,5)$ *hat keine disjunkten Träger und ist somit keine Zykeldarstellung einer Permutation im Sinne von Satz 1.1.34. Dies kann nur als Produkt zweier Permutationen* σ *und* τ *mit den Zykeldarstellungen*

$$\sigma : (1\,2\,3) \quad \textit{und} \quad \tau : (2\,5)$$

interpretiert werden, d.h. als Beschreibung der Komposition $\sigma \circ \tau$*. Dabei ist bei der Zykeldarstellung nicht eindeutig festgelegt, aus welcher* S_n *eine Permutation stammt, da die Fixpunkte nicht notiert werden und damit ein beliebig großes* n *angenommen werden kann, solange nur alle Einträge aus den Zykeln kleiner sind als* n *(siehe auch Bemerkung 0.4.26). In diesem Fall muß wegen der Zykeleinträge von* τ *die Bedingung* $n \geq 5$ *gelten.*
Um von $\pi := \sigma \circ \tau$ *eine Zykeldarstellung mit paarweise disjunkten Trägern zu gewinnen, muß nach vorher beschriebenem Verfahren eine Zykeldarstellung berechnet werden. Dabei ist darauf zu achten, daß die Abbildung* τ *zuerst ausgeführt ist (siehe Definition 0.4.10, Komposition von Abbildungen).*
Die Äquivalenzklasse von 1 *ergibt sich aus:*

$$\begin{aligned}
&[1] : 1, \\
&\quad \pi(1) = \sigma\big(\tau(1)\big) = \sigma(1) = 2 \\
&\quad \pi^2(1) = \pi(2) = \sigma\big(\tau(2)\big) = \sigma(5) = 5 \\
&\quad \pi^3(1) = \pi\big(\pi^2(1)\big) = \pi(5) = \sigma\big(\tau(5)\big) = \sigma(2) = 3 \\
&\quad \pi^4(1) = \pi(\big(\pi^3(1)\big) = \pi(3) = \sigma\big(\tau(3)\big) = \sigma(3) = 1 \\
\Longrightarrow\ &[1] = \{1, 2, 3, 5\},
\end{aligned}$$

und $\pi_{|_{[1]}}$ *hat die Zykeldarstellung* $(1\,2\,5\,3)$*.*
In dem Träger des vorherigen Zykels sind alle Zahlen enthalten, die von σ *oder* τ *bewegt werden, und so sind alle anderen Zahlen Fixpunkte von* π*. Damit ist* π *zyklisch.* □

Strukturen auf Mengen von Abbildungen.

Für die Menge der Selbstabbildungen einer gegebenen nicht-leeren Menge M sind in vorherigen Bemerkungen und Beispielen schon die folgenden Strukturaussagen gemacht worden und werden hier nur noch einmal gesammelt präsentiert:

Lemma 1.1.36.
Ist M *eine nicht-leere Menge, so gilt für die algebraische Struktur* $\big(\mathrm{Abb}(M, M), \circ\big)$*:*

$|M| = 1$: $\mathrm{Abb}(M, M) = \{\mathrm{id}_M\}$ *ist eine abelsche Gruppe.*
$|M| \geq 2$: $\big(\mathrm{Abb}(M, M), \circ\big)$ *ist ein nicht-kommutativer Monoid.*

Weiter gilt: $\big(S(M), \circ\big)$ *ist eine Untergruppe von* $\big(\mathrm{Abb}(M, M), \circ\big)$*, die für* $|M| \geq 3$ *nicht mehr abelsch ist.*

Beweis. Beispiel 1.1.5, Beispiel 1.1.14 und Beispiel 1.1.21. □

Sind zwei verschiedene Mengen gegeben M und N gegeben, so ist auf der Menge $\mathrm{Abb}(M,N)$ die Komposition keine innere Verknüpfung: Für $f,g \in \mathrm{Abb}(M,N)$ ist $f \circ g$ gar nicht definiiert, falls $M \neq N$ gilt (Def 0.4.10).
Wenn die Menge N jedoch auch eine algebraische Struktur mit einer inneren Verknüpfung „ $*$ “ ist, so kann auf der Menge $\mathrm{Abb}(M,N)$ eine innere Verknüpfung mit Hilfe der Verknüpfung „ $*$ “ des Wertebreiches definiert werden (und dies wird in Zukunft häufig geschehen):

Satz 1.1.37. *Es sei M eine nicht-leere Menge, und $(N,*)$ eine algebraische Struktur. Für $f,g \in \mathrm{Abb}(M,N)$ sei dann definiert:*

$$f \circledast g \colon M \longrightarrow N \quad \textit{mit} \quad m \mapsto f(m) * g(m).$$

Dann ist $\big(\mathrm{Abb}(M,N), \circledast\big)$ eine algebraische Struktur, welche die gleichen Eigenschaften besitzt wie $(N,*)$, d.h:

$$\begin{array}{llll} (N,*) & \textit{Halbgruppe} & \Longrightarrow & \big(\mathrm{Abb}(M,N),\circledast\big) \quad \textit{Halbgruppe.} \\ (N,*) & \textit{Monoid} & \Longrightarrow & \big(\mathrm{Abb}(M,N),\circledast\big) \quad \textit{Monoid.} \\ (N,*) & \textit{Gruppe} & \Longrightarrow & \big(\mathrm{Abb}(M,N),\circledast\big) \quad \textit{Gruppe.} \end{array}$$

Das Kommutativgesetz überträgt sich ebenso von „ $*$ “ auf „ $\circledast$ “.
Besitzt $(N,*)$ das neutrales Element e, so ist folgende Abbildung das neutrale Element in $\big(\mathrm{Abb}(M,N),\circledast\big)$:

$$\varepsilon \colon M \longrightarrow N \quad \textit{mit} \quad m \mapsto e.$$

Besitzt in $(N,*)$ jedes Element ein Inverses, so ist zu $f \in \mathrm{Abb}(N,M)$ folgende Abbildung eine Inverse bzgl. der Verknüpfung „ $\circledast$ “:

$$g \colon M \longrightarrow N \quad \textit{mit} \quad m \mapsto \big(f(m)\big)^{-1}.$$

Beweis.

Assoziativität: Sei „ $*$ “ assoziativ. Dann gilt für $f,g,h \in \mathrm{Abb}(M,N)$ und $m \in M$:

$$\begin{aligned} \big(f \circledast (g \circledast h)\big)(m) &= f(m) * (g \circledast h)(m) &&= f(m) * \big(g(m) * h(m)\big) \\ &\overset{(*\text{ ass.})}{=} \big(f(m) * g(m)\big) * h(m) &&= (f \circledast g)(m) * h(m) \\ &= \big((f \circledast g) \circledast h\big)(m). \end{aligned}$$

Also ist $f \circledast (g \circledast h) = (f \circledast g) \circledast h$ und „ $\circledast$ “ auch assoziativ.

Kommutativität: Sei „ $*$ “ kommutativ. Dann gilt für $f,g \in \mathrm{Abb}(M,N)$ und $m \in M$:

$$(f \circledast g)(m) = f(m) * g(m) \overset{(*\text{ komm})}{=} g(m) * f(m) = (g \circledast f)(m).$$

Also ist $f \circledast g = g \circledast f$ und „ $\circledast$ “ auch kommutativ.

Neutrales Element: Es gilt $f \circledast \varepsilon = \varepsilon \circledast f = f$ für alle $f \in \mathrm{Abb}(M,N)$, denn es folgt für $m \in M$:

$$\begin{aligned} (f \circledast \varepsilon)(m) &\overset{(\text{Def } \circledast)}{=} f(m) * \varepsilon(m) \overset{(\text{Def } \varepsilon)}{=} f(m) * e = f(m) \\ = e * f(m) &\overset{(\text{Def } \varepsilon)}{=} \varepsilon(m) * f(m) \overset{(\text{Def } \circledast)}{=} (\varepsilon \circledast f)(m). \end{aligned}$$

Existenz von Inversen: Es ist folgende Gleichung zu verifizieren:

$$g \circledast f = f \circledast g = \varepsilon.$$

Sie folgt sofort aus folgender Betrachtung für $m \in M$:

$$\begin{aligned}(g \circledast f)(m) &\overset{(\text{Def } \circledast)}{=} g(m) * f(m) \overset{(\text{Def } g)}{=} \big(f(m)\big)^{-1} * f(m) = e \overset{(\text{Def } \varepsilon)}{=} \varepsilon(m) \\ &\overset{(\text{Def } \varepsilon)}{=} e = f(m) * \big(f(m)\big)^{-1} \overset{(\text{Def } g)}{=} f(m) * g(m) \overset{(\text{Def } \circledast)}{=} (f \circledast g)(m). \qquad \square\end{aligned}$$

Bemerkung 1.1.38.

i.) Satz 1.1.37 kann natürlich auch auf den Fall $M = N$ angewandt werden, und als Beispiel dazu sei nun $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ betrachtet:

- *$(\mathbb{R}, +)$ ist eine abelsche Gruppe, und so liefert die in Satz 1.1.37 definierte Konstruktion der Verknüpfung „$\oplus$“, daß $\big(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), \oplus\big)$ ebenfalls eine abelsche Gruppe ist. Sind zum Beispiel die Abbildungen $f, g \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ gegeben mit $f\colon x \mapsto x^2$ und $g\colon x \mapsto x + 1$, so gilt $f \oplus g\colon x \mapsto x^2 + x + 1$.*
- *$(\mathbb{R}, \cdot)$ ist ein kommutativer Monoid, und so ist analog zum vorherigen Fall $\big(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), \odot\big)$ ein kommutativer Monoid. Sind z.B. $f\colon x \mapsto x + 1$ und $g\colon x \mapsto x - 1$ gegeben, so folgt $f \odot g\colon x \mapsto x^2 - 1$.*
- *Wegen der Gleichheit von Definitions- und Wertebereich ist auch die Komposition von Abbildungen definiert, und $\big(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), \circ\big)$ ist ein Monoid: hierbei wurde aber keine Struktur der Menge $\mathbb{R}$ zur Definition einer Struktur auf $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ herangezogen.*

Somit existieren auf der Menge $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ drei natürliche Verknüpfungen. Üblicherweise wird jedoch auf die Symbolunterscheidung aus Satz 1.1.37 verzichtet und in der Abbildungsstruktur das gleiche Verknüpfungssymbol wie in der Mengenstruktur verwendet: d.h. im obigen Fall, daß $f + g$ statt $f \oplus g$ und $f \cdot g$ statt $f \odot g$ geschrieben wird. Zum Beispiel wurde in der Schule ja auch schon bei den Ableitungsregeln differenzierbarer Abbildungen „salopp“ geschrieben:

$$(f + g)' = f' + g' \quad \textit{und} \quad (f \cdot g)' = f' \cdot g + f \cdot g'.$$

Dabei sind die Verknüpfungen in den Ableitungsregeln Verknüpfungen auf der Ebene der Abbildungen, also in $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$, aber es werden einfach die bekannten Verknüpfungssymbole aus $\mathbb{R}$ benutzt.

ii.) Für den Fall $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ seien noch einmal alle vorher genannten Strukturen übersichtlich gelistet:

	Struktur	*neutr. El.*	*inv. El. zu f*
$\big(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), \oplus\big)$	*abelsche Gruppe*	$\bar{0}\colon x \mapsto 0_{\mathbb{R}}$	$-f\colon x \mapsto -f(x)$
$\big(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), \odot\big)$	*kom. Monoid*	$\bar{1}\colon x \mapsto 1_{\mathbb{R}}$	\
$\big(\mathrm{Abb}(\mathbb{R}, \mathbb{R}), \circ\big)$	*Monoid*	$\mathrm{id}_{\mathbb{R}}$	\

$\square$

Die Konstruktion aus Satz 1.1.37 sei nun für die Menge $I := \{1, 2, 3\}$ und die abelsche Gruppe $(\mathbb{R}, +)$ unter folgendem Gesichtspunkt betrachtet. Für die Abbildungsmenge $\mathrm{Abb}(I, \mathbb{R})$ wird jetzt die Bezeichnung $\mathbb{R}^I$ verwendet (siehe auch Definition 0.4.21). Um eine Abbildung $f \in \mathbb{R}^I$ zu notieren, können die drei Bilder von 1, 2, und 3 unter

f explizit angegeben werden, etwa in der folgenden Form:

$$f\colon \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix} \qquad \text{oder kürzer:} \qquad \big(f(1), f(2), f(3)\big).$$

Dabei ist das 3-Tupel $\big(f(1), f(2), f(3)\big)$ nicht mit einer Zykeldarstellung einer Permutation aus S_n zu verwechseln: in dem 3-Tupel steht an der i-ten Stelle das Bild $f(i)$ von i unter f. In der Zykeldarstellung einer Permutation wird das Bild eines Elementes rechts neben dem Element notiert (bis auf das Bild des letzten Zykelelementes, welches am Anfang des Zykels steht), und es gibt keine Korrelation zwischen dem Element an der Stelle i des Zykels und dem Bild $f(i)$ von i unter f. Auch sind Zykel nur für Permutationen definiert und nicht für beliebige Abbildungen (Zykel werden auch *ohne* Komma geschrieben!)
Diese Tupelnotation von f läßt sich problemlos verallgemeinern auf den Fall einer endlichen Menge $I := \{1, \ldots, n\}$, wo dann f durch das n-Tupel $\big(f(1), \ldots, f(n)\big)$ dargestellt wird. Andersherum definiert jedes n-Tupel $(a_1, \ldots, a_n)$ durch die Abbildungsvorschrift $f(i) := a_i$ eindeutig ein $f \in \mathbb{R}^I$, so daß zwischen den folgenden beiden Mengen via dieser Interpretation eine Bijektion existiert:

$$\mathbb{R}^{\{1,\ldots,n\}} \quad \longleftrightarrow \quad \mathbb{R}^n,$$

wobei $\mathbb{R}^n$ als n-faches kartesisches Produkt von $\mathbb{R}$ mit sich selbst genau die Menge aller n-Tupel mit Einträgen aus $\mathbb{R}$ ist (Definition 0.2.2).
Wird nun auf $\mathbb{R}$ die Struktur $(\mathbb{R}, +)$ und dann auf $\mathbb{R}^I$ die davon induzierte Struktur $(\mathbb{R}^I, \oplus)$ betrachtet und zwei Abbildungen $f, g \in \mathbb{R}^I$ durch Tupel $f\colon (a_1, \ldots, a_n)$ und $g\colon (b_1, \ldots, b_n)$ dargestellt, so ergibt sich für die Summe $f \oplus g$ der Abbildungen sofort die Tupeldarstellung

$$f \oplus g\colon (a_1, \ldots, a_n) \oplus (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n).$$

Bei der Summe der Abbildungen wird ja pro abgebildetem Element $i \in I$ die Summe der Bilder unter f und g gebildet, d.h. $(f \oplus g)(i) := f(i) + g(i)$, und damit werden in den Tupeln genau die Komponenten addiert: und zwar in $(\mathbb{R}, +)$.
Sogar für jede beliebige Indexmenge I können die Abbildugen aus $\mathrm{Abb}(I, \mathbb{R}) = \mathbb{R}^I$ durch Tupel darstellen werden und umgekehrt: Für ein $f \in \mathbb{R}^I$ wird dann einfach die „nicht-sortierte“ Tupelschreibweise $\big(f(i)\big)_{i \in I}$ verwendet, und dieses I-Tupel ist ein Element des kartesischen Produktes $\prod_{i \in I} \mathbb{R}$ (Definition 0.2.2). Andersherum liefert auch jedes I-Tupel $(a_i)_{i \in I}$ aus diesem kartesischen Produkt via $f(i) := a_i$ eine Abbildung aus $\mathbb{R}^I$, und es gibt wieder wie vorher schon für den Fall der Menge $\{1, \ldots, n\}$ beschrieben eine Bijektion der Mengen:

$$\mathbb{R}^I \quad \longleftrightarrow \quad \prod_{i \in I} \mathbb{R}.$$

Natürlich überträgt sich wieder die algebraische Struktur von $(\mathbb{R}^I, \oplus)$ auf das kartesische Produkt, indem dort komponentenweise addiert wird - und zwar pro Komponente dann in der algebraischen Struktur $(\mathbb{R}, +)$.

Wird nun in obiger Konstruktion die abelsche Gruppe $(\mathbb{R}, +)$ durch eine beliebige algebraische Struktur $(M, *)$ ersetzt, so läßt sich Satz 1.1.37 uminterpretieren bzw. auf die speziellen kartesische Produkte (mit immer dem gleichen Faktor) $\prod_{i \in I} M$ übertragen:

SATZ 1.1.39. *Sei I eine nicht-leere Menge und $(M,*)$ eine algebraische Struktur. Dann gibt es eine kanonische Identifizierung*

$$M^I \longleftrightarrow \prod_{i\in I} M \quad \text{mit} \quad f \longleftrightarrow (x_i)_{i\in I},$$

wobei einem $f \in M^I$ das Tupel $\big(f(i)\big)_{i\in I}$ zugeordnet wird und einem Tupel $(x_i)_{i\in I}$ die Abbildung $f\colon I \longrightarrow M$ mit $i \mapsto x_i$.
Die durch „$*$“ induzierte innere Verknüpfung „$\circledast$“ auf $M^I = \mathrm{Abb}(I,M)$ (Satz 1.1.37) überträgt sich auf das kartesische Produkt, indem dort komponentenweise in M verknüpft wird:

$$(x_i)_{i\in I} \circledast (y_i)_{i\in I} := (x_i * y_i)_{i\in I}.$$

Damit gilt analog zu Satz 1.1.37:

$$\begin{array}{llll} (M,*) & \text{Halbgruppe} & \Longrightarrow & \big(M^I,\circledast\big) \ \text{Halbgruppe.} \\ (M,*) & \text{Monoid} & \Longrightarrow & \big(M^I,\circledast\big) \ \text{Monoid.} \\ (M,*) & \text{Gruppe} & \Longrightarrow & \big(M^I,\circledast\big) \ \text{Gruppe.} \end{array}$$

Das Kommutativgesetz überträgt sich ebenso von „$*$“ auf „$\circledast$“.
Ist e das neutrale Element in $(M,*)$, so ist $(e)_{i\in I}$ das neutrale Element in $(M^I,\circledast)$. Hat in $(x_i)_{i\in I} \in M^I$ jede Komponente x_i ein Inverses x_i^{-1} in $(M,*)$, so ist $(x_i^{-1})_{i\in I}$ das Inverse zu $(x_i)_{i\in I}$ in $(M^I,\circledast)$.

BEWEIS. Siehe die Betrachtungen vor dem Satz. □

BEISPIEL 1.1.40. *Aus der Schule ist schon bekannt, wie in den kartesischen Produkten $\mathbb{R}^2$, $\mathbb{R}^3$ oder allgemein $\mathbb{R}^n$ zwei Tupel addiert werden, nämlich komponentenweise:*

$$(x_1,\dots,x_n) \oplus (y_1,\dots,y_n) := (x_1+y_1,\dots,x_n+y_n).$$

Dies hat für den Fall $n \in \{1,2,3\}$ eine geometrische Interpretation, wo die Tupel dann als Koordinaten von Vektoren im „Raum“ $\mathbb{R}^n$ aufgefaßt werden.
Auch hier wird später bei der Verknüpfung der Vektoren das gleiche Verknüpfungszeichen benutzt wie bei den Komponenten, „$+$“ statt „$\oplus$“. □

Über den Umweg der Interpretation von Tupeln als Abbildungen wurde in Satz 1.1.39 auf dem I-fachen kartesischem Produkt M^I einer algebraischen Struktur $(M,*)$ mit sich selbst eine komponentenweise Verknüpfung definiert und so M^I ebenfalls zu einer algebraischen Struktur gemacht. Dies hätte auch direkt geschehen können, und soll nun auch durchgeführt werden. Dabei wird sogar ein viel allgemeineres Ergebnis erzielt: vorher war im kartesischen Produkt M^I nur eine einzige Struktur I-fach vertreten, und in allen Komponenten wurde die gleiche Verknüpfung benutzt.

SATZ 1.1.41. *Es sei I eine nicht-leere Indexmenge, und für jedes $i \in I$ sei eine algebraische Struktur $(M_i,*_i)$ gegeben. Weiter sei folgende komponentenweise innere Verknüpfung definiert:*

$$\circledast\colon \prod_{i\in I} M_i \times \prod_{i\in I} M_i \longrightarrow \prod_{i\in I} M_i \qquad \text{mit} \qquad (x_i)_{i\in I} \circledast (y_i)_{i\in I} := (x_i *_i y_i)_{i\in I}.$$

Dann gilt:

$$\text{Alle } (M_i,*_i) \text{ sind Halbgruppen} \quad \Longrightarrow \quad \Big(\prod_{i\in I} M_i, \circledast\Big) \text{ ist eine Halbgruppe.}$$

$$\textit{Alle } (M_i, *_i) \textit{ sind Monoide} \quad \Longrightarrow \quad \Big(\prod_{i\in I} M_i, \circledast\Big) \textit{ ist ein Monoid.}$$

$$\textit{Alle } (M_i, *_i) \textit{ sind Gruppen} \quad \Longrightarrow \quad \Big(\prod_{i\in I} M_i, \circledast\Big) \textit{ ist eine Gruppe.}$$

Gilt für alle Verknüpfungen „$*_i$“ das Kommutativgesetz, so gilt dies auch für die Verknüpfung „$\circledast$“ im kartesischen Produkt der M_i.
Weiter sind folgende Eigenschaften erfüllt:

- *Besitzen alle $(M_i, *_i)$ ein neutrales Element, und ist dieses e_i, so ist $(e_i)_{i\in I}$ das neutrale Element im kartesischen Produkt bzgl. der Verknüpfung „$\circledast$“.*
- *Hat im I-Tupel $(x_i)_{i\in I}$ jede Komponente x_i im der jeweiligen Struktur $(M_i, *_i)$ ein Inverses x_i^{-1}, so ist $(x_i^{-1})_{i\in I}$ das Inverse zu $(x_i)_{i\in I}$ bzgl. der Verknüpfung „$\circledast$“.*

Beweis. Alle Aussagen können leicht komponentenweise verifiziert werden (siehe dazu auch den Beweis von Satz 1.1.37). □

Beispiel 1.1.42.
Es sei die abelsche Gruppe $(\mathbb{Z}, +)$ und der kommutative Monoid $(\mathbb{Z}, \cdot)$ betrachtet. Dann ist

$$\mathbb{Z} \times \mathbb{Z} \quad \textit{mit} \quad (a_1, a_2) \circledast (b_1, b_2) := (a_1 + b_1, a_2 \cdot b_2)$$

ein kommutativer Monoid mit dem neutralen Element $(0, 1)$. Es ist keine Gruppe, denn das Element $(1, 0) \in \mathbb{Z}^2$ hat kein Inverses bzgl. der Verknüpfung „$\circledast$“, da zwar 1 in $(\mathbb{Z}, +)$, aber nicht 0 in $(\mathbb{Z}, \cdot)$ invertierbar ist. □

1.2. Gruppen

Die Gruppentheorie ist ein weites Feld, das hier nicht einmal ansatzweise bestellt werden kann. Es werden im folgenden nur einige Objekte und Prinzipien betrachtet, die im weiteren Verlauf der Vorlesung auch für Vektorräume von Interesse sind. Insbesondere werden hier Quotientengruppen betrachtet, da im Falle von endlichen und insbesondere kleinen Gruppen Beispiele explizit durchgerechnet werden können, um das Prinzip zu verstehen. Dann wird dieses wichtige Konstruktionsverfahren der Algebra hoffentlich einsichtiger, als wenn es nur formal in unendlich großen Vektorräumen ausgeführt wird.
Mit Hilfe von Quotientenkonstruktionen werden in jeder algebraischen Theorie wesentliche Objekte definiert und analysiert.

Zur Untersuchung einer algebraischen Struktur werden oft die Unterstrukturen herangezogen. Daher zuerst einige Betrachtungen zu Untergruppen:

Untergruppen und Nebenklassen.

In Definition 1.1.1 wurden algebraische Unterstrukturen einer gegebenen Struktur so flexibel definiert, daß folgende Phänomene auftreten können:

Bemerkung 1.2.1.

i.) *Es sei der Monoid* $M := \mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q}$ *mit der komponentenweisen Multiplikation als Verknüpfung und darin der Untermonoid* $U := \mathbb{Q} \times \{0\} \subseteq M$ *betrachtet:*
- *In* M *ist* $(1,1)$ *das neutrale Element, aber* U *hat das neutrale Element* $(1,0)$.
- *In* U *ist das Element* $(2,0)$ *invertierbar, in* M *aber nicht.*

Somit können verschiedene neutrale Elemente auftreten, und Invertierbarkeit eines Elements im Untermonoid muß sich nicht auf den Obermonoid übertragen.

ii.) *Ist* $(M, *)$ *ein Monoid und* $U \subseteq M$ *ein Untermonoid, so gilt jedoch immer folgende Aussage für ein* $u \in U$*:*

Besitzt u *Inverse in* U *und* M*, so sind beide Inverse gleich, und auch die neutralen Elemente von* U *und* M *müssen übereinstimmen.*

Ist nämlich e *ein neutrales Element von* M *und* f *ein neutrales Element von* U*, und gilt* $a * u = u * a = e$ *mit* $a \in M$ *und* $b * u = u * b = f$ *mit* $b \in U$*, so folgt:*

$$e = u * a = (f * u) * a = f * (u * a) = f * e = f.$$

Für $f = e$ *ist* b *auch ein Inverses von* u *in* M *und damit wegen dessen Eindeutigkeit gleich* a. □

Werden als Strukturen nur Gruppen und Untergruppen betrachtet, ist die Situation einfacher:

Lemma 1.2.2. *Sei* $(G, *)$ *eine Gruppe und* $U \subseteq G$ *eine Untergruppe. Dann gelten:*

i.) *Das neutrale Element von* U *ist gleich dem neutralen Element von* G.

ii.) *Ein Element* $u \in U$ *hat in* U *und* G *das gleiche Inverse.*

Beweis. Ein $u \in U$ ist per Definition in U und G invertierbar (beides sind Gruppen!). Dann stimmen nach Bemerkung 1.2.1 aber sowohl die jeweiligen Inversen als auch die neutralen Element von U und G überein. □

Bei Gruppen gibt es ein einfaches und nützliches Kriterium, um für eine Teilmenge zu überprüfen, ob sie eine Untergruppe ist:

Lemma 1.2.3. *Sei* $(G, *)$ *eine Gruppe und* $U \subseteq G$ *eine nicht-leere Teilmenge. Dann gilt für die Teilmenge* U*:*

$$U \text{ Untergruppe} \quad \Longleftrightarrow \quad a * b^{-1} \in U \text{ für alle } a, b \in U.$$

Bei dem Verknüpfungssymbol „+“ lautet die Bedingung wegen $a - b := a + (-b)$*:*

$$U \text{ Untergruppe} \quad \Longleftrightarrow \quad a - b \in U \text{ für alle } a, b \in U.$$

Beweis.
Sei e das neutrale Element in G.

$\Longrightarrow$: Seien $a, b \in U$. Da U eine Untergruppe ist, liegt für jedes $b \in U$ auch sein Inverses b^{-1} in U. Weiter ist U unter der Verknüpfung abgeschlossen, und so folgt mit $a, b^{-1} \in U$ dann auch $a * b^{-1} \in U$.

$\Longleftarrow$: Es ist zu zeigen, daß U abgeschlossen ist unter der Verknüpfung, das neutrale Element enthält, und für jedes seiner Elemente auch das Inverse.

$e \in U$: Da U nicht leer ist, gibt es ein $a \in U$, und dann muß nach der Bedingung an U mit $b := a$ auch $e = a * a^{-1} \in U$ gelten.

Inverse in U: Für jedes $a \in U$ ist wegen $e \in U$ auch $a^{-1} = e * a^{-1} \in U$.
Abgeschlossenheit: Für $a, b \in U$ ist $b^{-1} \in U$, und wegen $b = (b^{-1})^{-1}$ dann auch $a * b = a * (b^{-1})^{-1} \in U$. □

Beispiel 1.2.4.

i.) Sei $(G, *)$ eine Gruppe. Für $g \in G$ sei folgende Teilmenge von G betrachtet:

$$\{\, g^i \mid i \in \mathbb{Z} \,\}.$$

Wegen der Potenzgesetze erfüllt diese Teilmenge offensichtlich das Untergruppenkriterium aus Lemma 1.2.3, denn für g^r, g^s mit $r, s \in \mathbb{Z}$ gilt:

$$g^r * (g^s)^{-1} = g^r * g^{-s} = g^{r-s} \in \{\, g^i \mid i \in \mathbb{Z} \,\}.$$

Aus den Potenzgesetzen folgt auch $g^i = (g^{-1})^{-i}$, und damit dann:

$$\{\, g^i \mid i \in \mathbb{Z} \,\} = \{\, (g^{-1})^i \mid i \in \mathbb{Z} \,\}.$$

ii.) Seien $I \subseteq M$ nicht-leere Mengen und

$$U_I := \{\, f \in S(M) \mid f_{|_I} = \mathrm{id}_I \,\}.$$

Für $f, g \in U_I$ folgt offensichtlich $g^{-1} \in U_I$ und U_I ist abgeschlossen unter der Komposition, so daß damit auch $f \circ g^{-1} \in U_I$ gilt. Also ist U_I nach Lemma 1.2.3 eine Untergruppe von $\big(S(M), \circ\big)$. □

Die Untergruppe $\{\, g^i \mid i \in \mathbb{Z} \,\} \subseteq G$ aus Beispiel 1.2.4 soll nun näher betrachtet werden. Dazu sei vorbereitend folgende grundsätzlich nützliche Abbildung definiert:

Definition 1.2.5. *Sei $(G, *)$ eine Gruppe. Dann heißt für $g \in G$ die folgende Abbildung Linksmultiplikation mit g in G:*

$$\ell_g \colon G \longrightarrow G \quad \text{mit} \quad h \mapsto g * h.$$ □

Es ergibt sich sofort für die Linksmultiplikation in einer Gruppe:

Lemma 1.2.6. *Sei $(G, *)$ eine Gruppe. Dann ist für $g \in G$ die Linksmultiplikation ℓ_g eine Bijektion (d.h. $\ell_g \in S(G)$) und es gilt $(\ell_g)^{-1} = \ell_{g^{-1}}$.*

Beweis. Offensichtlich gilt für g, g^{-1} und h aus G:

$$\begin{aligned}(\ell_g \circ \ell_{g^{-1}})(h) &= \ell_g\big(\ell_{g^{-1}}(h)\big) = \ell_g(g^{-1} * h) = g * (g^{-1} * h) = h = \mathrm{id}_G(h)\\ &= h = g^{-1} * (g * h) = \ell_{g^{-1}}(g * h) = \ell_{g^{-1}}\big(\ell_g(h)\big) = (\ell_{g^{-1}} \circ \ell_g)(h).\end{aligned}$$

Daraus folgen für die beiden Abbildungen ℓ_g und $\ell_{g^{-1}}$ die Identitäten:

$$\ell_g \circ \ell_{g^{-1}} = \mathrm{id}_G \qquad \text{und} \qquad \ell_{g^{-1}} \circ \ell_g = \mathrm{id}_G,$$

und ℓ_g und $\ell_{g^{-1}}$ sind zueinander inverse Bijektionen mit $(\ell_g)^{-1} = \ell_{g^{-1}}$. □

Wird nun für ein $g \in G$ die durch die Permuation $\ell_g \in S(G)$ auf G induzierte Äquivalenzrelation aus Lemma 1.1.33 betrachtet, also

$$x \sim y \quad := \quad \exists i \in \mathbb{Z} : y = (\ell_g)^i(x),$$

so ist die Untergruppe $\{\, g^i \mid i \in \mathbb{Z} \,\}$ nichts anderes als die Äquivalenzklasse des neutralen Elementes e von G:

$$g^i = g^i * e = (\ell_g)^i(e) \quad \Longrightarrow \quad \{\, g^i \mid i \in \mathbb{Z} \,\} = [e].$$

Damit folgt sofort aus der Diskussion der Äquivalenzklassen nach dem Lemma 1.1.33 für den Fall, daß die Klasse $[e]$ endlich ist:

LEMMA 1.2.7. *Sei $(G,*)$ eine Gruppe mit dem neutralen Element e. Wenn für $g \in G$ die Untergruppe $\{\, g^i \mid i \in \mathbb{Z} \,\}$ endlich ist, gibt es ein minimales $k \in \mathbb{N}$, so daß gilt:*

$$\{\, g^i \mid i \in \mathbb{Z} \,\} = \{e, g, g^2, \ldots, g^{k-1}\} \quad \textit{und} \quad g^k = e.$$

BEWEIS. Siehe die Argumente vor diesem Lemma und die Diskussion der Äquivalenzklassen aus und nach Lemma 1.1.33. □

Die vorherigen Betrachtungen führen zu folgenden Definitionen:

DEFINITION 1.2.8. *Sei $(G,*)$ eine Gruppe. Dann heißt für $g \in G$ die Menge/Gruppe*

$$\langle\, g \,\rangle := \{\, g^i \mid i \in \mathbb{Z} \,\}$$

die von g erzeugte zyklische Untergruppe von G und g ihr Erzeuger. Die Gruppe G heißt zyklisch, wenn es ein $g \in G$ gibt mit $G = \langle\, g \,\rangle$.
Für $g \in G$ ist dann seine Ordnung definiert als die Ordnung der erzeugten zyklischen Untergruppe $\langle\, g \,\rangle$, und es wird notiert:

$$\operatorname{ord}(g) := |\langle\, g \,\rangle| \in \mathbb{N} \,\dot\cup\, \{\infty\}. \qquad \square$$

BEMERKUNG 1.2.9.

i.) *Das neutrale Element einer Gruppe ist offensichtlich das einzige Element darin mit der Ordnung Eins.*

ii.) *Nach Lemma 1.2.7 gilt für ein $g \in G$: Hat g eine endliche Ordnung und ist $k := \operatorname{ord}(g) \in \mathbb{N}$, so ist k die kleinste positive Potenz mit $g^k = e$, und es gilt $g^{-1} = g^{k-1}$.*

iii.) *Ist die Gruppe G endlich, so hat jedes Element von G eine endliche Ordnung, da in G nur endliche Untergruppen liegen können.*

iv.) *Aus $\{\, g^i \mid i \in \mathbb{Z} \,\} = \{\, (g^{-1})^i \mid i \in \mathbb{Z} \,\}$ (Bemerkung 1.2.4) folgt sofort:*

$$\langle\, g \,\rangle = \langle\, g^{-1} \,\rangle \quad \textit{und} \quad \operatorname{ord}(g) = \operatorname{ord}(g^{-1}).$$

v.) *Die Gruppe $(\mathbb{Z},+)$ ist zyklisch wegen $\mathbb{Z} = \langle\, 1 \,\rangle = \langle\, -1 \,\rangle$. Bei dem Verknüpfungszeichen „$+$“ wird die i-te Potenz von 1 geschrieben als $i \bullet 1$, und es gilt im Falle der Gruppe $(\mathbb{Z},+)$ ja $i \bullet 1 = i \cdot 1 = i$ (Definition 1.1.27 und Bemerkung 1.1.28).*

vi.) *Eine unendliche Gruppe kann Elemente endlicher Ordnung enthalten: Sei dazu aus den Gruppen $(\mathbb{Z},+)$ und S_3 das kartesische Produkt $(\mathbb{Z} \times S_3, *)$ betrachtet (mit komponentenweiser Verknüpfung, siehe Satz 1.1.41), welches offensichtlich keine endliche Gruppe ist. Das Element $(0,\mathrm{id})$ ist das neutrale Element dieser Gruppe, und für $\sigma := (1\,2) \neq \mathrm{id}$ folgt dann mit $g := (0,\sigma) \neq (0,\mathrm{id})$ und $\sigma^2 = \mathrm{id}$:*

$$g^2 = g * g = (0+0, \sigma \circ \sigma) = (0, \sigma^2) = (0, \mathrm{id}) \quad \Longrightarrow \quad \operatorname{ord}(g) = 2. \qquad \square$$

Die zyklischen Gruppen sind alle abelsch, wie folgende kurze Rechnung zeigt:

LEMMA 1.2.10. *Sei $(G,*)$ eine Gruppe. Dann gilt:*

$$G \textit{ zyklisch} \quad \Longrightarrow \quad G \textit{ abelsch.}$$

Beweis. Sei g ein Erzeuger von G, d.h. es gilt $G = \langle g \rangle$. Dann haben $a, b \in G$ die Form $a = g^i$ und $b = g^j$ für geeignete $i, j \in \mathbb{Z}$, und es folgt aus den Potenzgesetzen:

$$a * b = g^i * g^j = g^{i+j} = g^{j+i} = g^j * g^i = b * a. \qquad \square$$

Bemerkung 1.2.11.

i.) Alle zyklischen Gruppen sind abelsch, wie die vorherige Aussage zeigt. Bei endlichen Gruppen ist die Beziehung zwischen beiden Gruppentypen sogar noch enger: die zyklischen Gruppen können als Bausteine der abelschen Gruppen aufgefaßt werden, denn jede endliche abelsche Gruppe ist im gewissen Sinne ein eindeutiges kartesisches Produkt von endlich vielen zyklischen Gruppen (siehe auch Satz 1.1.41 zum kartesichen Produkt verschiedener Gruppen). Dieses Ergebnis wird ein Speziallfall des Klassifikationssatzes von endlich erzeugten Moduln über Hauptidealringen in LA IIa sein.

ii.) Folgende Aussagen geben ein genaues Bild über die Struktur der endlichen zyklischen Gruppen, und der Beweis jeder Aussage ist eine leichte bis mittelschwere Übungsaufgabe (bei Aussage B ist die Eindeutigkeitsaussage der schwere Teil):

Aussage A: *Ist $(G, *)$ eine zyklische Gruppe und $U \subseteq G$ eine Untergruppe, so ist auch U zyklisch.*

Aussage B: *Ist $(G, *)$ eine endliche zyklische Gruppe der Ordnung $n := |G|$, so gibt es zu jedem Teiler k von n genau eine Untergruppe $U \subseteq G$ der Ordnung k.*

Natürlich liefert Aussage A, daß dann in Aussage B die Untergruppe U der Ordnung k auch zyklisch ist.

In Aussage B wird nur die Existenz von Untergruppen geliefert, deren Ordnung ein Teiler der Gruppenordnung ist. Der Grund liegt in der allgemeinen Aussage über endliche Gruppen, daß es höchstens zu Teilern der Gruppenordnung eine Untergruppe der entsprechenden Größe gibt. Dies wird in Kürze auch im „Satz von Lagrange“ (Satz 1.2.20) bewiesen, wenn der technische Apparat über Nebenklassen einer Untergruppe entwickelt ist. $\square$

Aussage A und B aus Bemerkung 1.2.11 erklären, wie die Untergruppen einer zyklischen Gruppe aussehen. Da im folgenden insbesondere die Untergruppen von $(\mathbb{Z}, +)$, dem „Prototyp“ einer zyklischen Gruppe, eine Rolle spielen, wird hier der konkrete Fall bewiesen (aus den folgenden Argumenten läßt sich jedoch leicht ein Beweis der zitierten Aussagen ableiten):

Satz 1.2.12. *In der Gruppe $(\mathbb{Z}, +)$ gilt:*

$$U \subseteq \mathbb{Z} \text{ Untergruppe} \quad \Longleftrightarrow \quad \exists k \in \mathbb{N}_0 : \quad U = \langle k \rangle.$$

Insbesondere sind damit alle Untergruppen von $(\mathbb{Z}, +)$ zyklisch.

Die Untergruppe $\langle k \rangle \subseteq \mathbb{Z}$, die der „$\mathbb{Z}$-Potenzen/-Vielfache“ von k, hat in bei dem Verknüpfungssymbol „ $+$ “ die Form:

$$\langle k \rangle = \{ a \bullet k \mid a \in \mathbb{Z} \},$$

(siehe Definition 1.1.27), und im speziellen Fall der Gruppe $(\mathbb{Z}, +)$ gilt nach Bemerkung 1.1.28 sogar mit der normalen Multiplikation „ $\cdot$ “ in $\mathbb{Z}$:

$$\langle k \rangle = \{ a \bullet k \mid a \in \mathbb{Z} \} = \{ a \cdot k \mid a \in \mathbb{Z} \}.$$

Beweis.
In diesem Beweis meint nach den Definitionen (additive Schreibweise) für $a, b \in \mathbb{Z}$ das Produkt $a \cdot b$ die a-fache Verknüpfung von b mit sich selbst. Insbesondere gilt dann für eine Untergruppe U und $u \in U$ immer $a \cdot u \in U$ für alle $a \in \mathbb{Z}$.
Die Differenz $a-b$ für $a, b \in \mathbb{Z}$ meint die additive Verknüpfung von a mit dem Inversen von b. Also gilt insbesondere für $a, b \in U$ dann $a - b \in U$ für eine Untergruppe U.

$\Longrightarrow$: Ist $U = \{0\}$, so ist die Aussage mit $k := 0$ bewiesen.
Sei also nun $U \neq \{0\}$, und so gibt es ein $a \in U \setminus \{0\}$. Dann liegt auch $-a$ in U, und $U \cap \mathbb{N}$ ist nicht leer.
Sei nun $k := \min(U \cap \mathbb{N})$. Zu zeigen ist, daß nun jedes $a \in U$ ein $\mathbb{Z}$-Vielfaches von k ist. Nach Satz 0.3.5 (Division mit Rest) existieren eindeutig bestimmte Elemente $q, r \in \mathbb{Z}$, für die gilt:

$$a = q \cdot k + r \quad \text{und} \quad 0 \leq r < k.$$

Mit k ist auch $q \cdot k \in U$, und damit $r = a - q \cdot k \in U$. Da $k \in U \cap \mathbb{N}$ minimal gewählt war, muß wegen $0 \leq r < k$ dann $r = 0$ gelten und $a = q \cdot k$.

$\Longleftarrow$: Nach Lemma 1.2.3 muß für $x, y \in U := \langle k \rangle$ gezeigt werden, daß auch $x - y \in U$ gilt. Es gibt für $x, y \in \langle k \rangle$ per Definition Elemente $a_1, a_2 \in \mathbb{Z}$ mit $x = a_1 \cdot k$ und $y = a_2 \cdot k$, woraus dann folgt:

$$x - y = a_1 \cdot k - a_2 \cdot k = (a_1 - a_2) \cdot k \in \langle k \rangle = U. \qquad \square$$

Ist G eine Gruppe und $U \subseteq G$ eine Untergruppe, so kann mit Hilfe von U auf G eine wesentliche Äquivalenzrelation definiert werden:

Lemma 1.2.13. *Sei $(G, *)$ eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann ist folgende durch U definierte Relation für $a, b \in G$ eine Äquivalenzrelation auf G:*

$$a \sim b \quad := \quad a^{-1} * b \in U.$$

Beweis.
„$\sim$“ reflexiv: Für alle $a \in G$ gilt $a^{-1} * a = e \in U$ und somit $a \sim a$.
„$\sim$“ symmetrisch: Für $a, b \in G$ folgt:

$$\begin{aligned} a \sim b \quad &\overset{\text{Def}}{\Longrightarrow} \quad a^{-1} * b \in U \quad \overset{U \text{ UG}}{\Longrightarrow} \quad \left(a^{-1} * b\right)^{-1} \in U \\ &\overset{1.1.25}{\Longrightarrow} \quad b^{-1} * a \in U \quad \overset{\text{Def}}{\Longrightarrow} \quad b \sim a. \end{aligned}$$

„$\sim$“ transitiv: Für $a, b, c \in G$ folgt:

$$\begin{aligned} a \sim b,\ b \sim c \quad &\Longrightarrow \quad a^{-1} * b,\ b^{-1} * c \in U \quad \overset{U \text{ UG}}{\Longrightarrow} \quad (a^{-1} * b) * (b^{-1} * c) \in U \\ &\Longrightarrow \quad a^{-1} * c \in U \quad \Longrightarrow \quad a \sim c. \end{aligned} \qquad \square$$

Beispiel 1.2.14.

i.) Es sei die Gruppe $(\mathbb{Z}, +)$ betrachtet und darin die Untergruppe

$$\langle 2 \rangle = \{ k \cdot 2 \mid k \in \mathbb{Z} \} \subseteq \mathbb{Z}.$$

Die in Lemma 1.2.13 durch $\langle 2 \rangle$ definierte Äquivalenzrelation heißt nun:

$$a \sim b \quad \Longleftrightarrow \quad -a + b \in \langle 2 \rangle \quad \Longleftrightarrow \quad a - b \in \langle 2 \rangle \quad \Longleftrightarrow \quad a - b \text{ ist gerade.}$$

Dies ist die Aufgabe: Übungsblatt 1, Aufgabe 1.c.) Relation (i).

Wird anstelle der Untergruppe $\langle 2 \rangle$ die triviale Untergruppe $\langle 0 \rangle = \{0\} \subseteq \mathbb{Z}$ betrachtet, ist die in Lemma 1.2.13 betrachtete Äquivalenzrelation von der Form:

$$a \sim b \quad \Longleftrightarrow \quad -a + b \in \langle 0 \rangle \quad \Longleftrightarrow \quad a - b = 0 \quad \Longleftrightarrow \quad a = b.$$

Dies ist die Aufgabe: Übungsblatt 1, Aufgabe 1.c.) Relation (iv).

ii.) Es sei die Gruppe S_3 betrachtet. Darin ist $\{\mathrm{id}, (1\,2)\}$ eine Untergruppe. Die Relation hat keine anschauliche Interpretation wie im vorherigen Beispiel, so daß sie am Besten durch die Angabe der Äquivalenzklassen beschrieben werden kann: denn zwei Elemente sind genau dann in Relation, wenn sie in der gleichen Äquivalenzklasse liegen. Eine Rechung mit den sechs Elementen von S_3 ergibt die folgenden Äquivalenzklassen:

$$\begin{aligned} [\mathrm{id}] &= \{\mathrm{id}, (1\,2)\} &&= [(1\,2)], \\ [(1\,3)] &= \{(1\,3), (1\,2\,3)\} &&= [(1\,2\,3)], \\ [(2\,3)] &= \{(2\,3), (1\,3\,2)\} &&= [(1\,3\,2)]. \end{aligned}$$

□

Eine Gruppe G kann also bzgl. einer Untergruppe disjunkt in die Äquivalenzklassen der Relation aus Lemma (1.2.13) zerlegt werden: allerdings ist nicht offensichtlich, wie die einzelnen Äquivalenzklassen systematisch beschrieben werden können. Dazu muß zuerst eine Verknüpfung von Teilmengen in einer Gruppe definieren werden:

Definition 1.2.15. *Sei $(G, *)$ eine Gruppe, und seien $A, B \subseteq G$ nicht-leere Teilmengen (ohne Strukturanforderung). Dann ist eine Verknüpfung der beiden Teilmengen (und damit eine innere Verknüpfung auf der Potenzmenge $\mathcal{P}(G)$ von G) definiert durch:*

$$A * B := \{\, a * b \mid a \in A, b \in B \,\}.$$

Ist $A := \{g\}$ einelementig, so wird $A * B = \{g\} * B$ auch notiert als $g * B$, analog dazu für $B := \{g\}$ dann $A * B = A * \{g\}$ als $A * g$.
Ist U eine Untergruppe von G und $g \in G$, so heißt $g * U$ die Linksnebenklasse von U mit dem Repräsentanten g, und entsprechend $U * g$ die Rechtsnebenklasse von U mit dem Repräsentanten g.
Mit G/U wird die Menge aller Linksnebenklassen von U bezeichnet, d.h. die Menge

$$G/U := \{\, g * U \mid g \in G \,\}.$$

Achtung: Die Menge G/U ist eine Menge von Teilmengen von G. Damit gilt:

$$G/U \not\subseteq G, \quad \textit{aber} \quad G/U \subseteq \mathcal{P}(G).$$

□

Bemerkung 1.2.16. *Ist $(G, *)$ eine Gruppe und $U \subseteq G$ eine Untergruppe, so gilt für eine Linksnebenklasse $g * U$ offensichtlich $g * U = \ell_g(U)$, d.h. sie ist das Bild von U unter der Linksmultiplikation ℓ_g mit g. Da ℓ_g eine Permutation von G ist, kann dann $g * U$ als Verschiebung von U unter der Bijektion ℓ_g aufgefaßt werden.* □

Es stellt sich nun heraus, daß die Äquivalenzklassen aus der Relation in Lemma 1.2.13 genau die Linksnebenklassen $g * U$ von U sind:

LEMMA 1.2.17. *Sei $(G,*)$ eine Gruppe und U eine Untergruppe. Auf G sei die Äquivalenzrelation aus Lemma 1.2.13 definiert:*

$$a \sim b \quad := \quad a^{-1} * b \in U.$$

Die Äquivalenzklasse von $g \in G$ sei mit $[g]_U$ bezeichnet (in leichter Abweichung zur Notation aus Definition 0.2.4, denn U ist hier nicht die Relation an sich, aber wesentlich für deren Definition). Dann ist die Äquivalenzklasse $[g]_U$ gleich der Linksnebenklasse $g * U$:

$$[g]_U = g * U.$$

Insbesondere übertragen sich auf die Linksnebenklassen von U die Eigenschaften von Klassen einer Äquivalenzrelation, woraus dann die folgenden nützlichen Aussagen über Linksnebenklassen hergeleitet werden können:

i.) Zwei Linksnebenklassen $g * U$ und $h * U$ sind entweder gleich oder disjunkt.

ii.) Für $h \in g * U$ gilt $h * U = g * U$.

iii.) $g * U = h * U \iff g^{-1} * h \in U$ und $g * U = U \iff g \in U$.

iv.) $g * U$ ist eine Untergruppe $\iff g \in U$.

BEWEIS.
Die Mengengleichheit $[g]_U = g * U$ ergibt sich sofort aus folgender Betrachtung:

$$\begin{aligned} h \in [g]_U \quad &\iff \quad g \sim h \\ &\iff \quad g^{-1} * h \in U \\ &\iff \quad g^{-1} * h = u \text{ für ein } u \in U \\ &\iff \quad h = g * u \text{ für ein } u \in U \\ &\iff \quad h \in g * U. \end{aligned}$$

Zu den weiteren Aussagen: Sei e das neutrale Element von U.

i.) Dies gilt für Äquivalenzklassen einer Äquivalenzrelation (siehe Satz 0.2.6).

ii.) Dies folgt ebenso sofort aus den Eigenschaften einer Äquivalenzrelation:

$$h \in g * U \quad \iff \quad h \in [g]_U \quad \overset{0.2.6}{\iff} \quad [h]_U = [g]_U \quad \iff \quad h * U = g * U.$$

iii.) Die erste Äquivalenz folgt aus:

$$g * U = h * U \quad \iff \quad [g]_U = [h]_U \quad \overset{0.2.6}{\iff} \quad g \sim h \quad \iff \quad g^{-1} * h \in U.$$

Offensichtlich ist $e * U = \ell_e(U) = \mathrm{id}_G(U) = U$, und dann liefert die vorherige Äquivalenzaussage:

$$U = g * U \quad \iff \quad e * U = g * U \quad \iff \quad e^{-1} * g \in U \quad \iff \quad g \in U.$$

iv.) $\Longleftarrow$: Ist $g \in U$, so gilt nach vorheriger Aussage $g * U = U$, so daß $g * U$ eine Untergruppe ist.

$\Longrightarrow$: Ist $g * U$ eine Untergruppe, so gilt $e \in g * U$ und damit:

$$g * U = [g]_U = [e]_U = U \quad \Longrightarrow \quad g \in U. \qquad \square$$

Bemerkung 1.2.18. *Sei $(G,*)$ eine Gruppe und U eine Untergruppe. Auf G kann mit Hilfe von U analog zu Lemma 1.2.13 auch die Äquivalenzrelation*

$$a \sim b \quad := \quad b * a^{-1} \in U$$

definiert (und analog bewiesen) werden. Dann sind die sich daraus ergebenden Äquivalenzklassen genau die Rechtsnebenklassen von U und Lemma 1.2.17 kann entsprechend umformuliert und analog bewiesen werden. □

Beispiel 1.2.19.

i.) Ist $(G,*)$ eine endliche Gruppe kleiner Ordnung und $U \subseteq G$ eine Untergruppe, so kann die Menge G/U der Linksnebenklassen sukzessiv mit Hilfe der Aussagen über Linksnebenklassen aus Lemma 1.2.17 berechnet werden. Als Äquivalenzklassen überdecken sie G disjunkt, und folgender Algorithmus liefert sie alle:

- *Die Untergruppe U ist selbst eine Linksnebenklasse von sich.*
- *Eine neue Linksnebenklasse ergibt sich, indem ein Element $g \in G \backslash U$ gewählt und dann die Linksnebenklasse $g * U$ berechnet wird.*
- *Solange ein Element aus G nicht in einer der schon berechneten Linksnebenklassen enthalten ist, wird mit diesem Element eine weitere Linksnebenklasse berechnet.*

Die Anzahl der Linksnebenklassen ist gleich $\frac{|G|}{|U|}$ (dies liefert der bald folgende Satz von Lagrange, Satz 1.2.20).

ii.) In Beispiel 1.2.14 wurde die durch $U := \{\mathrm{id}, (1\,2)\} \subseteq S_3$ definierte Äquivalenzrelation betrachtet. Die dort berechneten Äquivalenzklassen lassen sich nun als Linksnebenklassen von U interpretieren, und es gilt insbesondere mit den Regeln über Linknebenklassen aus Lemma 1.2.17:

$$\begin{aligned} U &= \{\mathrm{id}, (1\,2)\} &&= (1\,2)U, \\ (1\,3)U &= \{(1\,3), (1\,2\,3)\} &&= (1\,2\,3)U, \\ (2\,3)U &= \{(2\,3), (1\,3\,2)\} &&= (1\,3\,2)U. \end{aligned}$$

Hier ist zwischen dem Repräsentanten der Linksnebenklasse und der Untergruppe kein Verknüpfungssymbol notiert, da dieses auch bei Zykeln üblicherweise weggelassen wird. □

Nach Lemma 1.2.17 liefern die Linksnebenklassen aus G/U als Äquivalenzklassen einer Äquivalenzrelation eine disjunkte Zerlegung von G. Ist G eine endliche Gruppe, so sind natürlich auch alle Linksnebenklassen von U endlich und deren Anzahl (d.h. $|G/U|$), und die Größe von G kann durch (endliche) Summation aus den Größen aller Teilmengen der disjunkten Zerlegung berechnet werden. In diesem (endlichen) Fall gilt also:

$$G = \dot{\bigcup_{g*U \in G/U}} g * U \qquad \Longrightarrow \qquad |G| = \sum_{g*U \in G/U} |g * U|.$$

Die Linksnebenklasse $g * U$ ist das Bild von U unter der Permutation $\ell_g \in S(G)$, und offensichtlich ist die Abbildung $(\ell_g)_{|U}$ eine Bijektion von U nach $g * U$, so daß folgt:

$$|U| = |g * U|.$$

Wird dies nun in obige Gleichung eingesetzt, ergibt sich sofort:

$$|G| = \sum_{g*U \in G/U} |g * U| = \sum_{g*U \in G/U} |U| = |G/U| \cdot |U|.$$

Diese Gleichung ist als der Satz von Lagrange bekannt:

Satz 1.2.20. *(Satz von Lagrange)*
Sei $(G, *)$ eine endliche Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt:

$$|G| = |U| \cdot |G/U|.$$

Damit sind insbesondere $|U|$ und $|G/U|$ Teiler von $|G|$, und die Anzahl der Linksnebenklassen von U ist:

$$|G/U| = \frac{|G|}{|U|}.$$

Beweis. Siehe die Diskussion vor dem Satz. □

Bemerkung 1.2.21.

i.) Der Deutlichkeit halber hier noch einmal eine im Satz von Lagrange enthaltene Aussage in anderer Formulierung:

> *Ist G eine Gruppe der Ordnung n, so gibt es höchstens zu einem Teiler k von n eine Untergruppe der Ordnung k.*

Damit kann z.B. die Gruppe S_3 der Ordnung 6 höchstens Untergruppen der Ordnung 1, 2, 3 oder 6 haben.

ii.) Ist G eine Gruppe der Ordnung n, so gibt es genau eine Untergruppe der Ordnung 1, nämlich $\{e\}$ mit dem neutralen Element e von G, und genau eine Untergruppe der Ordnung n, nämlich G selbst. Zu echten Teilern der Gruppenordnung gibt es keine allgemeine Aussage.

iii.) Bei speziellen Gruppentypen kann mehr zur Existenz von Untergruppen gegebener Ordnung gesagt werden. Eine Aussage über zyklische Gruppen findet sich schon in Bemerkung 1.2.11 (und wird hier zitiert in Aussage 1), und auch für abelsche Gruppen existiert eine analoge Aussage:

Aussage 1: *Ist $(G, *)$ eine endliche zyklische Gruppe der Ordnung $n := |G|$, so gibt es zu jedem Teiler k von n genau eine Untergruppe $U \subseteq G$ der Ordnung k.*

Aussage 2: *Ist $(G, *)$ eine endliche abelsche Gruppe der Ordnung $n := |G|$, so gibt es zu jedem Teiler k von n mindestens eine Untergruppe $U \subseteq G$ der Ordnung k.*

Hierbei sei beachtet, daß die zyklischen Gruppen ebenfalls abelsche Gruppen sind (Lemma 1.2.10), und passend dazu ist die Aussage 1 auch eine Verschärfung der Aussage 2. (Eine Herleitung von Aussage 2 findet sich z.B. im Buch [**RSV**, Satz 56, Seite 58]*).*

Über nicht-abelsche Gruppen gibt es keine Existenzaussagen zu allen Teilern der Gruppenordnung: außer zu Primzahlpotenzen, welche die Gruppenordnung teilen. Auch dazu existieren dann immer Untergruppen der entsprechenden Ordnung, und es gibt sogar Einschränkungen zur möglichen Anzahl solcher Untergruppen und zusätzliche Strukturaussagen. Dies alles ist kummuliert in den sogenannten „Sylow-Sätzen“, über die auch in [**RSV**] *ausführlich gesprochen wird.* □

Der Satz von Lagrange (Satz 1.2.20) liefert sofort eine schöne Strukturaussage über endliche Gruppen:

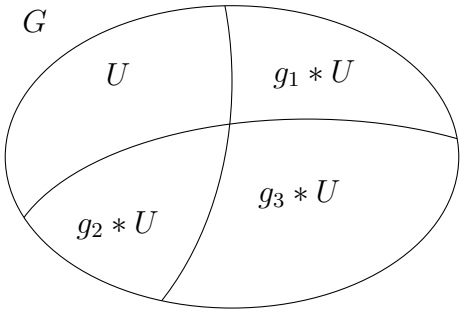
Satz 1.2.22. *Sei G eine endliche Gruppe mit dem neutralen Element e. Dann gilt:*

$$|G| \text{ ist eine Primzahl} \quad \Longrightarrow \quad G \text{ ist zyklisch und jedes } g \neq e \text{ ein Erzeuger von } G.$$

Beweis.
Ist $p := |G|$ eine Primzahl, dann gibt es nach dem Satz von Lagrange (Satz 1.2.20) nur Untergruppen der Ordnung 1 und p in G, also nur $\{e\}$ und G selbst. Für jedes $g \in G$ mit $g \neq e$ ist die von g erzeugte zyklische Untergruppe $\langle g \rangle$ nicht $\{e\}$ und damit aber schon ganz G. □

Normalteiler und Quotientengruppen.

Im Abschnitt über Nebenklassen einer Untergruppe wurde gezeigt, daß sich eine Gruppe G bzgl. einer Untergruppe U in deren disjunkte Linksnebenklassen $g * U$ zerlegen läßt, da diese gleich den Äquivalenzklassen der durch U definierten Äquivalenzrelation aus Lemma 1.2.13 sind:



Ziel ist es nun, auf der Menge G/U der Linksnebenklassen von U eine Gruppenstruktur zu definieren, die eng mit der Gruppenstruktur auf G verknüpft ist. Ein Aspekt davon ist zum Beispiel, daß je nach Wahl eines U die Menge G/U wesentlich kleiner ist als G, und so besteht die Hoffnung, die „kleinere Gruppe“ G/U besser verstehen und so Informationen auf die Gruppe G zurückziehen zu können.
Bei endlichen Gruppen ist der „Verkleinerungseffekt“ durch den Satz von Lagrange (Satz 1.2.20) beschrieben, da in diesem Fall gilt:

$$|G/U| = \frac{|G|}{|U|}.$$

Die obige Vorgabe, daß die gesuchte Gruppenstruktur auf G/U „eng“ mit der Gruppenstruktur auf G zusammenhängt, läßt natürlich Spielraum, denn „eng“ ist kein präziser Begriff. Die im folgenden vorgestellte Konstruktion/Diskussion, die leider nur für bestimmte Untergruppen U eines G eine Gruppenstruktur auf G/U liefert, ist aus guten mathematischen Gründen die einzig sinnvolle - jedoch fehlt noch einiges an Voraussetzungen, um diese Gründe hier zu nennen.

Um auf den Linksnebenklassen von U, welche ja Teilmengen von G und damit Elemente der Potenzmenge $\mathcal{P}(G)$ sind, eine Verknüpfung zu definieren, könnte auf die

Definition 1.2.15 zurückgriffen werden: dort ist schon eine innere Verknpüfung auf $\mathcal{P}(G)$ definiert, für zwei Teilmengen $A, B \in \mathcal{P}(G)$ das „elementweise“ Produkt

$$A * B := \{\, a * b \mid a \in A, b \in B \,\}.$$

Da bei dieser elementweisen Verknüpfung der Linksnebenklassen die Gruppenverknüpfung eingeht, ist ein Zusammenhang der Verknüpfungen sicher gegeben.
Es ist aber nicht klar, ob die Teilmenge $G/U \subseteq \mathcal{P}(G)$ abgeschlossen unter dieser Verknüpfung ist, d.h. ob das elementweise Produkt zweier Linksnebenklassen wieder eine Linksnebenklasse ist. Eine kleine Beispielrechnung zeigt, daß dies nicht immer der Fall ist, und als Gegenbeispiel wird die Untergruppe $U := \{\mathrm{id}, (1\,2)\} \subseteq S_3$ gewählt, deren Linksnebenklassen in Beispiel 1.2.19 aufgeführt sind. Folgende Rechnung zeigt, daß in diesem Fall das elementweise Produkt zweier Linksnebenklassen keine Linksnebenklasse sein muß:

$$(1\,3)U * (2\,3)U = \{(1\,3\,2), (2\,3), (1\,2), \mathrm{id}\} \notin S_3/U. \tag{1.2.23}$$

Das Problem, daß G/U nicht abgeschlossen ist unter der elementweisen Verknüpfung der Linksnebenklassen, kann durch zusätzliche Forderungen an U behoben werden (die dann obige Untergruppe nicht erfüllt). Aber diese Diskussion wird hier nicht geführt.
Stattdessen wird versucht, auf den Linksnebenklassen mit Hilfe ihrer Repräsentanten eine Verknüpfung zu definieren, da eine Linksnebenklasse meist eh nur über einen geschickt gewählten Repräsentanten beschrieben wird. Das später resultierende Ergebnis dieser Untersuchung und Konstruktion ist jedoch das gleiche, als ob die Analyse der elementweisen Verknüpfung weiter vorangetrieben worden wäre.

Da Linksnebenklassen einer Untergruppe $U \subseteq G$ mit Hilfe eines Repräsentanten aus G beschrieben werden können, liegt es nun nahe zu untersuchen, ob die Verknüpfung auf G eine Verknüpfung auf der Menge der Linksnebenklassen G/U induziert, indem Linksnebenklassen mit Hilfe der Repräsentanten verknüpft werden:

$$(g * U) \circledast (h * U) := (g * h) * U. \tag{1.2.24}$$

Problematisch könnte dabei sein, daß die Repräsentanten einer Linksnebenklasse $g*U$ nicht eindeutig sind: jedes Element $h \in g*U$ erfüllt $h*U = g*U$ und ist ein möglicher Repräsentant (siehe Lemma 1.2.17), und für $|U| > 1$ gibt es dann wegen $|g*U| = |U|$ immer mehrere Repräsentanten für $g*U$. Zu untersuchen ist also, ob die obige Definition der Verknüpfung „$\circledast$“ wohldefiniert ist, d.h. bei einem Repräsentantenwechsel immer das gleiche Ergebnis liefert und damit folgende Bedingung erfüllt:

$$g * U = \tilde{g} * U, \quad h * U = \tilde{h} * U \quad \overset{?}{\Longrightarrow} \quad (g * h) * U = (\tilde{g} * \tilde{h}) * U.$$

Daß tatsächlich der Fall auftreten kann, wo Repräsentantenwechsel zu unterschiedlichen Ergebnissen führt, zeigt das folgende Beispiel, in dem die gleichen Nebenklassen wie im Gegenbeispiel zur elementweisen Verknüpfung benutzt werden (1.2.23), um auch unter den neuen Gesichtspunkten ein Gegenbeispiel zu liefern:

Beispiel 1.2.25. *In S_3 sei folgende Untergruppe gewählt: $U := \{\mathrm{id}, (1\,2)\}$. Dann gilt für folgende Linksnebenklassen:*

$$(1\,3)U = \{(1\,3), (1\,2\,3)\} = (1\,2\,3)U \quad \textit{und} \quad (2\,3)U = \{(2\,3), (1\,3\,2)\} = (1\,3\,2)U.$$

Werden die Linksnebenklassen nun mit „ $\circledast$ “ aus 1.2.24 verknüpft, so ergeben sich je nach Repräsentantenwahl verschiedenen Ergebnisse:

$$\begin{array}{ccccccccc}
(1\,3)U & \circledast & (2\,3)U & \overset{(\text{Def } 1.2.24)}{=} & (1\,3)(2\,3)U & = & (1\,3\,2)U & = & (2\,3)U \\
\| & & \| & & & & & & \nparallel \\
(1\,2\,3)U & \circledast & (1\,3\,2)U & \overset{(\text{Def } 1.2.24)}{=} & (1\,2\,3)(1\,3\,2)U & = & \mathrm{id} * U & = & U \qquad \square
\end{array}$$

Dem kann Abhilfe geschaffen werden durch die Einschränkung der Konstruktion auf spezielle Untergruppen, die nun ersteinmal einzuführen sind:

Definition 1.2.26. *Sei $(G, *)$ eine Gruppe. Eine Untergruppe $N \subseteq G$ heißt Normalteiler, falls für alle $g \in G$ ihre Linksnebenklasse bzgl. g mit der Rechtsnebenklasse bzgl. g übereinstimmt, d.h. falls gilt:*

$$g * N = N * g \quad \text{für alle} \quad g \in G.$$

Dies ist äquivalent zu der Forderung, daß für alle $g \in G$ gilt: $g * N * g^{-1} = N$. $\square$

Bemerkung 1.2.27.

i.) In der Definition eines Normalteilers tritt ein Term auf, der strenggenommen noch nicht definiert wurde: $g * N * g^{-1}$. Allerdings ist die elementweise Verknüpfung von Mengen aus Definition 1.2.15 eine assoziative innere Verknüpfung auf $\mathcal{P}(G)$, d.h. es gilt für $A, B, C \subseteq G$

$$A * (B * C) = (A * B) * C,$$

so daß obiger Term als Kurzschreibweise aufzufassen ist für:

$$\{g\} * \big(N * \{g^{-1}\}\big) = \big(\{g\} * N\big) * \{g^{-1}\}.$$

ii.) Bei einem Normalteiler $N \subseteq G$ ist verlangt, daß für jedes $g \in G$ die Linksnebenklasse von N bzgl. g gleich der entsprechenden Rechtsnebenklasse ist, also $g * N = N * g$ gilt. Dies ist jedoch nur eine Gleichheit der Mengen, und für ein $n \in N$ kann durchaus der Fall $g * n \neq n * g$ auftreten!

Beispiel 1.2.28.

i.) In einer abelsche Gruppe sind alle ihre Untergruppen auch Normalteiler.
Ist G eine abelsche Gruppe und $U \subseteq G$ eine Untergruppe, so gilt nicht nur für ein $g \in G$ die Mengengleichheit $g * U = U * g$, sondern sogar elementweise $g * u = u * g$ für alle $u \in U$.

ii.) Es ist eine leichte Übungsaufgabe zu zeigen, daß die folgende Untergruppe von S_3 sogar ein Normalteiler ist:

$$A_3 := \langle\, (1\,2\,3)\,\rangle \subseteq S_3.$$

Insbesondere gilt dann die Mengengleichheit $(1\,2)A_3 = A_3(1\,2)$, aber das Element $(1\,2\,3) \in A_3$ kommutiert nicht mit $(1\,2)$:

$$(1\,2)(1\,2\,3) = (2\,3) \neq (1\,3) = (1\,2\,3)(1\,2).$$

iii.) Die Untergruppe $U := \{\mathrm{id}, (12)\} \subseteq S_3$ aus Beispiel 1.2.25 ist kein Normalteiler, denn es gilt:

$$(1\,3)U = \{(1\,3), (1\,2\,3)\} \neq \{(1\,3), (1\,3\,2)\} = U(1\,3). \qquad \square$$

Der nächste Satz zeigt nun, daß es für Normalteiler möglich ist, auf der Menge der Linksnebenklassen eine Verknüpfung mit Hilfe der Repräsentaten zu definieren, die unabhängig von der Wahl des jeweiligen Repräsentanten ist:

Satz 1.2.29. *Sei $(G, *)$ eine Gruppe und $N \subseteq G$ ein Normalteiler. Auf der Menge der Linksnebenklassen G/N sei definiert:*

$$(g * N) \circledast (h * N) := (g * h) * N.$$

Dann ist „ $\circledast$ “ eine wohldefinierte innere Verknüpfung auf G/N und $(G/N, \circledast)$ eine Gruppe. Wohldefiniert heißt in diesem Zusammenhang, daß die Verknüpfung repräsentantenunabhängig ist, also für $g * N = \tilde{g} * N$ und $h * N = \tilde{h} * N$ gilt:

$$(g * N) \circledast (h * N) = (\tilde{g} * N) \circledast (\tilde{h} * N).$$

Das neutrale Element in $(G/N, \circledast)$ ist der Normalteiler N selbst (oder auch z.B. geschrieben als Nebenklasse $e_G * N$ mit dem neutralen Element $e_G \in G$).
Für eine Linksnebenklasse $g * N$ ist $g^{-1} * N$ das inverse Element.
Weiter gilt: Ist $(G, *)$ eine abelsche Gruppe, so auch $(G/N, \circledast)$.

Beweis.

„ $\circledast$ “ wohldefiniert: Zu zeigen ist:

$$g * N = \tilde{g} * N \quad \text{und} \quad h * N = \tilde{h} * N \quad \Longrightarrow \quad (g * N) \circledast (h * N) = (\tilde{g} * N) \circledast (\tilde{h} * N).$$

Aus $g * N = \tilde{g} * N$ folgt $g \in \tilde{g} * N$ und $g = \tilde{g} * n_1$ für ein $n_1 \in N$, und analog dazu gilt $h = \tilde{h} * n_2$ für ein $n_2 \in N$. Da N ein Normalteiler ist, gilt $N * \tilde{h} = \tilde{h} * N$, und zu $n_1 \in N$ muß es ein $\tilde{n}_1$ geben mit $n_1 * \tilde{h} = \tilde{h} * \tilde{n}_1$. Dann folgt mit Lemma 1.2.17 wegen $(\tilde{g} * \tilde{h})^{-1} * (\tilde{g} * \tilde{h} * \tilde{n}_1 * n_2) \in N$:

$$\begin{aligned}(g * N) \circledast (h * N) &\overset{(\text{Def})}{=} (g * h) * N = (\tilde{g} * n_1 * \tilde{h} * n_2) * N = (\tilde{g} * \tilde{h} * \tilde{n}_1 * n_2) * N \\ &\overset{(1.2.17)}{=} (\tilde{g} * \tilde{h}) * N \overset{(\text{Def})}{=} (\tilde{g} * N) \circledast (\tilde{h} * N).\end{aligned}$$

„ $\circledast$ “ innere Verknüpfung: Dies ist per Definition erfüllt, denn zwei Linksnebenklassen werden zu einer neuen Linksnebenklasse verknüpft. Somit $(G/N, \circledast)$ eine algebraische Struktur.

„ $\circledast$ “ assoziativ: Die Assoziativität von „ $\circledast$ “ ergibt sich sofort aus der Assoziativität der Verknüpfung „ $*$ “, denn für $g * N$, $h * N$ und $w * N$ gilt:

$$\begin{aligned}\big((g * N) \circledast (h * N)\big) \circledast (w * N) &\overset{(\text{Def})}{=} \big((g * h) * N\big) \circledast (w * N) \overset{(\text{Def})}{=} \big((g * h) * w\big) * N \\ &\overset{(* \text{ ass})}{=} \big(g * (h * w)\big) * N \overset{(\text{Def})}{=} (g * N) \circledast \big((h * w) * N\big) \\ &\overset{(\text{Def})}{=} (g * N) \circledast \big((h * N) \circledast (w * N)\big).\end{aligned}$$

Neutrales Element: N ist das neutrales Element bzgl. der Verknüpfung „ $\circledast$ “, denn nach Lemma 1.2.17 gilt $N = e_G * N$, und es folgt sofort für jedes $g * N \in G/N$:

$$N \circledast (g * N) \overset{(1.2.17)}{=} (e_G * N) \circledast (g * N) \overset{(\text{Def})}{=} (e_G * g) * N \overset{(e_G \text{ neutr})}{=} g * N.$$

$$(g * N) \circledast N \overset{(1.2.17)}{=} (g * N) \circledast (e_G * N) \overset{(\text{Def})}{=} (g * e_G) * N \overset{(e_G \text{ neutr})}{=} g * N.$$

Inverses zu $g * N$: Die Linksnebenklasse $g^{-1} * N$ erfüllt die nötigen Gleichungen:

$$(g * N) \circledast (g^{-1} * N) \overset{\text{(Def)}}{=} (g * g^{-1}) * N = e_G * N = N.$$

$$(g^{-1} * N) \circledast (g * N) \overset{\text{(Def)}}{=} (g^{-1} * g) * N = e_G * N = N.$$

Somit ist $(G/N, \circledast)$ eine Gruppe.
Ist G sogar eine abelsche Gruppe, so gilt dies auch für G/N, denn für $g * N$ und $h * N$ aus G/N folgt:

$$(g * N) \circledast (h * N) \overset{\text{(Def)}}{=} (g * h) * N \overset{(* \text{ komm})}{=} (h * g) * N \overset{\text{(Def)}}{=} (h * N) \circledast (g * N). \quad \square$$

Bemerkung 1.2.30. *Sei $(G, *)$ eine Gruppe, $U \subseteq G$ eine Untergruppe und G/U die Menge der Linksnebenklassen von U. Für die „Repräsentantenverknüpfung“ zweier Linksnebenklassen (siehe 1.2.24) in G/U wurde bisher gezeigt:*

i.) Die Verknüpfung „$\circledast$“ auf den Linksnebenklassen ist nicht immer wohldefiniert (siehe Beispiel 1.2.25).
ii.) Falls U ein Normalteiler ist, so ist die Verknüpfung „$\circledast$“ wohldefiniert (siehe 1.2.29).

Offen ist noch die Frage, ob die Wohldefiniertheit von „$\circledast$“ schon impliziert, daß U ein Normalteiler ist.
Auch folgende Frage ist noch offen: Ist die eingangs betrachtete elementweise Multiplikation von Linksnebenklassen auch eine innerere Verknüpfung auf G/U, wenn U ein Normalteiler ist? Und gilt dies auch umgekehrt?
Die Antwort auf diese Fragen liefern folgende Äquivalenzen (Übung!):

i.) U ist ein Normalteiler.
ii.) Die Repräsentantenverknüpfung auf den Linksnebenklassen ist wohldefiniert, d.h. unabhängig von der Repräsentantenwahl.
iii.) Die elementweise Verknüpfung ist eine innere Verknüpfung auf G/U, d.h. das Produkt zweier Linksnebenklassen liefert eine Linksnebenklasse.

Ist G/U unter der elementweisen Verknüpfung abgeschlossen, so muß das elementweise Produkt zweier Linksnebenklassen mit deren Repräsentantenprodukt übereinstimmen, denn für die Mengenverknüpfung gilt:

$$(g * U) * (h * U) = \{\, g * u * h * \tilde{u} \mid u, \tilde{u} \in U \,\} \quad \Longrightarrow \quad g * h \in (g * U) * (h * U),$$

und ist das Mengenprodukt eine Linksnebenklasse $x * U$, so folgt wegen $g * h \in x * U$ dann $x * U = (g * h) * U$ (Lemma 1.2.17).
Es ist also egal und eine Geschmacksfrage, ob eine Verknüpfung auf den Linksnebenklassen durch eine Repräsentantenverknüpfung oder elementweise Verknüpfung definiert wird, denn diese Möglichkeiten sind äquivalent und das resultierende Ergebnis gleich: entscheidend ist das Ergebnis, daß eine Verknüpfung für Normalteiler (und nur für Normalteiler) definierbar ist und in beiden Fällen die gleiche Gruppenstruktur auf der Menge G/U liefert. $\square$

Damit kann nun definiert werden:

Definition 1.2.31. *Sei $(G, *)$ ein Gruppe und $N \subseteq G$ ein Normalteiler. Dann heißt die in Satz 1.2.29 konstruierte Gruppe $(G/N, \circledast)$ die Quotientengruppe (oder auch Faktorgruppe) von G nach N.* $\square$

Beispiel 1.2.32. *Sei $(G,*)$ eine Gruppe und $N \subseteq G$ ein Normalteiler mit*

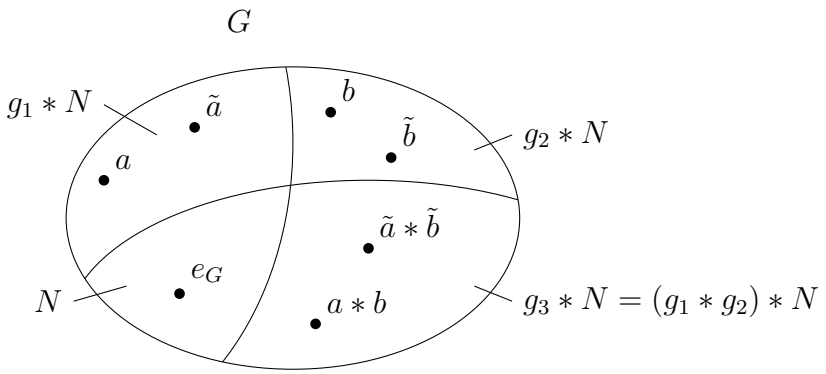
$$G/N = \{\, N, g_1 * N, g_2 * N, g_3 * N \,\} \quad \text{und} \quad g_1 * g_2 = g_3.$$

Dann liefern die vier Linksnebenklassen eine disjunkte Zerlegung von G, und es gilt mit $a, \tilde{a} \in g_1 * N$ und $b, \tilde{b} \in g_2 * N$:

i.) $a * N = \tilde{a} * N = g_1 * N$ *und* $b * N = \tilde{b} * N = g_2 * N$.

ii.) $a * b, \tilde{a} * \tilde{b} \in g_3 * N = (g_1 * g_2) * N$.

Folgende Skizze veranschaulicht die obigen Aussagen:



□

Ein wichtiges Beispiel von Quotientengruppen ist das folgende: In der zyklischen und damit abelschen Gruppe $(\mathbb{Z}, +)$ ist jede Untergruppe ein Normalteiler und nach Satz 1.2.12 von der Form:

$$\langle\, n \,\rangle = \{\, a \cdot n \mid a \in \mathbb{Z} \,\}.$$

Nun sind sowohl $\mathbb{Z}$ als auch die Untergruppe $\langle\, n \,\rangle$ unendliche Mengen, so daß a priori nicht klar ist, ob $\mathbb{Z}/\langle\, n \,\rangle$ eine endliche oder unendliche Gruppe ist. Der folgende Satz jedoch klärt über die Struktur dieser Quotientengruppe auf:

Satz 1.2.33. *Sei $n \in \mathbb{N}$. Dann ist nach Satz 1.2.12 die Menge*

$$\langle\, n \,\rangle := \{\, a \cdot n \mid a \in \mathbb{Z} \,\}$$

eine Untergruppe der zyklischen und damit abelschen Gruppe $(\mathbb{Z}, +)$, und somit sogar ein Normalteiler.
Die Linksnebenklassen von $\langle\, n \,\rangle$ in $\mathbb{Z}$ lassen sich alle eindeutig durch einen Repräsentanten aus der Menge $\{0, \ldots, n-1\}$ beschreiben, und damit hat die die Quotientengruppe $(\mathbb{Z}/\langle\, n \,\rangle, \oplus)$ (Satz 1.2.29) die Form:

$$\mathbb{Z}/\langle\, n \,\rangle = \{\, 0 + \langle\, n \,\rangle, \ldots, (n-1) + \langle\, n \,\rangle \,\}.$$

Zwei Linksnebenklassen $a + \langle\, n \,\rangle$, $b + \langle\, n \,\rangle$ werden repräsentantenweise verknüpft:

$$\big(a + \langle\, n \,\rangle\big) \oplus \big(b + \langle\, n \,\rangle\big) = (a + b) + \langle\, n \,\rangle.$$

Das neutrale Element in $\mathbb{Z}/\langle\, n \,\rangle$ ist $0 + \langle\, n \,\rangle = \langle\, n \,\rangle$.
Das Inverse einer Linksnebenklasse $a + \langle\, n \,\rangle$ ist $(n - a) + \langle\, n \,\rangle$, denn es gilt:

$$(n - a) + \langle\, n \,\rangle = (-a) + \langle\, n \,\rangle.$$

Die Gruppe $(\mathbb{Z}/\langle\, n \,\rangle, \oplus)$ ist zyklisch und damit abelsch, und $1 + \langle\, n \,\rangle$ ist ein Erzeuger.

Beweis. Zuerst wird gezeigt, daß jede Linksnebenklasse aus $\mathbb{Z}/\langle n \rangle$ einen eindeutigen Repräsentanten aus der Menge $\{0, \ldots, n-1\}$ hat.

Existenz: Für $a \in \mathbb{Z}$ wird gezeigt, daß es ein $r \in \mathbb{Z}$ mit $0 \leq r \leq n-1$ gibt, so daß gilt: $a + \langle n \rangle = r + \langle n \rangle$. Dazu wird die Division mit Rest (Satz 0.3.5) auf n und a angewandt. Es exitieren eindeutig bestimmte Elemente $q, r \in \mathbb{Z}$ mit:

$$a = q \cdot n + r \quad \text{und} \quad 0 \leq r < n,$$

und mit Lemma 1.2.17 folgt dann:

$$a - r = q \cdot n \in \langle n \rangle \quad \overset{1.2.17}{\Longrightarrow} \quad a + \langle n \rangle = r + \langle n \rangle.$$

Eindeutigkeit: Es reicht zu zeigen, daß für $0 \leq a \leq b < n$ gilt:

$$a + \langle n \rangle = b + \langle n \rangle \quad \Longrightarrow \quad a = b.$$

Aus $a + \langle n \rangle = b + \langle n \rangle$ folgt mit Lemma 1.2.17 dann $b - a \in \langle n \rangle$, also ist $b - a = k \cdot n$. Wegen $b - a \geq 0$ und $n \geq 0$ ist $k \geq 0$. Dies liefert sofort:

$$0 \leq b - a = k \cdot n \leq b < n \quad \Longrightarrow \quad 0 \leq k \cdot n < n.$$

Es folgt $k = 0$, und damit ist $b - a = 0$ und $b = a$.

Die repräsentantenweise Verknüpfung in $\mathbb{Z}/\langle n \rangle$ ist genau so in Satz 1.2.29 definert. Da 0 das neutrale Element ist, folgt nach Satz 1.2.29 (bzw. aus der repräsentantenweisen Verknüpfung), daß $0 + \langle n \rangle$ das neutrale Element in $\mathbb{Z}/\langle n \rangle$ ist.
Das Inverse zu $a + \langle n \rangle$ ist nach Satz 1.2.29 die Linksnebenklasse $(-a) + \langle n \rangle$, und es gilt mit Lemma 1.2.17:

$$-(-a) + (n - a) = n \in \langle n \rangle \quad \overset{1.2.17}{\Longrightarrow} \quad (-a) + \langle n \rangle = (n - a) + \langle n \rangle.$$

$1 + \langle n \rangle$ ist offensichtlich ein Erzeuger von $(\mathbb{Z}/\langle n \rangle, \oplus)$, und die Gruppe damit zyklisch und abelsch. □

Da die Gruppe $(\mathbb{Z}/\langle n \rangle, \oplus)$ eine wichtige Rolle spielt, bekommt sie eine kürzere Notation und einen eigenen Namen:

Definition 1.2.34. *Sei $n \in \mathbb{N}$. Die in Satz 1.2.33 konstruierte Quotientengruppe von $(\mathbb{Z}, +)$ modulo des Normalteilers $\langle n \rangle$ heißt die n-te Restklassengruppe und wird notiert als $(\mathbb{Z}_n, +)$. Eine Linksnebenklasse mit dem Repräsentanten $a \in \mathbb{Z}$ wird mit $[a]_n$ bezeichnet und heißt auch Restklasse von a modulo n. So gilt:*

$$\mathbb{Z}_n = \{ [0]_n, \ldots, [n-1]_n \} \quad \textit{und} \quad [a]_n + [b]_n = [a + b]_n.$$

Gilt $[a]_n = [b]_n$, so ist „a gleich b modulo n“ oder „a kongruent b modulo n“:

$$a \equiv b \mod n.$$ □

Beispiel 1.2.35. *Es sei die Restklassengruppe $\mathbb{Z}_5$ betrachtet: Die folgende Tabelle listet zu jeden Element aus $\mathbb{Z}_5$ das Inverse auf:*

$\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$:

$[a]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[-a]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Hat $a \in \mathbb{Z}$ die Zerlegung $a = q \cdot 5 + r$ mit $0 \leq r < 5$, so gilt $[a]_5 = [r]_5$, so daß folgt:

$$[-23]_5 = [(-5) \cdot 5 + 2]_5 = [2]_5 \quad \textit{und} \quad [123]_5 = [24 \cdot 5 + 3]_5 = [3]_5.$$

Ist eine Restklasse modulo n mit einem großen Repräsentanten beschrieben, so kann auch schrittweise ein Repräsentant aus der Menge $\{0, \ldots, n-1\}$ berechnet werden, indem Stück für Stück der jeweilig aktuelle Repräsentant in eine Summe aufgesplittet wird, dessen Summanden leicht modulo n gerechnet werden können (z.B. weil er ein Vielfaches von n ist). Dies liefert z.B. für den Fall $n = 5$:

$$[873]_5 = [800+73]_5 = [800]_5 + [73]_5 = [0]_5 + [70+3]_5 = [70]_5 + [3]_5 = [0]_5 + [3]_5 = [3]_5.$$

Im bald kommenden Abschnitt über Ringe wird auch noch die Multiplikation in $\mathbb{Z}$ in die Rechnung modulo n mit einbezogen, so daß weitere Betrachtungen bis dahin aufgeschoben werden. □

Es soll noch ein weiteres nützliches Beispiel für die Bestimmung der Linksnebenklassen einer Untergruppe durch die geschickte Auswahl von Repräsentanten betrachtet werden. Dabei ist im folgenden Fall die Untergruppe kein Normalteiler (Übung!), so daß keine Quotientengruppenstruktur auf der Menge der Linksnebenklassen existiert:

Lemma 1.2.36. *Sei $n \in \mathbb{N}$. In S_n sei die Untergruppe U_n aller derjenigen Permutationen betrachtet, die n als Fixpunkt haben (Beispiel 1.2.4):*

$$U_n := \{\, f \in S_n \mid f(n) = n \,\}.$$

Dann läßt sich jede Linksnebenklasse von U_n eindeutig durch einen Repräsentanten aus der Menge $\big\{\, \mathrm{id}, (1\,n), (2\,n), \ldots, \big((n-1)\,n\big)\big\}$ beschreiben, so daß folgt:

$$S_n/U_n = \big\{\, \mathrm{id}\, U_n, (1\,n)U_n, \ldots, \big((n-1)\,n\big)U_n \big\} \quad \textit{und} \quad |S_n/U_n| = n.$$

Beweis. Wesentlich für den Beweis ist folgende Aussage aus Lemma 1.2.17:

$$\sigma_1 \circ U_n = \sigma_2 \circ U_n \quad \Longleftrightarrow \quad (\sigma_1^{-1} \circ \sigma_2) \in U_n.$$

Zuerst wird gezeigt, daß jedes $f \in S_n$ in einer Nebenklasse $\sigma \circ U_n$ mit einem Element $\sigma \in \big\{\, \mathrm{id}, (1\,n), \ldots, \big((n-1)\,n\big)\big\}$ liegt. Dazu reicht es nach obiger Äquivalenzaussage, ein σ mit $\sigma^{-1} \circ f \in U_n$ zu finden, was wegen $\sigma^{-1} = \sigma$ für jedes der speziellen Repräsentanten gleichbedeutend damit ist, daß $\sigma \circ f$ den Fixpunkt n besitzt.
Für $f \in U_n$ ist „id“ ein geeigneter Repräsentant. Ist $i := f(n) \neq n$, so muß $1 \leq i < n$ gelten, und es folgt:

$$((i\,n) \circ f)(n) = (i\,n)\big(f(n)\big) = (i\,n)(i) = n \quad \Longrightarrow \quad f \in \sigma \circ U_n.$$

Um einzusehen, daß alle angegebenen Nebenklassen verschieden sind, muß nach der Äquivalenzaussage am Anfang des Beweises gezeigt werden, daß für zwei unterschiedliche Elemente $\sigma_i, \sigma_j \in \big\{\, \mathrm{id}, (1\,n), \ldots, (n-1\,n)\big\}$ das Produkt $\sigma_i^{-1} \circ \sigma_j$ nicht in U_n liegt, d.h. nicht n als Fixpunkt hat. Da alle Repräsentanten selbstinvers sind, reicht es, den Test für $\sigma_i \circ \sigma_j$ durchzuführen.

Außer „id“ liegt keiner der speziellen Repräsentanten in U_n, so daß nur Produkte $\sigma_i \circ \sigma_j$ betrachtet werden müssen, die nicht den Faktor „id“ enthalten. Für $(i\,n), (j\,n)$ mit $i \neq j$ und $i, j < n$ folgt aber:

$$(i\,n)(j\,n) = (j\,i\,n) \notin U_n. \qquad \square$$

Bemerkung 1.2.37. *Die Aussage aus Lemma 1.2.36 wird unter folgendem Gesichtspunkt besonders interessant: Die Gruppe S_n ist formal keine Untergruppe von S_{n+1}, da die Permutationen aus verschiedenen Gruppen verschiedene Definitions- und Wertebereiche haben. Aber eine Permutation $f \in S_n$ kann einfach zu einer Permutation aus $\tilde{f} \in S_{n+1}$ „erweitert“ werden, in dem der Fixpunkt $n+1$ „hinzugefügt“ wird:*

$$\tilde{f}(i) := \begin{cases} f(i) & \text{für } 1 \leq i \leq n, \\ n+1 & \text{für } i = n+1, \end{cases}$$

und eine solche Zuordnung $f \mapsto \tilde{f}$ liefert offensichtlich eine Bijektion von der Gruppe S_n auf die Untergruppe $U_{n+1} \subseteq S_{n+1}$.
Werden die Permutationen f und $\tilde{f}$ in Zykeldarstellung notiert (Satz 1.1.34), werden die beiden Permutationen sowieso als gleiche behandelt, da der Fixpunt n von $\tilde{f}$ nicht notiert wird.
Somit gilt insbesondere $|S_n| = |U_{n+1}|$, und nach Lemma 1.2.36 folgt mit dem Satz von Lagrange $|S_{n+1}| = (n+1) \cdot |U_{n+1}|$. Durch vollständige Induktion über n mit dem Induktionsanfang $|S_1| = |\{\mathrm{id}\}| = 1$ folgt:

$$|S_{n+1}| = (n+1) \cdot |S_n| \quad \overset{\text{Induktion}}{\Longrightarrow} \quad |S_n| = n! = 1 \cdot 2 \cdot \dots \cdot n. \qquad \square$$

Gruppenhomomorphismen.

Als nächstes werden Abbildungen zwischen Gruppen behandelt, die auch mit der algebraischen Struktur auf den jeweiligen Mengen verträglich sind. Was dies genau bedeuten soll, legt folgende Definition fest:

Definition 1.2.38. *Seien $(M, *)$ und $(N, \diamond)$ algebraische Strukturen, und weiter sei $\varphi\colon M \longrightarrow N$ eine Abbildung. φ heißt strukturverträglich bzw. strukturerhalend, falls für alle $a, b \in M$ gilt:*

$$\varphi(a * b) = \varphi(a) \diamond \varphi(b).$$

Eine solche Abbildung wird auch Homomorphismus genannt.
Tragen $(M, *)$ und $(N, \diamond)$ die gleiche algebraische Struktur (beide sind Halbgruppen, Monoide oder Gruppen), so heißt φ dementsprechend Halbgruppenhomomorphismus, Monoidhomomorphismus oder Gruppenhomomorphismus.
Ein Homomorphismus heißt Isomorphismus, falls er auch bijektiv ist. Er heißt Epimorphismus, falls er surjektiv ist, und Monomorphismus oder Einbettung, falls er injektiv ist.
Gilt $M = N$, so heißt ein Homomorphismus auch Endomorphismus, und ein Isomorphismus auch Automorphismus.
Die Menge aller Homomorphismen von $(M, *)$ nach $(N, \diamond)$ wird mit $\mathrm{Hom}(M, N)$ bezeichnet, die Menge aller Endomorphismen von $(M, *)$ mit $\mathrm{End}(M)$, und die Menge aller Automorphismen von $(M, *)$ mit $\mathrm{Aut}(M)$.

Zwei algebraische Strukturen M und N heißen isomorph, falls es einen Isomorphismus $\varphi\colon M \longrightarrow N$ gibt, und dies wird bezeichnet durch:

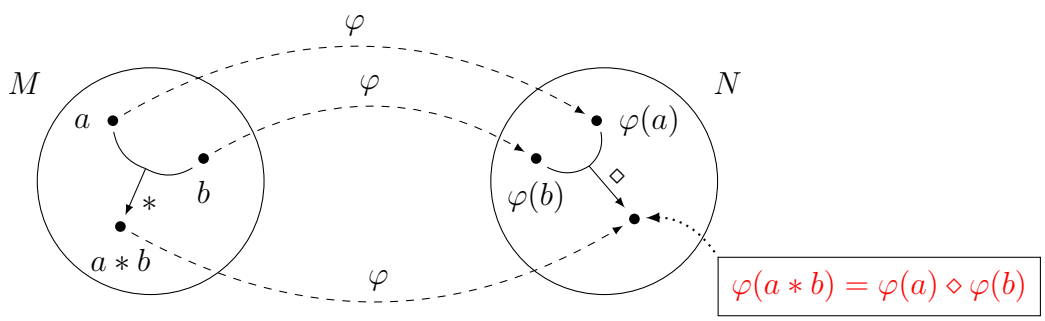
$$M \cong N. \qquad \square$$

Bemerkung 1.2.39.

i.) Bei einem Homomorphismus zwischen algebraischen Strukturen gilt also immer die Faustformel:

erst verknüpfen, dann abbilden $\overset{!!!}{\Longleftrightarrow}$ *erst abbilden, dann verknüpfen.*

Dies wird durch folgende Skizze veranschaulicht:



ii.) Die verschiedenen Bezeichnungen strukturerhaltender Abbildungen aus Definition 1.2.38 zwischen zwei Gruppen seien hier noch einmal tabellarisch aufgelistet:

$$\varphi\colon G \longrightarrow H$$

Abbildung:	*keine Anforderung.*
Homomorphismus:	*strukturerhaltend.*
Monomorphismus / Einbettung:	*strukturerhaltend und injektiv.*
Epimorphismus:	*strukturerhaltend und surjektiv.*
Isomorphismus:	*strukturerhaltend und bijektiv.*

$$\varphi\colon G \longrightarrow G$$

Abbildung:	*keine Anforderung.*
Endomorphismus:	*strukturerhaltend.*
Automorphismus:	*strukturerhaltend und bijektiv.* $\square$

Beispiel 1.2.40.

i.) Ist G eine Gruppe, so ist id_G offensichtlich ein Gruppenautomorphismus.

ii.) Die Zuordnungsvorschrift $f(x) := x^2$ ist auf den additiven Gruppen $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ wegen

$$f(1+1) = f(2) = 4 \neq 2 = 1 + 1 = f(1) + f(1)$$

kein Gruppenendomorphismus, aber auf den beiden multiplikativen Gruppen $\big(\mathbb{Q} \setminus \{0\}, \cdot\big)$ und $\big(\mathbb{R} \setminus \{0\}, \cdot\big)$ wegen

$$f(a \cdot b) = (a \cdot b)^2 = a^2 \cdot b^2 = f(a) \cdot f(b).$$

iii.) Die Exponentialabbildung $x \mapsto e^x$ ist wegen

$$e^{x+y} = e^x \cdot e^y \quad \text{und} \quad e^x > 0 \text{ für } x \in \mathbb{R}$$

ein Gruppenhomomorphismus von $(\mathbb{R}, +)$ nach $\big(\mathbb{R} \setminus \{0\}, \cdot\big)$.

iv.) *Ist $(G,*)$ eine Gruppe, so ist für ein $g \in G$ wegen $g^{i+j} = g^i * g^j$ (Potenzgesetz) folgende Abbildung ein Gruppenhomomorphismus von $(\mathbb{Z},+)$ nach $(G,*)$:*

$$\varphi_g \colon \mathbb{Z} \longrightarrow G \quad \textit{mit} \quad n \mapsto g^n.$$

v.) *Ist $(G,*)$ eine abelsche Gruppe, so ist folgende Abbildung wegen des Potenzgesetzes $(g_1 * g_2)^n = g_1^n * g_2^n$ für ein $n \in \mathbb{Z}$ eine Gruppenendomorphismus:*

$$\rho_n \colon G \longrightarrow G \quad \textit{mit} \quad g \mapsto g^n.$$

vi.) *Ist $(G,*)$ ein Gruppe, so ist für $g \in G$ die folgende Abbildung ein Gruppenautomorphismus (Übung!):*

$$\kappa_g \colon G \longrightarrow G \quad \textit{mit} \quad h \mapsto g * h * g^{-1}.$$

Diese Automorphismen (für verschiedene g) sind besonders interessant und tragen deshalb einen eigenen Namen: κ_g heißt die Konjugation mit g. Sind $x, y \in G$ und gibt es ein $g \in G$ mit $y = \kappa_g(x)$, so heißen x und y zueinander konjugiert. Auf der Gruppe G ist „konjugiert sein“ eine Äquivalenzrelation (Übung!):

$$x \sim y \quad := \quad \exists g \in G : y = \kappa_g(x).$$

Die Äquivalenzklassen dieser Relation heißen Konjugationsklassen von G und spielen bei der Analyse von Gruppen eine große Rolle.

vii.) *Es sei $f \colon M \longrightarrow N$ eine Bijektion zwischen nicht-leeren Mengen. Dann ist folgende Abbildung ein Gruppenisomorphismus (Übung!):*

$$\Phi \colon S(M) \longrightarrow S(N) \quad \textit{mit} \quad \sigma \mapsto f \circ \sigma \circ f^{-1}.$$

Daraus folgt insbesondere sofort für eine endliche Menge M mit $n := |M|$:

$$S(M) \cong S_n,$$

denn eine Aufzählung der Elemente von M liefert eine Bijektion zwischen M und der Menge $\{1,\dots,n\}$. Dabei hängt die Bijektion f von M nach $\{1,\dots,n\}$ von der Aufzählung ab, und die von f induzierte Abbildung von $S(M)$ nach S_n ebenfalls.

Damit gibt es vor allen Dingen bei einer endlichen Gruppe G immer einen Gruppenisomorphismus von $S(G)$ nach $S_{|G|}$, wobei dieser auch wieder von einer (willkürlichen) Aufzählung der Gruppenelemente von G abhängt (siehe dazu auch Aufgabenblatt 5, Aufgabe 3).

viii.) *Es sei $n \in \mathbb{N}$ und U_{n+1} die Untergruppe von S_{n+1} aus Lemma 1.2.36 (alle Permutationen aus S_{n+1}, die den Fixpunkt $n+1$ haben).*

Für ein $f \in S_n$ sei $\tilde{f} \in S_{n+1}$ diejenige Abbildung mit

$$\tilde{f}(i) = \begin{cases} f(i) & \textit{für } i \in \{1,\dots,n\}, \\ n+1 & i = n+1. \end{cases}$$

Dann ist folgende Abbildung ein injektiver Gruppenhomomorphismus:

$$\varphi \colon S_n \longrightarrow S_{n+1} \quad \textit{mit} \quad f \mapsto \tilde{f}.$$

Es gilt $\operatorname{im}(\varphi) = U_{n+1}$, und damit ist $S_n \cong U_{n+1}$ (Übung!)

Damit ist die Konstruktion aus Bemerkung 1.2.37 noch verbessert, denn dort wurde nur auf den Aspekt hingewiesen, daß die Zuordnung $f \mapsto \tilde{f}$ eine Bijektion von S_n auf U_{n+1} ist - tatsächlich ist sie sogar ein Gruppenisomorphismus.

In diesem Sinne wird S_n als Untergruppe von S_{n+1} betrachtet. Wird eine Permutation in Zykeldarstellung notiert und werden damit ihre Fixpunkte nur implizit beschrieben durch Auslassung, ist sowieso nicht zu entscheiden, aus welcher S_n z.B. die Transposition $(1\,2)$ stammt. □

Folgende Definition gibt speziellen Gruppenhomomorphismen einen eigenen Namen, da sie fundamental für die Gruppentheorie sind:

Definition 1.2.41. *Sei G eine Gruppe und M eine nicht-leere Menge. Falls ein Gruppenhomomorphismus*

$$\Psi\colon G \longrightarrow S(M)$$

existiert, so operiert G auf M vermöge/mittels/durch Ψ. □

Bemerkung 1.2.42.

i.) *Die Gruppentheorie entwickelte sich ursprünglich aus Betrachtungen von speziellen Objekten/Mengen und (speziellen) Permutationen dieser Menge: somit waren die ersten betrachteten Gruppen immer Untergruppen einer $S(M)$. Eine Gruppe war immer im Kontext mit einem Objekt, auf dem sie wirkte durch das Anwenden der Permutationen.*
Mittlerweile hat sich die Gruppentheorie als eigenständige Kategorie in der Mathematik etabliert, und Gruppen werden dabei zuersteinmal abstrakt und kontextlos als algebraische Strukturen mit speziellen Eigenschaften definiert. Aber durch die Operation einer Gruppe G auf einer Menge M wird ihr der ursprüngliche Wesenszug einer Gruppe zurückgegeben: auf einem Objekt (einer Menge) zu wirken! Denn über den Gruppenhomomorphismus $\Psi\colon G \longrightarrow S(M)$ kann ein Gruppenelement $g \in G$ via Ψ als Permutation von M aufgefaßt werden, da $\Psi(g)$ ja in $S(M)$ liegt.

ii.) *Ist eine nicht-leere Menge M gegeben, so operiert jede Untergruppe der Permutationsgruppe $S(M)$ offensichtlich auf M, denn für ein $U \subseteq S(M)$ ist folgende Abbildung ein Gruppenhomomorphismus:*

$$U \longrightarrow S(M) \quad \textit{mit} \quad u \mapsto u.$$

Ein wichtiges Beispiel dafür ist gegeben durch die folgende Konstruktion: Für ein $f \in S(M)$ operiert die von f erzeugte zyklische Untergruppe $\langle f \rangle \subseteq S(M)$ auf M, indem Potenzen von f auf M angewendet werden.

iii.) *Sei G eine Gruppe, die auf der nicht-leeren Menge M operiert via dem Gruppenhomomorphismus $\Psi\colon G \longrightarrow S(M)$. Auf M kann folgendermaßen eine Äquivalenzrelation definiert werden (Übung!):*

$$y \sim x \quad := \quad \exists g \in G : y = \Psi(g)(x).$$

Die Äquivalenzklasse eines $x \in M$ bzgl. dieser Relation wird als Orbit von x unter G bezeichnet, und M ist dann die disjunkte Vereinigung solcher Orbits.

iv.) *In Lemma 1.1.33 und in der anschließenden Diskussion wurde für eine nicht-leere Menge M eine Permutation $f \in S(M)$ analysiert. Die in Lemma 1.1.33 konstruierte Äquivalenzrelation läßt sich nun folgendermaßen interpretieren: Sie ist genau die oben beschriebene Äquivalenzrelation, die von der auf M operierenden Gruppe $\langle f \rangle \subseteq S(M)$ induziert wird, und die im Anschluß an Lemma 1.1.33 angehängte Analyse der Äquivalenzklassen beschreibt die Orbite dieser Operation.*

Im Falle einer Permutation $\sigma \in S_n$ wurde in Satz 1.1.34 eine Produktzerlegung $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$ in zyklische Permutationen mit disjunkten Trägern aus diesen Betrachtungen hergeleitet. Auch dies läßt sich nun in neuer Terminologie formulieren: die Träger der zyklischen Permutationen entsprechen genau den Orbiten der Länge ungleich Eins der Operation von $\langle \sigma \rangle \subseteq S_n$ auf der Menge $\{1, \ldots, n\}$.

v.) *In Aufgabenblatt 5 werden in Aufgabe 3 und Aufgabe 4 jeweils Operationen einer Gruppe G auf sich selbst eingeführt, via der Linksmultiplikation und der Konjugation:*

$$\Psi_G \colon G \longrightarrow S(G) \quad \textit{mit} \quad g \mapsto \ell_g,$$
$$\Phi_G \colon G \longrightarrow S(G) \quad \textit{mit} \quad g \mapsto \kappa_g.$$

ℓ_g ist dabei definiert in Definition 1.2.5, κ_g in Beispiel 1.2.40. Die in Beispiel 1.2.40 definierte Konjugationsklasse eines $x \in G$ ist nichts anderes als der Orbit von x unter der oben definierten Operation Φ_G. □

Es folgen noch einige weitere wesentliche Beispiele für Gruppenhomomorphismen, die auch im weiteren Verlauf der Vorlesung eine Rolle spielen:

Lemma 1.2.43. *Sei $(G, *)$ eine Gruppe und $N \subseteq G$ ein Normalteiler. Dann ist die kanonische Projektion von G auf die Quotientengruppe $(G/N, \circledast)$ (siehe Satz 1.2.29) ein Gruppenhomomorphismus:*

$$\pi_N \colon G \longrightarrow G/N \quad \textit{mit} \quad g \mapsto g * N.$$

Beweis. Die Linksnebenklassenrechnung ist genau so definiert:

$$\pi_N(g_1 * g_2) \overset{\text{(Def)}}{=} (g_1 * g_2) * N \overset{(1.2.29)}{=} (g_1 * N) \circledast (g_2 * N) \overset{\text{(Def)}}{=} \pi_N(g_1) \circledast \pi_N(g_2). \quad \square$$

Bemerkung 1.2.44. *In diesem Lemma (1.2.43) liegt der mathematische Grund, die Verknüpfung von Linksnebenklassen eines Normalteilers $N \subseteq G$ genau so zu definieren wie geschehen: nur wenn die Verknüpfung repräsentantenweise möglich ist, wird die kanonische Projektion von G auf G/N aus Lemma 1.2.43 zu einem Gruppenhomomorphismus! Und Homomorphismen stellen im algebraischen Sinne „Zusammenhang“ zwischen Objekten her. Siehe dazu auch die einleitende Diskussion zur Quotientengruppenkonstruktion auf Seite 54, wo die kommende Konstruktion als „die einzig sinnvolle“ bezeichnet wurde, aber dies noch nicht begründet werden konnte.* □

Für die symmetrischen Gruppen S_n ist folgender Gruppenhomomorphismus von Bedeutung:

Lemma 1.2.45. *Sei $n \in \mathbb{N}$. Dann ist die folgende Abbildung ein Gruppenhomomorphismus von S_n in die multiplikative Gruppe $\big(\{\pm 1\}, \cdot\big)$:*

$$\operatorname{sign} \colon S_n \longrightarrow \{\pm 1\} \quad \textit{mit} \quad \sigma \mapsto \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Dabei wird $\operatorname{sign}(\sigma)$ das Signum von σ genannt.

Beweis. Anhang A.3, Lemma A.3.2. □

Die Signum-Abbildung „sign“ aus Lemma 1.2.45 ist strenggenommen für jedes $n \in \mathbb{N}$ eine eigene Abbildung, da der Definitionsbereich S_n ja von n abhängt. Trotzdem taucht in ihrer Bezeichnung diese Unterscheidung nicht auf. Der Grund dafür ist folgender: Eine symmetrische Gruppe S_n kann kanonisch in eine andere symmetrische Gruppe S_m (mit $n \leq m$) eingebettet werden, indem ein $f \in S_n$ einfach genügend viele Fixpunkte hinzugefügt bekommt, so daß die resultierende Permutation $\tilde{f}$ dann in S_m liegt und sich auf der Teilmenge $\{1, \ldots, n\} \subseteq \{1, \ldots, m\}$ verhält wie f (siehe auch Beispiel 1.2.40). Dann kann gezeigt werden, daß $f \in S_n$ und $\tilde{f} \in S_m$ das gleiche Signum haben.
Ein weiterer Grund liegt im folgenden Lemma, nach dem das Signum einer Permutation an deren Zykeldarstellung abgelesen werden kann: und diese ist ja auch unabhängig von der konkreten S_n, aus der eine Permutation gewählt wurde:

Lemma 1.2.46. *Sei $\sigma \in S_n$ eine zyklische Permutation. Dann gilt:*

$$\sigma = (a_1\, a_2\, \ldots\, a_k) \quad \Longrightarrow \quad \operatorname{sign}(\sigma) = (-1)^{k-1}.$$

Daraus folgt insbesondere für eine beliebige Permutation $f \in S_n$ und eine Produktdarstellung $f = \sigma_1 \circ \cdots \circ \sigma_r$ mit zyklischen Permutationen $\sigma_1, \ldots, \sigma_r$ (mit nicht notwendigerweise disjunkten Trägern) durch die Homomorphismus-Eigenschaft von „sign“:

$$f = \underbrace{(a_{1,1}\, \ldots\, a_{1,k_1})}_{\text{Zykeldarst. } \sigma_1}\underbrace{(a_{2,1}\, \ldots\, a_{2,k_2})}_{\text{Zykeldarst. } \sigma_2}\cdots\underbrace{(a_{r,1}\, \ldots\, a_{r,k_r})}_{\text{Zykeldarst. } \sigma_r} \quad \Longrightarrow \quad \operatorname{sign}(f) = \prod_{i=1}^{r}(-1)^{k_i-1}.$$

Beweis. Anhang A.3, Lemma A.3.5. □

Bemerkung 1.2.47. *Der Gruppenhomomorphismus* $\operatorname{sign}\colon S_n \longrightarrow \{\pm 1\}$ *ist in Lemma 1.2.45 in dieser „Produktform“ eingeführt worden, da das Produkt ohne weitere Diskussion wohldefiniert ist - anschaulich ist es nicht. Auch ist nicht ohne weiteres klar, daß mit dieser Definition das Signum einer Permutation in der Menge $\{\pm 1\}$ liegt, und der Zusammenhang des Signums mit Zykeln aus Lemma 1.2.46 ist alles andere als evident.*
Es gibt die zur „Produktdefinition“ des Signums äquivalente Möglichkeit, das Signum einer Permutation σ mit Hilfe von Zykeln zu definieren: dazu muß aber ersteinmal folgendes erstaunliche Ergebnis hergeleitet werden:

> *Zerlegungen von $\sigma \in S_n$ in ein Produkt von 2-Zykeln (die nicht notwendigerweise disjunkte Träger haben müssen) enthalten entweder immer eine gerade Anzahl von Faktoren, oder immer eine ungerade Anzahl von Faktoren.* $(\star)$

Aus der Zykelzerlegung $(a_1\, a_2\, \ldots\, a_k) = (a_1\, a_2)(a_2\, \ldots\, a_k)$ folgt per vollständiger Induktion über Zykellängen sofort, daß jedes Zykel ein Produkt von 2-Zykeln ist, und daraus dann, daß jede Permutation eine Produktdarstellung aus 2-Zykeln hat, und es kann mit obigem Ergebnis $(\star)$ dann (wohl-)definiert werden:

$$\operatorname{sign}(\sigma) := (-1)^{\text{Anzahl von Faktoren in einer Produktzerlegung von } \sigma \text{ in 2-Zykel}}.$$

Aus dieser Definition lassen sich leicht alle relevanten Aussagen über die Signum-Abbildung ablesen.

Damit stellt sich die grundsätzliche Frage, wie das Signum von Permutationen definiert wird:

- *Kurz und knapp wie in Lemma 1.2.45, aber dann müssen die Eigenschaften mühsam herausgearbeitet werden, was hier in den Anhang verlagert ist.*
- *Mit Hilfe einer tieferen Analyse von Zykeldarstellungen in der S_n, aber dafür fallen alle wichtigen Eigenschaften sofort ab.*

Wird sich intensiv mit der S_n beschäftigt, ist sicher der zweite Weg der bessere. Eine schöne intensive Behandlung der S_n findet sich z.B. in dem Buch [**RSV**, Kapitel 7].

Nun wird betrachtet, wie sich die Strukturerhaltung von Abbildungen mit deren Verknüpfungen verträgt. Als erstes soll dabei die Komposition von Abbildungen untersucht werden:

Satz 1.2.48. *Seien $(G,*)$, $(H,\star)$ und $(K,\diamond)$ Gruppen mit Gruppenhomomrphismen:*

$$\varphi\colon G \longrightarrow H \qquad \text{und} \qquad \psi\colon H \longrightarrow K$$

Dann ist die Komposition $\psi\circ\varphi$ ein Gruppenhomomorphismus von G nach K. Insbesondere ist dann die Menge $\operatorname{End}(G)$ abgeschlossen unter der Komposition und $\big(\operatorname{End}(G),\circ\big)$ ein Untermonoid von $\big(\operatorname{Abb}(G,G),\circ\big)$ mit dem neutralen Element id_G.

Ist φ bijektiv, so ist auch die (mengentheoretische) Umkehrabbildung φ^{-1} ein Gruppenhomomorphismus. Insbesondere ist dann $\big(\operatorname{Aut}(G),\circ\big)$ eine Untergruppe des Monoides $\big(\operatorname{End}(G),\circ\big)$ und der Gruppe $\big(S(G),\circ\big)$.

Beweis.

$\psi\circ\varphi$ Gruppenhomomorphismus: Für $a,b\in G$ gilt:

$$\begin{aligned}(\psi\circ\varphi)(a*b) &= \psi\big(\varphi(a*b)\big) \overset{(\varphi\text{ GrHom})}{=} \psi\big(\varphi(a)\star\varphi(b)\big) \overset{(\psi\text{ GrHom})}{=} \psi\big(\varphi(a)\big)\diamond\psi\big(\varphi(b)\big)\\ &= (\psi\circ\varphi)(a)\diamond(\psi\circ\varphi)(b).\end{aligned}$$

Damit ist $\psi\circ\varphi$ strukturerhaltend und ein Gruppenhomomorphismus, und insbesondere $\operatorname{End}(G)$ abgeschlossen unter der Komposition von Abbildungen.
$\big(\operatorname{Abb}(G,G),\circ\big)$ ist nach Lemma 1.1.36 ein (nicht-kommutativer) Monoid mit dem neutralen Element id_G, und id_G ist ein Gruppenautomorphismus (Beispiel 1.2.40). Damit ist $\big(\operatorname{End}(G),\circ\big)$ eine Halbgruppe und wegen $\operatorname{id}_G\in\operatorname{End}(G)$ sogar ein Untermonoid von $\big(\operatorname{Abb}(G,G),\circ\big)$ mit dem neutralen Element id_G.

φ^{-1} Gruppenhomomorphismus: Sei nun φ bijektiv, und es seien $x,y\in H$. Es gibt dann wegen der Bijektivität von φ eindeutig bestimmte Elemente $a,b\in G$ mit

$$\varphi(a)=x \text{ und } \varphi(b)=y \quad\Longrightarrow\quad a=\varphi^{-1}(x) \text{ und } b=\varphi^{-1}(y),$$

und es folgt:

$$\varphi^{-1}(x\star y)=\varphi^{-1}\big(\varphi(a)\star\varphi(b)\big) \overset{(\varphi\text{ Hom})}{=} \varphi^{-1}\big(\varphi(a*b)\big) \overset{(\text{Umkehrabb})}{=} a*b=\varphi^{-1}(x)*\varphi^{-1}(y).$$

Damit ist auch φ^{-1} strukturerhaltend und ein Gruppenhomomorphismus.
Die Menge $\operatorname{Aut}(G)$ ist abgeschlossen unter der Komposition, da die Komposition von Gruppenhomomorphismen wieder einen Gruppenhomomorphismus liefert (siehe oben), und die Komposition bijektiver Abbildungen wieder bijketiv ist (Lemma 0.4.11). Da die Identität id_G in $\operatorname{Aut}(G)$ liegt, ist $\big(\operatorname{Aut}(G),\circ\big)$ sogar ein Monoid, und da für jedes $\varphi\in\operatorname{Aut}(G)$ eine Umkehrabbildung φ^{-1} existiert (Satz 0.4.15) und diese auch ein Gruppenhomomorphismus ist (siehe oben), hat

jedes Element aus $\mathrm{Aut}(G)$ ein Inverses bzgl. der Komposition und $\big(\mathrm{Aut}(G), \circ\big)$ ist eine Gruppe.
Offensichtlich gilt $\mathrm{Aut}(G) \subseteq \mathrm{End}(G)$ und $\mathrm{Aut}(G) \subseteq S(G)$. □

Sind $(G, \star)$ und $(H, *)$ Gruppen, so induziert die Gruppenstruktur auf H ja eine Gruppenstruktur auf $\big(\mathrm{Abb}(G, H), \circledast\big)$ (die Gruppenstruktur auf G spielt dafür überhaupt keine Rolle), wie in Satz 1.1.37 untersucht (und definiert). Die Frage ist, ob $\mathrm{Hom}(G, H) \subseteq \mathrm{Abb}(G, H)$ dann abgeschlossen ist unter der Verknüpfung „ $\circledast$ “, also für zwei Gruppenhomomorphismen $\psi, \varphi \in \mathrm{Hom}(G, H)$ auch $\varphi \circledast \psi$ ein Gruppenhomomorphismus aus $\mathrm{Hom}(G, H)$ ist. Dies wird im allgemeinen nur für eine abelsche Gruppe H funktionieren, wie ein Gegenbeispiel nach dem folgenden Satz zeigt:

Satz 1.2.49. *Sei $(G, \star)$ eine Gruppe und $(H, *)$ eine abelsche Gruppe. Weiter sei $\big(\mathrm{Abb}(G, H), \circledast\big)$ die in Satz 1.1.37 betrachtete abelsche Gruppe. Für zwei Gruppenhomomorphismen $\varphi, \psi \in \mathrm{Hom}(G, H)$ ist dann auch $\varphi \circledast \psi$ ein Gruppenhomomorphismus von G nach H, und die Teilmenge $\mathrm{Hom}(G, H) \subseteq \mathrm{Abb}(G, H)$ damit abgeschlossen bzgl. der Verknüpfung „ $\circledast$ “.*
Ist e_H das neutrale Element von H und dann nach Satz 1.1.37 die Abbildung

$$\varepsilon \colon G \longrightarrow H \quad \textit{mit} \quad g \mapsto e_H$$

das neutrale Element in $\big(\mathrm{Abb}(G, H), \circledast\big)$, so ist ε auch ein Gruppenhomomorphismus, d.h. $\varepsilon \in \mathrm{Hom}(G, H)$.
Für ein $\varphi \in \mathrm{Hom}(G, H) \subseteq \mathrm{Abb}(G, H)$ sei $\psi \in \mathrm{Abb}(G, H)$ die Inverse Abbildung bzgl. der Verknüpfung „ $\circledast$ “. Dann ist auch ψ ein Gruppenhomomorphismus von G nach H, d.h. $\psi \in \mathrm{Hom}(G, H)$.
Zusammenfassend gilt dann:
Ist $(H, *)$ eine abelsche Gruppe, so ist $\big(Hom(G, H), \circledast\big)$ ein abelsche Untergruppe von $\big(\mathrm{Abb}(G, H), \circledast\big)$.
Insbesondere ist dann für eine abelsche Gruppe $(G, *)$ wegen $\mathrm{End}(G) = \mathrm{Hom}(G, G)$ auch $\big(\mathrm{End}(G), \circledast\big)$ eine abelsche Gruppe.

Beweis.

$\varphi \circledast \psi$ Gruppenhomomorphismus: Nach der Definition von $\varphi \circledast \psi$ in Satz 1.1.37 gilt für ein $g \in G$:

$$(\varphi \circledast \psi)(g) := \varphi(g) * \psi(g).$$

Zu zeigen ist, daß diese Abbildung strukturerhaltend ist. Dazu sei für $a, b \in G$ betrachtet:

$$\begin{aligned}(\varphi \circledast \psi)(a \star b) = \varphi(a \star b) * \psi(a \star b) &\overset{(\varphi \text{ und } \psi \text{ GrHom})}{=} \big(\varphi(a) * \varphi(b)\big) * \big(\psi(a) * \psi(b)\big) \\ &\overset{(H \text{ abelsch})}{=} \big(\varphi(a) * \psi(a)\big) * \big(\varphi(b) * \psi(b)\big) = (\varphi \circledast \psi)(a) * (\varphi \circledast \psi)(b).\end{aligned}$$

Also ist $\varphi \circledast \psi$ auch ein Gruppenhomomorphismus und $\mathrm{Hom}(G, H)$ damit abgeschlossen unter der Verknüpfung „ $\circledast$ “, somit $\big(\mathrm{Hom}(G, H), \circledast\big)$ eine Halbgruppe.

ε Gruppenhomomorphismus: Offensichtlich gilt für alle $a, b \in G$:

$$\varepsilon(a \star b) = e_H = e_H * e_H = \varepsilon(a) * \varepsilon(b).$$

Damit liegt ε in $\mathrm{Hom}(G, H)$ und $\big(\mathrm{Hom}(G, H), \circledast\big)$ ist ein Monoid.

ψ Gruppenhomomorphismus: Nach der Definition aus Satz 1.1.37 gilt für ψ und $g \in G$:

$$\psi(g) := \big(\varphi(g)\big)^{-1}.$$

Zu zeigen ist nun, daß ψ auch strukturerhaltend ist. Dazu sei für $a, b \in G$ betrachtet:

$$\psi(a \star b) = \big(\varphi(a \star b)\big)^{-1} \overset{(\varphi \text{ GrHom})}{=} \big(\varphi(a) * \varphi(b)\big)^{-1} \overset{(\text{Lem } 1.1.25)}{=} \big(\varphi(b)\big)^{-1} * \big(\varphi(a)\big)^{-1}$$
$$\overset{(H \text{ abelsch})}{=} \big(\varphi(a)\big)^{-1} * \big(\varphi(b)\big)^{-1} = \psi(a) * \psi(b).$$

Da nun für jedes $\varphi \in \mathrm{Hom}(G, H)$ auch das Inverse bzgl. der Verknüpfung „ $\circledast$ “ in $\mathrm{Hom}(G, H)$ liegt, ist $\big(\mathrm{Hom}(G, H), \circledast\big)$ eine Gruppe.

Nach Satz 1.1.37 überträgt sich die Kommutativität der Verknüpfung „ $*$ “ auf die Verknüpfung „ $\circledast$ “, so daß $\big(\mathrm{Hom}(G, H), \circledast\big)$ sogar eine abelsche Gruppe ist. □

Bemerkung 1.2.50.

i.) Für die nicht-abelsche Gruppe S_3 sei die nicht-abelsche Gruppe $\big(\mathrm{Abb}(S_3, S_3), \circledast\big)$ aus Satz 1.1.37 betrachtet. In diesem Fall ist für $f, g \in S_3$ die Verknüpfung $f \circledast g$ definiert durch:

$$(f \circledast g)(\pi) := f(\pi) \circ g(\pi) \quad \textit{für} \quad \pi \in S_3.$$

Die Abbildung id_{S_3} ist offensichtlich in $\mathrm{Hom}(S_3, S_3)$, aber $\mathrm{id}_{S_3} \circledast \mathrm{id}_{S_3}$ liegt nicht darin, wie folgende Rechung zeigt, und $\mathrm{Hom}(S_3, S_3)$ ist damit nicht abgeschlossen unter der Verknüpfung „ $\circledast$ “:

$$(\mathrm{id}_{S_3} \circledast \mathrm{id}_{S_3})\big((1\,2)(2\,3)\big) = (\mathrm{id}_{S_3} \circledast \mathrm{id}_{S_3})\big((1\,2\,3)\big) = (1\,2\,3)(1\,2\,3) = (1\,3\,2)$$

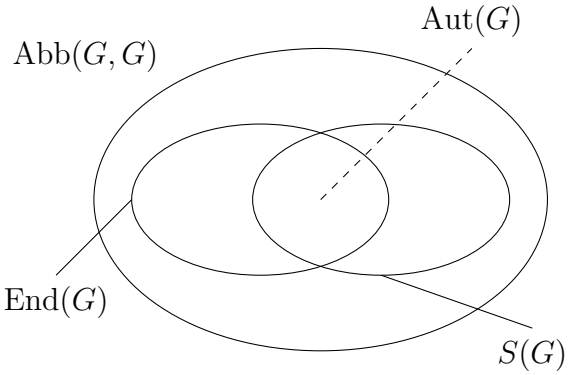
aber es gilt:

$$(\mathrm{id}_{S_3} \circledast \mathrm{id}_{S_3})\big((1\,2)\big) \circ (\mathrm{id}_{S_3} \circledast \mathrm{id}_{S_3})\big((2\,3)\big) = (1\,2)(1\,2)(2\,3)(2\,3) = \mathrm{id}\,. \qquad \square$$

ii.) Sei G eine Gruppe. Dann gilt offensichtlich

$$\mathrm{Aut}(G) = \mathrm{End}(G) \cap S(G),$$

und Satz 1.2.48 sowie Satz 1.2.49 liefern folgende Strukturaussagen:



$\big(\mathrm{Abb}(G, G), \circ\big)$: *Monoid*
$\big(S(G), \circ\big)$: *Gruppe*
$\big(\mathrm{End}(G), \circ\big)$: *Monoid*
$\big(\mathrm{Aut}(G), \circ\big)$: *Gruppe*

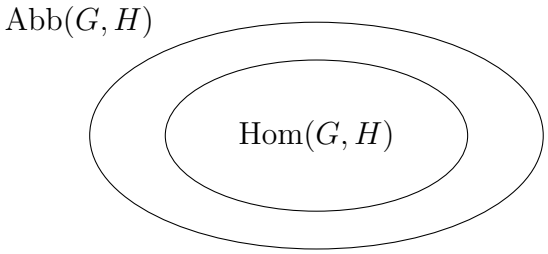
Falls $(G, *)$ zusätzlich abelsch:

$\big(\mathrm{End}(G), \circledast\big)$: *abelsche Gruppe*

iii.) Ist die Abbildung $f\colon M \longrightarrow N$ zwischen den beiden nicht-leeren Mengen M und N bijektiv, so gibt es eine Umkehrabbildung f^{-1} zu f (Satz 0.4.15).
Tragen die beiden Mengen M und N eine algebraische Struktur und ist f strukturerhaltend, so überträgt sich diese Eigenschaft auf ihre inverse Abbildung, wie Satz 1.2.48 zeigt, und f^{-1} ist auch strukturerhaltend (in diesem Satz ist die

Aussage zwar nur für Gruppenisomorphismen formuliert, aber sie gilt auch für andere algebraische Strukturen).
Besitzen die Mengen M und N eine topologische Struktur (siehe die Einleitung zu algebraischen Strukturen, Seite 25), und ist die Abbildung f topologisch strukturerhaltend, d.h. stetig, so muß die Umkehrabbildung f^{-1} nicht stetig sein!

iv.) Seien G und H Gruppen. Dann liefert Satz 1.2.49 folgende Strukturaussage:



Falls $(H, *)$ zusätzlich abelsch:

$\big(\mathrm{Abb}(G,H), \circledast\big)$: *abelsche Gruppe*

$\big(\mathrm{Hom}(G,H), \circledast\big)$: *abelsche Gruppe*

v.) Sei $(G, *)$ eine abelsche Gruppe. Dann ist für $n \in \mathbb{Z}$ nach Beispiel 1.2.40 die Abbildung $\rho_n \in \mathrm{Abb}(G,G)$ mit $g \mapsto g^n$ sogar ein Endomorphismus von G und damit $\rho_n \in \mathrm{End}(G)$. Des weiteren ist die folgende Zurordnung

$$\psi\colon \mathbb{Z} \longrightarrow \mathrm{End}(G) \quad \textit{mit} \quad n \mapsto \rho_n$$

ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $\big(\mathrm{End}(G), \circledast\big)$ (Übung!). □

Aus dem Strukturerhaltenden von Gruppenhomomorphismen folgen sofort einige nützliche Eigenschaften:

Lemma 1.2.51. *Seien $(G, *)$ und $(H, \diamond)$ Gruppen mit den neutralen Elementen e_G und e_H, und es sei $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gilt:*

$$\varphi(e_G) = e_H \qquad \textit{und} \qquad \varphi(g^{-1}) = \big(\varphi(g)\big)^{-1} \textit{ für } g \in G.$$

Insbesondere ist damit die Faser von $e_H \in H$ nicht leer, da sie immer e_G enthält.

Beweis.

$\varphi(e_G) = e_H$: Aus der Existenz des Inversen von $\varphi(e_G)$ in H folgt sofort durch Multiplikation mit $\varphi(e_G)^{-1}$ von links in folgender Gleichung:

$$\varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \diamond \varphi(e_G) \quad \overset{\varphi(e_G)^{-1}}{\Longrightarrow} \quad e_H = \varphi(e_G).$$

$\varphi(g^{-1}) = \big(\varphi(g)\big)^{-1}$: Aus der ersten Aussage folgt sofort die zweite Aussage, wenn in der folgenden Gleichung von links mit $\big(\varphi(g)\big)^{-1}$ multipliziert wird:

$$e_H = \varphi(e_G) = \varphi(g * g^{-1}) = \varphi(g) \diamond \varphi(g^{-1}) \quad \overset{\big(\varphi(g)\big)^{-1}}{\Longrightarrow} \quad \big(\varphi(g)\big)^{-1} = \varphi(g^{-1}). \qquad \square$$

Der wesentliche Begriff im Zusammenhang mit Homomorphismen ist ihr Kern:

Definition 1.2.52. *Seien $(G, *)$ und $(H, \diamond)$ Gruppen, e_H das neutrale Element von H und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann ist der Kern von φ definiert als die Faser von e_H (die nach Lemma 1.2.51 wegen $e_G \in \varphi^{-1}(e_H)$ nicht leer ist):*

$$\ker(\varphi) := \{\, g \in G \mid \varphi(g) = e_H \,\} = \varphi^{-1}(e_H). \qquad \square$$

Die Betrachtung des Kerns eines Gruppenhomomorphismus verrät sofort, ob er injektiv ist, und liefert somit ein nützliches Kriterium für den Test auf diese Eigenschaft:

LEMMA 1.2.53. *Seien $(G,*)$ und $(H,\diamond)$ Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann sind äquivalent:*

$$\varphi \text{ injektiv} \quad \Longleftrightarrow \quad \ker(\varphi) = \{e_G\}.$$

BEWEIS.

$\Longrightarrow$: Nach Lemma 1.2.51 ist $\varphi(e_G) = e_H$ und damit $e_G \in \ker(\varphi)$. Wegen der Injektivität von φ enthalten alle Fasern von φ höchstens ein Element und es folgt $\ker(\varphi) = \{e_G\}$.

$\Longleftarrow$: Seien $a, b \in G$ mit $\varphi(a) = \varphi(b)$. Es zu nun zu zeigen, daß daraus $a = b$ folgt:

$$\begin{aligned} \varphi(a) = \varphi(b) \quad &\Longrightarrow \quad \varphi(b)^{-1} \diamond \varphi(a) = e_H \quad \overset{(1.2.51)}{\Longrightarrow} \quad \varphi(b^{-1}) \diamond \varphi(a) = e_H \\ &\overset{(\varphi \text{ Hom})}{\Longrightarrow} \quad \varphi(b^{-1} * a) = e_H \quad \Longrightarrow \quad b^{-1} * a \in \ker(\varphi) = \{e_G\}. \end{aligned}$$

Also ist $b^{-1} * a = e_G$ und damit $a = b$. □

BEMERKUNG 1.2.54. *Eine Abbildung ist genau dann injektiv, wenn jede ihrer Fasern höchstens ein Element enthält (Bemerkung 0.4.8). Bei Gruppenhomomorphismen muß dazu nach Lemma 1.2.53 nur eine einzige Faser untersucht werden: die des neutralen Elementes des Wertebreiches.*
Anders ausgedrückt: bei einer „gewöhnlichen“ Abbildung muß bei einem Test auf Injektivität für jedes Element des Wertebereichs überprüft werden, wie oft es unter der Abbildung getroffen wird - bei einem Gruppenhomomorphismus nur ein einziges Element des Wertebereich, nämlich das neutrale Element.
Dies liefert folgende Anschauung: Bei einem Gruppenhomomorphismus ist die globale Eigenschaft, injektiv zu sein, schon lokal determiniert durch sein Verhalten bzgl. eines einzigen speziellen Elementes. □

Als nächstes wird gezeigt, daß der Kern eines Gruppenhomomorphismus nicht nur eine Menge ist, sondern sogar ein Normalteiler:

LEMMA 1.2.55. *Seien $(G,*)$ und $(H,\diamond)$ Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann ist $\ker(\varphi)$ ein Normalteiler in G, also insbesondere auch eine Untergruppe.*

BEWEIS.
Sei e_H das neutrale Element von H.
Zuerst wird mit dem Untergruppenkriterium (1.2.3) gezeigt, daß $\ker(\varphi)$ eine Untergruppe von G ist. Seien dazu $a, b \in \ker(\varphi)$. Zu zeigen ist dann nach dem Untergruppenkriterium $a * b^{-1} \in \ker(\varphi)$, was äquivalent ist zu $\varphi(a * b^{-1}) = e_H$:

$$\varphi(a * b^{-1}) = \varphi(a) \diamond \varphi(b^{-1}) \overset{(1.2.51)}{=} \varphi(a) \diamond \varphi(b)^{-1} \overset{(a,b \in \ker(\varphi))}{=} e_H \diamond e_H^{-1} = e_H.$$

Es bleibt zu zeigen, daß $\ker(\varphi)$ sogar ein Normalteiler ist, also für alle $a \in G$ gilt:

$$a * \ker(\varphi) * a^{-1} = \ker(\varphi).$$

Sei dazu $a \in G$ gewählt. Es wird wieder ausgenutzt, daß für $g \in G$ die Bedingung $g \in \ker(\varphi)$ äquivalent ist zu der Bedingung $\varphi(g) = e_H$.

$a * \ker(\varphi) * a^{-1} \subseteq \ker(\varphi)$: Für $x \in \ker(\varphi)$ ist $a * x * a^{-1} \in \ker(\varphi)$ zu zeigen:

$$\varphi(a * x * a^{-1}) = \varphi(a) \diamond \varphi(x) \diamond \varphi(a^{-1}) = \varphi(a) \diamond e_H \diamond \varphi(a)^{-1} = e_H.$$

$\ker(\varphi) \subseteq a * \ker(\varphi) * a^{-1}$: Für $x \in \ker(\varphi)$ liegt wegen obigem Argument auch $a^{-1} * x * a \in \ker(\varphi)$, und damit folgt wie gewünscht

$$x = a * \underbrace{(a^{-1} * x * a)}_{\in \ker(\varphi)} * a^{-1} \in a * \ker(\varphi) * a^{-1}. \qquad \square$$

Bemerkung 1.2.56.

i.) Ist $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus, so ist nach Lemma 1.2.55 sein Kern ein Normalteiler in G. Ist andersherum $N \subseteq G$ ein Normalteiler, so ist N nach Lemma 1.2.43 der Kern der kanonischen Projektion von G auf die Quotientengruppe G/N, so daß sich folgende wesentliche Beziehung zwischen Kernen von Gruppenhomomorphismen und Normalteilern ergibt:

Für eine Untergruppe $U \subseteq G$ ist äquivalent:

$$U \text{ ist ein Normalteiler} \iff U \text{ ist Kern eines Gruppenhomomorphismus.}$$

ii.) Lemma 1.2.55 liefert zusammen mit Lemma 1.2.43 auch eine Antwort auf die Frage, ob nur mit einem Normalteiler $U \subseteq G$ eine Quotientengruppenkonstruktion G/U mit repräsentantenweiser Verknüpfung der Linksnebenklassen von U möglich ist: Wenn die repräsentantenweise Verknüpfung der Linksnebenklassen einer Untergruppe U eine Gruppenstruktur auf G/U liefert, so ist nach Lemma 1.2.43 die kanonische Projektion auf G/U ein Gruppenhomomorphismus, und nach Lemma 1.2.55 sein Kern U dann ein Normalteiler (siehe dazu auch Bemerkung 1.2.30). $\square$

Und nun folgt ein zentraler Satz der Gruppentheorie:

Satz 1.2.57. *(Homomorphie-Satz für Gruppen Version I)*
Seien $(G, *)$ und $(H, \diamond)$ Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Weiter sei $N \subseteq G$ ein Normalteiler mit $N \subseteq \ker(\varphi)$, $(G/N, \circledast)$ die Quotientengruppe von G modulo N und $\pi_N\colon G \longrightarrow G/N$ die kanonische Projektion aus Lemma 1.2.43. Dann gibt es genau einen Gruppenhomomorphismus $\xi_N\colon G/N \longrightarrow H$, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi_N"'] & H \\ G/N \arrow[ur, "\xi_N"'] & \end{tikzcd} \qquad \text{mit} \quad \varphi = \xi_N \circ \pi_N.$$

Für den Homomorphismus ξ_N gelten dabei die folgenden Äquivalenzen:

$$\xi_N \text{ injektiv} \iff \ker(\varphi) = N \qquad \text{und} \qquad \xi_N \text{ surjektiv} \iff \varphi \text{ surjektiv.}$$

Beweis.
Sei e_H das neutrale Element von H.

Existenz von ξ_N: Es gibt wegen der Forderung $\varphi = \xi_N \circ \pi_N$ nur eine mögliche Abbildungsvorschrift für $\xi_N\colon G/N \longrightarrow H$, denn für $g * N$ muß gelten:

$$\xi_N(g * N) = \xi_N\big(\pi_N(g)\big) = \varphi(g).$$

Es ist zu zeigen, daß diese Abbildungsvorschrift $g * N \mapsto \varphi(g)$ unabhängig vom gewählten Repräsentanten einer Linksnebenklasse $g * N$ ist, also daß gilt:

$$g * N = \tilde{g} * N \quad \Longrightarrow \quad \xi_N(g * N) = \xi_N(\tilde{g} * N).$$

Dazu gilt mit Lemma 1.2.17 und $\xi_N(g * N) := \varphi(g)$:

$$\begin{aligned} g * N = \tilde{g} * N \quad &\overset{1.2.17}{\Longrightarrow} \quad \tilde{g}^{-1} * g \in N \subseteq \ker(\varphi) \quad \Longrightarrow \quad \varphi(\tilde{g}^{-1} * g) = e_H \\ &\Longrightarrow \quad \varphi(\tilde{g})^{-1} \diamond \varphi(g) = e_H \quad \Longrightarrow \quad \varphi(g) = \varphi(\tilde{g}). \end{aligned}$$

Nun muß noch gezeigt werden, daß die Abbildungsvorschrift $\xi_N(g*N) := \varphi(g)$ ein Gruppenhomomorphismus ist. Dies ergibt sich aber sofort aus der repräsentantenweisen Verknüpfung zweier Linksnebenklassen und der Strukturerhaltung von φ:

$$\begin{aligned} \xi_N\big((g_1 * N) \circledast (g_2 * N)\big) = \xi_N\big((g_1 * g_2) * N\big) &\overset{(\mathrm{Def})}{=} \varphi(g_1 * g_2) \\ \overset{(\varphi\ \mathrm{Hom})}{=} \varphi(g_1) \diamond \varphi(g_2) &\overset{(\mathrm{Def})}{=} \xi_N(g_1 * N) \diamond \xi_N(g_2 * N). \end{aligned}$$

Eindeutigkeit von ξ_N: Diese folgt, wie schon im Existenzbeweis gezeigt, aus der Forderung $\varphi = \xi_N \circ \pi_N$.

Äquivalenzaussagen: Die rechte Äquivalenz ergibt sich sofort aus der Definition der Abbildung ξ_N, denn es gilt offensichtlich $\mathrm{im}(\xi_N) = \mathrm{im}(\varphi)$ und damit:

$$\xi_N \text{ surjektiv} \quad \Longleftrightarrow \quad \varphi \text{ surjektiv}.$$

Zu der Aussage über die Injektivität von ξ_N: Aus der Definition von ξ_N folgt sofort:

$$\begin{aligned} g * N \in \ker(\xi_N) \quad &\Longleftrightarrow \quad \xi_N(g * N) = e_H \quad \Longleftrightarrow \quad (\xi_N \circ \pi_N)(g) = e_H \\ &\Longleftrightarrow \quad \varphi(g) = e_H \quad \Longleftrightarrow \quad g \in \ker(\varphi). \qquad (\star) \end{aligned}$$

Es gilt nach Lemma 1.2.53 die Äquivalenz

$$\xi_N \text{ injektiv} \quad \Longleftrightarrow \quad \ker(\xi_N) = \{N\},$$

so daß zum Beweis der Behauptung zu zeigen bleibt:

$$\ker(\xi_N) = \{N\} \quad \Longleftrightarrow \quad \ker(\varphi) = N.$$

$\Longrightarrow$: Die Inklusion $N \subseteq \ker(\varphi)$ ist nach Voraussetzung erfüllt, so daß nur die Inklusion $\ker(\varphi) \subseteq N$ bewiesen werden muß:

$$g \in \ker(\varphi) \quad \overset{(\star)}{\Longrightarrow} \quad g * N \in \ker(\xi_N) \overset{\ker(\xi_N)=\{N\}}{\Longrightarrow} g * N = N \overset{\text{Lem } 1.2.17}{\Longrightarrow} g \in N.$$

$\Longleftarrow$: Die Inklusion $\{N\} \subseteq \ker(\xi_N)$ ist gilt immer, da N das neutrale Element von G/N ist und damit im Kern des Gruppenhomomorphismus ξ_N (Lemma 1.2.51), so daß nur die Inklusion $\ker(\xi_N) \subseteq \{N\}$ zu zeigen ist:

$$g * N \in \ker(\xi_N) \quad \overset{(\star)}{\Longrightarrow} \quad g \in \ker(\varphi) \overset{\ker(\varphi)=N}{\Longrightarrow} g \in N \overset{\text{Lem } 1.2.17}{\Longrightarrow} g * N = N. \quad \square$$

Der Homomorphie-Satz (Version I) für Gruppen ist ein unverzichtbares Arbeitsmittel in der Gruppentheorie und taucht in vielen Beweisen und Konstruktionen auf. Hier werden nur einige wenige Folgerungen aus ihm hergeleitet, und für eine wesentliche davon ist vorher noch zu betrachten:

Lemma 1.2.58. *Seien $(G, *)$ und $(H, \diamond)$ Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann ist das Bild $\mathrm{im}(\varphi)$ von φ eine Untergruppe von H.*

Beweis. Seien $h_1, h_2 \in \operatorname{im}(\varphi)$ und $g_1, g_2 \in G$ mit $\varphi(g_i) = h_i$ für $i \in \{1, 2\}$. Nach dem Untergruppenkriterium 1.2.3 ist zu zeigen, daß dann $h_1 \diamond h_2^{-1} \in \operatorname{im}(\varphi)$ gilt:

$$h_1 \diamond h_2^{-1} = \varphi(g_1) \diamond \varphi(g_2)^{-1} = \varphi(g_1) \diamond \varphi(g_2^{-1}) = \varphi(g_1 * g_2^{-1}) \in \operatorname{im}(\varphi). \qquad \square$$

Nun kann mit Hilfe des Homomorphie-Satzes (Version I) für Gruppen die zentrale Beziehung zwischen einem Gruppenhomomorphismus und seinem Kern hergeleitet werden, die hier als Homomorphie-Satz Version II bezeichnet wird, da der Homomorphie-Satz (Version I) oft nur in dieser spezielleren Form formuliert wird:

Satz 1.2.59. *(Homomorphie-Satz für Gruppen Version II und Folgerungen)*
Seien $(G, *)$ und $(H, \diamond)$ Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann induziert φ genau einen Gruppenisomorphismus ξ, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi_{\ker(\varphi)}"'] & \operatorname{im}(\varphi) \\ G/\ker(\varphi) \arrow[ur, "\xi"'] & \end{tikzcd} \qquad \textit{mit} \quad \varphi = \xi \circ \pi_{\ker(\varphi)}.$$

Die Abbildung ξ hat damit die Form:

$$\xi\colon G/\ker(\varphi) \longrightarrow \operatorname{im}(\varphi) \subseteq H \quad \textit{mit} \quad g * \ker(\varphi) \mapsto \varphi(g).$$

Aus dieser Fassung des Homomorphie-Satzes folgt sofort für die Fasern von φ:

$$\varphi^{-1}(h) = \begin{cases} g * \ker(\varphi) & \textit{für } h \in \operatorname{im}(\varphi) \textit{ und } g \in G \textit{ mit } \varphi(g) = h, \\ \emptyset & \textit{für } h \notin \operatorname{im}(\varphi). \end{cases}$$

Insbesondere sind die nicht-trivialen Fasern von φ also allesamt Linksnebenklassen des Kerns von φ und damit alle gleichmächtig.
Der obige Isomorphismus ξ und der Satz von Lagrange (1.2.20) liefern dann sofort für eine endliche Gruppe G die nützlichen Aussagen:

$$G/\ker(\varphi) \cong \operatorname{im}(\varphi) \implies |G/\ker(\varphi)| = |\operatorname{im}(\varphi)| \overset{\textit{Lagrange}}{\implies} |G| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|.$$

Beweis.

Zum Isomorphismus ξ: $\ker(\varphi)$ ist nach Lemma 1.2.55 ein Normalteiler von G, und mit diesem liefert der Homomorphie-Satz Version I (1.2.57) ein kommutatives Diagramm

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi_{\ker(\varphi)}"'] & H \\ G/\ker(\varphi) \arrow[ur, "\xi_{\ker(\varphi)}"'] & \end{tikzcd} \qquad \text{mit} \quad \varphi = \xi_{\ker(\varphi)} \circ \pi_{\ker(\varphi)},$$

und $\xi_{\ker(\varphi)}$ ist offensichtlich sogar ein injektiver Gruppenhomomorphismus (setze $N := \ker(\varphi)$ im Homomorphie-Satz Version I, 1.2.57). Es gilt $\operatorname{im}(\xi_{\ker(\varphi)}) = \operatorname{im}(\varphi)$, und es sei

$$\xi\colon G/\ker(\varphi) \longrightarrow \operatorname{im}(\varphi) \quad \text{mit} \quad \xi\big(g * \ker(\varphi)\big) := \xi_{\ker(\varphi)}\big(g * \ker(\varphi)\big) = \varphi(g),$$

also derjenige Gruppenhomomorphismus, der aus $\xi_{\ker(\varphi)}$ durch die formale Einschränkung des Wertebereiches H auf $\operatorname{im}(\varphi)$ entsteht.

Dann ist ξ nicht nur wie $\xi_{\ker(\varphi)}$ injektiv, sondern erzwungenermaßen auch surjektiv und damit sogar ein Isomorphismus.

Die Fasern von φ: Die Aussage ist klar für $h \notin \operatorname{im}(\varphi)$.
Sei also $h \in \operatorname{im}(\varphi)$ und $g \in G$ mit $\varphi(g) = h$. Weiter sei e_H das neutrale Element von H. Zu zeigen ist $\varphi^{-1}(h) = g * \ker(\varphi)$.

$\varphi^{-1}(h) \subseteq g * \ker(\varphi)$: Für $x \in \varphi^{-1}(h)$ gilt $\varphi(x) = h = \varphi(g)$, und es folgt:

$$\begin{aligned} \varphi(x) = \varphi(g) \quad &\Longrightarrow \quad \varphi(g^{-1} * x) = e_H \quad &&\Longrightarrow \quad (g^{-1} * x) \in \ker(\varphi) \\ &\Longrightarrow \quad x * \ker(\varphi) = g * \ker(\varphi) \quad &&\Longrightarrow \quad x \in g * \ker(\varphi). \end{aligned}$$

$g * \ker(\varphi) \subseteq \varphi^{-1}(h)$: Für $x \in g * \ker(\varphi)$ gilt $x * \ker(\varphi) = g * \ker(\varphi)$, und mit $\varphi = \xi_{\ker(\varphi)} \circ \pi_{\ker(\varphi)}$ folgt:

$$\left.\begin{aligned} \varphi(x) &= \xi_{\ker(\varphi)}\big(\pi_{\ker(\varphi)}(x)\big) = \xi_{\ker(\varphi)}\big(x * \ker(\varphi)\big) \\ &= \xi_{\ker(\varphi)}\big(g * \ker(\varphi)\big) = \xi_{\ker(\varphi)}\big(\pi_{\ker(\varphi)}(g)\big) \\ &= \varphi(g) = h \end{aligned}\right\} \quad \Longrightarrow \quad x \in \varphi^{-1}(h).$$

$|G| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|$: Der Isomorphismus ξ von $G/\ker(\varphi)$ nach $\operatorname{im}(\varphi)$ ist insbesondere eine Bijektion und liefert die Mächtigkeitsaussage, auf die dann der Satz von Lagrange (1.2.20) mit $|G/\ker(\varphi)| = \frac{|G|}{|\ker(\varphi)|}$ angewendet werden kann. □

Bemerkung 1.2.60.

i.) Bei einer Abbildung zwischen zwei Mengen können Fasern unterschiedlicher Größe auftreten, auch gleichzeitig endliche und unendliche. Satz 1.2.59 zeigt, daß bei Gruppenhomomorphismen die nicht-trivialen Fasern als Linksnebenklassen des Kerns des Homomorphismus alle die gleiche Größe haben: nämlich die Mächtigkeit des Kerns. Auch sind die nicht-trivialen Fasern als Linksnebenklassen des Kerns alle systematisch aus diesem generierbar, wenn die Gruppe klein oder ein geeignetes Repräsentantensystem der Linksnebenklassen bekannt ist.
So sind z.B. für einen Gruppenhomomorphismus $\varphi\colon \mathbb{Z} \longrightarrow G$ in eine Gruppe G mit dem Kern $\langle n \rangle := \ker(\varphi) \subseteq \mathbb{Z}$ (Satz 1.2.12) seine nicht-trivialen Fasern gegeben durch die Linksnebenklassen $[0]_n, \ldots, [n-1]_n$.

ii.) Für einen Gruppenhomomorphismus $\varphi\colon G \longrightarrow H$ trägt die Menge der nicht-trivialen Fasern sogar selbst eine Gruppenstruktur, da der Kern des Homomorphismus ein Normalteiler ist und damit seine Linksnebenklassen (welche die nicht-trivialen Fasern sind) bei repräsentantenweiser Verknüpfung eine Gruppe bilden.

iii.) Ist $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus, so liefert dieser drei wichtige (Unter-)Gruppen: den Definitionsbereich G, seinen Kern, den Normalteiler $\ker(\varphi) \subseteq G$, und sein Bild $\operatorname{im}(\varphi) \subseteq H$. Mit dem Isomorphismus

$$G/\ker(\varphi) \;\cong\; \operatorname{im}(\varphi)$$

lassen sich evt. bei genauer Kenntnis von zweien dieser Gruppen Informationen über die dritte Gruppe herleiten.

Mit Hilfe des Homomorphie-Satzes Version II (1.2.59) lassen sich nun alle zyklischen Gruppen (bis auf Isomorphie) beschreiben und klassifizieren:

Satz 1.2.61. *(Klassifikation der zyklischen Gruppen)*
Sei $(G, *)$ eine zyklische Gruppe. Dann gilt:

$$\begin{aligned} G \text{ unendliche zyklische Gruppe} \quad &\Longrightarrow \quad G \cong \mathbb{Z}, \\ G \text{ endliche zyklische Gruppe} \quad &\Longrightarrow \quad G \cong \mathbb{Z}_n \text{ mit } n := |G|. \end{aligned}$$

Und die Gruppen $\mathbb{Z}$ und $\mathbb{Z}_n$ mit $n \in \mathbb{N}$ sind offensichtlich alle paarweise nicht-isomorph zueinander, da sie alle verschiendene Ordnungen haben.

Beweis.
Ist G eine zyklische Gruppe, so existiert ein $g \in G$ mit

$$G = \langle\, g \,\rangle = \{\, g^i \mid i \in \mathbb{Z} \,\}.$$

Es sei folgende Abbildung von der Gruppe $(\mathbb{Z}, +)$ nach G betrachtet:

$$\varphi_g \colon \mathbb{Z} \longrightarrow G \quad \text{mit} \quad i \mapsto g^i.$$

Die Abbildung φ ist offensichtlich surjektiv, d.h. $\operatorname{im}(\varphi) = G$, und sie ist wegen des Potenzgesetzes $g^{i+j} = g^i * g^j$ auch ein Gruppenhomomorphismus (siehe auch Beispiel 1.2.40):

$$\varphi_g(i + j) = g^{i+j} = g^i * g^j = \varphi_g(i) * \varphi_g(j).$$

Dann liefert der Homomorphie-Satz Version II sofort die folgenden Aussagen:

$$\mathbb{Z}/\ker(\varphi) \cong \operatorname{im}(\varphi) = G \quad \Longrightarrow \quad |\mathbb{Z}/\ker(\varphi)| = |G|.$$

$\ker(\varphi)$ ist eine Untergruppe von $\mathbb{Z}$ und nach Satz 1.2.12 dann entweder $\{0\}$ oder $\langle\, n \,\rangle$ für ein $n \in \mathbb{N}$. Dann gibt es zwei Fälle zu unterscheiden:

- Im Falle $\ker(\varphi_g) = \{0\}$ ist φ_g nach Lemma 1.2.53 injektiv, also ingesamt bijektiv und damit ein Gruppenisomorphismus von $\mathbb{Z}$ nach G, d.h. $G \cong \mathbb{Z}$.
- Im Falle $\ker(\varphi_g) = \langle\, n \,\rangle$ mit $n \in \mathbb{N}$ ist G isomorph zu $\mathbb{Z}_n$ mit der Ordnung $|\mathbb{Z}_n| = n$ (siehe Satz 1.2.33 und Definition 1.2.34).

Aus diesen beiden Fällen folgen sofort die behaupteten Implikationen. □

Bemerkung 1.2.62.

i.) Die Klassifikation der zyklischen Gruppen ist eine Klassifikation „bis auf Isomorphie“. Sind zwei Gruppen G und H isomorph, so gibt es eine bijektive strukturverträgliche Abbildung φ von G nach H, so daß beide Mengen Eins-zu-Eins aufeinander abgebildet werden. Die Abbildung φ besitzt auf Grund ihrer Bijektivität eine Umkehrabbildung φ^{-1}, die nach Satz 1.2.48 auch strukturverträglich ist. So kann zwischen beiden Mengen strukturverträglich Hin und Her gewechselt werden, und im algebraischen Sinne sind sie völlig gleichwertig: ist G oder H bekannt, so können Eigenschaften und Ergebnisse ohne Informationsverlust aus der einen Struktur zur anderen geschoben werden.
Ein Beispiel dazu sind die folgenden beiden Gruppen:

$$\begin{aligned} \langle\, (1\,2\,3) \,\rangle &= \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\} \subseteq S_3, \\ \mathbb{Z}_3 &= \{[0]_3, [1]_3, [2]_3\}. \end{aligned}$$

Die Elemente der beiden Gruppen sind als Objekte völlig verschieden: einmal sind es Permutationen der Menge $\{1, 2, 3\}$, und einmal Linksnebenklassen der

Untergruppe $\langle\, 3\,\rangle \subseteq \mathbb{Z}$, *also unendlich große Teilmengen von* $\mathbb{Z}$. *Aber mit folgender Zuordnung wird ein Gruppenisomorphismus definiert:*

$$\mathrm{id} \mapsto [0]_3, \quad (1\,2\,3) \mapsto [1]_3, \quad (1\,3\,2) \mapsto [2]_3,$$

und somit sind beide Gruppen strukturell identisch, was sich auch zeigt, wenn die beiden Gruppentafeln miteinander verglichen werden:

$\circ$	id	$(1\,2\,3)$	$(1\,3\,2)$
id	id	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	id
$(1\,3\,2)$	$(1\,3\,2)$	id	$(1\,2\,3)$

und

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

.

Damit unterscheiden sich die beiden Gruppen im algebraischen Sinne nicht und werden als „algebraisch gleich“, d.h. isomorph bezeichnet.

ii.) *Die Klassifikation der zyklischen Gruppen läßt sich also auch so lesen:*

> *Im Sinne algebraischer Gleichheit (Isomorphie) gibt es nur die verschiedenen zyklischen Gruppen* $\mathbb{Z}$ *und* $\mathbb{Z}_n$ *für* $n \in \mathbb{N}$.

iii.) *Nach Satz 1.2.22 sind alle Gruppen mit Primzahlordnung zyklisch, so daß sich für* $n \in \mathbb{N}$ *sofort folgende Aussage ergibt:*

$$n \text{ Primzahl} \quad \Longrightarrow \quad \begin{array}{l}\text{Es gibt bis auf Isomorphie nur eine Gruppe}\\ \text{der Ordnung } n\text{, und zwar } \mathbb{Z}_n.\end{array}$$

iv.) *Es stellt sich natürlich sofort die Frage, ob sich die vorherige Aussage umdrehen läßt: Muß* n *eine Primzahl sein, wenn es bis auf Isomorphie nur eine Gruppe der Ordnung* n *gibt? Die Antwort darauf ist nein, denn z.B.* $n = 15$ *erfüllt die Bedingung, daß es bis auf Isomorphie nur eine Gruppe der Ordnung* 15 *gibt, aber* 15 *ist keine Primzahl.*
Aber es existiert folgende Aussage: Für $n \in \mathbb{N}$ *sind äquivalent:*

$$\mathrm{ggT}\,\big(n, \varphi(n)\big) = 1 \quad \Longleftrightarrow \quad \begin{array}{l}\text{Es gibt bis auf Isomorphie nur eine Gruppe}\\ \text{der Ordnung } n\text{, und zwar } \mathbb{Z}_n.\end{array}$$

Dabei bezeichnet $\mathrm{ggT}(a,b)$ *den „größten gemeinsamen Teiler“ von* a *und* b, *und* $\mathrm{ggT}(a,b) = 1$ *ist dann gleichbedeutent damit, daß* a *und* b *teilerfremd sind.*
$\varphi(n)$ *ist die Eulersche* φ*-Funktion, und kann berechnet werden, wenn die Primfaktorzerlegung von* n *bekannt ist:*

$$n = \prod_{i=1}^{k} p_i^{r_i} \ \text{ Primfaktorzerlegung} \quad \Longrightarrow \quad \varphi(n) = \prod_{i=1}^{k} (p_i - 1) \cdot p_i^{r_i - 1}.$$

Mit Hilfe der Primfaktorzerlegung $\prod_{i=1}^{k} p_i^{r_i}$ *von* n *läßt sich auch die Bedingung* $\mathrm{ggT}\,\big(n, \varphi(n)\big) = 1$ *für* $n > 2$ *äquivalent umformulieren zu:*

$$\mathrm{ggT}\,\big(n, \varphi(n)\big) = 1 \quad \Longleftrightarrow \quad \begin{cases} n \text{ ist ungerade,} \\ r_i = 1 \text{ für } 1 \le i \le k, \\ p_i \text{ teilt nicht } (p_j - 1) \text{ für } 1 \le i, j \le k. \end{cases}$$

Jede Primzahl größer als Zwei erfüllt die drei Bedingungen, und die beiden ersten Nicht-Primzahlen, die diese Bedingung erfüllen, sind $15 = 3 \cdot 5$ *und* $33 = 3 \cdot 11$. *(Mehr zu dieser Aussage kann im Internet unter dem Stichwort „cyclicity-forcing numbers“ gefunden werden.)*

v.) Folgende Tabelle gibt einen Überblick über die Gruppen bis zur Ordnung 10*, d.h. jede Gruppe mit höchstens* 10 *Elementen ist isomorph zu einer der folgenden Gruppen:*

Ordnung	*Anzahl Typen*	*Gruppen-Typ*
1	1	$(\{0\},+)$
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_4$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6,\ S_3$
7	1	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_8,\ D_4,\ Q_8$
9	2	$\mathbb{Z}_3 \times \mathbb{Z}_3,\ \mathbb{Z}_9$
10	2	$\mathbb{Z}_{10},\ D_5$

Die nicht-abelschen Gruppen in dieser Liste sind S_3, D_4, Q_8, D_5. Die Gruppe Q_8 ist die sogenannte „Quaternionengruppe“, D_4, D_5 sind Diedergruppen (siehe Aufgabenblatt 4 und Aufgabenblatt 5).
Übung: Zu welcher Gruppe der Tabelle ist die Kleinsche Vierergruppe aus Aufgabenblatt 3 isomorph? □

1.3. Ringe und Körper

In den letzten Abschnitten wurden algebraische Strukturen bestehend aus einer Menge zusammen mit einer inneren Verknüpfung betrachtet. Nun wird dieses Konzept erweitert zu Strukturen, die aus einer Menge zusammen mit zwei inneren Verknüpfungen konstruiert sind, die beide miteinander via Distributivgesetzen „harmonieren“ müssen:

Definition 1.3.1. *Sei R eine nicht-leere Menge, und seien „$*$“ und „$\diamond$“ innere Verknüpfungen auf R. Dann heißt $(R, *, \diamond)$ Ring, falls gilt:*

i.) $(R, *)$ ist eine abelsche Gruppe.
ii.) $(R, \diamond)$ ist eine Halbgruppe.
iii.) Es gelten die beiden Distributivgesetze für alle $a, b, c \in R$:

$$D1: \quad a \diamond (b * c) = (a \diamond b) * (a \diamond c).$$
$$D2: \quad (b * c) \diamond a = (b \diamond a) * (c \diamond a).$$

Die Verknüpfung der Gruppenstruktur auf R wird im allgemeinen als Addition bezeichnet und meist mit mit dem Symbol „$+$“ statt „$*$“ geschrieben, falls nicht schon ein gesondert eingeführtes Symbol als Verknüpfung benutzt werden soll. Das neutrale Element der Gruppenstruktur heißt Null, und wird bei Verwendung des Verknüpfungssymbols „$+$“ mit „0“ notiert (evt. der Deutlichkeit halber auch mit O_R).
Die Verknüpfung der Halbgruppenstruktur auf R wird im allgemeinen als Multiplikation bezeichnet und meist mit dem Symbol „$\cdot$“ statt „$\diamond$“ geschrieben, falls nicht schon ein gesondert eingeführtes Symbol als Verknüpfung benutzt werden soll.
Besitzt R bzgl. seiner Multiplikation ein neutrales Element ungleich der Null (damit ist die Halbgruppenstruktur sogar eine Monoidstruktur), so wird es als Eins des Ringes bezeichnet und bei der Verwendung des Verknüpfungssymbols „$\cdot$“ mit „1“ notiert (evt. der Deutlichkeit halber auch mit 1_R). Der Ring heißt dann auch Ring mit Eins.

Ist die Multiplikation des Ringes kommutativ, so wird R als kommutativer Ring bezeichnet (die Addition ist nach Voraussetzung immer kommutativ).
Wird die übliche Notation $(R, +, \cdot)$ für den Ring verwendet, also die beiden Verknüpfungssymbole „$+$“ und „$\cdot$“, so sind folgende Konventionen üblich:

- *Es gilt die „Punkt-vor-Strich-Regelung“, d.h. bei Termen mit mehreren Verknüpfungen bindet „$\cdot$“ stärker als „$+$“ (damit können oft Klammern gespart werden).*
- *Das Verknüpfungssymbol „$\cdot$“ kann weggelassen werden, wenn der Zusammenhang klar ist.*

Diese Konventionen bedeuten anschaulich:

$$ab + ac := (a \cdot b) + (a \cdot c).$$

Die Distributivgesetze lauten in diesem Fall dann:

$$D1: \quad a(b+c) = ab + ac \qquad \text{und} \qquad D2: \quad (b+c)a = ba + ca.$$

Wird R als Ring bezeichnet ohne explizite Angabe von Verknüpfungssymbolen, so ist damit $(R, +, \cdot)$ gemeint. □

Bemerkung 1.3.2.

i.) *In den letzten Abschnitten wurden bei der Betrachtung von algebraischen Strukturen immer explizit Verknüpfungssymbole angegeben, und wenn mehrere verschiedene Strukturen in einem Kontext vorkamen, diese auch durch verschiedene Symbole bezeichnet. Da vorher immer pro algebraischer Struktur nur eine Verknüpfung relevant war, konnte dies mit einem überschaubaren Symbolvorat erreicht werden.*
Bei Ringen sind nun pro Struktur schon zwei Verknüpfungen vorhanden, bei zwei Ringen dann insgesamt vier, und wenn dann noch die Abbildungsmengen zwischen Ringen zu Ringen gemacht werden, wird es unübersichtlich. Daher wird ab diesem Abschnitt die in der Literatur übliche Form gewählt, durchaus mit dem gleichen Symbol in verschiedenen Strukturen unterschiedliche Verknüpfungen zu beschreiben. Das verlangt dann vom Leser, sich immer genau bewußt zu sein, in welchem Kontext ein Symbol auftritt, und was eigentlich damit gemeint ist.
Wird in Zukunft zum Beispiel von zwei Ringen R und S gesprochen, so sind damit implizit Ringe $(R, +, \cdot)$ und $(S, +, \cdot)$ gemeint, deren Verknüpfungen aber trotz gleicher Schreibweise völlig andere Bedeutung haben können, so daß eine ausführliche Notation eigentlich von Ringen $(R, *, \diamond)$ und $(S, \star, \bullet)$ reden sollte.

ii.) *Ist $(R, +, \cdot)$ ein Ring mit Eins, so gilt nach den Notationsregeln in Definition 1.3.1 und der Festlegung, daß die Eins ungleich der Null sein muß, immer $0 \neq 1$.*

iii.) *In einem Ring ist die Null und zu jedem Element a sein additives Inverses $-a$ eindeutig bestimmt (Lemma 1.1.12 und Lemma 1.1.17).*

iv.) *In einem Ring mit Eins (multiplikativer Monoid) ist die Eins eindeutig bestimmt (Lemma 1.1.12), und falls ein Element a ein multiplikatives Inverses a^{-1} hat, dieses ebenfalls (Lemma 1.1.17).* □

Beispiel 1.3.3.

i.) *$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind kommutative Ringe mit Eins, und deren Null- und Einselement sind jeweils die Zahlen 0 und 1.*

Werden im folgenden diese Zahlenmengen als Ringe referenziert, so sind immer diese beiden Standardverknüpfungen auf ihnen gemeint.

ii.) *Sei* $(G,+)$ *eine abelsche Gruppe. Dann ist* $\big(\mathrm{End}(G),\oplus,\circ\big)$ *ein Ring mit dem Einselement* id_G*. Dies folgt aus Satz 1.2.48, Satz 1.2.49 und Bemerkung 1.2.50, denn danach ist* $\big(\mathrm{End}(G),\oplus\big)$ *eine abelsche Gruppe und* $\big(\mathrm{End}(G),\circ\big)$ *ein Monoid - und die Distributivgesetze*

$$D1:\ \varphi\circ(\psi\oplus\xi)=(\varphi\circ\psi)\oplus(\varphi\circ\xi)\qquad \textit{und}\qquad D2:\ (\psi\oplus\xi)\circ\varphi=(\psi\circ\varphi)\oplus(\xi\circ\varphi)$$

lassen sich leicht auf den Elementen von G *nachrechnen:*

$$\begin{aligned}
D1:\quad \big(\varphi\circ(\psi\oplus\xi)\big)(g)&=\varphi\big(\psi(g)+\xi(g)\big)\overset{(\varphi\ \textit{Hom!})}{=}\varphi\big(\psi(g)\big)+\varphi\big(\xi(g)\big)\\
&=(\varphi\circ\psi)(g)+(\varphi\circ\xi)(g),\\
D2:\quad \big((\psi\oplus\xi)\circ\varphi\big)(g)&=(\psi\oplus\xi)\big(\varphi(g)\big)=\psi\big(\varphi(g)\big)+\xi\big(\varphi(g)\big)\\
&=(\psi\circ\varphi)(g)+(\xi\circ\varphi)(g).
\end{aligned}$$

Bei der Überprüfung des Distributivgesetzes D1 *ist die Homomorphie-Eigenschaft von* φ *wichtig - somit ist* $\big(\mathrm{Abb}(G,G),\oplus,\circ\big)$ *im allgemeinen kein Ring! Hier sind die beiden Verknüpfungssymbole im Ring explizit angegeben: „* $\oplus$ *“ um anzudeuten, daß die Verknüpfung zwischen Endomorphismen von der Verknüpfung „* $+$ *“ aus dem Wertebereich* G *induziert ist, und „* $\circ$ *“, weil so üblicherweise die Komposition von Abbildungen notiert wird, die in dieser Ringstruktur der Multiplikation entspricht. In der Literatur wird meist anstelle von „* $\oplus$ *“ einfach nur „* $+$ *“ geschrieben, und teilweise für „* $\circ$ *“ auch „* $\cdot$ *“. Daraus ergibt sich dann z.B. eine Formel*

$$(\psi+\tau)(r+s)=\psi(r+s)+\tau(r+s),$$

die in ausführlicher Schreibweise so aussähe:

$$(\psi\oplus\tau)(r+s)\overset{(\star)}{=}\psi(r+s)+\tau(r+s).$$

Bei der ausführlichen Fassung ist sofort klar, daß bei der Gleichung $(\star)$ *die Verknüpfung zwischen Abbildungen zurückgeführt wird auf die Verknüpfung der Bilder im Wertebereich. Dies läßt sich auch aus der ersten Fassung herauslesen, aber es muß einem schon bewußt sein, daß auf den verschiedenen Strukturebenen* G *und* $\mathrm{End}(G)$ *addiert wird.*

iii.) *Das vorherige Beispiel für den Endomorphismenring einer abelschen Gruppe kann nun auf jeden Ring* $(R,+,\cdot)$ *angewendet werden:* $(R,+)$ *ist per Definition eine abelsche Gruppe, und so bilden deren Endomorphismen den Edomorphismenring* $\big(\mathrm{End}(R),\oplus,\circ\big)$*.*

iv.) *Sei* $(R,+,\cdot)$ *ein Ring und* I *eine nicht-leere Menge. Auf* $R^I=\mathrm{Abb}(I,R)$ *sind dann wie in Satz 1.1.37 folgende Verknüpfungen für* $f,g\in R^I$ *über die Verknüpfungen auf* R *defniert:*

$$\begin{aligned}
f\oplus g:&\quad x\mapsto f(x)+g(x).\\
f\odot g:&\quad x\mapsto f(x)\cdot g(x).
\end{aligned}$$

$(R,+)$ *ist eine abelsche Gruppe, und dies überträgt sich nach Satz 1.1.37 auf* $(R^I,\oplus)$*. Weiter ist* $(R,\cdot)$ *ein Halbgruppe, und dieses überträgt sich dann auf* $(R^I,\odot)$*. Die Distributivgesetze für* $(R^I,\oplus,\odot)$ *folgen direkt aus den Distributivgesetzen für* R *(Übung!), und so ist* $(R^I,\oplus,\odot)$ *ebenfalls ein Ring.*

Besitzt der Ring R eine Eins, so gilt dies auch für R^I, und ist R ein kommutativer Ring, dann ebenso R^I (dies alles folgt aus Satz 1.1.37).
In $(R^I, \oplus, \odot)$ haben die Null „$\bar{0}$“ und eine evt. existierende Eins „$\bar{1}$“ als Abbildungen von I nach R folgende Form (0_R die Null in R und 1_R die Eins in R - falls existent):

$$\bar{0}\colon x \mapsto 0_R \qquad \text{und} \qquad \bar{1}\colon x \mapsto 1_R.$$

v.) *Sei $(R, +, \cdot)$ ein Ring und I eine nicht-leere Menge. Wird die kanonische Identifikation des R^I mit dem kartesischen Produkt $\prod_{i\in I} R$ vorgenommen wie zwischen Satz 1.1.37 und Satz 1.1.39 diskutiert, so ergibt sich aus der Übertragung obiger Betrachtungen von R^I auf $\prod_{i\in I} R$ eine Ringstruktur, indem dort I-Tupel des kartesischen Produktes komponentenweise (und pro Komponente dann in R) verknüpft werden:*

$$(x_i)_{i\in I} \oplus (y_i)_{i\in I} := (x_i + y_i)_{i\in I} \qquad \text{und} \qquad (x_i)_{i\in I} \odot (y_i)_{i\in I} := (x_i \cdot y_i)_{i\in I}.$$

Die Null in $\prod_{i\in I} R$ hat dann die Form $(0_R)_{i\in I}$, und besitzt R eine Eins, so ist $(1_R)_{i\in I}$ eine Eins in $\prod_{i\in I} R$.
Ist R ein kommutativer Ring, so überträgt sich dies wegen der komponentenweisen Rechnung mit den I-Tupeln natürlich auf den Ring $\prod_{i\in I} R$.
Alle diese Aussagen gelten insbesondere für den Spezialfall $I := \{1, \ldots, n\}$, wo das kartesische Produkt R^n aus n-Tupeln mit Einträgen aus R besteht. Die Null in R^n ist das n-Tupel $(0_R, \ldots, 0_R)$, die Eins das n-Tupel $(1_R, \ldots, 1_R)$.

vi.) *Sei I eine nicht-leere Indexmenge, und es seien $(R_i, *_i, \diamond_i)$ Ringe. Dann ist auch das kartesische Produkt $\prod_{i\in I} R_i$ bei komponentenweiser Verknüpfung ein Ring (siehe den Spezialfall $R_i := R$ im vorherigen Beispiel). Haben alle Ringe R_i eine Eins, so auch $\prod_{i\in I} R_i$, und sind alle Ringe R_i kommutativ, so auch $\prod_{i\in I} R_i$.*

vii.) *Sei M eine nicht-leere Menge und $\mathcal{P}(M)$ ihre Potenzmenge. Auf $\mathcal{P}(M)$ sei für $A, B \in \mathcal{P}(M)$ die symmetrische Differenz definiert durch:*

$$A \ominus B := (A \cup B) \setminus (A \cap B).$$

$\big(\mathcal{P}(M), \ominus\big)$ ist eine abelsche Gruppe mit den neutralen Element $\emptyset$, in der jedes Element zu sich selbst invers ist: $A \ominus A = \emptyset$ für alle $A \in \mathcal{P}(M)$ (siehe Aufgabenblatt 3, Aufgabe 4).
Wird als zweite innere Verknüpfung auf $\mathcal{P}(M)$ der Schnitt von Teilmengen hinzugenommen, so ist $\big(\mathcal{P}(M), \ominus, \cap\big)$ sogar ein kommutativer Ring mit dem Einselement „M“. (Übung!) □

Als erstes sollen einige Rechengesetze in Ringen hergeleitet werden, die aus den Distributivgesetzen folgen, die eine Beziehung zwischen der additiven Verknüpfung und der multiplikativen Verknüpfung in Ringen herstellten.

Lemma 1.3.4. *Sei R ein Ring. Dann gilt für das neutrale Element 0 der Addition:*

$$0 \cdot a = 0 \text{ und } a \cdot 0 = 0 \text{ für alle } a \in R.$$

Beweis. Es gilt für $a \in R$:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \quad \overset{-(0\cdot a)}{\Longrightarrow} \quad 0 = 0 \cdot a.$$

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \quad \overset{-(a\cdot 0)}{\Longrightarrow} \quad 0 = a \cdot 0.$$

□

Bemerkung 1.3.5. *Sei R ein Ring mit Eins. Nach der Definition eines Ringes (1.3.1) ist es nicht erlaubt, daß die Null und die Eins des Ringes das gleiche Element sind. Nach Lemma 1.3.4 wäre dies auch nur für den trivialen Ring $R = \{0\}$ möglich, denn bei $1 = 0$ folgt ja für alle $a \in R$:*

$$a = 1 \cdot a \overset{(1 \overset{!}{=} 0)}{=} 0 \cdot a \overset{(1.3.4)}{=} 0 \quad \Longrightarrow \quad R = \{0\}. \qquad \square$$

Lemma 1.3.6. *Sei R ein Ring mit Eins. Dann gilt für alle $a \in R$:*

$$(-1) \cdot a = -a \quad \text{und} \quad a \cdot (-1) = -a,$$

wobei -1 das additive Inverse zu 1 und $-a$ das additive Inverse zu a ist. Insbesondere gilt dann für $a, b \in R$:

$$(-a) \cdot b = -(ab) = a \cdot (-b) \quad \text{und} \quad (-a) \cdot (-b) = ab.$$

Beweis. Es gilt:

$$\begin{aligned} 0 = 0 \cdot a = \big(1 + (-1)\big) \cdot a = a + (-1) \cdot a \quad &\overset{+(-a)}{\Longrightarrow} \quad -a = (-1) \cdot a. \\ 0 = a \cdot 0 = a \cdot \big(1 + (-1)\big) = a + a \cdot (-1) \quad &\overset{+(-a)}{\Longrightarrow} \quad -a = a \cdot (-1). \end{aligned}$$

Die weiteren Behauptungen folgen sofort aus dem bisherigen und dem Assoziativgesetz für die Verknüpfung „ $\cdot$ “:

$$\begin{aligned} (-a)b &= \big((-1) \cdot a\big)b = (-1) \cdot (ab) = -(ab). \\ a(-b) &= a\big((-1) \cdot b\big) = \big((-1) \cdot a\big)b = (-1) \cdot (ab) = -(ab). \end{aligned}$$

und

$$(-a) \cdot (-b) = -\big(a \cdot (-b)\big) = -\big(-(ab)\big) = ab. \qquad \square$$

Lemma 1.3.4 zeigt, daß bei einer Multiplikation mit dem Faktor Null immer die Null herauskommt. In $\mathbb{R}^2$ mit komponentenweiser Multiplikation ist $(1, 0) \cdot (0, 1) = (0, 0)$, so daß auch bei einem Produkt zweier Elemente ungleich dem Nullelement die Null als Ergebnis herauskommen kann. Dazu sei definiert:

Definition 1.3.7. *Sei R ein Ring. Ein Element $a \in R \setminus \{0\}$ heißt Nullteiler in R, falls es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$ oder $ba = 0$. Ein Ring ohne Nullteiler heißt nullteilerfrei.*
Ein kommutativer nullteilerfreier Ring wird auch Integritätsring genannt. $\square$

Bemerkung 1.3.8. *Ist $a \neq 0$ kein Nullteiler im Ring R und gilt $ab = 0$ oder $ba = 0$, so folgt $b = 0$.* $\square$

Beispiel 1.3.9.

i.) $\mathbb{Z}$, $\mathbb{Q}$ *und* $\mathbb{R}$ *sind Integritätsringe.*

ii.) *Ist* $(R, +, \cdot)$ *ein Ring und* I *eine nicht-leere Menge mit mindestens zwei Elementen* $a \neq b \in I$, *so ist* $(R^I, \oplus, \odot)$ *nicht nullteilerfrei, denn die Abbildungen*

$$f\colon x \mapsto \begin{cases} 1_R & \text{für } x = a, \\ 0_R & \text{sonst,} \end{cases} \qquad \text{und} \qquad g\colon x \mapsto \begin{cases} 1_R & \text{für } x = b, \\ 0_R & \text{sonst} \end{cases}$$

sind beide nicht die Nullabbildung $\bar{0}$ *(siehe Beispiel 1.3.3), aber wegen* $a \neq b$ *gilt* $f \cdot g = \bar{0}$.

iii.) *Sei* $(R, +, \cdot)$ *ein Ring und* I *eine nicht-leere Menge mit mindestens zwei Elementen* $a \neq b \in I$. *Dann ist auch das kartesische Produkt* $\prod_{i \in I} R$ *mit komponentenweiser Verknüpfung der* I*-Tupel (siehe auch Beispiel 1.3.3) nicht nullteilerfrei. Dazu brauchen die im vorherigen Beispiel konstruierten Abbildungen* $f, g \in R^I$ *nur in Tupel übersetzt werden:*

$$f \rightsquigarrow (x_i)_{i \in I} \text{ mit } x_i := \begin{cases} 1_R & \text{für } i = a, \\ 0_R & \text{sonst,} \end{cases} \quad \text{und} \quad g \rightsquigarrow (x_i)_{i \in I} \text{ mit } y_i := \begin{cases} 1_R & \text{für } i = b, \\ 0_R & \text{sonst.} \end{cases}$$

Dann sind $(x_i)_{i \in I}$ *und* $(y_i)_{i \in I}$ *nicht die Null, aber deren Produkt:*

$$(x_i)_{i \in I} \odot (y_i)_{i \in I} = (x_i \cdot y_i)_{i \in I} = (0_R)_{i \in I}.$$

Besonders einsichtig ist dies für den Spezialfall $I := \{1, \ldots, n\}$ *mit* $n \geq 2$, *denn dann sind folgende Elemente nicht die Null, aber deren Produkt:*

$$x := (1, 0, \underbrace{\ldots}_{\text{nur } 0}) \quad \text{und} \quad y := (0, 1, \underbrace{\ldots}_{\text{nur } 0}) \quad \Longrightarrow \quad x \odot y = (0, \ldots, 0).$$

iv.) *Sei* M *eine nicht-leere Menge. Weiter sei* $A \in \mathcal{P}(M)$ *eine echte Teilmenge von* M, *d.h.* $\emptyset \subsetneq A \subsetneq M$. *Dann ist auch* $B := M \setminus A$ *eine echte Teilmenge von* M *und es gilt*

$$A \cap B = B \cap A = \emptyset,$$

so daß im Ring $\big(\mathcal{P}(M), \ominus, \cap\big)$ *alle Elemente außer der Null* ($\emptyset$) *und der Eins* (M) *Nullteiler sind.* □

Ist R ein Ring mit Eins, so trägt $(R, \cdot)$ eine Monoidstruktur, und die Menge der multiplikativ invertierbaren Elemente $E(R)$ ist nach Lemma 1.1.25 eine Untergruppe von $(R, \cdot)$. Wegen ihrer Relevanz bekommen diese Objekte eigenständige Bezeichnungen:

Definition 1.3.10.

Sei R *ein Ring mit Eins. Ein Element* $a \in R$ *heißt Einheit, falls es ein* $b \in R$ *gibt mit* $ab = ba = 1$. *Die Menge aller Einheiten von* R *wird mit* R^* *bezeichnet und heißt die Einheitengruppe von* R *(siehe Lemma 1.1.25).* □

Bemerkung 1.3.11. *Sei* R *ein Ring mit Eins.*

i.) *Ist* a *eine Einheit, so folgt* $a \neq 0$, *denn Null ist nach Lemma 1.3.4 keine Einheit.*

ii.) *Ist* a *eine Einheit und* $ab = ba = 1$, *so folgt* $(-a) \cdot (-b) = (-b) \cdot (-a) = 1$ *(siehe Lemma 1.3.6), so daß auch* $-a$ *eine Einheit ist. Wegen* $a + (-a) = 0$ *ist die Menge der Einheiten* R^* *bzgl. der Addition nicht abgeschlossen und trägt also nur bzgl. der Multiplikation eine algebraische Struktur (Gruppenstruktur).* □

Beispiel 1.3.12.

i.) *Es gilt* $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ *und* $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

ii.) *Sei* $(G, +)$ *eine abelsche Gruppe. Dann ist nach Beispiel 1.3.3* $\big(\mathrm{End}(G), \oplus, \circ\big)$ *ein Ring mit Eins, und seine Einheitengruppe ist* $\big(\mathrm{Aut}(G), \circ\big)$. □

Nullteiler und Einheiten sind im gewissen Sinne Gegenpaare in einem Ring, denn ein Element kann nur das eine oder das andere sein:

Lemma 1.3.13. *Sei R ein Ring mit Eins. Dann gelten für ein $a \in R$ die beiden zueinander äquivalenten Aussagen:*

$$\begin{aligned} a \text{ Nullteiler} \quad &\Longrightarrow \quad a \text{ keine Einheit.} \\ a \text{ Einheit} \quad &\Longrightarrow \quad a \text{ kein Nullteiler.} \end{aligned}$$

Beweis. Es reicht, eine der beiden äquivalenten Aussagen zu beweisen. Sei dazu a eine Einheit und $ab = ba = 1$ für geeignetes b. Wäre a auch ein Nullteiler, so gäbe es ein $c \neq 0$ mit $ca = 0$ oder $ac = 0$. Dann würde jeweils folgen:

$$\begin{aligned} ca = 0 \quad &\Longrightarrow \quad c = c \cdot 1 = cab = 0 \cdot b = 0. \\ ac = 0 \quad &\Longrightarrow \quad c = 1 \cdot c = bac = b \cdot 0 = 0. \end{aligned}$$

In beiden Fällen ergibt sich ein Widerspruch zur Wahl von $c \neq 0$, so daß a kein Nullteiler sein kann. □

Bemerkung 1.3.14. *In einem Ring kann kein Element gleichzeitig Einheit und Nullteiler sein (Lemma 1.3.13), aber es braucht keines von beiden zu sein, wie der Ring $\mathbb{Z}$ zeigt, wo jedes $a \notin \{-1, 0, 1\}$ weder ein Nullteiler noch eine Einheit ist. Somit läßt sich ein Ring R folgendermaßen in disjunkte Teilmengen zerlegen:*

$$R = \{0\} \dot\cup \{\text{ Einheiten }\} \dot\cup \{\text{ Nullteiler }\} \dot\cup \{\text{ weder } 0 \text{ noch Einheit noch Nullteiler }\}. \quad \square$$

Auf einem Ring R kann bzgl. eines Elementes $a \in R$ eine Linksmultiplikation mit a definiert werden:

Definition 1.3.15. *Sei R ein Ring und $a \in R$. Dann heißt die folgende Abbildung die Linksmultiplikation mit a:*

$$\lambda_a \colon R \longrightarrow R \quad \text{mit} \quad x \mapsto ax. \qquad \square$$

Bemerkung 1.3.16.

i.) *Sei $(R, +, \cdot)$ ein Ring und $a \in R$. Dann ist insbesondere $(R, +)$ eine (abelsche) Gruppe, und bzgl. dieser Gruppenstruktur ist in Definition 1.2.5 schon eine Linksmultiplikation ℓ_a mit a durch*

$$\ell_a \colon R \longrightarrow R \quad \text{mit} \quad x \mapsto a + x$$

definiert worden, die immer eine Bijektion von R ist (Lemma 1.2.6). Aber ℓ_a ist kein Gruppenhomomorphismus von $(R, +)$.
Die Linksmultiplikation λ_a mit a bzgl. der Ringstruktur auf R muß keine Bijektion von R sein, denn die Linksmultiplikation λ_0 mit Null ist nach Lemma 1.3.4 für einen Ring $R \neq \{0\}$ nicht injektiv.
Die Distributivgesetze D1 *und* D2 *in R liefern für λ_a bzgl. der Gruppenstruktur $(R, +)$ folgende Aussagen:*

D1*: λ_a ist ein Gruppenendomorphismus von $(R,+)$ wegen*

$$\lambda_a(x+y) = a(x+y) \overset{(D1)}{=} ax + ay = \lambda_a(x) + \lambda_a(y).$$

D2*: Die folgende Abbildung ist ein Gruppenhomomorphismus von $(R,+)$ nach $\big(\mathrm{End}(R), \oplus\big)$:*

$$\Lambda_R \colon R \longrightarrow \mathrm{End}(R) \quad \textit{mit} \quad a \mapsto \lambda_a.$$

Zu zeigen ist dazu die Gleichung $\Lambda_R(a+b) = \Lambda_R(a) \oplus \Lambda_R(b)$ für alle $a, b \in R$, und es gilt für alle $x \in R$:

$$\begin{aligned}\Lambda_R(a+b)(x) = \lambda_{a+b}(x) = (a+b)x &\overset{(D2)}{=} ax + bx = \lambda_a(x) + \lambda_b(x)\\ &= (\lambda_a \oplus \lambda_b)(x) = (\Lambda_a \oplus \Lambda_b)(x).\end{aligned}$$

ii.) Sei $(R,+,\cdot)$ Ring und $a \in R$ mit $a \neq 0$. Dann gilt für die Linksmultiplikation λ_a (Übung!):

$$a \textit{ ist kein Nullteiler} \quad \Longrightarrow \quad \lambda_a \textit{ injektiv.}$$

Ist R auch ein kommutativer Ring, so gilt sogar (Übung!):

$$a \textit{ ist kein Nullteiler} \quad \Longleftrightarrow \quad \lambda_a \textit{ injektiv.}$$

Im Fall eines nicht-kommutativen Ringes kann λ_a injektiv sein und a trozdem ein Nullteiler, wie folgendes Beispiel zeigt: Es sei der Ring $R := \prod_{i\in\mathbb{N}} \mathbb{R}$ betrachtet und der nicht-kommutative Endomorphismenring $\big(\mathrm{End}(R), \oplus, \circ\big)$ seiner additiven abelschen Gruppe $(R,+)$. Dann sind folgende Abbildungen Gruppenendomorphismen von $(R,+)$ und damit Elemente aus $\mathrm{End}(R)$:

$$\begin{aligned}\varphi &\colon R \longrightarrow R \quad \textit{mit} \quad (x_1, x_2, \ldots) \mapsto (0, x_1, x_2, \ldots),\\ \psi &\colon R \longrightarrow R \quad \textit{mit} \quad (x_1, x_2, \ldots) \mapsto (x_2, x_3, \ldots),\\ \xi &\colon R \longrightarrow R \quad \textit{mit} \quad (x_1, x_2, \ldots) \mapsto (x_1, 0, 0, \ldots),\end{aligned}$$

und es gelten die Gleichungen:

$$\psi \circ \varphi = \mathrm{id}_R \quad \textit{und} \quad \xi \circ \varphi = \bar{0}.$$

Die rechte Gleichung zeigt, daß φ ein Nullteiler im Ring $\mathrm{End}(R)$ ist, und aus der linken Gleichung folgt, daß λ_φ eine injektive Abbildung ist, denn λ_φ ist ein Gruppenendomorphismus von $\mathrm{End}(R)$ und es gilt $\ker(\lambda_\varphi) = \{\bar{0}\}$:

$$\lambda_\varphi(\eta) = \bar{0} \quad \Longrightarrow \quad \varphi \circ \eta = \bar{0} \quad \Longrightarrow \quad \underbrace{\psi \circ \varphi}_{\mathrm{id}_R} \circ \eta = \underbrace{\psi \circ \bar{0}}_{\textit{Null}} \quad \Longrightarrow \quad \eta = \bar{0}.$$

iii.) Sei $(R,+,\cdot)$ nun ein kommutativer Ring mit Eins und $a \in R$. Dann gilt für die Linksmultiplikation λ_a (Übung!):

$$a \textit{ ist eine Einheit} \quad \Longleftrightarrow \quad \lambda_a \textit{ bijektiv} \qquad \square$$

Die vorherigen Betrachtungen zeigen schon, daß die Einheiten in Ringen mit Eins eine besondere Rolle spielen. Der bestmögliche Fall in einem Ring mit Eins ist, daß alle Elemente außer der Null eine Einheit sind, und diese Ringe tragen einen speziellen Namen:

Definition 1.3.17. *Ist R ein Ring mit Eins, in dem alle Elemente außer der Null Einheiten sind, so heißt R Schiefkörper. Ein kommutativer Schiefkörper heißt Körper. Damit ist also insbesondere ein Körper K ein kommutativer Ring mit Eins, in dem folgende zueinander äquivalente Bedingungen gelten:*

- *Alle Elemente außer der Null sind Einheiten.*
- $K^* = K \setminus \{0\}$.
- $(K \setminus \{0\}, \cdot)$ *ist eine abelsche Gruppe.* □

Bemerkung 1.3.18.

i.) *Ein Körper besitzt nach Lemma 1.3.13 keine Nullteiler. Insbesondere folgt in einem Körper dann aus der Gleichung $ab = 0$ entweder $a = 0$ oder $b = 0$ (siehe auch Bemerkung 1.3.8).*

ii.) *Ein Körper kann auch beschrieben werden als Integritätsring mit Eins, in dem alle Elemente außer der Null Einheiten sind. Daß dies nicht in jedem Integritätsring mit Eins erfüllt ist, zeigt das Beispiel $(\mathbb{Z}, +, \cdot)$, in dem nur die zwei Elemente $\{\pm 1\}$ Einheiten sind: $\mathbb{Z}$ ist damit kein Körper.* □

Beispiel 1.3.19.

i.) *$\mathbb{Q}$ und $\mathbb{R}$ sind Körper, und dies sind die einzigen in der Vorlesung bisher bekannten. Weitere Beispiele werden bald konstruiert.*

ii.) *Ist K ein Körper und I eine Menge mit $|I| \geq 2$, so ist der Ring $(K^I, \oplus, \odot)$ zwar ein kommutativer Ring mit Eins, wie Beispiel 1.3.3 zeigt, aber kein Körper, da er nach Beispiel 1.3.9 Nullteiler besitzt.*
Dies gilt nach den gleichen zitierten Beispielen auch für das kartesische Produkt $\prod_{i \in I} K$ und den Speziallfall K^n mit $n \geq 2$ bei komponentenweiser Addition und Multiplikation.
Besonders bei den I-Tupeln des kartesischen Produktes $\prod_{i \in I} K$ fällt auf, daß sich wegen der komponentenweisen Rechnung fast alle Eigenschaften von den Komponenten (Rechnen in K) auf die Tupel übertragen, nur nicht die Nullteilerfreiheit. □

Unterringe, Nebenklassen, Ideale und Quotientenringe.

Auch für die algebraische Struktur „Ringe“ werden nun Unterstrukturen eingeführt:

Definition 1.3.20. *Sei $(R, +, \cdot)$ ein Ring. Eine nicht-leere Teilmenge $U \subseteq R$ heißt Unterring von R, falls $(U, +)$ eine Untergruppe von $(R, +)$ ist und $(U, \cdot)$ eine Unterhalbgruppe.*
Damit ist insbesondere $(U, +, \cdot)$ selbst ein Ring, da sich die Distributivgesetze von R auf U übertragen (die Einschränkung der inneren Verknüpfungen „$+$“ und „$\cdot$“ von R auf U wird mit den gleichen Symbolen wie in R bezeichnet). □

Bemerkung 1.3.21.

i.) *Ist R ein Ring mit Eins und $U \subseteq R$ ein Unterring mit Eins, so müssen die beiden Einselemente nicht übereinstimmen! Als Beispiel sei dazu der Ring $\mathbb{Z} \times \mathbb{Z}$ und der folgende Unterring betrachtet:*

$$U := \mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

Im kartesischen Produkt $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$ mit komponentenweiser Addition und Multiplikation ist $(1,1)$ die Eins, und im Unterring ist das Element $(1,0)$ eine Eins (siehe zum Ring $\mathbb{Z}^2$ auch Beispiel 1.3.3, und zur Diskussion von neutralen Elementen in Unter- und Ober-Monoid Bemerkung 1.2.1).

ii.) *Sei R ein Ring mit Eins und $U \subseteq R$ ein Unterring mit Eins. Enthält U ein Element in a, welches in R kein Nullteiler ist, so gilt mit Bemerkung 1.3.8 die Gleichheit beider Einselemente:*

$$\begin{aligned} a = a \quad &\Longrightarrow \quad a \cdot 1_U = a \cdot 1_R \quad \Longrightarrow \quad a \cdot (1_U - 1_R) = 0 \\ &\overset{1.3.8}{\Longrightarrow} \quad 1_U - 1_R = 0 \quad \Longrightarrow \quad 1_U = 1_R. \end{aligned}$$

□

Ist R ein Ring und $U \subseteq R$ ein Unterring, dann ist insbesondere $(U,+)$ eine Untergruppe von $(R,+)$, und da $(R,+)$ abelsch ist, sogar ein Normalteiler. Damit kann R in Linksnebenklassen $a+U$ zerlegt werden mit

$$a + U := \{\, a + u \mid u \in U \,\},$$

und die repräsentantenweise Verknüpfung $(a+U) \oplus (b+U) := (a+b)+U$ der Linksnebenklassen definiert eine Gruppenstruktur auf der Nebenklassenmenge R/U (siehe dazu den Abschnitt über Normalteiler und Quotientengruppen, insbesondere Satz 1.2.29).

Problematisch bei der Konstruktion war die Wohldefiniertheit der Repräsentantenverknüpfung, daß sich bei Repräsentantenwechsel in einer Verknüpfung immer die gleiche Linksnebenklasse als Ergebnis ergibt:

$$a + U = \tilde{a} + U, \;\; b + U = \tilde{b} + U \quad \Longrightarrow \quad (a+b) + U = (\tilde{a} + \tilde{b}) + U,$$

Dies ist bei einem Normalteiler U jedoch immer erfüllt (Satz 1.2.29).

Es liegt nun nahe, auf den Linksnebenklassen des Unterrings eine weitere Verknüpfung repräsentantenweise durch die Ringmultiplikation zu definieren, um auf der Quotientengruppe R/U so eine Ringstruktur zu erhalten:

$$(a+U) \odot (b+U) := (a \cdot b) + U.$$

Dabei stellt sich wieder die Frage, ob die Definition des Produktes zweier Linksnebenklassen auf Repräsentanten wohldefiniert ist, d.h. bei einem Wechsel der Repräsentanten das gleiche Ergebis liefert:

$$a + U = \tilde{a} + U, \;\; b + U = \tilde{b} + U \quad \overset{?}{\Longrightarrow} \quad (a \cdot b) + U = (\tilde{a} \cdot \tilde{b}) + U.$$

Folgendes Beispiel zeigt, daß dies nicht immer der Fall ist:

Beispiel 1.3.22. *Im Ring $\mathbb{Z} \times \mathbb{Z}$ (komponentenweise Verknüpfung) sei folgender Unterring betrachtet:*

$$\Delta := \{\, (k,k) \mid k \in \mathbb{Z} \,\}.$$

Für zwei Nebenklassen des Unterringes Δ gilt nach Lemma 1.2.17:

$$a + \Delta = b + \Delta \quad \Longleftrightarrow \quad a - b \in \Delta.$$

Damit gilt für folgende Linksnebenklassen von Δ:

$$(1,0) + \Delta = (2,1) + \Delta \qquad \textit{und} \qquad (0,2) + \Delta = (1,3) + \Delta.$$

Allerdings ist bei diesen die repräsentantenweise Verknüpfung nicht wohldefiniert:

$$\big((1,0) + \Delta\big) \odot \big((0,2) + \Delta\big) = \Delta \neq (2,3) + \Delta = \big((2,1) + \Delta\big) \odot \big((1,3) + \Delta\big). \quad \square$$

Bei den Gruppen war mit „beliebigen“ Untergruppen eine repräsentantenweise Verknüpfung von Linksnebenklassen nicht immer möglich (Beispiel 1.2.25), und an die Untergruppe mußten weitere Forderungen gestellt werden, um eine Quotientenkonstruktion zu ermöglichen. Auch bei Ringen muß nun eine Klasse von speziellen Unterringen eingeführt werden, um die repräsentantenweise Multiplikation von Linksnebenklassen zu ermöglichen:

Definition 1.3.23. *Sei R ein Ring und $U \subseteq R$ eine nicht-leere Teilmenge. U heißt Ideal von R, falls U ein Unterring ist und zusätzlich für alle $x \in R$ gilt:*

$$xy \in U \text{ und } yx \in U \text{ für alle } y \in U. \qquad \square$$

Eine äquivalente Definitionsmöglichkeit für Ideale liefert das folgende Lemma:

Lemma 1.3.24. *Sei $(R, +, \cdot)$ ein Ring und $U \subseteq R$ eine nicht-leere Teilmenge. Dann sind äquivalent:*

$$U \text{ ist ein Ideal} \quad \Longleftrightarrow \quad \begin{array}{l} U \text{ ist eine Untergruppe von } (R,+) \text{ und} \\ x \in R,\ y \in U \implies xy,\ yx \in U. \end{array}$$

Beweis.

$\Longrightarrow$: Dies folgt aus den Definitionen von Idealen (1.3.23) und Unterringen (1.3.20).

$\Longleftarrow$: Es ist nur zu zeigen, daß U ein Unterring ist, da die Zusatzbedingung an Unterringe, ein Ideal zu sein, schon erfüllt ist. Die Voraussetzung an U impliziert aber insbesondere für $a, b \in U$ schon $ab \in U$, so daß U unter der Multiplikation abgeschlossen ist und damit $(U, \cdot)$ eine Halbgruppe (die Assoziativität der Multiplikation überträgt sich vom Ring R auf die Teilmenge U). $\square$

Beispiel 1.3.25. *(Für Unterringe und Ideale)*

i.) *$\mathbb{Z}$ ist ein Unterring in $\mathbb{Q}$, und $\mathbb{Z}$, $\mathbb{Q}$ sind Unterringe in $\mathbb{R}$.*

ii.) *In $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ mit komponentenweiser Verknüpfung ist folgende Teilmenge ein Unterring, aber kein Ideal: $\Delta := \{\, (k,k) \mid k \in \mathbb{Z} \,\}$. (Übung!)*

iii.) *In $(\mathbb{Z}, +)$ haben alle Untergruppen die Form $\langle\, k \,\rangle$ mit $k \in \mathbb{Z}$ (siehe Satz 1.2.12), und jede dieser Untergruppen ist auch ein Ideal im Ring $\mathbb{Z}$. (Übung!)*

iv.) *Folgende Aussage ist eine leichte Übung:*

Ein Körper K enthält nur die Ideale $\{0\}$ und K.

Damit ist insbesondere $\mathbb{Z}$ kein Ideal in $\mathbb{Q}$, und $\mathbb{Z}$ und $\mathbb{Q}$ sind keine Ideale in $\mathbb{R}$ (aber Unterringe, siehe obiges Beispiel). $\square$

Das oben gezeigte Beispiel des Ringes $\mathbb{Z}$ ist in soforn besonders, daß für eine Teilmenge $U \subseteq \mathbb{Z}$ äquivalent sind:

$$U \text{ Untergruppe von } (\mathbb{Z},+) \quad \Longleftrightarrow \quad U \text{ Unterring von } \mathbb{Z} \quad \Longleftrightarrow \quad U \text{ Ideal in } \mathbb{Z}.$$

Die Untergruppen, und damit Ideale; in $\mathbb{Z}$ sind alle von der speziellen Form

$$\{\, k \cdot a \mid k \in \mathbb{Z} \,\}.$$

Dieser Typ von Idealen läßt sich folgendermaßen auf beliebige kommutative Ringe mit Eins verallgemeinern:

Lemma 1.3.26. *Sei R ein kommutativer Ring mit Eins und $a \in R$. Dann ist folgende Menge ein Ideal in R und heißt das von a erzeugte Hauptideal:*

$$(a)_R := \{\, xa \mid x \in R \,\}.$$

Beweis.
Daß $(a)_R$ eine Untergruppe von $(R,+)$ ist, folgt direkt aus dem Untergruppenkriterium Lemma 1.2.3, nachdem für $y_1, y_2 \in (a)_R$ die Bedingung $y_1 - y_2 \in (a)_R$ nachzuprüfen ist:

$$\begin{aligned} y_1, y_2 \in (a)_R \quad &\Longrightarrow \quad \exists x_1, x_2 \in R : y_1 = x_1 a, y_2 = x_2 a \\ &\Longrightarrow \quad y_1 - y_2 = x_1 a - x_2 a = (x_1 - x_2)a \in (a)_R. \end{aligned}$$

Nach Lemma 1.3.24 reicht es nun für die Untergruppe $(a)_R$ zu zeigen, daß für $x \in R$ und $y \in (a)_R$ auch $xy, yx \in (a)_R$ gilt. Mit $y = ra$ folgt sofort wegen der Kommutativität von R:

$$yx = xy = xra = (xr)a \in (a)_R. \qquad \square$$

Doch nun zu der Aussage, daß Ideale die „passenden“ Unterringe sind, um mit ihnen eine wohldefinierte Quotientenringstruktur zu definieren:

Satz 1.3.27. *Sei $(R,+,\cdot)$ ein Ring und $I \subseteq R$ ein Ideal. Weiter sei R/I die Menge der Linksnebenklassen $a + I$ von I und $(R/I, \oplus)$ die Quotientengruppe bzgl. des Normalteilers I in der abelschen Gruppe $(R,+)$ mit der Verknüpfungen:*

$$(a+I) \oplus (b+I) := (a+b) + I. \qquad \text{(siehe Satz 1.2.29)}$$

Auf R/I sei folgende Verknüpfung definert:

$$(a+I) \odot (b+I) := (a \cdot b) + I.$$

Dann gilt: Die Verknüpfung „$\odot$“ ist eine wohldefinierte innere Verknüpfung auf R/I und $(R/I, \oplus, \odot)$ ist ein Ring mit dem Nullelement $0_R + I = I$. Dier Ring R/I wird auch der Quotientenring von R und I genannt.
Besitzt R ein Einselement 1_R, so ist $1_R + I$ das Einselement in R/I, und ist R kommutativ, so gilt dies auch für R/I.

Beweis.
„$\odot$“ wohldefiniert: Zu zeigen ist:

$$a + I = \tilde{a} + I \quad \text{und} \quad b + I = \tilde{b} + I \quad \Longrightarrow \quad (a+I) \odot (b+I) = (\tilde{a}+I) \odot (\tilde{b}+I).$$

Nach Lemma 1.2.17 gilt für Linksnebenklassen von I:

$$x + I = y + I \quad \Longleftrightarrow \quad x - y \in I \quad \Longleftrightarrow \quad \exists i \in I : x - y = i. \qquad (*)$$

Daraus folgt dann sofort die Existenz von Elementen $i, j \in I$ mit

$$\tilde{a} = a + i \quad \text{und} \quad \tilde{b} = b + j.$$

Da I ein Ideal ist, gilt aj, ib, $ij \in I$ und damit auch $aj + ib + ij \in I$, und es folgt:

$$\begin{aligned} (\tilde{a}+I) \odot (\tilde{b}+I) &= (\tilde{a}\tilde{b}) + I = \big((a+i)(b+j)\big) + I \\ &= (ab + \underbrace{aj + ib + ij}_{\in I}) + I \overset{(*)}{=} (ab) + I = (a+I) \odot (b+I). \end{aligned}$$

Also ist „ $\odot$ “ unabhängig von der Wahl der Nebenklassenrepräsentanten und damit wohldefiniert.

„ $\odot$ innere Verknüpfung: Dies folgt offensichtlich aus der Definition, denn zwei Linksnebenklassen werden zu einer Linksnebenklasse verknüpft.

„ $\odot$ “ assoziativ: Seien dazu $a, b, c \in R$. Dann folgt aus der Assoziativität der Verknüpfung „ $\cdot$ “ im Ring R:

$$\begin{aligned}\big((a+I)\odot(b+I)\big)\odot(c+I) &= \big((ab)+I\big)\odot(c+I) = \big((ab)c\big)+I\\ &= \big(a(bc)\big)+I = (a+I)\odot\big((bc)+I\big)\\ &= (a+I)\odot\big((b+I)\odot(c+I)\big).\end{aligned}$$

Distributivgesetze: Die Distributivgesetze übertragen sich auch aus denen im Ring R. Für $a, b, c \in R$ folgt:

$$\begin{aligned}D1:\ (a+I)\odot\big((b+I)\oplus(c+I)\big) &= (a+I)\odot\big((b+c)+I\big) = \big(a(b+c)\big)+I\\ &= (ab+ac)+I = \big((ab)+I\big)\oplus\big((ac)+I\big)\\ &= \big((a+I)\odot(b+I)\big)\oplus\big((a+I)\odot(c+I)\big).\\ D2:\ \big((b+I)\oplus(c+I)\big)\odot(a+I) &= \big((b+c)+I\big)\odot(a+I) = \big((b+c)a\big)+I\\ &= (ba+ca)+I = \big((ba)+I\big)\oplus\big((ca)+I\big)\\ &= \big((b+I)\odot(a+I)\big)\oplus\big((c+I)\odot(a+I)\big).\end{aligned}$$

Damit ist $(R/I, \oplus, \odot)$ ein Ring, und offensichtlich $0_R + I = I$ sein Nullelement (siehe auch Satz 1.2.29).
Besitzt R das Einselement 1_R, so gilt für alle $a \in R$:

$$(1_R+I)\odot(a+I) = (1_R\cdot a)+I = a+I = (a\cdot 1_R)+I = (a+I)\odot(1_R+I),$$

so daß $1_R + I$ ein Einselement in R/I ist.
Ist R ein kommutativer Ring, so folgt für $a, b \in R$:

$$(a+I)\odot(b+I) = (ab)+I \overset{(R\text{ komm})}{=} (ba)+I = (b+I)\odot(a+I),$$

und auch R/I ist kommutativ. □

Bemerkung 1.3.28.

i.) Die Bildung von Quotientenringen ist ein wichtiges Hilfsmittel zur Konstruktion von Körpern.
Ist R ein Ring und $I \subseteq R$ ein Ideal, dann heißt I maximales Ideal in R, wenn es kein Ideal $J \subsetneq R$ gibt mit $I \subsetneq J$, also aus $I \subseteq J \subseteq R$ immer $I = J$ oder $J = R$ folgt.
Ist R ein kommutativen Ring mit Eins, so gilt bzgl. maximaler Ideale folgende wesentliche Äquivalenz:

$$I \text{ maximales Ideal in } R \quad\Longleftrightarrow\quad R/I \text{ ist ein Körper.}$$

ii.) Im Ring $\mathbb{Z}$ existiert folgende Aussage über maximale Ideale:

$$a \in \mathbb{Z} \text{ Primzahl} \quad\Longleftrightarrow\quad (a)_{\mathbb{Z}} \text{ ist ein maximales Ideal in } \mathbb{Z}.$$

Zusammen mit der vorherigen Aussage über Quotienten mit maximalen Idealen ergibt sich also:

$$a \in \mathbb{Z} \text{ Primzahl} \quad \Longleftrightarrow \quad \mathbb{Z}/(a)_{\mathbb{Z}} \text{ ist ein Körper.}$$

$\mathbb{Z}/(a)_{\mathbb{Z}}$ ist aber nichts anderes als der Restklassenring $\mathbb{Z}_a$.
Diese wichtige Aussage wird in Satz 1.3.34 bewiesen, jedoch mit elementaren Argumenten, ohne obigen Umweg über die maximalen Ideale. □

Da im Falle des Ringes $\mathbb{Z}$ die Untergruppen von $(\mathbb{Z}, +)$ mit den Idealen des Ringes übereinstimmen, kann nun die Konstruktion der Restklassengruppe $\mathbb{Z}_n$ (Satz 1.2.33 und Definition 1.2.34) komplett übernommen und ringtheoretisch formuliert werden:

Satz 1.3.29. *Sei $n \in \mathbb{N}$. $\mathbb{Z}$ ist ein kommutativer Ring mit Eins, und nach Lemma 1.3.26 die Menge*

$$\langle\, n \,\rangle \overset{(1.2.12)}{=} \{\, kn \mid k \in \mathbb{Z} \,\} \overset{(1.3.26)}{=} (n)_{\mathbb{Z}}$$

ein Ideal in $\mathbb{Z}$ und damit nach Satz 1.3.27

$$\mathbb{Z}/(n)_{\mathbb{Z}} = \mathbb{Z}/\langle\, n \,\rangle \overset{(1.2.34)}{=} \mathbb{Z}_n$$

ein kommutativer Ring mit dem Nullelement $[0]_n$ und dem Einselement $[1]_n$. Nach Satz 1.2.33 und Definition 1.2.34 gilt

$$\mathbb{Z}_n := \{[0]_n, \ldots, [n-1]_n\},$$

und die Linksnebenklassen werden dabei verknüpft durch:

$$[a]_n + [b]_n = [a+b]_n \quad \text{und} \quad [a]_n \cdot [b]_n = [a \cdot b]_n.$$ □

Bemerkung 1.3.30. *Wird im Restklassenring $\mathbb{Z}_n$ die additive Gruppe betrachtet, also die Restklassengruppe $\mathbb{Z}_n$, so werden darin Potenzen von Elementen wegen der additiven Verknüpfung als Vielfache notiert, d.h. für $k \in \mathbb{Z}$ und $[a]_n \in \mathbb{Z}_n$ gilt nach Definition 1.1.27:*

$$k \bullet [a]_n = \begin{cases} \underbrace{[a]_n + [a]_n + \cdots + [a]_n}_{k\text{-mal}} & \text{für } k > 0, \\ [0]_n & \text{für } k = 0, \\ |k| \bullet [-a]_n & \text{für } k < 0. \end{cases}$$

Es folgt sofort für alle $k \in \mathbb{Z}$ und der Multiplikation im Restklassenring:

$$k \bullet [a]_n = [k \cdot a]_n = [k]_n \cdot [a]_n.$$

Da in obiger Formel k und a in $\mathbb{Z}$ liegen, folgt sogar:

$$k \bullet [a]_n = a \bullet [k]_n.$$ □

Definition 1.3.31. *Für $n \in \mathbb{N}$ wird der in Satz 1.3.29 konstruierte Ring $(\mathbb{Z}_n, +, \cdot)$ der n-te Restklassenring genannt, und seine Einheitengruppe $\mathbb{Z}_n^*$ die n-te Einheitengruppe. Weiter ist die Eulersche φ-Funktion definiert durch:*

$$\varphi \colon \mathbb{N} \longrightarrow \mathbb{N} \quad \text{mit} \quad n \mapsto |\mathbb{Z}_n^*|.$$ □

Bemerkung 1.3.32.

i.) *Die Eulersche φ-Funktion ist wohldefiniert, denn für jedes $n \in \mathbb{N}$ gilt wegen $[1]_n \in \mathbb{Z}_n^*$ die Abschätzung $1 \leq |\mathbb{Z}_n^*| \leq |\mathbb{Z}_n| = n$ und damit $\varphi(n) \in \mathbb{N}$.*

ii.) *Es gilt folgende Aussage für ein $[a]_n \in \mathbb{Z}_n$ (Aufgabenblatt 7, Aufgabe 2.b):*

$$[a]_n \in \mathbb{Z}_n^* \quad \Longleftrightarrow \quad \langle\, [a]_n \,\rangle = \mathbb{Z}_n.$$

Diese Äquivalenz stellt einen Zusammenhang zwischen der Ringstruktur auf $\mathbb{Z}_n$ (n-ter Restklassenring) und der (additiven) Gruppenstruktur auf $\mathbb{Z}_n$ her (n-te Restklassengruppe, Definition 1.2.34): Ein Element ist genau dann eine Einheit im n-ten Restklassenring, wenn es ein Erzeuger der (zyklischen) n-ten Restklassengruppe ist.
Die Einheiten im Restklassenring $\mathbb{Z}_n$ und damit Erzeuger der zyklischne Restklassengruppe $\mathbb{Z}_n$ können auch folgendermaßen charakterisiert werden (Übung!):

$$[a]_n \in \mathbb{Z}_n^* \quad \Longleftrightarrow \quad \mathrm{ggT}(a,n) = 1.$$

Die Bedingung $\mathrm{ggT}(a,n) = 1$ ist gleichbedeutend damit, daß a und n keinen gemeinsamen Teiler haben (außer natürlich 1 und -1).
Damit ergeben sich folgende drei äquivalente Aussagen für die Eulersche φ-Funktion:

$$\begin{aligned}
\varphi(n) &= |\{\, \textit{Einheiten im Ring } \mathbb{Z}_n \,\}|.\\
\varphi(n) &= |\{\, \textit{Erzeuger der Gruppe } \mathbb{Z}_n \,\}|.\\
\varphi(n) &= |\{\, r \mid 0 < r < n \textit{ und } \mathrm{ggT}(r,n) = 1 \,\}|.
\end{aligned}$$

iii.) *Mit obigen Äquivalenzen für die Eulersche φ-Funktion lassen sich folgende beiden Aussagen beweisen (Übung!):*
- *Sind $a, b \in \mathbb{N}$ teilerfremd, d.h. $\mathrm{ggT}(a,b) = 1$, so gilt: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.*
- *Ist $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N}$, so gilt: $\varphi(p^n) = (p-1) \cdot p^{n-1}$.*

Dies ermöglicht dann eine Berechnung von $\varphi(n)$, falls die Primfaktorzerlegung von n bekannt ist:

$$n = \prod_{i=1}^{k} p_i^{r_i} \ \textit{Primfaktorzerlegung} \quad \Longrightarrow \quad \varphi(n) = \prod_{i=1}^{k} (p_i - 1) \cdot p_i^{r_i - 1}.$$

(Siehe auch Bemerkung 1.2.62). □

Es wird nun untersucht, wann der Restklassenring $\mathbb{Z}_n$ ein Körper ist. Dazu wird folgende Hilfsaussage benutzt:

Lemma 1.3.33. *Sei $p \in \mathbb{N}$ eine Primzahl und $1 \leq m < p$. Dann existieren $a, b \in \mathbb{Z}$ mit $1 = ap + bm$.*

Beweis. Es sei folgende Teilmenge von $\mathbb{Z}$ definert:

$$U := \{\, ap + bm \mid a, b \in \mathbb{Z} \,\} \subseteq \mathbb{Z}.$$

Behauptung: U ist eine Untergruppe von $(\mathbb{Z}, +)$ und $U \neq \{0\}$.

Beweis der Behauptung: Es ist $m \in U$ und damit U nicht leer. Nach dem Untergruppenkriterium aus Lemma 1.2.3 ist die nicht-leere Teilmenge $U \subseteq \mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$, wenn für alle $x, y \in U$ auch $x - y \in U$ gilt. Seien also die Elemente $x := ap + bm$ und $y := \tilde{a}p + \tilde{b}m$ aus U. Dann folgt:

$$x - y = (ap + bm) - (\tilde{a}p + \tilde{b}m) = (a - \tilde{a})p + (b - \tilde{b})m \in U.$$

U ist also eine Untergruppe von $(\mathbb{Z}, +)$, und aus $1 \leq m \in U$ folgt auch $U \neq \{0\}$, so daß die Behauptung bewiesen ist.

Nach Satz 1.2.12 gibt es für die Untergruppe U ein geeignetes $d \in \mathbb{N}_0$ mit $U = \langle d \rangle_{\mathbb{Z}}$, und aus $U \neq \{0\}$ folgt dann $d \in \mathbb{N}$.
Nun wird gezeigt, daß $d = 1$ gelten muß, wobei die bekannte Tatsache über Primzahlen benutzt wird, daß p keine echten positiven Teiler hat, also aus $p = ab$ mit $a, b \in \mathbb{N}$ entweder $a = 1$ und $b = p$ folgt oder umgekehrt.
Es gilt $m, p \in U = \langle d \rangle$ und damit $k_1 d = m$ und $k_2 d = p$ für geeignete $k_1, k_2 \in \mathbb{Z}$, wobei k_1, k_2 wegen $d, m, p \in \mathbb{N}$ positiv sein müssen. Aus p prim folgt $d, k_2 \in \{1, p\}$, und wegen $0 \leq d \leq m < p$ gilt dann $k_2 = p$ und $d = 1$.
Somit ist $1 \in U$ und $1 = ap + bm$ für geeignete $a, b \in \mathbb{Z}$. □

Nun ergibt sich sofort die gewünschte Aussage über die Restklassenringe:

Satz 1.3.34. *Sei $n \in \mathbb{Z}$. Dann gilt:*

$$\mathbb{Z}_n \text{ ist ein Körper} \iff n \text{ ist eine Primzahl.}$$

Beweis.

$\Longrightarrow$: Wäre n keine Primzahl, so gäbe es $0 < a \leq b < n$ mit $ab = n$. Dann wären $[a]_n$ und $[b]_n$ in $\mathbb{Z}_n$ Nullteiler und $\mathbb{Z}_n$ damit kein Körper (Bemerkung 1.3.8):

$$[a]_n \cdot [b_n] = [a \cdot b]_n = [n]_n = [0]_n \qquad \text{aber} \qquad [a]_n, [b]_n \neq [0]_n.$$

$\Longleftarrow$: Nach Satz 1.3.29 ist der Restklassenring $\mathbb{Z}_n$ ein kommutativer Ring mit Eins, so daß nur überprüft werden muß, daß für n prim jedes Element außer der Null eine Einheit ist. Sei dazu ein Repräsentant $0 < r < n$ gewählt. Nach Lemma 1.3.33 existieren dann $a, b \in \mathbb{Z}$ mit $1 = an + br$, und es folgt:

$$[1]_n = [an + br]_n = [a]_n[n]_n + [b]_n[r]_n \overset{([n]_n = [0]_n)}{=} [b]_n[r]_n \overset{(\mathbb{Z}_n \text{ komm})}{=} [r]_n[b]_n.$$

Damit ist $[b]_n$ ein Inverses zu $[r]_n$ und dieses eine Einheit. □

Bemerkung 1.3.35.

i.) Die Menge der endlichen Körper ist vollständig (bis auf Isomorphie) klassifiziert. Es gelten folgende Aussagen:

- *Zwei endliche Körper gleicher Größe sind isomorph (via einem Körperisomorphismus).*
- *Für $n \in \mathbb{N}$ gilt die Äquivalenz:*

$$n \text{ ist eine Primzahlpotenz} \iff \begin{array}{l}\text{Es gibt einen endlichen}\\ \text{Körper der Größe } n.\end{array}$$

Dies läßt sich zu folgendem Klassifikationssatz über endliche Körper zusammenfassen:

Nur zu einer Primzahlpotenz gibt es einen (und dann bis auf Isomorphie eindeutig bestimmten) endlichen Körper dieser Größe.

Damit gibt es endliche Körper der Größe $2, 3, 4, 5, 7, 8, 9$*, aber nicht der Größe* 6 *oder* 10*.*
Achtung: Die endlichen Körper zu einer echten Primzahlpotenz p^n *mit* $n \geq 2$*, also z.B.* $4, 8, 9$*, sind nicht die Restklassenringe* $\mathbb{Z}_{p^n}$*! Laut Satz 1.3.34 sind nur die Restklassenringe* $\mathbb{Z}_p$ *(p prim) Körper.*
Ein Körper der Größer p^n *mit* $n \geq 2$ *wird im allgemeinen folgendermaßen konstruiert: Im Polynomring* $\mathbb{Z}_p[t]$ *über* $\mathbb{Z}_p$ *wird ein geeignetes Polynom* f *vom Grad* n *gewählt, und dann der Quotientenring* $\mathbb{Z}_p[t]/(f)_{\mathbb{Z}_p[t]}$ *gebildet, also von* $\mathbb{Z}_p[t]$ *mit dem von* f *erzeugten Hauptideal. Bei geeigneter Wahl von* f *ist dieses Hauptideal maximal und der Quotient dann ein Körper (siehe dazu auch Bemerkung 1.3.28).* □

Ringhomomorphismen.

Wie bei Gruppen (und allen anderen algebraischen Strukturen) sind bei Ringen wieder die strukturverträglichen Abbildungen von Interesse. Da Ringe zwei innere Verknüpfungen besitzen, soll für beide das schon in Bemerkung 1.2.39 diskutierte Prinzip gelten:

erst verknüpfen, dann abbilden $\iff$ erst abbilden, dann verknüpfen.

Definition 1.3.36. *Seien* $(R, *, \diamond)$ *und* $(S, \star, \bullet)$ *Ringe. Eine Abbildung* $\varphi\colon R \longrightarrow S$ *heißt Ringhomomorphismus, falls sie strukturverträglich bzgl. beider Verknüpfungen ist, d.h. es gilt für alle* $a, b \in R$*:*

$$\varphi(a * b) = \varphi(a) \star \varphi(b) \quad \text{und} \quad \varphi(a \diamond b) = \varphi(a) \bullet \varphi(b).$$

Insbesondere ist dann φ *ein Gruppenhomomorphismus von* $(R, *)$ *nach* $(S, \star)$ *und ein Halbgruppenhomomorphismus von* $(R, \diamond)$ *nach* $(S, \bullet)$*.*
Sind R *und* S *beide Körper, so wird* φ *auch als Körperhomomorphismus bezeichnet. Entsprechend den Bezeichnungsregeln aus Definition 1.2.38 werden injektive, surjektive und bijektive Homomorphismen jeweils als Mono-, Epi- und Isomorphismen bezeichnet, und sind Defininitionsbereich und Wertebreich gleich, so Homomorphismen als Endomorphismen und Isomorphismen als Automorphismen (siehe auch Bemerkung 1.2.39).*
Die Menge aller Ringhomomorphismen von R *nach* S *wird mit* $\mathrm{Hom}_{Ring}(R, S)$ *bezeichnet, und für den Ring* R *die Menge aller Ringendomorphismen mit* $\mathrm{End}_{Ring}(R)$ *und die Menge aller Ringautomorphismen mit* $\mathrm{Aut}_{Ring}(R)$*.* □

Bemerkung 1.3.37.

i.) Werden für zwei Ringe R *und* S *nicht explizit Verknüpfungssymbole angegeben, so greift die „implizite Standardnotationsregel“, und es werden die Verknüpfungen* $(R, +, \cdot)$ *und* $(S, +, \cdot)$ *ergänzt mit Mehrfachbedeutung der einzelnen Symbole. Für einen Ringhomomorphismus* φ *verkürzen sich dann die Strukturerhaltungsregeln zu*

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{und} \quad \varphi(ab) = \varphi(a)\varphi(b),$$

und es obliegt dem Leser, die Verknüpfungen kontextabhängig zu interpretieren.

ii.) *Ist R ein Ring, so ist mit dem Endomorphismenring $\operatorname{End}(R)$ (oder präziser: $\big(\operatorname{End}(R), \oplus, \circ\big)$) immer derjenige Ring gemeint, der aus den Gruppenendomorphismen der abelschen Gruppe $(R,+)$ gebildet wird (Beispiel 1.3.3).*
Die Menge $\operatorname{End}_{Ring}(R)$ der Ringendomorphismen von R bildet keinen Ring, wie später gezeigt wird.

iii.) *Sind R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus, so muß $\varphi(0_R) = 0_S$ gelten, da φ ein Gruppenhomorphismus von $(R,+)$ nach $(S,+)$ ist und dieser nach Lemma 1.2.51 die neutralen Elemente aufeinander abbildet.*

iv.) *Achtung: Sind R, S jeweils Ringe mit Eins und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus, so müssen die neutralen Elemente der Monoidstrukturen $(R,\cdot)$ und $(S,\cdot)$, also 1_R und 1_S, nicht aufeinander abgebildet werden!*
Gegenbeispiel: Die Abbildung $\bar{0}$ mit $r \mapsto 0_S$ für alle $r \in R$ ist ein Ringhomomorphismus, und 1_R wird nicht auf 1_S abgebildet.
In folgender Situation, die allerdings häufig auftritt, wird trotzdem impliziert, daß auch die multiplikativen neutralen Elemente (Einsen) von einem Ringhomomorphismus aufeinander abgebildet werden:
Aussage: Liegt in $\operatorname{im}(\varphi) \subseteq S$ mindestens ein Element, das kein Nullteiler in S ist, so muß aber $\varphi(1_R) = 1_S$ gelten.
Beweis der Aussage: Sei $a \in R$, so daß $\varphi(a)$ kein Nullteiler in S ist. Es folgt mit Bemerkung 1.3.8:

$$\begin{aligned}
& \varphi(a) = \varphi(1_R \cdot a) = \varphi(1_R)\cdot\varphi(a) && \overset{-\varphi(a)}{\Longrightarrow} && \varphi(1_R)\cdot\varphi(a) - \varphi(a) = 0_S \\
\Longrightarrow\ & \varphi(1_R)\cdot\varphi(a) - 1_S\cdot\varphi(a) = 0_S && \Longrightarrow && (\varphi(1_R) - 1_S)\cdot\varphi(a) = 0_S \\
\overset{1.3.8}{\Longrightarrow}\ & \varphi(1_R) - 1_S = 0_S && \Longrightarrow && \varphi(1_R) = 1_S. \qquad \square
\end{aligned}$$

Beispiel 1.3.38.

i.) *Für Ringe R und S sind folgende Abbildungen Ringhomomorphismen (Übung!):*

$$\mathrm{id}_R\colon R \longrightarrow R \quad \textit{mit} \quad r \mapsto r \qquad \textit{und} \qquad \bar{0}\colon R \longrightarrow S \quad \textit{mit} \quad r \mapsto 0_S.$$

ii.) *Sei $\mathcal{F}(\mathbb{Q})$ die Menge aller rationalen Folgen, $\mathcal{F}_K(\mathbb{Q})$ die Menge aller konvergenten rationalen Folgen, $\mathcal{F}_C(\mathbb{Q})$ die Menge aller rationalen Cauchy-Folgen und $\mathcal{F}_N(\mathbb{Q})$ die Menge aller rationalen Nullfolgen.*
Alle diese Mengen sind zusammen mit den Verknüpfungen „Summe und Produkt von Folgen“ kommutative Ringe mit Eins. Es gelten die Inklusionen

$$\mathcal{F}_N(\mathbb{Q}) \subseteq \mathcal{F}_K(\mathbb{Q}) \subseteq \mathcal{F}_C(\mathbb{Q}) \subseteq \mathcal{F}(\mathbb{Q}),$$

und die Mengen sind jeweils Unterringe im passenden Oberring. Dabei sind die rationalen Nullfolgen $\mathcal{F}_N(\mathbb{Q})$ sogar ein Ideal in $\mathcal{F}_K(\mathbb{Q})$ und in $\mathcal{F}_C(\mathbb{Q})$, aber nicht in $\mathcal{F}(\mathbb{Q})$. Dies folgt sofort aus den Aussagen zu Folgen in jedem Einführungsbuch zur Analysis I, z.B. in [**FAn1**, §4, Folgen,Grenzwerte].
Alle rationalen Cauchy-Folgen sind in $\mathbb{R}$ konvergent, besitzen damit einen reellen Grenzwert, und folgende Abbildung ist ein Ringhomomorphismus:

$$\mathcal{G}\colon \mathcal{F}_C(\mathbb{Q}) \longrightarrow \mathbb{R} \quad \textit{mit} \quad (a_i)_{i\in\mathbb{N}_0} \mapsto \textit{Grenzwert von } (a_i)_{i\in\mathbb{N}_0} \textit{ in } \mathbb{R}. \qquad \square$$

Ein wichtiges Beispiel für einen Ringhomomorphismus ist die Übertragung von Lemma 1.2.43 auf Ringe:

Lemma 1.3.39. .
Sei R ein Ring und $I \subseteq R$ ein Ideal in R. Dann ist die kanonische Projektion von R auf den Quotientenring R/I (siehe Satz 1.3.27) ein Ringhomomorphismus:

$$\pi_I \colon R \longrightarrow R/I \quad \textit{mit} \quad x \mapsto x + I.$$

Beweis.
Die Abbildung π_I ist nach Lemma 1.2.43 schon ein Gruppenhomomorphismus der additiven Gruppen beider Ringe, und aus der Defnition der Linksnebenklassenrechnung in Satz 1.3.27 ergibt sich auch direkt die Strukturverträglichkeit bzgl. der Multiplikation in den Ringen:

$$\pi_I(ab) \overset{\text{(Def)}}{=} ab + I = (a+I) \odot (b+I) \overset{\text{(Def)}}{=} \pi_I(a) \odot \pi_I(b). \qquad \square$$

Als nächstes wird betrachtet, wie sich Ringhomomorphismen bzgl. der Kompositionsverknüpfung verhalten (siehe dazu auch den analogen Satz 1.2.48 für Gruppen):

Satz 1.3.40. *Seien R, S und T Ringe mit Ringhomomorphismen:*

$$\varphi \colon R \longrightarrow S \qquad \textit{und} \qquad \psi \colon S \longrightarrow T.$$

Dann ist die Komposition $\psi \circ \varphi$ ein Ringhomomorphismus von R nach T. Insbesondere ist dann die Menge $\mathrm{End}_{Ring}(R)$ abgeschlossen unter der Komposition von Abbildungen und $\big(\mathrm{End}_{Ring}(R), \circ\big)$ ein Untermonoid von $\big(\mathrm{Abb}(R,R), \circ\big)$ mit dem neutralen Element id_R.

Ist φ bijektiv, so ist auch die (mengentheoretische) Umkehrabbildung φ^{-1} ein Ringhomomorphismus. Insbesondere ist dann $\big(\mathrm{Aut}_{Ring}(R), \circ\big)$ eine Untergruppe des Monoides $\big(\mathrm{End}_{Ring}(R), \circ\big)$ und der Gruppe $\big(S(R), \circ\big)$.

Beweis.

$\psi \circ \varphi$ Ringhomomorphismus: Nach Satz 1.2.48 ist $\psi \circ \varphi$ schon ein Gruppenhomomorphismus, so daß nur noch die Strukturverträglichkeit bzgl. der Multiplikation überprüft werden muß. Für $a, b \in R$ gilt dazu:

$$\begin{aligned}(\psi \circ \varphi)(ab) &= \psi\big(\varphi(ab)\big) \overset{(\varphi\ \mathrm{RHom})}{=} \psi\big(\varphi(a)\varphi(b)\big) \overset{(\psi\ \mathrm{RHom})}{=} \psi\big(\varphi(a)\big)\psi\big(\varphi(b)\big) \\ &= (\psi \circ \varphi)(a)(\psi \circ \varphi)(b).\end{aligned}$$

Damit ist $\psi \circ \varphi$ ein Ringhomomorphismus, und insbesondere $\mathrm{End}_{\mathrm{Ring}}(R)$ abgeschlossen unter der Komposition von Abbildungen.
$\big(\mathrm{Abb}(R,R), \circ\big)$ ist nach Lemma 1.1.36 ein (nicht-kommutativer) Monoid mit dem neutralen Element id_R, und id_R ist ein Ringautomorphismus (Beispiel 1.3.38). Damit ist $\big(\mathrm{End}_{\mathrm{Ring}}(R), \circ\big)$ eine Halbgruppe und wegen $\mathrm{id}_R \in \mathrm{End}_{\mathrm{Ring}}(R)$ sogar ein Untermonoid von $\big(\mathrm{Abb}(R,R), \circ\big)$ mit dem neutralen Element id_R.

φ^{-1} Ringhomomorphismus: Nach Satz 1.2.48 ist φ^{-1} ein Gruppenhomomorphismus, und es muß nur gezeigt werden, daß dieser auch mit der multiplikativen Verknüpfung verträglich ist. Seien dazu $x, y \in S$. Es gibt dann wegen der Bijektivität von φ eindeutig bestimmte Elemente $a, b \in R$ mit

$$\varphi(a) = x \text{ und } \varphi(b) = y \quad \Longrightarrow \quad a = \varphi^{-1}(x) \text{ und } b = \varphi^{-1}(y),$$

und es folgt:

$$\varphi^{-1}(xy) = \varphi^{-1}\big(\varphi(a)\varphi(b)\big) \overset{(\varphi\ \mathrm{RHom})}{=} \varphi^{-1}\big(\varphi(ab)\big) \overset{(\mathrm{Umkehrabb})}{=} ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

Damit ist φ^{-1} sogar ein Ringhomomorphismus.
Die Menge $\mathrm{Aut}_{\mathrm{Ring}}(R)$ ist abgeschlossen unter der Komposition, da die Komposition von Ringhomomorphismen wieder einen Ringhomomorphismus liefert (siehe oben), und die Komposition bijektiver Abbildungen wieder bijketiv ist (Lemma 0.4.11). Da die Identität id_R in $\mathrm{Aut}_{\mathrm{Ring}}(R)$ liegt, ist $\big(\mathrm{Aut}_{\mathrm{Ring}}(R), \circ\big)$ sogar ein Monoid, und da für jedes $\varphi \in \mathrm{Aut}_{\mathrm{Ring}}(R)$ eine Umkehrabbildung φ^{-1} existiert (Satz 0.4.15) und diese auch ein Ringhomomorphismus ist (siehe oben), hat jedes Element aus $\mathrm{Aut}_{\mathrm{Ring}}(R)$ ein Inverses bzgl. der Komposition und $\big(\mathrm{Aut}_{\mathrm{Ring}}(R), \circ\big)$ ist eine Gruppe.
Offensichtlich gilt $\mathrm{Aut}_{\mathrm{Ring}}(R) \subseteq \mathrm{End}_{\mathrm{Ring}}(R)$ und $\mathrm{Aut}_{\mathrm{Ring}}(R) \subseteq S(R)$. □

Sind R und S Ringe, so induzieren die Verknüpfungen auf $(S, +, \cdot)$ jeweils Verknüpfungen auf $\mathrm{Abb}(R, S)$ (siehe Satz 1.1.37):

$$\begin{aligned} f \oplus g\colon R \longrightarrow S \quad &\text{mit} \quad (f \oplus g)(a) := f(a) + g(a), \\ f \odot g\colon R \longrightarrow S \quad &\text{mit} \quad (f \odot g)(a) := f(a) \cdot g(a). \end{aligned}$$

Die Frage ist nun, ob die Teilmenge $\mathrm{Hom}_{\mathrm{Ring}}(R, S)$ invariant unter diesen Verknüpfungen ist. Im Fall der abelschen Gruppen $(R, +)$ und $(S, +)$ gilt dies nach Satz 1.2.49 für die Gruppenhomomorphismen $\mathrm{Hom}(R, S)$, und $\big(\mathrm{Hom}(R, S), \oplus\big)$ ist sogar eine abelsche Gruppe.
Bei Ringhomomorphismen ist dies nicht der Fall: sowohl die „Summe“ $f \oplus g$ von Abbildungen als auch deren „Produkt“ $f \odot g$ müssen keine Ringhomomorphismen sein, wie folgende Bemerkung zeigt, und somit kann auf $\mathrm{Hom}_{\mathrm{Ring}}(R, S)$ und damit auch auf $\mathrm{End}_{\mathrm{Ring}}(R)$ keine algebraische Struktur mit den obigen Verknüpfungen definiert werden.

Bemerkung 1.3.41. *Es sei der Ring $\mathbb{Z}$ betrachtet und $\mathrm{id}_{\mathbb{Z}} \in \mathrm{End}_{Ring}(\mathbb{Z})$. Dann ist die Abbildung $\mathrm{id}_{\mathbb{Z}} \oplus \mathrm{id}_{\mathbb{Z}}$ kein Ringendomorphismus von $\mathbb{Z}$ wegen:*

$$(\mathrm{id}_{\mathbb{Z}} \oplus \mathrm{id}_{\mathbb{Z}})(1 \cdot 1) \overset{(Def)}{=} 1 \cdot 1 + 1 \cdot 1 \neq (1+1) \cdot (1+1) \overset{(Def)}{=} (\mathrm{id}_{\mathbb{Z}} \oplus \mathrm{id}_{\mathbb{Z}})(1) \cdot (\mathrm{id}_{\mathbb{Z}} \oplus \mathrm{id}_{\mathbb{Z}})(1).$$

Auch die Abbildung $\mathrm{id}_{\mathbb{Z}} \odot \mathrm{id}_{\mathbb{Z}}$ ist kein Ringendomorphismus von $\mathbb{Z}$ wegen:

$$(\mathrm{id}_{\mathbb{Z}} \odot \mathrm{id}_{\mathbb{Z}})(1+1) \overset{(Def)}{=} (1+1) \cdot (1+1) \neq (1 \cdot 1) + (1 \cdot 1) \overset{(Def)}{=} (\mathrm{id}_{\mathbb{Z}} \odot \mathrm{id}_{\mathbb{Z}})(1) + (\mathrm{id}_{\mathbb{Z}} \odot \mathrm{id}_{\mathbb{Z}})(1).$$

Damit ist die Menge $\mathrm{End}_{Ring}(\mathbb{Z}) = \mathrm{Hom}_{Ring}(\mathbb{Z}, \mathbb{Z})$ nicht abgeschlossen unter den Verknüpfungen „$\oplus$“ und „$\odot$“. □

Auch bei Ringhomomorphismen ist analog zu Gruppenhomomorphismen der Kern des Homomorphismus ein wesentliches Objekt zu dessen Analyse. Da ein Ring nur bzgl. seiner additiven Struktur immer ein neutrales Element besitzt, und ein Ringhomomorphismus bzgl. der additiven Gruppenstruktur des Ringes auch ein Gruppenhomomorphismus ist, für den schon ein Kern definiert ist, wird festgelegt:

Definition 1.3.42. *Seien R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann ist der Kern von φ definiert als:*

$$\ker(\varphi) := \{\, x \in R \mid \varphi(x) = 0_S \,\}. \qquad \square$$

Da der Kern eines Ringhomomorphismus $\varphi\colon R \longrightarrow S$ gleich dem Kern des Gruppenhomomorphismus $\varphi\colon (R,+) \longrightarrow (S,+)$ ist, kann folgende Aussage direkt aus Lemma 1.2.53 übernommen werden:

Lemma 1.3.43. *Für Ringe R, S und einen Ringhomomorphismus $\varphi\colon R \longrightarrow S$ gilt:*

$$\varphi \text{ injektiv} \quad \Longleftrightarrow \quad \ker(\varphi) = \{0_R\}. \qquad \square$$

Bei einem Gruppenhomomorphismus war dessen Kern ein Normalteiler, also eine spezielle Untergruppe, auf deren Linksnebenklassen durch repräsentantenweise Verknüpfung eine Gruppenstruktur wohldefiniert war, d.h. eine Quotientengruppe konstruiert werden konnte.
Bei Ringen sind die speziellen Unterringe, auf deren Linksnebenklassen durch repräsentantenweise Verknüpfung eine Ringstruktur wohldefiniert ist und ein Quotientenring konstruiert werden kann, die Ideale. Und es ergibt sich analog zu den Gruppen, daß Kerne von Ringhomomorphismen auch solche speziellen Unterstrukturen sind:

Lemma 1.3.44. *Seien R und S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann ist $\ker(\varphi)$ ein Ideal in R, also insbesondere auch ein Unterring.*

Beweis.
Nach Satz 1.2.55 ist $\ker(\varphi)$ eine Untergruppe von $(R,+)$, und es muß nach Lemma 1.3.24 nur nachgeprüft werden, daß für alle $a \in R$ und $x \in \ker(\varphi)$ auch xa und ax in $\ker(\varphi)$ liegen:

$$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)\cdot 0 \overset{(1.3.4)}{=} 0 \quad \Longrightarrow \quad ax \in \ker(\varphi).$$
$$\varphi(xa) = \varphi(x)\varphi(a) = 0\cdot\varphi(a) \overset{(1.3.4)}{=} 0 \quad \Longrightarrow \quad xa \in \ker(\varphi).$$

Damit ist $\ker(\varphi)$ ein Ideal in R und damit auch ein Unterring. $\square$

Bemerkung 1.3.45.
Ist $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus, so ist nach Lemma 1.3.44 der Kern von φ ein Ideal in R. Ist andersherum $I \subseteq R$ ein Ideal, so ist I nach Lemma 1.3.39 der Kern der kanonischen Projektion von R auf den Quotientenring R/I, so daß zusammenfassend folgende wesentliche Beziehung zwischen Kernen von Ringhomomorphismen und Idealen ergibt:

Für einen Unterring $U \subseteq R$ sind äquivalent:

$$U \text{ ist ein Ideal} \quad \Longleftrightarrow \quad U \text{ ist Kern eines Ringhomomorphismus.}$$

(Siehe auch Bemerkung 1.2.56, die analoge Aussage aus der Gruppentheorie.)

Analog zur Gruppentheorie existiert auch in der Ringtheorie ein Homomorphie-Satz:

Satz 1.3.46. *(Homomorphie-Satz für Ringe Version I)*
Seien R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Weiter sei $I \subseteq R$ ein Ideal mit $I \subseteq \ker(\varphi)$, R/I der Quotientenring von R modulo I und $\pi_I\colon R \longrightarrow R/I$ die kanonische Projektion aus Lemma 1.3.39.
Dann gibt es genau einen Ringhomomorphismus $\xi_I\colon R/I \longrightarrow S$, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi_I"'] & S \\ R/I \arrow[ur, "\xi_I"'] & \end{tikzcd} \qquad \text{mit} \quad \varphi = \xi_I \circ \pi_I.$$

Für den Homomorphismus ξ_I gelten dabei die folgenden Äquivalenzen:

$$\xi_I \text{ injektiv} \iff \ker(\varphi) = I \qquad \text{und} \qquad \xi_I \text{ surjektiv} \iff \varphi \text{ surjektiv.}$$

Beweis.
Da $(R,+)$ und $(S,+)$ Gruppen sind, φ ein Gruppenhomomorphismus von R nach S und das Ideal $I \subseteq \ker(\varphi)$ eine Untergruppe in der abelschen Gruppe $(R,+)$ und damit ein Normalteiler, kann der Homomorphie-Satz für Gruppen in Version I (1.2.57) auf obiges Diagramm angewendet werden. Er liefert einen eindeutigen Gruppenhomomorphismus $\xi_I\colon R/I \longrightarrow S$ mit $\varphi = \xi_I \circ \pi_I$. Es bleibt zu zeigen, daß die Abbildung ξ_I auch bzgl. der Multiplikation strukturverträglich ist und damit ein Ringhomomorphismus, d.h. es muß gelten:

$$\xi_I\big((a+I)(b+I)\big) = \xi_I(a+I)\xi_I(b+I).$$

Dies folgt aus der Gleichung $\varphi = \xi_I \circ \pi_I$ und der Tatsache, daß φ und π_I Ringhomomorphismen sind:

$$\begin{aligned} \xi_I\big((a+I)(b+I)\big) &= \xi_I(ab+I) = \xi_I\big(\pi_I(ab)\big) = (\xi_I \circ \pi_I)(ab) = \varphi(ab) = \varphi(a)\varphi(b) \\ &= (\xi_I \circ \pi_I)(a) \cdot (\xi_I \circ \pi_I)(b) = \xi_I(a+I) \cdot \xi_I(b+I). \end{aligned}$$

Natürlich ist ξ_I auch ein eindeutiger Ringhomomorphismus für das kommutative Diagramm, da dies schon für den Gruppenhomomorphismus gilt.
Die Äquivalenz-Aussage über die Injektivität von ξ_I gilt nach dem Homomorphie-Satz 1.2.57 für den Gruppenhomomorphismus ξ_I, die Zusatzeigenschaft, ein Ringhomomorphismus zu sein, ändert daran nichts.
Die Äquivalenzaussage über die Surjektivität folgt auch schon aus dem Homomorphie-Satz 1.2.57, denn auch dabei spielt es keine Rolle, ob ξ_I ein Ringhomomorphismus ist. □

Wie bei den Gruppen spielt auch bei den Ringen der Homomorphie-Satz eine wesentliche Rolle und taucht in vielen Beweisen und Konstruktionen auf. Und analog zu den Gruppen soll auch hier eine weitere Version hergeleitet werden. Dazu sei ebenfalls analog zu den Gruppen (siehe Lemma 1.2.58) zuerst gezeigt:

Lemma 1.3.47. *Seien R, S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann ist das Bild $\operatorname{im}(\varphi)$ von φ ein Unterring von S.*

Beweis.
Nach Lemma 1.2.58 ist $\operatorname{im}(\varphi)$ eine Untergruppe von $(S,+)$, da φ ein Gruppenhomomorphismus zwischen den Gruppen $(R,+)$ und $(S,+)$ ist. Es bleibt nur zu zeigen, daß $\operatorname{im}(\varphi)$ abgeschlossen unter der Multiplikation ist und damit eine Unterhalbgruppe in $(S,\cdot)$. Seien dazu $b_1, b_2 \in \operatorname{im}(\varphi)$ und $a_1, a_2 \in R$ mit $\varphi(a_i) = b_i$ für $i \in \{1,2\}$. Dann folgt wie gewünscht $b_1 b_2 \in \operatorname{im}(\varphi)$:

$$b_1 b_2 = \varphi(a_1)\varphi(a_2) = \varphi(a_1 a_2) \in \operatorname{im}(\varphi). \qquad \square$$

Nun kann mit Hilfe des Homomorphie-Satzes (Version I) für Ringe die zentrale Beziehung zwischen einem Ringhomomorphismus und seinem Kern hergeleitet werden, die hier als Homomorphie-Satz Version II bezeichnet wird, da der Homomorphie-Satz (Version I) oft nur in dieser spezielleren Form formuliert wird:

Satz 1.3.48. *(Homomorphie-Satz für Ringe Version II und Folgerungen)*
Seien R und S Ringe und $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann induziert φ genau einen Ringisomorphismus ξ, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi_{\ker(\varphi)}"'] & \operatorname{im}(\varphi) \\ R/\ker(\varphi) \arrow[ur, "\xi"'] & \end{tikzcd} \qquad \textit{mit} \quad \varphi = \xi \circ \pi_{\ker(\varphi)}.$$

Die Abbildung ξ hat damit die Form:

$$\xi\colon R/\ker(\varphi) \longrightarrow \operatorname{im}(\varphi) \subseteq S \quad \textit{mit} \quad a + \ker(\varphi) \mapsto \varphi(a),$$

und liefert einen Ringisomorphismus:

$$R/\ker(\varphi) \cong \operatorname{im}(\varphi).$$

Aus dieser Fassung des Homomorphie-Satzes folgt sofort für die Fasern von φ:

$$\varphi^{-1}(b) = \begin{cases} a + \ker(\varphi) & \textit{für } b \in \operatorname{im}(\varphi) \textit{ und } a \in R \textit{ mit } \varphi(a) = b, \\ \emptyset & \textit{für } b \notin \operatorname{im}(\varphi). \end{cases}$$

Insbesondere sind die nicht-trivialen Fasern von φ also allesamt Linksnebenklassen des Kerns von φ und damit alle gleichmächtig.

Beweis.
Da $(R,+)$ und $(S,+)$ Gruppen sind und φ ein Gruppenhomomorphismus, liefert der Homomorphie-Satz für Gruppen (Version II, Satz 1.2.59) einen eindeutigen Gruppenisomorphismus ξ, der die Bedingung $\varphi = \xi \circ \ker_{\ker(\varphi)}$ erfüllt. Analog wie im Beweis des Homomorphie-Satzes für Ringe in Version I (1.3.46) für die Abbildung ξ_I kann hier für ξ sofort auf den Linksnebenklassen von $\ker(\varphi)$ nachgerechnet werden, daß ξ auch multiplikativ strukturverträglich ist:

$$\begin{aligned} \xi\big((a+I)(b+I)\big) &= \xi(ab+I) = \xi\big(\pi_{\ker(\varphi)}(ab)\big) = (\xi \circ \pi_{\ker(\varphi)})(ab) = \varphi(ab) = \varphi(a)\varphi(b) \\ &= (\xi \circ \pi_{\ker(\varphi)})(a) \cdot (\xi \circ \pi_{\ker(\varphi)})(b) = \xi(a+I) \cdot \xi(b+I). \end{aligned}$$

Somit ist ξ wie gewünscht ein Ringisomorphismus, der natürlich eindeutig ist, da dies für den Gruppenisomorphismus gilt.

Die Aussagen über die Fasern von φ folgen aus dem Homomorphie-Satz für Gruppen (Satz 1.2.59), da φ auch ein Gruppenhomomorphismus ist und seine Fasern nicht von der zusätzlichen Eigenschaft abhängen, auch ein Ringhomomorphismus zu sein. □

Bemerkung 1.3.49. *Aus dem Homomorphie-Satz für Ringe in Version II folgen für Ringhomomorphismen die analogen Aussagen wie schon für Gruppenhomomorphismen in Bemerkung 1.2.60: Die nicht-trivialen Fasern eines Ringhomomorphismus $\varphi\colon R \longrightarrow S$ sind Linksnebenklassen seines Kerns und damit alle gleichmächtig. Außerdem bilden die nicht-trivialen Fasern von φ den Quotientenring $R/\ker(\varphi)$, der isomorph zu $\operatorname{im}(\varphi)$ ist, und aus der Kenntnis von zwei der drei Ringe R, $\ker(\varphi)$ und $\operatorname{im}(\varphi)$ lassen sich über die Isomorphie $R/\ker(\varphi) \cong \operatorname{im}(\varphi)$ im Idealfall Informationen über den dritten gewinnen.* □

Beispiel 1.3.50.

i.) In Beispiel 1.3.38 wurde der Ringhomomorphismus

$$\mathcal{G}\colon \mathcal{F}_C(\mathbb{Q}) \longrightarrow \mathbb{R} \quad \textit{mit} \quad (a_i)_{i\in\mathbb{N}_0} \mapsto \textit{Grenzwert von } (a_i)_{i\in\mathbb{N}_0} \textit{ in } \mathbb{R}.$$

betrachtet, der jeder rationalen Cauchy-Folge ihren Grenzwert in $\mathbb{R}$ zuordnet. Offensichtlich sind die rationalen Nullfolgen $\mathcal{F}_N(\mathbb{Q})$ der Kern dieser Abbildung, und die Abbildung ist surjektiv, da jede reelle Zahl der Grenzwert einer rationalen Cauchy-Folge ist. Damit liefert der Homomorphie-Satz für Ringe (Version II, 1.3.48) sofort einen Ringisomorphismus:

$$\mathcal{F}_C(\mathbb{Q})/\mathcal{F}_N(\mathbb{Q}) \cong \mathbb{R},$$

d.h. der Körper der reellen Zahlen ist isomorph zum Quotientenring der rationalen Cauchy-Folgen modulo den rationalen Nullfolgen.

ii.) Der Körper der reellen Zahlen ist a priori gar nicht gegeben, sondern wird aus den rationalen Zahlen z.B. mit Hilfe von Intervallschachtelungen oder Dedekindschen Schnitten konstruiert. Obiger Isomorphismus gibt eine algebraische Möglichkeit, $\mathbb{R}$ überhaupt ersteinmal zu konstruieren: Sind nur die rationalen Zahlen gegeben und $\mathbb{R}$ noch unbekannt, kann eine Theorie konvergenter rationaler Folgen (und Null- sowie Cauchy-Folgen) durch eine ε-Konvergenz mit $\varepsilon \in \{\frac{1}{n} \mid n \in \mathbb{N}\}$ statt ε-Konvergenz mit $\varepsilon \in \mathbb{R}, \varepsilon > 0$ aufgebaut werden. Da Konvergenz von „beliebiger Nähe“ abhängt, reicht die Betrachtung der „beliebig kleinen Abstände $\frac{1}{n}$“. Alle bekannten Ergebnisse für (rationale) Folgen bleiben erhalten.

Dann kann leicht gezeigt werden, daß die rationalen Cauchy-Folgen $\mathcal{F}_C(\mathbb{Q})$ ein Ring und die Nullfolgen $\mathcal{F}_N(\mathbb{Q})$ darin ein maximales Ideal sind, so daß $\mathcal{F}_C(\mathbb{Q})/\mathcal{F}_N(\mathbb{Q})$ ein Körper ist (siehe dazu auch Bemerkung 1.3.28). Dieser Körper kann dann als der Körper der reellen Zahlen definiert werden.

Ist $\mathbb{R} := \mathcal{F}_C(\mathbb{Q})/\mathcal{F}_N(\mathbb{Q})$ konstruiert, liefert folgende Abbildung einen injektiven Körperhomomorphismus, so daß $\mathbb{Q}$ als Unterkörper von $\mathbb{R}$ aufgefaßt werden kann:

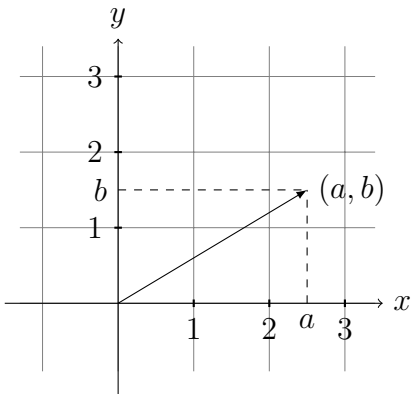
$$\mathbb{Q} \longrightarrow \mathbb{R} := \mathcal{F}_C(\mathbb{Q})/\mathcal{F}_N(\mathbb{Q}) \quad \textit{mit} \quad q \mapsto \underbrace{(q)_{i\in\mathbb{N}_0}}_{\textit{konst. Folge}} + \mathcal{F}_N(\mathbb{Q}).$$ □

KAPITEL 2

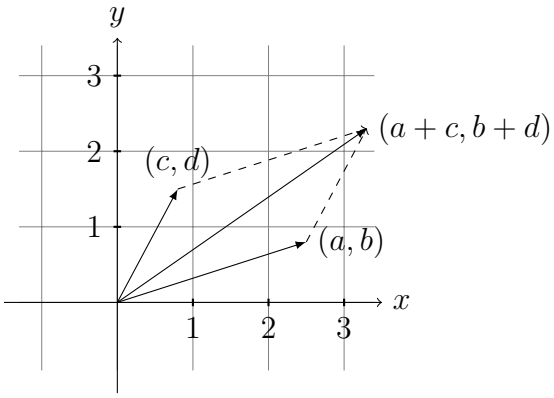
Vektorräume

2.1. Vektorräume und Moduln

Nachdem im vorherigen Kapitel algebraische Strukturen betrachtet wurden, die aus einer Menge zusammen mit einer (Halbgruppen, Monoide, Gruppen) oder zwei (Ringe, Körper) inneren Verknüpfungen konstruiert waren, stehen mit Vektorräumen und Moduln nun komplexere algebraische Strukturen im Fokus. Zur Motivation der Objekte sei folgende anschauliche und aus der Schule bekannte Situation im $\mathbb{R}^2$, der reellen Ebene, näher betrachtet:
Die Punkte des $\mathbb{R}^2 = \{ (x, y) \mid x, y \in \mathbb{R} \}$ können als Vektoren aufgefaßt und geometrisch interpretiert werden.



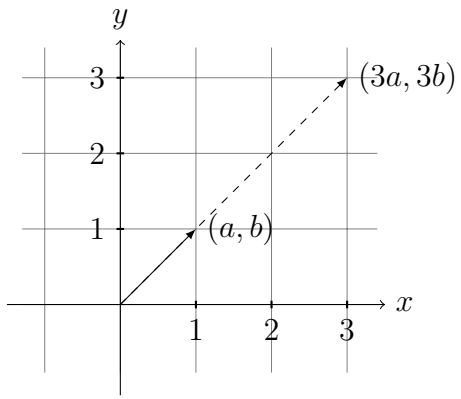
Der Vektor (a, b) kann z.B. als eine Bewegung in der Ebene aufgefaßt werden, vom Ursprung bis zu seinem durch die Koordinaten a und b gegebenen Endpunkt.
In natürlicher Weise ist eine Addition von Vektoren gegeben: algebraisch durch die komponentenweise Addition, geometrisch durch das Ansetzen des einen Vektors an den anderen (was einer Ausführung einer Bewegungen nach der anderen entspricht):



Die Vektoren des $\mathbb{R}^2$ bilden bzgl. der komponentenweisen Vektoraddition eine abelsche Gruppe:

$$+\colon \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \text{mit} \quad (a,b)+(c,d) := (a+c, b+d).$$

Das neutrale Element ist dabei der Nullvektor $(0,0)$, und der inverse Vektor zu (a,b) ist der Vektor $(-a,-b)$.
Eine natürliche geometrische Operation für Vektoren ist deren Streckung um einen Faktor:



Dies kann algebraisch folgendermaßen durch eine Verknüpfung formalisiert werden:

$$\bullet\colon \mathbb{R} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \text{mit} \quad \lambda \bullet (x,y) := (\lambda x, \lambda y).$$

Es ist offensichtlich, wie dieses Beispiel auf den $\mathbb{R}^n$ übertragen werden kann.

Definitionen und elementare Eigenschaften.

Es soll nun die vorherige Betrachtung des $\mathbb{R}^2$ verallgemeinert werden, und dabei werden folgende Erweiterungen gemacht:

- Anstelle der abelschen Gruppe $\mathbb{R}^2$ werden „Vektoren“ aus irgendeiner abelschen Gruppe zugelassen.
- Anstelle der Streckungsfaktoren aus dem Körper $\mathbb{R}$ werden Streckungsfaktoren aus einem kommutativen Ring mit Eins zugelassen.

Um eine Verknüpfung „Streckungsfaktor mal Vektor“, die im allgemeinen nicht innerhalb einer Menge stattfindet, formal zu beschreiben, wird zuerst als Erweiterung einer „inneren Verknüpfung“ auf einer Menge eine „äußere Verknüpfung“ zwischen Mengen definiert:

Definition 2.1.1. *Sind A, B und C drei nicht-leere Mengen, so heißt eine Abbildung*

$$\bullet\colon A \times B \longrightarrow C$$

äußere Verknüpfung. Es gilt dabei die gleiche Konvention für die Schreibweise wie bei einer inneren Verknüpfung (Definition 1.1.1): $a \bullet b := \bullet(a,b)$. □

Damit kann nun das obige Verallgemeinerungsprogramm des einleitenden Beispiels $\mathbb{R}^2$ formalisiert werden:

Definition 2.1.2. *(Moduln und Vektorräume, Version I)*
Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $(M, *)$ eine abelsche Gruppe. Weiter sei eine äußere Verknüpfung

$$\bullet\colon R \times M \longrightarrow M$$

gegeben, die folgende vier Bedingungen erfüllt:

$$\begin{array}{lcl} V1: & 1_R \bullet m = m & \text{für alle } m \in M. \\ V2: & r \bullet (m * n) = (r \bullet m) * (r \bullet n) & \text{für alle } r \in R,\ m, n \in M. \\ V3: & (r + s) \bullet m = (r \bullet m) * (s \bullet m) & \text{für alle } r, s \in R,\ m \in M. \\ V4: & (r \cdot s) \bullet m = r \bullet (s \bullet m) & \text{für alle } r, s \in R,\ m \in M. \end{array}$$

Dann wird M als ein R-Modul bezeichnet. Ist R sogar ein Körper, heißt M auch ein R-Vektorraum. Die Elemente aus der abelschen Gruppe M heißen dabei Vektoren und die Verknüpfung „$*$“ auch Vektoradditon, die Elemente aus dem Ring R Skalare und die äußere Verknüpfung „$\bullet$“ auch skalare Multiplikation.
Das neutrale Element der abelschen Gruppe M wird als Null bezeichnet oder auch als Nullvektor und mit dem Symbol 0 geschrieben (ebenso wie die Null im Ring R, so daß bei Verwechslungsgefahr auch 0_M und 0_R notiert wird).

Üblicherweise wird die Addition im Ring R und in der abelschen Gruppe M mit dem gleichen Symbol „$+$“ notiert, und auch für die Multiplikation im Ring und die skalare Multiplikation (äußere Verknüpfung) zwischen R und M wird normalerweise das gleiche Symbol „$\cdot$“ verwendet. Dabei tritt dann auch die Konvention aus der Definition von Ringen (Definition 1.3.1) in Kraft, das Multiplikationssymbol „$\cdot$“ oft wegzulassen und die Punkt-vor-Strich-Regelung anzuwenden. Die Bedingungen $V1$ bis $V4$ für die skalare Multiplikation schreiben sich dann folgendermaßen:

$$\begin{array}{lcl} V1: & 1_R \cdot m = m & \text{für alle } m \in M. \\ V2: & r(m + n) = rm + rn & \text{für alle } r \in R,\ m, n \in M. \\ V3: & (r + s)m = rm + sm & \text{für alle } r, s \in R,\ m \in M. \\ V4: & (rs)m = r(sm) & \text{für alle } r, s \in R,\ m \in M. \end{array}$$

□

Bemerkung 2.1.3.

i.) Moduln und Vektorräume sind nach dem gleichen Schema definiert, sie unterscheiden sich ersteinmal nur durch den verwendeten Skalarbereich: bei Moduln werden die Skalare aus Ringen genommen, bei Vektorräumen aus Körpern, also ganz speziellen Ringen. Damit sind Vektorräume spezielle Moduln, und alle Aussagen über Moduln gelten insbesondere für Vektorräume. Die Tatsache, daß in Körpern jedes Element außer der Null ein multiplikatives Inverses besitzt, hat jedoch weitreichende Folgen für die Theorie der Vektorräume im Vergleich zur Theorie von Moduln.
Bei Ringen gibt es mehrere feine Stufen von Eigenschaften, die sie besitzen können, um sie handhabbarer zu machen, und dies beinflußt stark die Möglichkeiten, die damit konstruierten Moduln zu analysieren. Solche Betrachtungen werden hier unterlassen. Im zweiten Semester wird jedoch die Theorie ganz spezieller Moduln (endlich erzeugter Moduln über Hauptidealringen) benutzt, um Vektorraumendomorphismen zu beschreiben und zu klassifizieren.

Im weiteren Verlauf dieses Semesters wird im wesentlichen die Theorie der Vektorräume vorangetrieben - allerdings werden Begriffe und Konstruktionen über Moduln definiert und ausgeführt, wenn dies keinen formalen Mehraufwand bedeutet.

ii.) *Auch in diesem Abschnitt wird in den meisten Fällen, wie bei den Ringen, allgemein üblich notiert, d.h. auf eine feine Unterscheidung bei den Verknüpfungssymbolen verzichtet. Ansonsten müßten z.B. bei zwei verschiedenen auftretenden Vektorräumen sechs verschiedene Verknüpfungssymbole genutzt werden.*

iii.) *Ist M ein R-Modul, so sind in der abelschen Gruppe M das neutrale Element und die jeweiligen Inversen eindeutig bestimmt, und Analoges gilt für den Ring R. Es gibt also genau einen Nullvektor in M.* □

Beispiel 2.1.4.

i.) *Sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Dann ist insbesondere $(R, +)$ eine abelsche Gruppe, und folgendes äußere Produkt erfüllt die Bedingungen $V1$ bis $V4$ einer skalaren Multiplikation*

$$\bullet\colon R \times R \longrightarrow R \quad \textit{mit} \quad r \bullet s := r \cdot s$$

und macht R zu einem R-Modul. Die skalare Multiplikation fällt also mit der Multiplikation im Ring zusammen (Übung!).
Insbesondere ist dann jeder Körper K mit dieser skalaren Multiplikation ein K-Vektorraum.

ii.) *Sei I eine nicht-leere Menge und R ein kommutativer Ring mit Eins. Dann ist $(R, +)$ eine abelsche Gruppe, und dadurch induziert das kartesische Produkt $\prod_{i\in I} R$ durch komponentenweise Addition ebenfalls eine abelsche Gruppe (siehe auch Satz 1.1.39 und Beispiel 1.3.3). Folgende Definition eines äußeren Produktes erfüllt die Bedingungen $V1$ bis $V4$ und macht damit $\prod_{i\in I} R$ zu einem R-Modul (Übung!):*

$$\bullet\colon R \times \prod_{i\in I} R \longrightarrow \prod_{i\in I} R \quad \textit{mit} \quad r \bullet (x_i)_{i\in I} := (r \cdot x_i)_{i\in I}.$$

Für den Spezialfall $I := \{1, \ldots, n\}$ ist dann insbesondere R^n ein R-Modul.
Für einen Körper K ist mit dieser skalaren Multiplikation $\prod_{i\in I} K$ ein K-Vektorraum, und für den Spezialfall $I := \{1, \ldots, n\}$ insbesondere K^n ein K-Vektorraum.

iii.) *Sei I eine nicht-leere Menge und $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Dann ist $R^I = \mathrm{Abb}(I, R)$ mit der Verknüpfung*

$$f \oplus g : x \mapsto f(x) + g(x)$$

eine abelsche Gruppe (siehe auch Satz 1.1.37 und Bemerkung 1.3.3), und folgende äußere Verknüpfung erfüllt die Bedingugen $V1$ bis $V4$, so daß R^I zu einem R-Modul wird:

$$\bullet\colon R \times R^I \longrightarrow R^I \quad \textit{mit} \quad r \bullet f : x \mapsto r \cdot f(x).$$

Insbesondere ist dann für einen Körper K mit dieser skalaren Multiplikation der K^I ein K-Vektorraum.

iv.) *Sei $\mathcal{C}^0(\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ die Menge aller stetigen Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$. Für stetige Abbildungen $f, g \in \mathcal{C}^0(\mathbb{R})$ ist auch $f \oplus g$ stetig, und mit $a \in \mathbb{R}$ auch $a \bullet f$ (siehe die äußere Verknüpfung im vorherigen Beispiel).*

$(\mathcal{C}^0(\mathbb{R}), \oplus)$ ist eine abelsche Gruppe, und die äußere Verknüpfung „$\bullet$“ erfüllt die Bedingungen $V1$ bis $V4$, so daß $\mathcal{C}^0(\mathbb{R})$ ein $\mathbb{R}$-Vektorraum ist.

v.) *Sei $\mathcal{D}(\mathbb{R}) \subseteq \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ die Menge aller differenzierbaren Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$. Mit $f, g \in \mathcal{D}(\mathbb{R})$ ist auch $f \oplus g$ differenzierbar, und $(\mathcal{D}(\mathbb{R}), \oplus)$ ist eine abelsche Gruppe. Mit $a \in \mathbb{R}$ ist auch $a \bullet f$ differenzierbar, und die äußere Verknüpfung „$\bullet$“ erfüllt die Bedingungen $V1$ bis $V4$, so daß $\mathcal{D}(\mathbb{R})$ ein $\mathbb{R}$-Vektorraum ist.*

vi.) *Sei $\mathcal{I}_{a,b}(\mathbb{R}) \subseteq \mathrm{Abb}([a, b], \mathbb{R})$ die Menge aller auf dem abgeschlossenen Intervall $[a, b] \subseteq \mathbb{R}$ Riemann-integrierbaren Abbildungen. Für $f, g \in \mathcal{I}_{a,b}(\mathbb{R})$ ist auch $f \oplus g$ Riemann-integrierbar und $(\mathcal{I}_{a,b}(\mathbb{R}), \oplus)$ eine abelsche Gruppe. Mit $a \in \mathbb{R}$ ist auch $a \bullet f$ Riemann-integrierbar, und die äußere Verknüpfung „$\bullet$“ erfüllt die Bedingungen $V1$ bis $V4$, so daß $\mathcal{I}_{a,b}(\mathbb{R})$ ein $\mathbb{R}$-Vektorraum ist.*

vii.) *Sei M eine nicht-leere Menge. Dann ist $\big(\mathcal{P}(M), \ominus\big)$ eine abelsche Gruppe (siehe Beispiel 1.3.3 und Aufgabenblatt 3, Aufgabe 4), und folgende äußere Verknüpfung erfüllt die Bedingungen $V1$ bis $V4$, so daß $\mathcal{P}(M)$ ein $\mathbb{Z}_2$-Vektorraum ist:*

$$\bullet\colon \mathbb{Z}_2 \times \mathcal{P}(M) \longrightarrow \mathcal{P}(M) \quad \textit{mit} \quad [a]_2 \bullet A := \begin{cases} \emptyset & \textit{für } [a]_2 = [0]_2, \\ A & \textit{für } [a]_2 = [1]_2. \end{cases}$$

($\mathbb{Z}_2$ ist nach Satz 1.3.34 ein Körper.) □

In Moduln/Vektorräumen ist die Linksmultiplikation mit einem Skalar eine nützliche Abbildung:

Definition 2.1.5. *Sei M ein R-Modul, $a \in R$ und „$\bullet$“ die skalare Multiplikation. Dann ist die Linksmultiplikation l_a in M mit a definiert durch:*

$$l_a\colon M \longrightarrow M \quad \textit{mit} \quad x \mapsto a \bullet x \qquad \textit{(Kurznotation: } a \mapsto ax\textit{).}$$ □

Bemerkung 2.1.6.

i.) *Es sind bisher in drei algebraischen Strukturen Linksmultiplikationen eingeführt worden:*

1.) *In Gruppen (Definition 1.2.5). In einer Gruppe G existiert nur eine Verknüpfung, so daß die Linksmultiplikation kanonisch definiert ist. Für $a \in G$ ist die Linksmultiplikation ℓ_a mit a eine Permutation, aber i.a. kein Gruppenendomorphismus von G (Lemma 1.2.6 und Bemerkung 1.3.16).*

2.) *In Ringen (Definition 1.3.15). In einem Ring R ist für $a \in R$ die Linksmultiplikation λ_a über die Multiplikation in R definiert (also nicht über die Addition, bzgl. der R eine Gruppenstruktur hat!). λ_a ist i.a. keine Permutation von R, aber ein Gruppenendomorphismus von $(R, +)$.*

3.) *In Moduln/Vektorräumen (Definition 2.1.5). Dort ist die Linksmultiplikation über die skalare Multiplikation definiert. Die Eigenschaften der Linksmultiplikation werden im nächsten Punkt beschrieben.*

ii.) *Bei Ringen lieferte die Linksmultiplikationsabbildung (Definition 1.3.15) eine gute Interpretation/Motivation für die Distributivgesetze: für einen Ring R und $a \in R$ sorgt das Distributivgesetz $D1$ dafür, daß die Linksmultiplikation λ_a mit a ein Gruppenendomorphismus von $(R, +)$ ist, und das Distributivgesetz $D2$, daß die Zuordnung $\Lambda_R\colon R \longrightarrow \mathrm{End}(R)$ mit $a \mapsto \lambda_a$ ein Gruppenhomomorphismus (Bemerkung 1.3.16). Auch im Fall von Moduln/Vektorräumen können die*

Bedingungen $V1$ bis $V4$ an die skalare Multiplikation durch die Linksmultiplikation in ihnen veranschaulicht werden: Sei dazu ein R-Modul M gegeben. Für die abelsche Gruppe $(M,+)$ ist die Menge ihrer Gruppenendomorphismen ein Ring $\mathrm{End}(M,\oplus,\circ)$ *mit der Eins* id_M *(siehe Beispiel 1.3.3), und $V1$ bis $V4$ liefern dann folgende Eigenschaften:*

$$\begin{aligned} V1: &\quad l_{1_R} = \mathrm{id}_M\,. \\ V2: &\quad l_a \in \mathrm{End}(M) \text{ für } a \in R. \\ V3 \text{ und } V4: &\quad \Psi_R\colon R \longrightarrow \mathrm{End}(M) \text{ mit } a \mapsto l_a \text{ ist ein Ringhomomorphismus.} \end{aligned}$$

Die Abbildung Ψ_R ist also ein Ringhomomorphismus von R in den Endomorphismenring $\mathrm{End}(R)$*, der die Eins von R auf die Eins von* $\mathrm{End}(R)$ *abbildet. Offensichtlich ist l_a i.a. keine Permutation, da der Ringhomomorphismus Ψ_R die Null des Ringes auf die Nullabbildung in* $\mathrm{End}(M)$ *abbildet. Für eine Einheit $a \in R^*$ ist jedoch l_a eine Bijektion, da dann ein Inverses a^{-1} existiert und aus dem Ringhomomorphismus Ψ_R folgt:*

$$\left.\begin{aligned} l_a \circ l_{a^{-1}} &= \Psi_R(a) \circ \Psi_R(a^{-1}) = \Psi_R(aa^{-1}) = \Psi_R(1) = \mathrm{id}_M \\ &= \Psi_R(a^{-1}a) = \Psi_R(a^{-1} \circ \Psi_R(a) = l_{a^{-1}} \circ l_a \end{aligned}\right\} \overset{0.4.15}{\Longrightarrow} l_a \text{ Bijektion.}$$

iii.) In einem K-Vektorraum V ist für jedes $a \in K$ mit $a \neq 0$ die Linksmultiplikation l_a ein Automorphismus von V, da die Abbildung nach obigen Betrachtungen ein Endomorphismus von V ist und a eine Einheit.

iv.) Im $\mathbb{Z}$-Modul $\mathbb{Z}_2$ (mit $z \bullet [a]_2 := [za]_2$) ist die Linksmultiplikation l_2 die Nullabbildung, obwohl 2 in $\mathbb{Z}$ kein Nullteiler ist. □

Die Aussage aus Bemerkung 2.1.6, daß die skalare Multiplikation eines R-Moduls M einen Ringhomomorphismus von R in den Endomorphismenring $\mathrm{End}(M)$ via Linksmultiplikation induziert, führt zu einer alternativen, äquivalenten Definition von Moduln und Vektorräumen, die zwar abstrakter ist, aber dafür sehr kompakt und für tiefere Betrachtungen sehr nützlich:

Definition 2.1.7. *(Moduln und Vektorräume, Version II)*
Sei R ein kommutativer Ring mit Eins und M eine abelsche Gruppe. Ein Ringhomomorphismus

$$\Psi_R\colon R \longrightarrow \mathrm{End}(M) \quad \text{mit} \quad \Psi_R(1_R) = \mathrm{id}_M$$

heißt Modulstruktur auf M, und M dann R-Modul. Ist R sogar ein Körper, so heißt M auch R-Vektorraum. □

Bemerkung 2.1.8.

i.) Sei M ein R-Modul mit der Modulstruktur

$$\Psi_R\colon R \longrightarrow \mathrm{End}(M) \quad \text{mit} \quad \Psi_R(1_R) = \mathrm{id}_M\,.$$

Die Modulstruktur Ψ_R induziert dann eine äußere Verknüpfung:

$$\bullet_{\Psi_R}\colon R \times M \longrightarrow M \quad \text{mit} \quad r \bullet_{\Psi_R} m := \Psi_R(r)(m),$$

welche die Bedingungen $V1$ bis $V4$ der skalaren Multiplikation aus Definition 2.1.2 erfüllt. Dabei gilt:

$$\begin{aligned} \Psi_R(1_R) = \mathrm{id}_M \quad &\Longrightarrow \quad V1. \\ \Psi_R(r) \in \mathrm{End}(M) \quad &\Longrightarrow \quad V2. \end{aligned}$$

$$\Psi_R \text{ Ringhomomorphismus} \quad \Longrightarrow \quad V3 \text{ und } V4.$$

ii.) *Durch die Definition von Moduln/Vektorräumen in Version II können sehr effizient Moduln/Vektorräume kreiert werden. Sind z.B. R und S kommutative Ringe mit Eins und ist $\varphi\colon R \longrightarrow S$ ein Ringhomomorphismus mit $\varphi(1_R) = 1_S$, so induziert φ via der Linksmultiplikation im Ring S (Definition 1.3.15) einen Ringhomomorphismus*

$$\Psi\colon R \longrightarrow \mathrm{End}(S) \quad \text{mit} \quad r \mapsto \lambda_{\varphi(r)},$$

mit $\Psi(1_R) = \mathrm{id}_S$: Nach Bemerkung 1.3.16 ist $\lambda_s \in \mathrm{End}(S)$ für alle $s \in S$, und es folgt mit den weiteren Aussagen aus Bemerkung 1.3.16:

$$\Psi(r_1 + r_2) = \lambda_{\varphi(r_1+r_2)} = \lambda_{\varphi(r_1)+\varphi(r_2)} = \lambda_{\varphi(r_1)} \oplus \lambda_{\varphi(r_2)} = \Psi(r_1) \oplus \Psi(r_2).$$
$$\Psi(r_1 r_2) = \lambda_{\varphi(r_1 r_2)} = \lambda_{\varphi(r_1)\varphi(r_2)} = \lambda_{\varphi(r_1)} \circ \lambda_{\varphi(r_2)} = \Psi(r_1) \circ \Psi(r_2).$$

Somit ist Ψ ein Ringhomomorphismus, und es gilt auch

$$\Psi(1_R) = \lambda_{\varphi(1_R)} = \lambda_{1_S} = \mathrm{id}_S\,.$$

Dadurch wird S zu einem R-Modul. □

Beispiel 2.1.9.

i.) *Ist S ein kommutativer Ring mit Eins und $R \subseteq S$ ein Unterring mit Eins (dieser ist offensichtlich auch kommutativ), so ist folgende Einbettung ein Ringhomomorphismus:*

$$i\colon R \longrightarrow S \quad \text{mit} \quad r \mapsto r.$$

Dies induziert nach Bemerkung 2.1.8 einen Ringhomomorphismus

$$\Psi\colon R \longrightarrow \mathrm{End}(S) \quad \text{mit} \quad r \mapsto \lambda_{i(r)},$$

und S ist damit ein R-Modul. Die skalare Multiplikation ist darin nach Bemerkung 2.1.8 gegeben durch $r \bullet s := \Psi(r)(s)$. Aus $i(r) = r$ folgt $\lambda_{i(r)} = \lambda_r$ und damit für die skalare Multiplikation

$$r \bullet s = \Psi(r)(s) = \lambda_r(s) = rs.$$

Damit entspricht die skalare Multiplikation zwischen Unterring R (Skalare) und Oberring S (Vektoren) der Multiplikation im Ring S.
Diese Konstruktion liefert insbesondere für einen Körper K mit einem Unterkörper $L \subseteq K$, daß K ein L-Vektorraum ist, also z.B. $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum.

ii.) *Obige Konstruktion kann natürlich auch durch die direkte Angabe einer äußeren Verknüpfung angegeben werden: Ist S ein kommutativer Ring mit Eins und $R \subseteq S$ ein Unterring mit Eins, so liefert folgende Definition eine äußere Verknüpfung, welche die Bedingungen $V1$ bis $V4$ erfüllt und damit S zu einem R-Vektorraum macht (Übung!):*

$$\bullet\colon R \times S \longrightarrow S \quad \text{mit} \quad r \bullet s := rs.$$

iii.) *Sei $(G, *)$ eine abelsche Gruppe und $\big(\mathrm{End}(G), \circledast, \circ\big)$ der Ring der Gruppenendomorphismen von G (Beispiel 1.3.3). Für $n \in \mathbb{Z}$ ist die Abbildung ρ_n mit $\rho_n(g) := g^n$ ein Gruppenendomorphismus (Beispiel 1.2.40). Die Zuordnung*

$$\Psi_G\colon \mathbb{Z} \longrightarrow \mathrm{End}(G) \quad \text{mit} \quad n \mapsto \rho_n$$

ist ein Ringhomomorphismus mit $\Psi_G(1) = \mathrm{id}_G$ (Aufgabenblatt 6, Aufgabe 4 und Aufgabenblatt 8, Aufgabe 4), so daß G damit ein $\mathbb{Z}$-Modul ist. □

Es sollen nun einige Rechengesetze für Moduln und Vektorräume hergeleitet werden. Dabei gilt immer, daß Regeln für Moduln immer auch für Vektorräume gelten, da die Vektorräume Moduln mit besonderen Skalaren sind (aus einem Körper, also einem speziellen Ring).
Die Umkehrung davon gilt natürlich nicht! Wenn in einem Beweis einer Aussage über Vektorräume benutzt wird, daß Skalare (ungleich der Null) multiplikative Inverse besitzten, was in Körpern immer gilt, aber nicht unbedingt in Ringen, dann kann diese Aussage nicht allgemein auf Moduln übertragen werden.

Lemma 2.1.10. *Sei M ein R-Modul (was auch Vektorräume umfaßt). Dann gelten folgende Aussagen:*

i.) $0_R \cdot m = 0_M$ *für alle* $m \in M$.
ii.) $r \cdot 0_M = 0_M$ *für alle* $r \in R$.
iii.) $(-1_R) \cdot m = -m$ *für alle* $m \in M$.

Ist R ein Körper und M damit ein Vektorraum, so gilt zusätzlich zu den allgemeinen Aussagen i.) bis iii.) für $r \in R$ und $m \in M$:

$$r \cdot m = 0_M \quad \Longrightarrow \quad r = 0_R \text{ oder } m = 0_M.$$

Beweis.
Beim Beweis der Aussagen *i.*) bis *iii.*) werden nur Eigenschaften der verwendeten Skalare genutzt, die in allen kommutativen Ringen mit Eins gelten, und damit gelten *i.*) bis *iii.*) auch in allen Moduln.
Beim Beweis der letzten Aussage wird die Existenz von multiplikativen Inversen gebraucht, so daß als Skalarbereich ein Körper nötig ist und damit die Aussage nur in Vektorräumen gilt.

i.) Zu dem Vektor $0_R \cdot m \in M$ existiert ein Inverses $-(0_R \cdot m)$, und es folgt mit $V3$:

$$0_R \cdot m = (0_R + 0_R) \cdot m \overset{(V3)}{=} 0_R \cdot m + 0_R \cdot m \overset{-(0_R \cdot m)}{\Longrightarrow} 0_R \cdot m = 0_M.$$

ii.) Zu dem Vektor $r \cdot 0_M \in M$ existiert ein Inverses $-(r \cdot 0_M)$, und es folgt mit $V2$:

$$r \cdot 0_M = r \cdot (0_M + 0_M) \overset{(V2)}{=} r \cdot 0_M + r \cdot 0_M \overset{-(r \cdot 0_M)}{\Longrightarrow} r \cdot 0_M = 0_M.$$

iii.) Aus $0_R \cdot m = 0_M$ und $V3$ folgt

$$0_M = 0_R \cdot m = \big(1_R + (-1_R)\big) \cdot m \overset{(V3)}{=} 1_R \cdot m + (-1_R) \cdot m = m + (-1_R) \cdot m,$$

und wegen der Eindeutigkeit von Inversen in M und $0_M = m + (-1_R) \cdot m$ gilt dann $-m = (-1_R) \cdot m$.

Sei R nun ein Körper und $r \cdot m = 0_M$. Ist $r \neq 0$, so ist $m = 0_M$ zu zeigen. Dazu wird ausgenutzt, daß in einem Körper jedes Element außer der Null eine Einheit ist und deshalb für $r \neq 0$ ein Inverses r^{-1} mit $r^{-1} \cdot r = 1_R$ existiert. Damit folgt dann:

$$m \overset{(V1)}{=} 1_R \cdot m = (r^{-1} \cdot r) \cdot m \overset{(V4)}{=} r^{-1} \cdot \underbrace{(r \cdot m)}_{=0_M} \overset{(ii)}{=} 0_M. \qquad \square$$

Bemerkung 2.1.11.

i.) Die Aussagen i.) bis iii.) gelten selbstverständlich in jedem Vektorraum, da Vektorräume Moduln über speziellen Ringen, nämlich Körpern, sind.
Die letzte Aussage ist nur in Vektorräumen allgemeingültig, denn z.B. im $\mathbb{Z}$-Modul $\mathbb{Z}_2$ gilt: $2 \in \mathbb{Z}$ ist nicht Null, $[1]_2 \in \mathbb{Z}_2$ ist nicht der Nullvektor, aber $2 \cdot [1]_2 = [2]_2 = [0]_2$.

ii.) Die Aussagen i.) bis iii.) haben große Ähnlichkeit zu den Aussagen in Lemma 1.3.4 und Lemma 1.3.6, wo die Beziehung zwischen den beiden inneren Verknüpfungen in einem Ring betrachtet wurden. Hier werden jedoch immer „Produkte“ zwischen Skalaren und Vektoren gebildet, d.h. es wird die äußere Verknüpfung im Modul/Vektorraum untersucht. □

Untervektorräume, Nebenklassen und Quotientenvektorräume.

Definition 2.1.12. *Sei M ein R-Modul. Eine nicht-leere Teilmenge $U \subseteq M$ heißt Untermodul, falls U eine Untergruppe von M ist und die skalare Multiplikation von R und M auf U eingeschränkt werden kann, d.h. für $r \in R$ und $u \in U$ auch $ru \in U$ gilt (dann heißt U auch abgeschlossen unter der skalaren Multiplikation). Ist R sogar ein Körper und damit M ein Vektorraum, so heißt ein Untermodul auch Untervektorraum.* □

Analog zum Untergruppenkriterium in Lemma 1.2.3 gibt es auch für Moduln/Vektorräume einen einfachen Test, um für eine Teilmenge zu überprüfen, ob sie eine Unterstruktur ist:

Lemma 2.1.13. *Sei M ein R-Modul und $U \subseteq M$ eine nicht-leere Teilmenge. Dann gilt:*

$$U \text{ Untermodul} \quad \Longleftrightarrow \quad au + bv \in U \text{ für alle } a, b \in R \text{ und } u, v \in U.$$

Dies umfaßt dann den Fall, daß R ein Körper und M ein R-Vektorraum ist, und es läßt sich in diesem Fall formulieren:

$$U \text{ Untervektorraum} \quad \Longleftrightarrow \quad au + bv \in U \text{ für alle } a, b \in R \text{ und } u, v \in U.$$

Beweis.
Der folgende Beweis benutzt wieder nur Eigenschaften der Skalare, die in allen kommutativen Ringen mit Eins gelten - multiplikative Inverse von Skalaren, die nur in Körpern vorausgesetzt werden können, treten nicht auf:

„$\Longrightarrow$“: Wegen der Abgeschlossenheit von U unter der skalaren Multiplikation gilt $au, bv \in U$, und da U eine Untergruppe ist, liegt auch deren Verknüpfung $au + bv$ in U.

„$\Longleftarrow$“: Nach dem Untergruppenkriterium (1.2.3) ist U genau dann eine Untergruppe von M, wenn für alle $u, v \in U$ auch $u - v \in U$ gilt. Mit $a := 1_R$ und $b := -1_R$ folgt dies aber wegen $-1_R \cdot v = -v$ (Lemma 2.1.10) und der Voraussetzung $au + bv \in U$ für alle $a, b \in R$, $u, v \in U$.
Es bleibt zu zeigen, daß U unter der skalaren Multiplikation abgeschlossen ist: für $u \in U$ und $a \in R$ folgt aber mit $b := 0_R$ aus Lemma 2.1.10 mit der Voraussetzung:

$$au = au + 0_M \overset{(2.1.10)}{=} au + bu \in U.$$ □

Beispiel 2.1.14.

i.) *Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann ist nach Beispiel 2.1.4 der R^n ein R-Modul mit der Vektoradditon:*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

und der skalaren Multiplikation:

$$r \cdot (x_1, \ldots, x_n) := (rx_1, \ldots, rx_n).$$

Das Untermodulkriterium (Lemma 2.1.13) liefert sofort, daß folgende offensichtlich nicht-leere Menge dann ein Untermodul ist (Übung!):

$$U := \{\, (x_1, \ldots, x_n) \mid \sum_{i=1}^{n} x_i = 0 \,\}.$$

Selbstverständlich gilt die Aussage auch für einen Körper R, wo R^n dann sogar ein Vektorraum und U ein Untervektorraum ist.

ii.) *Ist R ein kommutativer Ring mit Eins, und wird wieder der R-Modul R^n betrachtet ($n \in \mathbb{N}$), so liefert das Untermodulkriterium für eine beliebige Teilmenge $J \subseteq \{1, \ldots, n\}$ sofort, daß folgende offensichtlich nicht-leere Menge ein Untermodul ist (Übung!):*

$$U := \{\, (x_1, \ldots, x_n) \mid x_j = 0 \text{ für } j \in J \,\}.$$

Selbstverständlich gilt die Aussage auch für einen Körper R, wo R^n dann sogar ein Vektorraum und U ein Untervektorraum ist.

iii.) *Nach Beispiel 2.1.4 sind $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ und $\mathcal{C}^0(\mathbb{R})$ (Menge der stetigen Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$) jeweils $\mathbb{R}$-Vektorräume. Da $\mathrm{id}_{\mathbb{R}}$ stetig ist, gilt $\emptyset \neq \mathcal{C}^0(\mathbb{R})$. Weil für stetige Abbildungen $f, g \in \mathcal{C}^0(\mathbb{R})$ und $\alpha, \beta \in \mathbb{R}$ auch $\alpha \cdot f + \beta \cdot g$ stetig ist, liefert das Untervektorraumkriterium (2.1.13) sofort, daß $\mathcal{C}^0(\mathbb{R})$ ein Untervektorraum von $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ ist.* □

Mit Hilfe von Untermoduln bzw. Untervektorräumen sollen nun wieder Quotientenkonstruktionen durchgeführt werden. Ist dazu M ein R-Modul und $U \subseteq M$ ein Untermodul, so ist vor allem $(U, +)$ eine Untergruppe in der abelschen Gruppe $(R, +)$ und damit ein Normalteiler - was natürlich auch im Fall eines Vektorraumes M und eines Untervektorraumes $U \subseteq M$ gilt. Dann ist schon eine Zerlegung von M in Linksnebenklassen $x + U$ von U definert, und die Menge der Linksnebenklassen M/U von U ist bei repräsentantenweiser Verknüpfung

$$(x + U) \oplus (y + U) := (x + y) + U$$

eine abelsche Gruppe (Satz 1.2.29). Im R-Modul M existiert schon eine skalare Multiplikation, und es liegt nahe, diese skalare Multiplikaton auf Nebenklassen zu übertragen, indem das r-fache einer Linksnebenklasse $x + U$ als Linksnebenklasse $(rx) + U$ des r-fachen des Repräsentanten definiert wird:

$$r \bullet (x + U) := (rx) + U.$$

Dabei stellt sich, wie üblich bei Konstruktionen auf Repräsentanten von Linksnebenklassen, die Frage, ob diese Definition mit einem Repräsentantenwechsel verträglich ist, ob also gilt:

$$x + U = y + U \quad \overset{?}{\Longrightarrow} \quad (rx) + U = (ry) + U.$$

Bei Gruppen und Ringen traten Probleme bei Quotientenkonstruktionen auf, wenn eine beliebige Unterstruktur (Untergruppe bzw. Unterring) gewählt wurde, und es konnen nur Unterstrukturen mit speziellen zusätzlichen Eigenschaften verwendet werden (Normalteiler bzw. Ideale). Im Falle von Moduln und Vektorräumen wird dieses Problem nicht auftauchen, wie folgender Satz zeigt - jeder Untermodul bzw. Untervektorraum ermöglicht eine Quotientenkonstruktion:

Satz 2.1.15. *Sei M ein R-Modul und $U \subseteq M$ ein Untermodul. Weiter sei M/U die Menge der Linksnebenklassen $x+U$ von U, und $(M/U, \oplus)$ die Quotientengruppe bzgl. des Normalteilers U in der abelschen Gruppe $(M,+)$ mit der Verknüpfung*

$$(x+U) \oplus (y+U) := (x+y)+U. \qquad \text{(siehe Satz 1.2.29)}$$

Dann ist folgende äußere Verknüpfung wohldefiniert:

$$\bullet\colon R \times (M/U) \longrightarrow M/U \quad \textit{mit} \quad r \bullet (x+U) := (rx)+U,$$

und sie erfüllt die Bedingungen $V1$ bis $V4$ aus Definition 2.1.2, so daß M/U damit zu einem R-Modul wird. M/U wird auch als Quotientenmodul von M und U bezeichnet.

Dies umfaßt wieder den Fall, daß R sogar ein Körper und damit M ein Vektorraum und U ein Untervektorraum ist: in diesem Fall ist M/U sogar ein Vektorraum, der sogenannte Quotientenvektorraum von M und U.

Beweis.

„ $\bullet$ wohldefiniert: Zu zeigen ist:

$$x+U = y+U \quad \Longrightarrow \quad (rx)+U = (ry)+U.$$

Wegen $x+U = y+U$ gilt $x \in y+U$ und somit $x = y+u$ für ein $u \in U$. Da U als Untermodul abgeschlossen ist unter der skalaren Multiplikation, gilt $ru \in U$ für jedes $r \in R$, und dann folgt mit Lemma 1.2.17 die Gleichung $(ru)+U = U$. Dies liefert dann zusammengefaßt:

$$(rx)+U = \big(r(y+u)\big)+U = (ry+ru)+U = \big((ry)+U\big) \oplus \big(\underbrace{(ru)+U}_{=U}\big) = (ry)+U,$$

da U das neutrale Element in der Quotientengruppe M/U ist.

$V1$ bis $V4$: Diese Bedingungen gelten alle für den R-Modul M, und da in M/U die Linksnebenklassen von U mit Repräsentanten aus M beschrieben und verknüpft werden, übertragen sich alle Aussagen sofort von der skalaren Multiplikation bzgl. M auf die äußere Verknüpfung bzgl. M/U:

$$\begin{aligned}
V1: \quad & 1_R \bullet (x+U) = (1_R \cdot x)+U = x+U. \\
V2: \quad & r \bullet \big((x+U) \oplus (y+U)\big) = r \bullet \big((x+y)+U\big) = \big(r(x+y)\big)+U \\
& = (rx+ry)+U = \big((rx)+U\big) \oplus \big((ry)+U\big) \\
& = \big(r \bullet (x+U)\big) \oplus \big(r \bullet (y+U)\big). \\
V3: \quad & (r+s) \bullet (x+U) = \big((r+s)x\big)+U = (rx+sx)+U \\
& = \big((rx)+U\big) \oplus \big((sx)+U\big) \\
& = \big(r \bullet (x+U)\big) \oplus \big(s \bullet (x+U)\big).
\end{aligned}$$

$$V4: \qquad (rs) \bullet (x+U) = \big((rs)x\big) + U = \big(r(sx)\big) + U = r \bullet (sx+U) = r \bullet \big(s \bullet (x+U)\big).$$

Auch in diesem Beweis wurde für die Skalare nie gebraucht, daß sie ein multiplikatives Inverses besitzen, und somit gilt die Aussage für alle Moduln und Vektorräume. □

Lineare Abbildungen.

Es sollen nun Homomorphismen zwischen Moduln bzw. Vektorräumen betrachtet werden. Ein R-Modul M ist dabei eine algebraische Struktur, in der eine abelsche Gruppe M und ein Ring R durch eine skalare Multiplikation $R \times M \longrightarrow M$ verwoben sind. Für einen R-Modul M und einen S-Modul N ist dann die Frage, was überhaupt aufeinander abgebildet werden soll: Die Vektoren aus M auf die Vektoren aus N, oder die Skalare aus R auf die Skalare aus S, oder Vektoren aus M *und* Skalare aus R auf Vektoren aus N *und* Skalare aus S?

$$M \xrightarrow{?} N, \quad R \xrightarrow{?} S, \quad R, M \xrightarrow{?} S, N.$$

Das folgende Beispiel zeigt, daß Vektoren und Skalare in einem Modul/Vektorraum so verschiedene Objekte sein können, daß eine Abbildungsvorschrift für ein Objekt sicher nichts für das andere impliziert:

> Sei dazu die nicht-leere Menge $X := \mathcal{F}(\mathbb{R}) := \prod_{i \in \mathbb{N}_0} \mathbb{R}$ aller reellen Folgen betrachtet und deren Potenzmenge $\mathcal{P}(X)$. Diese ist nach (Beispiel 2.1.4) ein $\mathbb{Z}_2$-Vektorraum. Ein Vektor ist in diesem Fall also eine Teilmenge von X und damit eine Menge von reellen Folgen. Ein Skalar ist eine Linksnebenklasse der Untergruppe $\langle\, 2 \,\rangle \subseteq \mathbb{Z}$.

Tatsächlich sind bei einem R-Modul/Vektorraum M die Vektoren aus M die wesentlichen Elemente, die Skalare aus R werden nur als Streckungsfaktoren von ihnen aufgefaßt. Daher soll eine Abbildung zwischen Moduln/Vektorräumen nur die Vektoren aufeinander abbilden, die Skalare haben zuersteinmal mit der Abbildung nichts zu tun. Für einen R-Modul M und einen S-Modul N soll ein Homomorphismus also ein Element von $\mathrm{Abb}(M, N)$ sein:

$$\varphi \colon M \longrightarrow N$$

Homomorphismen sind dann wie bei Gruppen und Ringen auch bei Moduln/Vektorräumen wieder die strukturverträglichen Abbildungen, wobei die Strukturverträglichkeit hier konzeptionell erweitert werden muß: Die Vektoren bilden eine abelsche Gruppe, und für diese soll φ dann ein Gruppenhomomorphismus sein, d.h. es soll wieder das schon eingeführte Prinzip gelten:

$$\text{erst verknüpfen, dann abbilden} \quad \Longleftrightarrow \quad \text{erst abbilden, dann verknüpfen}$$
$$\rightsquigarrow \qquad \varphi(a+b) = \varphi(a) + \varphi(b).$$

Bezüglich der Streckungen mit Skalaren soll dann folgende einleuchtende Strukturverträglichkeitsregel gelten:

$$\text{erst strecken, dann abbilden} \quad \Longleftrightarrow \quad \text{erst abbilden, dann strecken}$$
$$\rightsquigarrow \qquad \varphi(\lambda a) = \lambda \varphi(a).$$

Nun stellt sich noch die Frage, ob bei zwei Moduln M und N deren Skalare (Streckungsfaktoren) überhaupt in verschiedenen Ringen liegen dürfen, wenn eine strukturelle Beziehung zwischen den Moduln bestehen soll. Die kurze Antwort darauf ist nein! Es wären zwar durchaus sinnvolle Konstruktionen denkbar, dann aber nur für spezielle Fälle von Skalarbereichen, die in gewisser Beziehung zu einander stehen - und dies soll hier nicht vertieft werden.

Im folgenden werden nur Moduln/Vektorräume aufeinander abgebildet, wenn sie den gleichen Skalarbereich haben!

Dies führt dann zu folgenden Definitionen:

Definition 2.1.16. *Sei $(R, +, \cdot)$ ein Ring, und seien $(M, *)$ und $(N, \star)$ jeweils R-Moduln mit äußeren Verknüpfungen:*

$$\bullet\colon R \times M \longrightarrow M \qquad \text{und} \qquad \diamond\colon R \times N \longrightarrow N.$$

Eine Abbildung $\varphi\colon M \longrightarrow N$ heißt R-Modulhomomorphismus, wenn sie ein Gruppenhomomorhpsismus von $(M, *)$ nach $(N, \star)$ ist und sich mit Streckungen bzgl. Skalaren aus R verträgt, d.h. es sollen gelten:

$$\begin{aligned} \varphi(a * b) &= \varphi(a) \star \varphi(b) && \text{für alle } a, b \in M, && \text{(Gruppenhomomorphismus)} \\ \varphi(\lambda \bullet a) &= \lambda \diamond \varphi(a) && \text{für alle } \lambda \in R,\ a \in M. && \text{(streckungsverträglich)} \end{aligned}$$

Üblicherweise werden in Moduln nur die Verknüpfungssymbole „$+$“ (für die Addition im Ring/Körper und der abelschen Gruppe) und „$\cdot$“ (für die Multiplikation im Ring/Körer und die skalare Multiplikation) genutzt und das Multiplikationszeichen „$\cdot$“ sogar meist nicht notiert, so daß sich obige Bedingungen an einen Modulhomomorphismus dann schreiben als:

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b) && \text{für alle } a, b \in M, && \text{(Gruppenhomomorhphismus)} \\ \varphi(\lambda a) &= \lambda \varphi(a) && \text{für alle } \lambda \in R,\ a \in M. && \text{(streckungsverträglich)} \end{aligned}$$

Ist R ein Körper, und sind M, N somit Vektorräume, so wird φ auch als Vektorraumhomomorphismus bezeichnet. Ein Modul- bzw. Vektorraumhomorphismus heißt auch R-lineare Abbildung.
Entsprechend den Bezeichnungsregeln aus Definition 1.2.38 werden injektive, surjektive und bijektive Homomorphismen jeweils als Mono-, Epi- und Isomorphismen bezeichnet, und sind Defininitionsbereich und Wertebreich gleich, so Homomorphismen als Endomorphismen und Isomorphismen als Automorphismen (siehe auch Bemerkung 1.2.39).
Die Menge aller R-Modul- bzw. Vektorraumhomomorphismen von M nach N wird mit $\mathrm{Hom}_R(M, N)$ bezeichnet, und für den R-Modul/Vektorraum M die Menge aller Endomorphismen mit $\mathrm{End}_R(M)$ und die Menge aller Automorphismen mit $\mathrm{Aut}_R(M)$. Die Menge $\mathrm{Aut}_R(M)$ trägt üblicherweise die Bezeichnung $\mathrm{GL}_R(M)$ und heißt die allgemeine lineare Gruppe von M („GL“ von „general linear group“) - wobei erst später bewiesen wird, daß die Menge $\mathrm{GL}_R(M)$ tatsächlich eine Gruppe ist!
Zwei R-Moduln/Vektorräume M, N heißen isomorph, falls es einen Isomorphismus $\varphi\colon M \longrightarrow N$ gibt, und dies wird bezeichnet durch:

$$M \cong N. \qquad \square$$

Bemerkung 2.1.17.

i.) *Seien M, N Moduln/Vektorräume über dem Ring/Körper R, und $\varphi\colon M \longrightarrow N$ sei eine lineare Abbildung. Dann ist φ insbesondere ein Gruppenhomomorphismus von $(M,+)$ nach $(N,+)$, und es folgt aus Lemma 1.2.51:*

$$\varphi(0_M) = 0_N \quad \textit{und} \quad \varphi(-x) = -\varphi(x) \textit{ für alle } x \in M.$$

ii.) *Sind M und N Moduln/Vektorräume über dem Ring/Körper R, so ist eine lineare Abbildung $\varphi \in \mathrm{Hom}_R(M,N)$ insbesondere auch ein Gruppenhomomorphismus zwischen den abelschen Gruppe $(M,+)$ und $(N,+)$, d.h. $\varphi \in \mathrm{Hom}(M,N)$, so daß folgt:*

$$\mathrm{Hom}_R(M,N) \subseteq \mathrm{Hom}(M,N).$$

iii.) *Sei R ein kommutativer Ring mit Eins (damit kann R auch ein Körper sein). Dann ist nach Beispiel 2.1.4 R ein R-Modul (und falls R ein Körper ist, ein R-Vektorraum), wenn als skalare Multiplikation die Ringmultiplikation gewählt wird. In diesem Fall ist die Menge $\mathrm{End}_R(R)$ aller Modul-/Vektoraumendomorphismen leicht zu bestimmen, denn es gilt für $\varphi \in \mathrm{End}_R(R)$ und $x \in R$:*

$$\varphi(x) = \varphi(x \cdot 1) \overset{(\varphi \text{ linear})}{=} x\varphi(1) \overset{(R \text{ komm})}{=} \varphi(1)x = ax \textit{ mit } a := \varphi(1).$$

Also ist jede lineare Abbildung von R nach R von der Form $x \mapsto ax$ für ein bestimmtes $a \in R$ (a das Bild der Eins unter der linearen Abbildung).
Andererseits ist für jedes $a \in R$ die Abbildung $x \mapsto ax$ von R nach R offensichtlich linear:

$$a(x+y) \overset{(\text{Distr. D1})}{=} ax + ay \qquad \textit{und} \qquad a(rx) \overset{(R \text{ komm})}{=} r(ax).$$

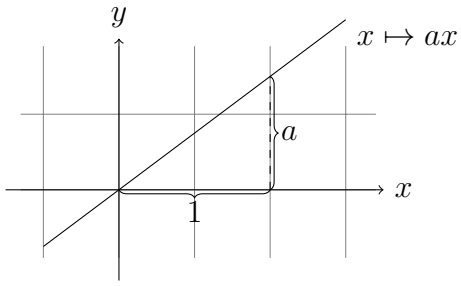
Dies ergibt zusammengefaßt:

$$\mathrm{End}_R(R) = \{\, x \mapsto ax \mid a \in R \,\}.$$

iv.) *Nach vorherigem Beispiel ist der Körper $\mathbb{R}$ ein Vektorraum über sich selbst, und die Menge aller linearen Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$ ist von der Form*

$$\mathrm{End}_{\mathbb{R}}(\mathbb{R}) = \{\, x \mapsto ax \mid a \in \mathbb{R} \,\} \subseteq \mathrm{Abb}(\mathbb{R},\mathbb{R}).$$

Der Graph der Abbildung $x \mapsto ax$ ist eine Ursprungsgerade mit der Steigung a:



v.) *Ist R ein kommutativer Ring mit Eins, so trägt die Menge R drei natürliche algebraische Strukturen:*
- *$(R,+)$ ist eine abelsche Gruppe.*
- *$(R,+,\cdot)$ ist ein kommutativer Ring mit Eins.*
- *R ist ein R-Modul (mit dem Ringprodukt als skalarer Multiplikation).*

Für die jeweiligen Endomorphismenmengen gilt:

$$\underbrace{\mathrm{End}_R(R)}_{\textit{lineare Abbildungen}} \subseteq \underbrace{\mathrm{End}(R)}_{\textit{Gruppenhom.}} \qquad \textit{und} \qquad \underbrace{\mathrm{End}_{Ring}(R)}_{\textit{Ringhom.}} \subseteq \underbrace{\mathrm{End}(R).}_{\textit{Gruppenhom.}}$$

Die Frage ist, wie sich Ringendomorphismen von R zu R-linearen Abbildungen auf R verhalten. Dabei gilt:

$$\begin{aligned} \varphi \in \mathrm{End}_{Ring}(R) \quad &\Longrightarrow \quad \varphi(ab) = \varphi(a)\varphi(b) \quad \textit{für alle } a, b \in R, \\ \varphi \in \mathrm{End}_R(R) \quad &\Longrightarrow \quad \varphi(ab) = a\varphi(b) \qquad \textit{für alle } a, b \in R. \end{aligned}$$

Die Menge $\mathrm{End}_R(R)$ wurde oben schon beschrieben, und es gilt:

$$\mathrm{End}_R(R) = \{\, x \mapsto ax \mid a \in R \,\},$$

und die Frage ist, welche dieser Abbildungen auch ein Ringhomomorphismus sein kann. Ist $x \mapsto ax$ ein Ringhomomorphismus, so folgt:

$$a = a \cdot 1 = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) = a \cdot 1 \cdot a \cdot 1 = a^2.$$

Die Bedingung $a^2 = a$ ist auch hinreichend dafür, daß $x \mapsto ax$ ein Ringhomomorphismus ist, und es folgt (Übung!):

$$\mathrm{End}_{Ring}(R) \cap \mathrm{End}_R(R) = \{x \mapsto ax \mid a \in R \textit{ mit } a^2 = a\,\}.$$

Über die Bedingung $a^2 = a$ läßt sich leicht zeigen (Übung!):

$$a^2 = a \qquad \Longrightarrow \qquad a = 0 \quad \textit{oder} \quad a = 1 \quad \textit{oder} \quad a \textit{ Nullteiler.}$$

Die obige Aussage ist keine Äquivalenz, denn z.B. in $\mathbb{Z}_4$ ist $[2]_4$ zwar ein Nullteiler, aber es gilt nicht $([2]_4)^2 = [2]_4$.
Ist R dann ein Integritätsring (d.h. nullteilerfrei), was insbesondere Körper umfaßt, so gilt:

$$\mathrm{End}_{Ring}(R) \cap \mathrm{End}_R(R) = \{\bar{0}, \mathrm{id}_R\}.$$

Im Ring $\mathbb{Z}_6$ (mit Nullteilern) dagegen gilt:

$$\{\, a \in \mathbb{Z}_6 \mid a^2 = a \,\} = \{[0]_6, [1]_6, [3]_6, [4]_6\}. \qquad \square$$

Beispiel 2.1.18.

i.) Für R-Moduln M und N sind folgende Abbildungen linear (Übung!):

$$\mathrm{id}_M \colon M \longrightarrow M \quad \textit{mit} \quad x \mapsto x \qquad \textit{und} \qquad \bar{0} \colon M \longrightarrow N \quad \textit{mit} \quad x \mapsto 0_N.$$

ii.) Es sei $[a, b] \subseteq \mathbb{R}$ ein abgeschlossenes Intervall und $\mathcal{I}_{a,b}(\mathbb{R})$ der $\mathbb{R}$-Vektorraum aller Riemann-integrierbaren Abbildungen (Beispiel 2.1.4). Es sei folgende Abbildung betrachtet:

$$I \colon \mathcal{I}_{a,b} \longrightarrow \mathbb{R} \quad \textit{mit} \quad f \mapsto \int_a^b f(x)\, dx.$$

$\mathbb{R}$ ist ebenfalls ein $\mathbb{R}$-Vektorraum, und die obige Abbildung I ist linear, denn es gilt für $f, g \in \mathcal{I}_{a,b}(\mathbb{R})$ und $\alpha \in \mathbb{R}$:

$$\begin{aligned} I(f+g) &= \int_a^b (f+g)(x)\, dx = \int_a^b f(x)\, dx + \int_a^b g(x)\, dx = I(f) + I(g), \\ I(\alpha f) &= \int_a^b \alpha f(x)\, dx = \alpha \int_a^b f(x)\, dx = \alpha I(f). \end{aligned}$$

iii.) Im Beispiel 2.1.4 wurden der folgende $\mathbb{R}$-Vektorraum betrachtet:

$$\mathcal{D}(\mathbb{R}) := \{\, f\colon \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ differenzierbar} \,\}.$$

Die Ableitung f' einer differenzierbaren Abbildung $f \in \mathcal{D}(\mathbb{R})$ ist eine Abbildung aus $\mathrm{Abb}(\mathbb{R},\mathbb{R})$, welches auch wieder ein $\mathbb{R}$-Vektorraum ist (ebenfalls Beispiel 2.1.4). Für $f, g \in \mathcal{D}(\mathbb{R})$ und $\alpha \in \mathbb{R}$ gelten die Ableitungsregeln:

$$(f+g)' = f' + g' \quad \text{und} \quad (\alpha f)' = \alpha f',$$

so daß folgende Abbildung $\mathbb{R}$-linear ist:

$$D\colon \mathcal{D}(\mathbb{R}) \longrightarrow \mathrm{Abb}(\mathbb{R},\mathbb{R}) \quad \text{mit} \quad f \mapsto f'.$$

iv.) Es werden in $\mathcal{D}(\mathbb{R})$ folgende Untervektorräume (Übung!) betrachtet:

Für $n \in \mathbb{N}$: $\mathcal{C}^n(\mathbb{R}) := \{\, f\colon \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ } n\text{-mal stetig differenzierbar} \,\}$,

$\mathcal{C}^\infty(\mathbb{R}) := \{\, f\colon \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ unendlich oft stetig differenzierbar} \,\}$.

Dies ergibt insbesondere folgende unendliche Kette von Untervektorräumen:

$$\mathcal{C}^\infty(\mathbb{R}) \subseteq \ldots \subseteq \mathcal{C}^2(\mathbb{R}) \subseteq \mathcal{C}^1(\mathbb{R}) \subseteq \mathcal{C}^0(\mathbb{R}).$$

Die Ableitungsabbildung ist dann für jedes $n \in \mathbb{N}$ eine $\mathbb{R}$-lineare Abbildung

$$D\colon \mathcal{C}^n(\mathbb{R}) \longrightarrow \mathcal{C}^{n-1}(\mathbb{R}) \quad \text{mit} \quad f \mapsto f',$$

und es ergibt sich folgende Sequenz von Vektorräumen und linearen Abbildungen:

$$\ldots \xrightarrow{D} \mathcal{C}^n(\mathbb{R}) \xrightarrow{D} \mathcal{C}^{n-1}(\mathbb{R}) \xrightarrow{D} \ldots \xrightarrow{D} \mathcal{C}^1(\mathbb{R}) \xrightarrow{D} \mathcal{C}^0(\mathbb{R}).$$

Strenggenommen müßte jeder Abbildung D hier ein Index verpaßt werden, denn die Definitionsbereiche und Wertebereiche ändern sich ja ständig. Wird D jedoch immer als Einschränkung der Ableitungsabbildung von $\mathcal{D}(\mathbb{R})$ nach $\mathrm{Abb}(\mathbb{R},\mathbb{R})$ aufgefaßt, ist klar, was gemeint ist. □

Ein wesentliches Beispiel für Modul/Vektorraumhomomorphismen ist das folgende:

Lemma 2.1.19. *Sei R ein kommutativer Ring mit Eins, und es seien $n, m \in \mathbb{N}$. Weiter seien $a_{i,j} \in R$ gegeben für $1 \le i \le m$ und $1 \le j \le n$ (also insgesamt $n \cdot m$ Elemente aus R). Dann ist die folgende zwischen den R-Moduln R^n und R^m gegebene Abbildung R-linear:*

$$\varphi\colon R^n \longrightarrow R^m \quad \text{mit} \quad (x_1, \ldots, x_n) \mapsto \Big(\sum_{k=1}^n a_{1,k} x_k, \ldots, \sum_{i=1}^n a_{m,k} x_k \Big).$$

Beweis.
Für $x, y \in R^n$ und $r \in R$ sind folgende Gleichungen zu verifizieren:

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{und} \quad \varphi(rx) = r\varphi(x).$$

$\varphi(x+y) = \varphi(x) + \varphi(y)$: Da $x, y \in R^n$ Vektoren mit n Komponenten aus R sind und deren Addition komponentenweise in R erfolgt, ergibt sich sofort aus den Rechengesetzen in R:

$$\begin{aligned}\varphi\big((x_1, \ldots, x_n) + (y_1, \ldots, y_n)\big) &= \varphi\big((x_1 + y_1, \ldots, x_n + y_n)\big) \\ &= \Big(\sum_{k=1}^n a_{1,k}(x_k + y_k), \ldots, \sum_{k=1}^n a_{m,k}(x_k + y_k) \Big)\end{aligned}$$

$$
\begin{aligned}
&= \Big(\sum_{k=1}^{n}(a_{1,k}x_k + a_{1,k}y_k), \ldots, \sum_{k=1}^{n}(a_{m,k}x_k + a_{m,k}y_k)\Big) \\
&= \Big(\sum_{k=1}^{n} a_{1,k}x_k + \sum_{k=1}^{n} a_{1,k}y_k, \ldots, \sum_{k=1}^{n} a_{m,k}x_k + \sum_{k=1}^{n} a_{m,k}y_k\Big) \\
&= \Big(\sum_{k=1}^{n} a_{1,k}x_k, \ldots, \sum_{k=1}^{n} a_{m,k}x_k\Big) + \Big(\sum_{k=1}^{n} a_{1,k}y_k, \ldots, \sum_{k=1}^{n} a_{m,k}y_k\Big) \\
&= \varphi\big((x_1, \ldots, x_n)\big) + \varphi\big((y_1, \ldots, y_n)\big).
\end{aligned}
$$

$\varphi(rx) = r\varphi(x)$: Da Vektoren aus R^n bzw. R^m mit einem Skalar $r \in R$ komponentenweise in R multipliziert werden, folgt auch hier der Beweis aus den Rechengesetzen in R, insbesondere aus der Kommutativität von R, die $ra = ar$ für $r, a \in R$ liefert:

$$
\begin{aligned}
\varphi\big(r(x_1, \ldots, x_n)\big) &= \varphi\big((rx_1, \ldots, rx_n)\big) \\
&= \Big(\sum_{k=1}^{n} a_{1,k}(rx_k), \ldots, \sum_{k=1}^{n} a_{m,k}(rx_k)\Big) \\
&= \Big(\sum_{k=1}^{n} r(a_{1,k}x_k), \ldots, \sum_{k=1}^{n} r(a_{m,k}x_k)\Big) \\
&= \Big(r \cdot \sum_{k=1}^{n} a_{1,k}x_k, \ldots, r \cdot \sum_{k=1}^{n} a_{m,k}x_k\Big) \\
&= r \cdot \Big(\sum_{k=1}^{n} a_{1,k}x_k, \ldots, \sum_{k=1}^{n} a_{m,k}x_k\Big) \\
&= r\varphi\big((x_1, \ldots, x_n)\big).
\end{aligned}
$$

□

Beispiel 2.1.20. *Lemma 2.1.19 sei durch folgendes kleines Beispiel illustriert, wo eine lineare Abbildung von $\mathbb{R}^3$ nach $\mathbb{R}^2$ konstruiert sei (d.h. $n := 3$ und $m := 2$) mit*

$$a_{1,1} := 1, \quad a_{1,2} := -2, \quad a_{1,3} := 3, \quad a_{2,1} := 3, \quad a_{2,2} := 0, \quad a_{2,3} := -1.$$

Dann hat die lineare Abbildung φ die Form:

$$\varphi\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad (x_1, x_2, x_3) \mapsto (x_1 - 2x_2 + 3x_3,\ 3x_1 - x_3).$$

□

Ein weiteres Beispiel für einen Modulhomomorphismus ist die Übertragung von Lemma 1.2.43 bzw. Lemma 1.3.39 auf Moduln/Vektorräume:

Lemma 2.1.21. .
Sei M ein R-Modul und $U \subseteq M$ ein Untermodul. Dann ist die kanonische Projektion von M auf den Quotientenmodul M/U (siehe Satz 2.1.15) eine R-lineare Abbildung:

$$\pi_U\colon M \longrightarrow M/U \quad \textit{mit} \quad x \mapsto x + U.$$

Beweis.
Die Abbildung π_U ist nach Lemma 1.2.43 schon ein Gruppenhomomorphismus der additiven Gruppen beider Moduln, und aus der Defnition der Linksnebenklassenrechnung in Satz 2.1.15 ergibt sich auch direkt die Strukturverträglichkeit bzgl. der skalaren Multiplikation:

$$\pi_U(rx) \overset{\text{(Def)}}{=} (rx) + U = r \bullet (x + U) \overset{\text{(Def)}}{=} r \bullet \pi_U(x). \qquad \square$$

Als nächstes wird betrachtet, wie sich lineare Abbildungen bzgl. der Kompositionsverknüpfung verhalten (siehe dazu auch den analogen Satz 1.2.48 für Gruppen oder Satz 1.3.40 für Ringe):

Satz 2.1.22. *Seien M, N und L Moduln/Vektorräume über dem Ring/Köper R mit den linearen Abbildungen:*

$$\varphi\colon M \longrightarrow N \qquad \text{und} \qquad \psi\colon N \longrightarrow L.$$

Dann ist die Komposition $\psi\circ\varphi$ eine lineare Abbildung von M nach L. Insbesondere ist dann die Menge $\operatorname{End}_R(M)$ abgeschlossen unter der Komposition von Abbildungen und $\big(\operatorname{End}_R(M), \circ\big)$ ein Untermonoid von $\big(\operatorname{Abb}(M, M), \circ\big)$ mit dem neutralen Element id_M.

Ist φ bijektiv, so ist auch die (mengentheoretische) Umkehrabbildung φ^{-1} eine lineare Abbildung. Insbesondere ist dann $\big(\operatorname{GL}_R(M), \circ\big)$ eine Untergruppe des Monoides $\big(\operatorname{End}_R(M), \circ\big)$ und der Gruppe $\big(S(M), \circ\big)$.

Beweis.

$\psi \circ \varphi$ lineare Abbildung: Nach Satz 1.2.48 ist $\psi \circ \varphi$ schon ein Gruppenhomomorphismus, so daß nur noch die Strukturverträglichkeit bzgl. der skalaren Multiplikation überprüft werden muß. Für $r \in R$ und $x \in M$ gilt dazu:

$$(\psi \circ \varphi)(rx) = \psi\big(\varphi(rx)\big) \overset{(\varphi\text{ lin.})}{=} \psi\big(r\varphi(x)\big) \overset{(\psi\text{ lin.})}{=} r\psi\big(\varphi(x)\big) = r(\psi \circ \varphi)(x).$$

Damit ist $\psi\circ\varphi$ eine lineare Abbildung, und insbesondere $\operatorname{End}_R(M)$ abgeschlossen unter der Komposition von Abbildungen.
$\big(\operatorname{Abb}(M, M), \circ\big)$ ist nach Lemma 1.1.36 ein (nicht-kommutativer) Monoid mit dem neutralen Element id_M, und id_M ist eine lineare Abbildung (Beispiel 2.1.18). Damit ist $\big(\operatorname{End}_R(M), \circ\big)$ eine Halbgruppe und wegen $\operatorname{id}_M \in \operatorname{End}_R(M)$ sogar ein Untermonoid von $\big(\operatorname{Abb}(M, M), \circ\big)$ mit dem neutralen Element id_M.

φ^{-1} lineare Abbildung: Nach Satz 1.2.48 ist φ^{-1} ein Gruppenhomomorphismus, und es muß nur gezeigt werden, daß dieser auch mit der skalaren Multiplikation verträglich ist. Sei dazu $y \in N$ und $r \in R$. Es gibt dann wegen der Bijektivität von φ ein eindeutig bestimmtes Elemente $x \in R$ mit

$$\varphi(x) = y \qquad \Longrightarrow \qquad x = \varphi^{-1}(y),$$

und es folgt:

$$\varphi^{-1}(ry) = \varphi^{-1}\big(r\varphi(x)\big) \overset{(\varphi\text{ lin.})}{=} \varphi^{-1}\big(\varphi(rx)\big) \overset{\text{(Umkehrabb)}}{=} rx = r\varphi^{-1}(y).$$

Damit ist φ^{-1} sogar eine lineare Abbildung.
Die Menge $\operatorname{GL}_R(M)$ ist abgeschlossen unter der Komposition, da die Komposition von linearen Abbildungen wieder eine lineare Abbildung liefert (siehe oben), und die Komposition bijektiver Abbildungen wieder bijketiv ist (Lemma 0.4.11). Da

die Identität id_M in $\mathrm{GL}_R(M)$ liegt, ist $\big(\mathrm{GL}_R(M), \circ\big)$ sogar ein Monoid, und da für jedes $\varphi \in \mathrm{GL}_R(M)$ eine Umkehrabbildung φ^{-1} existiert (Satz 0.4.15) und diese auch eine lineare Abbildung ist (siehe oben), hat jedes Element aus $\mathrm{GL}_R(M)$ ein Inverses bzgl. der Komposition und $\big(\mathrm{GL}_R(M), \circ\big)$ ist eine Gruppe.
Offensichtlich gilt $\mathrm{GL}_R(M) \subseteq \mathrm{End}_R(M)$ und $\mathrm{GL}_R(M) \subseteq S(M)$. □

Für zwei Gruppen G und H ist auf der Menge ihrer Gruppenhomomorphismen $\mathrm{Hom}(G, H)$ eine Verknüpfung über die Verknüpfung im Wertebereich H definiert, falls $(H, *)$ eine abelsche Gruppe ist:

$$(\varphi \circledast \psi)\colon G \longrightarrow H \quad \text{mit} \quad g \mapsto \varphi(g) * \psi(g). \qquad \text{(siehe Satz 1.2.49)}$$

Bei Ringen R und S ist diese Konstruktion für $\mathrm{Hom}_{\mathrm{Ring}}(R, S)$ nicht immer möglich, da die von $(S, +, \cdot)$ induzierte Multiplikaton „ $\odot$ “ auf keine innere Verknüpfung auf $\mathrm{Hom}_{\mathrm{Ring}}(R, S)$ sein muß, d.h. für $\psi, \varphi \in \mathrm{Hom}_{\mathrm{Ring}}(R, S)$ ist $\varphi \odot \psi$ nicht unbedingt ein Ringhomomorphismus von R nach S (siehe das Gegenbeispiel in Bemerkung 1.3.41). Im Falle von Moduln/Vektorräumen kann jedoch wieder analog zum Fall der Gruppen auf der Menge der linearen Abbildungen (Homomorphismen) über die Verknüpfung im Wertebereich eine Verknüpfung auf den Abbildungen definiert werden:

Satz 2.1.23. *Seien M, N Moduln/Vektorräume über dem Ring/Körper R. Weiter sei $\big(\mathrm{Hom}(M, N), \oplus\big)$ die in Satz 1.2.49 betrachtete abelsche Gruppe mit*

$$\varphi \oplus \psi\colon M \longrightarrow N \quad \textit{mit} \quad x \mapsto \varphi(x) + \psi(x).$$

Für zwei lineare Abbildungen $\varphi, \psi \in \mathrm{Hom}_R(M, N)$ ist dann auch $\varphi \oplus \psi$ eine lineare Abbildung von M nach N, und die Teilmenge $\mathrm{Hom}_R(M, N) \subseteq \mathrm{Hom}(M, N)$ damit abgeschlossen bzgl. der Verknüpfung „$\oplus$“.
Das neutrale Element $\bar{0}\colon M \longrightarrow N$ mit $x \mapsto 0_N$ aus $\mathrm{Hom}(M, N)$ ist auch eine lineare Abbildung, so daß $\big(\mathrm{Hom}(M, N), \oplus\big)$ ein Monoid ist.
Für ein $\varphi \in \mathrm{Hom}_R(M, N) \subseteq \mathrm{Hom}(M, N)$ sei $\psi \in \mathrm{Hom}(M, N)$ die Inverse Abbildung bzgl. der Verknüpfung „$\oplus$“. Dann ist auch ψ eine lineare Abbildung von M nach N, d.h. $\psi \in \mathrm{Hom}_R(M, N)$.
Zusammenfassend gilt dann:
$\big(Hom_R(M, N), \oplus\big)$ ist ein abelsche Untergruppe von $\big(\mathrm{Hom}(M, N), \oplus\big)$.
Insbesondere ist dann wegen $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ auch $\big(\mathrm{End}_R(M), \oplus\big)$ eine abelsche Gruppe.

Beweis.

$\varphi \oplus \psi$ lineare Abbildung: Die Abbildung $\varphi \oplus \psi$ ist nach Satz 1.2.49 schon ein Gruppenhomomorphismus von $(M, +)$ nach $(N, +)$, und es ist zu zeigen, daß sie auch strukturerhaltend bzgl. der skalaren Multiplikation ist. Dies folgt für $x \in M$ und $r \in R$ schon aus der Linearität von φ und ψ:

$$\begin{aligned}(\varphi \oplus \psi)(rx) &\overset{\text{(Def)}}{=} \varphi(rx) + \psi(rx) \overset{(\varphi,\psi\text{ lin.})}{=} r\varphi(x) + r\psi(x) \overset{\text{(V2)}}{=} r\big(\varphi(x) + \psi(x)\big)\\ &\overset{\text{(Def)}}{=} r\big((\varphi \oplus \psi)(x)\big).\end{aligned}$$

$\bar{0}$ lineare Abbildung: Beispiel 2.1.18.

ψ lineare Abbildung: Nach der Definition aus Satz 1.1.37 gilt für $x \in M$:

$$\psi(x) := -\varphi(x),$$

und nach Satz 1.2.49 ist dies auch ein Gruppenhomomorphismus von $(M,+)$ nach $(N,+)$. Zu zeigen ist noch, daß ψ auch strukturerhaltend bzgl. der skalaren Multiplikation ist. Dazu sei für $r \in R$ und $x \in M$ betrachtet:

$$\begin{aligned}\psi(rx) &\overset{\text{(Def)}}{=} -\varphi(rx) \overset{(\varphi\text{ lin.})}{=} -\big(r\varphi(x)\big) \overset{\text{(Lem 2.1.10)}}{=} (-1_R)\big(r\varphi(x)\big)\\ &\overset{\text{(V4)}}{=} r\big((-1_R)\varphi(x)\big) \overset{\text{(Lem 2.1.10)}}{=} r\big(-\varphi(x)\big) \overset{\text{(Def)}}{=} r\psi(x).\end{aligned}$$

Da nun für jedes $\varphi \in \mathrm{Hom}_R(M,N)$ auch das Inverse bzgl. der Verknüpfung „ $\oplus$ “ in $\mathrm{Hom}_R(M,N)$ liegt, ist $\big(\mathrm{Hom}_R(M,N),\oplus\big)$ eine Gruppe.

Nach Satz 1.1.37 überträgt sich die Kommutativität der Verknüpfung „ $+$ “ in der abelschen Gruppe $(N,+)$ auf die Verknüpfung „ $\oplus$ “, so daß $\big(\mathrm{Hom}_R(M,N),\oplus\big)$ sogar eine abelsche Gruppe ist. □

Insbesondere ergibt sich aus den bisherigen Strukturaussagen von Modul-/Vektorraumendomorphismen:

Lemma 2.1.24. *Sei M ein R-Modul/Vektorraum. Dann ist $\big(\mathrm{End}_R(M),\oplus,\circ\big)$ ein Ring mit der Eins id_M, der sogenannte Endomorphismenring des R-Moduls/Vektorraumes M.*

Beweis.
Nach Beispiel 1.3.3 ist $\big(\mathrm{End}(M),\oplus,\circ\big)$ ein Ring mit der Eins id_M (die Gruppenendomorphismen von $(M,+)$). Nach Satz 2.1.23 ist $\big(\mathrm{End}_R(M),\oplus\big)$ eine abelsche Untergruppe von $\big(\mathrm{End}(M),\oplus\big)$, und nach Satz 2.1.22 $\big(\mathrm{End}_R(M),\circ\big)$ ein Untermonoid von $\big(\mathrm{End}(M),\circ\big)$ mit dem neutralen Element id_M, so daß dann $\big(\mathrm{End}_R(M),\oplus,\circ\big)$ nach Definition 1.3.20 ein Unterring von $\big(\mathrm{End}(M),\oplus,\circ\big)$ ist mit der Eins id_M. □

Für zwei R-Moduln/Vektorräume M und N läßt sich auf der abelschen Gruppe $\mathrm{Hom}_R(M,N)$ mit Hilfe der skalaren Multiplikation auf N eine skalare Multiplikation definieren, so daß $\mathrm{Hom}_R(M,N)$ sogar zu einem R-Modul/Vektorraum wird:

Satz 2.1.25. *Seien M, N Moduln/Vektorräume über dem Ring/Körper R. Dann ist mit Hilfe der skalaren Multiplikation zwischen R und M eine skalare Multiplikaton definiert:*

$$\bullet\colon R \times \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(M,N) \quad \textit{mit} \quad (r,\varphi) \mapsto r \bullet \varphi,$$

mit

$$r \bullet \varphi\colon M \longrightarrow N \quad \textit{mit} \quad x \mapsto r\varphi(x).$$

Damit ist $\mathrm{Hom}_R(M,N)$ ein R-Modul/Vektorraum.

Beweis.
Es sind die Bedingungen $V1$ bis $V4$ für eine skalare Multiplikation nachzuprüfen (Definition 2.1.2):

$$\begin{aligned}V1:\quad & (1_R \bullet \varphi)(x) \overset{\text{(Def)}}{=} 1_R\varphi(x) \overset{(V1\text{ in }N)}{=} \varphi(x)\\ & \Longrightarrow \quad 1_R \bullet \varphi = \varphi.\\ V2:\quad & \big(r \bullet (\varphi \oplus \psi)\big)(x) \overset{\text{(Def)}}{=} r\big((\varphi \oplus \psi)(x)\big) \overset{\text{(Def }\oplus)}{=} r\big(\varphi(x) + \psi(x)\big)\\ & \overset{(V2\text{ in }N)}{=} r\varphi(x) + r\psi(x)\end{aligned}$$

$$\overset{(\text{Def})}{=} (r \bullet \varphi)(x) + (r \bullet \psi)(x) \overset{(\text{Def } \oplus)}{=} \big((r \bullet \varphi) \oplus (r \bullet \psi)\big)(x)$$
$$\Longrightarrow \quad r \bullet (\varphi \oplus \psi) = (r \bullet \varphi) \oplus (r \bullet \psi).$$

$$V3: \quad \big((r+s) \bullet \varphi\big)(x) \overset{(\text{Def})}{=} (r+s)\varphi(x) \overset{(V3 \text{ in } N)}{=} r\varphi(x) + s\varphi(x)$$
$$\overset{(\text{Def})}{=} (r \bullet \varphi)(x) + (s \bullet \varphi)(x) \overset{(\text{Def } \oplus)}{=} \big((r \bullet \varphi) \oplus (s \bullet \varphi)\big)(x)$$
$$(r+s) \bullet \varphi = (r \bullet \varphi) \oplus (s \bullet \varphi).$$

$$V4: \quad \big((rs) \bullet \varphi\big)(x) \overset{(\text{Def})}{=} (rs)\varphi(x) \overset{(V4 \text{ in } N)}{=} r\big(s\varphi(x)\big) \overset{(\text{Def})}{=} r\big((s \bullet \varphi)(x)\big)$$
$$\overset{(\text{Def})}{=} \big(r \bullet (s \bullet \varphi)\big)(x)$$
$$\Longrightarrow \quad (rs) \bullet \varphi = r \bullet (s \bullet \varphi).$$

Da $\big(\operatorname{Hom}_R(M,N), \oplus\big)$ eine abelsche Gruppe ist (Satz 2.1.23), wird $\operatorname{Hom}_R(M,N)$ mit obiger skalarer Multiplikation zu einem R-Modul/Vektorraum. □

Auch bei Modul-/Vektorraumhomomorphismen ist analog zu Gruppenhomomorphismen und Ringhomomorphismen der Kern des Homomorphismus ein wesentliches Objekt zu dessen Analyse. Da Moduln auch abelsche Gruppen sind und lineare Abbildungen Gruppenhomomorphismen, für die schon ein Kern definiert ist, wird festgelegt:

Definition 2.1.26. *Seien M, N Moduln/Vektorräume über dem Ring/Körper R, und sei $\varphi\colon M \longrightarrow N$ eine lineare Abbildung. Dann ist der Kern von φ definiert als:*

$$\ker(\varphi) := \{\, x \in M \mid \varphi(x) = 0_N \,\}.$$ □

Da der Kern eines Modulhomomorphismus $\varphi\colon M \longrightarrow N$ gleich dem Kern des Gruppenhomomorphismus $\varphi\colon (M,+) \longrightarrow (N,+)$ ist, kann folgende Aussage direkt aus Lemma 1.2.53 übernommen werden:

Lemma 2.1.27. *Für Ringe M, N Moduln/Vektorräume über dem Ring/Körper R und eine linearen Abbildung $\varphi\colon M \longrightarrow N$ gilt:*

$$\varphi \text{ injektiv} \quad \Longleftrightarrow \quad \ker(\varphi) = \{0_M\}.$$ □

Bei Gruppenhomomorphismen und Ringhomomorphismen waren deren Kerne jeweils Unterstrukturen (Untergruppen und Unterringe), und sogar jeweils spezielle, denn es waren genau diejenigen Unterstrukturen, mit denen Quotientenkonstruktionen durchgeführt werden konnten (also Normalteiler und Ideale). Im Fall von Moduln/Vektorräumen sind Quotientenkonstruktionen mit jedem Untermodul/-Vektorraum möglich, so daß auch für den Kern einer linearen Abbildung nur das Ergebnis zu erwarten ist, daß er ein Untermodul/-Vektorraum ist:

Lemma 2.1.28. *Seien M und N Moduln/Vektorräume über dem Ring/Körper R, und sei $\varphi\colon M \longrightarrow N$ eine lineare Abbildung. Dann ist $\ker(\varphi)$ ein Untermodul/Untervektorraum in M.*

Beweis.
Nach dem Untermodulkriterium in Lemma 2.1.13 ist für $a, b \in R$ und $u, v \in \ker(\varphi)$ zu zeigen, daß auch $au + bv$ in $\ker(\varphi)$ liegt:

$$\varphi(au + bv) = \varphi(au) + \varphi(bv) = a\underbrace{\varphi(u)}_{=0_N} + b\underbrace{\varphi(v)}_{=0_N} = 0_N \quad \Longrightarrow \quad au + bv \in \ker(\varphi). \quad \square$$

Analog zur Gruppen- und Ringtheorie existiert auch in der Modul-/Vektorraumtheorie ein Homomorphie-Satz:

Satz 2.1.29. *(Homomorphie-Satz für Moduln und Vektorräume Version I)*
Seien M, N Moduln/Vektorräume über dem Ring/Körper R und $\varphi\colon M \longrightarrow N$ eine lineare Abbildung. Weiter sei $U \subseteq M$ ein Untermodul/-Vektorraum mit $U \subseteq \ker(\varphi)$, M/U der Quotientenmodul/-Vektorraum von M modulo U und $\pi_U\colon M \longrightarrow M/U$ die kanonische Projektion aus Lemma 2.1.21.
Dann gibt es genau eine lineare Abbildung $\xi_U\colon M/U \longrightarrow N$, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi_U"'] & N \\ M/U \arrow[ur, "\xi_U"'] & \end{tikzcd} \qquad \text{mit} \quad \varphi = \xi_U \circ \pi_U.$$

Für die lineare Abbildung ξ_U gelten dabei die folgenden Äquivalenzen:

$$\xi_U \text{ injektiv} \iff \ker(\varphi) = U \qquad \text{und} \qquad \xi_U \text{ surjektiv} \iff \varphi \text{ surjektiv.}$$

Beweis.
Da $(M, +)$ und $(N, +)$ Gruppen sind, φ ein Gruppenhomomorphismus von M nach N und der Untermodul $U \subseteq \ker(\varphi)$ eine Untergruppe in der abelschen Gruppe $(M, +)$ und damit ein Normalteiler, kann der Homomorphie-Satz für Gruppen in Version I (1.2.57) auf obiges Diagramm angewendet werden. Er liefert einen eindeutigen Gruppenhomomorphismus $\xi_U\colon M/U \longrightarrow N$ mit $\varphi = \xi_U \circ \pi_U$. Es bleibt zu zeigen, daß die Abbildung ξ_U auch bzgl. der skalaren Multiplikation strukturverträglich ist und damit eine lineare Abbildung, d.h. es muß gelten:

$$\xi_U\big(r(x + U)\big) = r\big(\xi_U(x + U)\big).$$

Dies folgt aus der Gleichung $\varphi = \xi_U \circ \pi_U$ und der Tatsache, daß φ und π_U lineare Abbildungen sind:

$$\begin{aligned} \xi_U\big(r(x + U)\big) &= \xi_U(rx + U) = \xi_U\big(\pi_U(rx)\big) = (\xi_U \circ \pi_U)(rx) = \varphi(rx) = r\varphi(x) \\ &= r(\xi_U \circ \pi_U)(x) = r\big(\xi_U(x + U)\big). \end{aligned}$$

Natürlich ist ξ_U auch eine eindeutige lineare Abbildung für das kommutative Diagramm, da dies schon für den Gruppenhomomorphismus gilt.
Die Äquivalenz-Aussage über die Injektivität von ξ_U gilt nach dem Homomorphie-Satz 1.2.57 für den Gruppenhomomorphismus ξ_U, die Zusatzeigenschaft, eine lineare Abbildung zu sein, ändert daran nichts.
Die Äquivalenzaussage über die Surjektivität folgt auch schon aus dem Homomorphie-Satz 1.2.57, denn auch dabei spielt es keine Rolle, ob ξ_U zusätzlich eine lineare Abbildung ist. $\square$

Wie bei den Gruppen und Ringen spielt auch bei den Moduln/Vektorräumen der Homomorphie-Satz eine wesentliche Rolle und taucht in vielen Beweisen und Konstruktionen auf. Und analog zu den Gruppen und Ringen soll auch hier eine weitere Version hergeleitet werden. Dazu sei ebenfalls analog zu den Gruppen (siehe Lemma 1.2.58) und Ringen (siehe Lemma 1.3.47) zuerst gezeigt:

Lemma 2.1.30. *Seien M, N Moduln/Vektorräume über dem Ring/Körper R und $\varphi\colon M \longrightarrow N$ eine lineare Abbildung. Dann ist das Bild $\operatorname{im}(\varphi)$ von φ ein Untermodul/Untervektorraum von N.*

Beweis.
Nach dem Untermodulkriterium 2.1.13 muß für $u, v \in \operatorname{im}(\varphi)$ und $a, b \in R$ gezeigt werden, daß $au + bv$ in $\operatorname{im}(\varphi)$ liegt. Seien dazu $x, y \in M$ mit $\varphi(x) = u$ und $\varphi(y) = v$. Dann folgt wie gewünscht aus der Linearität von φ:

$$au + bv = a\varphi(x) + b\varphi(y) = \varphi(ax) + \varphi(by) = \varphi(ax + by) \in \operatorname{im}(\varphi). \qquad \square$$

Nun kann mit Hilfe des Homomorphie-Satzes (Version I) für Moduln/Vektorräume die zentrale Beziehung zwischen einer linearen Abbildung und ihrem Kern hergeleitet werden, die hier als Homomorphie-Satz Version II bezeichnet wird, da der Homomorphie-Satz (Version I) oft nur in dieser spezielleren Form formuliert wird:

Satz 2.1.31. *(Homomorphie-Satz für Moduln und Vektorräume Version II und Folgerungen)*
Seien M und N Moduln/Vektorräume über dem Ring/Körper R und $\varphi\colon M \longrightarrow N$ eine lineare Abbildung. Dann induziert φ genau einen Modul-/Vektorraum-Isomorphismus ξ, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi_{\ker(\varphi)}"'] & \operatorname{im}(\varphi) \\ M/\ker(\varphi) \arrow[ur, "\xi"'] & \end{tikzcd} \qquad \textit{mit} \quad \varphi = \xi \circ \pi_{\ker(\varphi)}.$$

Die Abbildung ξ hat damit die Form:

$$\xi\colon M/\ker(\varphi) \longrightarrow \operatorname{im}(\varphi) \subseteq N \quad \textit{mit} \quad x + \ker(\varphi) \mapsto \varphi(x),$$

und liefert eine Modul-/Vektorraum-Isomorphismus:

$$M/\ker(\varphi) \cong \operatorname{im}(\varphi).$$

Aus dieser Fassung des Homomorphie-Satzes folgt sofort für die Fasern von φ:

$$\varphi^{-1}(y) = \begin{cases} x + \ker(\varphi) & \textit{für } y \in \operatorname{im}(\varphi) \textit{ und } x \in M \textit{ mit } \varphi(x) = y, \\ \emptyset & \textit{für } y \notin \operatorname{im}(\varphi). \end{cases}$$

Insbesondere sind die nicht-trivialen Fasern von φ also allesamt Linksnebenklassen des Kerns von φ und damit alle gleichmächtig.

Beweis.
Da $(M,+)$ und $(N,+)$ Gruppen sind und φ ein Gruppenhomomorphismus, liefert der Homomorphie-Satz für Gruppen (Version II, Satz 1.2.59) einen eindeutigen Gruppenisomorphismus ξ, der die Bedingung $\varphi = \xi \circ \ker_{\ker(\varphi)}$ erfüllt. Analog wie im Beweis des Homomorphie-Satzes für Moduln und Vektorräume in Version I (2.1.29) für die Abbildung ξ_U kann hier für ξ sofort auf den Linksnebenklassen von $\ker(\varphi)$ nachgerechnet werden, daß ξ auch mit der skalaren Multiplikation strukturverträglich ist:

$$\begin{aligned}\xi\big(r(x+U)\big) &= \xi(rx+U) = \xi\big(\pi_{\ker(\varphi)}(rx)\big) = (\xi\circ\pi_{\ker(\varphi)})(rx) = \varphi(rx) = r\varphi(x)\\ &= r\big((\xi\circ\pi_{\ker(\varphi)})(x)\big) = r\big(\xi(x+U)\big).\end{aligned}$$

Somit ist ξ wie gewünscht eine lineare Abbildung, die natürlich eindeutig ist, da dies für den Gruppenisomorphismus gilt.
Die Aussagen über die Fasern von φ folgen aus dem Homomorphie-Satz für Gruppen (Satz 1.2.59), da φ auch ein Gruppenhomomorphismus ist und seine Fasern nicht von der zusätzlichen Eigenschaft abhängen, auch eine lineare Abbildung zu sein. □

Bemerkung 2.1.32. *Aus dem Homomorphie-Satz für Moduln und Vektorräume in Version II folgen für lineare Abbildungen die analogen Aussagen wie schon für Gruppen- und Ringhomomorphismen in Bemerkung 1.2.60 und Bemerkung 1.3.49: Die nicht-trivialen Fasern einer linearen Abbildung $\varphi\colon M \longrightarrow N$ sind Linksnebenklassen ihres Kerns und damit alle gleichmächtig. Außerdem bilden die nicht-trivialen Fasern von φ den Quotientenmodul/-Vektorraum $R/\ker(\varphi)$, der isomorph zu $\operatorname{im}(\varphi)$ ist, und aus der Kenntnis von zwei der drei Moduln/Vektorräume M, $\ker(\varphi)$ und $\operatorname{im}(\varphi)$ lassen sich über die Isomorphie $M/\ker(\varphi) \cong \operatorname{im}(\varphi)$ im Idealfall Informationen über den dritten gewinnen.* □

Beispiel 2.1.33.

i.) Es sei die folgende $\mathbb{R}$-lineare Abbildung zwischen den $\mathbb{R}$-Vektorräumen $\mathbb{R}^2$ und $\mathbb{R}$ betrachtet:

$$\varphi\colon \mathbb{R}^2 \longrightarrow \mathbb{R} \quad \textit{mit} \quad (x,y) \mapsto x-y.$$

Für den Kern von φ gilt:

$$\begin{aligned}\ker(\varphi) &= \{\,(x,y)\in\mathbb{R}^2 \mid \varphi\big((x,y)\big)=0\,\} = \{\,(x,y)\in\mathbb{R}^2 \mid x-y=0\,\}\\ &= \{\,(x,y)\in\mathbb{R}^2 \mid x=y\,\} \qquad\qquad = \{\,(x,x) \mid x\in\mathbb{R}\,\}.\end{aligned}$$

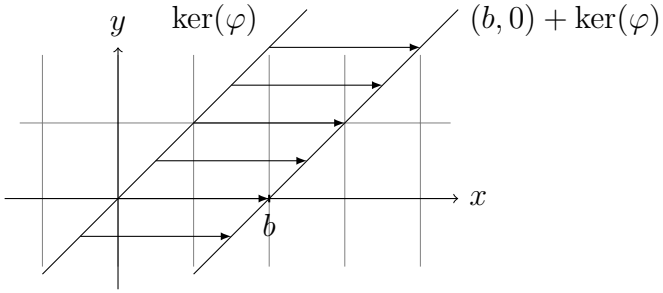
Die Abbildung φ ist surjektiv, denn für $b\in\mathbb{R}$ ist $(b,0)$ ein Urbild unter φ wegen:

$$\varphi\big((b,0)\big) = b-0 = b.$$

Nach dem Homomorphie-Satz für Vektorräume in Version II (2.1.31) gilt dann für die Fasern von φ:

$$\varphi^{-1}(b) = (b,0)+\ker(\varphi) = \{\,(b+x,x) \mid x\in\mathbb{R}\,\} \quad \textit{für jedes } b\in\mathbb{R}.$$

Die Faser $\varphi^{-1}(b)$ *ist die Linksnebenklasse* $(b,0)+\ker(\varphi)$ *des Untermoduls* $\ker(\varphi)$ *und damit die um den Vektor* $(b,0)$ *verschobene Faser* $\varphi^{-1}(0)=\ker(\varphi)$*:*



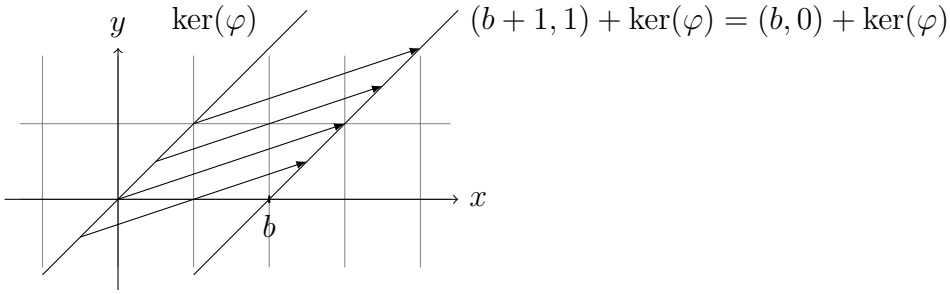
Die Wahl des Repräsentanten $(b,0)$ *der Faser* $\varphi^{-1}(b)$ *ist willkürlich, es wäre auch möglich, den Vektor* $(b+1,1)$ *als Repräsentanten zu wählen, denn es gilt:*

$$(b,0)-(b+1,1)=(-1,-1)\in\ker(\varphi)\overset{\text{Lem 1.2.17}}{\Longrightarrow}(b,0)+\ker(\varphi)=(b+1,1)+\ker(\varphi),$$

oder auch:

$$\varphi\big((b+1,1)\big)=(b+1)-1=b=b-0=\varphi\big((b,0)\big).$$

Die obige Skizze hätte mit dem Repräsentanten und damit „Verschiebevektor“ $(b+1,1)$ *dann folgende Gestalt:*



ii.) Es sei die folgende lineare Abbildung aus Beispiel 2.1.18 näher betrachtet:

$$D\colon \mathcal{C}^1(\mathbb{R})\longrightarrow\mathcal{C}^0(\mathbb{R})\quad\textit{mit}\quad f\mapsto f'.$$

Ist $g\in\mathcal{C}^0(\mathbb{R})$ *im Bild von* D*, so heißt ein* $f\in\mathcal{C}^1(\mathbb{R})$ *mit* $D(f)=f'=g$ *Stammfunktion von* g*. Die nicht-leeren Fasern der Abbildung* D *sind also Stammfunktionen gewisser stetiger Abbildungen.*
Folgende Sätze aus Analysis I helfen bei der Untersuchung der Abbildung D*:*

Mittelwertsatz der Differenzialrechnung (MWSD): *Sei* $f\colon\mathbb{R}\longrightarrow\mathbb{R}$ *eine differenzierbare Funktion, und es seien* $a,b\in\mathbb{R}$ *mit* $a<b$*. Dann existiert ein* $\xi\in]a,b[$ *mit:*

$$f(b)-f(a)=f'(\xi)(b-a).$$

Beweis: z.B. in [**FAn1**, § 16,Corollar 1,Seite 110].

Hauptsatz der Differenzial- und Integralrechnung (HDI): *Sei* $f\colon\mathbb{R}\longrightarrow\mathbb{R}$ *eine stetige Funktion und* $x_0\in\mathbb{R}$*. Dann ist*

$$F(x):=\int_{x_0}^{x}f(t)\,dt$$

differenzierbar, und es gilt $F'=f$*.*
Beweis: z.B. in [**FAn1**, § 19,Satz 1,Seite 139].

Der HDI liefert sofort, daß die Abbildung D surjektiv ist, denn für jedes stetige Funktion $g \in \mathcal{C}^0(\mathbb{R})$ wird dort eine Stammfunktion und damit ein Urbild unter D angegeben. Aus dem Homomorphie-Satz für Vektorräume in Version II (2.1.31) folgt dann sofort für ein $g \in \mathcal{C}^0(\mathbb{R})$:

$$\{\,\textit{Stammfunktonen von } g\,\} = D^{-1}(g) = G + \ker(D) \quad \textit{mit } G' = g,\ G \textit{ wie im HDI.}$$

Zur Bestimmung des Kerns von D hilft der Mittelwertsatz MWSD, denn aus diesem folgt sofort (Übung!):

$$f' = \bar{0} \quad \Longrightarrow \quad f = \textit{konstante Funktion.}$$

($\bar{0}$ ist hierbei die Nullabbildung von $\mathbb{R}$ nach $\mathbb{R}$.)
Zusammengefaßt liefert dies:

$$\{\,\textit{Stammfunkitonen von } g\,\} = D^{-1}(g) = G + \ker(D) = G + \{\,\textit{konstante Funktionen}\,\},$$

wobei G wieder eine gewählte Stammfunktion von g ist (z.B. wie im HDI). Insbesondere sind zwei Stammfunktionen von g durch Addition einer konstanten Funkion ineinander überführbar (bzw. deren Differenz konstant). □

Lineare Gleichungssysteme.

Mit den bisherigen Ergebnissen ist es schon möglich, die Lösungsmengen linearer Gleichungssysteme zu beschreiben, d.h. zum Beispiel die Lösungsmenge eines Systems von vier linearen Gleichungen über den reellen Zahlen:

$$\begin{array}{lrcrcrcr} A\colon & 3x & + & 4y & - & 6z & = & 3, \\ B\colon & x & - & 2y & + & 2z & = & 1, \\ C\colon & 2x & & & + & z & = & 2, \\ D\colon & -x & + & y & - & z & = & -1. \end{array}$$

Eine Lösung des obigen Systems kann als Vektor $(c_1, c_2, c_3) \in \mathbb{R}^3$ aufgefaßt werden, dessen Komponeten $c_1, c_2, c_3 \in \mathbb{R}$ alle vier linearen Gleichungen gleichzeitig erfüllen. Dies läßt sich auch mit Hilfe folgender Abbildung beschreiben:

$$\varphi\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^4 \quad \text{mit} \quad (x,y,z) \mapsto (\underbrace{3x+4y-6z}_{A},\ \underbrace{x-2y+2z}_{B},\ \underbrace{2x+z}_{C},\ \underbrace{-x+y-z}_{D}).$$

Es folgt sofort:

$$\{\text{Lösung des Gleichungssystems}\} \quad = \quad \varphi^{-1}\big((3,1,2,-1)\big).$$

Nach Lemma 2.1.19 ist die Abbildung φ eine lineare Abbildung zwischen den beiden $\mathbb{R}$-Vektorräumen $\mathbb{R}^3$ und $\mathbb{R}^4$, so daß sich nach dem Homomorphie-Satz für Vektorräume Version II (2.1.31) die Lösungsmenge des obigen linearen Gleichungssystems auch beschreiben läßt als Linksnebenklasse des Kernes von φ. Ein passender Repräsentant der Linksnebenklasse von $\ker(\varphi)$ ist ein gewähltes Element aus der Faser von $\varphi^{-1}\big((3,1,2,-1)\big)$, d.h. eine spezielle Lösung des Gleichungssystems, z.B. hier der Lösungsvektor $(1,0,0)$, und es ergibt sich:

$$\{\text{Lösung des Gleichungssystems}\} \quad = \quad \varphi^{-1}\big((3,1,2,-1)\big) \quad = \quad (1,0,0) + \ker(\varphi).$$

Wird bei den vier Gleichungen nur die rechte Seite verändert, d.h. zum Beispiel das folgende System betrachtet:

$$\begin{array}{lrcrcrcr} A\colon & 3x & + & 4y & - & 6z & = & 6, \\ B\colon & x & - & 2y & + & 2z & = & 2, \\ C\colon & 2x & & & + & z & = & 1, \\ D\colon & -x & + & y & - & z & = & -1, \end{array}$$

so wird die Lösungsmenge des neuen linearen Gleichungssystems wieder durch die gleiche Abbildung φ beschrieben, und dessen Lösungsmenge ist nun die Faser der „neuen rechten Seite“, d.h. die Faser $\varphi^{-1}\big((6,2,1,-1)\big)$:

$$\{\text{Lösung des Gleichungssystems}\} \quad = \quad \varphi^{-1}\big((6,2,1,-1)\big).$$

Auch in diesem Fall ist dann die Faser wieder eine Linksnebenklasse des Kerns von φ, und dessen Repräsentant ein gewähltes Urbild von $(6,2,1,-1)$ unter φ bzw. eine Lösung des linearen Gleichungssystems, z.B. hier der Vektor $(0,0,1)$:

$$\{\text{Lösung des Gleichungssystems}\} \quad = \quad \varphi^{-1}\big((6,2,1,-1)\big) \quad = \quad (0,0,1)+\ker(\varphi).$$

Auch die prinzipielle Lösbarkeit des linearen Gleichungssystems läßt sich über die Abbildung φ beschreiben: ist die rechte Seite des obigen linearen Gleichungssystems durch den Vektor $b := (b_1,b_2,b_3,b_4) \in \mathbb{R}^4$ gegeben, so gilt offensichtlich:

$$\left.\begin{array}{l}\text{Das oben gegebene lineare Glei-}\\ \text{chungssystem mit der rechten Sei-}\\ \text{te } (b_1,b_2,b_3,b_4) \text{ hat eine Lösung.}\end{array}\right\} \quad \Longleftrightarrow \quad \varphi^{-1}(b) \neq \emptyset \quad \Longleftrightarrow \quad b \in \operatorname{im}(\varphi).$$

Diese Beobachtungen sollen nun formalisiert werden:

Definition 2.1.34. *Sei R ein kommutativer Ring mit Eins. Eine lineare Gleichung in n Unbekannten $z_1,\dots,z_n$ über R ist gegeben durch Koeffizienten $a_1,\dots,a_n \in R$, $b \in R$ und eine Gleichung:*

$$a_1z_1 + a_2z_2 + \cdots + a_nz_n = b.$$

Eine Lösung der linearen Gleichung ist ein Vektor $(c_1,\dots,c_n) \in R^n$, der die lineare Gleichung erfüllt, d.h. für den $\sum_{i=1}^n a_ic_i = b$ gilt.
Ein lineares Gleichungssystem mit m Gleichungen in n Unbekannten ist gegeben durch m lineare Gleichungen über R in n Unbekannten, d.h. durch Koeffizienten $a_{i,j} \in R$ mit $1 \le i \le m$ und $1 \le j \le n$ und $b_1,\dots,b_m \in R$:

$$\begin{array}{rcrcl} a_{1,1}z_1 & +\ldots+ & a_{1,n}z_n & = & b_1, \\ a_{2,1}z_1 & +\ldots+ & a_{2,n}z_n & = & b_2, \\ & \vdots & & \vdots & \\ a_{m,1}z_1 & +\ldots+ & a_{m,n}z_n & = & b_m. \end{array}$$

Eine Lösung des Gleichungssystems ist ein Vektor $(c_1,\dots,c_n) \in R^n$, dessen Komponenten alle m Gleichung erfüllen.
Der Vektor $b := (b_1,\dots,b_m) \in R^m$ heißt die rechte Seite des linaren Gleichungssystems.
Ein lineares Gleichungssystem heißt homogen, falls seine rechte Seite b der Nullvektor ist, ansonsten inhomogen. □

Aus den einleitenden Betrachtungen folgt dann sofort:

Satz 2.1.35. *Sei R ein kommutativer Ring mit Eins. Weiter sei ein lineares Gleichungssystem (LGS) über R mit m Gleichungen in n Unbekannten $z_1, \ldots, z_n$ gegeben durch die Koefffizienten $a_{i,j} \in R$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$ und die rechte Seite $b := (b_1, \ldots, b_m) \in R^m$:*

$$\begin{array}{ccccc} a_{1,1}z_1 & + \ldots + & a_{1,n}z_n & = & b_1, \\ a_{2,1}z_1 & + \ldots + & a_{2,n}z_n & = & b_2, \\ & \vdots & & \vdots & \\ a_{m,1}z_1 & + \ldots + & a_{m,n}z_n & = & b_m. \end{array}$$

Weiter sei φ die wie in Lemma 2.1.19 durch die Koeffizienten $a_{i,j}$ definierte lineare Abbildung zwischen den R-Moduln R^n und R^m:

$$\varphi\colon R^n \longrightarrow R^m \quad \textit{mit} \quad (x_1, \ldots, x_n) \mapsto \Big(\sum_{k=1}^{n} a_{1,k}x_k, \ldots, \sum_{k=1}^{n} a_{m,k}x_k \Big).$$

Dann beschreibt die lineare Abbildung φ das lineare Gleichungssystem, und es folgt:

$$\textit{Das LGS ist lösbar} \quad \Longleftrightarrow \quad b \in \operatorname{im}(\varphi).$$

Für die Lösungsmenge des Gleichungssystems gilt:

$$\{\, \textit{Lösung des LGS} \,\} \quad = \quad \varphi^{-1}(b).$$

Ist die Lösungsmenge nicht leer und $x \in R^n$ eine Lösung, d.h. $\varphi(x) = b$, so folgt:

$$\{\, \textit{Lösung des LGS} \,\} \quad = \quad \varphi^{-1}(b) \quad = \quad x + \ker(\varphi) \quad = \quad x + \varphi^{-1}(0).$$

Eine nicht-leere Lösungsmenge des linearen Gleichungssystems erfüllt also die folgenden Strukturaussagen:

- *Ist das lineare Gleichungssystem homogen, d.h. $b = 0$, so ist seine Lösungsmenge der Kern von φ und damit ein Untermodul des R^n.*
- *Ist das lineare Gleichungssystem inhomogen, d.h. $b \neq 0$, so ist seine Lösungsmenge eine echte Linksnebenklasse des Kerns von φ und damit kein Untermodul.*

Zu dem linearen Gleichungssystem kann, falls es inhomogen ist, das dazugehörige homogene lineare Gleichungssystem betrachtet werden, indem als rechte Seite der Nullvektor gewählt wird. Da die Lösungsmenge des inhomogenen Systems nur eine Linksnebenklasse der Lösungsmenge des homogenen Systems ist, sind eine inhomogene Lösungsmenge und die homogene Lösungsmenge gleichmächtig, und es läßt sich anschaulich schreiben:

$$\{\textit{Lösung des inhomogenen LGS}\} = \textit{spezielle Lösung} + \{\textit{Lösung des homogenen LGS}\}.$$

Beweis.
Lemma 2.1.19 liefert die Beschreibung des linearen Gleichungssystems mittels der linearen Abbildung φ, und alle weiteren Aussagen folgen dann sofort aus dem Homomorphie-Satz für Moduln/Vektorräume in Version II (2.1.31). $\square$

Bemerkung 2.1.36. *In Satz 2.1.35 ist die Lösungsmenge eines linearen Gleichungssystems strukturell beschrieben, insbesondere der Zusammenhang der Lösungsmenge eines inhomogenen linearen Gleichungssystems zu der des dazugehörigen homogenen Systems.*
Dieser Zusammenhang gibt aber bisher noch keine Auskunft, wie die Lösung eines linearen Gleichungssystems im konkreten Fall gefunden werden kann: nur wenn der Kern der beschreibenden linearen Abbildung φ und eine spezielle Lösung x bekannt ist, kann sofort die Lösungsmenge $x + \ker(\varphi)$ bestimmet werden.
Im weiteren Verlauf der Vorlesung wird jedoch gezeigt, wie mit Hilfe des Gauß-Algorithmus der Kern einer linearen Abbildung über Vektorräumen bestimmt werden kann, so daß im Fall von linearen Gleichungssystemen über einem Körper immer ein Algorithmus existiert, um die Lösungsmenge zu berechnen. □

2.2. Erzeugendensysteme und Basen

Es soll nun ein wesentliches Hilfsmittel eingeführt werden, mit dem lineare Abbildungen zwischen Vektorräumen analysiert werden können: *Basen*.
Die vorherige Einschränkung von Moduln auf Vektorräume ist darin begründet, daß nicht alle Moduln Basen besitzen - für Vektorräume ist das der Fall. Allerdings existieren auch Moduln, die keine Vektorräume sind, für die aber trotzdem Bases existieren.
Insbesondere für Vektorräume ist mit Basen auch die Definition eines nützlichen Dimensionsbegriffes möglich - eine analoge Konstruktion bei Moduln mit Basen ist dort weniger stark, da sich wichtige Aussagen nicht von Vektorräumen auf Moduln mit Basen übertragen lassen.

Erzeugendensysteme.

Bevor der Begriff eines Erzeugendensystems (und dann später einer Basis) eingeführt wird, sei zur Motivation zunächst einmal der $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ betrachtet: Es gilt definitionsgemäß:

$$\mathbb{R}^2 := \{\, (x, y) \mid x, y \in \mathbb{R} \,\},$$

und jeder Vektor des $\mathbb{R}^2$ läßt sich als Summe von Vielfachen der beiden Vektoren $(1, 0)$ und $(0, 1)$ schreiben:

$$(x, y) = x \cdot (1, 0) + y \cdot (0, 1).$$

Ist ein $\mathbb{R}$-Vektorraum V gegeben und eine lineare Abbildung $\varphi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, V)$, so gilt dann nach den Linearitätseigenschaften (Definition 2.1.16):

$$\varphi\big((x, y)\big) = \varphi\big(x\cdot(1, 0)+y\cdot(0, 1)\big) = \varphi\big(x\cdot(1, 0)\big)+\varphi\big(y\cdot(0, 1)\big) = x\cdot\varphi\big((1, 0)\big)+y\cdot\varphi\big((0, 1)\big).$$

Dies hat zwei wesentliche Konsequenzen:

- Alle Bilder von φ auf dem ganzen Definitionsbereich $\mathbb{R}^2$ sind schon durch die beiden Bilder der Vektoren $(1, 0)$ und $(0, 1)$ festgelegt, denn mit $v_1 := \varphi\big((1, 0)\big)$ und $v_2 := \varphi\big((0, 1)\big)$ gilt dann für alle $(x, y) \in \mathbb{R}^2$:

$$\varphi\big((x, y)\big) = xv_1 + yv_2.$$

- Es gilt für zwei Abbildungen $\varphi, \psi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2, V)$, daß sie schon auf dem ganzen Definitionsbereich $\mathbb{R}^2$ übereinstimmen, wenn sie nur auf den beiden Vektoren $(1,0)$ und $(0,1)$ die gleichen Bilder haben:

$$\varphi = \psi \quad \Longleftrightarrow \quad \varphi\big((1,0)\big) = \psi\big((1,0)\big) \text{ und } \varphi\big((0,1)\big) = \psi\big((0,1)\big).$$

Der Schlüssel obiger Argumentation ist, daß jeder Vektor des $\mathbb{R}^2$ eine Summe von Vielfachen der beiden Vektoren $(1,0)$ und $(0,1)$ ist, und lineare Abbildungen mit Summenbildung und Streckungen von Vektoren strukturverträglich sind.
Anstelle der beiden Vektoren $(1,0)$ und $(0,1)$, die sofort ins Auge fallen, wäre es auch möglich gewesen, für obige Betrachtungen die beiden Vektoren $(1,1)$ und $(-1,1)$ zu wählen, denn es gilt für alle $(x,y) \in \mathbb{R}^2$:

$$(x,y) = \tfrac{1}{2}(x+y)\cdot(1,1) + \tfrac{1}{2}(-x+y)\cdot(-1,1).$$

Also läßt sich auch jeder Vektor des $\mathbb{R}^2$ als Summe von Vielfachen der Vektoren $(1,1)$ und $(-1,1)$ schreiben. Eine solche „Summe von Vielfachen“ gegebener Vektoren heißt Linearkombination der Vektoren.
Bevor der Begriff von Linearkombinationen formalisiert wird, und zwar gleich für eine beliebige Anzahl von Vektoren, soll vorher aber noch ein Aspekt betrachtet werden, der im weiteren Verlauf eine große Rolle spielen wird:

Die beiden oben gewählten Vektoren $(1,0)$ und $(0,1)$ können als zweielementige Menge $\{(1,0),(0,1)\} \subseteq \mathbb{R}^2$ aufgefaßt werden. In einer Menge spielt die Reihenfolge der Elemente keine Rolle, es gilt

$$\{(1,0),(0,1)\} = \{(0,1),(1,0)\}.$$

Auch bei der obigen Summendarstellung von (x,y) durch Vielfache von $(1,0)$ und $(0,1)$ spielt die Reihenfolge der Summanden keine Rolle, da die Addition von Vektoren in einer abelschen Gruppe stattfindet und damit kommutativ ist:

$$(x,y) = x\cdot(1,0) + y\cdot(0,1) = y\cdot(0,1) + x\cdot(1,0).$$

Es wird in späteren Betrachtungen aber wesentlich darauf ankommen, in welcher Reihenfolge Vektoren angeordnet und in Summen verwendet werden, so daß zunächst anstelle einer „ungeordneten Auswahl“ mittels einer „Menge von Vektoren“ eine „geordnete Auswahl“ mittels eines „Systems von Vektoren“ eingeführt wird. Inspiriert wird die Definition von „Systemen“ von folgender Beobachtung: Werden die beiden Vektoren $(1,0)$ und $(0,1)$ nicht in einer Menge, sondern in einem Tupel

$$\big(\ (1,0),\ (0,1)\ \big) \in (\mathbb{R}^2)^2$$

zusammengefaßt, so spielt die Reihenfolge in dem Tupel eine Rolle, denn es gilt nach Definition 0.2.2:

$$\big(\ (1,0),\ (0,1)\ \big) \neq \big(\ (0,1),\ (1,0)\ \big).$$

Dies führt zu folgender Definition:

Definition 2.2.1. *Sei M eine nicht-leere Menge und I eine nicht-leere Indexmenge. Ein System von Elementen aus M ist ein I-Tupel $(m_i)_{i\in I} \in \prod_{i\in I} M$.*
Für die Indexmenge $I := \{1,\dots,n\}$ wird auch $(m_1,\dots,m_n)$ anstelle von $(m_i)_{i\in\{1,\dots,n\}}$ geschrieben. □

Bemerkung 2.2.2.

i.) *Ein System $(m_i)_{i\in I}$ von Elementen aus einer Menge M ist keine Teilmenge von M, sondern ein Element aus $\prod_{i\in I} M$.*

ii.) *Systeme von Elementen aus einer Menge M unterscheiden sich noch in einem weiteren Aspekt (zusätzlich zur Ordnung) von Teilmengen aus M: in einer Teilmenge von M sind Elemente aus M nur* einmal *enthalten, da in Mengen Elemente nicht mehrfach vorkommen dürfen (siehe auch Definition 0.2.1). In einem System kann an mehrere Stellen das gleiche Element stehen:*

$$\{1,1,2\} \subseteq \mathbb{N} \text{ ist nicht erlaubt, aber } (1,1,2) \in \mathbb{N}^3.$$

iii.) *Ist eine nicht-leere Menge M gegeben und eine nicht-leere Teilmenge $N \subseteq M$, so kann die Menge N zu einem System von Elementen aus M gemacht werden, welches jedes Element aus N genau einmal enthält:*

$$N \quad \rightsquigarrow \quad (n)_{n\in N}.$$

iv.) *Ist M eine nicht-leere Menge und $\{m_1,\dots,m_k\} \subseteq M$ gewählt, so kann diese Teilmenge in natürlicher Weise in ein System aus Elementen in M transformiert werden:*

$$\{m_1,\dots,m_k\} \quad \rightsquigarrow \quad (m_1,\dots,m_k).$$

Hier wird eine „ungeordnete“ Auswahl von Elementen m_i zu einer „geordneten“ Auswahl, und die Ordnung wird von der Reihenfolge, in der die Elemente in der Teilmenge aufgelistet werden, induziert. Eine Änderung der Reihenfolge in der Teilmenge verändert diese nicht, liefert aber ein anderes System.

v.) *Aus einem System $(m_i)_{i\in I}$ von Elementen aus M kann kanonisch eine Teilmenge von M gemacht werden, indem die Komponenteneinträge des I-Tupels gesammelt werden:*

$$(m_i)_{i\in I} \quad \rightsquigarrow \quad \{\, m_i \mid i \in I \,\}.$$

Dabei geht dann die frühere Ordnung innerhalb des Systems verloren, und die Teilmenge wird mitunter „kleiner“ als das System, denn ein mehrfach im I-Tupel vorkommendes Element tritt nur einmal in der gewonnenen Teilmenge auf. □

Wie schon einleitend erwähnt, sollen „Linearkombinationen“ d.h. Summen von Vielfachen gegebener Vektoren, für eine beliebige Anzahl von Vektoren definiert werden - allerdings sind nur Summen endlich vieler Vektoren formal definiert (siehe dazu auch Definition 1.1.7, wo in algebraischen Strukturen nur die Verknüpfung endlich vieler Elemente erlaubt ist)! Diese Beschränkung kann durch folgenden Trick aufgehoben werden:

Wenn in einer Summe beliebig vieler Vektoren nur endlich viele ungleich dem Nullvektor zugelassen werden, so ist die Summe der Nicht-Nullvektoren wohldefiniert - und wenn dann noch beliebig oft eine Null hinzugefügt wird, so kann als Gesamtergebnis das Ergebnis der endlichen Summation der Nicht-Nullvektoren definiert werden.

Da in einem R-Modul M für $x \in M$ nach Lemma 2.1.10 immer $0_R \cdot x = 0_M$ gilt, kann in einer Summe über eine beliebige nicht-leere Indexmenge I der Form:

$$\sum_{i\in I} a_i x_i \quad \text{mit } a_i \in R, x_i \in M$$

durch die Forderung:

$$„a_i \neq 0_R \text{ nur für endlich viele } i \in I“$$

erzwungen werden, daß nur endlich viele Summanden ungleich dem Nullvektor sind, und die Summe wäre nach der obigen Festlegung definiert.

Daß in einem System von Skalaren oder Vektoren nur endlich viele ungleich Null sind, wird folgendermaßen formalisiert:

Definition 2.2.3.

i.) Sei G eine Gruppe mit dem neutralen Element e_G und I eine nicht-leere Indexmenge. Dann ist definiert:

$$\bigoplus_{i\in I} G := \{\, (g_i)_{i\in I} \mid g_i \neq e_G \text{ nur für endlich viele } i \in I \,\} \subseteq \prod_{i\in I} G.$$

ii.) Sei R ein Ring und I eine nicht-leere Indexmenge. Dann ist definiert:

$$\bigoplus_{i\in I} R := \{\, (a_i)_{i\in I} \mid a_i \neq 0_R \text{ nur für endlich viele } i \in I \,\} \subseteq \prod_{i\in I} R. \qquad \square$$

Bemerkung 2.2.4. *Ist I eine nicht-leere endliche Menge, so gilt für die beiden vorherigen Definitionen:*

$$\bigoplus_{i\in I} G = \prod_{i\in I} G \quad \text{und} \quad \bigoplus_{i\in I} R = \prod_{i\in I} R. \qquad \square$$

Nun kann definiert werden, was die „Linearkombination“ eines beliebigen Systems von Vektoren ist:

Definition 2.2.5. *Sei M ein R-Modul/Vektorraum und I eine nicht-leere Indexmenge. Für ein System $(x_i)_{i\in I}$ von Vektoren aus M und ein System $(a_i)_{i\in I} \in \bigoplus_{i\in I} R$ ist definiiert:*

$$\sum_{i\in I} a_i x_i := \sum_{\substack{i\in I \\ a_i x_i \neq 0_M}} a_i x_i \qquad \text{(nur endlich viele Skalare } a_i \neq 0\text{, und damit nur endlich viele Vektoren } a_i x_i \neq 0\text{!)}$$

Eine solche Summe heißt Linearkombination von $(x_i)_{i\in I}$ mit dem Koeffizientensystem $(a_i)_{i\in I}$. Spielt die Reihenfolge keine Rolle, wird auch salopp von einer Linearkombination der x_i mit den Koeffizienten a_i gesprochen.
Für $I := \{1, \ldots, n\}$ wird eine Linearkombination von $(x_i)_{i\in I}$ mit den Koeffizienten $(a_i)_{i\in I}$ auch $\sum_{i=1}^n a_i x_i$ geschrieben.
Die Menge aller möglichen Linearkombinationen des Systems $(x_i)_{i\in I}$ wird das Erzeugnis von $(x_i)_{i\in I}$ genannt und notiert mit: $\langle\, x_i \mid i \in I \,\rangle$ oder $\langle\, x_i \,\rangle_{i\in I}$, d.h. es gilt:

$$\langle\, x_i \,\rangle_{i\in I} := \Big\{ \sum_{i\in I} a_i x_i \mid (a_i)_{i\in I} \in \bigoplus_{i\in I} R \Big\}.$$

Das Erzeugnis von $(x_i)_{i\in I}$ wird auch der Spann oder die lineare Hülle von $(x_i)_{i\in I}$ genannt.
Für die Indexmenge $I := \{1, \ldots, n\}$ wird das Erzeugnis des Systems $(x_1, \ldots, x_n)$ auch notiert als:

$$\langle\, x_1, \ldots, x_n \,\rangle := \langle\, x_i \mid i \in I \,\rangle. \qquad \square$$

Bemerkung 2.2.6.

i.) Tritt im folgenden Text eine Summe $\sum_{i\in I} a_i x_i$ auf, so ist damit immer eine Linearkombination der x_i gemeint, und damit sind höchstens endlich viele Koeffizienten a_i ungleich Null - egal, wie groß die Indexmenge ist.

Die Summe unendlich vieler Vektoren ist weiterhin nicht erlaubt!

ii.) Da Linearkombinationen eines Systems $(x_i)_{i\in I}$ defacto immer endliche Summen in einer abelschen Gruppe sind (die Vektoren eines Moduls/Vektorraumes bilden eine additive abelsche Gruppe), spielt die Reihenfolge der Summation keine Rolle, und für eine beliebige Permutation $\pi \in S(I)$ der Indexmenge I gilt mit einem Koeffizientensystem $(a_i)_{i\in I}$:

$$\sum_{i\in I} a_i x_i = \sum_{i\in I} a_{\pi(i)} x_{\pi(i)} \quad \text{und damit} \quad \langle\, x_i \mid i \in I \,\rangle = \langle\, x_{\pi(i)} \mid i \in I \,\rangle.$$

iii.) Für ein System $(x_i)_{i\in I}$ können verschiedene Koeffizientensysteme die gleiche Linearkombination ergeben. Sei dazu folgendes System des $\mathbb{R}^2$ betrachtet:

$$\big((1,0),\ (0,1),\ (1,1)\big).$$

Dann liefern die beiden Koeffizientensysteme $(1,2,0)$ und $(0,1,1)$ die gleiche Linearkombination:

$$1\cdot(1,0) + 2\cdot(0,1) + 0\cdot(1,1) = (1,2) = 0\cdot(1,0) + 1\cdot(0,1) + 1\cdot(1,1). \qquad \square$$

Beispiel 2.2.7.

i.) Für den $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ gilt nach den einleitenden Betrachtungen:

$$\langle\, (1,0),(0,1) \,\rangle = \mathbb{R}^2 = \langle\, (1,1),(-1,1) \,\rangle.$$

ii.) Für jeden kommutativen Ring mit Eins R gilt für den R-Modul R:

$$\langle\, 1_R \,\rangle = R.$$

iii.) Für den $\mathbb{Z}$-Modul $\mathbb{Z}$ gilt:

$$\langle\, a \,\rangle = \mathbb{Z} \quad \Longleftrightarrow \quad a \in \{\pm 1\}. \qquad \square$$

Nach Bemerkung 2.2.6 spielt es bei der Bildung einer Linearkombination keine Rolle, in welcher Reihenfolge die Vektoren summiert werden - damit kann der Begriff der Linearkombination eines Systems von Vektoren auf eine Menge von Vektoren übertragen werden, da jede Menge N nach Bemerkung 2.2.2 zu einem System $(n)_{n\in N}$ gemacht werden, kann, welches als Elemente genau die der Menge hat - die willkürlich dadurch implizierte Ordnung auf der Menge wirkt sich bei der Linearkombination nicht aus. Mit gleichen Argumenten kann deshalb auch das Erzeugendensystem einer Menge definiert werden:

Definition 2.2.8. *Sei M ein R-Modul/Vektorraum und $N \subseteq M$ eine Teilmenge. Für $(a_n)_{n\in N} \subseteq \bigoplus_{n\in N} R$ ist dann die Linearkombination der Vektoren aus N mit Hilfe des Systems $(n)_{n\in N}$ definiert als:*

$$\sum_{n\in N} a_n n. \qquad \text{(unabhängig von der Reihenfolge!)}$$

Das Erzeugnis der Vektoren aus N ist die Menge aller Linearkombinationen der Vektoren aus N. Es wird dann auch notiert:

$$\langle N \rangle := \langle n \mid n \in N \rangle. \qquad \square$$

Mit Linearkombinationen von Vektoren kann gerechnet werden wie mit „endlichen Summen“, egal wie groß das System ist, wie folgendes Lemma zeigt:

Lemma 2.2.9. *Sei M ein R-Modul/Vektorraum und I eine nicht-leere Indexmenge. Weiter sei $(x_i)_{i\in I}$ ein System von Vektoren aus M, $r \in R$, und $(a_i)_{i\in I}, (b_i)_{i\in I}$ seien Koeffizientensysteme aus $\bigoplus_{i\in I} R$.*

i.) Es gilt $(a_i + b_i)$, $(ra_i) \in \bigoplus_{i\in I} R$, und $\bigoplus_{i\in I} R$ ist ein R-Untermodul/Untervektorraum von $\prod_{i\in I} R$.

ii.) Für Linearkombinationen $\sum_{i\in I} a_i x_i$ und $\sum_{i\in I} b_i x_i$ folgt:

$$\Big(\sum_{i\in I} a_i x_i\Big) + \Big(\sum_{i\in I} b_i x_i\Big) = \sum_{i\in I} (a_i + b_i) x_i \quad \text{und} \quad r\Big(\sum_{i\in I} a_i x_i\Big) = \sum_{i\in I} r a_i x_i.$$

Beweis.

i.) Sei $J \subseteq I$ diejenige Menge der Indizes, für die $a_i \neq 0_R$ gilt, und analog $K \subseteq I$ diejenige mit $b_i \neq 0$. Beide Mengen J, K sind per Definition endlich, und damit auch $J \cup K$.
Dann gilt $a_i + b_i = 0_R$ für $i \notin J \cup K$, und $ra_i = 0_R$ für $i \notin J$, so daß auch in den Systemen $(a_i + b_i)_{i\in I}$ und $(ra_i)_{i\in I}$ nur endlich viele Komponenten ungleich Null sind und damit beide in $\bigoplus_{i\in I} R$ liegen.
Wegen obiger Aussagen ist offensichtlich das Untermodul-/Untervektorraumkriterium 2.1.13 für $\bigoplus_{i\in I} R$ erfüllt:

$$r, s \in R,\ (a_i)_{i\in I}, (b_i)_{\in I} \in \bigoplus_{i\in I} R \quad \Longrightarrow \quad r \cdot (a_i) + s \cdot (b_i) = (ra_i + sb_i)_{i\in I} \in \bigoplus_{i\in I} R.$$

ii.) Für die Linearkombinationen $\sum_{i\in I} a_i x_i$ und $\sum_{i\in I} b_i x_i$ gilt dann mit obigen Indexmengen J, K:

$$\sum_{i\in I} a_i x_i \overset{\text{(Def)}}{=} \sum_{i\in J} a_i x_i = \sum_{i\in J\cup K} a_i x_i \quad \text{und} \quad \sum_{i\in I} b_i x_i \overset{\text{(Def)}}{=} \sum_{i\in K} b_i x_i = \sum_{i\in J\cup K} b_i x_i$$

sowie

$$\sum_{i\in I} (a_i + b_i) x_i \overset{\text{(Def)}}{=} \sum_{i\in J\cup K} (a_i + b_i) x_i \quad \text{und} \quad \sum_{i\in I} r a_i x_i \overset{\text{(Def)}}{=} \sum_{i\in J} r a_i x_i,$$

woraus dann sofort die behaupteten Gleichungen folgen, wenn mit den endlichen Summen gerechnet wird:

$$\Big(\sum_{i\in I} a_i x_i\Big) + \Big(\sum_{i\in I} b_i x_i\Big) \overset{\text{(Def)}}{=} \Big(\sum_{i\in J} a_i x_i\Big) + \Big(\sum_{i\in K} b_i x_i\Big) = \Big(\sum_{i\in J\cup K} a_i x_i\Big) + \Big(\sum_{i\in J\cup K} b_i x_i\Big)$$

$$\overset{(J\cup K \text{ endlich})}{=} \sum_{i\in J\cup K}(a_i+b_i)x_i = \sum_{i\in I}(a_i+b_i)x_i,$$

und

$$r\Big(\sum_{i\in I} a_i x_i\Big) \overset{(\text{Def})}{=} r\Big(\sum_{i\in J} a_i x_i\Big) \overset{(J \text{ endlich})}{=} \sum_{i\in J} r a_i x_i = \sum_{i\in I} r a_i x_i. \qquad \square$$

Es folgt sofort, daß das Erzeugnis von Vektoren ist nicht nur irgendeine Teilmenge des Raumes ist, sondern sogar immer eine Unterstruktur, d.h. ein Untermodul oder Untervektorraum:

Lemma 2.2.10. *Sei M ein R-Modul/Vektoraum und $(x_i)_{i\in I}$ ein System von Vektoren aus M. Dann ist deren Erzeugnis $\langle x_i \rangle_{i\in I}$ ein Untermodul/Untervektorraum von M, und zwar der kleinste, der alle x_i für $i \in I$ enthält; d.h. es gilt:*

$$U \subseteq M \text{ Untermodul/UVR und } x_i \in U \text{ für alle } i \in I \quad \Longrightarrow \quad \langle x_i \rangle_{i\in I} \subseteq U.$$

Analog dazu gilt: Ist $N \subseteq M$ eine Teilmenge, so ist deren Erzeugnis $\langle N \rangle$ der kleinste Untermodul/Untervektorraum von M, der N enthält.

Beweis.
Es reicht, die Aussage für das Erzeugnis eines Systems von Vektoren zu zeigen, da das Erzeugnis einer Menge darüber definiert ist.
Zum Beweis wird das Untermodulkriterium 2.1.13 herangezogen, und es muß gezeigt werden:

$$a,b \in R,\ \Big(\sum_{i\in I} a_i x_i\Big), \Big(\sum_{i\in I} b_i x_i\Big) \in \langle x_i \rangle_{i\in I} \implies a\Big(\sum_{i\in I} a_i x_i\Big) + b\Big(\sum_{i\in I} b_i x_i\Big) \in \langle x_i \rangle_{i\in I}.$$

Dies folgt aber sofort aus den Rechenregeln für Linearkombinationen in Lemma 2.2.9:

$$a\Big(\sum_{i\in I} a_i x_i\Big) + b\Big(\sum_{i\in I} b_i x_i\Big) \overset{(2.2.9)}{=} \Big(\sum_{i\in I} a a_i x_i\Big) + \Big(\sum_{i\in I} b b_i x_i\Big) = \sum_{i\in I}(a a_i + b b_i) x_i \in \langle x_i \rangle_{i\in I}.$$

Daß $\langle x_i \rangle_{i\in I}$ in jedem Untermodul/Untervektorraum $U \subseteq M$ liegt, der alle x_i für $i \in I$ enthält, ist klar, da ein solches U abgeschlossen ist unter endlichen Summen und Streckungen und somit jede Linearkombination von $(x_i)_{i\in I}$ enthält. $\square$

Dies liefert sofort folgende Definition:

Definition 2.2.11. *Sei M ein R-Modul/Vektorraum. Ein System $(x_i)_{i\in I}$ von Vektoren aus M heißt Erzeugendensystem von M, falls gilt:*

$$\langle x_i \rangle_{i\in I} = M.$$

Ist $N \subseteq M$, so wird M von N erzeugt, falls gilt: $\langle N \rangle = M$. $\square$

Jeder Modul/Vektorraum besitzt ein Erzeugendensystem:

Lemma 2.2.12. *Sei M ein R-Modul/Vektorraum. Dann wird M von M erzeugt, und $(m)_{m\in M}$ ist ein Erzeugendensystem von M.*

Beweis.
Die Aussage braucht nur für das System $(m)_{m\in M}$ gezeigt zu werden, und dafür muß für jedes $x \in M$ eine Linearkombination von $(m)_{m\in M}$ gefunden werden mit

$$x = \sum_{m\in M} a_m m.$$

Das passenden System von Koeffizienten dazu ist $(a_m)_{m\in M}$ mit

$$a_m := \begin{cases} 0_R & \text{für } m \neq x, \\ 1_R & \text{für } m = x \end{cases} \qquad \Longrightarrow \qquad (a_m)_{m\in M} \in \bigoplus_{m\in M} R. \qquad \square$$

Einleitend wurde an einem Beispiel motiviert, daß Erzeugendensysteme nützlich zur Analyse von linearen Abbildungen sind. Dies kann hier nun ausfürhrlich und allgemein formuliert werden:

Lemma 2.2.13. *Sei M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein Erzeugendensystem von M. Ist V ein weiterer R-Modul/Vektorraum und $\varphi\colon M \longrightarrow V$ eine lineare Abbildung, so gilt:*

i.) Für eine Linearkombination $x := \sum_{i\in I} a_i x_i$ gilt: $\quad \varphi(x) = \sum_{i\in I} a_i \varphi(x_i)$.

ii.) $\big(\varphi(x_i)\big)_{i\in I}$ ist ein Erzeugendensystem von $\operatorname{im}(\varphi) \subseteq V$.

iii.) φ ist durch seine Bilder auf Erzeugendensystem eindeutig festgelegt, d.h. es gilt für $\varphi, \psi \in \operatorname{Hom}_R(M, V)$:

$$\varphi = \psi \quad \Longleftrightarrow \quad \varphi(x_i) = \psi(x_i) \text{ für alle } i \in I.$$

Beweis.

i.) Sei $J \subseteq I$ diejenige Menge der Indizes, für die $a_i \neq 0$ gilt. Dann folgt, weil φ mit endlicher Summenbildung und Streckungen verträglich ist:

$$\begin{aligned} \varphi(x) = \varphi\Big(\sum_{i\in I} a_i x_i\Big) &\overset{\text{(Def)}}{=} \varphi\Big(\sum_{i\in J} a_i x_i\Big) \overset{(J \text{ endlich})}{=} \sum_{i\in J} \varphi(a_i x_i) \\ &= \sum_{i\in J} a_i \varphi(x_i) = \sum_{i\in I} a_i \varphi(x_i). \end{aligned}$$

ii.) Dies folgt sofort aus der vorherigen Aussage, denn es ist:

$$\operatorname{im}(\varphi) = \{\, v \in V \mid \exists x \in X : \varphi(x) = v \,\},$$

und jedes x ist eine Linearkombination von $(x_i)_{i\in I}$ und dann $\varphi(x)$ eine Linearkombination von $\varphi(x_i)$, sogar mit den gleichen Koeffizienten:

$$v = \varphi(x) = \varphi\Big(\sum_{i\in I} a_i x_i\Big) = \sum_{i\in I} a_i \varphi(x_i).$$

iii.) $\Longrightarrow$: Trivial, da alle x_i in M liegen.

$\Longleftarrow$: Für $x \in M$ ist zu zeigen: $\varphi(x) = \psi(x)$. Da $(x_i)_{i\in I}$ ein Erzeugendensystem in M ist, gibt es eine Darstellung von x als Linearkombination von $(x_i)_{i\in I}$, und es folgt:

$$\varphi(x) = \varphi\Big(\sum_{i\in I} a_i x_i\Big) = \sum_{i\in I} a_i \varphi(x_i) \overset{(\varphi(x_i) = \psi(x_i))}{=} \sum_{i\in I} a_i \psi(x_i) = \psi\Big(\sum_{i\in I} a_i x_i\Big) = \psi(x).$$

$\square$

Bemerkung 2.2.14. *Die Aussagen von Lemma 2.2.13 sollen noch einmal plakativ als Merksatz formuliert werden:*

- *Die Bilder eines Erzeugendensystems bilden ein Erzeugendensystem des Bildes.*
- *Zwei lineare Abbildungen stimmen genau dann überein, wenn sie auf einem Erzeugendensystem übereinstimmen.* □

Ist M ein R-Modul/Vektorraum, und sind $X, Y \subseteq M$ Teilmengen, so folgt offensichtlich:

$$X \subseteq Y \qquad \Longrightarrow \qquad \langle X \rangle \subseteq \langle Y \rangle,$$

da bei $X \subseteq Y$ ja jede Linearkombination von Vektoren aus X auch eine Linearkombination von Vektoren aus Y ist, wenn für die Vektoren aus $Y \setminus X$ der Koeffizient Null gewählt wird. Damit ergibt sich sofort:

Wird M von $X \subseteq M$ erzeugt, und ist $Y \subseteq M$ eine Teilmenge mit $X \subseteq Y$, so wird M auch von Y erzeugt.

Analog dazu soll nun formalisiert werden, was eine „Vergrößerung“ (oder auch „Verkleinerung“) eines Erzeugendensystems sein soll - dazu muß eine Ordnung auf Systemen definiert werden:

Definition 2.2.15. *Sei M eine nicht-leere Menge. Sind $J \subseteq I$ nicht-leere Indexmengen und $(y_j)_{j\in J}$ und $(x_i)_{i\in I}$ Systeme von Elementen aus M mit $y_j = x_j$ für $j \in J$, so heißt $(y_j)_{j\in J}$ ein Teilsystem von $(x_i)_{i\in I}$, und dieses ein Obersystem oder eine Erweiterung (erweitertes System) von $(y_j)_{j\in J}$.*
Dies definiert eine partielle Ordnung auf Systemen von Elementen aus M, und in diesem Sinne werden Begriffe wie „größer“ und „kleiner“ bezüglich Systemen verwendet.
Ist M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein Erzeugendensystem von M, so heißt es minimales Erzeugendensystem, falls jedes echt kleinere Teilsystem von $(x_i)_{i\in I}$ kein Erzeugendensystem von M mehr ist. □

Beispiel 2.2.16.

i.) Die Teilsysteme von $(1,1,2)$ sind:

$$(1),\ (2),\ (1,1),\ (1,2),\ (1,1,2).$$

ii.) $(2,1)$ ist kein Teilsystem von $(1,2)$, aber von $(1,2,1)$. □

Damit kann nun formuliert werden:

Lemma 2.2.17. *Sei M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein Erzeugendensystem von M. Dann ist auch jede Erweiterung von $(x_i)_{i\in I}$ ein Erzeugendensystem von M.*

Beweis.
Sei $(y_j)_{j\in J}$ eine Erweiterung von $(x_i)_{i\in I}$, d.h. es gilt $I \subseteq J$ und $x_i = y_i$ für $i \in I$.
Ist $x \in M$ eine Linearkombination des Erzeugendensystems $(x_i)_{i\in I}$ mit dem Koeffizientensystem $(a_i)_{i\in I} \in \bigoplus_{i\in I} R$, so sei das System $(b_j)_{j\in J}$ definiert durch:

$$b_j := \begin{cases} a_j & \text{für } j \in I, \\ 0_R & \text{für } j \notin I. \end{cases}$$

Dann gilt offensichtlich $(b_j)_{j\in J} \in \bigoplus_{j\in J} R$, und es folgt:

$$\sum_{j\in J} b_j y_j = \sum_{j\in I} b_j y_j = \sum_{j\in I} a_j x_j = x.$$

Somit ist auch $(y_j)_{j\in J}$ ein Erzeugendensystem von M. □

Bemerkung 2.2.18. *Im Hinblick auf Lemma 2.2.13 ist es zur Analyse von linearen Abbildungen natürlich sinnvoll, Erzeugendensysteme zu verkleinern, anstatt sie zu vergrößern. Die Frage nach minimalen Erzeugendensystemen wird hier jedoch nicht weiter verfolgt, da im nächsten Abschnitt ein wesentlich nützlicherer Begriff, der des „linear unabhängigen Erzeugendensystems“ (bzw. Basis) betrachtet wird, der zumindest in Vektorräumen den Begriff des minimalen Erzeugendensystems ersetzt.* □

Basen.

Im Abschnitt über Erzeugendensysteme wurde im $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ das Erzeugendensystem $\big((1,0),\,(0,1)\big)$ betrachtet, und offensichtlich existiert zu jedem Vektor $(x,y) \in \mathbb{R}^2$ genau ein Koeffizientensystem, mit dem sich (x,y) als Linearkombination von $\big((1,0),\,(0,1)\big)$ schreiben läßt:

$$(x,y) = \alpha\cdot(1,0) + \beta\cdot(0,1) \text{ mit } (\alpha,\beta) \in \mathbb{R}^2 \quad \Longrightarrow \quad (\alpha,\beta) = (x,y).$$

Dabei ist (x,y) auf der linken Seite der Aussage ein Vektor des $\mathbb{R}^2$, auf der rechten Seite ein Koeffizientensystem - beides fällt hier zusammen.
In Bemerkung 2.2.6 trat das Beispiel auf, daß bzgl. eines Erzeugendensystems ein Vektor auch mit mehreren verschiedenen Koeffizientensystemen als Linearkombination dargestellt werden kann: $\big((1,0),\,(0,1),\,(1,1)\big)$ ist ein Erzeugendensystem des $\mathbb{R}^2$, und der Vektor $(1,2) \in \mathbb{R}^2$ ist eine Linearkombination dessen mit den Koeffizientensystemen $(1,2,0)$ und $(0,1,1)$.
Dies führt zu folgender Definition:

Definition 2.2.19. *Sei M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein Erzeugendensystem von M. Dieses heißt Basis, wenn jeder Vektor $x \in M$ mit genau einem Koeffizientensystem als Linearkombination von $(x_i)_{i\in I}$ dargestellt werden kann. Diese Koeffizienten heißen dann auch die Koordinaten von x.* □

Bemerkung 2.2.20. *Jeder R-Modul M besitzt nach Lemma 2.2.12 ein Erzeugendensystem (nämlich sich selbst), aber es ist nicht klar, ob es immer ein so spezielles Erzeugendensystem wie eine „Basis“ gibt: Allgemein kann dies später für Vektorräume gezeigt werden, also Moduln mit Skalaren aus einen Körper - für Moduln über allgemeineren Ringen gilt eine so allgemeine Existenzaussage nicht. Zum Beispiel besitzt der $\mathbb{Z}$-Modul $\mathbb{Q}$ keine Basis.* □

Beispiel 2.2.21.

i.) Die beiden Erzeugendensysteme $\big((1,0),\,(0,1)\big)$ *und* $\big((1,1),\,(-1,1)\big)$ *des* $\mathbb{R}^2$ *sind gleichzeitig auch Basen.*

ii.) $(1_{\mathbb{Z}})$ *ist eine Basis des* $\mathbb{Z}$*-Moduls* $\mathbb{Z}$. □

Ist M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein Erzeugendensystem, so kann der Test, ob jedes $x \in M$ eine eindeutige Darstellung als Linearkombination von $(x_i)_{i\in I}$ hat und dieses System dann sogar eine Basis ist, auf den Test der Null eingeschränkt werden, denn es gilt:

Lemma 2.2.22. *Sei* M *ein* R*-Modul/Vektorraum und* $(x_i)_{i\in I}$ *ein Erzeugendensystem. Dann sind äquivalent:*

i.) Der Nullvektor $0_M \in M$ *hat eine eindeutige Darstellung als Linearkombination von* $(x_i)_{i\in I}$.

ii.) Jedes $x \in M$ *hat eine eindeutige Darstellung als Linearkombination von* $(x_i)_{i\in I}$ *(d.h.* $(x_i)_{i\in I}$ *ist eine Basis von* M*).*

Beweis.

i.) $\Longrightarrow$ *ii.)*: $x \in M$ habe die beiden Linearkombinationsdarstellungen:

$$\sum_{i\in I} a_i x_i = x = \sum_{i\in I} b_i x_i.$$

Es folgt sofort:

$$\sum_{i\in I} a_i x_i - \sum_{i\in I} b_i x_i = 0_M \quad\Longrightarrow\quad \sum_{i\in I}(a_i - b_i)x_i = 0_M.$$

Der Nullvektor 0_M hat auf jeden Fall eine Linearkombinationsdarstellung

$$0_M = \sum_{i\in I} 0_R \cdot x_i,$$

so daß wegen der Eindeutigkeit der Darstellung der Null dann gilt:

$$a_i - b_i = 0_R \text{ für alle } i \in I \quad\Longrightarrow\quad a_i = b_i \text{ für alle } i \in I$$

Mit $a_i = b_i$ für alle $i \in I$ sind die Koeffizientensysteme der beiden Linearkombinationsdarstellungen von x gleich, was zu zeigen war.

ii.) $\Longrightarrow$ *i.)*: Trivial. □

Beim obigen Beweis wurde benutzt, daß der Nullvektor sich immer als triviale Linearkombination eines Systems schreiben läßt (nur Nullen als Koeffizienten), was sofort folgende offensichtliche Äquivalenz liefert:

$$0_M \text{ hat eine eindeutige Darstellung als Linearkombination von } (x_i)_{i\in I}.$$
$$\Updownarrow$$
$$\sum_{i\in I} a_i x_i = 0_M \quad\Longrightarrow\quad a_i = 0_R \text{ für alle } i \in I.$$

Dies liefert Anlaß zu folgender Definition:

Definition 2.2.23. *Sei M ein R-Modul/Vektorraum. Ein System $(x_i)_{i\in I}$ von Vektoren aus M heißt linear unabhängig, falls gilt:*

$$\sum_{i\in I} a_i x_i = 0_M \quad \Longrightarrow \quad a_i = 0_R \text{ für alle } i \in I.$$

Ein System von Vektoren $(x_i)_{i\in I}$ heißt linear abhängig, falls es nicht linear unabhängig ist. □

Bemerkung 2.2.24.

i.) *Ist M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein System von Vektoren aus M, so ist dieses offensichtlich lineaer abhängig, wenn ein x_k der Nullvektor ist, da dann eine nicht-triviale Linearkombination von $(x_i)_{i\in I}$ der Null existiert:*

$$\sum_{i\in I} a_i x_i = 0 \quad \text{mit} \quad a_i := \begin{cases} 1 & \text{für } i = k, \\ 0 & \text{sonst.} \end{cases}$$

Als Beispiel sei folgendes System von Vektoren des $\mathbb{R}^2$ betrachtet, welches den Nullvektor enthält:

$$\big((0,0),\ (1,2),\ (2,1) \big).$$

Dann wäre das einleitend dazu konstruierte nicht-triviale Koeffizientensystem $(1,0,0)$, und es gilt:

$$1 \cdot (0,0) + 0 \cdot (1,2) + 0 \cdot (2,1) = (0,0).$$

ii.) *Ist M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein System von Vektoren aus M, so ist dieses linear abhängig, wenn es zwei gleiche Vektoren enthält, denn für $x_j = x_k$ mit $j \neq k$ existiert offensichtlich eine nicht-triviale Linearkombination von $(x_i)_{i\in I}$ der Null:*

$$\sum_{i\in I} a_i x_i = 0 \quad \text{mit} \quad a_i := \begin{cases} 1 & \text{für } i = j, \\ -1 & \text{für } i = k, \\ 0 & \text{sonst.} \end{cases}$$

Als Beispiel sei ein System (x, y, z, x) von Vektoren $x, y, z \in M$ betrachtet. Das oben dazu konstruierte nicht-triviale Koeffizientensystem wäre dann $(1, 0, 0, -1)$, und es gilt:

$$1 \cdot x + 0 \cdot y + 0 \cdot z + (-1) \cdot x = x - x = 0.$$

iii.) *Ist M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein linear abhängiges System von Vektoren aus M, so ist jede Erweiterung $(y_j)_{j\in J}$ davon auch linear abhängig, denn ist $\sum_{i\in I} a_i x_i = 0$ eine nicht-triviale Linearkombination der Null (d.h. mindestens ein $a_k \neq 0$), so liegt mit $I \subseteq J$ auch das erweiterte Koeffizientensystem*

$$(b_j)_{j\in J} \quad \text{mit} \quad b_j := \begin{cases} a_j & \text{für } j \in I, \\ 0 & \text{sonst} \end{cases} \qquad \text{mit } b_k = a_k \neq 0$$

in $\bigoplus_{j\in J} R$ und liefert eine nicht-triviale Linearkombination von $(y_j)_{j\in J}$ der Null:

$$\sum_{j\in J} b_j y_j = \sum_{j\in I} b_j y_j = \sum_{i\in I} a_i x_i = 0.$$

Anschaulich wird für jeden Vektor, der in das System $(x_i)_{i\in I}$ hinzugefügt wird, in das Koeffizientensystem $(a_i)_{i\in I}$ an entsprechender Stelle ein Koeffizient Null eingeführt, so daß sich in der erweiterten Linearkombination nichts ändert.

iv.) *Ist M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein linear unabhängiges System von Vektoren, so ist auch jedes Teilsystem $(y_j)_{j\in J}$ davon linear unabhängig, denn wäre $\sum_{j\in J} a_j y_j = 0$ eine nicht-triviale Linearkombination der Null (d.h. mindestens ein $a_k \neq 0$), so läge mit $J \subseteq I$ auch das „aufgefüllte" Koeffizientensystem*

$$(b_i)_{i\in I} \quad \text{mit} \quad b_i := \begin{cases} a_i & \text{für } i \in J, \\ 0 & \text{sonst} \end{cases} \qquad \text{mit } b_k = a_k \neq 0$$

in $\bigoplus_{i\in I} R$ und es wäre

$$\sum_{i\in I} b_i x_i = \sum_{i\in J} b_i x_i = \sum_{j\in J} a_j y_j = 0$$

eine nicht-triviale Linearkombination der Null und damit $(x_i)_{i\in I}$ linear abhängig, im Widerspruch zur Voraussetzung.

v.) *Die obigen vier Aussagen seien noch einmal salopp als Merkregeln formuliert:*
- *Ein System, das einen Nullvektor enthält, ist linear abhängig.*
- *Ein System, das zwei gleiche Vektoren enthält, ist linear abhängig.*
- *Eine Erweiterung eines linear abhängigen Systems ist linear abhängig.*
- *Ein Teilsystem eines linear unabhängigen Systems ist linear unabhängig.* □

Beispiel 2.2.25.

i.) *Sei K ein Körper und V ein K-Vektorraum. Ist $v \in V$ nicht der Nullvektor, so ist (v) ein einelementiges linear unabhängiges System, denn nach Lemma 2.1.10 gilt in dem Vektorraum V mit $v \neq 0_V$ für ein $\alpha \in K$:*

$$\alpha \cdot \underbrace{v}_{\neq 0_V} = 0_V \qquad \Longrightarrow \qquad \alpha = 0.$$

Damit gilt vor allen Dingen:

In einem Vektorraum V mit $V \neq \{0_V\}$ existieren linear unabhängige Systeme.

ii.) *Es sei der $\mathbb{Z}$-Modul $\mathbb{Z}_n$ betrachtet (skalare Multiplikation: $a \bullet [b]_n := [ab]_n$). Dann gilt für ein beliebiges System $\big([a_i]_n\big)_{i\in I}$ von Vektoren aus $\mathbb{Z}_n$:*

$$\sum_{i\in I} n \bullet [a_i]_n = \sum_{i\in I} [na_i]_n = \sum_{i\in I} [0]_n = [0]_n,$$

und wegen $n \neq 0$ ist das System $\big([a_i]_n\big)_{i\in I}$ dann linear abhängig. Damit gilt vor allen Dingen:

Der $\mathbb{Z}$-Modul $\mathbb{Z}_n$ enthält kein linear unabhängiges System.

iii.) *Für den $\mathbb{Z}$-Modul $\mathbb{Q}$ gilt: jedes System mit mindestens zwei Vektoren ist linear abhängig. Enthält $(x_i)_{i\in I}$ mit $|I| \geq 2$ eine Null, so ist das System nach Bemerkung 2.2.24 linear abhängig. Ansonsten gibt es mindestens zwei Vektoren x_j und x_k, die nicht der Nullvektor sind, und die Brüche $x_j = \frac{z_j}{n_j}$ und $x_k = \frac{z_k}{n_k}$ mit*

$z_j, n_j, z_k, n_k \in \mathbb{Z} \setminus \{0\}$ erlauben dann eine nicht-triviale Linearkombination von $(x_i)_{i\in I}$ der Null mit dem Koeffizientensystem:

$$\sum_{i\in I} a_i x_i = 0 \quad \textit{mit} \quad a_i := \begin{cases} -n_j z_k & \textit{für } i = j, \\ n_k z_j & \textit{für } i = k, \\ 0 & \textit{sonst.} \end{cases}$$

Ein Beispiel dazu wäre das System $\left(\frac{7}{2}, \frac{5}{3}, \frac{11}{17}\right)$, und eine oben dazu konstruierte nicht-triviale Linearkombination (aus den ersten beiden Brüchen):

$$\underbrace{(-2\cdot 5,\, 3\cdot 7,\, 0)}_{\textit{Koeffizientensystem}} \quad \Longrightarrow \quad (-2\cdot 5)\cdot\frac{7}{2} + (3\cdot 7)\cdot\frac{5}{3} + 0\cdot\frac{11}{17} = 0. \qquad \square$$

Damit läßt sich eine Basis eines Moduls/Vektorraumes durch folgende Äquivalenzen beschreiben:

Satz 2.2.26. *Sei M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ ein System von Vektoren aus M. Dann sind äquivalent:*

i.) $(x_i)_{i\in I}$ ist eine Basis von M.
ii.) Jedes $x \in M$ hat eine eindeutige Darstellung als Linearkombination von $(x_i)_{i\in I}$.
iii.) $(x_i)_{i\in I}$ ist ein linear unabhängiges Erzeugendensystem von M.

Beweis.

i.) $\Longleftrightarrow$ *ii.)*: Definition 2.2.19: *ii.)* die die Definition einer Basis.

ii.) $\Longrightarrow$ *iii.)*: Da jeder Vektor aus M eine Darstellung als Linearkombination von $(x_i)_{i\in I}$ hat, ist dies ein Erzeugendensystem von M, und da der Nullvektor eine eindeutige Darstellung hat, ist das System linear unabhängig.

iii.) $\Longrightarrow$ *ii.)*: Da $(x_i)_{i\in I}$ ein Erzeugendensystem ist, hat jeder Vektor eine Darstellung als Linearkombination von $(x_i)_{i\in I}$.
Die lineare Unabhängigkeit von $(x_i)_{i\in I}$ ist äquivalent zur eindeutigen Darstellbarkeit des Nullvektors, und dies ist nach Lemma 2.2.22 wiederum äquivalent zur eindeutigen Darstellbarkeit eines jeden Vektors. $\square$

Die Bedingung der linearen Unabhängigkeit ist ein nützliches Testkritierium, wenn ein Erzeugendensystem darauf getestet werden soll, ob es auch eine Basis ist. Eine Anwendung davon liefern die folgenden Betrachtungen:
Die Vektoren $(1,0)$ und $(0,1)$ bilden im $\mathbb{R}^2$ offensichtlich eine Basis $\big((1,0), (0,1)\big)$, da in dem Tupel-Raum $\mathbb{R}^2$ komponentenweise gerechnet wird. Um dies zu verallgemeinern, sei definiert:

Definition 2.2.27. *Ist I eine nicht-leere Indexmenge, so ist für $i, j \in I$ das Symbol $\delta_{i,j}$ definiert durch:*

$$\delta_{i,j} := \begin{cases} 0 & \textit{für } i \neq j, \\ 1 & \textit{für } i = j. \end{cases}$$

$\delta_{i,j}$ heißt auch das Kroneckersymbol.
Sei R ein kommutativer Ring mit Eins und I eine nicht-leere Indexmenge. Dann ist für $k \in I$ definiert:

$$e_k^{I,R} := (\delta_{i,k})_{i\in I} \in \prod_{i\in I} R.$$

Hierbei wird stillschweigend vorausgesetzt, daß das Kroneckersymbol die Werte 0_R und 1_R aus dem Ring annimmt.
Wenn der Kontext klar ist, in dem ein I-Tupel $e_k^{I,R}$ auftritt, dann wird nur e_k anstelle von $e_k^{I,R}$ geschrieben. □

Bemerkung 2.2.28. *Wegen der komponentenweisen Addition und skalaren Multiplikation im R-Modul/Vektorraum $\prod_{i\in I} R$ gilt für eine Linearkombination von $(e_i)_{i\in I}$ mit einem Koeffizientensystem $(a_i)_{i\in I}$ offensichtlich:*

$$\sum_{i\in I} a_i e_i = (a_i)_{i\in I},$$

da im Vektor $a_i e_i$ genau an der i-ten Komponente a_i steht und sonst nur Nullen.
Ein Beispiel dazu wäre:

$$3\cdot(1,0,0)+4\cdot(0,1,0)-2\cdot(0,0,1)=(3,0,0)+(0,4,0)+(0,0,-2)=(3,4,-2).$$ □

Es gilt dann:

Lemma 2.2.29. *Sei R ein kommutativer Ring mit Eins bzw. ein Körper, und I eine nicht-leere Indexmenge. Weiter seien $e_k := (\delta_{i,k})_{i\in I}$ für $k \in I$ wie in Definition 2.2.27. Es gilt:*

i.) $(e_i)_{i\in I}$ ist eine Basis des R-Moduls/Vektorraumes $\bigoplus_{i\in I} R$. Und ist I eine endliche Menge, so ist das System $(e_i)_{i\in I}$ auch eine Basis des R-Moduls/Vektorraums $\prod_{i\in I} R$ (siehe auch Bemerkung 2.2.4).
Insbesondere für die Indexmenge $I := \{1,\dots,n\}$ ist folgendes System eine Basis des R-Moduls/Vektorraumes R^n:

$$(e_1,\dots,e_n) \quad \text{mit} \quad e_k := (0,\dots,0,\underbrace{1}_{k\text{-te Stelle}},0,\dots,0)\in R^n.$$

Die Basis $(e_i)_{i\in I}$ des R-Moduls $\bigoplus_{i\in I} R$ wird auch häufig dessen Standard-Basis oder kanonische Basis genannt.

ii.) Ist I keine endliche Menge, so ist das System $(e_i)_{i\in I}$ zwar linear unabhängig, aber kein Erzeugendensystem des R-Moduls/Vektorraumes $\prod_{i\in I} R$.

Beweis.

i.) Ein Vektor $x \in \bigoplus_{i\in I} R$ hat die Form:

$$x = (x_i)_{i\in I} \quad \text{mit:} \quad \text{nur endlich viele } x_i \in R \text{ sind ungleich Null.}$$

Nach Bemerkung 2.2.28 ist x eine Linearkombination von $(e_i)_{i\in I}$ mit dem Koeffizientensystem $(x_i)_{i\in I}$ und $(e_i)_{i\in I}$ somit ein Erzeugendensystem von $\bigoplus_{i\in I} R$:

$$x = \sum_{i\in I} x_i \cdot e_i = (x_i)_{i\in I}.$$

Das System $(e_i)_{i\in I}$ ist linear unabhängig, denn der Nullvektor $(0_R)_{i\in I} \in \bigoplus_{i\in I} R$ hat offensichtlich eine eindeutige Darstellung als Linearkombination von $(e_i)_{i\in I}$:

$$\sum_{i\in I} a_i e_i = (0_R)_{i\in I} \quad \overset{2.2.28}{\Longrightarrow} \quad (a_i)_{i\in I} = (0_R)_{i\in I} \quad \Longrightarrow \quad a_i = 0_R \text{ für alle } i \in I.$$

Für eine endliche Menge I gilt nach Bemerkung 2.2.4 $\bigoplus_{i\in I} R = \prod_{i\in I} R$, so daß die weiteren Aussagen klar sind.

ii.) Ist I eine unendliche Menge, so ist $(1_R)_{i\in I} \in \prod_{i\in I} R$ keine Linearkombination von $(e_i)_{i\in I}$, denn wegen

$$\sum_{i\in I} a_i e_i = (a_i)_{i\in I}$$

können Linearkombinationen von $(e_i)_{i\in I}$ immer nur endlich viele $a_i \neq 0_R$ enthalten. Die lineare Unabhängigkeit des Systems $(e_i)_{i\in I}$ gilt nach dem ersten Teil. □

Bemerkung 2.2.30.

i.) Im R-Modul/Vektorraum R^n ist die Standard-Basis $(e_1, \ldots, e_n)$ besonders nützlich, da zu einem Vektor $x := (x_1, \ldots, x_n) \in R^n$ sofort das Koeffizientensystem gegeben ist, mit dem der Vektor x als (eindeutige) Linearkombination der Standard-Basis geschrieben werden kann - also dessen Koordinaten bzgl. der Standard-Basis:

$$x = (x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i e_i \quad \rightsquigarrow \quad \left.\begin{array}{l}\textit{Koordinaten von } x \textit{ bzgl. der} \\ \textit{Basis } (e_1, \ldots, e_n)\end{array}\right\} : (x_1, \ldots, x_n).$$

ii.) Bei den Tupelräumen R^n tritt bzgl. der Standard-Basis das Phänomen auf, daß der Vektor und seine Koordinaten die gleiche Form haben. Dies führt mitunter zur Verwirrung - die nicht besser wird, wenn Koordinaten eines Tupels bzgl. einer anderen Basis im Tupelraum betrachtet werden: Zum Beispiel ist $B := \big((1,2), (2,1)\big)$ eine Basis des $\mathbb{R}^2$, und der Vektor $(3,3) \in \mathbb{R}^2$ hat bzgl. dieser Basis die Koordinaten $(1,1)$:

$$(3,3) = 1 \cdot (1,2) + 1 \cdot (2,1) \quad \rightsquigarrow \quad \textit{Koordinaten von } (3,3) \textit{ bzgl. der Basis } B : (1,1).$$

iii.) Werden die beiden Tupelräume R^n und R^m betrachtet und darin deren Standard-Basen, so wird z.B. meist kurz geschrieben:

Wähle die Standard-Basis $(e_1, \ldots, e_m)$ des R^m und $(e_1, \ldots, e_n)$ des R^n ...

Dabei ist dann der Vektor $e_i \in R^m$ ein m-Tupel, und $e_i \in R^n$ ein n-Tupel, und es werden zwei verschiedene Objekte mit dem gleichen Symbol geschrieben. Eine Lösung wäre eine „sperrige“ Schreibweise „e_i^n“ analog zur formalen Definition in 2.2.27, aber es wird fast immer darauf vertraut, daß der Leser sich zurechtfindet, welches Objekt er gerade vor sich hat.

iv.) Im R-Modul R ist die Standard-Basis von der Form (1_R), und im R^1 von der Form $\big((1_R)\big)$: oft wird dann jede Klammerung weggelassen und einfach von der Basis “1_R„ geredet. □

In Lemma 2.2.13 wurde schon gezeigt, daß Erzeugendensysteme nützlich für die Betrachtung linearer Abbildungen sind - dessen Aussage kann nun durch die Beschränkung auf Basen, also spezielle Erzeugendensysteme, wesentlich verbessert werden:

Satz 2.2.31. *(Hauptsatz über lineare Abbildungen und Basen)*
Sei M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ eine Basis von M. Es sei V ein weiterer R-Modul/Vektorraum. Dann gelten:

i.) Konstruktion linearer Abbildungen:
Sei $(v_i)_{i\in I}$ ein beliebiges System von Vektoren aus V. Dann gibt es eine eindeutig bestimmte lineare Abbildung $\varphi \in \mathrm{Hom}_R(M,V)$, für die gilt:

$$\varphi(x_i) = v_i \text{ für alle } i \in I, \text{ und damit allgemein}: \varphi\Big(\sum_{i\in I} a_i x_i\Big) = \sum_{i\in I} a_i v_i.$$

Damit können insbesondere für die Basisvektoren x_i aus M beliebige Bilder v_i aus V vorgegeben werden, und die rechte Seite liefert eine dadurch induzierte Abbildungsvorschrift für eine lineare Abbildung von M nach V:

$$f\colon x_i \mapsto v_i \text{ für alle } i \in I \quad \rightsquigarrow \quad \varphi\colon \sum_{i\in I} a_i x_i \mapsto \sum_{i\in I} a_i v_i.$$

Dann heißt φ auch die lineare Fortsetzung der Abbildung f, die nur auf der Menge der Basisvektoren aus M definiert ist: $f\colon \{\, x_i \mid i \in I \,\} \longrightarrow V$.

ii.) Für eine lineare Abbildung $\varphi \in \mathrm{Hom}_R(M,V)$ gilt:

$$\begin{aligned} \varphi \text{ injektiv} \quad &\Longleftrightarrow \quad \big(\varphi(x_i)\big)_{i\in I} \text{ ist ein linear unabhängiges System.} \\ \varphi \text{ surjektiv} \quad &\Longleftrightarrow \quad \big(\varphi(x_i)\big)_{i\in I} \text{ ist ein Erzeugendensystem von } V. \\ \varphi \text{ bijektiv} \quad &\Longleftrightarrow \quad \big(\varphi(x_i)\big)_{i\in I} \text{ ist eine Basis von } V. \end{aligned}$$

iii.) Für zwei lineare Abbildungen $\varphi, \psi \in \mathrm{Hom}_R(M,V)$ gilt:

$$\varphi = \psi \quad \Longleftrightarrow \quad \varphi(x_i) = \psi(x_i) \text{ für alle } i \in I.$$

Zwei lineare Abbildungen stimmen also (auf dem ganzen Raum) überein, wenn sie schon auf einer Basis übereinstimmen.

Beweis.

i.) Zur Existenz von φ: Jeder Vektor $x \in M$ hat eine eindeutige Darstellung $\sum_{i\in I} a_i x_i$ als Linearkombination von $(x_i)_{i\in I}$, da dieses System eine Basis von M ist. Mit Hilfe der eindeutigen Koordinaten $(a_i)_{i\in I} \in \bigoplus_{i\in I} R$ von x bzgl. der Basis $(x_i)_{i\in I}$ kann eine Abbildung von M nach V definiert werden durch:

$$\varphi\colon M \longrightarrow V \quad \text{mit} \quad x \mapsto \sum_{i\in I} a_i v_i, \quad (a_i)_{i\in I} \text{ die Koordinaten von } x \text{ bzgl. } (x_i)_{i\in I}.$$

Es muß nun gezeigt werden, daß φ eine lineare Abbildung ist, was sich sofort aus den Regeln für das Rechnen mit Linearkombinationen ergibt (siehe Lemma 2.2.9), denn für $x := \sum_{i\in I} a_i x_i$ und $y := \sum_{i\in I} b_i x_i$ und $r \in R$ folgt:

$$\begin{aligned} \varphi(x+y) &= \varphi\Big(\sum_{i\in I} a_i x_i + \sum_{i\in I} b_i x_i\Big) \overset{(2.2.9)}{=} \varphi\Big(\sum_{i\in I} (a_i+b_i) x_i\Big) \overset{(\mathrm{Def})}{=} \sum_{i\in I} (a_i+b_i) v_i \\ &\overset{(2.2.9)}{=} \Big(\sum_{i\in I} a_i v_i\Big) + \Big(\sum_{i\in I} b_i v_i\Big) \overset{(\mathrm{Def})}{=} \varphi\Big(\sum_{i\in I} a_i x_i\Big) + \varphi\Big(\sum_{i\in I} b_i x_i\Big) \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

$$\varphi(rx) = \varphi\Big(r \sum_{i\in I} a_i x_i\Big) \overset{(2.2.9)}{=} \Big(\sum_{i\in I} (ra_i) x_i\Big) \overset{(\mathrm{Def})}{=} \sum_{i\in I} (ra_i) v_i \overset{(2.2.9)}{=} r \sum_{i\in I} a_i v_i$$

$$\overset{\text{(Def)}}{=} r\varphi\Big(\sum_{i\in I} a_i x_i\Big) = r\varphi(x).$$

Die so definierte lineare Abbildung erfüllt offensichtlich die geforderten Bedingungen, und sie ist nach Lemma 2.2.13 eindeutig durch ihre Festlegung auf der Basis $(x_i)_{i\in I}$, da diese insbesondere ein Erzeugendensystem ist.

ii.) φ injekiv $\Longrightarrow \big(\varphi(x_i)\big)_{i\in I}$ l.u.: Es ist zu zeigen:

$$\sum_{i\in I} a_i\varphi(x_i) = 0_V \qquad \Longrightarrow \qquad a_i = 0_R \text{ für alle } i \in I.$$

Da φ injektiv ist, gilt nach Lemma 2.1.27 $\ker(\varphi) = \{0_M\}$, woraus sofort mit der linearen Unabhängigkeit von $(x_i)_{i\in I}$ folgt:

$$0_V = \sum_{i\in I} a_i\varphi(x_i) \overset{(2.2.13)}{=} \varphi\Big(\sum_{i\in I} a_i x_i\Big) \qquad \Longrightarrow \qquad \sum_{i\in I} a_i x_i \in \ker(\varphi) = \{0_M\}$$

$$\Longrightarrow \qquad \sum_{i\in I} a_i x_i = 0_M \overset{(x_i)_{i\in I}\text{ l.u.}}{\Longrightarrow} a_i = 0_R \text{ für alle } i \in I.$$

$\big(\varphi(x_i)\big)_{i\in I}$ l.u. $\Longrightarrow \varphi$ injektiv: Nach Lemma 2.1.27 reicht es zu zeigen, daß gilt:

$$\ker(\varphi) = \{0_M\}.$$

Sei nun $x \in \ker(\varphi)$. Dann ist x eine Linearkombination $x = \sum_{i\in I} a_i x_i$ der Basis $(x_i)_{i\in I}$, und es folgt mit der linearen Unabhängigkeit von $\big(\varphi(x_i)\big)_{i\in I}$:

$$x \in \ker(\varphi) \qquad \Longrightarrow \qquad \varphi(x) = 0_V \qquad \Longrightarrow \qquad \varphi\Big(\sum_{i\in I} a_i x_i\Big) = 0_V$$

$$\Longrightarrow \qquad \sum_{i\in I} a_i\varphi(x_i) = 0_V \overset{(\varphi(x_i))_{i\in I}\text{ l.u.}}{\Longrightarrow} a_i = 0_R \text{ für alle } i \in I$$

$$\Longrightarrow \qquad x = \sum_{i\in I} a_i x_i = 0_M.$$

Also enthält der Kern von φ nur den Nullvektor aus M und φ ist injektiv.

φ surjektiv $\Longrightarrow \big(\varphi(x_i)\big)_{i\in I}$ EZS von V: Nach Lemma 2.2.13 ist $\big(\varphi(x_i)\big)_{i\in I}$ ein Erzeugendensystem von $\operatorname{im}(\varphi)$, und da φ surjektiv ist, gilt $\operatorname{im}(\varphi) = V$, und $\big(\varphi(x_i)\big)_{i\in I}$ ist somit sogar ein Erzeugendensystem von V.

$\big(\varphi(x_i)\big)_{i\in I}$ EZS von $V \Longrightarrow \varphi$ surjektiv: Es gilt $\langle\, \varphi(x_i)\,\rangle_{i\in I} = V$, und nach Lemma 2.2.13 auch $\langle\, \varphi(x_i)\,\rangle_{i\in I} = \operatorname{im}(\varphi)$, also $\operatorname{im}(\varphi) = V$, und φ ist damit surjektiv.

φ bijektiv $\Longleftrightarrow \big(\varphi(x_i)\big)_{i\in I}$ Basis: Dies folgt aus den vorherigen Aussagen, denn bijektiv entspricht injektiv *und* surjekiv, und Basis entspricht linear unabhängig *und* Erzeugendensystem (Satz 2.2.26).

iii.) Da Basen auch Erzeugendensysteme sind, gilt diese Äquivalenz nach Lemma 2.2.13. $\square$

Bemerkung 2.2.32.

i.) Bei der Konstruktion von linearen Abbildungen durch die Festlegung von Bildern auf einer Basis kann mit Satz 2.2.31.ii.) mitunter sogar eine gewünschte Eigenschaft wie „injektiv“, „surjektiv“ oder „bijektiv“ erreicht werden, wenn das System der Bilder mit entsprechender Eigenschaft gewählt werden kann.
So sind z.B. die beiden Systeme $\big((1,0),\,(0,1)\big)$ *und* $\big((1,2),\,(2,1)\big)$ *Basen des* $\mathbb{R}^2$*, und die Zuordnung*

$$f\colon (1,0)\mapsto(1,2),\quad (0,1)\mapsto(2,1)$$

liefert dann eine bijektive lineare Abbildung von $\mathbb{R}^2$ *nach* $\mathbb{R}^2$*, also einen Vektorraumautomorphismus von* $\mathbb{R}^2$*, durch lineare Fortsetzung:*

$$\varphi\colon \mathbb{R}^2\longrightarrow\mathbb{R}^2 \quad \textit{mit} \quad (x,y)\mapsto(x+2y,\,2x+y).$$

Dies folgt aus der Koordinatendarstellung $(x,y)=x\cdot(1,0)+y\cdot(0,1)$ *bzgl. der Standard-Basis des* $\mathbb{R}^2$ *und der in Satz 2.2.31 beschriebenen „Koordinaten“-Zuordnung* $\varphi\colon\ \sum_{i\in I}a_ix_i\mapsto\sum_{i\in I}a_iv_i$*:*

$$(x,y)=x\cdot\underbrace{(1,0)}_{x_1}+y\cdot\underbrace{(0,1)}_{x_2}\mapsto x\cdot\underbrace{(1,2)}_{v_1}+y\cdot\underbrace{(2,1)}_{v_2}=(x,2x)+(2y,y)=(x+2y,\,2x+y).$$

ii.) Im vorherigen Beispiel wurde auf der Standard-Basis des $\mathbb{R}^2$ *eine Automorphismus definiert, in dem dieser eine weitere Basis des* $\mathbb{R}^2$ *zugeordnet wurde:* $(1,0)\mapsto(1,2)$ *und* $(0,1)\mapsto(2,1)$*. Insbesondere konnte dann die Abbildung für jeden Vektor* $(x,y)\in\mathbb{R}^2$ *aus der Koordinatendarstellung von* (x,y) *bzgl. der Standard-Basis hergeleitet werden:* $(x,y)\mapsto(x+2y,\,2x+y)$*.*
Wird auf einer „Nicht-Standard-Basis“ des $\mathbb{R}^2$ *durch lineare Fortsetzung eine lineare Abbildung konstruiert, z.B. auf* $\big((2,3),\,(1,1)\big)$ *durch*

$$(2,3)\mapsto 3 \quad \textit{und} \quad (1,1)\mapsto 7,$$

so ist nicht sofort klar, wie das Bild eines Vektors $(x,y)\in\mathbb{R}^2$ *unter der linearen Fortsetzung obiger Festlegung aussieht, da dazu die Koordinaten von* (x,y) *bzgl. der Basis* $\big((2,3),\,(1,1)\big)$ *nötig sind:*

$$(x,y)=\alpha\cdot(2,3)+\beta\cdot(1,1) \qquad\Longrightarrow\qquad (x,y)\mapsto\alpha\cdot 3+\beta\cdot 7.$$

Es folgt $\alpha=-x+y$ *und* $\beta=3x-2y$*, und es folgt als allgemeine Abbildungsvorschrift:*

$$(x,y)\mapsto(-x+y)\cdot 3+(3x-2y)\cdot 7=18x-11y.$$

iii.) Auf einem Erzeugendensystem eines Moduls/Vektorraumes kann im Gegensatz zu einer Basis nicht durch willkürliche Zuordnung von Bildern eine lineare Abbildung definiert werden. Dazu sei das Erzeugendensystem $\big((1,0),\,(0,1),\,(1,1)\big)$ *des* $\mathbb{R}^2$ *betrachtet: Zum Beispiel kann die Zuordnung*

$$(1,0)\mapsto 1,\quad (0,1)\mapsto 2 \quad \textit{und} \quad (1,1)\mapsto 4$$

nicht zu einer linearen Abbildung $\varphi\colon\mathbb{R}^2\longrightarrow\mathbb{R}$ *fortgesetzt werden, denn es gilt:*

$$\varphi\big((1,0)+(0,1)\big)=\varphi\big((1,1)\big)=4\neq 3=1+1=\varphi\big((1,0)\big)+\varphi\big((0,1)\big).$$

iv.) *In Gruppen können auch Erzeugendensysteme defniert werden - jedoch gibt es dort kein Äquivalent zu Basen in Moduln/Vektorräumen. Daher ist es auch nicht möglich, bei Gruppen Homomorphismen irgendwie durch Vorgabe von Bildern zu konstruieren.*

v.) *Für den $\mathbb{Z}$-Modul $\mathbb{Z}$ ist $(1_{\mathbb{Z}})$ eine Basis. Jede abelsche Gruppe $(G, *)$ ist ein $\mathbb{Z}$-Modul mit der skalaren Multiplikation $n \bullet g := g^n$ (siehe auch Beispiel 2.1.9), und so kann von $\mathbb{Z}$ nach G eine lineare Abbildung konstruiert werden, in dem $1_{\mathbb{Z}}$ auf ein beliebiges Element $x \in G$ abgebildet und dies dann durch $n \mapsto x^n$ linear fortgesetzt wird. Da jede lineare Abbildung insbesondere auch ein Gruppenhomomorphismus zwischen den „Gruppen der Vektoren“ist, hier $(\mathbb{Z}, +)$ und $(G, *)$, können auf diese Weise auch Gruppenhomomorphismen von $(\mathbb{Z}, +)$ in eine abelsche Gruppe konstruiert werden.*

vi.) *Für den $\mathbb{Z}$-Modul $\mathbb{Z}_n$ ist obige Konstruktion eines Gruppenhomomorphismus in eine abelsche Gruppe G nicht möglich, da $\mathbb{Z}_n$ keine Basis besitzt: nach Beispiel 2.2.25 besitzt $\mathbb{Z}_n$ kein $\mathbb{Z}$-linear unabhängiges System, und damit vor allem kein linear unabhängiges Erzeugendensystem (d.h. eine Basis).* □

Beispiel 2.2.33.

i.) *Es gibt eine surjektive lineare Abbildung von $\mathbb{R}^3$ nach $\mathbb{R}^2$, denn die Standard-Basis (e_1, e_2, e_3) des $\mathbb{R}^3$ kann auf die Standard-Basis (e_1, e_2) des $\mathbb{R}^2$ zum Beispiel durch*

$$f\colon (1,0,0) \mapsto (1,0), \quad (0,1,0) \mapsto (0,1) \quad \textit{und} \quad (0,0,1) \mapsto (1,0)$$

abgebildet werden, und dies liefert durch lineare Fortsetzung einen Vektorraum-epimorphismus:

$$\varphi\colon \mathbb{R}^3 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad (x,y,z) \mapsto (x+z, y).$$

ii.) *Ist $n \geq m$, so kann von dem R-Modul R^n immer eine surjektive lineare Abbildung in den R-Modul R^m über deren Standard-Basen konstruiert werden:*

$$e_i \in R^n \mapsto \begin{cases} e_i \in R^m & \textit{für } i \leq m, \\ 0 & \textit{für } m < i. \end{cases}$$

iii.) *Ist $n \leq m$, so kann von dem R-Modul R^n immer eine injektive lineare Abbildung in den R-Modul R^m über deren Standard-Basen konstruiert werden:*

$$e_i \in R^n \mapsto e_i \in R^m \quad \textit{für } 1 \leq i \leq n.$$ □

Existenz von Basen.

Im letzten Abschnitt wurde gezeigt, wie nützlich Basen bei der Analyse - oder sogar Konstruktion - von linearen Abbildungen zwischen Moduln/Vektorräumen sind: siehe insbesondere den Hauptsatz über lineare Abbildungen und Basen - Satz 2.2.31. Die Frage ist nur, ob es in einem Modul/Vektorraum überhaupt eine Basis gibt.

Die Antwort dazu lautet: allgemein in Moduln nein - in Vektorräumen ja!

Daß es Moduln ohne Basen gibt, wurde schon gezeigt, denn eine Basis ist ein linear unabhängiges Erzeugendensystem (Satz 2.2.26), und Moduln haben zwar immer Erzeugendensysteme (Lemma 2.2.12), aber es gibt Moduln ohne linear unabhängige Systeme (Beispiel 2.2.25, $\mathbb{Z}_n$ als $\mathbb{Z}$-Modul).

Um für Vektorräume eine Basis finden zu können, sei zuersteinmal deren Eigenschaft, ein linear unabhängiges Erzeugendensystem zu sein, näher betrachtet. Es sind also Systeme zu finden, die zwei Eigenschaften aufweisen:

- Das System muß ein Erzeugendensystem sein.
- Das System muß linear unabhängig sein.

Ein erster Ansatz könnte also sein, ein Erzeugendensystem zu nehmen und dieses zu verkleinern, um es evt. linear unabhängig zu machen, denn die lineare Abhängigkeit hat sicher etwas damit zu tun, daß zwischen Vektoren des Systems eine Relation besteht und zu viele Vektoren vorhanden sind.
Ein zweiter Ansatz wäre, linear unabhängige Systeme soweit „linear uanbhängig“ aufzufüllen, bis sie auch ein Erzeugendensystem sind.

Daß beide Ideen mögliche Ansätze sind, impliziert auch folgende Aussage:

Lemma 2.2.34. *Sei M ein R-Modul/Vektorraum und $(x_i)_{i\in I}$ eine Basis von M. Dann gelten folgende Aussagen:*

i.) $(x_i)_{i\in I}$ ist ein minimales Erzeugendensystem in M, d.h. jedes echte Teilsystem von $(x_i)_{i\in I}$ ist kein Erzeugendensystem von M mehr.

ii.) $(x_I)_{i\in I}$ ist ein maximal linear unabhängiges System, d.h. jede echte Erweiterung von $(x_i)_{i\in I}$ ist kein linear unabhängiges System mehr.

Es gelten also in Moduln/Vektorräumen die folgenden beiden Implikationen:

$$(x_i)_{i\in I} \text{ Basis} \quad \Longrightarrow \quad (x_i)_{i\in I} \text{ minimales Erzeugendensystem.}$$
$$(x_i)_{i\in I} \text{ Basis} \quad \Longrightarrow \quad (x_i)_{i\in I} \text{ maximal linear unabhängiges System.}$$

Beweis.

i.) Es ist zu zeigen, daß jedes echte Teilsystem von $(x_i)_{i\in I}$ kein Erzeugendensystem von M ist. Sei dazu $J \subsetneq I$ eine echte Teilmenge und $(y_j)_{j\in J}$ das zugehörige echte Teilsystem von $(x_i)_{i\in I}$ mit $y_j = x_j$ für $j \in J$. Dann gibt es einen Index $k \in I \setminus J$, und es reicht zu zeigen, daß x_k nicht im Erzeugnis des Teilsystems $(y_j)_{j\in J}$ liegt und dieses damit kein Erzeugendensystem von M sein kann.
Angenommen, es würde $x_k \in \langle\, y_j \,\rangle_{j\in J}$ gelten. Dann würde eine Linearkombination
$$x_k = \sum_{j\in J} b_j y_j \qquad \Longleftrightarrow \qquad 0 = (-1)\cdot x_k + \sum_{j\in J} b_j y_j$$
existieren und eine nicht-triviale Linearkombination $\sum_{i\in I} a_i x_i = 0$ implizieren mit dem Koeffizientensystem
$$(a_i)_{i\in I} \quad \text{mit} \quad a_i := \begin{cases} b_i & \text{für } i \in J, \\ -1 & \text{für } i = k, \\ 0 & \text{für } i \notin J \cup \{k\}, \end{cases}$$
wie folgende Rechnung zeigt:
$$\sum_{i\in I} a_i x_i = \sum_{i\in J\cup\{k\}} a_i x_i = a_k x_k + \sum_{i\in J} a_i x_i = -x_k + \sum_{j\in J} b_j y_j = 0.$$
Dies widerspräche aber der linearen Unabhängigkeit von $(x_i)_{i\in I}$, so daß x_k nicht im Erzeugnis des Teilsystems $(y_j)_{j\in J}$ liegen kann. Somit muß $(x_i)_{i\in I}$ schon ein minimales Erzeugendensystem sein.

ii.) Es ist zu zeigen, daß jedes echte Erweiterungssystem von $(x_i)_{i\in I}$ linear abhängig ist. Sei dazu $(y_j)_{j\in J}$ eine echte Erweiterung mit $I \subsetneq J$ und $x_i = y_i$ für $i \in I$. Weiter sei $k \in J \setminus I$, und der Vektor y_k kann dann als Linearkombination der Basis $(x_i)_{i\in I}$ geschrieben werden:

$$y_k = \sum_{i\in I} a_i x_i \qquad \Longrightarrow \qquad 0 = -y_k + \sum_{i\in I} a_i x_i.$$

Dies liefert mit folgenden Koeffizientensystem

$$(b_j)_{j\in J} \quad \text{mit} \quad b_j := \begin{cases} a_j & \text{für } j \in I, \\ -1 & \text{für } j = k, \\ 0 & \text{für } j \notin I \cup \{k\} \end{cases}$$

eine nicht-triviale Linearkombinationsdarstellung der Null bzgl. $(y_j)_{j\in J}$, so daß dieses System linear abhängig ist:

$$\sum_{j\in J} b_j y_j = \sum_{j\in I\cup\{k\}} b_j y_j = b_k y_k + \sum_{i\in I} b_i y_i = -y_k + \sum_{i\in I} a_i x_i = 0_M.$$

Damit muß $(x_i)_{i\in I}$ ein maximal linear unabhängiges System sein. □

In Moduln lassen sich allgemein die beiden Implikationen aus Lemma 2.2.35 nicht umkehren, denn es gilt zum Beispiel für den $\mathbb{Z}$-Modul $\mathbb{Z}$ (Übung!):

- $(2, 3)$ ist ein minimales Erzeugendensystem, aber keine Basis.
- (2) ist ein maximal linear unabhängiges System, aber keine Basis.

Aber In Vektorräumen gelten die Umkehrungen der beiden Implikationen aus Lemma 2.2.34, denn bei Skalaren aus einem Körper besitzen alle Skalare ungleich der Null ein multiplikatives Inverses und es kann durch sie geteilt werden:

Lemma 2.2.35. *Sei V ein Vektorraum über dem Körper K. Dann gelten für ein System $(x_i)_{i\in I}$ von Vektoren aus V folgende Aussagen.*

i.) Ist $(x_i)_{i\in I}$ ein minimales Erzeugendensystem von V, so ist $(x_i)_{i\in I}$ auch eine Basis von V.

ii.) Ist $(x_i)_{i\in I}$ ein maximal linear unabhängiges System von V, so ist $(x_i)_{i\in I}$ auch eine Basis von V.

Es gelten also in Vektorräumen die folgenden beiden Implikationen:

$$(x_i)_{i\in I} \text{ minimales Erzeugendensystem} \quad \Longrightarrow \quad (x_i)_{i\in I} \text{ Basis.}$$
$$(x_i)_{i\in I} \text{ maximal linear unabhängiges System} \quad \Longrightarrow \quad (x_i)_{i\in I} \text{ Basis.}$$

Beweis.
Da die Skalare/Koeffizienten alle aus dem Körper K stammen, existiert zu jedem Koeffizient ungleich Null ein multiplikatives Inverses, d.h. es kann durch den Koeffizienten geteilt werden!

i.) Da das System $(x_i)_{i\in I}$ schon ein (minimales) Erzeugendensystem ist, muß nur noch gezeigt werden, daß es auch linear unabhängig ist. Dazu sei eine Linearkombination

$$\sum_{i\in I} a_i x_i = 0$$

betrachtet, und es ist zu zeigen, daß dann alle Koeffizienten a_i Null sein müssen. Angenommen, es gäbe einen Koeffizienten $a_k \neq 0$. Daraus würde folgen:

$$\sum_{i\in I} a_i x_i = 0 \quad \Longrightarrow \quad -a_k x_k = \sum_{\substack{i\in I\\ i\neq k}} a_i x_i \quad \text{mit } a_k \neq 0 \quad \overset{\cdot(-a_k^{-1})}{\Longrightarrow} \quad x_k = \sum_{\substack{i\in I\\ i\neq k}} -\frac{a_i}{a_k} x_i.$$

Offensichtlich wäre dann $(x_i)_{i\in I}$ im Widerspruch zur Annahme kein minimales Erzeugendensystem, denn der Vektor x_k könnte aus dem System herausgenommen werden und das verbleibende echte Teilsystem wäre immer noch ein Erzeugendensystem, da für jede Linearkombination $x = \sum_{i\in I} b_i x_i$ folgen würde:

$$\begin{aligned} x &= \sum_{i\in I} b_i x_i = b_k x_k + \sum_{\substack{i\in I\\ i\neq k}} b_i x_i = b_k \cdot \sum_{\substack{i\in I\\ i\neq k}} -\frac{a_i}{a_k} x_i + \sum_{\substack{i\in I\\ i\neq k}} b_i x_i \\ &= \sum_{\substack{i\in I\\ i\neq k}} -\frac{b_k a_i}{a_k} x_i + \sum_{\substack{i\in I\\ i\neq k}} b_i x_i = \sum_{\substack{i\in I\\ i\neq k}} \big(b_i - \frac{b_k a_i}{a_k}\big) x_i. \end{aligned}$$

Also kann es kein $a_k \neq 0$ geben und das System $(x_i)_{i\in I}$ ist auch linear unabhängig.

ii.) Es ist zu zeigen, daß das (maximal) linear unabhängige System $(x_i)_{i\in I}$ auch ein Erzeugendensystem ist. Wäre dies nicht der Fall, so würde es einen Vektor $x \in V$ geben, der keine Linearkombination von $(x_i)_{i\in I}$ ist.
Es wird nun gezeigt, daß dann der Vektor x dem System $(x_i)_{i\in I}$ hinzugefügt werdenn könnte und das echt erweiterte System auch linear unabhängig wäre, im Widerspruch zur Maximalität von $(x_i)_{i\in I}$ als linear unabhängiges System.
Dazu reicht es zu übperprüfen, ob es eine nicht-triviale Linearkombinationsdarstellung der Null mit dem erweiterten System geben kann. Sei also

$$ax + \sum_{i\in I} a_i x_i = 0.$$

Es gilt $a = 0$, denn aus $a \neq 0$ würde folgen, daß x im Widerspruch zu dessen Wahl eine Linearkombination von $(x_i)_{i\in I}$ wäre:

$$\underbrace{a}_{\neq 0} x + \sum_{i\in I} a_i x_i = 0 \quad \overset{\cdot a^{-1}}{\Longrightarrow} \quad x + \sum_{i\in I} \frac{a_i}{a} x_i = 0 \quad \Longrightarrow \quad x = \sum_{i\in I} -\frac{a_i}{a} x_i.$$

Aus $a = 0$ folgt dann aber $\sum_{i\in I} a_i x_i = 0$, und da das System $(x_i)_{i\in I}$ linear unabhängig ist, auch $a_i = 0$ für alle $i \in I$. Somit wäre das erweiterte System linear unabhängig, was nicht sein kann, und $(x_i)_{i\in I}$ muß schon ein Erzeugendensystem sein. □

Bemerkung 2.2.36. *Im Beweis von Lemma 2.2.36 mußte für jede der beiden zu zeigenden Aussagen durch einen Skalar/Koeffizienten ungleich Null geteilt werden, d.h. es war die Existenz seines multiplikativen Inversen nötig. Der Beweis kann somit nicht auf beliebige Moduln übertragen werden, da dort die Skalare aus einem Ring stammen und mitunter keine multiplikativen Inversen haben.* □

In einem Vektorraum gelten also die folgenden wesentlichen Äquivalenzen:

Satz 2.2.37. *Sei V ein Vektorraum über dem Körper K und $(x_i)_{i\in I}$ ein System von Vektoren aus V. Dann sind äquivalent:*

i.) $(x_i)_{i\in I}$ *ist eine Basis von* V.
ii.) Jedes $x \in V$ *hat eine eindeutige Darstellung als Linearkombination von* $(x_i)_{i\in I}$.
iii.) $(x_i)_{i\in I}$ *ist ein linear unabhängiges Erzeugendensystem von* V.
iv.) $(x_i)_{i\in I}$ *ist ein minimales Erzeugendensystem von* V.
v.) $(x_i)_{i\in I}$ *ist ein maximal linear unabhängiges System von* V.

Beweis.
Nach Satz 2.2.26 sind die Aussagen *i.)* bis *iii.)* äquivalent. Die Äquivalenz von *i.)* zu *iv.)* und zu *v.)* folgt aus Lemma 2.2.34 und Lemma 2.2.35. □

Um zu zeigen, daß in Vektorräumen Basen existieren, reicht es also, die Existenz von minimalen Erzeugendensystemen oder maximal linear unabhängigen Systemen nachzuweisen. Dazu gilt folgende allgemeine Aussage:

Satz 2.2.38. *Sei M ein Modul/Vektorraum über dem Ring/Körper R. Dann gilt:*

i.) Enthält M ein linear unabhängige System, so enthält M auch ein maximal linear unabhängiges System.
ii.) Ist R ein Körper und M damit ein Vektorraum, und gilt $M \neq \{0\}$, so enthält M ein maximal linear unabhängiges System, welches dann auch eine Basis von M ist.

Beweis.

i.) Der Beweis dieser Aussage ist im wesentlichen mengentheoretischer Natur und beruht dann auf dem Zornschen Lemma, welches äquivalent zum Auswahlaxiom ist. Außer seinem Ergebnis liefert er keine Einblicke in die Modul-/Vektorraumtheorie und wird deshalb hier nicht ausgeführt.
In [**SSAlg1**, § 23, Satz 23.5, Seite 127] findet sich ein (noch viel allgemeinerer) Beweis der Aussage: anstelle des dort vorausgesetzten Erzeugendensystems muß dann nur der ganze Modul als Erzeugendensystem genommen werden, um die speziellere Aussage in *i.)* zu erhalten. In [**SSAlg3**] findet sich noch ein Beweis des Zornschen Lemmas.

ii.) Ist M ein Vektorraum mit $M \neq \{0\}$, so enthält er mindestens einen Vektor $x \neq 0$, und (x) ist dann ein einelementiges linear unabhängiges System (siehe Beispiel 2.2.25). Da M ein linear unabhängiges System enthält, enthält es nach *i.)* aucn ein maximal linear unabhängiges System, und dieses ist nach Satz 2.2.37 eine Basis von M. □

Bemerkung 2.2.39.

i.) Die Existenzaussage von Basen in Vektorräumen in Satz 2.2.38.ii) ist nur für Vektorräume ungleich dem Nullraum gemacht. In dem Vektorraum $\{0\}$ kann es nach Definition 2.2.1 gar kein linear unabhängigen Systeme $(x_i)_{i\in I}$ geben, da in dem System nur der Nullvektor vorkommen kann und wegen $I \neq \emptyset$ auch mindestens einmal vorkommen muß, und das System dann linear abhängig ist (Bemerkung 2.2.24).
Wenn auch leere Systeme $(x_i)_{i\in\emptyset}$ zugelassen werden und leere Linearkombinationen $\sum_{i\in\emptyset} a_i x_i$ als Nullvektor definiert werden, so gilt: Das leere System ist

ein Erzeugendensystem von $\{0\}$*, und die eindeutige Darstellbarkeit ist in sofern gewährleistet, daß nur das „eindeutige“ leere Koeffizientensystem* $(a_i)_{i\in\emptyset}$ *gewählt werden kann. Damit könnte das leere System als Basis von* $\{0\}$ *aufgefaßt werden. In vielen Büchern wird daher die leere Menge (d.h. das „leere System“) als Basis des Nullraumes definiert.*

ii.) *In* [**BrLAI**, §6.7, Basen] *findet sich eine sehr ausführliche Diskussion (und ein Beweis) der Aussage, daß ein Vektorraum* V *mit* $V \neq \{0\}$ *eine Basis besitzt. Der Beweis läuft über das Lemma von Tukey, welches äquivalent zum Zornschen Lemma ist, und beinhaltet die gleichen Ideen wie der Beweis in* [**SSAlg1**] *und könnte leicht zu einem Beweis von 2.2.38.i) erweitert werden.*

iii.) *Meist wird in der einführenden Literatur zur linearen Algebra die Existenz von Basen in einem Vektorraum (ungleich dem Nullraum) unter der Voraussetzung bewiesen, daß schon ein endliches Erzeugendensystem gegeben ist. Da eine Basis in einem Vektorraum nach Satz 2.2.37 ein minimales Erzeugendensystem ist, braucht das vorgegebene endliche Erzeugendensystem nur sukzessive verkleinert zu werden, bis es minimal ist - was wegen dessen Endlichkeit konstruktiv möglich ist. (Übung!)*

iv.) *Nach der allgmeinen Ausssage in Satz 2.2.38.i) besitzt ein Modul ein maximales linear unabhängiges System, wenn er überhaupt ein linear unabhängiges System besitzt. Dies garantiert aber noch nicht die Existenz einer Basis, da in einem Modul maximal linear unabhängige Systeme keine Basis sein müssen.*
Zum Beispiel im $\mathbb{Z}$*-Modul* $\mathbb{Q}$ *ist für jedes* $\alpha \in \mathbb{Q}$ *mit* $\alpha \neq 0$ *das System* (α) *linear unabhängig - und nach Beispiel 2.2.25 sind dies die einzigen linear unabhängigen Systeme in* $\mathbb{Q}$ *und damit auch alle maximal linear unabhängige Systeme. Aber keines dieser (maximal) linear unabhängigen Systeme ist auch ein Erzeugendensystem, da sich offensichtlich nicht alle Brüche in* $\mathbb{Q}$ *als ganzzahlige Vielfache eines Bruches* $\alpha \in \mathbb{Q}$ *darstellen lassen. Also besitzt* $\mathbb{Q}$ *zwar maximal linear unabhängige Systeme, aber kein linear unabhängiges Erzeugendensystem und damit keine Basis (Satz 2.2.26).*

v.) *Zum Beweis der Existenz von Basen in Vektorräumen standen zwei Ansätze zur Verfügung: ein maximal linear unabhängiges System zu finden oder ein minimales Erzeugendensystem. Gewählt wurde in Satz 2.2.38 der Weg über maximal linear unabhängige Systeme, und die Aussage über deren Existenz sogar in Moduln ist sehr allgemein, denn es muß nur überhaupt ein linear unabhängiges System existieren, um ein maximal linear unabhängiges zu erhalten.*
Die obige „Anfangsvoraussetzung“ ist bei Erzeugendensystemen immer gegeben, denn Erzeugendenssysteme existieren nach Lemma 2.2.12 in jedem Modul. Allerdings kann dann nicht *auf die Existenz von minimalen Erzeugensystemen geschlossen werden: Es gibt Moduln, die kein minimales Erzeugendensystem besitzen.*
Ein Beispiel dazu ist der $\mathbb{Z}$*-Modul* $\mathbb{Q}$*. Es gelten darin folgende beide Aussagen:*

Aussage A: $\mathbb{Q}$ *enthält als* $\mathbb{Z}$*-Modul kein endliches Erzeugendensystem.*

Aussage B: *Ist* $(x_i)_{i\in I}$ *ein Erzeugendensystem des* $\mathbb{Z}$*-Moduls* $\mathbb{Q}$*, so gilt für jede Indexmenge* $J \subseteq I$ *mit* $|I \setminus J| < \infty$*, daß auch das Teilsystem* $(y_j)_{j\in J}$ *von* $(x_i)_{i\in I}$ *ein Erzeugendensystem von* $\mathbb{Q}$ *ist.*

Beide Aussagen zusammen liefern, daß jedes Erzeugendensystem von $\mathbb{Q}$ um beliebig endlich viele Vektoren verkleinert werden kann, und trotzdem noch ein Erzeugendensystem bleibt, und damit kein minimales Erzeugendensystem existieren kann. □

Diejenigen Moduln, die eine Basis besitzen, haben eine spezielle Bezeichnung:

Definition 2.2.40. *Sei M ein R-Modul. Er heißt freier Modul, wenn er eine Basis besitzt.* □

Bemerkung 2.2.41. *Wenn ein Modul frei ist, liegt die Vermutung nahe, daß dann auch die Äquivalenzen über Basen aus Satz 2.2.37 wie in einem Vektorraum gelten. Dies ist nicht der Fall!*
Der $\mathbb{Z}$-Modul $\mathbb{Z}$ ist ein freier Modul, denn das einelementige System (1) ist eine Basis von $\mathbb{Z}$ (Beispiel 2.2.21). Aber $\mathbb{Z}$ enthält z.B. das maximal linear unabhängige System (2), welches keine Basis von $\mathbb{Z}$ ist, und auch das minimale Erzeugendensystem $(2,3)$, welches auch keine Basis ist (Übung!). Damit können die „fehlenden" Implikationen aus Lemma 2.2.35 nicht in freien Moduln gerettet werden. □

Beispiel 2.2.42.

i.) *Ist V ein K-Vektorraum mit $V \neq \{0\}$, so besitzt V nach Satz 2.2.38 eine Basis und ist damit ein freier Modul.*

ii.) *Ist R ein kommutativer Ring mit Eins und I eine nicht-leere Indexmenge, so besitzt der R-Modul $\bigoplus_{i\in I} R$ nach Lemma 2.2.29 die Standard-Basis $(e_i)_{i\in I}$ und ist somit ein freier Modul.*

iii.) *Die vorherige Aussage über die direkte Summe $\bigoplus_{i\in I} R$ läßt sich nicht auf ein unendliches Produkt $\prod_{i\in I} R$ übertragen: zum Beispiel ist der $\mathbb{Z}$-Modul $\prod_{i\in\mathbb{N}} \mathbb{Z}$ nicht frei (siehe* [**LaMR**, §2, Projective Moduls, Example 2.8, Seite 23]*).*

iv.) *Die $\mathbb{Z}$-Moduln $\mathbb{Z}_n$ sind für $n > 1$ nicht frei, da es darin keine linear unabhängigen Systeme und damit auch keine Basen gibt (siehe Beispiel 2.2.25).*

v.) *Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist nicht frei, da er kein linear unabhängiges Erzeugendensystem enthält (siehe auch Bemerkung 2.2.39).* □

Bisher ist nur gezeigt worden, daß in Vektorräumen eine Basis existiert und diese ein minimales Erzeugendensystem und auch ein maximal linear unabhängiges System ist. Es stellen sich sofort folgende Fragen:

- Kann ein vorgegebenes Erzeugendensystem eines Vektorraums zu einer Basis minimiert werden?
- Kann ein vorgegebenes linear unabhängiges System eines Vektorraumes zu einer Basis maximiert werden?

Die Antwort auf beide Fragen ist ja:

Satz 2.2.43. *Sei V ein K-Vektorraum und $V \neq \{0\}$. Dann gelten folgende Aussagen:*

Basisauswahlsatz: *Sei $(x_i)_{i\in I}$ ein Erzeugendensystem von V. Dann existiert ein Teilsystem $(y_j)_{j\in J}$ mit $J \subseteq I$ und $y_j = x_j$ für $j \in J$, welches eine Basis von V ist und damit ein minimales Erzeugendensystem.*

Insbesondere kann damit jedes Erzeugendensystem von V zu einer Basis von V minimiert werden!

Basisergänzungssatz: *Sei $(x_i)_{i\in I}$ ein linear unabhängiges System. Dann gibt es ein Erweiterungssystem $(y_j)_{j\in J}$ mit $I \subseteq J$ und $x_i = y_i$ für $i \in I$, das eine Basis von V ist.*

Insbesondere kann damit jedes linear unabhängige System zu einer Baisis von V maximiert werden!

Austauschsatz: *Sei $(x_i)_{i\in I}$ ein Erzeugendensystem von V und $(y_i)_{i\in J}$ ein linear unabhängiges System. Ist $(x_i)_{i\in I}$ keine Basis, so existiert ein Teilsystem $(x_k)_{k\in K}$ des Erzeugendensystems $(x_i)_{i\in I}$, das zusammen mit dem linear unabhängigen System $(y_j)_{j\in J}$ eine Basis von V ist.*
Dabei ist die Zusammensetzung zweier Systeme ein neues System, dessen Einträge genau die Einträge der beiden vorherigen Systeme sind:

$$(x_k)_{k\in K},\ (y_j)_{j\in J} \quad \rightsquigarrow \quad (z_s)_{s\in S} \quad \textit{mit} \quad S := K \times \{0\} \cup J \times \{1\} \quad \textit{und}$$
$$z_s := \begin{cases} x_k & \textit{für } s = (k,0), \\ y_j & \textit{für } s = (j,1). \end{cases}$$

Für den folgenden (endlichen) Spezialfall bedeutet dies insbesondere:
Ist $(x_1, \ldots, x_k)$ ein linear unabhängiges System und $(y_1, \ldots, y_m)$ ein Erzeugendensystem von V, so können Vektoren $y_{i_1}, \ldots, y_{i_r}$ aus dem Erzeugendensystem gewählt werden, daß $(x_1, \ldots, x_k, y_{i_1}, \ldots, y_{i_r})$ eine Basis von V ist.
Falls $(x_1, \ldots, x_k)$ schon eine Basis ist, gilt $r = 0$, d.h. es werden keine *Vektoren aus dem Erzeugendensystem hinzugenommen.*

Beweis.
Alle drei Sätze werden über eine äquivalente Version des Auswahlaxioms bewiesen und sind im wesentlichen wieder mengentheoretischer Natur. Der Austauschsatz liefert in einer allgemeinen Version (mit leeren Systemen) die beiden anderen Aussagen (Basisauswahlsatz und Basisergänzungssatz), und der Beweis des Auswahlsatzes ist fast gleich zum Beweis von Satz 2.2.38.i.). Wegen seines ausschließlich technischen Charakters wird hier auf den Beweis verzichtet.
Beweise finden sich in [**SSAlg1**, §23, Korollar 23.6, Seite 127] und [**BrLAI**, Satz 6.27 Corollar 6.28 und Corollar 6.29, Seite 263]. □

Bemerkung 2.2.44.

i.) *Die drei Sätze in 2.2.43 sind alle reine Existenzaussagen und nicht-konstruktiv.*
- *Ist ein Erzeugendensystem eines Vektorraumes gegeben, so kann daraus eine Basis ausgewählt werden, aber es gibt keine Aussage darüber, wie.*
- *Ist ein linear unabhängiges System gegeben, so kann dies zu einer Basis des Vektorraumes ergänzt werden, aber es gibt keine Aussage darüber, wie.*
- *Ein linear unabhängiges System kann sogar aus einem vorgegebenen Erzeugendensystem heraus zu einer Basis ergänzt werden, aber es gibt keine Aussage darüber, wie.*

Somit sind diese Aussagen eher für theoretische Betrachtungen von Interesse.

ii.) *Alle drei Sätze aus 2.2.43 lassen sich nicht auf Moduln übertragen, auch nicht auf freie Moduln.*
Als Gegenbeispiel sei der freie $\mathbb{Z}$-Modul $\mathbb{Z}$ betrachtet:

- $(2,3)$ *ist ein linear abhängiges Erzeugendensystem von* $\mathbb{Z}$ *und damit keine Basis, und es kann darin kein echtes Teilsystem gewählt werden, daß eine Basis von* $\mathbb{Z}$ *ist, denn die einzigen beiden echten Teilsysteme sind* (2) *und* (3)*, die beide nicht* $\mathbb{Z}$ *erzeugen.*
  Damit gilt im freien $\mathbb{Z}$*-Modul* $\mathbb{Z}$ *nicht der Basisauswahlsatz.*
- (2) *ist ein (maximal) linear unabhängiges System, aber kein Erzeugendensystem von* $\mathbb{Z}$*. Damit kann das System nicht zu einer Basis von* $\mathbb{Z}$ *erweitert werden, denn jede Erweiterung des Systems würde wegen dessen Maximalität die lineare Unabhängigkeit zerstören.*
  Damit gilt im freien $\mathbb{Z}$*-Modul* $\mathbb{Z}$ *nicht der Basisergänzungssatz.*
- *Es kann wieder das System* (2) *betrachtet werden: wenn es überhaupt nicht zu einer Basis von* $\mathbb{Z}$ *erweitert werden kann (s.o.), dann auch nicht aus einem vorgegebenen Erzeugendensystem.*
  Damit gilt im freien $\mathbb{Z}$*-Modul* $\mathbb{Z}$ *nicht der Austauschsatz.* □

Dimension.

Im letzten Abschnitt wurde gezeigt, daß ein Vektorraum eine Basis besitzt. Wobei präziser ist, daß er *mindestens* eine Basis besitzt, denn Basen sind bis auf wenige Ausnahmen nicht eindeutig (bis auf Isomorphie erfüllt nur der $\mathbb{Z}_2$-Vektorraum $\mathbb{Z}_2$ die Bedingung, genau eine Basis zu besitzen!). Folgende kleine Übung zeigt, wie aus einer gegebenen Basis neue gewonnen werden können:

Bemerkung 2.2.45. *Sei* M *ein* R*-Modul und* $(x_i)_{i\in I}$ *eine Basis von* M*. Weiter sei* $(a_i)_{i\in I}$ *ein System aus Einheiten* a_i *von* R*, also* $(a_i)_{i\in I} \in \prod_{i\in I} R^*$*. Dann ist auch* $(a_i x_i)_{i\in I}$ *eine Basis von* M*. (Übung!)* □

Sind dann in einem K-Vektorraum V zum Beispiel die zwei Basen $(x_1,\dots,x_n)$ und $(y_1,\dots,y_m)$ gegeben, ist bisher nichts dazu gesagt worden, ob die Systeme gleichgroß sind. Zwar sind beide Basen maximal linear unabhängige Systeme, aber die Maximalität bezieht sich nicht auf Größenvergleiche zwischen verschiedenen Systemen, sondern darauf, ob ein System linear unabhängig erweitert werden kann oder nicht. Somit könnte es sein, daß in V ein System der länge 17 nicht weiter linear unabhängig erweitert werden kann und ein anderes, dazu völlig unabhängiges System der Länge 23, ebenso nicht.

Tatsächlich tritt dieser Fall nicht auf, denn alle Basen eines Vektorraums haben die gleiche Größe:

Satz 2.2.46. *Sei* V *ein* K*-Vektorraum und* $V \neq \{0\}$*. Sind dann Basen* $(x_i)_{i\in I}$ *und* $(y_j)_{j\in J}$ *von* V *gegeben, so gilt:* $|I| = |J|$*, d.h. die beiden Basen sind gleichmächtig und es existiert eine Bijektion* $f\colon I \longrightarrow J$*.*
Insbesondere bedeutet dies für zwei endliche Basen $(x_1,\dots,x_n)$ *und* $(y_1,\dots,y_m)$ *die Beziehung* $n = m$*.*

Beweis.
Der allgemeine Beweis des Satzes für Basen mit unendlichen Indexmengen verlangt einigen mengentheoretischen Hintergrund und wird hier nicht ausgeführt. Eine ausführliche Diskussion und ein ausführlicher Beweis findet sich in [**BrLAI**, §6.7, Basen, Satz 6.39, Seite 278]. □

Mit Satz 2.2.46 ist nun folgende Definition möglich:

Definition 2.2.47. *Sei V ein K-Vektorraum.*

i.) Gilt $V = \{0\}$, so heißt V endlich-dimensionaler Vektorraum der Dimension Null.

ii.) Für $V \neq \{0\}$ enthält V (mindestens) eine Basis $(x_i)_{i\in I}$. Dann haben alle Basen nach Satz 2.2.46 die Mächtigkeit $|I|$, und dies ist die Dimension von V.

- *Ist I ein endliche Menge so heißt V endlich-dimensionaler Vektorraum.*
- *Ist I eine unendliche Menge, so heißt V unendlich-dimensionaler Vektorraum.*

Die Dimension von V wird auch folgendermaßen notiert:

$$\dim_K(V) := 0 \text{ für } V = \{0\}, \quad \text{ansonsten:} \quad \dim_K(V) := |I|. \qquad \square$$

Bemerkung 2.2.48. *Mit Satz 2.2.37 ergeben sich folgende nützliche Aussagen für ein System von Vektoren in einem K-Vektorraum V:*

- *Jedes linear unabhängige System mit $\dim_K(V)$ Elementen ist eine Basis von V.*
- *Jedes Erzeugendensystem mit $\dim_K(V)$ Elementen ist eine Basis von V.*

Dies bedeutet, daß bei bekannter Dimension des Raumes für ein gegebenes System nicht beide Eigenschaften (lineare Unabhängigkeit und *Erzeugendensyste) nachgeprüft werden müssen, ob es eine Basis ist: wenn die Größe stimmt, reicht eine der beiden Eigenschaften.*
Damit ist zum Beispiel jedes linear unabhängige System mit drei Elementen im $\mathbb{R}^3$ schon eine Basis, oder auch jedes Erzeugendensystem mit drei Elementen. $\square$

Beispiel 2.2.49.

i.) Sei K ein Körper. Dann existiert im K-Vektorraum K^n nach Lemma 2.2.29 die Standard-Basis $(e_1, \ldots, e_n)$ der Größe n, und der K^n hat damit die Dimension n, d.h. es gilt $\dim_K(K^n) = n$.

ii.) Für einen Körper K und eine nicht-leere Indexmenge I enthält der K-Vektorraum $V := \bigoplus_{i\in I} K$ nach Lemma 2.2.29 die Standard-Basis $(e_i)_{i\in I}$. Damit gilt $\dim_K(V) = |I|$.

iii.) Ist $M := \{1, \ldots, n\}$, so gilt für den $\mathbb{Z}_2$-Vektorraum $\mathcal{P}(M)$ (Übung!):

$$\text{Das System } \big(\{1\}, \ldots, \{n\}\big) \text{ ist eine Basis von } \mathcal{P}(M).$$

Dann hat $\mathcal{P}(M)$ die Dimension n, d.h. es gilt $\dim_{\mathbb{Z}_2}\big(\mathcal{P}(M)\big) = n$. $\square$

Es ist nun möglich, eine Abschätzung zwischen der Größe von linear unabhängigen Systemen und Erzeugendensystemen in einem Vektorraum herzustellen, denn es gilt:

Lemma 2.2.50. *Sei V ein K-Vektorraum. Weiter sei $(x_i)_{i\in I}$ ein linear unabhängiges System und $(y_j)_{j\in J}$ ein Erzeugendensystem von V. Dann gilt folgende Abschätzung:*

$$|I| \leq \dim_K(V) \leq |J|.$$

Insbesondere für ein linear unabhängiges System $(x_1, \ldots, x_n)$ und ein Erzeugendensystem $(y_1, \ldots, y_m)$ gilt dann die Ungleichung:

$$n \leq \dim_K(V) \leq m.$$

Beweis.
Nach dem Basisergänzungssatz 2.2.43 existiert eine Basis $(z_r)_{r\in R}$ von V, die eine Erweiterung des linear unabhängigen Systems $(x_i)_{i\in I}$ mit $I \subseteq R$ und $x_i = z_i$ für $i \in I$ ist. Es folgt sofort:

$$|I| \overset{I\subseteq R}{\leq} |R| \overset{\text{(Def. Dim)}}{=} \dim_K(V).$$

Nach Dem Basisauswahlsatz 2.2.43 existiert eine Basis $(w_s)_{s\in S}$, die ein Teilsystem des Erzeugendensystems $(y_j)_{j\in J}$ ist mit $S \subseteq J$ und $w_s = y_s$ für $s \in S$. Dies liefert:

$$\dim_K(V) \overset{\text{(Def. Dim)}}{=} |S| \overset{S\subseteq J}{\leq} |J|.$$

Werden beide Abschätzungen zusammengefügt, ergibt sich die behauptete Ungleichungskette:

$$|I| \leq |R| = \dim_K(V) = |S| \leq |J|.$$

Die Aussage über die endlichen Systeme ist ein offensichtlicher Spezialfall. □

Als nächstes soll betrachtet werden, welche Dimensionsbeziehung zwischen einem Vektorraum und einem seiner Untervektorräume besteht. Dazu wird zuerst eine Hilfsaussage bewiesen, die auch für sich alleine von Interesse ist:

Lemma 2.2.51. *Sei V ein K-Vektorraum und $(x_i)_{i\in I}$ ein linear unabhängiges System. Weiter sei ein Vektor $x \in V$ gegeben und $(y_j)_{j\in J}$ das um den Vektor x erweiterte Sytem $(x_i)_{i\in I}$, d.h. es gilt $|J \setminus I| = 1$, und für $j \in J$ folgt:*

$$y_j = x_j \text{ für } j \in I \quad \text{und} \quad y_j = x \text{ für } j \notin I.$$

Dann gilt folgende Äquivalenz:

$$(y_j)_{j\in J} \text{ ist linear unabhängig} \quad \Longleftrightarrow \quad x \notin \langle x_i \rangle_{i\in I}.$$

Insbesondere gilt für ein linear unabhängiges System $(x_1, \ldots, x_n)$ und $x \in V$:

$$(x_1, \ldots, x_n, x) \text{ linear unabhängig} \quad \Longleftrightarrow \quad x \notin \langle x_1, \ldots, x_n \rangle.$$

Beweis.
„$\Longrightarrow$“: Angenommen, x läge im Erzeugnis von $(x_i)_{i\in I}$. Dann gäbe es eine Linearkombinationsdarstellung $x = \sum_{i\in I} a_i x_i$, und es folgt:

$$x = \sum_{i\in I} a_i x_i \quad \Longrightarrow \quad 0 = (-1)\cdot x + \sum_{i\in I} a_i x_i \quad \Longrightarrow \quad \sum_{j\in J} b_j y_j = 0$$

mit $b_j := a_j$ für $j \in I$ und $b_j := -1$ für $j \notin I$, also mindestens einem Koeffizienten ungleich Null. Damit wäre das System $(y_j)_{j\in J}$ linear abhängig, im Widerspruch zur Vorraussetzung. Also kann x nicht im Erzeugnis von $(x_i)_{i\in I}$ liegen.

„$\Longleftarrow$“: Es sei eine Linearkombinationsdarstellung $\sum_{j\in J} b_j y_j = 0$ betrachtet, geschrieben in der Form:

$$0 = bx + \sum_{j\in I} b_j y_j = bx + \sum_{i\in I} b_i x_i.$$

Gilt $b = 0$, so folgt aus der linearen Unabhängigkeit des Systems $(x_i)_{i\in I}$ auch $b_i = 0$ für alle $i \in I$, und die Linearkombinationsdarstellung der Null ist trivial.

Aus $b \neq 0$ würde im Widerspruch zur Voraussetzung folgen:

$$0 = bx + \sum_{i \in I} b_i x_i \quad \Longrightarrow \quad -bx = \sum_{i \in I} b_i x_i \quad \overset{b \neq 0}{\Longrightarrow}$$

$$x = \sum_{i \in I} -\frac{b_i}{b} x_i \quad \Longrightarrow \quad x \in \langle\, x_i \,\rangle_{i \in I}.$$

Also kann der Fall $b \neq 0$ nicht auftreten.
Mit $b = 0$ existieren nach vorherigen Betrachtungen nur triviale Linearkombinationsdarstellungen der Null mit dem System $(y_j)_{j \in J}$, welches dann linear unabhängig ist. □

Bemerkung 2.2.52. *Lemma 2.2.51 liefert eine Möglichkeit, linear unabhängige Systeme zu konstruieren, denn ein gegebenes linear unabhängiges System kann sukzessive erweitert werden, indem ein Vektor außerhalb dessen Erzeugnisses hinzugefügt wird. Zum Beispiel kann der Vektor* $(1, 2, 3)$ *zu einer Basis des* $\mathbb{R}^3$ *erweitert werden durch folgende Schritte:*

$$(1,0,0) \notin \langle\, (1,2,3) \,\rangle \quad \Longrightarrow \quad \big(\, (1,2,3),\, (1,0,0) \,\big) \text{ l.u.}$$

$$(0,0,1) \notin \langle\, (1,2,3),\, (1,0,0) \,\rangle \quad \Longrightarrow \quad \big(\, (1,2,3),\, (1,0,0),\, (0,0,1) \,\big) \text{ l.u.}$$

Das resultierende System aus drei Vektoren ist wegen $\dim_{\mathbb{R}}(\mathbb{R}^3) = 3$ *und Bemerkung 2.2.48 eine Basis des* $\mathbb{R}^3$. □

Lemma 2.2.53. *Sei V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum. Dann gelten folgende Aussagen:*

i.) Zu jeder Basis $(u_j)_{j \in J}$ von U existiert eine Basis $(x_i)_{i \in I}$ von V, die $(u_j)_{j \in J}$ als Teilsystem enthält. Oder: jede Basis von U kann zu einer Basis von V erweitert werden.

ii.) $\dim_K(U) \leq \dim_K(V)$.
Insbesondere ist für einen endlich-dimensionalen Vektorraum auch jeder seiner Untervektorräume endlich-dimensional.

iii.) Ist V ein endlich-dimensionaler Vektorraum, so gilt die Äquivalenz:

$$U = V \quad \Longleftrightarrow \quad \dim_K(U) = \dim_K(V).$$

Beweis.

i.) Eine Basis von U ist ein linear unabhängiges System in V, und dieses kann nach dem Basisergänzungssatz zu einer Basis von V erweitert werden.

ii.) Nach der vorherigen Aussage ist jede Basis $(u_j)_{j \in J}$ ein Teilsystem einer geeigneten Basis $(x_i)_{i \in I}$ von V, d.h. es gilt vor allem $J \subseteq I$. Dann folgt sofort aus der Dimensionsdefinition:

$$\dim_K(U) = |J| \quad \overset{J \subseteq I}{\leq} \quad |I| = \dim_K(V).$$

iii.) „$\Longrightarrow$“: Trivial.
„$\Longleftarrow$“: Angenommen, es wäre $U \subsetneq V$, d.h. es gäbe ein $x \in V \setminus U$. Dann könnte nach Lemma 2.2.51 eine Basis von U um den Vektor x linear unabhängig erweitert werden, und es würde folgen:

$$\dim_K(U) + 1 \leq \dim_K(V),$$

im Widerspruch zur Voraussetzung. Also muß $U = V$ gelten. $\square$

Bemerkung 2.2.54. *Die Einschränkung von Aussage* iii.) *aus Lemma 2.2.53 auf einen endlichdimensionalen Vektorraum V ist nötig, wie folgendes Beispiel zeigt, wo ein echter Unterraum die gleiche Dimension wie der Vektorraum selbst hat:*
Sei $V := \bigoplus_{i\in N_0} \mathbb{R}$ der $\mathbb{R}$-Vektorraum aller reellen Folgen mit höchstens endlich vielen Folgengliedern ungleich Null. Nach Lemma 2.2.29 hat der Raum die Standard-Basis $(e_i)_{i\in\mathbb{N}_0}$ und damit die Dimension $\dim_{\mathbb{R}}(V) = |\mathbb{N}_0|$.
Es sei $U \subseteq V$ der von $(e_i)_{i\in\mathbb{N}}$ aufgespannte Unterraum, also alle Folgen aus V, deren erstes Folgenglied immer Null ist. U ist ein echter Unterraum von V, da die Folge $(1, 0, 0, \ldots)$ in $V \setminus U$ liegt, und es gilt $\dim_{\mathbb{R}}(U) = |\mathbb{N}|$.
Da es eine Bijektion zwischen $\mathbb{N}_0$ und $\mathbb{N}$ gibt (z.B. $n \mapsto n + 1$), gilt $|\mathbb{N}_0| = |\mathbb{N}|$ und damit $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}(V)$. $\square$

Lemma 2.2.55. *Sei V ein K-Vektorraum und $U \subseteq V$ ein Untervektorraum. Dann gelten folgende Aussagen:*

i.) Es sei $(u_j)_{j\in J}$ eine Basis von U und $(x_i)_{i\in I}$ eine Basis von V, die $(u_j)_{j\in J}$ als Teilsystem enthält. Dann ist $(x_i + U)_{i\in I\setminus J}$ eine Basis von V/U.

ii.) Ist $(u_1, \ldots, u_m)$ eine Basis von U und $(u_1, \ldots, u_m, x_1, \ldots, x_n)$ eine Basis von V, so ist $(x_1 + U, \ldots, x_n + U)$ eine Basis von V/U.

iii.) Ist V ein endlich-dimensionaler Vektorraum, so gilt:

$$\dim_K(V/U) = \dim_K(V) - \dim_K(U).$$

Beweis.

i.) Die kanonische Projektion $\pi_U \colon V \longrightarrow V/U$ mit $x \mapsto x + U$ ist surjektiv, und damit ist $\big(\pi_U(x_i)\big)_{i\in I}$ nach Satz 2.2.31 ein Erzeugendensystem von V/U. Aus einem Erzeugendensystem können Nullvektoren entfernt werden, ohne das Erzeugnis zu verändern, so daß Vektoren $\pi_U(x_i)$ mit $x_i \in \ker(\pi_U)$ gestrichen werden können. Wegen $\ker(\pi_U) = U$ fallen damit alle $\pi_U(x_i)$ mit $i \in J$ heraus, und das folgende System

$$\big(\pi_U(x_i)\big)_{i\in I\setminus J} = (x_i + U)_{i\in I\setminus J}$$

ist immer noch ein Erzeugendensystem, was nur noch auf lineare Unabhängigkeit getestet werden muß.
Sei dazu eine Linearkombination $\sum_{i\in I\setminus J} a_i(x_i + U) = 0 + U = U$ betrachtet, und es ist zu zeigen, daß alle Koeffizienten a_i mit $i \in I \setminus J$ Null sind. Es gilt:

$$U = \sum_{i\in I\setminus J} a_i(x_i + U) = \Big(\sum_{i\in I\setminus J} (a_i x_i)\Big) + U \quad \overset{1.2.17}{\Longrightarrow} \quad \sum_{i\in I\setminus J} a_i x_i \in U.$$

Liegt $\sum_{i\in I\setminus J} a_i x_i$ in U, läßt es sich als Linearkombination bzgl. dessen Basis $(u_j)_{j\in J}$ schreiben (ein Teilsystem der Basis $(x_i)_{i\in I}$), und es folgt:

$$\sum_{i\in I\setminus J} a_i x_i = \sum_{j\in J} b_j u_j \quad \Longrightarrow \quad \sum_{i\in I\setminus J} a_i x_i - \sum_{j\in J} b_j u_j = 0 \quad \overset{u_j = x_j \text{ für } j\in J}{\Longrightarrow}$$

$$\sum_{i\in I\setminus J} a_i x_i + \sum_{j\in J} (-b_j) x_j = 0 \quad \Longrightarrow \quad \sum_{i\in I\setminus J} a_i x_i + \sum_{i\in J} (-b_i) x_i = 0.$$

Dies ist eine Linearkombination der Null mit der Basis $(x_i)_{i\in I}$, so daß alle Koeffizienten und damit insbesondere alle a_i mit $i \in I \setminus J$ Null sein müssen, und das System $(x_i + U)_{i\in I\setminus J}$ ist auch linear unabhängig und damit auch eine Basis.

ii.) Dies ist nur ein Spezialfall von *i.)*.

iii.) Sei eine Basis $(u_1, \ldots, u_k)$ eine Basis vom U, so daß $\dim_K(U) = k$ gilt. Nach Lemma 2.2.53 kann diese zu einer Basis $(u_1, \ldots, u_k, x_1, \ldots, x_n)$ von V erweitert werden, und V hat die Dimension $k+n$. Nach *ii.)* ist dann $(x_1+U, \ldots, x_n+U)$ eine Basis von V/U, woraus $\dim_K(V/U) = n$ folgt, so daß zusammenfassend gilt:

$$\dim_K(V/U) = n = n + k - k = \dim_K(V) - \dim_K(U). \qquad \square$$

Dies liefert folgendes wesentliche Ergebnis über lineare Abbildungen:

Satz 2.2.56. *Seien V, W jeweils K-Vektorräume, V sei endlich-dimensional und $\varphi\colon V \longrightarrow W$ eine lineare Abbildung. Dann gilt:*

$$\dim_K(V) = \dim_K\big(\ker(\varphi)\big) + \dim_K\big(\operatorname{im}(\varphi)\big).$$

Beweis.
Aus dem Homomorphie-Satz für Moduln/Vektorräume in Version II (2.1.31) und Lemma 2.2.55 folgt:

$$\begin{aligned} V/\ker(\varphi) \overset{2.1.31}{\cong} \operatorname{im}(\varphi) \quad &\Longrightarrow \quad \dim_K\big(V/\ker(\varphi)\big) = \dim_K\big(\operatorname{im}(\varphi)\big) \\ &\overset{2.2.55}{\Longrightarrow} \quad \dim_K(V) - \dim_K\big(\ker(\varphi)\big) = \dim_K\big(\operatorname{im}(\varphi)\big) \\ &\Longrightarrow \quad \dim_K(V) = \dim_K\big(\ker(\varphi)\big) + \dim_K\big(\operatorname{im}(\varphi)\big). \qquad \square \end{aligned}$$

Bemerkung 2.2.57.

i.) Ein Vektorraumhomomorphismus $\varphi\colon V \longrightarrow W$ ist auch ein Gruppenhomomorphismus zwischen den Gruppen $(V,+)$ und $(W,+)$, so daß auch der Homorphie-Satz für Gruppen in Version II eine (Gruppen-)Isomorphie $V/\ker(\varphi) \cong \operatorname{im}(\varphi)$ liefert. Sind V und W dann endliche Gruppen, so liefert der Satz von Lagrange auch noch die Beziehung

$$|V| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|.$$

Ist der Skalarkörper K des Vektorraumes V unendlich groß, wie z.B. bei $K := \mathbb{Q}$ oder $K := \mathbb{R}$, so ist auch der Vektorraum V (für $V \neq \{0\}$) unendlich groß, da für jeden Vektor $v \in V$ mit $v \neq 0$ gilt:

$$\alpha, \beta \in K, \alpha \neq \beta \quad \Longrightarrow \quad \alpha v \neq \beta v.$$

Somit kann ist obige Formel nutzlos, und es steht nur die Dimensionsformel aus Satz 2.2.56 zur Verfügung.

ii.) Die Formel aus Satz 2.2.56 liefert sofort eine Abschätzung für die Größe des Kerns einer linearen Abbildungen $\varphi\colon V \longrightarrow W$, wenn W eine kleinere Dimension als V hat, denn es gilt:

$$\dim_K\big(\operatorname{im}(\varphi)\big) \leq \dim_K(W) \quad \Longrightarrow \quad \dim_K\big(\ker(\varphi)\big) \geq \dim_K(V) - \dim_K(W).$$

So muß einen lineare Abbildung $\varphi\colon \mathbb{R}^7 \longrightarrow \mathbb{R}^4$ mindestens einen Kern der Dimension $7 - 4 = 3$ besitzen.

iii.) Obige Abschätzung über die Größe des Kerns einer linearen Abbildung kann auch für lineare Gleichungssysteme genutzt werden:
Ist ein homogenes lineares Gleichungssystem mit m Gleichungen in n Unbekannten über dem Körper K gegeben (siehe Definition 2.1.34), so läßt sich dieses durch eine lineare Abbildung $\varphi\colon K^n \longrightarrow K^m$ beschreiben, so daß die Lösungsmenge des Gleichungssystems dem Kern von φ entspricht (Satz 2.1.35). Gibt es dann weniger Gleichungen als Unbekannte (d.h. $m < n$), so gilt nach obiger Abschätzung für den Kern von φ und damit die Lösungsmenge des Gleichungssystems, daß es mindenstens die Dimension $n - m > 0$ hat und damit nicht-triviale Lösungen existieren. □

Satz 2.2.56 ist auch unter dem Namen „Rangsatz“ bekannt, und zu dieser Umformulierung ist folgende Definition nötig:

Definition 2.2.58. *Seien V, W jeweils K-Vektorräume, und $\varphi\colon V \longrightarrow W$ sei eine lineare Abbildung. Dann ist der Rang von φ die Dimension seines Bildes, welches nach Lemma 2.1.30 ein Untervektorraum von W ist. Notation:*

$$\mathrm{rg}(\varphi) := \dim_K\big(\mathrm{im}(\varphi)\big).$$ □

Nun läßt sich Satz 2.2.56 umformulieren zu:

Satz 2.2.59. *(Rangsatz)*
Seien V, W jeweils K-Vektorräume, V sei endlich-dimensional und $\varphi\colon V \longrightarrow W$ eine lineare Abbildung. Dann gilt:

$$\dim_K(V) = \dim_K\big(\ker(\varphi)\big) + \mathrm{rg}(\varphi).$$

Beweis. Satz 2.2.56. □

Für Endomorphismen eines endlich-dimensionalen Vektorraumes folgt nun:

Lemma 2.2.60. *Sei V ein endlich-dimensionaler K-Vektorraum und $\varphi \in \mathrm{End}_K(V)$. Dann gilt:*

$$\varphi \text{ injektiv} \iff \varphi \text{ surjektiv.}$$

Insbesondere sind dann folgende Aussagen äquivalent:

i.) φ ist injektiv.
ii.) φ ist surjektiv.
iii.) φ ist bijektiv.

Beweis.
Da V ein endlich-dimensionaler K-Vektorraum ist, kann auf den Vektorraumendomorphismus $\varphi\colon V \longrightarrow V$ der Rangsatz (2.2.59 oder 2.2.56) angewendet werden, und es gilt:

$$\dim_K(V) = \dim_K\big(\ker(\varphi)\big) + \dim_K\big(\mathrm{im}(\varphi)\big).$$

φ injektiv $\implies$ φ surjektiv: Ist φ injektiv, so ist nach Lemma 2.1.27 $\ker(\varphi) = \{0\}$ und es folgt mit obigem Rangsatz:

$$\ker(\varphi) = \{0\} \implies \dim_K\big(\ker(\varphi)\big) = 0 \overset{\text{Rangsatz}}{\implies} \dim_K(V) = \dim_K\big(\mathrm{im}(\varphi)\big).$$

Dann ist aber nach Lemma 2.2.53 wegen der Endlichdimensionalität der Objekte $V = \mathrm{im}(\varphi)$ und φ surjektiv.

φ surjektiv $\implies$ φ injektiv: Ist φ surjektiv, so gilt mit dem Rangsatz:

$$V = \operatorname{im}(\varphi) \quad \implies \quad \dim_K(V) = \dim_K\big(\operatorname{im}(\varphi)\big) \overset{\text{Rangsatz}}{\implies} \dim_K\big(\ker(\varphi)\big) = 0$$

Also ist $\ker(\varphi) = \{0\}$, und nach Lemma 2.1.27 dann φ injektiv.

Zu den drei Äquivalenzen: Es ist schon die Äquivalenz von *i.)* und *ii.)* gezeigt, und es folgt sofort die Äquivalenz beider Aussagen zu *iii.)* wegen:

„bijektiv = injektiv und surjektiv“. □

Weiter gilt noch folgende weitreichende Tatsache:

Satz 2.2.61. *Seien V, W jeweils K-Vektorräume. Dann gilt:*

$$\dim_K(V) = \dim_K(W) \quad \iff \quad V \cong W, \text{ d.h. beide Räume sind isomorph.}$$

Insbesondere gilt dann für jeden K-Vektorraum V der Dimension n:

$$V \cong K^n,$$

und ganz allgemein gilt für einen K-Vektorraum V mit einer Basis $(x_i)_{i\in I}$ nach Lemma 2.2.29:

$$V \cong \bigoplus_{i\in I} K.$$

Beweis.
Die Aussage ist klar, wenn einer der beiden (und damit beide) der Nullraum ist. Seien also nun $V, W \neq \{0\}$.

„$\implies$“: Sei $(x_i)_{i\in I}$ eine Basis von V und $(y_j)_{j\in J}$ eine Basis von W. Aus der Voraussetzung $\dim_K(V) = \dim_K(W)$ folgt $|I| = |J|$ und damit die Existenz einer Bijektion $\tilde{f}\colon I \longrightarrow J$. Dann ist die lineare Fortsetzung $\varphi\colon V \longrightarrow W$ der folgenden Abbildung

$$f\colon x_i \mapsto y_{\tilde{f}(i)} \quad \text{für} \quad i \in I$$

nach dem Hauptsatz über lineare Abbildungen und Basen (2.2.31) ein Vektorraumisomorphismus, da per Konstruktion $\big(\varphi(x_i)\big)_{i\in I} = (y_{\tilde{f}(i)})_{i\in I}$ eine Basis von W ist, denn jedes y_j mit $j \in J$ tritt genau einmal in diesem System auf.

„$\impliedby$“: Wegen $V \cong W$ existiert ein Vektorraumisomorphismus $\varphi\colon V \longrightarrow W$. Sei $(x_i)_{i\in I}$ ein Basis von V. Dann ist nach dem Hauptsatz über lineare Abbildungen und Basen das System $\big(\varphi(x_i)\big)_{i\in I}$ eine Basis von W und damit insbesondere $\dim_K(V) = |I| = \dim_K(W)$. □

Bemerkung 2.2.62. *Ist K ein endlicher Körper mit $q := |K|$ und V ein K-Vektorraum der Dimension n, so gilt nach Satz 2.2.61 $V \cong K^n$, und K^n ist die Menge aller n-Tupel mit Einträgen aus K. Somit enthält K^n und damit V genau q^n Elemente. Damit läßt sich für die endliche Menge $M := \{1, \ldots, n\}$ beweisen, daß die Potenzmenge $\mathcal{P}(M)$ aus 2^n Elementen besteht, denn $\mathcal{P}(M)$ ist ein $\mathbb{Z}_2$-Vektorraum und $\big(\{1\}, \ldots, \{n\}\big)$ eine Basis (siehe Beispiel 2.2.49), also $\dim_{\mathbb{Z}_2} \mathcal{P}(M) = n$ und damit $\mathcal{P}(M) \cong (\mathbb{Z}_2)^n$ mit $|(\mathbb{Z}_2)^n| = 2^n$.* □

KAPITEL 3

Matrizen

3.1. Matrizen

Im folgenden Kapitel werden Matrizen behandelt: Diese sind per Definition nichts anderes als „Zahlentafeln“ bzw. „zweidimensionale Vektoren“. Allerdings lassen sich alle linearen Abbildungen zwischen endlich-dimensionalen Vektorräumen (nach Basiswahl in den Räumen!) als Matrizen notieren, so daß aus den mitunter abstrakten Homomorphismen Zahlentafeln werden, die mit Algorithmen (insbesondere dem Gaußalgorithmus) bearbeitet werden können und die wesentlichen Kenngrößen einer linearen Abbildung (vor allem ihren Kern) berechenbar machen.

Definition und elementare Eigenschaften.

Es sei einleitend der Körper $\mathbb{R}$ betrachtet. Für $n \in \mathbb{N}$ werden die Vektoren/Systeme $(a_i)_{i\in\{1,\dots,n\}}$ des $\mathbb{R}^n := \prod_{i=1}^n \mathbb{R}$ übersichtlich notiert als n-Tupel $(a_1, \dots, a_n)$.
Sind $n, m \in \mathbb{N}$ gegeben und die Indexmenge $I_{m,n} := \{1, \dots, m\} \times \{1, \dots, n\}$, so können Vektoren/Systeme des Tupelraumes $\prod_{(i,j)\in I_{m,n}} \mathbb{R}$ „zweidimensional“, d.h. in rechteckigen Zahlentafeln notiert werden:

$$(a_{i,j})_{(i,j)\in I_{m,n}} \in \prod_{(i,j)\in I_{m,n}} \mathbb{R} \quad \rightsquigarrow \quad \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}.$$

Im $\mathbb{R}$-Vektorraum $\prod_{(i,j)\in I_{m,n}} \mathbb{R}$ werden Vektoren „komponentenweise“ addiert, was in obiger Notation dann folgende Form hat:

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} + \begin{pmatrix} b_{1,1} & \dots & b_{1,n} \\ \vdots & & \vdots \\ b_{m,1} & \dots & b_{m,n} \end{pmatrix} = \begin{pmatrix} a_{1,1} + b_{1,1} & \dots & a_{1,n} + b_{1,n} \\ \vdots & & \vdots \\ a_{m,1} + b_{m,1} & \dots & a_{m,n} + b_{m,n} \end{pmatrix}.$$

Die skalare Multiplikation eines Vektors mit einem Skalar hat dann die Form:

$$r \cdot \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} = \begin{pmatrix} r \cdot a_{1,1} & \dots & r \cdot a_{1,n} \\ \vdots & & \vdots \\ r \cdot a_{m,1} & \dots & r \cdot a_{m,n} \end{pmatrix}.$$

Es wird nun ganz allgemein definiert:

Definition 3.1.1. *Es sei R ein kommutativer Ring mit Eins. Für $n, m \in \mathbb{N}$ ist die Indexmenge $I_{m,n}$ defniert durch:*

$$I_{m,n} := \{1, \dots, m\} \times \{1, \dots, n\}.$$

Mit der Indexmenge $I_{m,n}$ ist dann definiert:

$$\mathrm{Mat}(m \times n, R) := \prod_{(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}} R,$$

und die Elemente aus $\mathrm{Mat}(m \times n, R)$ werden $(m \times n)$-Matrizen genannt (Singular: Matrix) und notiert in der Form:

$$(a_{i,j})_{(i,j) \in I_{m,n}} \in \prod_{(i,j) \in I_{m,n}} R \quad \rightsquigarrow \quad \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}.$$

Die Einträge $a_{i,j}$ heißen die Koeffizienten der Matrix, und i dabei der Zeilenindex und j der Spaltenindex des Koeffizienten.
Ist $A \in \mathrm{Mat}(m \times n, R)$ gegeben und $A := (a_{i,j})$, so wird der Koeffizient $a_{i,j}$ von A auch mit $(A)_{i,j}$ notiert.
Die i-te Zeile der obigen Matrix ist $(a_{i,1}, \dots, a_{i,n}) \in \mathrm{Mat}(1 \times n, R)$ und wird auch Zeilenvektor genannt, die j-te Spalte ist

$$\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix} \in \mathrm{Mat}(m \times 1, R),$$

und diese wird Spaltenvektor genannt.
Ist der Kontext klar, wird für eine Matrix $A \in \mathrm{Mat}(m \times n, R)$ auch nur $(a_{i,j})$ notiert, ohne Angabe der Zeilen- und Spaltenanzahl.
Die Nullmatrix in $\mathrm{Mat}(m \times n, R)$ ist diejenige, deren Koeffizienten allesamt die Null aus R sind.
Für $1 \leq k \leq m$ und $1 \leq l \leq n$ heißt $E^{m,n}_{k,l} := (a_{i,j}) \in \mathrm{Mat}(m \times n, R)$ mit

$$a_{k,l} = 1 \text{ und } a_{i,j} = 0 \text{ für } (i,j) \neq (k,l), \quad \Longrightarrow \quad E^{m,n}_{k,l} := \begin{array}{cc} & \begin{array}{cc} \textit{Ind.} & l \end{array} \\ k & \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix} \end{array}$$

Elementarmatrix, d.h. $E^{m,n}_{k,l}$ enthält genau eine Eins (in der k-ten Zeile und l-ten Spalte) und sonst nur Nullen. Mit Hilfe des Kroneckersymbols (2.2.27) läßt sich $E_{i,j}$ alternativ auch definieren als $E_{i,j} := (\delta_{i,k} \cdot \delta_{l,j})_{(k,l) \in I_{n,m}}$.
Wenn der Kontext klar ist, wird bei $E^{m,n}_{k,l}$ meist der „obere Index“ weggelassen und nur $E_{k,l}$ geschrieben.

Die für $m := n$ werden die Matrizen aus $\mathrm{Mat}(n \times n, R)$ auch als quadratische Matrizen bezeichnet, und für $A := (a_{i,j}) \in \mathrm{Mat}(n \times n, R)$ ist die Diagonale definiert als:

$$\mathrm{diag}(A) := (a_{1,1}, \dots, a_{n,n}),$$

wobei die $a_{i,i}$ für $1 \leq i \leq n$ dann die Diagonalelemente von A genannt werden.

Eine quadratische $(n \times n)$-Matrix heißt Diagonalmatrix, falls alle ihre Koeffizienten außerhalb der Diagonalen Null sind, d.h. es gilt:

$$(a_{i,j}) \in \mathrm{Mat}(n \times n, R) \text{ Diagonalmatrix} \quad \Longrightarrow \quad a_{i,j} = 0 \text{ für } i \neq j.$$

Dabei sind Nullen auf der Diagonale erlaubt!
Die n-te Einheitsmatrix ist diejenige quadratische $(n \times n)$-Matrix, deren Diagonale nur die Eins aus R enthält und außerhalb der Diagonalen nur Nullen:

$$E_n := \sum_{i=1}^{n} E_{i,i} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \in \mathrm{Mat}(n \times n, R).$$

Mit Hilfe des Kroneckersymbols (2.2.27) läßt sich die Einheitsmatrix alternativ auch defininieren als $E_n := (\delta_{i,j})_{(i,j) \in I_{n,n}}$. □

Bemerkung 3.1.2.

i.) *Für einen kommutativen Ring R mit Eins sind Matrizen aus $\mathrm{Mat}(m \times n, R)$ Elemente des R-Moduls $\prod_{(i,j) \in I_{m,n}} R$, so daß zwischen zwei Matrizen eine komponentenweise Addition*

$$(a_{i,j}) + (b_{i,j}) := (a_{i,j} + b_{i,j})$$

und eine skalare Multiplikation zwischen einem Skalar $\alpha \in R$ und einer Matrix $(a_{i,j}) \in \mathrm{Mat}(m \times n, R)$ definiert ist:

$$\alpha(a_{i,j}) := (\alpha a_{i,j}).$$

Siehe dazu auch Beispiel 2.1.4.

ii.) *Ist R ein kommutativer Ring mit Eins, so sind die Elemente des R^n Tupel mit n Einträgen aus R: $(x_1, \dots, x_n) \in R^n$.*
Die Elemente aus $\mathrm{Mat}(1 \times n, R)$ sind auch Tupel mit n Einträgen aus R, allerdings ist deren Indexmenge verschieden, denn die Indizes der Einträge sind aus der Indexmenge $\{1\} \times \{1, \dots, n\}$: $(x_{1,1}, \dots, x_{1,n}) \in \mathrm{Mat}(1 \times n, R)$.
Damit sind die beiden Objekte formal nicht gleich.
In Zukunft werden aber Matrizen aus $\mathrm{Mat}(1 \times n, R)$ mitunter auch mit den einfachen Indizes geschrieben, wenn aus dem Kontext klar ist, was gemeint ist.

iii.) *Die Matrizen aus $\mathrm{Mat}(n \times 1, R)$ sind auch nur „n-Tupel“, die senkrecht anstelle von waagerecht notiert sind. Wegen ihrer Indexmenge unterscheiden sie sich formal von den Elementen aus $\mathrm{Mat}(1 \times n, R)$ und R^n.*
Häufig wird in der Literatur zwischen Zeilen- und Spaltenvektoren je nach Bedarf Hin und Her gewechselt - meist aus Platzgründen in der Notation, da Spaltenvektoren aufwändiger zu notieren sind als Zeilenvektoren. □

Beispiel 3.1.3.

i.) *In $\mathrm{Mat}(2 \times 3, \mathbb{R})$ existieren sechs Elementarmatrizen:*

$$E_{1,1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$E_{2,1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad E_{2,2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad E_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

ii.) Für die Einheitsmatrix von $\mathrm{Mat}(2 \times 2, \mathbb{R})$ *gilt:*

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = E_{1,1} + E_{2,2}.$$

iii.) Folgende Matrizen sind Diagonalmatrizen:

$$E_n \text{ für } n \in \mathbb{N}, \quad \text{quadratische Nullmatrizen}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 7 \end{pmatrix}. \qquad \square$$

Wie in Bemerkung 3.1.2 schon angedeutet, sind die Matrizen auch $\mathrm{Mat}(m \times n, R)$ nichts anderes als „zweidimensionale Tupel“, auf denen eine R-Modulstruktur definiert ist (siehe Beispiel 2.1.4 und auch Lemma 2.2.29). Dies wird hier noch einmal ausführlich zusammengefaßt:

Satz 3.1.4. *Sei R ein kommutativer Ring mit Eins. Dann ist*

$$\mathrm{Mat}(m \times n, R) := \prod_{(i,j) \in I_{m,n}} R \qquad \text{(siehe Definition 3.1.1)}$$

mit der komponentenweisen Addition

$$(a_{i,j}) + (b_{i,j}) := (a_{i,j} + b_{i,j}) \quad \text{für} \quad (a_{i,j}), (b_{i,j}) \in \mathrm{Mat}(m \times n, R)$$

eine abelsche Gruppe und die Nullmatrix ihr neutrales Element.
Die folgende Definition ist eine skalare Multiplikation zwischen R und $\mathrm{Mat}(m \times n, R)$*:*

$$\alpha \cdot (a_{i,j}) := (\alpha \cdot a_{i,j}) \quad \text{für} \quad \alpha \in R, \ \ (a_{i,j}) \in \mathrm{Mat}(m \times n, R),$$

so daß $\mathrm{Mat}(m \times n, R)$ *ein R-Modul ist.*

$\mathrm{Mat}(m \times n, R)$ *ist sogar ein freier Modul, und das System der Elementarmatrizen* $(E_{i,j})_{(i,j) \in I_{m,n}}$ *eine Basis. Dann hat* $(a_{i,j}) \in \mathrm{Mat}(m \times n, R)$ *eine Linearkombinationsdarstellung bzgl. Elementarmatrizen, und die Koeffizienten der Matrix sind die Koordinaten dieser Linearkombination:*

$$(a_{i,j}) = \sum_{(i,j) \in I_{m,n}} a_{i,j} E_{i,j} = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} E_{i,j}.$$

Insbesondere gilt dann für einen Körper K, daß $\mathrm{Mat}(m \times n, K)$ *ein K-Vektorraum ist mit der Dimension:*

$$\dim_K \big(\mathrm{Mat}(m \times n, K) \big) = m \cdot n.$$

Beweis.
Mit $n, m \in \mathbb{N}$ ist die Indexmenge $I_{m,n}$ endlich und es gilt $|I_{m,n}| = m \cdot n$. Mit Bemerkung 2.2.4 folgt:

$$\mathrm{Mat}(m \times n, R) := \prod_{(i,j) \in I_{m,n}} R \overset{(2.2.4)}{=} \bigoplus_{(i,j) \in I_{m,n}} R.$$

Dann folgen alle Aussagen über den R-Modul $\mathrm{Mat}(m \times n, R)$ aus Lemma 2.2.29, da die Elementarmatrizen $E_{i,j}$ genau die Standard-Basisvektoren $\delta_{i,j}$ aus $\bigoplus_{(i,j) \in I_{m,n}} R$ sind (siehe Definition 2.2.27).
Für den Fall eines Körpers K ist die Dimension des Vektorraumes $\mathrm{Mat}(m \times n, K)$ gleich der Mächtigkeit der Basis $(E_{i,j})_{(i,j) \in I_{m,n}}$, und diese ist $|I_{m,n}| = m \cdot n$. $\square$

Für einen kommutativen Ring R mit Eins ist mit einer beliebigen nicht-leeren Indexmenge I auch $\prod_{i\in I} R$ ein kommutativer Ring mit Eins, wenn die Tupel komponentenweise multipliziert werden. Diese Multiplikation ist hier jedoch nicht von besonderem Interesse.
Insbesondere für die im folgenden betrachtete Korrespondenz von Matrizen zu linearen Abbildungen zwischen endlich-dimensionalen Vektorräumen (nach Basiswahl in den jeweiligen Räumen!) ist es nötig, ein anderes Produkt von Matrizen einzuführen, welches später zu der Komposition von Abbildungen korrespondieren wird. Dieses Matrizenprodukt ist dabei in seiner Definition ersteinmal unanschaulich und wird erst später durch seine Eigenschaften „gerechtfertigt“.
Für Matrizen spezieller Größen ist dann folgendes Produkt definiert:

Definition 3.1.5. *Sei R ein kommutativer Ring mit Eins. Für Matrizen A, B mit:*

$$A := (a_{i,j}) \in \mathrm{Mat}(m \times p, R) \quad \textit{und} \quad B := (b_{i,j}) \in \mathrm{Mat}(q \times n, R),$$

und somit:

$$A := \begin{pmatrix} a_{1,1} & \dots & a_{1,p} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,p} \end{pmatrix} \quad \textit{und} \quad B := \begin{pmatrix} b_{1,1} & \dots & b_{1,n} \\ \vdots & & \vdots \\ a_{q,1} & \dots & a_{q,n} \end{pmatrix}$$

ist das Matrizenprodukt $A \cdot B$ definiert, falls gilt:

$$\underbrace{\text{„Spaltenanzahl von } A\text{“}}_{\text{Zeilenlänge von } A} = \underbrace{\text{„Zeilenanzahl von } B\text{“}}_{\text{Spaltenlänge von } B}, \qquad \textit{also:} \qquad p = q.$$

Das Produkt $C := A \cdot B$ ist dann definiert als die folgende Matrix:

$$C := (c_{i,j}) \in \mathrm{Mat}(m \times n, R) \quad \textit{mit} \quad c_{i,j} := \sum_{k=1}^{p} a_{i,k} \cdot b_{k,j}.$$

Der Koeffizient $c_{i,j}$ des Produktes $C := A \cdot B$ berechnet sich also folgendermaßen: Die i-te Zeile von A und die j-te Spalte von B werden komponentenweise multipliziert, und dann alle Produkte aufsummiert. Und deshalb muß *die Zeilenlänge von A mit der Spaltenlänge von B übereinstimmen:*

$$i\begin{pmatrix} a_{i,1} & \dots & a_{i,p} \end{pmatrix} \cdot \begin{array}{c} j \\ \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{p,j} \end{pmatrix} \end{array} = \begin{array}{c} \\ i \end{array}\begin{array}{c} j \\ \begin{pmatrix} c_{i,j} \end{pmatrix} \end{array} \textit{ mit } c_{i,j} := \sum_{k=1}^{p} a_{i,k} \cdot b_{k,j}.$$

Die „Größen“ der einzelnen Matrizen erfüllen also:

$$(m \times p)\text{-Matrix} \quad \textit{mal} \quad (p \times n)\text{-Matrix} \quad = \quad (m \times n)\text{-Matrix}.$$

Bei dem Produk $A \cdot B$ wird auch oft das Produktsymbol „$\cdot$“ weggelassen und einfach AB geschrieben, wenn der Kontext klar ist. □

Spezielle Matrizenprodukte lassen sich besonders gut veranschaulichen und liefern dann auch Einblicke, wie sich das Matrizenprodukt generell verstehen läßt:

Lemma 3.1.6. *Sei R ein kommutativer Ring mit Eins, und es seien folgende Matrizen gegeben:*

$$\begin{aligned} A &:= \begin{pmatrix} a_1 & \dots & a_m \end{pmatrix} && \in \mathrm{Mat}(1 \times m, R), \\ B &:= (b_{i,j}) && \in \mathrm{Mat}(m \times n, R), \\ C &:= \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} && \in \mathrm{Mat}(n \times 1, R). \end{aligned}$$

Die Matrix B sei einmal spaltenweise und einmal zeilenweise notiert:

$$B = \begin{pmatrix} \text{—} & z_1 & \text{—} \\ & \vdots & \\ \text{—} & z_m & \text{—} \end{pmatrix} \qquad \textit{und} \qquad B = \begin{pmatrix} | & & | \\ s_1 & \dots & s_n \\ | & & | \end{pmatrix}.$$

Dann existieren die Matrizenprodukte AB und BC, und sie lassen sich folgendermaßen veranschaulichen:

$$AB \quad = \quad \begin{pmatrix} a_1 & \dots & a_m \end{pmatrix} \begin{pmatrix} \text{—} & z_1 & \text{—} \\ & \vdots & \\ \text{—} & z_m & \text{—} \end{pmatrix} \quad = \quad \sum_{i=1}^{m} a_i \cdot \left(\text{—} \, z_i \, \text{—} \right)$$

und

$$BC \quad = \quad \begin{pmatrix} | & & | \\ s_1 & \dots & s_n \\ | & & | \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \quad = \quad \sum_{i=1}^{n} c_i \cdot \begin{pmatrix} | \\ s_i \\ | \end{pmatrix}.$$

Für zwei Matrizen X, Y, deren Produkt XY definiert ist, gilt nach der der Definition des Matrizenproduktes (siehe Definition 3.1.5) allgemein:

$$\begin{aligned} i\text{-te Zeile von } XY &= (i\text{-te Zeile von } X) \text{ mal } Y, \\ j\text{-te Spalte von } XY &= X \text{ mal } (j\text{-te Spalte von } Y). \end{aligned}$$

Somit lassen sich obige Formeln/Produkte anwenden, und es ergibt sich:

i-te Zeile von XY:	*Die i-te Zeile von XY ist eine Linearkombination der Zeilen von Y mit den Koeffizienten aus der i-ten Zeile von X.*
j-te Spalte von XY:	*Die j-te Spalte von XY ist ein Linearkombination der Spalten von X mit den Koeffizienten aus der j-te Spalte von Y.*

Beweis.

AB: Das Produkt AB ist eine $(1 \times n)$-Matrix, also ein Zeilenvektor $(t_1, \dots, t_n)$. Mit dem Matrizenprodukt gilt für dessen Koeffizienten:

$$t_j := \sum_{i=1}^{m} a_i b_{i,j} \qquad \Longrightarrow \qquad AB = \Big(\sum_{i=1}^{m} a_i b_{i,1}, \dots, \sum_{i=1}^{m} a_i b_{i,n} \Big) = \sum_{i=1}^{m} (a_i b_{i,1}, \dots, a_i b_{i,n}).$$

Die i-te Zeile von B hat die Form $z_i = (b_{i,1}, \ldots, b_{i,n})$. Damit folgt:

$$\sum_{i=1}^{m} a_i \cdot \left(— z_i — \right) = \sum_{i=1}^{m} a_i \cdot (b_{i,1}, \ldots, b_{i,n}) = \sum_{i=1}^{m} (a_i b_{i,1}, \ldots, a_i b_{i,n}) \overset{\text{(s.o.)}}{=} AB.$$

BC: Das Produkt BC ist eine $(m \times 1)$-Matrix, also ein Spaltenvektor, und es folgt mit dem Matrizenprodukt:

$$BC := \begin{pmatrix} t_1 \\ \vdots \\ t_m \end{pmatrix} \quad \text{mit} \quad t_j = \sum_{i=1}^{n} b_{j,i} c_i \quad \Longrightarrow \quad BC = \begin{pmatrix} \sum\limits_{i=1}^{n} b_{1,i} c_i \\ \vdots \\ \sum\limits_{i=1}^{n} b_{m,i} c_i \end{pmatrix} = \sum_{i=1}^{n} c_i \begin{pmatrix} b_{1,i} \\ \vdots \\ b_{m,i} \end{pmatrix}.$$

Die gewünschte Gleichung ergibt sich dann aus folgender Rechnung:

$$\sum_{i=1}^{n} c_i \cdot \begin{pmatrix} | \\ s_i \\ | \end{pmatrix} = \sum_{i=1}^{n} c_i \begin{pmatrix} b_{1,i} \\ \vdots \\ b_{i,1} \end{pmatrix} \overset{\text{(s.o.)}}{=} BC.$$

Die weitern Aussagen sind dann nur eine Beschreibung des Matrizenproduktes und Anwendung der hergeleiteten Formeln. □

Beispiel 3.1.7.

i.)

$$\begin{pmatrix} 2 & -2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = 2 \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} + (-2) \begin{pmatrix} 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 6 \end{pmatrix} + \begin{pmatrix} -8 & -10 & -12 \end{pmatrix}$$
$$= \begin{pmatrix} -6 & -6 - 6 \end{pmatrix}.$$

ii.)

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 4 \end{pmatrix} + 1 \begin{pmatrix} 2 \\ 5 \end{pmatrix} + 2 \begin{pmatrix} 3 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 \\ 12 \end{pmatrix} + \begin{pmatrix} 2 \\ 5 \end{pmatrix} + \begin{pmatrix} 6 \\ 12 \end{pmatrix} = \begin{pmatrix} 11 \\ 29 \end{pmatrix}. \quad \square$$

Folgende wichtige Regeln gelten für das Produkt von Matrizen:

Satz 3.1.8. *Sei R ein kommutativer Ring mit Eins.*

i.) Es seien folgende Matritzen gegeben:

$$A \in \mathrm{Mat}(m \times p, R), \quad B \in \mathrm{Mat}(p \times q, R) \quad \textit{und} \quad C \in \mathrm{Mat}(q \times n, R).$$

Dann existieren folgende Matrizenprodukte und es gilt die Gleichung:

$$A(BC) = (AB)C.$$

ii.) Es seien folgende Matrizen gegeben:

$$X \in \mathrm{Mat}(m \times p, R) \quad \textit{und} \quad Y, Z \in \mathrm{Mat}(p \times n, R).$$

Dann existieren folgende Matrizenprodukte und es gilt die Gleichung:

$$X(Y + Z) = XY + XZ.$$

iii.) Es seien folgende Matrizen gegeben:

$$Y, Z \in \mathrm{Mat}(m \times p, R) \quad \textit{und} \quad X \in \mathrm{Mat}(p \times n, R).$$

Dann existieren folgende Matrizenprodukte und es gilt die Gleichung:

$$(Y + Z)X = YX + ZX.$$

iv.) Es seien folgende Matrizen gegeben:

$$G \in \mathrm{Mat}(m \times p, R) \quad \textit{und} \quad H \in \mathrm{Mat}(p \times n, R).$$

Dann existieren folgende Matrizenprodukte, und es gilt für $\alpha \in R$:

$$G(\alpha H) = (\alpha G)H = \alpha(GH).$$

v.) Für $F \in \mathrm{Mat}(m \times n, R)$ gilt:

$$E_m F = F = F E_n.$$

vi.) Es sei $E_{i,k} \in \mathrm{Mat}(m \times p, R)$ und $E_{l,j} \in \mathrm{Mat}(p \times n, R)$. Dann existiert das Matrizenprodukt $E_{i,k}E_{l,j}$, und es gilt:

$$E_{i,k}E_{l,j} = \begin{cases} E_{i,j} & \textit{für } k = l, \\ \textit{Nullmatrix} & \textit{für } k \neq l. \end{cases}$$

Beweis.

i.) Die Matrizenprodukte sind definiert, da die Größen der einzelnen Matrizen den Anforderungen aus Definition 3.1.5 genügen. Es seien definiert:

$$(a_{i,j}) := A, \quad (b_{i,j}) := B \quad \text{und} \quad (c_{i,j}) := C.$$

Weiter seien definiert:

$$\begin{aligned} (s_{i,j}) &:= BC \in \mathrm{Mat}(p \times n, R) & (t_{i,j}) &:= A(BC) \in \mathrm{Mat}(m \times n, R), \\ (u_{i,j}) &:= AB \in \mathrm{Mat}(m \times q, R) & (w_{i,j}) &:= (AB)C \in \mathrm{Mat}(m \times n, R). \end{aligned}$$

Es ist dann zu zeigen, daß $t_{i,j} = w_{i,j}$ für alle $(i, j) \in I_{m,n}$ gilt:

$$\begin{aligned} t_{i,j} &= \sum_{k=1}^{p} a_{i,k}s_{k,j} = \sum_{k=1}^{p} a_{i,k}\Big(\sum_{l=1}^{q} b_{k,l}c_{l,j}\Big) = \sum_{k=1}^{p}\Big(\sum_{l=1}^{q} a_{i,k}b_{k,l}c_{l,j}\Big) \\ &= \sum_{l=1}^{q}\Big(\sum_{k=1}^{p} a_{i,k}b_{k,l}c_{l,j}\Big) = \sum_{l=1}^{q} c_{l,j}\Big(\sum_{k=1}^{p} a_{i,k}b_{k,l}\Big) \\ &= \sum_{l=1}^{q} c_{l,j}u_{i,l} = \sum_{l=1}^{q} u_{i,l}c_{l,j} = w_{i,j}. \end{aligned}$$

ii.) Die Matrizenprodukte sind definiert, da die Größen der einzelnen Matrizen den Anforderungen aus Definition 3.1.5 genügen. Es seien definiert:

$$(x_{i,j}) := X, \quad (y_{i,j}) := Y \quad \text{und} \quad (z_{i,j}) := Z.$$

Dann gilt $Y + Z = (y_{i,j} + z_{i,j})$. Weiter seien definiert:

$$(u_{i,j}) := X(Y + Z), \quad (v_{i,j}) := XY \quad \text{und} \quad (w_{i,j}) := XZ.$$

Es ist nun zu zeigen, daß $u_{i,j} = v_{i,j} + w_{i,j}$ für alle $(i,j) \in I_{n,m}$ gilt:

$$\begin{aligned} u_{i,j} &= \sum_{k=1}^{p} x_{i,k}(y_{k,j} + z_{k,j}) = \sum_{k=1}^{p}(x_{i,k}y_{k,j} + x_{i,k}z_{k,j}) \\ &= \sum_{k=1}^{p} x_{i,k}y_{k,j} + \sum_{k=1}^{p} x_{i,k}y_{k,j} = v_{i,j} + w_{i,j}. \end{aligned}$$

iii.) Die Matrizenprodukte sind definiert, da die Größen der einzelnen Matrizen den Anforderungen aus Definition 3.1.5 genügen. Es seien definiert:

$$(x_{i,j}) :=, \quad (y_{i,j}) := Y \quad \text{und} \quad (z_{i,j}) := Z.$$

Dann gilt $Y + Z = (y_{i,j} + z_{i,j})$. Weiter seien definiert:

$$(u_{i,j}) := (Y + Z)X, \quad (v_{i,j}) := YX \quad \text{und} \quad (w_{i,j}) := ZX.$$

Es ist zu zeigen, daß dann $u_{i,j} = v_{i,j} + w_{i,j}$ für alle $(i,j) \in I_{n,m}$ gilt:

$$\begin{aligned} u_{i,j} &= \sum_{k=1}^{p}(y_{i,k} + z_{i,k})x_{k,j} = \sum_{k=1}^{p}(y_{i,k}x_{k,j} + z_{i,k}x_{k,j}) \\ &= \sum_{k=1}^{p} y_{i,k}x_{k,j} + \sum_{k=1}^{p} z_{i,k}x_{k,j} = v_{i,j} + w_{i,j}. \end{aligned}$$

iv.) Die Matrizenprodukte existieren alle, da die Größen der einzelnen Matrizen den Anforderungen aus Definition 3.1.5 genügen. Es sei definiert:

$$(g_{i,j}) := G \quad \text{und} \quad (h_{i,j}) := H.$$

Die skalare Multiplikation einer Matrix mit einem Skalar geschieht komponentenweise, so daß sich die Größe der Matrix nicht ändert, und es gilt $\alpha G = (\alpha g_{i,j})$ und $\alpha H = (\alpha h_{i,j})$.
Mit den Definitionen

$$(u_{i,j}) := G(\alpha H), \quad (v_{i,j}) := (\alpha G)H \quad \text{und} \quad (w_{i,j}) := GH.$$

gilt $\alpha(GH) = (\alpha w_{i,j})$, und für alle $(i,j) \in I_{m,n}$ ist dann $u_{i,j} = v_{i,j} = \alpha w_{i,j}$ zu zeigen:

$$u_{i,j} = \sum_{k=1}^{p} g_{i,k}(\alpha h_{k,j}) = \underbrace{\sum_{k=1}^{p}(\alpha g_{i,k})h_{k,j}}_{=v_{i,j}} = \alpha \sum_{k=1} g_{i,k}h_{k,j} = \alpha w_{i,j}.$$

v.) Die Matrizenprodukte existieren wegen der passenden Größen der Matrizen (siehe Definition 3.1.5). Es gilt $E_n = (\delta_{i,j})$ nach Definition 3.1.1 ($\delta_{i,j}$ das Kroneckersymbol, 2.2.27). Weiter seien definiert:

$$(f_{i,j}) := F, \quad (u_{i,j}) := E_m F \quad \text{und} \quad (v_{i,j}) := FE_n.$$

Es ist zu zeigen, daß für alle $(i,j) \in I_{n,m}$ die Gleichung $u_{i,j} = f_{i,j} = v_{i,j}$ gilt:

$$u_{i,j} = \sum_{k=1}^{m} \delta_{i,k}f_{k,j} = f_{i,j} = \sum_{k=1}^{n} f_{i,k}\delta_{k,j} = v_{i,j}.$$

vi.) Das Matrizenprodukt existiert wegen der passenden Größen der Matrizen (siehe Definition 3.1.5). Es sei definiert:

$$(a_{r,s}) := E_{i,k}, \quad (b_{r,s}) := E_{l,j}, \quad \text{und} \quad (c_{r,s}) := E_{i,k}E_{l,j}.$$

Die Matrizen $E_{i,k}$ und $E_{l,j}$ können nach Definition 3.1.1 beschrieben werden als:

$$E_{i,k} = (\delta_{i,u} \cdot \delta_{v,k})_{(u,v)\in I_{i,k}} \quad \text{und} \quad E_{l,j} = (\delta_{l,u} \cdot \delta_{v,j})_{(u,v)\in I_{l,j}},$$

so daß folgt:

$$a_{u,v} = \delta_{i,u} \cdot \delta_{v,k} \quad \text{und} \quad b_{u,v} = \delta_{l,u} \cdot \delta_{v,j}.$$

Für $c_{r,s}$ gilt dann die Gleichung:

$$c_{r,s} = \sum_{w=1}^{p} a_{r,w}b_{w,s} = \sum_{w=1}^{p} (\delta_{i,r} \cdot \delta_{w,k}) \cdot (\delta_{l,w} \cdot \delta_{s,j}).$$

Das Produkt $\delta_{i,r} \cdot \delta_{w,k} \cdot \delta_{l,w} \cdot \delta_{s,j}$ ist nur Eins, wenn für die Indizes gilt:

$$i = r, \quad \underbrace{w = k, \quad l = w}_{\Longrightarrow k=l} \quad \text{und} \quad s = j.$$

Also ist für $k \neq l$ jeder Koeffizient $c_{r,s}$ Null und $E_{i,k}E_{l,j}$ die Nullmatrix.
Für $k = l$ ist genau ein Koeffizient $c_{r,s}$ gleich Eins, nämlich der für $r = i$ und $s = j$, also $c_{i,j}$, und alle anderen Koeffizienten sind Null, so daß $E_{i,k}E_{l,j} = E_{i,j}$ folgt. □

Die Formeln aus Satz 3.1.8 liefertn sorfort für die quadratischen $(n \times n)$-Matrizen folgende Strukturaussage:

Satz 3.1.9. *Sei R ein kommutativer Ring mit Eins. Dann ist* $\mathrm{Mat}(n \times n, R)$ *mit der Matrizenmultiplikation ein Ring mit Eins, der für $n \geq 2$ nicht kommutativ ist.*

Beweis.
Daß $\mathrm{Mat}(n \times n, R)$ mit der Matrizenaddition

$$(a_{i,j}) + (b_{i,j}) := (a_{i,j} + b_{i,j}) \quad \text{für} \quad (a_{i,j}), (b_{i,j}) \in \mathrm{Mat}(n \times n, R)$$

eine abelsche Gruppe ist mit der Nullmatrix als neutralem Element, folgt schon aus der R-Modulstruktur von $\mathrm{Mat}(n \times n, R)$ - siehe Satz 3.1.4.
Die Matrizenmultiplikation zwischen quadratischen $(n \times n)$-Matrizen ist eine innere Verknüpfung (siehe Definition 3.1.5), die nach Satz 3.1.8 assoziativ ist und das neutrale Element E_n besitzt, denn es gilt:

$$A(BC) = (AB)C \qquad \text{und} \qquad E_nA = A = AE_n.$$

Die Distributivgesetze gelten ebenfalls nach Satz 3.1.8:

$$A(B + C) = AB + AC \quad \text{und} \quad (B + C)A = BA + CA.$$

Das Matrizenprodukt ist in $\mathrm{Mat}(n \times n, R)$ für $n \geq 2$ nicht kommutativ, denn nach Satz 3.1.8 gilt:

$$E_{1,2}E_{2,1} \overset{(3.1.8)}{=} E_{1,1} \neq E_{2,2} \overset{(3.1.8)}{=} E_{2,1}E_{1,2}. \qquad \square$$

Für die quadratischen Matrizen sei dann definiert:

Definition 3.1.10. *Sei R ein kommutativer Ring mit Eins. Es sei $\mathrm{Mat}_n(R)$ der Ring $\mathrm{Mat}(n \times n, R)$ mit der Matrizenmultiplikation aus Satz 3.1.9. $\mathrm{Mat}_n(R)$ wird auch Matrizenring genannt.*
Die Einheitengruppe des Ringes $\mathrm{Mat}_n(R)$ (siehe auch Definition 1.3.10) wird mit $\mathrm{GL}_n(R)$ bezeichnet (mit „GL“ für „general linear group“). Ein $A \in \mathrm{GL}_n(R)$ heißt invertierbare Matrix. □

Um Eigenschaften von Matrizen besser untersuchen zu können, ist es nützlich, sie als lineare Abbildungen aufzufassen. Das Matrizenprodukt liefert zwei Änsätze dazu, denn aus der Multipliktions-Formel

$$(m \times p)\text{-Matrix} \quad \text{mal} \quad (p \times n)\text{-Matrix} \quad = \quad (m \times n)\text{-Matrix}.$$

folgt sofort anschaulich:

„Zeilen mal Matrix = Zeile“ und „Matrix mal Spalte = Spalte“,

so daß eine Matrix als Abbildung zwischen „Zeilenräumen“ oder „Spaltenräumen“ aufgefaßt werden kann (siehe dazu auch die Betrachtungen aus Lemma 3.1.6). Im Hinblick auf spätere Betrachtungen und hergeleitete Formeln ist es sinnvoll, hier zunächst die „Spaltenabbildung“ weiter zu betrachten. Dazu sei zuersteinmal der Spaltenraum $\mathrm{Mat}(n \times 1, R)$ kürzer notiert:

Definition 3.1.11. *Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann wird der nach Satz 3.1.4 freie R-Modul $\mathrm{Mat}(n \times 1, R)$ als Spaltenraum oder auch Koordinatenraum bezeichnet und mit $R^{[n]}$ notiert. Die Elemente des Spaltenraumes werden auch als Spaltenvektoren bezeichnet.*
Der freie R-Modul $\mathrm{Mat}(1 \times n, R)$ wird als Zeilenraum bezeichnet und dessen Elemente als Zeilenvektoren. □

Bemerkung 3.1.12.

i.) Nun werden spezielle Matrizen, die nur aus einer Zeile oder Spalte bestehen, sowohl als Matrix als auch als Vektor (Zeilen- oder Spaltenvektor) bezeichnet. Dies ist konsistent mit der Definition 3.1.1, wo einzelne Zeilen oder Spalten einer Matrix auch als Vektoren bezeichnet wurden.
Es ist anschaulicher, sich in einer Matrizenmultiplikation

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,n} & \dots & a_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

die beiden einspaltigen Matrizen als Vektoren vorzustellen.

ii.) Der Spaltenraum $R^{[n]}$ hat die Standard-Basis:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \dots, \quad e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

□

Es wurde in Bemerkung 3.1.2 schon darauf hingewiesen, daß die Elemente aus R^n und $\mathrm{Mat}(1 \times n, R)$ formal unterschiedliche Objekte sind, da die Indexmengen der jeweiligen n-Tupel (einmal $\{1, \ldots, n\}$ und einmal $\{1\} \times \{1, \ldots, n\}$) unterschiedlich sind, obwohl sich beide auf die gleiche Weise notieren lassen. Auch der Unterschied zwischen Zeilen- und Spaltenvektoren ist formal deren Indexmenge, obwohl es nur ein optischer Unterschied zu sein scheint, wie ein n-Tupel notiert wird. Daß alle drei Objekte auch mathematisch „fast“ identisch sind, zeigt folgende Aussage:

Lemma 3.1.13. *Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann sind folgende freien R-Moduln alle kanonisch isomorph:*

$$R^n \quad \cong \quad \mathrm{Mat}(1 \times n, R) \quad \cong \quad R^{[n]} = \mathrm{Mat}(n \times 1, R).$$

Ist insbesondere R ein Körper, so gilt für die dann R-Vektorräume:

$$\dim_R(R^n) = \dim_R\big(\mathrm{Mat}(1 \times n, R)\big) = \dim_R\big(\mathrm{Mat}(n \times 1)\big) = \dim_R(R^{[n]}) = n.$$

Beweis.
Die Elemente aus R^n sind n-Zeilentupel, ebenso die Elemente aus $\mathrm{Mat}(1 \times n, R)$, und alle R-Modulverknüpfungen sind komponentenweise definiert, so daß die offensichtliche Zuordnung

$$(x_1, \ldots, x_n) \mapsto (x_{1,1}, \ldots, x_{1,n})$$

ein R-Modulisomorphismus ist. Analoges gilt für die Zuordnung:

$$(x_{1,1}, \ldots, x_{1,n}) \mapsto \begin{pmatrix} x_{1,1} \\ \vdots \\ x_{n,1} \end{pmatrix},$$

die einen R-Modulisomorphismus von $\mathrm{Mat}(1 \times n, R)$ nach $R^{[n]} = \mathrm{Mat}(n \times 1, R)$ liefert. Die Aussagen über die Dimensionen im Fall eines Körpers als Skalarbereich sind dann klar wegen $\dim_R(R^n) = n$ (Lemma 2.2.29, und auch Satz 3.1.4). □

Trotzdem wird in diesem Text ein Unterschied zwischen R^n und $R^{[n]}$ gemacht, der sich im späteren Verlauf, wenn Matrizendarstellungen von linearen Abbildungen und dazu Koordinatenabbildungen intensiver betrachtet werden, als sehr nützlich erweisen wird.

Nun läßt sich formulieren, wie Matrizen als Abbildungen zwischen Spaltenräumen aufgefaßt werden sollen und welche Konsequenzen daraus folgen:

Satz 3.1.14. *Sei R ein kommutativer Ring mit Eins, und es seien $n, m \in \mathbb{N}$.*

i.) Es sei $A := (a_{i,j}) \in \mathrm{Mat}(m \times n, R)$ gegeben. Dann ist folgende Abbildung ein R-Modulhomomorphismus, d.h. eine lineare Abbildung:

$$\varphi_A \colon R^{[n]} \longrightarrow R^{[m]} \quad \textit{mit} \quad x \mapsto Ax.$$

Die Bilder der Standardbasis $(e_1, \dots, e_n)$ *des* $R^{[n]}$ *unter* φ_A *sind die Spaltenvektoren von* A*, d.h. es gilt:*

$$\varphi_A(e_i) = Ae_i = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} \underbrace{{}^{i-}\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}}_{\substack{i\text{-ter} \\ \text{Einheitsvektor}}} = \underbrace{\begin{pmatrix} a_{1,i} \\ \vdots \\ a_{m,i} \end{pmatrix}}_{\substack{i\text{-te Spalte} \\ \text{von } A}}$$

ii.) Die folgende Zuordnung ist eine injektive lineare Abbildung zwichen den beiden R*-Moduln* $\mathrm{Mat}(m \times n, R)$ *(siehe Satz 3.1.4) und* $\mathrm{Hom}_R(R^{[n]}, R^{[m]})$ *(siehe Satz 2.1.25):*

$$\Phi\colon \mathrm{Mat}(m \times n, R) \longrightarrow \mathrm{Hom}_R(R^{[n]}, R^{[m]}) \quad \textit{mit} \quad A \mapsto \varphi_A.$$

iii.) Die lineare Abbildung $\Phi\colon \mathrm{Mat}(m \times n, R) \longrightarrow \mathrm{Hom}(R^{[n]}, R^{[m]})$ *ist surjektiv. Ist* $\varphi \in \mathrm{Hom}_R(R^{[n]}, R^{[m]})$ *gegeben, so hat sie folgendes eindeutige Urbild* $[\varphi]$ *unter* Φ*: Die Spalten von* $[\varphi]$ *sind die Spaltenvektoren* $\varphi(e_i)$*, d.h. die Bilder der Standardbasis* $(e_1, \dots, e_n)$ *des* $R^{[n]}$ *unter der linearen Abbildung* φ*:*

$$[\varphi] := \begin{pmatrix} | & & | \\ \varphi(e_1) & \cdots & \varphi(e_n) \\ | & & | \end{pmatrix}.$$

Insbesondere ist damit $\Phi\colon \mathrm{Mat}(m \times n, R) \longrightarrow \mathrm{Hom}_R(R^{[n]}, R^{[m]})$ *ein* R*-Modulisomorphismus.*

iv.) Die Umkehrabbildung des obigen Modul-isomophismus Φ *ist:*

$$[\,\cdot\,]\colon \mathrm{Hom}_R(R^{[n]}, R^{[m]}) \longrightarrow \mathrm{Mat}(m \times n, R) \quad \textit{mit} \quad \varphi \mapsto [\varphi],$$

und es gelten damit für $A \in \mathrm{Mat}(m \times n, R)$ *und* $f \in \mathrm{Hom}_R(R^{[n]}, R^{[m]})$ *die Gleichungen:*

$$A = [\,\varphi_A\,] \qquad \textit{und} \qquad f = \varphi_{[f]}.$$

v.) Der R*-Modul* $\mathrm{Hom}_R(R^{[n]}, R^{[m]})$ *ist ein freier* R*-Modul, das System* $(\varphi_{i,j})_{(i,j)\in I_{m,n}}$ *mit* $\varphi_{i,j} := \Phi(E_{i,j})$ *als Bild der Standard-Basis* $(E_{i,j})_{(i,j)\in I_{m,n}}$ *von* $\mathrm{Mat}(m \times n, R)$ *unter* Φ *eine Basis, und es gilt:*

$$\varphi_{i,j}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = {}^{i-}\begin{pmatrix} 0 \\ \vdots \\ x_j \\ \vdots \\ 0 \end{pmatrix} \quad \textit{mit } x_j \textit{ an } i\textit{-ter Stelle} \quad = \quad x_j e_i.$$

Ist K *ein Körper, so gilt insbesondere für den* K*-Vektorraum* $\mathrm{Hom}_K(K^{[n]}, K^{[m]})$*:*

$$\dim_K\left(\mathrm{Hom}_K(K^{[n]}, K^{[m]})\right) = m \cdot n.$$

Beweis.

i.) Daß die Abbildung φ_A linear ist, liefern sofort die Rechenregeln von Satz 3.1.8, denn für $A \in \mathrm{Mat}(m \times n, R)$, $x, y \in R^{[n]}$ und $\alpha \in R$ gilt:

$$\begin{aligned} \varphi_A(x+y) &\overset{\text{(Def)}}{=} A(x+y) \overset{(3.1.8.ii)}{=} Ax + Ay = \varphi_A(x) + \varphi_A(y). \\ \varphi_A(\alpha x) &\overset{\text{(Def)}}{=} A(\alpha x) \overset{(3.1.8.iv)}{=} \alpha(Ax) = \alpha\varphi_A(x). \end{aligned}$$

Das Bild des i-ten Standardbasisvektors unter φ_A ergibt sich sofort mit Lemma 3.1.6:

$$\varphi_A(e_i) \overset{\text{(Def)}}{=} Ae_i = \begin{pmatrix} | & & | \\ s_1 & \cdots & s_n \\ | & & | \end{pmatrix} \underbrace{\begin{pmatrix} \delta_{1,i} \\ \vdots \\ \delta_{n,i} \end{pmatrix}}_{\substack{i\text{-ter} \\ \text{Einheitsvektor}}} = \sum_{k=1}^{n} \delta_{k,i} \begin{pmatrix} | \\ s_k \\ | \end{pmatrix}. = \begin{pmatrix} | \\ s_i \\ | \end{pmatrix}.$$

ii.) Daß Φ eine lineare Abbildung ist, ergibt sich sofort aus den Rechenregeln von Satz 3.1.8, denn für $A, B \in \mathrm{Mat}(m \times n, R)$, $x \in R^{[n]}$ und $\alpha \in R$ gilt:

$$\begin{aligned} \varphi_{A+B}(x) &\overset{\text{(Def)}}{=} (A+B)x \overset{(3.1.8.\text{iii})}{=} Ax + Bx = \varphi_A(x) + \varphi_B(x). \\ \varphi_{\alpha A}(x) &\overset{\text{(Def)}}{=} (\alpha A)x \overset{(3.1.8.\text{iv})}{=} \alpha(Ax) = \alpha\varphi_A(x). \end{aligned}$$

Damit folgen dann sofort die gewünschten Eigenschaften:

$$\begin{aligned} \Phi(A+B) &\overset{\text{(Def)}}{=} \varphi_{A+B} \overset{\text{(s.o.)}}{=} \varphi_A + \varphi_B = \Phi(A) + \Phi(B). \\ \Phi(\alpha A) &\overset{\text{(Def)}}{=} \varphi_{\alpha A} \overset{\text{(s.o.)}}{=} \alpha\varphi_A = \alpha\Phi(A). \end{aligned}$$

Die Abbildung Φ ist injektiv, denn es gilt: Ist A im Kern von Φ und damit $\Phi(A) = \varphi_A$ die Nullabbildung, so ist $\varphi_A(e_i)$ für alle Standard-Basisvektoren des $R^{[n]}$ der Nullvektor - und da nach obiger Aussage A als Spalten genau $\varphi(e_i)$ hat, A die Nullmatrix. Somit liegt im Kern von Φ nur die Null aus dem Raum $\mathrm{Mat}(m \times n, R)$, und nach Lemma 2.1.27 ist Φ injektiv.

iii.) Es ist zu zeigen, daß $\Phi\big([f]\big) = f$ gilt, d.h. $\varphi_{[f]} = f$, und nach Satz 2.2.31 muß dies nur auf der Standard-Basisvektoren des $R^{[n]}$ überprüft werden:

$$\varphi_{[f]}(e_i) \overset{\text{(s.o.)}}{=} i\text{-te Spalte von } [f] \overset{\text{(Def)}}{=} f(e_i).$$

iv.) Die Abbildung $[\,\cdot\,]$ ist nach obiger Aussage die Umkehrabbildung von Φ, da Φ eine Bijektion ist, und nach Satz 2.1.22 ist die mengentheoretische Umkehrabbildung einer linearen Abbildung auch linear.
Die Formeln folgen dann sofort aus den Definitionen und

$$\Phi \circ [\,\cdot\,] = \mathrm{id}_{\mathrm{Hom}_R(R^{[n]}, R^{[m]})} \qquad \text{und} \qquad [\,\cdot\,] \circ \Phi = \mathrm{id}_{\mathrm{Mat}(m \times n, R)}\,.$$

v.) Nach Satz 3.1.4 ist $\mathrm{Mat}(m \times n, R)$ ein freier R-Modul und $(E_{i,j})_{(i,j) \in I_{m,n}}$ eine Basis. Da Φ ein R-Modulisomorphismus ist, muß auch $\mathrm{Hom}_R(R^{[n]}, R^{[m]})$ ein freier R-Modul sein, und $\big(\Phi(E_{i,j})\big)_{(i,j) \in I_{m,n}}$ ist dann nach Satz 2.2.31 eine Basis von $\mathrm{Hom}_R(R^{[n]}, R^{[m]})$.

Es wird nun gezeigt, daß $\varphi_{i,j} := \Phi(E_{i,j})$ die behauptete Form hat, also gilt:

$$\varphi_{i,j}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = \varphi_{i,j}\Big(\sum_{k=1}^{n} a_k e_k\Big) \overset{(!)}{=} x_i e_j.$$

Da die Abbildung $\sum_{i=1}^{k} a_k e_k \mapsto x_j e_i$ offensichtlich linear ist, muß deren Übereinstimmung mit $\varphi_{i,j}$ nach Satz 2.2.31 nur auf den Standard-Basisvektoren $e_1, \ldots, e_n$ des $R^{[n]}$ überprüft werden.
Es ist $\varphi_{i,j} := \Phi(E_{i,j}) = \varphi_{E_{i,j}}$, und nach vorheriger Aussage ist $\varphi_{E_{i,j}}(e_k)$ gleich dem k-ten Spaltenvektor von $E_{i,j}$. Damit folgt:

$$\varphi_{E_{i,j}}(e_k) \quad = \quad \begin{cases} \text{Nullspalte} & \text{für } k \neq j, \\ e_i & \text{für } k = j \end{cases} \quad = \quad \varphi_{i,j}(e_k). \qquad \square$$

Wegen ihrer (auch konstruktiven) Relevanz seien die folgende Aussagen aus dem letzten Satzes noch einmal herausgehoben:

Bemerkung 3.1.15.

i.) *Ist eine Matrix $A \in \mathrm{Mat}(m \times n, R)$ gegeben, so ist φ_A die eindeutig bestimmte lineare Abbildung von $R^{[n]}$ nach $R^{[m]}$ mit*

$$Ax = \varphi_A(x)$$

für alle $x \in R^{[n]}$. Die Spalten der Matrix A sind dabei die Bilder der Standard-Basisvektoren des $R^{[n]}$ unter der Abbildung φ_A, die diese damit eindeutig beschreiben.

ii.) *Ist eine lineare Abbildung $\varphi\colon R^{[n]} \longrightarrow R^{[m]}$ gegeben, so ist $[\varphi] \in \mathrm{Mat}(m \times n, R)$ die eindeutig bestimmte Matrix mit*

$$\varphi(x) = [\varphi]x$$

für alle $x \in R^{[n]}$. Die Spalten von $[\varphi]$ sind dabei die Bilder der Standard-Basisvektoren des $R^{[n]}$ unter der Abbildung φ.

iii.) *Obige Beschreibungen liefern ein Verfahren, eine lineare Abbildung von $R^{[n]}$ nach $R^{[m]}$ zu konstruieren mit vorgegebenen Bildern der Standard-Basisvektoren. Die Existenz einer solchen Abbildung wurde schon in Satz 2.2.31 gezeigt, und diese dort durch lineare Fortsetzung definiert. Nun kann eine allgemeine Beschreibung konstruiert werden:*
Seien $e_1, \ldots, e_n$ die Standardbasisvektoren des $R^{[n]}$, und $b_1, \ldots, b_n \in R^{[m]}$ als deren Bilder gewählt. Weiter sei $A \in \mathrm{Mat}(m \times n, R)$ diejenige Matrix, in der die gewählten Bilder $b_1, \ldots, b_n$ als Spalten eingetragen sind:

$$e_1 \mapsto b_1, \ldots, e_n \mapsto b_n \qquad \rightsquigarrow \qquad A := \begin{pmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{pmatrix} \in \mathrm{Mat}(m \times n, R).$$

Dann ist φ_A eine lineare Abbildung von $R^{[n]}$ nach $R^{[m]}$ mit $\varphi_A(e_i) = b_i$, und für einen beliebigen Vektor $x \in R^{[n]}$ gilt:

$$\varphi_A(x) = Ax.$$

In Bemerkung 2.2.32 wurde eine lineare Abbildung $\varphi\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ definiert als lineare Fortsetzung von $e_1 \mapsto (1,2)$ und $e_2 \mapsto (2,1)$, und es ergab sich die allgemeine Abbildungsvorschrift:

$$e_1 \mapsto (1,2), \quad e_2 \mapsto (2,1) \qquad \rightsquigarrow \qquad \varphi\colon (x,y) \mapsto (x+2y,\, 2x+y).$$

Wird statt dem Zeilenraum $\mathbb{R}^2$ der Spaltenraum $\mathbb{R}^{[2]}$ gewählt und die gleiche Vorgabe gemacht, so ergibt obige Beschreibung folgende Matrix A:

$$e_1 \mapsto \begin{pmatrix}1\\2\end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix}2\\1\end{pmatrix} \qquad \rightsquigarrow \qquad A := \begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}.$$

Dies liefert dann folgende Abbildung $\varphi_A\colon \mathbb{R}^{[2]} \longrightarrow \mathbb{R}^{[2]}$:

$$\varphi_A\left(\begin{pmatrix}x\\y\end{pmatrix}\right) = \underbrace{\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}}_{=A}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}x+2y\\2x+y\end{pmatrix}. \qquad \square$$

Beispiel 3.1.16.

i.) Es sei die folgende lineare Abbildung gegeben (siehe auch Lemma 2.1.19):

$$\varphi\colon \mathbb{R}^{[3]} \longrightarrow \mathbb{R}^{[2]} \quad \textit{mit} \quad \begin{pmatrix}x\\y\\z\end{pmatrix} \mapsto \begin{pmatrix}3x-z\\x+y+z\end{pmatrix}.$$

Um die Matrix $[\varphi] \in \mathrm{Mat}(2\times 3, \mathbb{R})$ zu finden, muß die Abbildung φ auf die Standard-Basisvektoren $e_1, \ldots, e_3$ des $\mathbb{R}^{[3]}$ angewandt und die Spaltenvektoren $\varphi(e_i)$ in $[\varphi]$ eingetragen werden:

$$\varphi(e_1) = \varphi\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right) = \begin{pmatrix}3\\1\end{pmatrix}, \qquad \varphi(e_2) = \varphi\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right) = \begin{pmatrix}0\\1\end{pmatrix},$$

$$\varphi(e_3) = \varphi\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right) = \begin{pmatrix}-1\\1\end{pmatrix} \qquad \rightsquigarrow \qquad [\varphi] = \begin{array}{c} \begin{array}{ccc}\varphi(e_1) & \varphi(e_2) & \varphi(e_3)\end{array} \\ \begin{pmatrix}3 & 0 & -1\\1 & 1 & 1\end{pmatrix}\end{array}.$$

Es gilt nun für alle $x := \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} \in \mathbb{R}^{[3]}$:

$$\varphi(x) = \varphi\left(\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\right) = \begin{pmatrix}3x_1 - x_3\\x_1+x_2+x_3\end{pmatrix} = \begin{pmatrix}3 & 0 & -1\\1 & 1 & 1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} = [\varphi]x.$$

ii.) Es sei eine lineare Abbildung $\varphi\colon \mathbb{R}^{[2]} \longrightarrow \mathbb{R}^{[3]}$ gesucht, die folgende Bedingungen erfüllt:

$$e_1 \mapsto \begin{pmatrix}2\\1\\0\end{pmatrix} \quad \textit{und} \quad \varphi \textit{ ist injektiv.}$$

Die Abbildung φ ist nach Satz 2.2.31 injektiv, wenn die Bilder der Basis (e_1, e_2) unter φ linear unabhängig sind. Also kann für e_2 ein Bildvektor im $\mathbb{R}^{[3]}$ gesucht werden, der linear unabhängig zum Bild von e_1 ist, und mit den zwei Bildern

von e_1 und e_2 dann eine Abbildung φ konstruiert werden. Ein passender Vektor wäre zum Beispiel:

$$e_2 \mapsto \begin{pmatrix}0\\1\\2\end{pmatrix} \quad \textit{wegen} \quad \alpha\begin{pmatrix}2\\1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\\2\end{pmatrix} = \begin{pmatrix}2\alpha\\ \alpha+\beta\\ 2\beta\end{pmatrix} \overset{!}{=} \begin{pmatrix}0\\0\\0\end{pmatrix} \quad \Longrightarrow \quad \alpha = 0,\ \beta = 0.$$

Nach Bemerkung 3.1.15 kann nun eine Abbildung φ mit

$$\varphi\colon \quad e_1 \mapsto \begin{pmatrix}2\\1\\0\end{pmatrix} \quad \textit{und} \quad e_2 \mapsto \begin{pmatrix}0\\1\\2\end{pmatrix}$$

konstruiert werden, in dem die gewünschten Bilder der Standard-Basisvektoren e_1, e_2 als Spalten in eine Matrix A eingetragen werden: und dann erfüllt $\varphi := \varphi_A$ die gewünschten Eigenschaften.

$$A := \begin{array}{c} \begin{array}{cc}\varphi(e_1) & \varphi(e_2)\end{array} \\ \begin{pmatrix}2 & 0\\ 1 & 1\\ 0 & 2\end{pmatrix}\end{array} \quad \Longrightarrow \quad \varphi_A\left(\begin{pmatrix}x\\y\end{pmatrix}\right) = \begin{pmatrix}2 & 0\\ 1 & 1\\ 0 & 2\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}2x\\ x+y\\ 2y\end{pmatrix}. \qquad \square$$

Die Tatsache, daß für $A \in \mathrm{Mat}(m \times n, R)$ in dessen Spalten die Bilder der Standard-Basisvektoren des $R^{[n]}$ unter $\varphi_A\colon R^{[n]} \longrightarrow R^{[m]}$ stehen und damit nach dem Hauptsatz für lineare Abbildungen und Basen 2.2.31 viele Eigenschaften der durch A induzieren Abbildung φ_A ablesbar sind, ist im folgenden Lemma noch einmal zusammenfassend formuliert:

Lemma 3.1.17. *Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{Mat}(m \times n, R)$. Dann folgt für die durch A induzierte Abbildung φ_A:*

i.) φ_A ist eine lineare Abbildung von $R^{[n]}$ nach $R^{[m]}$.
ii.) Die Spalten von A sind ein Erzeugendensystem von $\mathrm{im}(\varphi_A)$.
iii.) Für φ_A gelten folgende Äquivalenzen:

$$\begin{array}{rcl} \varphi_A \textit{ injektiv} & \Longleftrightarrow & \textit{Die Spalten von } A \textit{ sind linear unabhängig.} \\ \varphi_A \textit{ surjektiv} & \Longleftrightarrow & \textit{Die Spalten von } A \textit{ erzeugen den } R^{[m]}. \\ \varphi_A \textit{ bijektiv} & \Longleftrightarrow & \textit{Die Spalten von } A \textit{ sind eine Basis des } R^{[m]}. \end{array}$$

Ist R ein Körper, so sind $R^{[n]}$ und $R^{[m]}$ Vektorräume, und es gilt zusätzlich:

- *Aus den Spalten von A kann eine Basis von $\mathrm{im}(\varphi_A)$ ausgewählt werden.*
- *φ_A ist genau dann surjektiv, wenn m Spalten von A linear unabhängig sind.*

Beweis.
Nach Satz 3.1.14 ist φ_A eine lineare Abbildung von $R^{[n]}$ nach $R^{[m]}$, und die Spalten von A sind die Bilder der Standard-Basisvektoren $e_1, \ldots, e_n \in R^{[n]}$ des $R^{[n]}$ unter φ_A. Da nach Lemma 2.2.13 die Bilder einer Basis unter φ_A ein Erzeugendensystem von $\mathrm{im}(\varphi_A)$ sind, gilt dies dann auch für die Spalten von A.
Die drei Äquivalenzen sind eine Übersetzung der Aussagen aus dem Hauptsatz über lineare Abbildungen und Basen 2.2.31, wobei „Bilder der Basis“ durch „Spalten von A“ ersetzt wurde.

Im Fall eines Vektorraumes kann aus einem Erzeugendensystem des Bildes $\operatorname{im}(\varphi_A)$ nach dem Basisauswahlsatz 2.2.43 immer eine Basis ausgewählt werden, also in diesem Fall aus den Spalten von A. Und für den Vektorraum $R^{[m]}$ gilt nach Lemma 2.2.53 die Äquivalenz:

$$\operatorname{im}(\varphi_A) = R^{[m]} \quad \Longleftrightarrow \quad \dim_R\big(\operatorname{im}(\varphi_A)\big) = m,$$

so daß auch die letzte Aussage sofort foglt. □

Beispiel 3.1.18.

i.) Es sei folgende Matrix $A \in \operatorname{Mat}(3 \times 2, \mathbb{R})$ *gegeben:*

$$A := \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Dann ist φ_A *eine Abbildung von* $\mathbb{R}^{[2]}$ *nach* $\mathbb{R}^{[3]}$*, und* φ_A *ist injektiv, da die beiden Spalten von* A *linear unabhängig sind (Übung!). Die Abbildung* φ_A *kann nicht surjektiv sein, da die Anzahl der Spalten von* A *kleiner ist als die Dimension von* $\mathbb{R}^{[3]}$ *(*$\mathbb{R}$*-Vektorraum!).*

ii.) Es sei folgende Matrix $B \in \operatorname{Mat}(2 \times 2, \mathbb{R})$ *gegeben:*

$$B := \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Dann ist φ_B *eine Abbildung von* $\mathbb{R}^{[2]}$ *nach* $\mathbb{R}^{[2]}$*, und* φ_B *ist injektiv, da die beiden Spalten von* B *linear unabhängig sind (Übung!). Die Abbildung* φ_B *ist auch surjektiv, da die Anzahl der Spalten von* B *gleich der Dimension des Wertebereichs* $\mathbb{R}^{[2]}$ *ist (*$\mathbb{R}$*-Vektorraum!), und damit zusammengefaßt ein Automorphismus.*

iii.) Wird die Matrix B *aus* $\operatorname{Mat}(2 \times 2, \mathbb{Z})$ *gewählt, ist mit den gleichen Argumenten* φ_B *ein injektiver* $\mathbb{Z}$*-Modulendomorphismus des* $\mathbb{Z}^{[2]}$*. Aber bei der Überprüfung der Surjektivität von* φ_B *kann das Argument über die Dimension nicht mehr verwandt werden, da* $\mathbb{Z}$ *kein Körper und damit* $\mathbb{Z}^{[2]}$ *kein Vektorraum ist. Tatsächlich ist* φ_B *dann auch nicht mehr surjektiv, was mit den bisherigen Mitteln nicht systematisch einzusehen ist. Wenn das bald entwickelte Instrument der Determinanten zur Verfügung steht, ist die Antwort leicht, denn* B *müßte dann eine Determinante haben, die eine Einheit in* $\mathbb{Z}$ *ist, was aber nicht der Fall ist (die Determinante von* B *ist* 3*).*
Für diesen konkreten Fall kann aber ein Vektor geraten werden, der nicht im Bild von φ_B *liegt, und dies wäre z.B.* $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$*:*

$$\varphi_B\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \Longrightarrow \quad \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \Longrightarrow \quad \begin{pmatrix} 2x + y \\ x + 2y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

und es würden sich die beiden Gleichungen $2x + y = 1$ *und* $x + 2y = 1$ *ergeben, die zu* $3x + 3y = 2$ *bzw.* $3(x + y) = 2$ *zusammengefaßt werden könnten. Aber die letzte Gleichung ist über* $\mathbb{Z}$ *nicht lösbar.* □

Die Identifikation von Matrizen und linearen Abbildungen zwischen Spaltenräumen ist auch verträglich mit dem Matrizenprodukt bzw. der Komposition von linearen Abbildungen:

Satz 3.1.19. *Sei R ein kommutativer Ring mit Eins.*

i.) Sei $A \in \mathrm{Mat}(m \times p, R)$ und $B \in \mathrm{Mat}(p \times n)$. Dann folgt für das Produkt der Matrizen $AB \in \mathrm{Mat}(m \times n, R)$, und es gilt:

$$\varphi_{AB} = \varphi_A \circ \varphi_B.$$

ii.) Sei $\varphi \in \mathrm{Hom}_R(R^{[p]}, R^{[m]})$ und $\psi \in \mathrm{Hom}_R(R^{[n]}, R^{[p]})$. Dann folgt für die Komposition der Abbildungen $(\varphi \circ \psi) \in \mathrm{Hom}_R(R^{[n]}, R^{[m]})$, und es gilt:

$$[\varphi \circ \psi] = [\varphi] \cdot [\psi].$$

Beweis.

i.) Die Aussage folgt sofort aus den Rechenregeln von Satz 3.1.8, denn es gilt für alle $x \in R^{[m]}$:

$$\varphi_{AB}(x) \overset{(\mathrm{Def})}{=} (AB)x \overset{(3.1.8)}{=} A(Bx) \overset{(\mathrm{Def})}{=} A\big(\varphi_B(x)\big) \overset{(\mathrm{Def})}{=} \varphi_A\big(\varphi_B(x)\big) = (\varphi_A \circ \varphi_B)(x).$$

ii.) Für $\varphi \circ \psi \in \mathrm{Hom}_R(R^{[n]}, R^{[m]})$ ist $[\varphi \circ \psi]$ die eindeutig bestimmte Matrix, so daß für $x \in R^{[n]}$ gilt:

$$(\varphi \circ \psi)(x) = [\varphi \circ \psi]x.$$

Mit den φ und ψ eindeutig zugeordneten Matrizen $[\varphi]$ und $[\psi]$ gilt nach den Rechenregeln aus Satz 3.1.8 für alle $x \in R^{[n]}$:

$$(\varphi \circ \psi)(x) = \varphi\big(\psi(x)\big) \overset{(\mathrm{Def})}{=} \varphi\big([\psi]x\big) \overset{(\mathrm{Def})}{=} [\varphi]([\psi]x) \overset{(3.1.8)}{=} ([\varphi] \cdot [\psi])x.$$

Dann folgt aus der eindeutigen Matrizendarstellung von $\varphi \circ \psi$ sofort:

$$[\varphi \circ \psi] = [\varphi] \cdot [\psi].$$

□

Dies liefert sofort für die beiden Ringe $\mathrm{Mat}_n(R)$ und $\mathrm{End}_R(R^{[n]})$:

Satz 3.1.20. *Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann sind $\mathrm{Mat}_n(R)$ und $\mathrm{End}_R(R^{[n]})$ Ringe mit Eins (Satz 3.1.9 und Lemma 2.1.24), und folgende Abbildungen sind zueinander inverse Ringisomorphismen (und gleichzeitig R-lineare Abbildungen):*

$$\begin{aligned} \Phi\colon \quad \mathrm{Mat}_n(R) &\longrightarrow \mathrm{End}_R(R^{[n]}) \quad \textit{mit} \quad A \mapsto \varphi_A, \\ [\,\cdot\,]\colon \mathrm{End}_R(R^{[n]}) &\longrightarrow \mathrm{Mat}_n(R) \quad \textit{mit} \quad \varphi \mapsto [\varphi]. \end{aligned}$$

Es gelten folgende Aussagen:

i.) Beide Ringisomorphismen bilden jeweils die Einselemente aufeinander ab:

$$\varphi_{E_n} = \mathrm{id} \qquad \textit{und} \qquad [\mathrm{id}] = E_n.$$

ii.) Für eine quadratische Matrix $A \in \mathrm{Mat}_n(R)$ und eine Abbildung $\varphi \in \mathrm{End}_R(R^{[n]})$ gelten die Äquivalenzen:

$$A \textit{ invertierbar} \iff \varphi_A \textit{ bijektiv} \qquad \textit{und} \qquad \varphi \textit{ bijektiv} \iff [\varphi] \textit{ invertierbar.}$$

iii.) Sind $A \in \mathrm{Mat}_n(R)$ und $\varphi \in \mathrm{End}_R(R^{[n]})$ invertierbar, so gilt:

$$\varphi_{A^{-1}} = (\varphi_A)^{-1} \qquad \textit{und} \qquad [\varphi^{-1}] = [\varphi]^{-1}.$$

Beweis.
Die beiden Abbildungen sind nach Satz 3.1.14 R-lineare Isomorphismen, so daß nur noch gezeigt werden muß, daß sie bzgl. der Ringmultiplikation strukturverträglich sind. Dies folgt aber sofort aus Satz 3.1.19.

i.) Für alle $x \in R^{[n]}$ gilt die Gleichung:

$$\varphi_{E_n}(x) \overset{\text{(Def)}}{=} E_n x \overset{(3.1.8)}{=} x,$$

so daß $\varphi_{E_n} = \mathrm{id}$ folgt. Dies liefert dann sofort mit Satz 3.1.8:

$$[id] = [\varphi_{E_n}] \overset{(3.1.8)}{=} E_n.$$

Also bilden beide Ringisomorphismen jeweils die Eins der Ringe aufeinaner ab.

ii.) A invertierbar $\Longrightarrow$ φ_A bijektiv: Ist A invertierbar, so gibt es eine Matrix B mit $AB = BA = E_n$. Dann folgt:

$$\left.\begin{aligned} \varphi_A \circ \varphi_B = \varphi_{AB} = \varphi_{E_n} = \mathrm{id}, \\ \varphi_B \circ \varphi_A = \varphi_{BA} = \varphi_{E_n} = \mathrm{id} \end{aligned}\right\} \overset{0.4.15}{\Longrightarrow} \varphi_A,\ \varphi_B \text{ bijektiv (und invers zueinander).}$$

φ_A bijektiv $\Longrightarrow$ A invertierbar: Ist φ_A bijektiv, so gibt es eine Umkehrabbildung $(\varphi_A)^{-1}$, und es folgt:

$$\left.\begin{aligned} A \cdot [(\varphi_A)^{-1}] = [\varphi_A] \cdot [(\varphi_A)^{-1}] = [\varphi_A \circ (\varphi_A)^{-1}] = [\mathrm{id}] = E_n, \\ [(\varphi_A)^{-1}] \cdot A = [(\varphi_A)^{-1}] \cdot [\varphi_A] = [(\varphi_A)^{-1} \circ \varphi_A] = [\mathrm{id}] = E_n \end{aligned}\right\} \Longrightarrow A \text{ invertierbar.}$$

Die zweite Äquivalenz folgt direkt aus der ersten.

iii.) Die behaupteten Identitäten folgen mit den Inversen A^{-1} von A und φ^{-1} von φ sofort aus folgenden Rechnungen:

$$\left.\begin{aligned} \varphi_A \circ \varphi_{A^{-1}} = \varphi_{AA^{-1}} = \varphi_{E_n} = \mathrm{id}, \\ \varphi_{A^{-1}} \circ \varphi_A = \varphi_{A^{-1}A} = \varphi_{E_n} = \mathrm{id} \end{aligned}\right\} \Longrightarrow (\varphi_A)^{-1} = \varphi_{A^{-1}}.$$

und

$$\left.\begin{aligned} [\varphi] \cdot [\varphi^{-1}] = [\varphi \circ \varphi^{-1}] = [\mathrm{id}] = E_n, \\ [\varphi^{-1}] \cdot [\varphi] = [\varphi^{-1} \circ \varphi] = [\mathrm{id}] = E_n \end{aligned}\right\} \Longrightarrow [\varphi^{-1}] = [\varphi]^{-1}. \qquad \square$$

3.2. Der Gauß-Algorithmus

Im folgenden wird gezeigt, daß für einen Körper K jede Matrix $A \in \mathrm{Mat}(m \times n, K)$ durch Multiplikation mit einer geeigneten invertierbaren Matrix $G \in \mathrm{GL}_n(K)$ (also einer Einheit im Matrizenring) in eine sogenannte „Zeilen-Stufen-Form“ transformieren läßt. Mit Hilfe dieser Zeilen-Stufen-Form von A lassen sich dann diverse Fragestellungen im Zusammenhang mit A klären: es können Gleichungssystem gelöst werden, die durch A beschrieben sind, für ein invertierbares A kann dessen Inverse berechnet werden etc. Die „geeignete“ invertierbare Matrix G wird dabei mit Hilfe des Gauß-Algorithmus konstruiert.

Viele Schritte dahin lassen sich allgemein über einem Ring formulieren und sind von allgemeinem Interesse, und auch der Gauß-Algorithmus kann in speziellen Situationen über einem Ring ausgeführt werden, so daß zunächst der allgemeiner Ansatz über einem Ring gewählt wird.

Zuersteinmal muß jedoch definiert werden, was eine Zeilen-Stufen-Form überhaupt sein soll. Dazu wird eine allgemein übliche Definition gegeben, und auch eine speziellere, die später von großem Nutzen ist, um obige Problemstellungen sehr effizient zu lösen:

Definition 3.2.1. *Sei R ein kommutativer Ring mit Eins. Dann besitzt eine Matrix $A := (a_{i,j}) \in \mathrm{Mat}(m \times n, R)$ Zeilen-Stufen-Form mit k Stufen, falls folgende Bedingungen erfüllt sind:*

- *Es gibt Spaltenindizes $1 \leq j_1 < \ldots < j_k \leq n$ mit $k \leq m$, so daß für die Koeffizienten $a_{i,j}$ von A gilt:*

$$\forall s \in \{1, \ldots, k\} : \quad i \geq s \text{ und } j < j_s \implies a_{i,j} = 0.$$

- *$a_{s,j_s} \neq 0$ für $1 \leq s \leq k$.*

Damit hat eine Zeilen-Stufen-Form mit k Stufen die Gestalt:

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \end{array}
\begin{array}{c}
\begin{array}{cccccc} & j_1 & & j_2 & & j_k \end{array} \\
\left(\begin{array}{ccccccc}
0 & 0 & *_1 & & & & \\
 & 0 & 0 & 0 & *_2 & & \\
 & & & 0 & 0 & 0 & \\
 & & & & & & \\
 & & & & & 0 & *_k \\
 & & & & & 0 & 0 \quad 0 \\
 & & & & & & 0
\end{array}\right)
\end{array}$$

beliebig

$i \geq 1$, $j < j_1$ | $i \geq 2$, $j < j_2$ | *Null* | $i \geq k$, $j < j_k$

mit:

i.) $*_i \neq 0$.
ii.) $*_i$ *in der j_i-ten Spalte.*
iii.) Null unterhalb der Treppe.

Die Matrix A hat spezielle Zeilen-Stufen-Form mit k Stufen, falls sie Zeilen-Stufen-Form hat und in der j_i-ten Spalte der i-te Standard-Basisvektor steht:

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \end{array}
\begin{array}{c}
\begin{array}{cccccc} & j_1 & & j_2 & & j_k \end{array} \\
\left(\begin{array}{ccccccc}
0 & 0 & 1 & & 0 & & 0 \\
 & 0 & 0 & 0 & 1 & & 0 \\
 & & & 0 & 0 & 0 & 0 \\
 & & & & & & \\
 & & & & & 0 & 1 \\
 & & & & & 0 & 0 \quad 0 \\
 & & & & & & 0
\end{array}\right)
\end{array}$$

Null

mit:

i.) e_i in der j_i-ten Spalte.
ii.) Null unterhalb der Treppe.

□

Beispiel 3.2.2.

i.) Die folgenden Matrizen haben Zeilen-Stufen-Form, aber keine spezielle Zeilen-Stufen-Form:

$$\begin{array}{c} \begin{array}{ccccc} & j_1 & & j_2 & j_3 \end{array} \\ \begin{pmatrix} 0 & 2 & 0 & 3 & 3 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix} \end{array}, \quad \begin{array}{c} \begin{array}{ccccc} & & j_1 & & \end{array} \\ \begin{pmatrix} 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \quad \textit{und} \quad \begin{array}{c} \begin{array}{cc} j_1 & j_2 \end{array} \\ \begin{pmatrix} 1 & 2 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} \end{array}.$$

ii.) Die folgenden Matrizen haben spezielle Zeilen-Stufen-Form:

$$\begin{array}{c} \begin{array}{ccccc} & j_1 & & j_2 & j_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}, \quad \begin{array}{c} \begin{array}{ccccc} & & j_1 & & \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \quad \textit{und} \quad \begin{array}{c} \begin{array}{cc} j_1 & j_2 \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \end{array}.$$

iii.) Die folgenden Matrizen haben keine Zeilen-Stufen-Form:

$$\begin{array}{c} \begin{array}{ccccc} & j_1 & & j_2 & j_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 3 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}, \quad \begin{array}{c} \begin{array}{ccccc} & & j_1 & & \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \quad \textit{und} \quad \begin{array}{c} \begin{array}{cc} j_1 & j_2 \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \end{array}. \qquad \square$$

Ziel ist nun, für eine Matrix A eine passende invertierbare Matrix G zu finden, so daß GA spezielle Zeilen-Stufen-Form hat. Die Matrix G wird dabei sukzessive als Produkt von speziellen invertierbaren Matrizen entwickelt: das Produkt von invertierbaren Matrizen ist natürlich wieder eine invertierbare Matrix, da die Einheiten eines Ringes eine multiplikative Gruppe sind. Als „Grundbausteine“ der folgenden Konstruktionen seien dazu folgende Matrizentypen betrachtet:

Definition 3.2.3. *Sei R ein kommutativer Ring mit Eins. Dann seien folgende drei Typen von quadratischen $(n \times n)$-Matrizen definiert:*

$$\begin{aligned} L_{i,j}^{(n)}(\lambda) &:= E_n + \lambda E_{i,j} && \textit{mit } \lambda \in R \textit{ und } i \neq j. \\ P_{i,j}^{(n)} &:= E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i} && \textit{mit } i < j. \\ D_i^{(n)}(\alpha) &:= E_n + (\alpha - 1)E_{i,i} && \textit{mit } \alpha \in R. \end{aligned} \qquad \square$$

Bemerkung 3.2.4.

i.) Bei den Matrizen $L_{i,j}^{(n)}(\lambda)$, $P_{i,j}^{(n)}$ und $D_i^{(n)}(\alpha)$ wird meist der obere Index „$^{(n)}$“ weggelassen, wenn keine Mißverständnisse auftreten können.

ii.) Die drei Matrizentypen aus der Definition 3.2.3 haben folgende schematische Darstellung:

$$L_{i,j}(\lambda) = \begin{array}{cc} & \begin{array}{cccc} & j & & \end{array} \\ i & \begin{pmatrix} 1 & & & \\ & 1 & & \\ & \lambda & 1 & \\ & & & \\ & & & 1 \end{pmatrix} \end{array}$$

Eine quadratische Einheitsmatrix mit genau einem Wert λ außerhalb der Diagonale, in der i-ten Zeile und j-ten Spalte. λ steht unterhalb der Diagonalen für $i > j$, und oberhalb der Diagonalen für $i < j$.

$$P_{i,j} = \begin{array}{c} \\ \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & i & j & & \end{array} \\ \begin{pmatrix} 1 & & & & \\ & & & & \\ & 0 & 1 & & \\ & & & & \\ & 1 & 0 & & \\ & & & & \\ & & & & 1 \end{pmatrix} \end{array}$$

Die i-te und j-te Spalte von E_n sind vertauscht.

$$D_i(\alpha) = \begin{array}{c} \\ \\ i \\ \\ \end{array} \begin{array}{c} \begin{array}{ccc} & i & \end{array} \\ \begin{pmatrix} 1 & & \\ & & \\ & \alpha & \\ & & \\ & & 1 \end{pmatrix} \end{array}$$

Diagonalmatrix mit lauter Einsen auf der Diagonalen, bis auf das i-te Diagonalelement, das α ist.

□

Beispiel 3.2.5. *Es seien folgende Matrizen aus* $\mathrm{Mat}(3 \times 3, \mathbb{Z})$ *betrachtet:*

$$L_{1,2}(3) = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad L_{3,1}(4) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}, \quad P_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$P_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad D_2(0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad D_3(4) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

□

Die Matrizen aus Definiton 3.2.3 sind fast alle invertierbar, nur bei dem Typ $D_i(\alpha)$ darf nicht ein beliebiges α gewählt werden. Gezeigt wird, daß für eine Einheit α, also ein (multiplikativ) invertierbares Element im Ring, auch $D_i(\alpha)$ invertierbar ist. Daß dies tatsächlich alle α sind und für eine Nicht-Einheit auch $D_i(\alpha)$ nicht invertierbar ist, wird erst im Abschnitt über Determinanten von Matrizen geklärt.

Satz 3.2.6. *Sei R ein kommutativer Ring mit Eins. Dann gelten für die Matrizen $L_{i,j}(\lambda), P_{i,j}$ und $D_i(\alpha)$ aus* $\mathrm{Mat}(n \times n, R)$ *folgende Aussagen:*

i.) $L_{i,j}(\lambda)$ ist invertierbar, und ihre Inverse ist $L_{i,j}(-\lambda)$, d.h. es gilt:

$$L_{i,j}(\lambda)L_{i,j}(-\lambda) = L_{i,j}(-\lambda)L_{i,j}(\lambda) = E_n.$$

ii.) $P_{i,j}$ ist invertierbar und zu sich selbst invers, d.h. es gilt:

$$P_{i,j}P_{i,j} = E_n.$$

iii.) Ist $\alpha \in R^*$ eine Einheit, so ist $D_i(\alpha)$ invertierbar, und ihre Inverse ist $D_i(\alpha^{-1})$, d.h. es gilt:

$$D_i(\alpha)D_i(\alpha^{-1}) = D_i(\alpha^{-1})D_i(\alpha) = E_n.$$

Beweis.

i.) Es ist $L_{i,j}(\lambda) = E_n + \lambda E_{i,j}$, und aus den Matrizenmultiplikationsregeln in Satz 3.1.8 und der Gleichung „$E_{i,j}E_{i,j} =$ Nullmatrix“ wegen $i \neq j$ folgt dann:

$$\begin{aligned} L_{i,j}(\lambda)L_{i,j}(-\lambda) &= \big(E_n + \lambda E_{i,j}\big)\big(E_n - \lambda E_{i,j}\big) \\ &= E_nE_n + E_n(-\lambda E_{i,j}) + (\lambda E_{i,j})E_n + (\lambda E_{i,j})(-\lambda E_{i,j}) \\ &= E_n + (-\lambda)(E_nE_{i,j}) + \lambda(E_{i,j}E_n) + \lambda(-\lambda)(E_{i,j}E_{i,j}) \\ &= E_n - \lambda E_{i,j} + \lambda E_{i,j} = E_n. \end{aligned}$$

Die Rechnung für $L_{i,j}(-\lambda)L_{i,j}(\lambda) = E_n$ läuft analog.

ii.) Es ist $P_{i,j} = E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, und die Matrizenmultiplikationsregeln 3.1.8 liefern mit $i \neq j$:

$$\begin{aligned} P_{i,j}P_{i,j} &= (E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i})(E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}) \\ &= E_nE_n - E_nE_{i,i} - E_nE_{j,j} + E_nE_{i,j} + E_nE_{j,i} && (*_1) \\ &\quad - E_{i,i}E_n + E_{i,i}E_{i,i} + E_{i,i}E_{j,j} - E_{i,i}E_{i,j} - E_{i,i}E_{j,i} && (*_2) \\ &\quad - E_{j,j}E_n + E_{j,j}E_{i,i} + E_{j,j}E_{j,j} - E_{j,j}E_{i,j} - E_{j,j}E_{j,i} && (*_3) \\ &\quad + E_{i,j}E_n - E_{i,j}E_{i,i} - E_{i,j}E_{j,j} + E_{i,j}E_{i,j} + E_{i,j}E_{j,i} && (*_4) \\ &\quad + E_{j,i}E_n - E_{j,i}E_{i,i} - E_{j,i}E_{j,j} + E_{j,i}E_{i,j} + E_{j,i}E_{j,i} && (*_5) \\ &= \underbrace{E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}}_{(*_1)} + \underbrace{(-E_{i,i}) + E_{i,i} - E_{i,j}}_{(\star_2)} \\ &\quad + \underbrace{(-E_{j,j}) + E_{j,j} - E_{j,i}}_{(\star_3)} + \underbrace{E_{i,j} - E_{i,j} + E_{i,i}}_{(\star_4)} + \underbrace{E_{j,i} - E_{j,i} + E_{j,j}}_{(\star 5)} \\ &= \underbrace{E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}}_{(*_1)} + \underbrace{(-E_{i,j})}_{(\star_2)} + \underbrace{(-E_{j,i})}_{(\star_3)} + \underbrace{E_{i,i}}_{(\star_4)} + \underbrace{E_{j,j}}_{(\star 5)} = E_n. \end{aligned}$$

iii.) Es ist $D_i(\alpha) = E_n + (\alpha - 1)E_{i,i}$, und die Matrizenmultiplikationsregeln aus Satz 3.1.8 liefern:

$$\begin{aligned} D_i(\alpha)D_i(\alpha^{-1}) &= \big(E_n + (\alpha - 1)E_{i,i}\big)(E_n + (\alpha^{-1} - 1)E_{i,i}) \\ &= E_nE_n + E_n\big((\alpha^{-1} - 1)E_{i,i}\big) + \big((\alpha - 1)E_{i,i}\big)E_n \\ &\quad + (\alpha - 1)E_{i,i}\big((\alpha^{-1} - 1)E_{i,i}\big)\big) \\ &= E_n + (\alpha^{-1} - 1)E_{i,i} + (\alpha - 1)E_{i,i} + (\alpha - 1)(\alpha^{-1} - 1)E_{i,i} \\ &= E_n + \big(\alpha^{-1} - 1 + \alpha - 1 + \underbrace{(\alpha - 1)(\alpha^{-1} - 1)}_{1-\alpha^{-1}-\alpha+1}\big)E_{i,i} = E_n. \end{aligned}$$

Die Rechnung für $D_i(\alpha^{-1})D_i(\alpha) = E_n$ läuft analog. □

Die Bedeutung der Matrizentypen $L_{i,j}(\lambda)$, $P_{i,j}$ und $D_i(\alpha)$ wird klar, wenn betrachtet wird, wie sie sich bei einem Produkt mit einer gegebenen Matrix A verhalten:

Satz 3.2.7. *Sei R ein kommutativer Ring mit Eins und $A := (a_{i,j}) \in \mathrm{Mat}(m \times n, R)$. Dann gelten für das Matrizenprodukt*

$$BA \quad \textit{mit} \quad B \in \{\, L_{i,j}(\lambda),\ P_{i,j},\ D_i(\alpha) \,\} \subseteq \mathrm{Mat}(m \times m, R)$$

die folgenden Bildungsgesetze:

$L_{i,j}(\lambda)A$: *Das λ-fache der j-ten Zeile von A wird zur i-ten Zeile A addiert.*

$P_{i,j}A$: *Die i-te und j-te Zeile von A werden vertauscht.*

$D_i(\alpha)A$: *Die i-te Zeile von A wird mit α multipliziert.*

Und für das Matrizenprodukt

$$AB \quad mit \quad B \in \{\, L_{i,j}(\lambda),\ P_{i,j},\ D_i(\alpha) \,\} \subseteq \mathrm{Mat}(n \times n, R)$$

gelten die folgenden Bildungsgesetze:

$AL_{i,j}(\lambda)$: *Das λ-fache der i-ten Spalte von A wird zur j-ten Spalte A addiert.*

$AP_{i,j}$: *Die i-te und j-te Spalte von A werden vertauscht.*

$AD_i(\alpha)$: *Die i-te Spalte von A wird mit α multipliziert.*

Beweis.

$L_{i,j}(\lambda)A$: Es ist $L_{i,j}(\lambda) = E_n + \lambda E_{i,j}$, und es folgt:

$$L_{i,j}(\lambda)A = (E_n + \lambda E_{i,j})A = E_nA + \lambda E_{i,j}A = A + \lambda E_{i,j}A.$$

Es ist also das Produkt $\lambda E_{i,j}A$ zu untersuchen. Nach Lemma 3.1.6 kann das Produkt $E_{i,j}A$ zeilenweise aufgebaut werden, und die k-te Zeile des Produktes ist gleich der k-ten Zeile von $E_{i,j}$ mal der Matrix A.
Da $E_{i,j}$ bis auf die i-te Zeile nur Nullzeilen enthält, gilt dies auch für das Produkt $E_{i,j}A$, so daß dann nur noch dessen i-te Zeile berechnet werden muß. In der i-ten Zeile von $E_{i,j}$ steht der j-te Standard-Basis-(Zeilen)-Vektor, so daß mit Lemma 3.1.6 folgt, wenn A zeilenweise notiert wird:

$$e_jA = \begin{array}{c} \qquad\quad j \\ \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \end{array} \begin{pmatrix} \text{—} \ z_1 \ \text{—} \\ \vdots \\ \text{—} \ z_m \ \text{—} \end{pmatrix} = \sum_{i=1}^{m} \delta_{i,j} \cdot \left(\text{—} \ z_i \ \text{—} \right)$$

$$= \left(\text{—} \ z_j \ \text{—} \right) \qquad \leftarrow \quad j\text{-te Zeile von } A.$$

Also ist $\lambda E_{i,j}A$ diejenige Matrix, die in der i-ten Zeile das λ-fache der j-ten Zeile von A enthält und sonst nur Nullzeilen, so daß bei der Summe $A + \lambda E_{i,j}A$ zur i-ten Zeile von A das λ-fache der j-ten Zeile von A addiert wird.

$P_{i,j}A$: Es ist $P_{i,j} = E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, und es folgt:

$$P_{i,j}A = (E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i})A = A - E_{i,i}A - E_{j,j}A + E_{i,j}A + E_{j,i}A.$$

Nach vorheriger Betrachtung ist $E_{k,l}A$ diejenige Matrix, die in der k-ten Zeile die l-te Zeile von A enthält und sonst nur Nullzeilen.
Damit wird in obiger Summe zuerst die i-te Zeile von A auf Null gesetzt (mit $-E_{i,i}A$) und später dort dessen j-te Zeile addiert/hingesetzt (mit $E_{i,j}A$). Analog wird in A die j-te Zeile auf Null gesetzt (mit $-E_{j,j}A$) und dann dort dessen i-te Zeile addiert/hingesetzt (mit $E_{j,i}A$). Somit sind zusammengefaßt die i-te und j-te Zeile von A vertauscht worden.

$D_i(\alpha)A$: Es ist $D_i(\alpha) = E_n + (\alpha - 1)E_{i,i}$, und es folgt:

$$D_i(\alpha)A = \big(E_n + (\alpha - 1)E_{i,i}\big)A = E_nA + (\alpha - 1)E_{i,i}A = A + \alpha E_{i,i}A - E_{i,i}A.$$

Nach vorheriger Betrachtung ist $E_{k,l}A$ diejenige Matrix, die in der k-ten Zeile die l-te Zeile von A enthält und sonst nur Nullzeilen.
Damit wird in A die i-te Zeile auf Null gesetzt (mit $-E_{i,i}A$), und dann dort das α-fache der i-ten Zeile von A addiert/hingesetzt (mit $\alpha E_{i,i}A$). Also steht in der i-ten Zeile von $D_i(\alpha)A$ das α-fache der i-ten Zeile von A, und die anderen Zeilen enthalten die entsprechenden Zeilen aus A.

$AL_{i,j}(\lambda)$: Es ist $L_{i,j}(\lambda) = E_n + \lambda E_{i,j}$, und es folgt:

$$AL_{i,j} = A(E_n + \lambda E_{i,j}) = AE_n + A(\lambda E_{i,j}) = A + \lambda AE_{i,j}.$$

Es ist also das Produkt $\lambda AE_{i,j}$ zu untersuchen. Nach Lemma 3.1.6 kann das Produkt $AE_{i,j}$ spaltenweise aufgebaut werden, und die k-te Spalte des Produktes ist gleich der Matrix A mal der k-ten Spalte von $E_{i,j}$.
Da $E_{i,j}$ bis auf die j-te Spalte nur Nullspalten enthält, gilt dies auch für das Produkt $AE_{i,j}$, so daß dann nur noch dessen j-te Spalte berechnet werden muß. In der j-ten Zeile von $E_{i,j}$ steht der i-te Standard-Basis-(Spalten)-Vektor, so daß mit Lemma 3.1.6 folgt, wenn A spaltenweise notiert wird:

$$Ae_i = \begin{pmatrix} | & & | \\ s_1 & \cdots & s_n \\ | & & | \end{pmatrix} i \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \sum_{k=1}^{n} \delta_{k,i} \cdot \begin{pmatrix} | \\ s_k \\ | \end{pmatrix} = \begin{pmatrix} | \\ s_i \\ | \end{pmatrix}.$$

Also ist $\lambda AE_{i,j}$ diejenige Matrix, die in der j-ten Spalte das λ-fache der i-te Spalte von A enthält und sonst nur Nullspalten, so daß bei der Summe $A + \lambda AE_{i,j}$ zur j-ten Spalte von A das λ-fache der i-ten Spalte von A addiert wird.

$AP_{i,j}$: Es ist $P_{i,j} = E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, und es folgt:

$$AP_{i,j} = A(E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}) = A - AE_{i,i} - AE_{j,j} + AE_{i,j} + AE_{j,i}.$$

Nach vorheriger Betrachtung ist $AE_{k,l}$ diejenige Matrix, die in der l-ten Spalte die k-te Spalte von A enthält und sonst nur Nullspalten.
Damit wird in obiger Summe zuerst die i-te Spalte von A auf Null gesetzt (mit $-AE_{i,i}$) und später dort dessen j-te Spalte addiert/hingesetzt (mit $AE_{j,i}$). Analog wird in A die j-te Spalte auf Null gesetzt (mit $-AE_{j,j}$) und dann dort dessen i-te Spalte addiert/hingesetzt (mit $AE_{i,j}A$). Somit sind zusammengefaßt die i-te und j-te Spalte von A vertauscht worden.

$AD_i(\alpha)$: Es ist $D_i(\alpha) = E_n + (\alpha - 1)E_{i,i}$, und es folgt:

$$AD_i(\alpha) = A\big(E_n + (\alpha - 1)E_{i,i}\big) = AE_n + (\alpha - 1)AE_{i,i} = A + \alpha AE_{i,i} - AE_{i,i}.$$

Nach vorheriger Betrachtung ist $AE_{k,l}$ diejenige Matrix, die in der l-ten Spalte die k-te Spalte von A enthält und sonst nur Nullspalten.
Damit wird in A die i-te Spalte auf Null gesetzt (mit $-AE_{i,i}$), und dann dort das α-fache der i-ten Spalte von A addiert/hingesetzt (mit $\alpha AE_{i,i}$). Also steht in der i-ten Spalte von $AD_i(\alpha)$ das α-fache der i-ten Spalte von A, und die anderen Spalten enthalten die entsprechenden Spalten aus A. □

Beispiel 3.2.8.

i.) Es sei folgende Matrix gegeben: $A := \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}(2 \times 2, \mathbb{R})$. *Dann gilt:*

$$\underbrace{\begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & 1 \end{pmatrix}}_{L_{2,1}\left(-\frac{1}{2}\right)} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & \frac{3}{2} \end{pmatrix}, \quad \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & \frac{2}{3} \end{pmatrix}}_{D_2\left(\frac{2}{3}\right)} \begin{pmatrix} 2 & 1 \\ 0 & \frac{3}{2} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\underbrace{\begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & 1 \end{pmatrix}}_{L_{1,2}(-1)} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \underbrace{\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}}_{D_1\left(\frac{1}{2}\right)} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Insbesondere ergibt sich aus obigen Rechnungen:

$$\underbrace{D_1\left(\tfrac{1}{2}\right) L_{1,2}(-1) D_2\left(\tfrac{2}{3}\right) L_{1,2}\left(-\tfrac{1}{2}\right)}_{=:B} A = E_2.$$

Folgende Gleichungen sind eine kleine Rechenübung:

$$B = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \qquad \textit{und} \qquad AB = BA = E_2.$$

Damit ist A invertierbar und B eine Inverse zu A. Daß aus der konstruierten Gleichung $BA = E_2$ schon die Invertierbarkeit von A folgt, wird bald bewiesen, und obige Rechnung ist ein Schema, welches zur generellen Berechnung von Inversen einer quadratischen Matrix eingesetzt werden kann (eine systematische Beschreibung folgt bald mit dem Gauß-Algorithmus).

ii.) Es sei folgende Matrix gegeben: $A := \left(\begin{smallmatrix} 1 & 2 \\ 0 & 4 \\ 2 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}(3 \times 2, \mathbb{Z})$. *Dann gilt:*

$$\begin{pmatrix} 1 & 2 \\ 0 & 4 \\ 2 & 2 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}}_{L_{1,2}(-2)} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 2 & -2 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 2 & -2 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{P_{1,2}} = \begin{pmatrix} 0 & 1 \\ 4 & 0 \\ -2 & 2 \end{pmatrix}. \qquad \square$$

Das erste Beispiel zeigt, wie mit Zeilenoperationen die Matrix A in eine spezielle Zeilen-Stufen-Form gebracht werden kann. Dabei wurde allerdings durch Koeffizienten geteilt, so daß diese Rechnung über $\mathbb{Z}$ nicht möglich gewesen wäre. Werden jedoch Matrizen mit Koeffizienten aus einem Körper betrachtet, so gilt allgemein:

Satz 3.2.9. *(Gauß-Algorithmus)*
Sei K ein Körper. Dann gilt für jede Matrix $A := (a_{i,j}) \in \mathrm{Mat}(m \times n, K)$ mit $A \neq$ Nullmatrix, daß es mindestens ein $G \in \mathrm{GL}_n(K)$ gibt, so daß GA eine spezielle Zeilen-Stufen-Form besitzt (und damit natürlich auch eine „einfache“ Zeilen-Stufen-Form).
Eine Matrix $G \in \mathrm{GL}_n(K)$ kann dabei durch folgenden Algorithmus gewonnen werden, der als Gauß-Algorithmus bekannt ist. Dabei sei die Matrix A auch spaltenweise notiert als:

$$A = \begin{pmatrix} | & & | \\ s_1 & \cdots & s_n \\ | & & | \end{pmatrix}.$$

Zuerst wird A in eine „einfache“ Zeilen-Stufen-Form gebracht:

1.) Schritt: *Sei $1 \leq j_1 \leq n$ der kleinste Index mit $s_{j_1} \neq$ Nullspalte. Da A keine Nullmatrix ist, muß es einen solchen Index geben.*
Da s_{j_1} keine Nullspalte ist, gibt es in der Spalte ein Element $a_1 := a_{l_1,j_1} \neq 0$. Dann hat das Produkt $P_{l_1,1}A$ folgende Gestalt:

$$P_{l_1,1}A = \begin{array}{c} \\ 1 \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccc} & & j_1 & & \end{array} \\ \begin{pmatrix} 0 & 0 & a_1 & * & \\ 0 & 0 & a_{2,j_1} & * & \\ 0 & 0 & a_{3,j_1} & * & \\ & & \vdots & & \\ 0 & 0 & a_{m,j_1} & * & \end{pmatrix} \end{array} \quad \textit{mit} \quad a_1 \neq 0.$$

Nun können alle Elemente der j_1-ten Spalte ab der zweiten Zeile zu Null gemacht werden, indem zur i-ten Zeile das $(-\frac{a_{i,j_1}}{a_1})$-fache der ersten Zeile addiert wird:

$$\underbrace{L_{m,1}(\lambda_m)\cdots L_{2,1}(\lambda_2)P_{l_1,1}}_{=:B_1}A = \begin{array}{c} \\ 1 \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccc} & & j_1 & & \end{array} \\ \begin{pmatrix} 0 & 0 & a_1 & * & \\ 0 & 0 & 0 & * & \\ 0 & 0 & 0 & * & \\ & & \vdots & & \\ 0 & 0 & 0 & * & \end{pmatrix} \end{array} \quad \textit{mit} \quad \lambda_i := -\frac{a_{i,j_1}}{a_1}.$$

2.) Schritt: *Wenn B_1A unterhalb der ersten Zeile nur Nullen enthält, ist B_1A eine Zeilen-Stufen-Form mit einer Stufe.*
Wenn es unterhalb der ersten Zeile einen Koeffizienten ungleich Null gibt, so sei $j_2 \leq n$ der kleinste Spaltenindex, dessen Spalte ein Element $a_2 := a_{l_2,j_2} \neq 0$ enthält (auf Grund der vorherigen Konstruktion muß $j_1 < j_2$ gelten). Die Matrix $P_{l_2,2}B_1A$ hat dann die Form:

$$P_{l_2,2}B_1A = \begin{array}{c} \\ 1 \\ 2 \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccc} & & j_1 & & & j_2 & \end{array} \\ \begin{pmatrix} 0 & 0 & a_1 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & a_2 & * \\ 0 & 0 & 0 & 0 & 0 & a_{3,j_2} & * \\ & & & & & \vdots & \\ 0 & 0 & 0 & 0 & 0 & a_{m,j_2} & * \end{pmatrix} \end{array} \quad \textit{mit} \quad a_1, a_2 \neq 0.$$

Nun können alle Elemente der j_2-ten Spalte ab der dritten Zeile zu Null gemacht werden, indem zur i-ten Zeile das $(-\frac{a_{i,j_2}}{a_2})$-fache der ersten Zeile addiert wird:

$$\underbrace{L_{m,2}(\lambda_m)\cdots L_{3,2}(\lambda_3)P_{l_2,1}}_{=:B_2}B_1A =$$

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccc} & & j_1 & & & j_2 & \end{array} \\ \begin{pmatrix} 0 & 0 & a_1 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & a_2 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & * \\ & & & & & \vdots & \\ 0 & 0 & 0 & 0 & 0 & 0 & * \end{pmatrix} \end{array} \quad \textit{mit} \quad \lambda_i := -\frac{a_{i,j_2}}{a_2}.$$

Algorithmus-Iteration: *Ist nach i-Schritten in der Matrix $B_iB_{i-1}\cdots B_1A$ unterhalb der i-ten Zeile kein Koeffizient ungleich Null vorhanden, ist eine gesuchte Zeilen-Stufen-Form mit i Stufen erreicht.*
Ansonsten wird der minimale Spaltenindex j_{i+1} gesucht und wie oben und analog weiter umgeformt.

Algorithmus-Terminierung: *Spätestens im m-ten Schritt sind unterhalb der m-ten Zeile keine Einträge ungleich Null mehr enthalten, da nur m Zeilen vorhanden sind, und der Algorithmus muß terminieren.*

Algorithmus-Ergebnis: *Es ist eine Zeilen-Stufen-Form mit k Stufen gefunden, mit Indizes $1 \le j_1 < \cdots < j_k \le n$, und Matrizen $B_1, \ldots, B_k$, so daß gilt:*

$$\underbrace{B_kB_{k-1}\cdots B_1}_{=:B}A = \begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccccccc} & & j_1 & & & j_2 & & & j_k & & \end{array} \\ \begin{pmatrix} 0 & 0 & a_1 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & a_2 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & & & & & \\ & & & & & & & & & \\ & & & & & & & 0 & a_k & * \\ & & & & & & & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Nun wird BA in spezielle Zeilen-Stufen-Form gebracht:

1.) Schritt: *Die Elemente $a_1, \ldots, a_k$ an den „Stufenecken“ werden zu Eins gemacht, indem die Zeilen $1, \ldots, k$ jeweils mit a_i^{-1} multipliziert werden, was wegen $a_i \neq 0$ möglich ist, da alle Elemente ungleich Null in einem Körper Einheiten sind. Es ergibt sich:*

$$\underbrace{D_k(a_k^{-1})\cdots D_1(a_1^{-1})}_{=:D}BA = \begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccccccc} & & j_1 & & & j_2 & & & j_k & & \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ & & & & & & & & & \\ & & & & & & & 0 & 1 & * \\ & & & & & & & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

2.) Schritt: *Die Spalte j_2 von DBA enthält evt. in der ersten Zeile, oberhalb der Eins, ein Element ungleich Null. Dies muß zur Null gemacht werden, um die spezielle Zeilen-Stufen-Form zu erreichen. Sei λ das entsprechende Element. Dann gilt:*

$$\underbrace{L_{1,2}(-\lambda)}_{=:C_2}DBA = \begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccccccc} & & j_1 & & & j_2 & & & j_k & & \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & * & * & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ & & & & & & & & & \\ & & & & & & & 0 & 1 & * \\ & & & & & & & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

3.) bis k.) Schritt: *Mit geeigneten Matrizen $C_3, \ldots, C_k$ können in den Spalten $j_3, \ldots, j_k$ oberhalb der Eins alle Elemente zu Null gemacht werden, wobei C_i dann ein Produkt $L_{1,i}(-\lambda_1) \cdots L_{i-1,i}(-\lambda_{i-1})$ ist mit $\lambda_1, \ldots, \lambda_{i-1}$ die Elemente in der j_i-ten Spalte oberhalb der Eins, und es ergibt sich letztendlich die gewünschte spezielle Zeilen-Stufen-Form:*

$$\underbrace{C_k \cdots C_2}_{=:C} DBA = \begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccccc} & & j_1 & & & j_2 & & & j_k & \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & * & * & 0 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ & & & & & & & & & \\ & & & & & & & 0 & 1 & * \\ & & & & & & & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Dann sei $G := CDB$, und GA hat obige spezielle Zeilen-Stufen-Form mit k-Stufen. Es ist $G \in GL_n(K)$, da es Produkt von inverterbaren Matrizen $P_{i,j}, L_{i,j}(\lambda)$ und $D_i(\alpha)$ ist (wegen $\alpha \neq 0 \implies \alpha \in K^*$). □

Bemerkung 3.2.10.

i.) *Es ist in der Literatur nicht eindeutig, was genau als Gauß-Algorithmus bezeichnet wird. Oft wird nur der Teil beschrieben, eine „allgemeine“ Zeilen-Stufen-Form zu erreichen. Auch wird er teilweise dahingegehend erweitert, daß neben Zeileoperationen auch Spaltenoperationen zugelassen werden, so daß dann eine Matrix A durch ein Produkt G_1AG_2 in eine dann noch speziellere Zeilen-Stufen-Form als die hier definierte spezielle Zeilen-Stufen-Form transformiert werden kann (G_1 und G_2 sind dann wieder Produkte von Matrizen der Form $L_{i,j}(\lambda)$, $P_{i,j}$ und $D_i(\alpha)$, und die Multiplikation von links arbeitet auf den Zeilen, und von rechts auf den Spalten).*

ii.) *Der Gauß-Algorithmus aus Satz 3.2.9 ist keine eindeutige Vorschrift, da beim Konstruieren einer „allgemeinen“ Zeilen-Stufen-Form die Wahl des „Ecken-Elementes“ a_i nicht eindeutig ist: es kann irgendein Nicht-Null-Element a_{l_i,j_i} der jeweiligen Nicht-Nullspalte gewählt und in die Ecken-Position getauscht werden. Dies führt dazu, daß die allgemeine Zeilen-Stufen-Form als Zwischenschritt dieses Gauß-Algorithmus nicht eindeutig ist. Da an dieser Stelle in vielen Büchern der Gauß-Algorithmus beendet ist, liefert er dann kein eindeutiges Ergebnis.*
Wird aber weiter verfahren wie in Satz 3.2.9, so korrigiert die Normierung der Ecken auf den Wert Eins und die Löschung der Einträge oberhalb der Einsen diese Mehrdeutigkeit, und es kann bewiesen werden, daß die dann erreichte spezielle Zeilen-Stufen-Form eindeutig ist.

iii.) *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$. Wird A mit Hilfe von Zeilenoperationsmatrizen $G_k \in \{ L_{i,j}(\lambda),\ P_{i,j},\ D_i(\alpha) \}$ in eine Matrix C transformiert, d.h. es gilt:*

$$\underbrace{G_s G_{s-1} \cdots G_1}_{=:G} A = C,$$

so ist manchmal die Matrix G von Interesse: z.B. wird bald gezeigt, daß aus einer Gleichung $GA = E_n$ schon A invertierbar und $G = A^{-1}$ folgt.

G kann natürlich immer als Produkt der G_i berechnet werden, aber dies erfordert das aufwändige Produkt vieler Matrizen. Wenn die Zeilenoperationsmatrizen G_i während eines Gauß-Algorithmus „konstruiert“ werden, so kann deren Produkt jedoch ohne viel Mehraufwand parallel berechnet werden: Dazu wird ausgenutzt, daß natürlich die Gleichung

$$G_s G_{s-1} \cdots G_1 = G_s G_{s-1} \cdots G_1 E_n$$

gilt, und das rechte Produkt durch die sukzessive Anwendung der Zeilenoperationen auf die Einheitsmatrix berechnet werden kann. Der Gauß-Algorithmus wird dann dahingehend „erweitert“, daß anstelle der schrittweisen Transformation von A in C durch Produkte:

$$G_i G_{i-1} \cdots G_1 A$$

gleichzeitig auch E_n mit den Zeilenoperationsmatrizen multipliziert bzw. einfach die jeweiligen Zeilenoperationen auf E_n angewand werden. Anstelle von A kann dann ein Erweitertes System $(A|E_n)$ bearbeitet werden, in dem beide Matrizen nebeneinanderstehen, und es gilt:

$$\underbrace{G_s G_{s-1} \cdots G_1}_{G}(A|E_n) = (GA|GE_n) = (C|G).$$

□

Beispiel 3.2.11. *i.) Es sei die folgende Matrix gegeben:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \mathrm{Mat}(3 \times 3, \mathbb{R}).$$

Um sie mit dem Gauß-Algorithmus in spezielle Zeilen-Stufen-Form zu bringen, wird sie zuerst in eine „allgemeine“ Zeilen-Stufen-Form gebracht:

1.) Schritt: Zuerst wird der Spaltenindex j_1 gesucht, die erste Spalte, die keine Nullspalte ist, und es folgt $j_1 = 1$. Dann muß ein Element der j_1-ten Spalte in die erste Zeile getauscht werden, welches nicht Null ist, aber da $a_{1,1} = 1 \neq 0$ gilt, kann dies unterbleiben.
Nun werden alle Elemente der j_1-ten Spalte unterhalb der Eins zu Null gemacht, indem geeignete Vielfache der ersten Zeile zu den folgenden addiert werden:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \xrightarrow[L_{3,1}(-7)]{L_{2,1}(-4)} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}.$$

Eine andere Notationsmöglichkeit wäre:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{matrix} -4 & -7 \\ + & \\ & + \end{matrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}.$$

2.) Schritt: Nun wird der Spaltenindex j_2 gesucht: die erste Spalte nach der j_1-ten, die unterhalb der ersten Zeile ein Element ungleich Null enthält, und es folgt $j_2 = 2$. Dann muß in der j_2-ten Spalte ein Element ungleich Null in die zweite Zeile getauscht werden, aber dort steht schon der Wert „-3“, so daß der Tausch unterbleiben kann.

Danach werden alle Elemente in der j_2-ten Spalte unterhalb der zweiten Zeile zu Null gemacht, indem geeignete Vielfache der zweiten Zeile zu den folgenden addiert werden:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \xrightarrow{L_{3,2}(-2)} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Eine andere Notationsmöglichkeit wäre:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \begin{array}{l} \\ -2 \\ + \end{array} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Die Matrix ist schon in Zeilen-Stufen-Form.
Nun wird die spezielle Zeilen-Stufen-Form konstruiert:

1.) Schritt: *Die Stufenecken, die im Moment die Werte 1 und -3 haben, werden alle zu Eins gemacht, indem die Zeilen mit den passenden Faktoren multipliziert werden:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{D_2\left(-\frac{1}{3}\right)} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Eine andere Notationsmöglichkeit wäre:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{l} \\ \mid \cdot \left(-\frac{1}{3}\right) \\ \\ \end{array} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

2.) Schritt: *Es muß noch in der j_2-ten Spalte oberhalb der Ecke jedes Element durch zu Null gemacht werden, indem ein geeignetes Vielfaches der zweiten Zeile addiert wird:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{L_{1,2}(-2)} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Eine andere Notationsmöglichkeit wäre:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{l} + \\ -2 \\ \\ \end{array} \longrightarrow \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Die resultierende Matrix ist schon eine spezielle Zeilen-Stufen-Form.
Es gilt damit:

$$\underbrace{L_{1,2}(-2)D_2\left(-\tfrac{1}{3}\right)L_{3,2}(-2)L_{3,1}(-7)L_{2,1}(-4)}_{=:G} A = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

ii.) Um im vorherigen Beispiel die Matrix G direkt zu erhalten, die A in die spezielle Zeilen-Stufen-Form C transformiert, kann der Gauß-Algorithmus auf das erweiterte System $(A|E_3)$ angewandt werden (siehe auch Bemerkung 3.2.10). Es ergibt sich dann

$$(A|E_3) \quad \rightsquigarrow \quad G(A|E_3) = (GA|GE_3) = (C|G)$$

mit $GA = C$.

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right) \begin{array}{l} -4 \\ + \\ -7 \\ + \end{array} \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{array}\right) \begin{array}{l} -2 \\ + \end{array} \longrightarrow$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right) \begin{array}{l} \\ |\cdot(-\frac{1}{3}) \\ \\ \end{array} \longrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right) \begin{array}{l} + \\ -2 \\ \\ \end{array}$$

$$\longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right)$$

Somit ist die transformierende Matrix G *von der Gestalt:*

$$G = \begin{pmatrix} -\frac{5}{3} & \frac{2}{3} & 0 \\ \frac{4}{3} & -\frac{1}{3} & 0 \\ 1 & -2 & 1 \end{pmatrix} \quad \textit{und} \quad \underbrace{\begin{pmatrix} -\frac{5}{3} & \frac{2}{3} & 0 \\ \frac{4}{3} & -\frac{1}{3} & 0 \\ 1 & -2 & 1 \end{pmatrix}}_{G} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}}_{A} = \underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}}_{C}.$$

iii.) Es sei folgende Matrix gegeben:

$$A := \begin{pmatrix} 0 & 0 & 1 & 2 & 1 \\ 1 & 1 & 2 & 3 & 0 \end{pmatrix} \in \mathrm{Mat}(2 \times 5, \mathbb{R}).$$

Um sie wie in Satz 3.2.9 in spezielle Zeilen-Stufen-Form zu bringen, sind folgende Schritte nötig (und es ergibt sich $j_1 = 1$ *und* $j_2 = 3$*):*

$$\begin{pmatrix} 0 & 0 & 1 & 2 & 1 \\ 1 & 1 & 2 & 3 & 0 \end{pmatrix} \begin{array}{l} \\ \\ \end{array} \longrightarrow \begin{pmatrix} 1 & 1 & 2 & 3 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix} \begin{array}{l} + \\ -2 \end{array} \longrightarrow \begin{pmatrix} 1 & 1 & 0 & -1 & -2 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix}.$$

iv.) Es sei die Matrix $A = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 5 \end{smallmatrix}\right) \in \mathrm{Mat}(2 \times 2, \mathbb{Q})$ *gegeben, und gesucht sind eine spezielle Zeilen-Stufen-Form von* A *und eine transformierende Matrix* G *aus dem Gauß-Algorithmus. Dazu wird der Gauß-Algorithmus auf das erweiterte System* $(A|E_2)$ *angewandt:*

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 2 & 5 & 0 & 1 \end{array}\right) \begin{array}{l} -2 \\ + \end{array} \longrightarrow \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{array}\right) \begin{array}{l} + \\ -2 \end{array} \longrightarrow \left(\begin{array}{cc|cc} 1 & 0 & 5 & -2 \\ 0 & 1 & -2 & 1 \end{array}\right).$$

Die spezielle Zeilen-Stufen-Form von A *ist dann* E_2*, und es gilt* $G = \left(\begin{smallmatrix} 5 & -2 \\ -2 & 1 \end{smallmatrix}\right)$*. Eine kurze Rechnung zeigt zusätzlich:* $GA = AG = E_2$*, so daß* G *sogar die Inverse zu* A *ist.* □

Anwendungen des Gauß-Algorithmus.

Rangbestimmung und Inverse.

Das letzte Beispiel zeigt wieder, wie auch schon ganz zu Anfang gesagt, daß der Gauß-Algorithmus die Inverse einer Matrix liefert, wenn deren spezielle Zeilen-Stufen-Form die Einheitsmatrix ist. Bevor dies bewiesen wird, soll noch der Rang einer Matrix definiert werden. Dazu wird zuerst der Zeilen- und Spaltenrang einer Matrix definiert, da eine Matrix wahleise als Zusammenfassung von Zeilenvektoren oder Spaltenvektoren aufgefaßt werden kann, und mit dem später folgendem Satz, daß Zeilen- und Spaltenrang einer Matrix immer übereinstimmen, kann dann „der“ Rang definiert werden.

Definition 3.2.12. *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$ keine Nullmatrix. Die Matrix A sei einmal spaltenweise und einmal zeilenweise notiert:*

$$A = \begin{pmatrix} \text{—} & z_1 & \text{—} \\ & \vdots & \\ \text{—} & z_m & \text{—} \end{pmatrix} \qquad \textit{und} \qquad A = \begin{pmatrix} | & & | \\ s_1 & \cdots & s_n \\ | & & | \end{pmatrix}.$$

Dann sind die Spalten $s_1, \ldots, s_n$ Elemente des K-Vektorraumes $K^{[m]}$, und der Spaltenrang von A ist defniert als:

$$\mathrm{rg}_{Spalte}(A) := \dim_K \big(\langle\, s_1, \ldots, s_n \,\rangle\big).$$

Die Zeilen $z_1, \ldots, z_m$ sind Elemente des K-Vektorraumes K^n, und der Zeilenrang von A ist definiert als:

$$\mathrm{rg}_{Zeile}(A) := \dim_K \big(\langle\, z_1, \ldots, z_m \,\rangle\big). \qquad \square$$

Bemerkung 3.2.13.

i.) Ist $A \in \mathrm{Mat}(m \times n, K)$ für einen Körper K, so ist die durch A induzierte lineare Abbildung φ_A aus $\mathrm{Hom}_K(K^{[n]}, K^{[m]})$ (siehe Satz 3.1.14), und die Bilder $\varphi_A(e_1), \ldots, \varphi_A(e_n)$ der Standard-Basisvektoren $e_1, \ldots, e_n$ des $K^{[n]}$ sind ein Erzeugendensystem von $\mathrm{im}(\varphi_A)$ (Lemma 2.2.13).
Nach Satz 3.1.14 sind die Bilder $\varphi_A(e_1), \ldots, \varphi_A(e_n)$ aber auch genau die Spalten von A, so daß sofort folgt:

$$\mathrm{rg}_{Spalte}(A) = \dim_K \big(\mathrm{im}(\varphi_A)\big) \overset{(Def\ 2.2.58)}{=} \mathrm{rg}_K(\varphi_A).$$

ii.) Für eine Matrix $A \in \mathrm{Mat}(m \times n, K)$ über einem Körper K gelten offensichtilich die Abschätzungen:

$$\mathrm{rg}_{Zeile}(A) \leq \dim_K(K^n) = n \quad \textit{und} \quad \mathrm{rg}_{Spalte}(A) \leq \dim_K(K^{[m]}) = m.$$

Außerdem gelten die Gleichungen:

$$\begin{aligned} \mathrm{rg}_{Zeile}(A) &= \text{„}\textit{Maximale Anzahl linear unabhängiger Zeilen von } A.\text{“} \\ \mathrm{rg}_{Spalte}(A) &= \text{„}\textit{Maximale Anzahl linear unabhängiger Spalten von } A.\text{“} \end{aligned} \qquad \square$$

Daß die maximale Anzahl linear unabhängiger Spalten und Zeilen einer Matrix immer gleich sind, ist nicht offensichtlich, aber dies folgt sofort für eine Matrix in spezieller Zeilen-Stufen-Form:

LEMMA 3.2.14. *Sei K ein Körper, und $A \in \mathrm{Mat}(m \times n, K)$ habe spezielle Zeilen-Stufen-Form mit k Stufen:*

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} & & j_1 & & j_2 & & j_k & \end{array} \\ \left(\begin{array}{cccccccc} 0 & 0 & 1 & & 0 & & 0 & \\ & 0 & 0 & 0 & 1 & & 0 & \\ & & & 0 & 0 & 0 & 0 & \\ & & & & & & & \\ & & & & & & 0 & 1 \\ & & \text{Null} & & & & 0 & 0 \\ & & & & & & & 0 \end{array}\right) \end{array} \quad \text{mit:} \quad \begin{array}{l} \text{i.) } e_i \text{ in der } j_i\text{-ten Spalte.} \\ \text{ii.) Null unterhalb der Treppe.} \end{array}$$

Dann gilt:

$$\mathrm{rg}_{Zeile}(A) = \mathrm{rg}_{Spalte}(A) = k.$$

BEWEIS.

$\mathrm{rg}_{Spalte}(A) = k$: Die Spalten mit den Spaltenindizes $j_1, \ldots, j_k$ sind die Standard-Basisvektoren $e_1, \ldots, e_k$ und damit linear unabhängig. Da alle Spalten von A nur Einträge in den ersten k Zeilen haben, sind sie auch ein Erzeugendensystem des von allen Spalten erzeugten Raumes.

$\mathrm{rg}_{Zeile}(A) = k$: Da nur die ersten k Zeilen von A ungleich dem Nullvektor sind, erzeugen sie schon den von allen Zeilen erzeugten Raum. Wegen ihrer speziellen Form (die i-te Zeile hat den ersten Eintrag ungleich Null an der j_i-ten Stelle) sind sie offensichtlich auch linear unabhängig (wegen $j_i < j_{i+1}$), so daß sie sogar eine Basis sind. □

Um für beliebige Matrizen eine Formel „Zeilenrang = Spaltenrang“ zu bekommen, reicht es nun zu zeigen, daß jede Matrix Matrix den gleichen Zeilen- und Spaltenrang hat wie ihre spezielle Zeilen-Stufen-Form. Und dazu genügt es zu zeigen, daß die Multiplikation von links mit einer invertierbaren Matrix beide Ränge nicht verändert.

LEMMA 3.2.15. *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$ keine Nullmatrix. Weiter seien $B \in \mathrm{GL}_m(K)$ und $C \in \mathrm{GL}_n(K)$. Dann gilt:*

$$\mathrm{rg}_{Zeile}(BA) = \mathrm{rg}_{Zeile}(A) \quad \textit{und} \quad \mathrm{rg}_{Spalte}(AC) = \mathrm{rg}_{Spalte}(A).$$

BEWEIS.

$\mathrm{rg}_{\mathrm{Zeile}}(BA) = \mathrm{rg}_{\mathrm{Zeile}}(A)$: Es seien $z_1, \ldots, z_m$ die Zeilen von A und $w_1, \ldots, w_m$ die Zeilen von BA. Nach Lemma 3.1.6 ist jede Zeile von BA eine Linearkombination der Zeilen von A, und es folgt:

$$\begin{aligned} \langle\, w_1, \ldots, w_m \,\rangle \subseteq \langle\, z_1, \ldots, z_m \,\rangle &\implies \dim_K \big(\langle\, w_1, \ldots, w_m \,\rangle\big) \leq \dim_K \big(\langle\, z_1, \ldots, z_m \,\rangle\big) \\ &\implies \mathrm{rg}_{\mathrm{Zeile}}(BA) \leq \mathrm{rg}_{\mathrm{Zeile}}(A). \end{aligned}$$

Da B invertierbar ist, existiert B^{-1} mit $B^{-1}B = E_m$, und wie oben argumentiert sind die Zeilen von $A = B^{-1}(BA)$ eine Linearkombination der Zeilen von BA, woraus dann folgt:

$$\begin{aligned} \langle\, z_1, \ldots, z_m \,\rangle \subseteq \langle\, w_1, \ldots, w_m \,\rangle &\implies \dim_K \big(\langle\, z_1, \ldots, z_m \,\rangle\big) \leq \dim_K \big(\langle\, w_1, \ldots, w_m \,\rangle\big) \\ &\implies \mathrm{rg}_{\mathrm{Zeile}}(A) \leq \mathrm{rg}_{\mathrm{Zeile}}(BA). \end{aligned}$$

Zusammengefaßt liefert dies wie gewünscht:

$$\mathrm{rg}_{\mathrm{Zeile}}(BA) = \mathrm{rg}_{\mathrm{Zeile}}(A).$$

$\mathrm{rg}_{\mathrm{Spalte}}(AC) = \mathrm{rg}_{\mathrm{Spalte}}(A)$: Es seien $s_1, \ldots, s_n$ die Spalten von A und $v_1, \ldots, v_n$ die Spalten von AC. Nach Lemma 3.1.6 sind die Spalten von AC eine Linearkombination der Spalten von A, und es folgt:

$$\begin{aligned} \langle\, v_1, \ldots, v_n \,\rangle \subseteq \langle\, s_1, \ldots, s_n \,\rangle &\implies \dim_K \big(\langle\, v_1, \ldots, v_n \,\rangle\big) \leq \dim_K \big(\langle\, s_1, \ldots, s_n \,\rangle\big) \\ &\implies \mathrm{rg}_{\mathrm{Spalte}}(AC) \leq \mathrm{rg}_{\mathrm{Spalte}}(A). \end{aligned}$$

Da C invertierbar ist, existiert C^{-1} mit $CC^{-1} = E_n$, und wie oben argumentiert sind die Spalten von $A = (AC)C^{-1}$ eine Linearkombination der Spalten von AC, woraus dann folgt:

$$\begin{aligned} \langle\, s_1, \ldots, s_n \,\rangle \subseteq \langle\, v_1, \ldots, v_n \,\rangle &\implies \dim_K \big(\langle\, s_1, \ldots, s_n \,\rangle\big) \leq \dim_K \big(\langle\, v_1, \ldots, v_n \,\rangle\big) \\ &\implies \mathrm{rg}_{\mathrm{Spalte}}(A) \leq \mathrm{rg}_{\mathrm{Spalte}}(AC). \end{aligned}$$

Zusammengefaßt liefert dies wie gewünscht:

$$\mathrm{rg}_{\mathrm{Spalte}}(AC) = \mathrm{rg}_{\mathrm{Spalte}}(A). \qquad \square$$

Lemma 3.2.16. *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$ keine Nullmatrix. Weiter sei $B \in \mathrm{GL}_m(K)$. Dann gilt:*

$$\mathrm{rg}_{Spalte}(BA) = \mathrm{rg}_{Spalte}(A).$$

Beweis.
Die Matrizen A, B induzieren folgendes kommutative Diagramm von linearen Abbildungen (siehe Satz 3.1.8):

$$\begin{tikzcd} K^{[n]} \arrow[r, "\varphi_A"] \arrow[dr, "\varphi_B \circ \varphi_A \overset{(3.1.19)}{=} \varphi_{BA}"'] & K^{[m]} \arrow[d, "\varphi_B"] \\ & K^{[m]} \end{tikzcd}$$

Es gilt dann folgende Aussage:

$$\varphi_B\big(\mathrm{im}(\varphi_A)\big) = \mathrm{im}(\varphi_B \circ \varphi_A). \qquad (\star)$$

Beweis der Aussage:

„$\subseteq$“: Ist $z \in \varphi_B\big(\mathrm{im}(\varphi_A)\big)$, so gibt es ein $y \in \mathrm{im}(\varphi_A)$ mit $\varphi_B(y) = z$, und ein $x \in K^{[n]}$ mit $y = \varphi_A(x)$, und es folgt zusammengefaßt:

$$z = \varphi_B(y) = \varphi_B\big(\varphi_A(x)\big) = (\varphi_B \circ \varphi_A)(x) \quad \implies \quad z \in \mathrm{im}(\varphi_B \circ \varphi_A).$$

„$\supseteq$“: Ist $z \in \mathrm{im}(\varphi_B \circ \varphi_A)$, so gibt es ein $x \in K^{[n]}$ mit $z = (\varphi_B \circ \varphi_A)(x)$. Mit $y := \varphi_A(x) \in \mathrm{im}(\varphi_A)$ folgt dann:

$$z = (\varphi_B \circ \varphi_A)(x) = \varphi_B\big(\underbrace{\varphi_A(x)}_{\in \mathrm{im}(\varphi_A)}\big) \quad \implies \quad z \in \varphi_B\big(\mathrm{im}(\varphi_A)\big).$$

Damit ist die (Hilfs-)Aussage gezeigt.
B ist invertierbar und somit nach Satz 3.1.20 auch φ_B (d.h. φ_B ist ein Isomorphismus), und es folgt sofort

$$\dim_K\big(\operatorname{im}(\varphi_A)\big) = \dim_K\Big(\varphi_B\big(\operatorname{im}(\varphi_A)\big)\Big), \tag{$*$}$$

da φ_B eine Basis von $\operatorname{im}(\varphi_A)$ auf eine Basis von $\varphi_B\big(\operatorname{im}(\varphi_A)\big)$ abbildet (siehe auch Satz 2.2.31).
Dies alles zusammengefaßt liefert dann:

$$\begin{aligned}\operatorname{rg}_{\text{Spalte}}(A) &\overset{(3.2.13)}{=} \dim_K\big(\operatorname{im}(\varphi_A)\big) \overset{(*)}{=} \dim_K\Big(\varphi_B\big(\operatorname{im}(\varphi_A)\big)\Big) \overset{(*)}{=} \dim_K\big(\operatorname{im}(\varphi_B\circ\varphi_A)\big)\\ &\overset{(3.1.19)}{=} \dim_K\big(\operatorname{im}(\varphi_{BA})\big) \overset{(3.2.13)}{=} \operatorname{rg}_{\text{Spalte}}(BA).\end{aligned}$$

□

Nun sind alle Teilaussagen bewiesen, um endgültig zu zeigen, daß bei jeder Matrix Zeilenrang und Spaltenrang übereinstimmen:

Satz 3.2.17. *Sei K ein Körper und $A \in \operatorname{Mat}(m\times n, K)$ keine Nullmatrix. Dann gilt:*

$$\operatorname{rg}_{Zeile}(A) = \operatorname{rg}_{Spalte}(A).$$

Beweis.
Es gibt eine invertierbare Matrix $G \in \operatorname{GL}_n(K)$, so daß GA eine spezielle Zeilen-Stufen-Form hat (Gauß-Algorithmus 3.2.9), und A und GA haben den gleichen Zeilenrang (Lemma 3.2.15) und den gleichen Spaltenrang (Lemma 3.2.16). Nach Lemma 3.2.14 sind bei GA Zeilen- und Spaltenrang gleich, so daß folgt:

$$\operatorname{rg}_{\text{Zeile}}(A) \overset{(3.2.15)}{=} \operatorname{rg}_{\text{Zeile}}(GA) \overset{(3.2.14)}{=} \operatorname{rg}_{\text{Spalte}}(GA) \overset{(3.2.16)}{=} \operatorname{rg}_{\text{Spalte}}(A).$$

□

Damit kann der Rang einer Matrix definiert werden:

Definition 3.2.18. *Sei K ein Körper und $A \in \operatorname{Mat}(m\times n, K)$ keine Nullmatrix. Dann ist der Rang von A definiert als der Spaltenrang von A, der nach Satz 3.2.17 gleich dem Zeilenrang von A ist.*

$$\operatorname{rg}(A) := \operatorname{rg}_{Spalte}(A) \overset{(3.2.17)}{=} \operatorname{rg}_{Zeile}(A).$$

□

Bemerkung 3.2.19.

i.) Nach Bemerkung 3.2.13 gilt für einen Körper K, $A \in \operatorname{Mat}(m\times n, K)$ und die durch A induzierte lineare Abbildung $\varphi_A\colon K^{[n]} \longrightarrow K^{[m]}$:

$$\operatorname{rg}(A) = \operatorname{rg}_K(\varphi_A).$$

ii.) Für $A \in \operatorname{Mat}(m\times n, K)$ gilt dann wegen der Gleichheit von Zeilenrang und Spaltenrang von A und Bemerkung 3.2.13 die Abschätzung:

$$\operatorname{rg}(A) \le \min(n, m).$$

□

Der Rang eines Matrizenproduktes läßt sich folgendermaßen Abschätzen:

Lemma 3.2.20. *Sei K ein Körper, und seien A und B keine Nullmatrizen und ihr Produkt AB existiere. Dann gilt:*

$$\operatorname{rg}(AB) \le \min\big(\operatorname{rg}(A), \operatorname{rg}(B)\big).$$

Beweis.

$\mathrm{rg}(AB) \leq \mathrm{rg}(B)$: Seien $z_1, \ldots, z_m$ die Zeilen von B und $w_1, \ldots, w_m$ die Zeilen von AB. Nach Lemma 3.1.6 sind die Zeilen von AB eine Linearkombination der Zeilen von B, und es folgt sofort:

$$\begin{aligned} \langle\, w_1, \ldots, w_m \,\rangle \subseteq \langle\, z_1, \ldots, z_m \,\rangle &\implies \dim_K \big(\langle\, w_1, \ldots, w_m \,\rangle\big) \leq \dim_K \big(\langle\, z_1, \ldots, z_m \,\rangle\big) \\ &\implies \mathrm{rg}_{\text{Zeile}}(AB) \leq \mathrm{rg}_{\text{Zeile}}(B) \\ &\implies \mathrm{rg}(AB) \leq \mathrm{rg}(B). \end{aligned}$$

$\mathrm{rg}(AB) \leq \mathrm{rg}(A)$: Seien $s_1, \ldots, s_n$ die Spalten von A und $v_1, \ldots, v_n$ die Spalten von AB. Nach Lemma 3.1.6 sind die Spalten von AB eine Linearkombination der Spalten von A, und es folgt sofort:

$$\begin{aligned} \langle\, v_1, \ldots, v_n \,\rangle \subseteq \langle\, s_1, \ldots, s_n \,\rangle &\implies \dim_K \big(\langle\, v_1, \ldots, v_n \,\rangle\big) \leq \dim_K \big(\langle\, s_1, \ldots, s_n \,\rangle\big) \\ &\implies \mathrm{rg}_{\text{Spalte}}(AB) \leq \mathrm{rg}_{\text{Spalte}}(A) \\ &\implies \mathrm{rg}(AB) \leq \mathrm{rg}(A). \end{aligned}$$

Beide Abschätzungen zusammengenommen liefern die Behauptung. □

Wird eine Matrix von links oder rechts mit einer invertierbaren Matrix multipliziert, so wird aus obiger Abschätzung eine Gleichung:

Satz 3.2.21. *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$ keine Nullmatrix. Weiter seien $B \in \mathrm{GL}_m(K)$ und $C \in GL_n(K)$. Dann gilt:*

$$\mathrm{rg}(A) = \mathrm{rg}(BA) = \mathrm{rg}(AC).$$

Insbesondere gilt dann für A und die aus dem Gauß-Algorithmus 3.2.9 entwickelte spezielle Zeilen-Stufen-Form GA, da G eine invertierbare Matrix ist:

$$\mathrm{rg}(A) = \mathrm{rg}(GA) \quad \leftarrow \quad \textit{Rang der speziellen Zeilen-Stufen-Form von } A.$$

Beweis.
Nach Lemma 3.2.15 gilt:

$$\mathrm{rg}_{\text{Zeile}}(BA) = \mathrm{rg}_{\text{Zeile}}(A) \quad \text{und} \quad \mathrm{rg}_{\text{Spalte}}(AC) = \mathrm{rg}_{\text{Spalte}}(A).$$

Da Zeilenrang gleich Spaltenrang gleich Rang einer Matrix ist, folgt die Behauptung sofort. □

Somit ist der Gauß-Algorithmus ein Verfahren, mit dem der Rang einer Matrix bestimmt werden kann. Der Rang einer quadratischen Matrix A wiederum ist ein Kriterium für die Invertierbarkeit von A, wie folgender Satz zeigt:

Satz 3.2.22. *Sei K ein Körper und $A \in \mathrm{Mat}(n \times n, K)$ eine quadratische $(n \times n)$-Matrix. Dann sind folgende Aussagen äquivalent:*

i.) $\mathrm{rg}(A) = n$.
ii.) *A ist invertierbar.*
iii.) *Es gibt ein $B \in \mathrm{Mat}(n \times n, K)$ mit $BA = E_n$.*
iv.) *Es gibt ein $C \in \mathrm{Mat}(n \times n, K)$ mit $AC = E_n$.*

Insbesondere folgt aus den obigen Äquivalenzen:

- *Existiert ein $B \in \mathrm{Mat}(n \times n, K)$ mit $BA = E_n$, so gilt auch $AB = E_n$, A ist invertierbar und $B = A^{-1}$.*

- *Existiert ein $C \in \mathrm{Mat}(n \times n, K)$ mit $AC = E_n$, so gilt auch $CA = E_n$, A ist invertierbar und $C = A^{-1}$.*
- *Liefert der Gauß-Algorithmus 3.2.9 eine spezielle Zeilen-Stufen-Form $GA = E_n$, so ist A invertierbar und $G = A^{-1}$.*

Beweis.

i.) $\Longrightarrow$ *ii.)*: Ist $\mathrm{rg}(A) = n$, so sind alle Spalten von A linear unabhängig, denn es gilt Rang = Spaltenrang. Wird die von A induzierte Abbildung $\varphi_A \in \mathrm{End}_K(K^{[n]})$ betrachtet, so sind die Spalten von A genau die Bilder $\varphi_A(e_1), \ldots, \varphi_A(e_n)$ der Standard-Basisvektoren $e_1, \ldots, e_n$ des $K^{[n]}$ (Satz 3.1.14).
Nach dem Hauptsatz über lineare Abbildungen und Basen 2.2.31 ist dann φ_A eine injektive Abbildung (Bilder einer Basis linear unabhängig!), und nach Lemma 2.2.60 der injektive Endomorphismus φ_A sogar bijektiv. Aus φ_A bijektiv folgt mit Satz 3.1.20 schließlich A invertierbar.

ii.) $\Longrightarrow$ *i.)*: Ist A invertierbar, so existiert eine Inverse A^{-1} mit $AA^{-1} = E_n$. Da A^{-1} natürlich auch invertierbar ist, liefert Satz 3.2.21:

$$\mathrm{rg}(A) = \mathrm{rg}(AA^{-1}) = \mathrm{rg}(E_n) = n.$$

ii.) $\Longleftrightarrow$ *iii.)*: Offensichtlich folgt mit $B := A^{-1}$ Aussage *iii.)* aus Aussage *ii.)*, so daß nur die Umkehrung gezeigt werden muß. Lemma 3.2.20 liefert dann:

$$n = \mathrm{rg}(E_n) = \mathrm{rg}(BA) \leq \mathrm{rg}(A) \leq n,$$

so daß $\mathrm{rg}(A) = n$ folgt und damit A invertierbar, wie vorher schon bewiesen.

ii.) $\Longleftrightarrow$ *iv.)*: Offensichtlich folgt mit $C := A^{-1}$ Aussage *iv.)* aus Aussage *ii.)*, so daß nur die Umkehrung gezeigt werden muß. Lemma 3.2.20 liefert dann:

$$n = \mathrm{rg}(E_n) = \mathrm{rg}(AC) \leq \mathrm{rg}(A) \leq n,$$

so daß $\mathrm{rg}(A) = n$ folgt und damit A invertierbar, wie vorher schon bewiesen.

Nach den obigen Äquivalenzen liefern die Gleichungen $BA = E_n$ und $AC = E_n$ jeweils, daß A invertierbar ist, und es folgt durch geeignete Multiplikation mit A^{-1}:

$$BA = E_n \quad \Longrightarrow \quad B = BAA^{-1} = E_nA^{-1} = A^{-1}$$

und analog $C = A^{-1}$. Die Aussage über den Gauß-Algorithmus ist dann klar. □

Bemerkung 3.2.23.

i.) Ist K ein Körper und $A \in \mathrm{Mat}(n \times n, K)$ eine quadratische Matrix, so liefert obiger Satz 3.2.23 sofort:

$$\mathrm{rg}(A) = n \quad \Longleftrightarrow \quad \varphi_A \text{ bijektiv},$$

denn nach Satz 3.1.20 ist φ_A genau dann bijektiv, wenn A invertierbar ist.

ii.) Wird mit dem Gauß-Algorithmus 3.2.9 der Rang einer quadratischen Matrix bestimmt, um sie auf Invertierbarkeit zu testen, kann die (mögliche) Inverse parallel zur Rangberechnung bestimmt werden: Denn wird eine Matrix A in spezielle Zeilen-Stufen-Form gebracht, um ihren Rang abzulesen, können die Zeilenoperationen gleich auf das erweiterte System $(A|E_n)$ angewendet werden. Ist dann die spezielle Zeilen-Stufen-Form GA die Einheitsmatrix E_n, so ist G schon

die Inverse zu A, und G wird bei der Anwendung der Zeilenoperationen auf E_n konstruiert:

$$(A|E_n) \quad \xrightarrow{\textit{Gauß-Algorithmus}} \quad (GA|GE_n) = (E_n|G) = (E_n|A^{-1}).$$

Siehe dazu auch die Bemerkung 3.2.10 und Beispiel 3.2.11. □

Lineare Gleichungssysteme und LR-Zerlegung.

Die bisherigen Konstruktionen können genutzt werden, um die Lösungen eines linearen Gleichungssystems über einem Körper zu beschreiben: Sei dazu über dem Körper K ein lineares Gleichungssystem

$$\begin{array}{ccccc} a_{1,1}z_1 & +\ldots+ & a_{1,n}z_n & = & b_1, \\ a_{2,1}z_1 & +\ldots+ & a_{2,n}z_n & = & b_2, \\ & \vdots & & \vdots & \\ a_{m,1}z_1 & +\ldots+ & a_{m,n}z_n & = & b_m \end{array}$$

mit $a_{i,j} \in K$, $(i,j) \in I_{m,n}$ gegeben. Dies läßt sich als Matrizengleichung schreiben:

$$Az = b,$$

wobei A, z und b definiert sind als Matrizen (bzw. Spaltenvektoren):

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix} \in \mathrm{Mat}(m \times n, K),\ z := \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \in K^{[n]},\ b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^{[m]}.$$

Die Lösungsmenge des linearen Gleichungssystems hat dann die Form:

$$\{\,\text{Lösung des LGS}\,\} \quad = \quad \{\, z \in K^{[n]} \mid Az = b \,\}.$$

Die Anwendung des Gauß-Algorithmus auf das lineare Gleichungssystem $Az = b$ bedeutet dabei die Multiplikation der Gleichung mit einer speziellen invertierbaren Matrix G (so daß GA spezielle Zeilen-Stufen-Form hat), d.h. es ergibt sich ein neues Gleichungssystem der Form:

$$Az = b \quad \rightsquigarrow \quad (GA)z = (Gb).$$

Daß sich dabei die Lösungsmenge nicht ändert, zeigt folgende Aussage:

Lemma 3.2.24. *Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{Mat}(m \times n, R)$. Weiter sei $b \in R^{[m]}$ und das lineare Gleichungssystem $Az = b$ gegeben. Dann gilt für jedes $C \in \mathrm{GL}_n(R)$, daß die linearen Gleichungssysteme*

$$Az = b \qquad \textit{und} \qquad (CA)z = (Cb)$$

die gleichen Lösungsmengen haben, d.h. es gilt:

$$\{\, z \in R^{[n]} \mid Az = b \,\} \quad = \quad \{\, z \in R^{[n]} \mid (CA)z = (Cb) \,\}.$$

Beweis.
Es wird die Gleichheit der Lösungsmengen gezeigt, daß eine Lösung z eines linearen Gleichungssystems auch Lösung des anderen linearen Gleichungssystems ist:

„$\subseteq$ “: Durch Linksmultiplikation mit C ergibt sich sofort:

$$Az = b \quad \Longrightarrow \quad (CA)z = (Cb).$$

„$\supseteq$ “: Da C invertierbar ist, existiert C^{-1}, und es gilt:

$$(CA)z = (Cb) \quad \Longrightarrow \quad (C^{-1}C)Az = (C^{-1}C)b \quad \Longrightarrow \quad Az = b. \qquad \square$$

Damit können anstelle der Lösungen eines linearen Gleichungssystems $Az = b$ die Lösungen des Gleichungssystems $(GA)z = Gb$ berechnet werden, wobei G diejenige Matrix ist, die A in eine spezielle Zeilen-Stufen-Form transformiert. Aus der einfachen Form der speziellen Zeilen-Stufen-Form GA können Lösungen von $(GA)z = Gb$ und damit $Az = b$ sofort mit Hilfe von Lemma 3.1.6 abgelesen werden, wie folgender Satz zeigt:

Satz 3.2.25. *Sei K ein Körper und $Az = b$ ein lineares Gleichungssystem über K mit $A \in \mathrm{Mat}(m \times n, K)$ in spezieller Zeilen-Stufen-Form:*

$$A = \begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccccc} & & j_1 & & & j_2 & & & j_k & \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & * & * & 0 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ & & & & & & & & & \\ & & & & & & & 0 & 1 & * \\ & & & & & & & 0 & 0 & 0 \end{pmatrix} \end{array} = \begin{pmatrix} | & & | \\ s_1 & \cdots & s_n \\ | & & | \end{pmatrix}.$$

(Die Matrix A hat den Rang k und an den Spalten $j_1, \ldots, j_k$ Stufenecken.)
Für die Spalten s_i von A gilt dabei:

$$i = j_r \quad \Longrightarrow \quad s_i = e_r \qquad \text{und} \qquad i < j_r \quad \Longrightarrow \quad s_i \text{ hat Nullen ab der } r\text{-ten Zeile.}$$

Ist b ein Vektor, zu dem es eine Lösung des linearen Gleichungssystems gibt, so ist $b = \sum_{i=1}^{k} b_i e_i$ mit $b_i \in K$, und folgender Vektor ist dann eine spezielle Lösung des linearen Gleichungssystems:

$$v_{sp} := \sum_{i=1}^{k} b_i e_{j_i} \in K^{[n]}.$$

Die gesamte Lösungsmenge des linearen Gleichungssystems $Az = b$ ergibt sich aus der speziellen Lösung v_{sp} und dem Kern der linearen Abbildung $\varphi_A \colon K^{[n]} \longrightarrow K^{[m]}$ mit $\varphi_A(z) = Az$ (2.1.35, 3.1.14), d.h. es gilt

$$\{\, \text{Lösung von } Az = b \,\} \quad = \quad v_{sp} + \ker(\varphi_A).$$

Der Kern von φ_A ist dabei ein Untervektorraum der Dimension $n-k$, was der Anzahl der Spalten von A entspricht, die keinen der Indizes $j_1, \ldots, j_k$ besitzt, und aus den Spalten s_i von A mit $i \notin \{j_1, \ldots, j_k\}$ kann eine Basis von $\ker(\varphi_A)$ konstruiert werden durch folgende Vorschrift:

$$i < j_1 : \quad s_i \rightsquigarrow w_i := -e_i,$$

$i > j_1$: *Sei r der maximale Index mit $j_r < i$. Dann liegt s_i in der r-ten Stufe von A und hat die Darstellung*

$$s_i = \sum_{t=1}^{r} a_{t,i} \cdot e_t = \sum_{t=1}^{r} a_{t,i} \cdot s_{j_t}$$

mit $a_{t,i}$ aus der Matrix $(a_{i,j}) := A$. Es sei definiert:

$$s_i \rightsquigarrow w_i := \Big(\sum_{t=1}^{r} a_{t,i} \cdot e_{j_t} \Big) - e_i.$$

Die $n-k$ konstruierten Vektoren $w_1, \ldots, w_n$ (die k Indizes $j_1, \ldots, j_k$ treten nicht auf) seien nun als $v_1, \ldots, v_{n-k}$ bezeichnet. Dann ist $(v_1, \ldots, v_{n-k})$ eine Basis von $\ker(\varphi_A)$, und es folgt für die Lösung des linearen Gleichundgssystems $Az = b$:

$$\{\, \text{Lösung von } Az = b \,\} \quad = \quad \{\, z \in K^{[n]} \mid Az = b \,\} \quad = \quad v_{sp} + \langle v_1, \ldots, v_{n-k} \rangle.$$

Ist für ein lineares Gleichungssystem $Az = b$ die Matrix A nicht in spezieller Zeilen-Stufen-Form gegeben, kann daß System $(A|b)$ mit dem Gauß-Algorithmus in eine Form $(GA|Gb)$ gebracht werden, in der die Matrix GA spezielle Zeilen-Stufen-Form hat (Satz 3.2.9, Bemerkung 3.2.10), und das oben beschriebene Lösungsverfahren auf das „passende“ lineare Gleichungssystem $(GA)z = (Gb)$ angewendet werden, denn es gilt nach Lemma 3.2.24:

$$\{\, \text{Lösungsmenge } Az = b \,\} \quad = \quad \{\, \text{Lösungsmenge } (GA)z = (Gb) \,\}.$$

Da die Lösungsmengen Nebenklassen der Kerne der entsprechenden linearen Abbildungen φ_A und φ_{GA} sind, folgt sofort auch die Gleichung $\ker(\varphi_A) = \ker(\varphi_{GA})$.

Beweis.

v_{sp} spezielle Lösung: Nach Lemma 3.1.6 ist Av_{sp} eine Linearkombination der Spalten s_i von A mit den Koeffizienten v_{sp_i} aus v_{sp}. Dieser enthält nach seiner Definition an der j_i-ten Komponente (mit $1 \le i \le k$) die i-te Komponente b_i von b und sonst nur Nullen. Damit und wegen $s_{j_i} = e_i$ gilt wie behauptet:

$$Av_{\text{sp}} = \sum_{i=1}^{n} v_{\text{sp}_i} \cdot s_i = \sum_{i=1}^{k} b_i \cdot s_{j_i} = \sum_{i=1}^{k} b_i \cdot e_i = b.$$

$\dim_K \big(\ker(\varphi_A) \big) = n - k$: Nach Bemerkung 3.2.19 gilt $\operatorname{rg}(\varphi_A) = \operatorname{rg}(A)$, und A hat den Rang k, da es k Zeilen-Stufen enthält. Mit dem Rangsatz 2.2.59 folgt dann

$$\dim_K \big(\ker(\varphi_A) \big) = \dim_K(K^{[n]}) - \operatorname{rg}(A) = n - k.$$

$v_1, \ldots, v_{n-k}$ Basis von $\ker(\varphi_A)$: Zurerst wird gezeigt, daß jedes v_j im Kern von φ_A liegt. Ein v_j ist dabei ein w_i mit $i \notin \{j_1, \ldots, j_k\}$ und einem zugeordneten Index r mit $j_r < i$ und $w_i = \big(\sum_{t=1}^{r} a_{t,i} \cdot e_{j_t} \big) - e_i$. Weiter gilt $Ae_l = s_l$, und es folgt:

$$Aw_i = A\big(\sum_{t=1}^{r} a_{t,i} \cdot e_{j_t} \big) - Ae_i = \big(\sum_{t=1}^{r} a_{t,i} \cdot Ae_{j_t} \big) - s_i = \big(\sum_{t=1}^{r} a_{t,i} \cdot s_{j_t} \big) - s_i = s_i - s_i = 0.$$

$v_1, \ldots, v_{n-k}$ sind linear unabhängig, da diese den Vektoren $w_1, \ldots, w_n$ entsprechen (mit den Indexlücken $j_1, \ldots, j_k$), und ein w_i enthält in der i-ten Komponente den Wert „-1“ und danach nur noch Nullen. Damit sind diese Vektoren offensichtlich linear unabhängig.

Dann ist $v_1, \ldots, v_{n-k}$ wegen $\dim_K \big(\ker(\varphi_A)\big) = n - k$ einmaximal linear unabhängiges System in $\ker(\varphi_A)$ und damit auch eine Basis. $\square$

Bemerkung 3.2.26.
Die obige Konstruktion beruht darauf, daß in der speziellen Zeilen-Stufen-Form in den Spalten $j_1, \ldots, j_k$ jeweils Einheitsvektoren stehen, und aus diesen Spalten gesuchte Vektoren leicht konstruiert werden können.
Linearkombinationen von Spalten einer Matrix können durch eine „Matrix mal Vektor"-Multiplikation beschrieben werden, wobei im Vektor die Koeffizienten der Linearkombination stehen (Lemma 3.1.6). Die konstruierten Vektoren v_{sp} und v_i bzw. w_i entstehen aus speziellen Linearkombinationen der Spalten von A.
So kann sofort der Lösungsvektor b des Gleichungssystems $Az = b$ aus den Einheitsvektorspalten in A zusammengesetzt werden, und diese Linearkombination liefert den speziellen Lösungsvektor v_{sp}.
Für die Basis des Kerns von φ_A müssen Lösungen des homogenen Systems $Az = 0$ gefunden werden, und dies geschieht, indem jeweils eine Spalte von A aus den Einheitsvektorspalten zusammengesetzt und sie selbst davon abgezogen wird (so werden die w_i konstruiert: s_i zusammensetzen aus den Einheitsvektorspalten, und dann abziehen). $\square$

Beispiel 3.2.27.

i.) Es sei folgendes reelle lineare Gleichungssystem $Az = b$ in Matrizenform gegeben, bei dem A schon in spezieller Zeilen-Stufen-Form vorliegt:

$$\underbrace{\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{ccccccc} & j_1 & & j_2 & & j_3 & \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 0 & 3 & 0 & 4 \\ 0 & 0 & 0 & 1 & 5 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}}_{=:A} \underbrace{\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_6 \\ z_7 \end{pmatrix}}_{=:z} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix}}_{=:b}.$$

Die Matrix A ist eine spezielle Zeilen-Stufen-Form mit drei Stufen und hat damit den Rang Drei (siehe Lemma 3.2.14), und wegen der letzten beiden Null-Zeilen in A müssen b_4 und b_5 Null sein, damit das System lösbar ist.
Der Vektor b (mit $b_4 = b_5 = 0$) kann dann als eine Linearkombination der Spalten $j_1 = 2$, $j_2 = 4$ und $j_3 = 6$ von A, welche die Standard-Basisvektoren e_1, e_2 und e_3 enthält, zusammengesetzt werden, und dies liefert sofort eine spezielle Lösung v_{sp} des linearen Gleichungssystems:

$$\left.\begin{aligned} b &= b_1 e_1 + b_2 e_2 + b_3 e_3 \\ &= \quad b_1 \cdot (\textit{Spalte } j_1) \\ &\quad + b_2 \cdot (\textit{Spalte } j_2) \\ &\quad + b_3 \cdot (\textit{Spalte } j_3) \end{aligned}\right\} = A \cdot \begin{array}{c} \\ j_1 \\ \\ j_2 \\ \\ j_3 \\ \end{array}\begin{pmatrix} 0 \\ b_1 \\ 0 \\ b_2 \\ 0 \\ b_3 \\ 0 \end{pmatrix} \quad \Longrightarrow \quad v_{sp} = \begin{array}{c} \\ j_1 \\ \\ j_2 \\ \\ j_3 \\ \end{array}\begin{pmatrix} 0 \\ b_1 \\ 0 \\ b_2 \\ 0 \\ b_3 \\ 0 \end{pmatrix}.$$

Nach dem Rangsatz 2.2.59 gilt im obigen Beispiel:

$$\dim_{\mathbb{R}}\big(\ker(\varphi_A)\big) = \dim_{\mathbb{R}}\mathbb{R}^{[7]} - \mathrm{rg}_{\mathbb{R}}(\varphi_A) \overset{(3.2.19)}{=} 7 - \mathrm{rg}(A) = 7 - 3 = 4.$$

Dies ist die Anzahl der Spalten von A, in denen keine neuen Stufen auftreten, d.h. die Spalten, die keinen der Indizes $j_1, \ldots, j_3$ besitzen. Es sind die Spalten s_1, s_3, s_5 und s_7, und aus jeder von ihnen wird ein Vektor w_i konstruiert, der ein Basisvektor von $\ker(\varphi_A)$ ist:

$i < j_1 = 2$: *s_1 ist eine Nullspalte, und so wird nach Satz 3.2.25 $w_1 := -e_1$ gesetzt.*

$i > j_1 = 2$: *Die Spalte s_3 liegt in der ersten Stufe von A und kann aus dem Spaltenvektor e_1 mit dem Index j_1 zusammengesetzt werden (dies liefert den Index $r = 1$ in obigem Satz).*

Die Spalte s_5 liegt in der zweiten Stufe von A und kann aus den Spaltenvektoren e_1 und e_2 mit den Spaltenindezes j_1 und j_2 zusammengesetzt werden (mit dem Index $r = 2$ in obigem Satz).

Die Spalte s_7 liegt in der dritten Stufe von A und kann aus den Spaltenvektoren e_1 bis e_3 mit den Spaltenindizes j_1 bis j_3 zusammengesetzt werden (mit dem Index $r = 3$ in obigem Satz).

Dabei geben die Einträge der Spalten s_3, s_5 und s_7 jeweils die Koeffizienten der Linearkombination an:

$$\begin{aligned} s_3 &= 2e_1 &&= 2s_2, \\ s_5 &= 3e_1 + 5e_2 &&= 3s_2 + 5s_4 \\ s_7 &= 4e_1 + 6e_2 + 7e_3 &&= 4s_2 + 6s_4 + 7s_6. \end{aligned}$$

Dies liefert folgende Linearkombinationen von Spalten von A, die den Null-Spaltenvektor ergeben, und damit die entsprechenden w_i:

$$\left.\begin{aligned} &2s_2 - s_3 = 0, \\ &3s_2 + 5s_4 - s_5 = 0, \\ &4s_2 + 6s_4 + 7s_6 - s_7 = 0. \end{aligned}\right\} \quad \Longrightarrow \quad w_3 := \begin{pmatrix} 0 \\ 2 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; w_5 := \begin{pmatrix} 0 \\ 3 \\ 0 \\ 5 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \; w_7 := \begin{pmatrix} 0 \\ 4 \\ 0 \\ 6 \\ 0 \\ 7 \\ -1 \end{pmatrix}.$$

Nach Umnumerierung ergeben sich dann die vier Basisvektoren $v_1, \ldots, v_4$ der Basis von $\ker(\varphi_A)$:

$$v_1 := w_1, \quad v_2 := w_3, \quad v_3 := w_5 \quad \textit{und} \quad v_4 := w_7.$$

Die Lösungsmenge des linearen Gleichungssystems $Az = b$ ist dann:

$$\{\, \textit{Lösungsmenge } Az = b \,\} \quad = \quad v_{sp} + \langle v_1, \ldots, v_4 \rangle.$$

ii.) *Es sei folgendes reelle lineare Gleichungssystem gegeben:*

$$Az = b \quad \textit{mit} \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \quad b = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}.$$

Die Matrix A liegt nicht in spezieller Zeilen-Stufen-Form vor, so daß das lineare Gleichungssystem noch durch eine Gauß-Matrix in geeignete Form transformiert werden muß (oder via Gauß-Algorithmus, da die Gauß-Matrix ja a priori nicht

bekannt ist). Da aber für die „Telephon-Matrix“ A die Gauß-Matrix G schon in Beispiel 3.2.11 berechnet wurde, die A in spezielle Zeilen-Stufen-Form bringt, kann hier auf den Gauß-Algorithmus verzichtet werden (Übung!), und es folgt:

$$G \overset{(3.2.11)}{=} \begin{pmatrix} -\frac{5}{3} & \frac{2}{3} & 0 \\ \frac{4}{3} & -\frac{1}{3} & 0 \\ 1 & -2 & 1 \end{pmatrix}, \qquad Az = b \quad \rightsquigarrow \quad (GA)z = (Gb)$$

Es ergibt sich ein neues lineares Gleichungssystem, welches jedoch die gleiche Lösungsmenge wie das ursprüngliche lineare Gleichungssystem hat (Lemma 3.2.24):

$$\underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}}_{GA} \cdot \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \underbrace{\begin{pmatrix} -2 \\ 2 \\ 0 \end{pmatrix}}_{Gb}.$$

Aus den ersten beiden Spalte von GA (nämlich $s_1 = e_1$ und $s_2 = e_2$ kann Gb zusammengesetzt werden, und es folgt sofort als spezielle Lösung:

$$v_{sp} = -2 \cdot e_1 + 2 \cdot e_2 = \begin{pmatrix} -2 \\ 2 \\ 0 \end{pmatrix}.$$

Die Matrix GA hat den Rang Zwei, so daß der Kern von φ_{GA} eindimensional ist, und zur Berechnung einer Basis des Kerns wird der dritte Spaltenvektor von GA benutzt, der als einziger keine Stufenecke bildet.
Der dritte Spaltenvektor ist eine Linearkombination der erste beiden Spalten, und es folgt für den Basisvektor w_3:

$$s_3 = -e_1 + 2 \cdot e_2 = -s_1 + 2 \cdot s_2 \quad \Longrightarrow \quad -s_1 + 2 \cdot s_2 - s_3 = 0 \quad \Longrightarrow \quad w_3 := \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}.$$

Nach der Umbenennung $v_1 := w_3$ folgt für die Lösungsmenge beider linearer Gleichungssysteme:

$$\{\, \textit{Lösungsmenge } Az = b \,\} \quad = \quad v_{sp} + \langle v_1 \rangle = \begin{pmatrix} -2 \\ 2 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix} \right\rangle. \qquad \square$$

In Satz 3.2.25 wurde nicht nur beschrieben, wie sich ein lineares Gleichungssystem $Az = b$ mit gegebener Matrix A und gegebenen Vektor b lösen läßt, sondern bei der Beschreibung der Lösung gleichzeitig das Problem gelöst, den Kern der linearen Abbildung $\varphi_A \colon K^{[n]} \longrightarrow K^{[m]}$ zu bestimmen. Dieser kann aus einer speziellen Zeilen-Stufen-Form von A abgelesen werden. Dies funktioniert auch für das Bild von φ_A, wie folgender Satz zeigt:

Satz 3.2.28. *Sei K ein Körper und $A \in \mathrm{Mat}(m \times n, K)$. Weiter sei $G \in \mathrm{GL}_n(K)$, so daß GA spezielle Zeilen-Stufen-Form hat (z.B. G aus dem Gauß-Algorithmus 3.2.9). Die Indizes der Stufen-Ecken-Spalten von GA seien $j_1, \ldots, j_k$. Dann ist das System der Spalten $j_1, \ldots, j_k$ von A eine Basis von $\mathrm{im}(\varphi_A)$.*

Beweis.
Die Matrix A und die Matrix GA haben den gleichen Rang, da G eine invertierbare Matrix ist (Satz 3.2.21), so daß $\dim_K \big(\operatorname{im}(\varphi_A)\big) = k$ folgt (Bemerkung 3.2.19).
Die Spalten von A sind ein Erzeugendensystem von $\operatorname{im}(\varphi_A)$ (Lemma 3.1.17) und liegen insbesondere in $\operatorname{im}(\varphi_A)$. Es reicht also zu zeigen, daß die Spalten $j_1, \ldots, j_k$ von A linear unabhängig sind, da sie dann als maximal linear unabhängiges System in $\operatorname{im}(\varphi_A)$ auch eine Basis dieses Raumes bilden.
Angenommen, es gäbe eine nicht-triviale Linearkombination der Spalten $j_1, \ldots, j_k$ von A zum Null-Vektor. Dann könnte daraus ein Nicht-Nullvektor z konstruiert werden mit $Az = 0$: der Vektor z besteht aus den Koeffizienten dieser Linearkombination an den entsprechenden Stellen und Nullen (Lemma 3.1.6). Dann würde sofort $GAz = G0 = 0$ folgen, und eine nicht-triviale Linearkombination der Spalten $j_1, \ldots, j_k$ von GA wäre Null. Dies stünde aber im Widerspruch dazu, daß in der speziellen Zeilen-Stufen-Form GA in diesen Spalten linear unabhängige Einheitsvektoren stehen. □

Wird beim Gauß-Algorithmus aus Satz 3.2.9 für eine Matrix A nur der erste Schritt angewandt, so ergibt sich eine „allgemeine“ Zeilen-Stufen-Form und noch nicht die spezielle Zeilen-Stufen-Form, die erst im zweiten Schritt aus der allgemeinen Zeilen-Stufen-Form konstruiert wird. Diese allgemeine Zeilen-Stufen-Form ist für viele Zwecke schon ausreichend, auch zum Lösen von linearen Gleichungssystemen: Jede Zeilen-Stufen-Form ermöglicht ein iteratives Auflösen des Gleichungssystems, und so wird meist in Büchern auch nur dieser Schritt beschrieben.
Aus dem ersten Schritt des Gauß-Algorithmus für eine Matrix A ergibt sich in speziellen Fällen eine schöne Beschreibung von A als Produkt von einer unteren Dreiecksmatrix L und einer oberen Dreicksmatrix R, die den ganzen Gauß-Algorithmus wiederspiegelt und LR-Zerlegung von A genannt wird. Dazu muß zuersteinmal jedoch definiert werden, was obere und untere Dreicksmatrizen überhaupt sind:

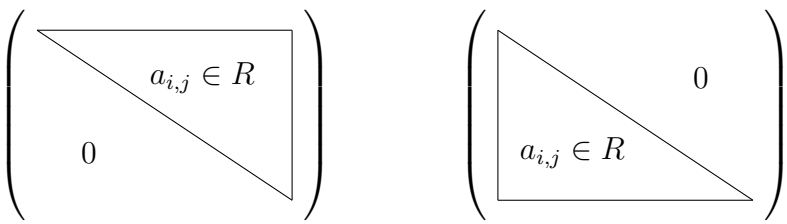
Definition 3.2.29. *Sei R ein kommutativer Ring mit Eins. Dann heißt eine Matrix $A := (a_{i,j}) \in \operatorname{Mat}_n(R)$ obere Dreiecksmatrix, falls unterhalb der Diagonalen alle ihre Koeffizienten Null sind, und eine untere Dreiecksmatrix, falls alle ihre Koeffizienten oberhalb der Diagonale Null sind:*

$$\begin{aligned} (a_{i,j}) \text{ obere Dreiecksmatrix} \quad &\Longleftrightarrow \quad i > j \implies a_{i,j} = 0, \\ (a_{i,j}) \text{ untere Dreiecksmatrix} \quad &\Longleftrightarrow \quad i < j \implies a_{i,j} = 0. \end{aligned}$$ □

Beispiel 3.2.30.

i.) Obere und untere Dreiecksmatrizen haben folgende Form:

obere Dreicksmatrix *untere Dreicksmatrix*



ii.) *Eine Diagonalmatrix ist sowohl eine untere als auch eine obere Dreiecksmatrix. Insbesondere zählen dazu die Matrizen $D_i(\alpha)$ aus Definition 3.2.3.*
Die Nullmatrix ist eine Diagonalmatrix und damit eine untere wie auch obere Dreiecksmatrix.

iii.) *Eine Matrix in Zeilen-Stufen-Form (Definiton 3.2.1) ist eine obere Dreiecksmatrix, insbesondere dann auch eine Matrix in spezieller Zeilen-Stufen-Form.*

iv.) *Die Matrizen $L_{i,j}(\lambda)$ aus Definition 3.2.3 sind für $i < j$ obere Dreiecksmatrizen und für $i > j$ untere Dreiecksmatrizen.* □

Es sei nun für einen Körper K eine Matrix $A \in \mathrm{Mat}(m \times n, K)$ gegeben. Wird der erste Schritt des Gauß-Algorithmus aus Satz 3.2.9 für A ausgeführt, ergibt sich folgende allgemeine Zeilen-Stufen-Form mit k Stufen:

$$\underbrace{B_k B_{k-1} \cdots B_1}_{=:B} A = \begin{array}{c} \\ 1 \\ 2 \\ \\ k \\ \\ \\ m \end{array} \begin{array}{c} \begin{array}{ccccccccccc} & & j_1 & & & j_2 & & & j_k & n \end{array} \\ \begin{pmatrix} 0 & 0 & a_1 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & a_2 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & & & & & \\ & & & & & & & 0 & a_k & * \\ & & & & & & & 0 & 0 & 0 \\ & & & & & & & 0 & 0 & 0 \end{pmatrix} \end{array} =: R.$$

Die Matrizen B_i liegen dabei in der Menge $\{L_{i,j}(\lambda), P_{i,j}\}$. Es sei nun vereinfachend angenommen, daß zur Durchführung des obigen Gauß-Algorithmus keine Zeilenvertauschungen nötig sind, d.h. daß keine Matrix $P_{i,j}$ unter den B_r vorkommt. Wenn dann die obere Dreiecksmatrix der rechten Seite (die Zeilen-Stufen-Form) mit R bezeichnet wird, schreibt sich obige Gleichung genauer als:

$$\begin{aligned} m > n: &\quad \underbrace{L_{m,n}(\lambda_{m,n})}_{n\text{-te Spalte bearbeiten}} \cdots \underbrace{L_{m,1}(\lambda_{m,1}) \cdots L_{2,1}(\lambda_{2,1})}_{1\text{-te Spalte bearbeiten}} A = R, \\ m = n: &\quad \underbrace{L_{n,n-1}(\lambda_{n,n-1})}_{(n-1)\text{-te Spalte bearbeiten}} \cdots \underbrace{L_{n,1}(\lambda_{n,1}) \cdots L_{2,1}(\lambda_{2,1})}_{1\text{-te Spalte bearbeiten}} A = R, \\ m < n: &\quad \underbrace{L_{m,m-1}(\lambda_{m,m-1})}_{(m-1)\text{-te Spalte bearbeiten}} \cdots \underbrace{L_{m,1}(\lambda_{m,1}) \cdots L_{2,1}(\lambda_{2,1})}_{1\text{-te Spalte bearbeiten}} A = R. \end{aligned} \tag{3.2.31}$$

Dabei ist zu bemerken, daß nur Matrizen $L_{i,j}(\lambda)$ auftreten mit $i > j$, also untere Dreiecksmatrizen.
Die Matrizen $L_{i,j}(\lambda)$ sind alle invertierbar, und es gilt nach Satz 3.2.6:

$$L_{i,j}^{-1}(\lambda) = L_{i,j}(-\lambda),$$

so daß für ein Produkt von Matrizen $L_{i,j}(\lambda)$ sofort folgt:

$$\big(L_{i_n,j_n}(\lambda_n) \cdots L_{i_1,j_1}(\lambda_1)\big)^{-1} = L_{i_1,j_1}(-\lambda_1) \cdots L_{i_n,j_n}(-\lambda_n).$$

Dies angewandt auf die Gleichungen (3.2.31) liefert dann Gleichungen:

$$\begin{aligned} m > n: &\quad A = \underbrace{L_{2,1}(-\lambda_{2,1}) \cdots L_{m,1}(-\lambda_{m,1}) \cdots L_{m,n}(-\lambda_{m,n})}_{L:=} R, \\ m = n: &\quad A = \underbrace{L_{2,1}(-\lambda_{2,1}) \cdots L_{n,1}(-\lambda_{n,1}) \cdots L_{n,n-1}(-\lambda_{n,n-1})}_{L:=} R, \end{aligned} \tag{3.2.32}$$

$$m < n: \quad A = \underbrace{L_{2,1}(-\lambda_{2,1}) \cdots L_{m,1}(-\lambda_{m,1}) \cdots L_{m,m-1}(-\lambda_{m,m-1})}_{L:=} R.$$

Die Matrizen $L_{i,j}(-\lambda)$ in den Gleichungen erfüllen alle die Bedingung $i > j$ und sind damit untere Dreiecksmatrizen (mit Einsen auf der Diagonale), und diese Eigenschaft gilt auch für deren Produkt L:

Lemma 3.2.33. *Sei R ein kommutativer Ring mit Eins, und es seien $L_{i_k,j_k}(\lambda_k)$ für $1 \leq k \leq n$ Gauß-Matrizen aus Definition 3.2.3, die jeweils $i_k > j_k$ erfüllen. Dann ist deren Produkt:*

$$L := L_{i_n,j_n}(\lambda_n) \cdots L_{i_1,j_1}(\lambda_1)$$

eine untere Dreiecksmatrix, die nur Einsen auf der Diagonalen hat.

Beweis.
Der Beweis wird durch Induktion über die Anzahl n der Matrizen $L_{i_k,j_k}(\lambda_k)$ geführt.

Induktionsanfang $n = 1$: Dies gilt wegen $i_1 > j_1$ und der Definition von $L_{i_1,j_1}(\lambda_1)$.
Induktionsschritt $n \rightsquigarrow n+1$: Es sei nun das Produkt:

$$L_{i_{n+1},j_{n+1}}(\lambda_{i_{n+1},j_{n+1}}) \cdot \underbrace{L_{i_n,j_n}(\lambda_n) \cdots L_{i_1,j_1}(\lambda_1)}_{L:=} = L_{i_{n+1},j_{n+1}}(\lambda_{i_{n+1},j_{n+1}}) \cdot L$$

betrachtet. L ist dabei nach der Induktionsannahme eine untere Dreiecksmatrix mit Einsen auf der Diagonalen. Das Produkt $L_{i_{n+1},j_{n+1}}(\lambda_{n+1}) \cdot L$ erfüllt dann wegen $i_{n+1} > j_{n+1}$ ebenfalls diese Bedingung, da durch die Multiplikation mit $L_{i_{n+1},j_{n+1}}(\lambda_{n+1})$ in L ein Vielfaches seiner (j_{n+1})-ten Zeile zur (i_{n+1})-ten Zeile addiert wird, also eine „obere“ zu einer „unteren“ Zeile, welches die spezielle Form einer unteren Dreiecksmatrix nicht zerstört und auch die Diagonale nicht verändert. □

Damit ist in den Gleichungen 3.2.32 A jeweils das Produkt von einer unteren Dreiecksmatrix L (sogar mit Einsen auf der Diagonalen) und einer Zeilen-Stufen-Form R, die im Falle $n = m$ eine obere Dreiecksmatrix ist.

Definition 3.2.34. *Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{Mat}_n(R)$. Wenn es eine untere Dreiecksmatrix L und eine obere Dreiecksmatrix R gibt mit $A = LR$, so wird dies als LR-Zerlegung von A bezeichnet.* □

Aus den Gleichungen 3.2.32 folgt sofort:

Lemma 3.2.35. *Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Wenn der Gauß-Algorithmus aus Satz 3.2.9 ohne Permutationsmatrizen $P_{i,j}$ die Matrix A in eine Zeilen-Stufen-Form R transformiert (aus dem ersten Schritt, keine spezielle Zeilen-Stufen-Form), so besitzt A eine LR-Zerlegung.*
Die Zeilen-Stufen-Form R als obere Dreiecksmatrix und die in der Gleichung 3.2.32 aus den Gauß-Schritten hergeleitet Matrix

$$L := L_{2,1}(-\lambda_{2,1}) \cdots L_{n,1}(-\lambda_{n,1}) \cdots L_{n,n-1}(-\lambda_{n,n-1}),$$

als untere Dreieckmatrix liefern dabei eine LR-Zerlegung von A (wie in 3.2.32 gezeigt). □

Der Gauß-Algorithmus für eine Matrix A liefert (falls ohne Zeilenpermutationen auskommend), sofort die Matrix R einer LR-Zerlegung von A. Die Matrix L aus Lemma 3.2.35, die aus den Zeilen-Eleminationsschritten des Gauß-Algorithmus zusammengesetzt wird, braucht auch nicht berechnet zu werden, denn das Produkt der auftretenden Matrizen $L_{i,j}(\lambda)$ ist wegen der speziellen Reihenfolge der Faktoren sofort bekannt, ohne daß eine Rechnung ausgeführt werden muß. Dazu ist folgende Aussage wesentlich:

LEMMA 3.2.36. *Sei R ein kommutativer Ring mit Eins. Wenn für $1 \leq k \leq t$ die Matrizen $L_{i_k,j_k}(\lambda_{i_k,j_k}) \in \mathrm{Mat}_n(R)$ folgende Bedingungen erfüllen:*

- $i_k > j_k$ *für alle* $1 \leq k \leq t$,
- $j_{k+1} \geq j_k$ *für* $1 \leq k < t$,

dann gilt für deren Produkt:

$$\prod_{k=1}^{t} L_{i_k,j_k}(\lambda_{i_k,j_k}) = E_n + \sum_{k=1}^{t}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k}).$$

BEWEIS.
Der Beweis wird per Induktion über die Anzahl t der Faktoren $L_{i,j}(\lambda)$ geführt.

Induktionsanfang $t = 1$: Dies gilt wegen der Definition 3.2.3 der Matrizen $L_{i,j}(\lambda)$:

$$L_{i_1,j_1}(\lambda_{i_1,j_1}) := E_n + \lambda_{i_1,j_1} \cdot E_{i_1,j_1}.$$

Induktionsschritt $t \rightsquigarrow t+1$: Es folgt mit der Definition der $L_{i,j}(\lambda)$ und Satz 3.1.8 über das Produkt der Elementarmatrizen $E_{i,j}$ wegen der speziellen Bedingungen an die Indizes (i_k, j_k):

$$\begin{aligned}
\prod_{k=1}^{t+1} L_{i_k,j_k}(\lambda_{i_k,j_k}) &= \Big(\prod_{k=1}^{t} L_{i_k,j_k}(\lambda_{i_k,j_k})\Big) \cdot L_{i_{t+1},j_{t+1}}(\lambda_{i_{t+1},j_{t+1}}) \\
&\overset{\text{(IAnn)}}{=} \Big(E_n + \sum_{k=1}^{t}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k})\Big) \cdot L_{i_{t+1},j_{t+1}}(\lambda_{i_{t+1},j_{t+1}}) \\
&= \Big(E_n + \sum_{k=1}^{t}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k})\Big) \cdot (E_n + \lambda_{i_{t+1},j_{t+1}} \cdot E_{i_{t+1},j_{t+1}}) \\
&= E_n + \Big(\sum_{k=1}^{t}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k})\Big) + (\lambda_{i_{t+1},j_{t+1}} \cdot E_{i_{t+1},j_{t+1}}) + \ldots \\
&\qquad \ldots + \Big(\sum_{k=1}^{t}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k})\Big) \cdot (\lambda_{i_{t+1},j_{t+1}} \cdot E_{i_{t+1},j_{t+1}}) \\
&= E_n + \sum_{k=1}^{t+1}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k}) + \underbrace{\sum_{k=1}^{t}(\delta_k \cdot E_{i_k,j_k} \cdot E_{i_{t+1},j_{t+1}})}_{\text{mit } \delta_k := \lambda_{i_k,j_k}\lambda i_{t+1},j_{t+1}} \\
&\overset{(*)}{=} E_n + \sum_{k=1}^{t+1}(\lambda_{i_k,j_k} \cdot E_{i_k,j_k}).
\end{aligned}$$

Dabei fällt im letzten Schritt $(*)$ die gesamte rechte Summe weg, da jeder Summand darin Null ist: Das Produkt $E_{i_k,j_k} \cdot E_{i_{t+1},j_{t+1}}$ ist nach Satz 3.1.8 genau dann ungleich der Nullmatrix, wenn $j_k = i_{t+1}$ gilt. Aber nach den Voraussetzungen an die Indizes gilt:

$$i_{t+1} > j_{t+1} \geq j_k \quad \text{für alle} \quad k \leq t \quad \Longrightarrow \quad i_{t+1} > j_k \quad \Longrightarrow \quad i_{t+1} \neq j_k. \qquad \square$$

Bemerkung 3.2.37. *Lemma 3.2.36 besagt anschaulich, daß sich bei einer „passenden“ Reihenfolge der Faktoren $L_{i_k,j_k}(\lambda_{i_k,j_k})$ die λ_{i_k,j_k} nur an die Stelle (i_k, j_k) bei der Einheitsmatrix eingetragen werden:*

$$L_{2,1}(a)L_{3,1}(b)L_{3,2}(c) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}.$$

Bei diesem Produkt darf die Reihenfolge der Matrizen $L_{2,1}(a)$ und $L_{3,1}(b)$ vertauscht werden, ohne daß die Indexbedingungen aus Lemma 3.2.36 verletzt werden, und es gilt ebenso:

$$L_{3,1}(b)L_{2,1}(a)L_{3,2}(c) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}.$$

Eine Änderung der Reihenfolge, bei der die Index-Forderungen aus Lemma 3.2.36 nicht mehr erfüllt sind, bringt jedoch den regelmäßigen Aufbau des Produktes durcheinander:

$$L_{3,1}(b)L_{3,2}(c)L_{2,1}(a) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ ac+b & c & 1 \end{pmatrix}. \qquad \square$$

Nun kann Lemma 3.2.36 auf die Matrix L aus Lemma 3.2.35 angewendet werden, und es ergibt sich sofort zusammenfassend:

Satz 3.2.38. *Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Die Matrix A sei mit dem Gauß-Algorithmus aus Satz 3.2.9 ohne Permutationsmatrizen $P_{i,j}$ in eine Zeilen-Stufen-Form R (obere Dreicksmatrix) überführbar (nur Schritt Eins in 3.2.9, nicht die spezielle Zeilen-Stufen-Form). Die für die Transformation nötigen Matrizen seien die $L_{i,j}(\lambda_{i,j})$ wie in der Gleichung 3.2.31, und L sei die in Gleichung 3.2.32 bzw. Lemma 3.2.35 aufgestellte Matrix.*
Dann ist $A = LR$ eine LR-Zerlegung von A, und es gilt:

$$L := L_{2,1}(-\lambda_{2,1}) \cdots L_{n,n-1}(-\lambda_{n,n-1}) = \begin{pmatrix} 1 & & & & & \\ -\lambda_{2,1} & 1 & & & & \\ -\lambda_{3,1} & -\lambda_{3,2} & 1 & & & \\ \vdots & & & \ddots & & \\ -\lambda_{n-1,1} & & & & 1 & \\ -\lambda_{n,1} & & \dots & & -\lambda_{n,n-1} & 1 \end{pmatrix}.$$

(Im Gauß-Algorithmus wird mit $\lambda_{i,j}$ gearbeitet, d.h. $L_{i,j}(\lambda_{i,j})$ angewendet, und in L dann $-\lambda_{i,j}$ an der Stelle (i,j) notiert!)

Beweis. Lemma 3.2.35 und Lemma 3.2.36. $\square$

Beispiel 3.2.39. *In Beispiel 3.2.11 wurde die Telephonmatrix mit dem Gauß-Algorithmus in eine obere Zeilen-Stufen-Form und damit obere Dreiecksform R gebracht durch folgende Schritte:*

$$\underbrace{\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}}_{A:=}\xrightarrow{L_{2,1}(-4)}\begin{pmatrix}1&2&3\\0&-3&-6\\7&8&9\end{pmatrix}\xrightarrow{L_{3,1}(-7)}\begin{pmatrix}1&2&3\\0&-3&-6\\0&-6&-12\end{pmatrix}\xrightarrow{L_{3,2}(-2)}\underbrace{\begin{pmatrix}1&2&3\\0&-3&-6\\0&0&0\end{pmatrix}}_{R:=}.$$

Die Matrix L für die LR-Zerlegung $A = LR$ kann nun nach Satz 3.2.38 sofort zusammengesetzt werden aus den drei Operationen $L_{2,1}(-4)$, $L_{3,1}(-7)$ und $L_{3,2}(-2)$, in dem der ***negative*** *Faktor des jeweiligen Gauß-Schrittes an entsprechender Stelle in eine Einheitsmatrix eingetragen wird (siehe auch 3.2.32), und es folgt:*

$$L=\begin{pmatrix}1&0&0\\4&1&0\\7&2&1\end{pmatrix}\quad \textit{und}\quad \underbrace{\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}}_{A}=\underbrace{\begin{pmatrix}1&0&0\\4&1&0\\7&2&1\end{pmatrix}}_{L}\underbrace{\begin{pmatrix}1&2&3\\0&-3&-6\\0&0&0\end{pmatrix}}_{R}.\qquad\square$$

Es seien noch kurz einige Bemerkungen zur Eindeutigkeit der LR-Zerlegung gemacht:

Bemerkung 3.2.40.

i.) Eine Matrix $A \in \mathrm{Mat}_n(K)$ kann mehrere LR-Zerlegungen haben, und dabei können sowohl L als auch R mehrdeutig sein. Ist z.B. A die Nullmatrix, die eine obere sowie untere Dreiecksmatrix ist, so gilt für beliebige untere Dreiecksmatrizen L und obere Dreiecksmatrizen R:

$$A = L \cdot \textit{Nullmatrix} = \textit{Nullmatrix} \cdot R.$$

ii.) Ist $A \in \mathrm{GL}_n(K)$, also invertierbar, so folgt für eine LR-Zerlegung $A = LR$ von A, falls sie existiert, daß auch L und R invertierbar sind (Übung! Betrachte $\varphi_A, \varphi_R, \varphi_L$ und Lemma 2.2.60). Dann kann aus L und R eine LR-Zerlegung $A = \widetilde{L}\widetilde{R}$ generiert werden, so daß $\widetilde{L}$ nur Einsen auf der Diagonalen hat. Die Diagonalelemente $l_{i,i}$ einer invertierbaren unteren Dreiecksmatrix L müssen nämlich ungleich Null sein (Übung!), und die folgende Konstruktion liefert wegen $D_i(\alpha)^{-1} = D_i(\alpha^{-1})$ die gewünschten Matrizen $\widetilde{L}$ und $\widetilde{R}$:

$$A = LR = \underbrace{L \cdot D_n(l_{n,n}^{-1}) \cdots D_1(l_{1,1}^{-1})}_{\widetilde{L}:=}\underbrace{D_1(l_{1,1}) \cdots D_n(l_{n,n}) \cdot R}_{\widetilde{R}:=}.$$

Eine solche LR-Zerlegung von A, so daß L nur Einsen auf der Diagonalen hat, sei eine spezielle LR-Zerlegung von A genannt. Eine solche ist für invertierbar A eindeutig, wie im nächsten Punkt besprochen wird.

iii.) Ist $A \in \mathrm{GL}_n(K)$, also invertierbar, so ist eine spezielle LR-Zerlegung von A eindeutig, falls sie existiert. Der Beweis dazu ist eine Übungsaufgabe und kann in folgenden Schritten bewiesen werden:

- *Die Menge der unteren Dreiecksmatrizen mit Diagonalelementen Eins ist eine Untergruppe von $\mathrm{GL}_n(K)$ bzgl. der Matrizenmultiplikation.*
- *Die Menge der invertierbaren oberen Dreiecksmatrizen ist eine Untergruppe von $\mathrm{GL}_n(K)$ bzgl. der Matrizenmultiplikation.*
- *Aus A invertierbar und $A = LR$ folgt $L, R \in \mathrm{GL}_n(K)$, d.h. beide Matrizen sind auch invertierbar.*

Dann liefert der Ansatz zweier spezieller LR-Zerlegungen $A = LR = \widetilde{L}\widetilde{R}$ sofort, da L und $\widetilde{L}$ und damit $(\widetilde{L})^{-1}L$ nur Einsen auf der Diagonalen haben:

$$\begin{aligned} LR = \widetilde{L}\widetilde{R} \quad &\Longrightarrow \quad (\widetilde{L})^{-1}L = \widetilde{R}R^{-1} \quad \Longrightarrow \quad (\widetilde{L})^{-1}L = \widetilde{R}R^{-1} = E_n \\ &\Longrightarrow \quad L = \widetilde{L} \quad \text{und} \quad R = \widetilde{R}. \end{aligned}$$

□

Die Ergebnisse dieses Abschnittes über die Anwendungen des Gauß-Algorithmus seien in folgendem Satz noch einmal aufgelistet:

Satz 3.2.41. *Bei Matrizen über einem Körper kann der Gauß-Algorithmus für folgende Problemestellungen benutzt werden:*

Rangbestimmung einer Matrix: *Der Rang einer Matrix ist gleich dem Rang ihrer Zeilen-Stufen-Form bzw. speziellen Zeilen-Stufen-Form, die mit Hilfe des Gauß-Algorithmus bestimmt werden kann. Siehe Satz 3.2.21.*

Konstruktion der Inversen einer Matrix: *Ist für eine Matrix A die spezielle Zeilen-Stufen-Form GA (mit der Gauß-Matrix G) gleich der Einheitsmatrix, d.h. es gilt $GA = E_n$, so ist A invertierbar und $A^{-1} = G$. Siehe Satz 3.2.22.*

Lösung eines linearen Gleichungssystems: *Ein allgemeines lineares Gleichungssystem $Az = b$ kann mit dem Gauß-Algorithmus in die Form $(GA)z = Gb$ gebracht werden, wobei GA eine spezielle Zeilen-Stufen-Form ist. Beide lineare Gleichungssysteme haben die gleiche Lösungsmenge, und aus der speziellen Form $(GA)z = Gb$ kann die Lösungsmenge sofort abgelesen werden. Siehe Satz 3.2.25.*

Finden einer Basis von $\ker(\varphi_A)$ und $\operatorname{im}(\varphi_A)$ für eine Matrix A: *Wird die allgemeine Matrix A mit dem Gauß-Algorithmus in spezielle Zeilen-Stufen-Form GA gebracht, kann aus GA eine Basis des Kerns und des Bildes von φ_A abgelesen werden. Siehe Satz 3.2.25 (Kern von φ_A) und Satz 3.2.28 (Bild von φ_A).*

LR-Zerlegung einer Matrix: *Wenn im ersten Schritt des Gauß-Algorithmus für eine quadratische Matrix A keine Permutationsmatrizen $P_{i,j}$ benötigt werden, existiert eine LR-Zerlegung von A (Definition 3.2.34). Dabei kann R als die Zeilen-Stufen-From gewählt werden, die sich aus dem Gauß-Algorithmus ergibt, und als L diejenige Matrix, die das Produkt der im Algorithmus auftretenden $L_{i,j}(\lambda_{i,j})$ ist (in umgekehrter Reihenfolge und mit Vorzeichenwechsel bei $\lambda_{i,j}$: siehe 3.2.32).* □

3.3. Determinanten

Ist R ein kommutativer Ring mit Eins, so bilden die quadratischen $(n \times n)$-Matrizen $\mathrm{Mat}_n(R)$ über R mit der Matrizenmultiplikation einen Ring, der für $n \geq 2$ nicht kommutativ ist (Satz 3.1.9). Es sei dann folgende nützliche Abbildung betrachtet:

Definition 3.3.1. *Sei R ein kommutativer Ring mit Eins und $\mathrm{Mat}_n(R)$ der Matrizenring der quadratischen $(n \times n)$-Matrizen über R für ein $n \in \mathbb{N}$. Dann sei mit Hilfe der symmetrischen Gruppe S_n folgende Abbildung definiert:*

$$\det\colon \mathrm{Mat}_n(R) \longrightarrow R \quad \textit{mit} \quad (a_{i,j})_{(i,j)\in I_{n,n}} \mapsto \sum_{\sigma\in S_n} \Big(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \Big).$$

Für $A \in \mathrm{Mat}_n(R)$ heißt $\det(A)$ die Determinante von A.

Die Determinante einer Matrix kann auf verschiedene äquivalente Weisen eingeführt werden, und die hier als Definition verwendete Formel:

$$\det\big((a_{i,j})\big) = \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n} a_{i,\sigma(i)}\Big)$$

wird auch die Leibniz-Formel für die Determinante der Matrix $(a_{i,j}) \in \mathrm{Mat}_n(R)$ *genannt.*
Für eine Matrix $A := (a_{i,j}) \in Mat_n(R)$ *wird zur Vermeidung von Klammern auch notiert:*

$$\det\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n}\end{pmatrix} := \begin{vmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n}\end{vmatrix} := \det\left(\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n}\end{pmatrix}\right) = \det(A).$$

□

Bemerkung 3.3.2.

i.) *Die obige Determinantenfunktion* $\det\colon \mathrm{Mat}_n(R) \longrightarrow R$ *ist strenggenommen für jedes* $n \in \mathbb{N}$ *eine eigene Abbildung, da der Definitionsbereich ja von* n *abhängt. Trotzdem wird in der Abbildung dieser Index „n“ nicht vermerkt. Ein ähnliches Phänomen trat schon bei der Definition der Signum-Abbildung auf (siehe Lemma 1.2.45 ff.).*

ii.) *In der Leibniz-Formel für die Determinante einer Matrix* $(a_{i,j}) \in \mathrm{Mat}_n(R)$ *werden* $n!$ *Produkte der Form:*

$$\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n} a_{i,\sigma(i)} \quad = \quad \operatorname{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdot\ldots\cdot a_{n,\sigma(n)}$$

gebildet und dann summiert. Der Term $\operatorname{sign}(\sigma)$ *ist dabei in Abhängigkeit von* σ *entweder „1“ oder „−1“, wobei „±1“ in dem kommutativen Ring mit Eins* R *wohldefiniert ist: eben Eins oder dessen additives Inverses.*
Hier wird also auch stillschweigend der Wertebreich der Signum-Funktion „angepaßt“, denn er soll ja im jeweiligen Ring liegen. In der Definition der Signum-Funktion in Lemma 1.2.45 wurde salopp $\{\pm 1\}$ *angegeben, ohne genau zu spezifizieren,* welche *Eins überhaupt gemeint ist. Das Verhalten von* ± 1 *bzgl. der Multiplikation ist aber unabhängig vom Ring (siehe Lemma 1.3.6).*

iii.) *Die hier gewählte Definition einer Determinante ist die kompakteste Fassung, wenn das Signum einer Permutation aus* S_n *schon bekannt ist: dann läßt sich die Determinante einer Matrix durch einen Term beschreiben. Allerdings ist dieser nicht übersichtlich, so daß Eigenschaften der Determinantenabbildung aus dieser Definition erst hergeleitet werden müssen.*
Ein abstrakter, aber durchaus üblicher Weg, die Determinante einer Matrix einzuführen, ist deren Definition als spezielle multilineare alternierende Abbildung (mehr dazu später). Dabei liefert dieser Definitionsweg der Determinante schon viele ihrer Eigenschaften, aber die Einführung der Objekte und die letztendliche Definition sind dafür umfangreicher. □

Beispiel 3.3.3.

i.) *Für* $n = 2$ *ist* $S_2 = \{\mathrm{id}, (1\,2)\}$, *und es ergibt sich für* $\left(\begin{smallmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{smallmatrix}\right) \in \mathrm{Mat}_2(R)$*:*

$$\begin{aligned}
\det\begin{pmatrix} a_{1,2} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} &= \sum_{\sigma\in S_2}\Big(\mathrm{sign}(\sigma)\cdot\prod_{i=1}^{2} a_{i,\sigma(i)}\Big) = \sum_{\sigma\in S_2}\mathrm{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)} \\
&= \sum_{\sigma\in\{\mathrm{id},(1\,2)\}}\mathrm{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)} \\
&= \underbrace{1\cdot a_{1,1}\cdot a_{2,2}}_{\sigma=\mathrm{id}} + \underbrace{(-1)\cdot a_{1,2}\cdot a_{2,1}}_{\sigma=(1,2)} = a_{1,1}\cdot a_{2,2} - a_{1,2}\cdot a_{2,1}.
\end{aligned}$$

Dies wird ohne Indizes meist in folgender kurzen Formel ausgedrückt:

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Ein konkretes Beispiel wäre dann:

$$\det\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 0\cdot 0 - (-1)\cdot 1 = -(-1) = 1.$$

Siehe dazu auch Aufgabenblatt 6 aus LA I, Aufgabe 1.c).

ii.) *Für* $n = 3$ *ist* $S_3 = \{\mathrm{id},\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2)\}$, *es gilt*

$$\mathrm{sign}(\sigma) = \begin{cases} 1 & \textit{für } \sigma \in \{\mathrm{id},\ (1\,2\,3),\ (1\,3\,2)\}, \\ -1 & \textit{für } \sigma \in \{(1\,2),\ (1\,3),\ (2\,3)\}, \end{cases}$$

und es ergibt sich analog zum Fall $n = 2$*:*

$$\begin{aligned}
\det\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} &= \sum_{\sigma\in S_3}\mathrm{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdot a_{3,\sigma(3)} \\
&= \underbrace{a_{1,1}a_{2,2}a_{3,3}}_{\sigma=\mathrm{id}} + \underbrace{a_{1,2}a_{2,3}a_{3,1}}_{\sigma=(1\,2\,3)} + \underbrace{a_{1,3}a_{2,1}a_{3,2}}_{\sigma=(1\,3\,2)} \\
&\quad \underbrace{-a_{1,3}a_{2,2}a_{3,1}}_{\sigma=(1\,3)} + \underbrace{(-a_{1,1}a_{2,3}a_{3,2})}_{\sigma=(2\,3)} + \underbrace{(-a_{1,2}a_{2,1}a_{3,3})}_{\sigma=(1\,2)}.
\end{aligned}$$

Ein konkretes Beispiel wäre dann:

$$\begin{aligned}
\det\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} &= 1\cdot 5\cdot 9 + 2\cdot 6\cdot 7 + 3\cdot 4\cdot 8 - 3\cdot 5\cdot 7 - 1\cdot 6\cdot 8 - 2\cdot 4\cdot 9 \\
&= 45 + 84 + 96 - 105 - 48 - 72 = 225 - 225 = 0.
\end{aligned}$$

iii.) *Die Determinantenberechnung für* (2×2)*-Matrizen und* (3×3)*-Matrizen können folgendermaßen veranschaulicht werden, wenn entlang der Diagonalen (Pfeile) Produkte gebildet werden, und die Produkte der Hauptdiagonalen (durchgezogene Pfeile) addiert und die der Nebendiagonalen (gestrichelte Pfeile) subtrahiert*

werden:

$$\begin{array}{c} + \\ \left|\begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array}\right| \\ - \end{array} \quad \textit{und} \quad \begin{array}{c} \begin{array}{ccc} + & + & + \end{array} \\ \left|\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}\right| \\ \begin{array}{ccc} - & - & - \end{array} \end{array}$$

Bei der Berechnung der Determinante der (3×3)*-Matrix werden dazu die ersten beiden Spalten rechts neben die Matrix kopiert, um die Diagonalen bilden zu können. Diese Methode ist auch unter dem Namen „Sarrussche Regel“ oder „Regel von Sarrus“ bekannt.*

Analoge Merkregeln für größere Matrizen existieren nicht! *Es ist ein häufiger Fehler, für die Berechnung der Determinante einer* (4×4)*-Matrix deren erste drei Spalten zu kopieren um analog zur Sarrusschen Regel jeweils vier Haupt- und Nebendiagonalen zu bilden: Aber auf diese Weise würden nur acht Terme der Form „*$\operatorname{sign}(\sigma)\cdot\prod a_{i,\sigma(i)}$*“ gebildet, und in der Leibniz-Formel treten* $24 = 4!$ *davon auf!. Für größere* n *wird dieses Mißverhältnis natürlich noch größer.* □

Aus der Leibniz-Formel ergibt sich schnell die Determinante von oberen und unteren Dreiecksmatrizen:

Lemma 3.3.4. *Sei* R *ein kommutativer Ring mit Eins und* $A := (a_{i,j}) \in \operatorname{Mat}_n(R)$ *eine obere oder untere Dreiecksmatrix. Dann ist die Determinante von* A *das Produkt der Diagonalelemente:*

$$\det(A) = \prod_{i=1}^{n} a_{i,i}.$$

Beweis.
Der Beweis beruht auf folgender Hilfsaussage:

Hilfsaussage: Ist $\sigma \in S_n$ und $\sigma \neq \mathrm{id}$, so gibt es Indizes i, j mit:

$$1 \leq i \neq j \leq n \quad \text{und} \quad i < \sigma(i),\ j > \sigma(j).$$

Beweis der Hilfsaussage: Sei i der kleinste und j der größte „Nicht-Fixpunkt“ von σ, also:

$$i := \min\{\, k \mid \sigma(k) \neq k \,\} \quad \text{und} \quad j := \max\{\, k \mid \sigma(k) \neq k \,\}.$$

Dann müssen wegen der Injektivität von σ offensichtlich die behaupteten Ungleichungen für i und j gelten und die Hilfsaussage ist bewiesen.

Es sei nun die Leibniz-Formel für die Determinante von A betrachtet:

$$\det(A) = \sum_{\sigma\in S_n} \Big(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \Big).$$

Für jedes $\sigma \in S_n$ mit $\sigma \neq \mathrm{id}$ ist nach der Hilfsaussage im Produkt $\prod_{k=1}^{n} a_{k,\sigma(k)}$ mindestens ein Koeffizient $a_{i,\sigma(i)}$ von oberhalb der Diagonalen ($i < \sigma(i)$) und ein Koeffizient $a_{j,\sigma(j)}$ von unterhalb der Diagonalen ($j > \sigma(j)$) enthalten, so daß in dem Produkt mindestens ein Faktor Null ist (A ist eine obere oder untere Dreiecksmatrix)

und damit das ganze Produkt gleich Null. Also ist nur der Term für $\sigma = \mathrm{id}$ in der Summe von Interesse, und es folgt:

$$\det(A) = \sum_{\sigma \in S_n} \left(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \right) \overset{(\sigma = \mathrm{id})}{=} \underbrace{\operatorname{sign}(\mathrm{id})}_{=1} \cdot \prod_{i=1}^{n} a_{i,\mathrm{id}(i)} = \prod_{i=1}^{n} a_{i,i}. \qquad \square$$

Beispiel 3.3.5.

i.) Für die Einheitsmatrix E_n gilt: $\det(E_n) = 1$.

ii.) Für die Matrizen $L_{i,j}(\lambda)$ und $D_i(\alpha)$ aus Definition 3.2.3 gilt:

$$\det\big(L_{i,j}(\lambda)\big) = 1 \quad \textit{und} \quad \det\big(D_i(\alpha)\big) = \alpha.$$

Insbesondere ist damit die Determinantenabbildung $\det\colon \mathrm{Mat}_n(R) \longrightarrow R$ *surjektiv, denn für jedes $\alpha \in R$ ist $D_i(\alpha) \in \mathrm{Mat}_n(R)$ definiert.*

iii.) Für $n \in \mathbb{N}$ und $\alpha \in R$ gilt: $\det(\alpha E_n) = (\alpha)^n$. $\square$

Die Determinantenabbildung zwischen den Ringen mit Eins $\mathrm{Mat}_n(R)$ und R ist für $n \geq 2$ kein Ringhomomorphismus, da sie dann nicht strukturverträglich mit der Addition ist, wie folgendes Beispiel zeigt ($n \geq 2$):

Beispiel 3.3.6. *Sei F die Diagonalmatrix $F := E_n - E_{1,1}$, so daß nach Lemma 3.3.4* $\det(F) = 0$ *gilt. Für $n \geq 2$ gilt* $\det(E_{i,i}) = 0$, *und es folgt:*

$$\det\big(F + E_{1,1}\big) = \det(E_n) \overset{(3.3.5)}{=} 1 \neq 0 = 0 + 0 \overset{(3.3.4)}{=} \det\big(F\big) + \det(E_{1,1}). \qquad \square$$

Allerdings ist die Determinantenabbildung mit der Multiplikation von Matrizen verträglich, was im bald folgenden Determinantenmultiplikationssatz gezeigt wird. Zuvor ist jedoch noch folgende Aussage zu beweisen:

Lemma 3.3.7. *Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{Mat}_n(R)$. Ist $n \geq 2$ und besitzt A zwei gleiche Zeilen, so gilt* $\det(A) = 0$.

Beweis.

Es sei $(a_{i,j}) := A$, und es seien $1 \leq k_1 < k_2 \leq n$ die Indizes der beiden gleichen Zeilen, d.h. es gilt $a_{k_1,i} = a_{k_2,i}$ für $1 \leq i \leq n$ $(*_1)$. Dann folgt für $\tau \in S_n$, da R ein kommutativer Ring ist und damit Produkte von Koeffizienten $a_{i,j}$ aus A umgestellt werden dürfen $(*_2)$:

$$\begin{aligned}
\prod_{i=1}^{n} a_{i,\tau\circ(k_1\,k_2)(i)} &\overset{(*_2)}{=} a_{k_1,\tau\circ(k_1\,k_2)(k_1)} \cdot a_{k_2,\tau\circ(k_1\,k_2)(k_2)} \cdot \prod_{\substack{i=1\\ i\neq k_1,k_2}}^{n} a_{i,\tau\circ(k_1\,k_2)(i)} \\
&= \underbrace{a_{k_1,\tau(k_2)}}_{\overset{(*_1)}{=} a_{k_2,\tau(k_2)}} \cdot \underbrace{a_{k_2,\tau(k_1)}}_{\overset{(*_1)}{=} a_{k_1,\tau(k_1)}} \cdot \prod_{\substack{i=1\\ i\neq k_1,k_2}}^{n} a_{i,\tau(i)} \overset{(*_2)}{=} \prod_{i=1}^{n} a_{i,\tau(i)}.
\end{aligned}$$

Es gilt also zusammengefaßt für alle $\tau \in S_n$ die Gleichung:

$$\prod_{i=1}^{n} a_{i,\tau\circ(k_1\,k_2)(i)} = \prod_{i=1}^{n} a_{i,\tau(i)}. \qquad (*_3)$$

Weiter sei der Gruppenhomomorphismus $\operatorname{sign}\colon S_n \longrightarrow \{\pm 1\}$ betrachtet (siehe Lemma 1.2.45 ff.): er ist surjektiv, so daß für seinen Kern $A_n := \ker(\operatorname{sign})$ (die alternierende Gruppe A_n) aus dem Homomorphie-Satz Version II 1.2.59 die Gleichung

$|S_n/A_n| = 2$ folgt (siehe auch Aufgabenblatt 6 aus LA I, Aufgabe 1). Für jede Transposition $(a\,b) \in S_n$ gilt $\operatorname{sign}\big((a\,b)\big) = -1$, also $(a\,b) \notin A_n$, und es folgt $S_n = A_n \dot\cup (a\,b)A_n$.
Da A_n als Kern eines Homomorphismus ein Normalteiler ist, gilt $(a\,b)A_n = A_n(a\,b)$, so daß dann ebenso die Zerlegung $S_n = A_n \dot\cup A_n(a\,b)$ folgt. Es ergibt sich dann zusammengefaßt mit der speziellen Transposition $(k_1\,k_2)$:

$$\begin{aligned}
\det(A) &= \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n a_{i,\sigma(i)}\Big) \qquad \big(\text{ mit } S_n = A_n \dot\cup A_n(k_1\,k_2)\ \big)\\
&= \underbrace{\sum_{\tau\in A_n}\Big(\operatorname{sign}(\tau)\cdot\prod_{i=1}^n a_{i,\tau(i)}\Big)}_{\rightsquigarrow\ \sigma:=\tau\in A_n} + \underbrace{\sum_{\tau\in A_n}\Big(\operatorname{sign}\big(\tau\circ(k_1\,k_2)\big)\cdot\prod_{i=1}^n a_{i,\tau\circ(k_1\,k_2)(i)}\Big)}_{\rightsquigarrow\ \sigma:=\tau\circ(k_1\,k_2)\in A_n(k_1\,k_2)}\\
&= \sum_{\tau\in A_n}\Big(\operatorname{sign}(\tau)\cdot\prod_{i=1}^n a_{i,\tau(i)} + \underbrace{\operatorname{sign}\big(\tau\circ(k_1\,k-2)\big)}_{-\operatorname{sign}(\tau)}\cdot\prod_{i=1}^n a_{i,\tau\circ(k_1\,k_2)(i)}\Big)\\
&= \sum_{\tau\in A_n}\operatorname{sign}(\tau)\cdot\Big(\prod_{i=1}^n a_{i,\tau(i)} - \prod_{i=1}^n a_{i,\tau\circ(k_1\,k_2)(i)}\Big)\\
&\overset{(*_3)}{=} \sum_{\tau\in A_n}\operatorname{sign}(\tau)\cdot\Big(\prod_{i=1}^n a_{i,\tau(i)} - \prod_{i=1}^n a_{i,\tau(i)}\Big) = 0.
\end{aligned}$$

□

Nun kann der Determinantenmultiplikationssatz formuliert werden:

Satz 3.3.8. *(Determinantenmultiplikationssatz)*
Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann gilt für $A, B \in \operatorname{Mat}_n(R)$:

$$\det(AB) = \det(A)\cdot\det(B).$$

Beweis. Siehe Anhang A.4: Satz A.4.1. □

Bemerkung 3.3.9.

i.) Der Determinantenmultiplikationssatz kann auf verschiedene Arten bewiesen werden, mit mehr oder weniger vorher entwickelter Theorie. In diesem Skript ist die Determinante so kompakt wie möglich eingeführt (Leibniz-Formel 3.3.1), und der Determinantenmultiplikationssatz mit minimalen Vorraussetzungen bewiesen. Auf Grund des Rechenumfanges ist der Beweis ausgelagert, da er trotz seiner Länge elementar ist und keine tieferen Einsichten verlangt oder liefert. Einzig Lemma 3.3.7 wird benötigt, welches selbst einen längeren, aber elementaren und rein kombinatorischen Beweis hat, der exemplarisch vorgeführt ist.

ii.) Für zwei Matrizen $A, B \in \operatorname{Mat}_n(R)$ gilt im allgemeinen $AB \neq BA$, aber da R ein kommutativer Ring ist und $\det(A), \det(B) \in R$ gilt, folgt für alle A, B:

$$\det(AB) = \det(A)\cdot\det(B) \overset{(R\ komm.)}{=} \det(B)\cdot\det(A) = \det(BA).$$

iii.) Ist A invertierbar, so existiert A^{-1} mit $AA^{-1} = A^{-1}A = E_n$, und es folgt:

$$\left.\begin{aligned} \det(A)\cdot\det(A^{-1}) &= \det(AA^{-1}) = \det(E_n) = 1 \\ \det(A^{-1})\cdot\det(A) &= \det(A^{-1}A) = \det(E_n) = 1 \end{aligned}\right\} \quad \Longrightarrow \quad \begin{aligned} &\det(A) \in R^* \text{ und} \\ &\det(A^{-1}) = \det(A)^{-1}. \end{aligned}$$

Insbesondere werden also invertierbare Matrizen, d.h. Einheiten im Matrizenring $\mathrm{Mat}_n(R)$, auf Einheiten in R abgebildet. □

Die Struktureigenschaften der Abbildung $\det\colon \mathrm{Mat}_n(R) \longrightarrow R$ zwischen den Ringen $\mathrm{Mat}_n(R)$ und R sind dann zusammengefaßt folgende:

Satz 3.3.10. *Sei R ein kommutativer Ring mit Eins und $n \geq 2$. Dann ist $\mathrm{Mat}_n(R)$ ein nicht-kommutativer Ring mit Eins (Satz 3.1.9). Die Determinantenabbildung:*

$$\det\colon \mathrm{Mat}_n(R) \longrightarrow R$$

ist kein Ringhomomorphismus, da sie nicht strukturverträglich mit der Addition ist (siehe Beispiel 3.3.6), aber ein Monoidhomomorphismus bzgl. der Multiplikation (Determinantenmultiplikationssatz 3.3.8), der die Einsen der Ringe aufeinander abbildet ($\det(E_n) = 1$ Beispiel 3.3.5).
Die Abbildung $\det\colon \mathrm{Mat}_n(R) \longrightarrow R$ ist wegen $\det\big(D_1(\alpha)\big) = \alpha$ surjektiv, (Beispiel 3.3.5), da für jedes $\alpha \in R$ die Matrix $D_1(\alpha) \in \mathrm{Mat}_n(R)$ definiert ist (Beispiel 3.3.5).

Von der Abbildung „det“ werden Einheiten aus $\mathrm{Mat}_n(R)$ auf Einheiten in R abgebildet (Bemerkung 3.3.9), so daß „det“ auf die Einheitengruppe $\mathrm{GL}_n(R)$ (Definition 3.1.10) von $\mathrm{Mat}_n(R)$ und R^* von R eingeschränkt werden kann:

$$\det\colon \mathrm{GL}_n(R) \longrightarrow R^*.$$

(Dabei wird auf eine besondere Bezeichnung der Einschränkung verzichtet!)
Die Abbildung $\det\colon \mathrm{GL}_n(R) \longrightarrow R^*$ ist dann ein surjektiver Gruppenhomomorphismus, und sein Kern wird mit $\mathrm{SL}_n(R)$ (mit „SL“ für „special linear group“, siehe auch Definition 3.1.10 für „GL“) bezeichnet und ist ein Normalteiler der Gruppe $\mathrm{GL}_n(R)$:

$$\mathrm{SL}_n(R) := \ker(\det) = \{\, A \in \mathrm{Mat}_n(R) \mid \det(A) = 1 \,\}.$$

Beweis.
Die Aussagen des ersten Teils sind alles Zitate.

$\det\colon \mathrm{GL}_n(R) \longrightarrow R^*$ ist ein Gruppenhomomorphismus: Wegen Bemerkung 3.3.9 gilt $\det\big(\mathrm{GL}_n(R)\big) \subseteq R^*$, so daß die Einschränkung von „det“ auf $\mathrm{GL}_n(R)$ eine wohldefinierte Abbildung ist. Die beiden Einheitengruppen sind multiplikative Gruppen, und die Abbildung „det “ ist nach dem Determinantenmultiplikationssatz 3.3.8 multiplikativ strukturverträglich, so daß „det“ auch ein Gruppenhomomorphismus ist.

$\det\colon \mathrm{GL}_n(R) \longrightarrow R^*$ ist surjektiv: Für $\alpha \in R^*$ gibt es ein $b \in R^*$ mit $ab = ba = 1$, und es gilt dann

$$D_1(a)D_1(b) = D_1(ab) = E_n = D_1(ba) = D_1(b)D_1(a),$$

so daß $D_1(\alpha) \in \mathrm{GL}_n(R)$ folgt. Wegen $\det\big(D_1(\alpha)\big) = \alpha$ hat jedes $\alpha \in R^*$ dann auch ein Urbild in $\mathrm{GL}_n(R)$. □

Bemerkung 3.3.11.

i.) $\det\colon \mathrm{GL}_n(R) \longrightarrow R^*$ *ist ein surjektiver Gruppenhomorphismus, und so sind alle Fasern von Elementen aus* R^* *von gleicher Mächtigkeit: Sie sind nach Satz 1.2.59 Nebenklassen des Kerns* $\mathrm{SL}_n(R)$*, und Nebenklassen einer Untergruppe sind alle gleichmächtig zu dieser Untergruppe. Es gibt also salopp gesprochen zu jedem Wert aus* R^* *genau gleichviele Matrizen aus* $\mathrm{GL}_n(R)$ *mit dieser Determinante. Außerdem liefert der Homorphie-Satz 1.2.59 für eine endliche Gruppe* $|\mathrm{GL}_n(R)|$ *noch die Beziehung:*

$$|\mathrm{GL}_n(R)| = |R^*| \cdot |\mathrm{SL}_n(R)| \quad \textit{bzw.} \quad |\mathrm{SL}_n(R)| = \frac{|\mathrm{GL}_n(R)|}{|R^*|}.$$

In Satz 3.3.12 wird eine explizite Formel z.B. für die Ordnung von $\mathrm{GL}_2(\mathbb{Z}_5)$ *angegeben (*$\mathbb{Z}_5$ *ist ein endlicher Körper), und es folgt* $|\mathrm{GL}_2(\mathbb{Z}_5)| = 24 \cdot 20 = 480$*. Wegen* $|\mathbb{Z}_5^*| = 4$ *gilt dann:*

- $|\mathrm{SL}_2(\mathbb{Z}_5)| = 120$.
- *Es gibt in* $\mathrm{GL}_2(\mathbb{Z}_5)$ *jeweils* 120 *Matrizen mit der Determinante* $[1]_5$, $[2]_5$, $[3]_5$ *und* $[4]_5$.

ii.) *Zwar ist die Determanantenabbildung* $\det\colon \mathrm{Mat}_n(R) \longrightarrow R$ *multiplikativ, aber* $\mathrm{Mat}_n(R)$ *und* R *sind keine multiplikativen Gruppen, und die obige Aussage über die Mächtigkeit der Fasern von Determinanten kann nicht auf* R *ausgeweitet werden. Im obigen Beispiel von quadratischen Matrizen über* $\mathbb{Z}_5$ *fehlt nur die Determinante Null als Nicht-Einheit, und die Anzahl der Matrizen mit der Determinante* $[0]_5$ *ist gleich:*

$$|\mathrm{Mat}_2(\mathbb{Z}_5)| - |\mathrm{GL}_2(\mathbb{Z}_5)| = 5^4 - 480 = 625 - 480 = 145,$$

also nicht $120 = |\mathrm{SL}_n(\mathbb{Z}_5)|$*, wie vermutet werden könnte.*

iii.) *Der Homorphie-Satz für Gruppen 1.2.59 liefert für jeden kommutativen Ring* R *einen Gruppenisomorphismus:*

$$\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \cong R^*.$$

($\mathrm{SL}_n(R)$ *ist als Kern der Determinantenabbildung ein Normalteiler von* $\mathrm{GL}_n(R)$*, so daß die Quotientengruppe* $\mathrm{GL}_n(R)/\mathrm{SL}_n(R)$ *definiert ist.)* □

Für einen endlichen Ring R ist $\mathrm{Mat}_n(R)$ eine endliche Menge, da es sich bei den quadratischen $(n \times n)$-Matrizen um Tupel mit n^2 Koeffizienten aus R handelt: es gibt also genau $|R|^{n^2}$ davon. Damit sind in diesem Fall auch die Gruppen $\mathrm{GL}_n(R)$ und $\mathrm{SL}_n(R)$ endlich, denn es gilt ja:

$$\mathrm{SL}_n(R) \subseteq \mathrm{GL}_n(R) \subseteq \mathrm{Mat}_n(R) \quad \text{und} \quad |\mathrm{Mat}_n(R)| = |R|^{n^2}.$$

Ist R ein endlicher Körper, so ist $R^{[n]}$ ein R-Vektorraum, und mit Hilfe der Ergebnisse der Vektorraumtheorie kann sogar eine explizite Formel für die Größe der beiden Gruppen $\mathrm{SL}_n(R)$ und $\mathrm{GL}_n(R)$ angegeben werden:

Satz 3.3.12. *Sei* K *ein endlicher Körper mit* $q := |K|$ *Elementen (Nach Bemerkung 1.3.35 ist* q *dann eine Primzahlpotenz). Dann haben die beiden Matrizengruppen* $\mathrm{GL}_n(K)$ *und* $\mathrm{SL}_n(K)$ *folgende Ordnung:*

$$|\mathrm{GL}_n(K)| = \prod_{i=0}^{n-1} \left(q^n - q^i\right) = q^{\frac{n(n-1)}{2}} \cdot \prod_{i=1}^{n} \left(q^i - 1\right). \quad \textit{und} \quad |\mathrm{SL}_n(K)| = \frac{|\mathrm{GL}_n(K)|}{q-1}.$$

Beweis.
Nach Satz 3.1.20 ist die folgenden Abbildung:

$$\Phi\colon\ \mathrm{Mat}_n(K) \longrightarrow \mathrm{End}_R(K^{[n]}) \quad \text{mit} \quad A \mapsto \varphi_A$$

ein Ringisomorphismus, der sich zu einen Gruppenisomorphismus:

$$\widehat{\Phi}\colon\ \mathrm{GL}_n(K) \longrightarrow \mathrm{GL}_K(K^{[n]})$$

einschränken läßt.
Nach dem Hauptsatz über lineare Abbildungen und Basen 2.2.31 sind alle Automorphismen des $K^{[n]}$ eindeutig durch deren Bilder auf Standardbasis $(e_1, \ldots, e_n)$ des $K^{[n]}$ festgelegt, und jede Basis $(x_1, \ldots, x_n)$ des $K^{[n]}$ definiert über die Zuordnung $e_i \mapsto x_i$ einen Automorphismus des $K^{[n]}$, so daß eine eineindeutige Beziehung zwischen Automorphismen und Basen des $K^{[n]}$, besteht, d.h. es gibt eine Bijektion:

$$\mathrm{GL}_K(K^{[n]}) \longleftrightarrow \{\ \text{Basen des } K^{[n]}\ \}.$$

Damit existiert also folgende Kette von Bijektionen:

$$\mathrm{GL}_n(K) \longleftrightarrow \mathrm{GL}_K(K^{[n]}) \longleftrightarrow \{\ \text{Basen des } K^{[n]}\ \},$$

so daß zur Berechnung der Ordnung von $\mathrm{GL}_n(K)$ die Anzahl der Basen des $K^{[n]}$ gezählt werden kann.
Die bisherigen Argumente verlangen nicht, daß K ein Körper ist, sie gelten für jeden kommutativen Ring mit Eins. Beim Zählen der Basen des $K^{[n]}$ ist es jedoch wesentlich, daß K ein Körper ist.
Für den K-Vektorraum $K^{[n]}$ (K Körper!) gilt, daß Basen und maximal linear unabhängige Systeme das Gleiche sind (Satz 2.2.37), und mit Hilfe von Lemma 2.2.51 können in Vektorräumen maximal linear unabhängige System konstruiert werden:

- Als Startvektor eines zu konstruierenden maximal linear unabhängigen Systems kann ein beliebiger Vektor ungleich Null aus $K^{[n]}$ gewählt werden, von denen es wegen $|K| = q$ und damit $|K^{[n]}| = q^n$ genau $q^n - 1$ gibt.
- Ist ein Vektor x_1 gewählt, spannt dieser einen eindimensionalen Untervektorraum U_1 auf mit $|U_1| = q^1 = q$ Vektoren, und jeder Vektor außerhalb dieses Erzeugnis ist linear unabhängig zu x_1 (Lemma 2.2.51), so daß $|K^{[n]}| - |U_1| = q^n - q$ Vektoren gewählt werden können, um ein linear unabhängiges System (x_1, x_2) zu konstruieren.
- Sind nun i linear unabhängige Vektoren $(x_1, \ldots, x_i)$ gewählt, spannen diese einen i-dimensionalen Untervektorraum U_i auf mit $|U_i| = q^i$ Vektoren, und jeder Vektor außerhalb dieses Erzeugnis ist linear unabhängig zu diesem System (Lemma 2.2.51), so daß $|K^{[n]}| - |U_i| = q^n - q^i$ Vektoren gewählt werden können, um das vorhandene linear unabhängige System um einen Vektor zu erweitern.

Dieses Konstruktionsverfahren muß n-mal ausgeführt werden ($\dim_K(K^{[n]}) = n$), um ein maximal linear unabhängiges System zu finden und liefert dann insgesamt:

$$(q^n - 1) \cdot (q^n - q) \cdot (q^n - q^2) \cdot \ldots \cdot (q^n - q^{n-1}) = \prod_{i=0}^{n-1} \left(q^n - q^i\right)$$

maximal linear unabhängige Systeme (Basen) in $K^{[n]}$.

Wird dabei aus jedem Term $q^n - q^i$ der Faktor q^i ausgeklammert, ergibt sich mit $\sum_{i=0}^{n-1} i = \frac{(n-1)n}{2}$ und $\prod_{i=0}^{n-1}(q^{n-i}-1) = \prod_{i=1}^{n}(q^i-1)$ die Formel:

$$\prod_{i=0}^{n-1}(q^n - q^i) = \Big(\prod_{i=0}^{n-1} q^i\Big) \cdot \Big(\prod_{i=1}^{n}\big(q^i-1\big)\Big) = q^{\sum_{i=0}^{n-1} i} \cdot \prod_{i=1}^{n}\big(q^i-1\big) = q^{\frac{n(n-1)}{2}} \cdot \prod_{i=1}^{n}\big(q^i-1\big).$$

Die Formel über $|\operatorname{SL}_n(K)|$ folgt dann sofort mit $|K^*| = q-1$ und Bemerkung 3.3.11. □

Bemerkung 3.3.13.

i.) Satz 3.3.12 läßt sich nicht für die Berechnung Größe der Automorphismengruppe $\operatorname{GL}_n(R)$ über einem kommutativen Ring R übertragen, wie folgendes Beispiel zeigt: Sei dazu der Ring $\mathbb{Z}_4$ betrachtet. Es gibt $4^4 = 256$ Matrizen in $\operatorname{Mat}_2(\mathbb{Z}_4)$, und eine kurze Berechnung all deren Determinante (per Computer) ergibt folgende Ergebnisse:

$\det(A)$:	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
Anzahl:	88	48	72	48

Würde die Formel aus Satz 3.3.12 für $\operatorname{GL}_n(\mathbb{Z}_4)$ gelten, müßte es wegen $|\mathbb{Z}_4| = 4$ insgesamt:

$$(4^2-1)\cdot(4^2-4) = 15 \cdot 12 = 180$$

invertierbare Matrizen in $\operatorname{Mat}_2(\mathbb{Z}_4)$ geben. Da invertierbare Matrizen aber nach Satz 3.3.10 eine Determinante aus $\mathbb{Z}_4^* = \{[1]_4, [3]_4\}$ haben, können nach obiger Tabelle höchstens $2 \cdot 48 = 96$ Elemente in $\operatorname{GL}_n(\mathbb{Z}_4)$ existieren.
Bisher ist noch nicht klar, ob eine Matrix, deren Determinante eine Einheit ist, invertierbar ist: nur die Umkehrung davon ist in Satz 3.3.10 bewiesen. Tatsächlich wird später die Äquivalenz beider Aussagen gezeigt, so daß dann tatsächlich $\operatorname{GL}_2(\mathbb{Z}_4) = 96$ gilt.

ii.) Sei K ein endlicher Körper mit q Elementen. Aus den beiden Gruppen $\operatorname{GL}_n(K)$ und $\operatorname{SL}_n(K)$ können wichtige weitere Gruppen konstruiert werden:
Für jede Gruppe G ist ihr Zentrum $Z(G)$ definiert durch:

$$Z(G) := \{\, g \in G \mid gh = hg \text{ für alle } h \in G \,\},$$

und dies ist nichts anderes als der Kern des folgenden Gruppenhomomorphismus:

$$\Phi_G \colon G \longrightarrow S(G) \quad \text{mit} \quad g \mapsto \kappa_g,$$

wobei $\kappa_g \colon G \longrightarrow G$ die Konjugationsabbildung $h \mapsto ghg^{-1}$ ist (siehe dazu LAI Aufgabenblatt 6, Aufgabe 3, und auch Beispiel 1.2.40). Damit ist das Zentrum einer Gruppe als Kern eines Gruppenhomomorphismus ein Normalteiler von G, so daß die Quotientengruppe $G/Z(G)$ gebildet werden kann.
Im Falle von $\operatorname{GL}_n(K)$ und $\operatorname{SL}_n(K)$ gilt für das Zentrum der Gruppen:

$$Z\big(\operatorname{GL}_n(K)\big) = \{\, \alpha \cdot E_n \mid \alpha \in K^* \,\} \quad \text{und} \quad Z\big(\operatorname{SL}_n(K)\big) = \{\, \alpha \cdot E_n \mid \alpha \in K^*, \alpha^n = 1 \,\},$$

und die Größe des jeweiligen Zentrums ist:

$$|Z\big(\operatorname{GL}_n(K)\big)| = q-1 \quad \text{und} \quad |Z\big(\operatorname{SL}_n(K)\big)| = \operatorname{ggT}(n, q-1).$$

(Siehe auch LAIIa Aufgabenblatt 2, Aufgabe 4).

Die jeweiligen Quotientengruppen haben eigene Bezeichnungen:

$$PGL_n(K) := \mathrm{GL}_n(K)/Z\big(\mathrm{GL}_n(K)\big) \qquad \textit{und} \qquad PSL_n(K) := \mathrm{SL}_n(K)/Z\big(\mathrm{SL}_n(K)\big),$$

wobei das „P“ in den Bezeichnungen für „projektiv“ steht. Mit den Satz von Lagrange 1.2.20 und den obigen Formeln für das Zentrum der Gruppen folgt sofort:

$$|PGL_n(K)| = \frac{|\mathrm{GL}_n(K)|}{q-1} \quad \textit{und} \quad |PSL_n(K)| = \frac{|\mathrm{SL}_n(K)|}{\mathrm{ggT}(n, q-1)}.$$

Die Gruppen $PSL_n(K)$ sind für $n \geq 2$ bis auf wenige Ausnahmen einfache Gruppen (Gruppen, die keine nicht-trivialen Normalteiler haben). Die Ausnahmen sind nur die Fälle $|K| = 2$ und $n = 2$ sowie $|K| = 3$ und $n = 2$. Dabei gilt:

$$PSL_2(\mathbb{Z}_2) \cong S_3 \qquad \textit{und} \qquad PSL_2(\mathbb{Z}_3) \cong A_4.$$

A_4 ist die alternierende Gruppe in S_4, d.h. der Kern der Signum-Abbildung $\mathrm{sign}\colon S_4 \longrightarrow \{\pm 1\}$, *mit $|A_4| = 12$.*
Zwei endliche Körper K_1 und K_2 mit gleicher Größe, d.h. $|K_1| = |K_2|$, sind isomorph, und auch die Matrizengruppen $\mathrm{GL}_n(K_1)$ und $\mathrm{GL}_n(K_2)$ sowie $\mathrm{SL}_n(K_1)$ und $\mathrm{SL}_n(K_2)$. Ebenso sind die daraus abgeleiteten projektiven Gruppen jeweils isomorph zueinander. Damit reduziert sich in obiger Aussage (bis auf Isomorphie) die Anzahl der Ausnahmen auf zwei, und diese werden genau durch die obigen beiden Beispiele beschrieben. □

Die Berechnung einer Determinante über die Leibniz-Formel ist sehr aufwendig, und selbst Computer müssen schnell die Waffen strecken, wenn $(n-1)\cdot n!$ Multiplikationen ausgeführt werden müssen: Stand Juni 2012 schafft der schnellste Computer der Welt laut Wikipedia maximal $2 \cdot 10^{16}$ Multiplikationen pro Sekunde (tatsächlich ca. 16 Petaflops), so daß die Berechnung der Determinante einer (25×25)-Matrix über die Leibniz-Formel mehr als 500 Jahre gebraucht hätte (grobe Abschätzung!).
Allerdings weist der Determinantenmultiplikationssatz einen einfacheren Weg der Berechnung. Mit dem Gauß-Algorithmus läßt sich eine Matrix über einem Körper in obere Dreiecksform bringen durch Multiplikation mit den speziellen Gauß-Matrizen $L_{i,j}(\lambda)$ und $P_{i,j}$:

$$A \xrightarrow{\text{Gauß-Algorithmus}} GA = R, \quad G \text{ Produkt von Matrizen } L_{i,j}(\lambda), P_{i,j}, \text{ Satz 3.2.9.}$$

Die Determinante der oberen Dreiecksmatrix R ist nach Lemma 3.3.4 leicht berechenbar. Wegen $\det\big(L_{i,j}(\lambda)\big) = 1$ (Beispiel 3.3.5) gilt nach dem Determinantenmultiplikationssatz 3.3.8:

$$\det\big(L_{i,j}(\lambda) \cdot A\big) = \underbrace{\det\big(L_{i,j}(\lambda)\big)}_{=1} \cdot \det(A) = \det(A),$$

so daß diese Schritte des Gauß-Algorithmus die Determinante gar nicht verändern.
Es wird jetzt noch untersucht, welche Auswirkung die Anwendung einer Zeilenvertauschung des Gauß-Algorithmus auf die Determinante der Matrix hat, wozu die Determinante der Matrix $P_{i,j}$ berechnet werden muß. Diese kann als leichte Übung mit dem Determinantenmultiplikationssatz aus den bisher bekannten Ergebnissen berechnet werden:

Beispiel 3.3.14. *Für die Matrizen $P_{i,j}$ aus Definition 3.2.3 gilt:*

$$\det(P_{i,j}) = -1.$$

Dazu sei folgende Konstruktion betrachtet (mit $i \neq j$):

$$\begin{aligned} L_{i,j}(-1)L_{j,i}(1)P_{i,j} &= (E_n - E_{i,j})(E_n + E_{j,i})(E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}) \\ &= (E_n - E_{i,j} + E_{j,i} - E_{i,i})(E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}) \\ &= (E_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}) + (-E_{i,j} + 0 + E_{i,j} - 0 - E_{i,i}) \\ &\quad + (E_{j,i} - E_{j,i} - 0 + E_{j,j} + 0) + (-E_{i,i} + E_{i,i} + 0 - E_{i,j} - 0) \\ &= E_n - 2E_{i,i} + E_{j,i}. \end{aligned}$$

Nun ist $E_n - 2E_{i,i} + E_{j,i}$ eine obere oder untere Dreiecksmatrix (je nachdem, ob $i > j$ oder $i < j$ gilt) mit lauter Einsen und einer Minus-Eins auf der Diagonalen, so daß $\det(E_n - 2E_{i,i} + E_{j,i}) = -1$ gilt (Lemma 3.3.4), und wegen $\det\big(L_{i,j}(\lambda)\big) = 1$ (Beispiel 3.3.5) folgt mit dem Determinantenmultiplikationssatz:

$$\begin{aligned} \det(P_{i,j}) &= \underbrace{\det\big(L_{i,j}(-1)\big)}_{=1} \cdot \underbrace{\det\big(L_{j,i}(1)\big)}_{=1} \cdot \det(P_{i,j}) = \det\big(L_{i,j}(-1)L_{j,i}(1)P_{i,j}\big) \\ &= \det(E_n - 2E_{i,i} + E_{j,i}) = -1. \end{aligned}$$

□

Nun liefert der Gauß-Algorithmus (Satz 3.2.9) mit den bisherigen Determinantenergebnissen:

Satz 3.3.15. *Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$ ungleich der Nullmatrix. Weiter seien $G \in \mathrm{GL}_n(K)$ und $R \in \mathrm{Mat}_n(K)$ diejenigen Matrizen mit $GA = R$, die sich aus dem ersten Schritt Gauß-Algorithmus in Satz 3.2.9 ergeben, d.h. R ist eine „allgemeine“ Zeilen-Stufen-Form (und damit insbesondere eine obere Dreiecksmatrix) und G ist ein Produkt von Matrizen des Types $L_{i,j}(\lambda)$ und $P_{i,j}$ aus dem Gauß-Algorithmus (siehe auch Definition 3.2.3).*
Es sei k die Anzahl der nötigen Zeilenvertauschungen im Gauß-Algorithmus, d.h. die Anzahl der Faktoren $P_{i,j}$ im Produkt G. Dann gilt:

$$\det(G) = (-1)^k \quad \textit{und} \quad \det(A) = (-1)^k \cdot \det(R).$$

Insbesondere folgt dann mit Lemma 3.3.4, wenn $r_{i,i}$ die Diagonalelemente der Zeilen-Stufen-Form R sind:

$$\det(A) = (-1)^k \cdot \prod_{i=1}^{n} r_{i,i}.$$

Beweis.
Sei $G = \prod_{t=1}^{r} G_t$ mit $G_t \in \{L_{i,j}(\lambda), P_{i,j}\}$. Es gilt dann:

$$\det(G_t) = \begin{cases} 1 & \text{für } G_t = L_{i,j}(\lambda), \\ -1 & \text{für } G_t = P_{i,j}, \end{cases} \tag{$*_1$}$$

und mit dem Determinantenmultiplikationssatz 3.3.8 folgt sofort:

$$\det(G) = \det\Big(\prod_{t=1}^{r} G_t\Big) \overset{(3.3.8)}{=} \prod_{t=1}^{r} \det(G_t) \overset{(*_1)}{=} (-1)^k.$$

Dann liefert die Gleichung $R = GA$ sofort mit dem Determinantenmultiplikationssatz:

$$\det(R) = \det(GA) \overset{(3.3.8)}{=} \det(G) \cdot \det(A) \overset{(*_1)}{=} (-1)^k \cdot \det(A).$$

Wird diese Gleichung mit $(-1)^k$ multipliziert, folgt wegen $\big((-1)^k\big)^2 = 1$ letztendlich:

$$(-1)^k \cdot \det(A) = \det(R) \qquad \overset{\cdot(-1)^k}{\Longrightarrow} \qquad \det(A) = (-1)^k \cdot \det(R). \qquad \square$$

Bemerkung 3.3.16.

i.) *Der Gauß-Algorithmus angewandt auf eine $(n \times n)$-Matrix verlangt ungefähr n^3 Multiplikationen, so daß z.B. eine (25×25)-Matrix mit ca. $25^3 = 15625$ Multiplikationen in obere Dreiecksform gebracht werden kann. Dies schafft ein moderner Computer im Bruchteil einer Sekunde (per Leibniz-Formel mehr als 500 Jahre!).*

ii.) *Wird für eine Matrix A mit dem Gauß-Algorithmus eine LR-Zerlegung konstruiert wie in Satz 3.2.38 beschrieben, so ist die Matrix L ein Produkt von Matrizen $L_{i,j}$ und hat folglich die Determinante Eins. Dann gilt:*

$$\det(A) = \det(LR) = \underbrace{\det(L)}_{=1} \cdot \det(R) = \det(R).$$

iii.) *Das Gauß-Verfahren kann im allgemeinen nicht in der Fassung von Satz 3.2.9 auf eine Matrix über einem Ring angewendet werden, da beim ersten Schritt zur Überführung der gegebenen Matrix in eine Zeilen-Stufen-Form mit Matrizen $L_{i,j}(\lambda)$ und $\lambda := -\frac{a_{i,j_k}}{a_k}$ die Elemente a_k Einheiten sein müssen, und es ist nach dem Algorithmus nur $a_k \neq 0$ garantiert (siehe Gauß-Algorithmus 3.2.9).*

iv.) *Ist eine Matrix A über $\mathbb{Z}$ gegeben, so kann der Gauß-Algorithmus über $\mathbb{Z}$ selten ausgeführt werden, da in $\mathbb{Z}$ nur die beiden Einheiten $\{\pm 1\}$ existieren. Allerdings kann A wegen $\mathbb{Z} \subseteq \mathbb{Q}$ als Matrix $A_{\mathbb{Q}}$ über dem Körper $\mathbb{Q}$ aufgefaßt werden, und über $\mathbb{Q}$ ist der Gauß-Algorithmus immer durchführbar. Die über $\mathbb{Q}$ und den Gauß-Algorithmus berechnete Determinante $\det(A_{\mathbb{Q}})$ muß dann wegen der Leibnizformel in $\mathbb{Z}$ liegen, und es gilt:*

$$\det(A) = \det(A_{\mathbb{Q}}).$$

v.) *In Aufgabenblatt 2 (LAIIa) wird gezeigt, daß eine Matrix A über einem Restklassenring $\mathbb{Z}_n$ als Matrix $A_{\mathbb{Z}}$ über $\mathbb{Z}$ aufgefaßt werden kann und mit dem Ringhomomorphismus $\pi_n \colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $a \mapsto [a]_n$ gilt:*

$$\det(A) = \pi_n\big(\det(A_{\mathbb{Z}})\big).$$

Dies kann noch mit vorheriger Bemerkung verknüpft werden, und wird $A_{\mathbb{Z}}$ als Matrix $A_{\mathbb{Q}}$ über $\mathbb{Q}$ aufgefaßt, ist eine Berechnung der Determinante von $A_{\mathbb{Q}}$ mit dem Gauß-Algorithmus möglich, und es folgt:

$$\det(A) = \pi_n\big(\det(A_{\mathbb{Q}})\big). \qquad \square$$

Beispiel 3.3.17.

i.) *Nach Beispiel 3.2.11 läßt sich die Telephonmatrix folgendermaßen mit dem Gauß-Algorithmus in Zeilen-Stufen-Form (obere Dreicksgestalt) bringen:*

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \xrightarrow{L_{3,2}(-2)L_{3,1}(-7)L_{2,1}(-4)} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Beim Algorithmus treten keine Zeilenvertauschungen auf, d.h. Matrizen $P_{i,j}$, und somit ist die Determinante von A gleich der Determinante der Zeilen-Stufen-Form, d.h. dem Produkt von deren Diagonalelementen:

$$\det(A) = 1 \cdot (-3) \cdot 0 = 0.$$

ii.) *Als Beispiel, bei dem der Gauß-Algorithmus nicht zur Determinantenberechnung angewendet werden kann, sei folgende Matrix über $\mathbb{Z}_6$ gegeben:*

$$A := \begin{pmatrix} [2]_6 & [1]_6 \\ [3]_6 & [0]_6 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}_6).$$

Hier ist der Gauß-Algorithmus aus Satz 3.2.9 nicht anwendbar, da in der ersten Spalte keine Einheit aus $\mathbb{Z}_6$ steht und damit keine geeignete Zeilenoperation laut Satz 3.2.9 möglich ist.
Natürlich ergibt sich in diesem speziellen Fall die Determinante ebenso leicht aus der Leibniz-Formel durch $\det(A) = [2]_6 \cdot [0]_6 - [1]_6 \cdot [3]_6 = [-3]_6 = [3]_6$, aber eben nicht mit Hilfe von Satz 3.3.15 und dem Gauß-Algorithmus.

iii.) *Es sei wieder die Matrix des vorherigen Beispiels betrachtet:*

$$A := \begin{pmatrix} [2]_6 & [1]_6 \\ [3]_6 & [0]_6 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}_6).$$

Nach Bemerkung 3.3.16 kann diese Matrix als Matrix $A_{\mathbb{Q}}$ über $\mathbb{Q}$ aufgefaßt werden, und über dem Körper $\mathbb{Q}$ dann der Gauß-Algorithmus zur Bereichnung von $\det(A_{\mathbb{Q}})$ ausgeführt werden. Es ergibt sich:

$$A_{\mathbb{Q}} = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} \xrightarrow[L_{2,1}(-\frac{3}{2})]{\textit{Gauß-Algorithmus}} \begin{pmatrix} 2 & 1 \\ 0 & -\frac{3}{2} \end{pmatrix} \quad \Longrightarrow \quad \det(A_{\mathbb{Q}}) = -3.$$

Die Determinante von A über $\mathbb{Z}_6$ ergibt sich dann mit der Anwendung des Ringhomomorphismus π_6:

$$\det(A) = \pi_6\big(\det(A_{\mathbb{Q}})\big) \quad \Longrightarrow \quad \det(A) = \pi_6(-3) = [-3]_6 = [3]_6. \qquad \square$$

Die im vorherigen Beispiel betrachtete Matrix:

$$A := \begin{pmatrix} [2]_6 & [1]_6 \\ [3]_6 & [0]_6 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}_6)$$

kann zwar über $\mathbb{Z}_6$ nicht mit Hilfe des Gauß-Algorithmus berechnet werden, aber leicht mit folgender Operation in eine obere Dreiecksgestalt gebracht werden, deren Determinante dann bekannt ist:

$$AP_{1,2} = \begin{pmatrix} [1]_6 & [2]_6 \\ [0]_6 & [3]_6 \end{pmatrix} \qquad \text{(Spaltentausch)}.$$

Damit folgt dann sofort:

$$\begin{aligned} \det(AP_{1,2}) = [1]_6 \cdot [3]_6 \quad &\Longrightarrow \quad \det(A) \cdot \underbrace{\det(P_{i,j})}_{=[-1]_6} = [3]_6 \\ &\Longrightarrow \quad \det(A) = [3]_6 \cdot [-1]_6 = [-3]_6 = [3]_6. \end{aligned}$$

Es ist also mitunter zur Determinantenberechnung sinnvoll, Gauß-Operationen anzuwenden, ohne den Gauß-Algorithmus streng durchzuführen: durch kleine „determinantenfreundliche“ Transformationen kann eine Matrix oft in eine Gestalt gebracht werden, deren Determinante sofort berechenbar ist.
Durch den Determinantenmultiplikationssatz und die speziellen Matrizen $L_{i,j}(\lambda)$, $P_{i,j}$ und $D_i(\alpha)$ läßt sich schon eine ganze Liste nützlicher Determinantenregeln erstellen, aufgefüllt mit weiteren schon erarbeiteten Regeln wie z.B. Lemma 3.3.4 über die Determinante von Dreiecksmatrizen etc. Bevor dies geschieht, seien aber noch zwei wesentliche Regeln für Determinanten herausgearbeitet, aus denen sich in Kombination mit anderen viele neue Eigenschaften ableiten lassen.
Die erste davon bezieht sich auf die „Transponierte“ einer Matrix, die hier zuerst definiert werden muß:

Definition 3.3.18. *Sei R ein kommutativer Ring mit Eins. Zu einer gegebenen Matrix $A := (a_{i,j}) \in \mathrm{Mat}(m \times n, R)$ ist die transponierte Matrix (oder kurz: deren Transponierte) definiert als diejenige Matrix $B := (b_{i,j}) \in \mathrm{Mat}(n \times m, R)$ mit $b_{i,j} := a_{j,i}$. Die Transponierte von $A := (a_{i,j})$ wird auch notiert als:*

$$A^t := (a_{i,j})^t := (a_{j,i}). \qquad \square$$

Beispiel 3.3.19.

i.) Die Transponierte einer Matrix entsteht, indem die Zeilen der gegebenen Matrix zu Spalten „umgeklappt“ werden:

$$A = \begin{pmatrix} — & z_1 & — \\ & \vdots & \\ — & z_m & — \end{pmatrix} \qquad \Longrightarrow \qquad A^t = \begin{pmatrix} | & & | \\ z_1 & \cdots & z_m \\ | & & | \end{pmatrix}.$$

ii.)

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \qquad \Longrightarrow \qquad A^t = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}.$$

iii.)

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \qquad \Longrightarrow \qquad A^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}. \qquad \square$$

Wesentlich ist nun der Zusammenhang zwischen den Determinanten einer Matrix und ihrer Transponierten:

Lemma 3.3.20. *Sei R ein kommutativer Ring mit Eins. Dann gilt für eine quadratische Matrix $A \in \mathrm{Mat}_n(R)$ und ihre Transponierte $A^t \in \mathrm{Mat}_n(R)$:*

$$\det(A) = \det(A^t).$$

Beweis.
Mit der Leibniz-Formel ergibt sich für die Matrix $(a_{i,j}) := A$:

$$\begin{aligned}
\det(A) &= \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n a_{i,\sigma(i)}\Big) &&\overset{(*_1)}{=} \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n a_{\sigma^{-1}(i),i}\Big)\\
&\overset{(*_2)}{=} \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma^{-1})\cdot\prod_{i=1}^n a_{\sigma^{-1}(i),i}\Big) &&\overset{(*_3)}{=} \sum_{\sigma^{-1}\in S_n}\Big(\operatorname{sign}(\sigma^{-1})\cdot\prod_{i=1}^n a_{\sigma^{-1}(i),i}\Big)\\
&\overset{(*_3)}{=} \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n a_{\sigma(i),i}\Big) &&\overset{(*_4)}{=} \det(A^t).
\end{aligned}$$

Erläuterungen zu den einzelnen Umformungen:

$*_1$: Der Ring R ist kommutativ, so daß in einem Produkt $a_{1,\sigma(i)}\cdots a_{n,\sigma(n)}$ beliebig die Reihenfolge der Faktoren vertauscht werden darf. Damit gilt für jedes $\pi\in S_n$ die Gleichung

$$\prod_{i=1}^n a_{i,\sigma(i)} = \prod_{i=1}^n a_{\pi(i),\pi(\sigma(i))},$$

und insbesondere für $\pi := \sigma^{-1}$ dann:

$$\prod_{i=1}^n a_{i,\sigma(i)} = \prod_{i=1}^n a_{\sigma^{-1}(i),\sigma^{-1}(\sigma(i))} = \prod_{i=1}^n a_{\sigma^{-1}(i),i}.$$

$*_2$: Für den Gruppenhomomorphismus $\operatorname{sign}\colon S_n \longrightarrow \{\pm 1\}$ gilt:

$$1 = \operatorname{sign}(\mathrm{id}) = \operatorname{sign}(\sigma\circ\sigma^{-1}) = \underbrace{\operatorname{sign}(\sigma)}_{\in\{\pm1\}}\cdot\underbrace{\operatorname{sign}(\sigma^{-1})}_{\in\{\pm1\}} \quad\Longrightarrow\quad \operatorname{sign}(\sigma) = \operatorname{sign}(\sigma^{-1}).$$

$*_3$: Die Abbildung $S_n \longrightarrow S_n$ mit $\sigma\mapsto\sigma^{-1}$ ist eine Bijektion, so daß der Wechsel des Summenindex genau die gleichen Summanden liefert.

$*_4$: Ist $(b_{i,j})$ die Transponierte von A, so gilt

$$\det(A^t) = \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n b_{i,\sigma(i)}\Big).$$

Da für die Transponierte $(b_{i,j})$ von $(a_{i,j})$ aber die Beziehung $b_{i,j} = a_{j,i}$ gilt, folgt $b_{i,\sigma(i)} = a_{\sigma(i),i}$ und

$$\det(A^t) = \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n b_{i,\sigma(i)}\Big) = \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^n a_{\sigma(i),i}\Big). \qquad \square$$

Eine weitere Eigenschaft der Determinante, die weniger eine konkrete Berechnungshilfe ist, sondern eher für spätere tiefere Sätze gebraucht wird:

Lemma 3.3.21. *Sei R ein kommutativer Ring mit Eins. Es seien folgende $n+1$ Zeilenvektoren des R^n gegeben mit einem $k\in\{1,\dots,n\}$:*

$$z_1,\dots,z_{k-1},\widetilde{z}_k,\hat{z}_k,z_{k+1},\dots z_n \in R^n.$$

Weiter seien $A, A_1, A_2 \in \mathrm{Mat}_n(R)$ diejenigen Matrizen, deren n Zeilen folgendermaßen aus den gegebenen Vektoren bestehen:

A_1 enthält die Zeilen $z_1,\dots,z_{k-1},\widetilde{z}_k,z_{k+1},\dots,z_n$,

A_2 enthält die Zeilen $z_1, \dots, z_{k-1}, \hat{z}_k, z_{k+1}, \dots, z_n$,
A enthält die Zeilen $z_1, \dots, z_{k-1}, \widetilde{z}_k + \hat{z}_k, z_{k+1}, \dots, z_n$.

Also sind alle Matrizen A, A_1, A_2 bis auf die k-te Zeile gleich, und A enthält in der k-ten Zeile die Summe der k-ten Zeile aus A_1 und der k-ten Zeile aus A_2. Dies sei schematisch dargestellt durch:

$$A_1 = \begin{pmatrix} \text{———} & z_1 & \text{———} \\ & \vdots & \\ \text{———} & \widetilde{z}_k & \text{———} \\ & \vdots & \\ \text{———} & z_n & \text{———} \end{pmatrix}, \qquad A_2 = \begin{pmatrix} \text{———} & z_1 & \text{———} \\ & \vdots & \\ \text{———} & \hat{z}_k & \text{———} \\ & \vdots & \\ \text{———} & z_n & \text{———} \end{pmatrix},$$

$$A = \begin{pmatrix} \text{———} & z_1 & \text{———} \\ & \vdots & \\ \text{———} & \widetilde{z}_k + \hat{z}_k & \text{———} \\ & \vdots & \\ \text{———} & z_n & \text{———} \end{pmatrix}$$

Die k-te Zeile von A entspricht der Summe der k-ten Zeile von A_1 und der k-ten Zeile von A_2.

Dann gilt:

$$\det(A) = \det(A_1) + \det(A_2).$$

Beweis.
Die Matrizen A, A_1 und A_2 haben folgende Koeffizienten:

$$(a_{i,j}) := A, \quad (\widetilde{a}_{i,j}) := A_1, \quad \text{und} \quad (\hat{a}_{i,j}) := A_2.$$

Es gilt dann folgende Beziehung zwischen den Koeffizienten der Matrizen:

$$a_{i,j} = \widetilde{a}_{i,j} = \hat{a}_{i,j} \quad \text{für } i \neq k, \tag{$*_1$}$$
$$a_{k,j} = \widetilde{a}_{k,j} + \hat{a}_{k,j}. \tag{$*_2$}$$

Damit folgt dann für die Determinante von A:

$$\begin{aligned}
\det(A) &= \sum_{\sigma \in S_n} \Big(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \Big) = \sum_{\sigma \in S_n} \Big(\operatorname{sign}(\sigma) \cdot a_{k,\sigma(k)} \cdot \prod_{\substack{i=1 \\ i \neq k}}^{n} a_{i,\sigma(i)} \Big) \\
&\overset{(*_2)}{=} \sum_{\sigma \in S_n} \Big(\operatorname{sign}(\sigma) \cdot (\widetilde{a}_{k,\sigma(k)} + \hat{a}_{k,\sigma(k)}) \cdot \prod_{\substack{i=1 \\ i \neq k}}^{n} a_{i,\sigma(i)} \Big) \\
&= \sum_{\sigma \in S_n} \Big(\operatorname{sign}(\sigma) \cdot \widetilde{a}_{k,\sigma(k)} \cdot \prod_{\substack{i=1 \\ i \neq k}}^{n} a_{i,\sigma(i)} + \operatorname{sign}(\sigma) \cdot \widetilde{a}_{k,\sigma(k)} \cdot \prod_{\substack{i=1 \\ i \neq k}}^{n} a_{i,\sigma(i)} \Big)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\widetilde{a}_{k,\sigma(k)}\cdot\prod_{\substack{i=1\\ i\neq k}}^{n} a_{i,\sigma(i)}\Big) + \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\hat{a}_{k,\sigma(k)}\cdot\prod_{\substack{i=1\\ i\neq k}}^{n} a_{i,\sigma(i)}\Big)\\
&\overset{(*_1)}{=} \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\widetilde{a}_{k,\sigma(k)}\cdot\prod_{\substack{i=1\\ i\neq k}}^{n} \widetilde{a}_{i,\sigma(i)}\Big) + \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\hat{a}_{k,\sigma(k)}\cdot\prod_{\substack{i=1\\ i\neq k}}^{n} \hat{a}_{i,\sigma(i)}\Big)\\
&= \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n} \widetilde{a}_{i,\sigma(i)}\Big) + \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n} \hat{a}_{i,\sigma(i)}\Big)\\
&= \det(A_1)+\det(A_2). \qquad \square
\end{aligned}
$$

Nun folgt die angekündigte Liste von Eigenschaften der Determinante einer quadratischen Matrix:

Satz 3.3.22. *Sei R ein kommutativer Ring mit Eins und $A \in \operatorname{Mat}_n(R)$. Dann gilt für die Determinante von A:*

i.) $\det(E_n) = 1$.

ii.) *Wird in A ein Vielfaches einer Spalte zu einer anderen Spalte addiert, ändert sich die Determinante nicht. Ebenso kann ein Vielfaches einer Zeile zu einer anderen Zeile addiert werden, ohne die Determinante zu ändern.*

iii.) *Werden in A zwei Spalten vertauscht, ändert sich das Vorzeichen der Determinante (bzw. sie wird mit -1_R multipliziert). Gleiches gilt für ein Vertauschen von Zeilen.*

iv.) *Wird in A eine Spalte mit dem Faktor $\alpha \in R$ multipliziert, muß auch die Determinante mit α multipliziert werden. Gleiches gilt analog für eine Zeile.*

v.) *Für $\alpha \in R$ gilt:*

$$\det(\alpha\cdot A) = \alpha^n\cdot\det(A).$$

vi.) *Es gilt* $\det(A) = \det(A^t)$.

vii.) *Besitzt A zwei gleiche Spalten oder Zeilen, so gilt* $\det(A) = 0$.

viii.) *Besitzt A eine Nullspalte oder eine Nullzeile, so gilt* $\det(A) = 0$.

ix.) *Ist eine Spalte von A eine Linearkombination der anderen Spalten von A, so gilt* $\det(A) = 0$. *Dies gilt auch, wenn eine Zeile von A eine Linearkombination der andern Zeilen ist.*

x.) *Sind die Spalten von A linear abhängig, so ist* $\det(A)$ *ein Nullteiler in R. Dies gilt auch, wenn die Zeilen von A linear abhängig sind:*

$$\textit{Spalten oder Zeilen von } A \textit{ linear abhängig} \quad\Longrightarrow\quad \det(A) \textit{ Nullteiler in } R.$$

Ist dabei R ein Körper, so ist der einzige Nullteiler in R die Null, und aus der linearen Abhängigkeit der Spalten oder der Zeilen folgt dann $\det(A) = 0$.

xi.) *Ist* $\det(A)$ *kein Nullteiler in R, so sind jeweils die Spalten und die Zeilen von A linear unabhängig:*

$$\det(A) \textit{ kein Nullteiler in } R \quad\Longrightarrow\quad \textit{Spalten oder Zeilen von } A \textit{ linear unabhängig.}$$

Ist dabei R ein Körper, so sind die Spalten von A eine Basis des $R^{[n]}$, und die Zeilen von A sind eine Basis des R^n:

$$\begin{aligned}
R \textit{ Körper:} \qquad \det(A)\neq 0 &\iff \textit{Spalten von } A \textit{ Basis des } R^{[n]}\\
&\iff \textit{Zeilen von } A \textit{ Basis des } R^n.
\end{aligned}$$

xii.) Ist A invertierbar, so ist $\det(A)$ eine Einheit in R:

$$A \text{ invertierbar} \quad \Longrightarrow \quad \det(A) \in R^*.$$

Dabei gilt:

$$\det(A^{-1}) = \big(\det(A)\big)^{-1} = \frac{1}{\det(A)}.$$

Ist dabei R ein Körper, so sind alle Elemente aus R außer der Null Einheiten, und es gilt sogar die Äquvialenz:

$$R \text{ Körper:} \quad A \text{ invertierbar} \quad \Longleftrightarrow \quad \det(A) \neq 0.$$

xiii.) Ist A eine obere oder untere Dreiecksmatrix, so ist die Determinante von A das Produkt der Diagonalelemente von A.

xiv.) Kann A mit dem Gauß-Algorithmus in Zeilen-Stufen-Form R gebracht werden, und ist k die Anzahl der dazu nötigen Zeilenvertauschungen, so gilt:

$$\det(A) = (-1)^k \cdot \det(R) = (-1)^k \cdot \prod_{i=1}^{n} r_{i,i}$$

mit den Diagonalelementen $r_{i,i}$ von R.

xv.) Sind $A_1, A_2 \in \mathrm{Mat}_n(R)$ Matrizen, so daß für ein $k \in \{1, \ldots, n\}$ gilt:

- *A_1 und A_2 haben die gleichen Spalten wie A bis auf die k-te Spalte.*
- *Die k-te Spalte von A ist die Summe der k-ten Spalte von A_1 und der k-ten Spalte von A_2.*

Dann gilt für $\det(A)$:

$$\det(A) = \det(A_1) + \det(A_2).$$

Die Aussage gilt analog für Zeilen von A (siehe Lemma 3.3.21).

Beweis.

i.) Bemerkung 3.3.5.

ii.) Die Addition des λ-fachen der j-ten Zeile zur i-ten Zeile von A und die Addition des λ-fachen der i-ten Spalte zur j-ten Spalte von A durch folgende Matrizenmultiplikationen realisiert werden (siehe Satz 3.2.7).

$L_{i,j}(\lambda)A$: Addition des λ-fachen der j-ten Zeile zur i-ten Zeile von A,

$AL_{i,j}(\lambda)$: Addition des λ-fachen der i-ten Spalte zur j-ten Spalte von A.

In beiden Fällen liefert der Determinantenmultiplikationssatz 3.3.8 zusammen mit $\det\big(L_{i,j}(\lambda)\big) = 1$ (Beispiel 3.3.5), daß sich die Determinante bei dieser Manipulation von A nicht ändert:

$$\underbrace{\det\big(L_{i,j}(\lambda)A\big)}_{\text{Zeilenoperation auf } A} \overset{(3.3.8)}{=} \underbrace{\det\big(L_{i,j}(\lambda)\big)}_{=1} \cdot \det(A) = \det(A),$$

$$\underbrace{\det\big(AL_{i,j}(\lambda)\big)}_{\text{Spaltenoperation auf } A} \overset{(3.3.8)}{=} \det(A) \cdot \underbrace{\det\big(L_{i,j}(\lambda)\big)}_{=1} = \det(A).$$

iii.) Das Vertauschen von Spalten und Zeilen von A kann durch folgende Matrizenmultiplikationen realisiert werden (siehe Satz 3.2.7):

$P_{i,j}A$ Vertauschen der i-ten und j-ten Zeile von A,

$$AP_{i,j} \quad \text{Vertauschen der } i\text{-ten und } j\text{-ten Spalte von } A.$$

Mit dem Determinantenmultiplikationssatz 3.3.8 und $\det(P_{i,j}) = -1$ (siehe Beispiel 3.3.14) folgt dann die Aussage:

$$\underbrace{\det(P_{i,j}A)}_{\text{Zeilenoperation auf } A}, \overset{(3.3.8)}{=} \underbrace{\det(P_{i,j})}_{=-1} \cdot \det(A) = -\det(A),$$

$$\underbrace{\det(AP_{i,j})}_{\text{Spaltenoperation auf } A} \overset{(3.3.8)}{=} \det(A) \cdot \underbrace{\det(P_{i,j})}_{=-1} \overset{(R \text{ komm.})}{=} -\det(A).$$

iv.) Das Multiplizieren einer Spalte oder Zeile von A mit einem Faktor α kann durch folgende Matrizenmultiplikation realisert werden (siehe Satz 3.2.7):

$$D_i(\alpha)A \quad \text{Multiplizieren der } i\text{-ten Zeile von } A \text{ mit } \alpha,$$
$$AD_i(\alpha) \quad \text{Multiplizieren der } i\text{-ten Spalte von } A \text{ mit } \alpha.$$

Mit dem Determinantenmultiplikationssatz 3.3.8 und $\det\big(D_i(\alpha)\big) = \alpha$ (siehe Beispiel 3.3.5) folgt dann die Aussage:

$$\underbrace{\det\big(D_i(\alpha)A\big)}_{\text{Zeilenoperation auf } A} \overset{(3.3.8)}{=} \underbrace{\det\big(D_i(\alpha)\big)}_{=\alpha} \cdot \det(A) = \alpha \cdot \det(A),$$

$$\underbrace{\det\big(AD_i(\alpha)\big)}_{\text{Spaltenoperation auf } A} \overset{(3.3.8)}{=} \det(A) \cdot \underbrace{\det\big(D_i(\alpha)\big)}_{=\alpha} \overset{(R \text{ komm.})}{=} \alpha \cdot \det(A).$$

v.) Es gilt $\alpha \cdot A = (\alpha \cdot E_n) \cdot A$, und mit $\det(\alpha \cdot E_n) = \alpha^n$ (Beispiel 3.3.5) und dem Determinantenmultiplikationssatz 3.3.8:

$$\det(\alpha \cdot A) = \det\big((\alpha \cdot E_n) \cdot A\big) \overset{(3.3.8)}{=} \underbrace{\det(\alpha \cdot E_n)}_{=\alpha^n} \cdot \det(A) = \alpha^n \cdot A.$$

Ein weiterer Beweis wäre der folgende: $\alpha \cdot A$ bedeuteutet, daß alle n Zeilen bzw. alle n Spalten von A mit dem Faktor α multipliziert werden, so daß n-maliges Anwenden der vorherigen Aussage auch das gewünschte Ergebnis liefert.

vi.) Lemma 3.3.20.

vii.) Lemma 3.3.7 liefert die Aussage für Zeilen. Die Aussage für Spalten folgt dann mit $\det(A) = \det(A^t)$, denn beim Transponieren von A werden Zeilen zu Spalten und umgekehrt:

$$A \text{ hat zwei gleiche Spalten} \quad \Longrightarrow \quad A^t \text{ hat zwei gleiche Zeilen}$$
$$\Longrightarrow \quad \det(A^t) = 0 \quad \Longrightarrow \quad \det(A) = 0.$$

viii.) Für $n = 1$ ist A mit einer Nullzeile oder Nullspalte die Nullmatrix, und diese hat offensichtlich die Determinante Null (Leibniz-Formel 3.3.1). Ist für $n \geq 2$ die i-te Zeile oder i-te Spalte Null, so gibt es einen weiteren Index $1 \leq i \neq j \leq n$, und mit $L_{i,j}(1) \cdot A$ oder $AL_{j,i}(1)$ wird die j-te Zeile oder Spalte in die i-te kopiert, so daß A zwei gleiche Zeilen oder Spalten hat und damit nach vorheriger Aussage die Determinante Null.

ix.) Sei die k-te Zeile z_k von A eine Linearkombination der anderen Zeilen z_i von A:

$$z_k = \sum_{\substack{i=1\\ i\neq k}}^{n} \lambda_i z_i \qquad \Longrightarrow \qquad z_k - \sum_{\substack{i=1\\ i\neq k}}^{n} \lambda_i z_i = 0.$$

Dann kann jeweils die λ_i-fache der i-ten Zeile von der k-ten Zeile abgezogen werden, ohne daß sich die Determinante ändert, und es entsteht eine Matrix mit einer Nullzeile, die dann die Determinante Null hat.
Analog kann mit der Aussage über die Spalten verfahren werden.
Mit $\det(A) = \det(A^t)$ kann die Aussage über Spalten auch auf die über Zeilen zurückgeführt werden.

x.) Es seien $z_1, \ldots, z_n$ die Zeilen von A. Sind diese linear abhängige, so gibt es Koeffizienten $\lambda_i \in R$ mit einem $\lambda_k \neq 0$ mit:

$$\sum_{i=1}^{n} \lambda_i z_i = 0 \qquad \Longrightarrow \qquad \lambda_k z_k = -\sum_{\substack{i=1\\ i\neq k}}^{n} \lambda_i z_i.$$

Wird dann die k-te Zeile von A mit dem Faktor λ_k multipliziert, und für $i \neq k$ jeweils das λ_i-fache der i-ten Zeile von der k-ten abgezogen, so entsteht eine Matrix mit einer Nullzeile und der Determinante Null:

$$\det\Big(\prod_{\substack{i=1\\ i\neq k}}^{n} L_{k,i}(-\lambda_i) \cdot D_k(\lambda_k) \cdot A\Big) = 0.$$

Es gilt $\det\big(L_{k,i}(-\lambda_i)\big) = 1$ und $\det\big(D_k(\lambda_k)\big) = \lambda_k$, und es folgt dann mit dem Determinantenmultiplikationssatz 3.3.8:

$$\lambda_k \cdot \det(A) \overset{(3.3.8)}{=} \det\Big(\prod_{\substack{i=1\\ i\neq k}}^{n} L_{k,i}(-\lambda_i) \cdot D_k(\lambda_k) \cdot A\Big) = 0 \qquad \Longrightarrow \qquad \det(A) \text{ Nullteiler.}$$

Analog kann mit der Aussage über die Spalten verfahren werden.

xi.) Die erste Implikation ist nur die logische Negation der vorherigen Aussage.
Zu dem Fall, daß R ein Körper ist:

$\det(A) \neq 0 \Longrightarrow$ Spalten von A Basis des $R^{[n]}$: Mit $\det(A) \neq 0$ ist die Determinante von A im Körper R eine Einheit und damit nach Lemma 1.3.13 kein Nullteiler, womit die Spalten von A nach vorheriger Aussage linear unabhängig sind. Die n Spalten von A sind dann im Vektorraum $R^{[n]}$ (R Körper!) sogar ein maximal linear unabhängiges System und damit eine Basis.

Spalten von A Basis des $R^{[n]} \Longrightarrow \det(A) \neq 0$: Sind die Spalten von A ein Basis des Vektorraumes $R^{[n]}$, so sind sie linear unabhängig und A hat den Rang n. Dann ist A nach Satz 3.2.22 invertierbar und $\det(A)$ nach Satz 3.3.10 eine Einheit in R, also ungleich Null.

Spalten von A Basis des $R^{[n]} \Longleftrightarrow$ Zeilen von A Basis des R^n: Da in einem Vektorraum maximal linear unabhängige Systeme Basen sind, gelten offensichtlich die beiden folgenden Äquivalenzen:

$$\begin{aligned} \text{Spalten von } A \text{ sind eine Basis des } R^{[n]} \quad &\Longleftrightarrow \quad \text{Spaltenrang von } A \text{ ist } n, \\ \text{Zeilen von } A \text{ sind eine Basis des } R^{n} \quad &\Longleftrightarrow \quad \text{Zeilenrang von } A \text{ ist } n. \end{aligned}$$

Dann folgt die Behauptung sofort aus Satz 3.2.17:

$$\text{Zeilenrang} = \text{Spaltenrang} = \text{Rang}.$$

xii.) Die erste Implikation ist Bemerkung 3.3.9 gezeigt.
Die Aussage im Falle eines Körpers folgt sofort aus der vorherigen Aussage und Lemma 3.1.17 sowie Satz 3.1.20:

$$\begin{aligned} \det(A) \neq 0 \quad &\Longleftrightarrow \quad \text{Spalten von } A \text{ Basis des } R^{[n]} \\ &\overset{3.1.17}{\Longleftrightarrow} \quad \varphi_A \text{ injektiv} \\ &\overset{3.1.20}{\Longleftrightarrow} \quad A \text{ invertierbar.} \end{aligned}$$

xiii.) Lemma 3.3.4.
xiv.) Satz 3.3.15.
xv.) Lemma 3.3.21. □

Bemerkung 3.3.23.

i.) In obigen Regeln für die Determinante sind zwei ähnlich klingende Aussagen formuliert:

$$\left.\begin{array}{l}\textit{Eine Spalte von } A \textit{ ist eine Linearkombination der anderen Spalten}\end{array}\right\} \quad \Longrightarrow \quad \det(A) = 0,$$

$$\textit{Die Spalten von } A \textit{ sind linear abhängig} \quad \Longrightarrow \quad \det(A) \textit{ Nullteiler in } R.$$

Die Forderung, daß eine Spalte als Linearkombination der anderen Spalten geschrieben werden kann, ist eine Verschärfung der Aussage, daß die Spalten linear abhängig sind:

$$s_k = \sum_{\substack{i=1\\ i\neq k}}^{n} \lambda_i s_i \quad \Longrightarrow \quad \sum_{i=1}^{n} \lambda_i s_i = 0 \textit{ mit } \lambda_k = -1 \neq 0.$$

Aus der linearen Abhängigkeit der Spalten folgt nur, daß ein Vielfaches einer Spalte eine Linearkombination der anderen Spalten ist:

$$\sum_{i=1}^{n} \lambda_i s_i = 0 \textit{ mit } \lambda_k \neq 0 \quad \Longrightarrow \quad \lambda_k s_k = -\sum_{\substack{i=1\\ i\neq k}}^{n} \lambda_i s_i.$$

Über einem Köper sind beide Aussagen äquivalent, da dann jedes $\lambda_k \neq 0$ eine Einheit ist, durch die geteilt werden kann, so daß die Spalte s_k auch eine Linearkombination der anderen Spalten ist.

ii.) Die Determinante bietet eine Möglichkeit, Spalten- oder Zeilenvektoren auf lineare Unabhängigkeit zu testen. Allerdings muß die aus den Vektoren zusammengesetzte Matrix quadratisch sein, so daß z.B. im R^3 mit der Determinante immer nur drei Vektoren auf lineare Unabhängigkeit getestet werden können.
Bei Vektorräumen (d.h. R Körper) ist damit immer gleich ein Basistest verbunden, denn darin sind maximal linear unabhängige Systeme gleich Basen.

iii.) Bei der obigen Liste fehlt noch eine wesentliche Aussage:

$$\det(A) \textit{ Einheit} \quad \Longrightarrow \quad A \textit{ invertierbar.}$$

Bisher ist nur die Umkehrung davon bewiesen. Die noch fehlende Impliktion wird bald mit der Cramerschen Regel bewiesen. □

Einige der Determinanteneigenschaften aus Satz 3.3.22 zeigen, daß die Determinantenfunktion eine spezielle „alternierende Multilinearform“ ist, was oft als alternative Definition einer Determinante verwendet wird. Dies soll kurz beleuchtet werden, wozu der obige Begriff ersteinmal definiert werden muß:

Definition 3.3.24. *Sei R ein kommutativer Ring mit Eins und M ein R-Modul. Eine Abbildung*

$$b\colon \underbrace{M \times \ldots \times M}_{n\text{-mal}} \longrightarrow R$$

heißt n-fache Multilinearform, falls sie linear in jeder der n Komponenten ist, d.h. es muß bzgl. jeder Komponente $1 \leq i \leq n$ gelten:

$$\begin{aligned} b(m_1, \ldots, m_{i-1}, m_i + \widetilde{m}_i, m_{i+1}, \ldots, m_n) = \quad & b(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n) \\ & + b(m_1, \ldots, m_{i-1}, \widetilde{m}_i, m_{i+1}, \ldots, m_n), \\ b(m_1, \ldots, m_{i-1}, r \cdot m_i, m_{i+1}, \ldots, m_n) = \; & r \cdot b(m_1, \ldots, m_{i-1}, m_i, m_{i+1}, \ldots, m_n). \end{aligned}$$

Für $n = 2$ heißt eine solche Abbildung auch Bilinearform
Wird anstelle des Wertebereichs R ein beliebiger anderer R-Modul N gewählt, so heißt eine Abbildung

$$b\colon \underbrace{M \times \ldots \times M}_{n\text{-mal}} \longrightarrow N$$

mit obigen Eigenschaften (linear in jeder Komponente) n-fach multilineare Abbildung bzw. bilineare Abbildung. Multilinearformen sind somit spezielle multilineare Abbildungen mit dem spezifischen Wertebereich R (als R-Modul).
Abkürzend wird auch nur von einer multilinearen Abbildung bzw. Multilinearform geredet, wenn die Anzahl der Komponenten klar ist.

Für $n \geq 2$ heißt eine multilineare Abbildung:

$$b\colon \underbrace{M \times \ldots \times M}_{n\text{-mal}} \longrightarrow N$$

symmetrisch, wenn für jedes $\pi \in S_n$ gilt:

$$b(m_1, \ldots, m_n) = b(m_{\pi(1)}, \ldots, m_{\pi(n)}).$$

Die multilineare Abbildung b heißt alternierend, falls zwei gleiche Parameter immer den Wert 0 implizieren, d.h. es gilt für $1 \leq i < j \leq n$:

$$m_i = m_j \quad \Longrightarrow \quad b(\ldots, m_i, \ldots, m_j, \ldots) = 0. \qquad \square$$

Bemerkung 3.3.25. *Die „Linearität in jeder Komponente“ bei einer multilinearen Abbildung liefert z.B. bei einer bilinearen Abbildung:*

$$b(\alpha \cdot v, \beta \cdot w) = \alpha \cdot b(v, \beta \cdot w) = (\alpha\beta) \cdot b(v, w).$$

Noch der Definition gilt dann bei einer bilinearen Abbildung ganz allgemein:

$$\begin{aligned} b(\alpha \cdot v + \widetilde{\alpha} \cdot \widetilde{v}, \beta \cdot w + \widetilde{\beta} \cdot \widetilde{w}) &= b(\alpha \cdot v, \beta \cdot w + \widetilde{\beta} \cdot \widetilde{w}) + b(\widetilde{\alpha} \cdot \widetilde{v}, \beta \cdot w + \widetilde{\beta} \cdot \widetilde{w}) \\ &= \quad b(\alpha \cdot v, \beta \cdot w) + b(\alpha \cdot v, \widetilde{\beta} \cdot \widetilde{w}) \\ &\quad + b(\widetilde{\alpha} \cdot \widetilde{v}, \beta \cdot w) + b(\widetilde{\alpha} \cdot \widetilde{v}, \widetilde{\beta} \cdot \widetilde{w}) \\ &= \quad (\alpha\beta) \cdot b(v, w) + (\alpha\widetilde{\beta}) \cdot b(v, \widetilde{w}) \end{aligned}$$

$$+ (\widetilde{\alpha}\beta) \cdot b(\widetilde{v}, w) + (\widetilde{\alpha}\widetilde{\beta}) \cdot b(\widetilde{v}, \widetilde{w}).$$

Es muß also jedesmal „pro“ Komponente aufgelöst werden, wobei sich bei der Bearbeitung einer Komponente die anderen kopieren! □

Beispiel 3.3.26.

i.) Sei R ein kommutativer Ring mit Eins. Dann ist die Ringmultiplikation eine symmetrische bilineare Abbildung bzw. sogar eine symmetrische Bilinearform (Übung!):

$$R \times R \longrightarrow R \quad \textit{mit} \quad (a, b) \mapsto a \cdot b.$$

ii.) Sei R ein kommutativer Ring mit Eins. Dann ist für $n \in \mathbb{N}$ die folgende Abbildung eine symmetrische Bilinearform (Übung!):

$$\langle \cdot, \cdot \rangle \colon R^n \times R^n \longrightarrow R \quad \textit{mit} \quad \big((x_1, \ldots, x_n), (y_1, \ldots, y_n) \big) \mapsto \sum_{i=1}^{n} x_i \cdot y_i.$$

iii.) Für den $\mathbb{R}$-Vektorraum $\mathcal{C}^0(\mathbb{R})$ der stetigen Abbildungen von $\mathbb{R}$ nach $\mathbb{R}$ ist die folgende Abbildung für $a, b \in \mathbb{R}$ mit $a < b$ eine symmetrische Bilinearform (Übung!):

$$b_{a,b} \colon \mathcal{C}^0(\mathbb{R}) \times \mathcal{C}^0(\mathbb{R}) \longrightarrow \mathbb{R} \quad \textit{mit} \quad (f, g) \mapsto \int_a^b f(x) \cdot g(x) dx.$$

Dies gilt selbstverständlich auch für den $\mathbb{R}$-Vektorraum $\mathcal{I}_{a,b}(\mathbb{R})$ der auf dem Intervall $[a, b]$ Riemann-integrierbaren Abbildungen. Siehe dazu auch Beispiel 2.1.4 und Beispiel 2.1.18. □

Nun soll die Determinantenfunktion als multilineare Abbildung betrachtet werden. Bisher war sie für eine quadratische Matrix definiert, aber eine $(n \times n)$-Matrix kann als Ansammlung von n Spalten aus dem $R^{[n]}$ oder n Zeilen aus dem R^n aufgefaßt werden, so daß folgende Konstruktionen möglich sind:

Satz 3.3.27. *Sei R ein kommutativer Ring mit Eins. Es seien folgende Abbildungen definiert:*

$$D_Z \colon \underbrace{R^n \times \ldots \times R^n}_{n\text{-mal}} \longrightarrow R \quad \textit{mit} \quad (x_1, \ldots, x_n) \mapsto \det \begin{pmatrix} — & x_1 & — \\ & \vdots & \\ — & x_n & — \end{pmatrix}$$

und

$$D_S \colon \underbrace{R^{[n]} \times \ldots \times R^{[n]}}_{n\text{-mal}} \longrightarrow R \quad \textit{mit} \quad (x_1, \ldots, x_n) \mapsto \det \begin{pmatrix} | & & | \\ x_1 & \cdots & x_n \\ | & & | \end{pmatrix}.$$

Dann sind die beiden Abbildungen D_Z und D_S alternierende n-Multilinearformen, die für die Standard-Basis-Vektoren $e_1, \ldots, e_n$ der jeweiligen Räume den Wert Eins annehmen, d.h. es gilt:

$$D_Z(e_1, \ldots, e_n) = D_S(e_1, \ldots, e_n) = 1.$$

Dies bedeutet, daß die Determinanenfunktion bzgl. der Spalten und bzgl. der Zeilen einer Matrix eine alternierende n-Multilinearform ist.

Beweis.
Die Eigenschaften von D_Z und D_S sind durch die Eigenschaften der Determinantenfunktion bzgl. Zeilen- und Spaltenmanipulation gegeben und in Satz 3.3.22 bewiesen. □

Bemerkung 3.3.28. *Sei R ein kommutativer Ring mit Eins. Die Konstruktion aus Satz 3.3.27 kann auch umgedreht werden: Ist*

$$\delta\colon \underbrace{R^n \times \ldots \times R^n}_{n\text{-}mal} \longrightarrow R$$

eine (alternierende) Multilinearform, so kann daraus eine Abbildung von $\mathrm{Mat}_n(R)$ nach R konstruiert werden, indem die n Zeilen einer Matrix in δ eingesetzt werden, um der Matrix einen Wert zuzuweisen:

$$D_\delta\colon \mathrm{Mat}_n(r) \longrightarrow R \quad \textit{mit} \quad A \mapsto \delta(z_1, \ldots, z_n) \quad \textit{und} \quad A = \begin{pmatrix} — & z_1 & — \\ & \vdots & \\ — & z_n & — \end{pmatrix}.$$

Ebenso könnte eine alternierende n-Multilinearform auf $R^{[n]}$ betrachtet werden, um darin dann die Spalten einer Matrix einzusetzen.
Es gilt nun folgende Aussage (die hier nicht bewiesen wird):

Satz: *Ist R ein kommutativer Ring mit Eins, so existiert je genau eine alternierende n-Multilinearform δ auf dem R^n bzw. $R^{[n]}$, die auf den Standard-Basis-Vektoren $e_1, \ldots, e_n$ des jeweiligen Raumes den Wert Eins annimmt:*

$$\delta(e_1, \ldots, e_n) = 1.$$

Für diese spezielle „normierte“ alternierende n-Multilinearform δ gilt dann mit obiger Konstruktion (entweder über Zeilen oder Spalten):

$$D_\delta = \det.$$

Dies liefert eine alternative Möglichkeit, die Determinante einer Matrix zu definieren (strenggenommen sogar zwei Möglichkeiten: über die Zeilen oder die Spalten).
Wird dieser Weg gewählt, sind schon viele Eigenschaften der Determinantenfunktion aus Satz 3.3.22 per Definition erfüllt, aber es muß eben vorher die Existenz und Eindeutigkeit der alternierenden n-Multilinearform δ aus obigem Satz gezeigt werden. Eine ausführliche „allgemeine“ Diskussion obigen Satzes für Ringe und Moduln findet sich z.B. in dem Buch [**SSAlg1**, §45-§47]. □

Als nächstes soll die Cramersche Regel hergeleitet werden, die wichtige Aussagen über die Determinantenfunktion erlaubt. Dazu ist zuerst folgende Definition nötig:

Definition 3.3.29. *Sei R ein kommutativer Ring mit Eins. Dann seien für $n \geq 2$ zu der quadratischen Matrix $A := (a_{i,j}) \in \mathrm{Mat}_n(R)$ folgende Matrizen definiert:*

$$A[i,j] := \text{Streichen der } i\text{-ten Zeile und } j\text{-ten Spalte von } A,$$

$$A^{ad} := \Big((-1)^{i+j} \cdot \det\big(A[i,j]\big)\Big)^t_{(i,j)\in I_{n,n}} = \Big((-1)^{i+j} \cdot \det\big(A[j,i]\big)\Big)_{(i,j)\in I_{n,n}}.$$

Die Matrix A^{ad} heißt die adjungierte Matrix zu A.
Weiter sei zu A definiert:

$$A_{e_i,e_j} := \begin{pmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{pmatrix}.$$

□

Bemerkung 3.3.30.

i.) Von den Matrizen aus Definition 3.3.29 ist vor allem die adjungierte Matrix A^{ad} zu einer Matrix A von Interesse. Die beiden anderen Matrizendefinitionen sind technischer Natur, wobei die Matrizen $A[i,j]$ ja zur Definition der adjungierten Matrix benutzt werden.

ii.) Für die Matrizen $A[i,j]$ und A_{e_i,e_j} aus Definition 3.3.29 gelten offensichtlich folgende Aussagen:
- *Die Matrix $A[i,j]$ liegt in $\mathrm{Mat}_{n-1}(R)$.*
- *Die Matrizen A^{ad} und A_{e_i,e_j} liegen in $\mathrm{Mat}_n(R)$.*
- *Die Matrix A_{e_i,e_j} entsteht aus A, indem die i-te Zeile aus A durch den Zeilen-Standard-Basis-Vektor e_j ersetzt wird und die j-te Spalte von A durch den Spalten-Standard-Basis-Vektor e_i.*
- *Es gilt $(A_{e_i,e_j})[i,j] = A[i,j]$.*

iii.) Aus der Definition der Adjungierten zu A ergibt sich:

$$\big(A^{ad}\big)^t = \big(A^t\big)^{ad}.$$

□

Beispiel 3.3.31.

i.) Es sei folgende Matrix gegeben:

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Dann ergeben sich folgende Matrizen $A[i,j]$ aus Definition 3.3.29:

$$A[1,1] = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}, \qquad A[1,2] = \begin{pmatrix} 4 & 6 \\ 7 & 9 \end{pmatrix}, \qquad A[1,3] = \begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix},$$

$$A[2,1] = \begin{pmatrix} 2 & 3 \\ 8 & 9 \end{pmatrix}, \qquad A[2,2] = \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix}, \qquad A[2,3] = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix},$$

$$A[3,1] = \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix}, \qquad A[3,2] = \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \qquad A[3,3] = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}.$$

Dies liefert dann folgende adjungierte Matrix zu A:

$$A^{ad} = \begin{pmatrix} \det\big(A[1,1]\big) & -\det\big(A[2,1]\big) & \det\big(A[3,1]\big) \\ -\det\big(A[1,2]\big) & \det\big(A[2,2]\big) & -\det\big(A[3,2]\big) \\ \det\big(A[1,3]\big) & -\det\big(A[2,3]\big) & \det\big(A[3,3]\big) \end{pmatrix} = \begin{pmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{pmatrix}.$$

ii.) Ein weiteres Beispiel ist:

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \Longrightarrow \qquad A^{ad} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

und es gilt:

$$A_{e_1,e_1} = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \quad A_{e_1,e_2} = \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix}, \quad A_{e_2,e_1} = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \quad A_{e_2,e_2} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}. \qquad \square$$

Zum Beweis der Cramerschen Regel müssen zuerst drei technische Aussagen bewiesen werden:

Lemma 3.3.32. *Sei R ein kommutativer Ring mit Eins. Weiter sei $A \in \mathrm{Mat}_n(A)$. Dann gilt:*

$$\det\big(A_{e_i,e_j}\big) = (-1)^{i+j} \cdot \det\big(A[i,j]\big).$$

Beweis. Der Beweis wird in zwei Schritten geführt:

1.) Schritt: Die Matrix A_{e_i,e_j} kann mit folgenden Zeilen- und Spaltenvertauschungen in Blockdiagonalmatrizenform gebracht werden:

$$P_{n-1,n} \dots P_{i+1,i+2} P_{i,i+1} A_{e_i,e_j} P_{j,j+1} P_{j+1,j+2} \dots P_{n-1,n} = \underbrace{\begin{pmatrix} A[i,j] & 0 \\ 0 & 1 \end{pmatrix}}_{=:B},$$

wobei die Null oberhalb der Eins der Nullspaltenvektor aus $R^{[n-1]}$ ist und die Null neben der Eins der Nullzeilenvektor aus R^{n-1}. Es folgt dann mit dem Determinantenmultiplikationssatz 3.3.8, da die Matrizen $P_{l,k}$ alle die Determinante „-1“ haben:

$$\begin{aligned} \det(B) &= (-1)^{n-i} \cdot \det(A_{e_i,e_j}) \cdot (-1)^{n-j} \\ &= (-1)^{2n-i-j} \cdot \det(A_{e_i,e_j}) \\ &\overset{(*)}{=} (-1)^{i+j} \cdot \det(A_{e_i,e_j}). \end{aligned}$$

Die letzte Umformung $(*)$ folgt dabei aus:

$$(-1)^{2n-i-j} \cdot (-1)^{i+j} = (-1)^{2n} = 1 \qquad \Longrightarrow \qquad (-1)^{2n-i-j} = (-1)^{i+j}.$$

Wegen $\big((-1)^{i+j}\big)^2 = 1$ gilt dann:

$$\det(B) = (-1)^{i+j} \cdot \det(A_{e_i,e_j}) \qquad \overset{\cdot(-1)^{i+j}}{\Longrightarrow} \qquad (-1)^{i+j} \cdot \det(B) = \det(A_{e_i,e_j}).$$

2.) Schritt: Nach obigen Umformungen muß nun noch gezeigt werden:

$$\det(B) = \det\big(A[i,j]\big).$$

Dazu wird zur Berechnung von $\det(B)$ die Leibniz-Formel auf $(b_{i,j}) := B$ angewendet:

$$\det(B) = \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n} b_{i,\sigma(i)}\Big).$$

Da B in der untersten Zeile bis auf die Eins in der rechten Ecke nur Nullen enthält, gilt

$$b_{n,\sigma(n)} \neq 0 \quad\Longleftrightarrow\quad \sigma(n) = n,$$

woraus sofort folgt:

$$\prod_{i=1}^{n} b_{i,\sigma(i)} \neq 0 \quad\Longleftrightarrow\quad \sigma(n) = n.$$

Wegen $b_{n,n} = 1$ ergibt sich für die Leibniz-Formel von $\det(B)$ bei $(*_1)$:

$$\det(B) = \sum_{\sigma\in S_n}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n} b_{i,\sigma(i)}\Big) \overset{(*_1)}{=} \sum_{\substack{\sigma\in S_n\\ \sigma(n)=n}}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n-1} b_{i,\sigma(i)}\Big).$$

Die Permutationen von S_n, die n als Fixpunkt haben, sind genau diejenigen (eingebetteten) aus S_{n-1}, so daß sich bei $(*_2)$ auch schreiben läßt:

$$\det(B) = \sum_{\substack{\sigma\in S_n\\ \sigma(n)=n}}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n-1} b_{i,\sigma(i)}\Big) \overset{(*_2)}{=} \sum_{\sigma\in S_{n-1}}\Big(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n-1} b_{i,\sigma(i)}\Big).$$

Damit treten bei der Berechnung von $\det(B)$ in obiger Formel nur noch Koeffizienten $b_{i,j}$ aus dem linken oberen Block $A[i,j]$ auf und es folgt das gewünschte $\det(B) = \det\big(A[i,j]\big)$. □

Bemerkung 3.3.33.
Die Gleichung von Lemma 3.3.32 liefert sofort eine weitere Identität für die Adjungierte einer Matrix A:

$$A^{ad} \overset{(Def)}{=} \big((-1)^{i+j}\cdot A[i,j]\big)^t \overset{(3.3.32)}{=} \big(\det(A_{e_i,e_j})\big)^t = \big(\det(A_{e_j,e_i})\big). \qquad \square$$

Lemma 3.3.34. *Sei R ein kommutativer Ring mit Eins. Dann gilt für $A \in \operatorname{Mat}_n(R)$ mit den Spalten $s_1,\dots,s_n$ und dem i-ten Spalten-Standard-Basis-Vektor:*

$$\det(A_{e_i,e_j}) = \det\begin{pmatrix} | & & | & | & | & & | \\ s_1 & \cdots & s_{j-1} & e_i & s_{j+1} & \cdots & s_n \\ | & & | & | & | & & | \end{pmatrix}.$$

Beweis. Die beiden Matrizen:

$$A_{e_i,e_j} \qquad \text{und} \qquad \begin{pmatrix} | & & | & | & | & & | \\ s_1 & \cdots & s_{j-1} & e_i & s_{j+1} & \cdots & s_n \\ | & & | & | & | & & | \end{pmatrix}$$

unterscheiden sich in den Spalten $s_1, \ldots, s_{j-1}$ und $s_{j+1}, \ldots, s_n$, und in diesen Spalten ist in der linken Matrix in der i-ten Zeile eine Null und in der rechten Matrix der Koeffizient $a_{i,k}$ aus $(a_{i,j}) := A$.
In der rechten Matrix kann dieser Koeffizient $a_{i,k}$ in jeder Spalte „gelöscht“ werden, indem das jeweilige $a_{i,k}$-fachen der j-ten Spalte von der k-ten Spalte abgezogen wird, da der j-te Spaltenvektor der i-te Standardbasisvektor ist und dieser bei obiger Operation nur in der i-ten Komponente der anderen Spalten etwas verändert.
Nach diesen Spaltenoperationen steht auf beiden Seiten die gleiche Matrix, und da die Spaltenoperationen die Determinante nicht ändern, folgt die Behauptung über die Determinanten der beiden Matrizen. □

Die letzte nützliche technisch Aussage zum Beweis der Cramerschen Regel ist auch vom allgemeinen Interesse:

Lemma 3.3.35. *Seien A, B Matrizen über einem kommutativen Ring R mit Eins, so daß deren Matrizenprodukt AB definiert ist. Dann ist auch das Matrizenprodukt B^tA^t definiert und es gilt:*

$$(AB)^t = B^tA^t.$$

Beweis. Sei $A \in \mathrm{Mat}(m \times n, R)$ und $B \in \mathrm{Mat}(k \times l, R)$. Damit das Matrizenprodukt AB definiert ist, muß $n = k$ gelten, und AB ist dann eine $(m \times l)$-Matrix.
Es gilt $B^t \in \mathrm{Mat}(l \times k, R)$, $A^t \in \mathrm{Mat}(n \times m, R)$, und wegen $k = n$ ist das Matrizenprodukt B^tA^t definiert und eine $(l \times m)$-Matrix.
Zu der Gleichung $(AB)^t = B^tA^t$: Es seien definiert:

$$(a_{i,j}) := A, \quad (b_{i,j}) := B, \quad (c_{i,j}) := C := AB$$

und

$$(\widetilde{a}_{i,j}) := A^t, \quad (\widetilde{b}_{i,j}) := B^t, \quad (d_{i,j}) := D := B^tA^t.$$

Es ist also die Gleichung $C^t = D$ zu zeigen und damit $c_{j,i} = d_{i,j}$:

$$c_{j,i} = \sum_{k=1}^{n} a_{j,k} \cdot b_{k,i} = \sum_{k=1}^{n} b_{k,i} \cdot a_{j,k} = \sum_{k=1}^{n} \widetilde{b}_{i,k} \cdot \widetilde{a}_{k,j} = d_{i,j}. \qquad \square$$

Nun kann die Cramersche Regel bewiesen werden:

Satz 3.3.36. *(Cramersche Regel)*
Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{Mat}_n(R)$. Dann gilt:

$$A^{ad} \cdot A = A \cdot A^{ad} = \det(A) \cdot E_n.$$

Beweis.

$A^{\mathrm{ad}} \cdot A = \det(A) \cdot E_n$: Es seien definiert:

$$(a_{i,j}) := A, \quad (b_{i,j}) := B := A^{\mathrm{ad}} \quad \text{und} \quad (c_{i,j}) := C := A^{\mathrm{ad}} \cdot A.$$

Weiter seien $s_1, \ldots, s_n$ die Spalten von A, und mit den Standard-Spalten-Basisvektoren $e_1, \ldots, e_n \in R^{[n]}$ folgt mit $s_j = \sum_{k=1}^n a_{k,j} \cdot e_k$ $(\star)$:

$$c_{i,j} = \sum_{k=1}^n b_{i,k} \cdot a_{k,j} \overset{(R \text{ komm.})}{=} \sum_{k=1}^n a_{k,j} \cdot b_{i,k} = \sum_{k=1}^n a_{k,j} \cdot \underbrace{(-1)^{i+k} \cdot A[k,i]}_{= b_{i,k}}$$

$$\overset{(3.3.32)}{=} \sum_{k=1}^n a_{k,j} \cdot \det(A_{e_k,e_i}) \overset{(3.3.34)}{=} \sum_{k=1}^n a_{k,j} \cdot \det(s_1, \ldots, s_{i-1}, e_k, s_{i+1}, \ldots, s_n)$$

$$\overset{(\star)}{=} \det(s_1, \ldots, s_{i-1}, s_j, s_{i+1}, \ldots, s_n) = \delta_{i,j} \cdot \det(A)$$

mit dem Kronecker-Symbol $\delta_{i,j}$ (Definition 2.2.27), da in der Matrix

$$(s_1, \ldots, s_{i-1}, s_j, s_{i+1}, \ldots, s_n)$$

für $j \neq i$ immer zwei gleiche Spalten sind und deren Determinante Null ist, und sie für $i = j$ genau die Matrix A ist.

Aus $c_{i,j} = \delta_{i,j} \cdot \det(A)$ folgt dann sofort $C = \det(A) \cdot E_n$, was zu zeigen war.

$A \cdot A^{\mathrm{ad}} = \det(A) \cdot E_n$: Anstelle des Matrizenproduktes AA^{ad} wird zuerst dessen Transponierte $\left(AA^{\mathrm{ad}}\right)^t$ betrachtet, und es folgt:

$$\left(AA^{\mathrm{ad}}\right)^t \overset{(3.3.35)}{=} \left((A^{\mathrm{ad}})^t A^t \overset{(3.3.30)}{=} (A^t)^{\mathrm{ad}} A^t \overset{(*)}{=} \det(A^t) \cdot E_n \overset{(3.3.20)}{=} \det(A) \cdot E_n.$$

Bei der Umformung $(*)$ wurde dabei die schon vorher bewiesene Aussage

$$A^{\mathrm{ad}} A = \det(A) \cdot E_n$$

auf die Matrix A^t angewendet. Also ist $\left(AA^{\mathrm{ad}}\right)^t$ eine Diagonalmatrix, die gleich ihrer Transponierten ist, und es folgt letztendlich:

$$\left(AA^{\mathrm{ad}}\right) = \left(\left(AA^{\mathrm{ad}}\right)^t\right)^t = \left(\det(A) \cdot E_n\right)^t = \det(A) \cdot E_n. \qquad \square$$

Aus der Cramerschen Regel folgen viele nützliche Aussagen, von denen einige nun präsentiert werden. Zuerst die noch offene Implikation

$$\det(A) \text{ Einheit} \quad \Longrightarrow \quad A \text{ invertierbar},$$

die im folgenden Satz mit weiteren Aussagen zusammengefaßt formuliert ist:

Satz 3.3.37. *Sei R ein kommutativer Ring mit Eins. Dann ist $A \in \mathrm{Mat}_n(R)$ genau dann invertierbar, wenn $\det(A)$ eine Einheit im Ring R ist:*

$$A \text{ invertierbar} \quad \Longleftrightarrow \quad \det(A) \in R^*.$$

Für die Inverse A^{-1} von A gilt in diesem Fall:

$$A^{-1} = \left(\det(A)\right)^{-1} \cdot A^{ad} \qquad \left(= \frac{1}{\det(A)} \cdot A^{ad}\right).$$

Beweis.
Die folgende Aussage ist schon in Satz 3.3.10 formuliert:

$$A \text{ invertierbar} \quad \Longrightarrow \quad \det(A) \in R^*.$$

Den Rest der Behauptung liefert die Cramersche Regel 3.3.36, denn gilt $\det(A) \in R^*$, so kann in der folgende Gleichung aus der Cramerschen Regel durch $\det(A)$ geteilt bzw. mit $\det(A)^{-1}$ multipliziert werden:

$$A^{\mathrm{ad}} \cdot A = \det(A) \cdot E_n \quad \overset{\cdot \det(A)^{-1}}{\Longrightarrow} \quad \Big(\det(A)^{-1} \cdot A^{\mathrm{ad}}\Big) \cdot A = E_n.$$

Nach Satz 3.2.22 reicht die rechte Gleichung schon aus, um zu folgern:

$$A \text{ invertierbar} \quad \text{und} \quad A^{-1} = \det(A)^{-1} \cdot A^{\mathrm{ad}}. \qquad \square$$

Bemerkung 3.3.38.

i.) *Die Inverse A^{-1} einer Matrix $A \in \mathrm{GL}_n(R)$ kann nach dem vorherigen Satz wegen $A^{-1} = \det(A)^{-1} \cdot A^{ad}$ durch Determinantenausdrücke beschrieben werden, denn auch A^{ad} ist aus Determinanten $\det\big(A[i,j]\big)$ aufgebaut (Definition 3.3.29).*

ii.) *Die Determinantenabbildung $\det\colon \mathrm{Mat}_n(R) \longrightarrow R$ kann als Polynom in n^2 Variablen über R aufgefaßt werden (Leibniz-Formel). Wird dann der spezielle Fall $R \in \{\mathbb{R}, \mathbb{C}\}$ betrachtet, so ist sie als reelles oder komplexes Polynom eine stetige und differenzierbare Abbildung. Damit hängt auch die Inverse einer Matrix $A \in \mathrm{GL}_n(R)$ in diesen Fällen stetig bzw. differenzierbar von A ab, denn die Zuordnung $A \mapsto A^{-1}$ ist im wesentlichen eine Kompositon von Detreminantenfunktionen, deren Parameter alle aus A entnommen sind.*

iii.) *Mit dem Kriterium aus Satz 3.3.37 kann nun in einem freien Modul $R^{[n]}$ getestet werden, ob ein linear unabhängiges System $x_1, \ldots, x_n$ mit $x_i \in R^{[n]}$ eine Basis von $R^{[n]}$ ist. Sei dazu $A \in \mathrm{Mat}_n(R)$ die Matrix mit den Spalten $x_1, \ldots, x_n$ und φ_A der von A induzierte Endomorphismus des $R^{[n]}$. Dann folgt:*

$$\begin{aligned} x_1, \ldots, x_n \text{ Basis des } R^{[n]} \quad &\overset{3.1.17}{\Longleftrightarrow} \quad \varphi_A \text{ bijektiv} \\ &\overset{3.1.20}{\Longleftrightarrow} \quad A \text{ invertierbar} \\ &\overset{3.3.37}{\Longleftrightarrow} \quad \det(A) \in R^*. \end{aligned}$$

Mit der gleichen Äquivalenzkette kann nun auch das Problem aus Beispiel 3.1.18 geklärt werden: darin war die Frage, festzustellen, ob der durch die Matrix

$$B := \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z})$$

induzierte Endomorphismus φ_B von $\mathbb{Z}^{[2]}$ eine bijektive Abbildung ist. Die dort gegebene Antwort (nein!) kann nun mit Hilfe der obigen Äquivalenzen schnell geklärt werden, denn es müßte

$$\det(B) \in \mathbb{Z}^* = \{\pm 1\}$$

gelten, was wegen $\det(B) = 4 - 1 = 3$ aber nicht erfüllt ist.

iv.) *In Satz 3.3.22 ist folgende Implikation über die Spalten einer quadratischen Matrix A über einen kommutativen Ring mit Eins formuliert:*

$$\det(A) \text{ ist kein Nullteiler} \quad \Longrightarrow \quad \text{Die Spalten von } A \text{ sind linear unabhängig.}$$

Diese Aussage läßt sich umkehren, allerdings sind zu dem Beweis Begriffe und Ergebnisse nötig, die bisher nicht erarbeitet wurden. Es gilt also:

Satz: *Ist R ein kommutativer Ring mit Eins und $A \in \mathrm{Mat}_n(R)$, so gilt folgende Äquivalenz:*

$$\det(A) \text{ ist kein Nullteiler} \quad \Longleftrightarrow \quad \text{Die Spalten von } A \text{ sind linear unabhängig.}$$

Ein Beweis findet sich z.B. in [**SSAlg1**, Satz 49.2, Seite 382].

Zusammen mit der vorherigen Äquivalenzkette und der darin enthaltenen Verschärfung dieses Satzes über kann nun also zusammenfassend der Zusammenhang über die Spalten einer quadratischen Matrix A über einem kommutativen Ring R mit Eins und deren Determinante formuliert werden:

$$\det(A) \text{ ist kein Nullteiler in } R \Longleftrightarrow \text{Die Spalten von } A \text{ sind linear unabhängig,}$$

$$\det(A) \text{ ist eine Einheit in } R \Longleftrightarrow \text{Die Spalten von } A \text{ sind eine Basis des } R^{[n]}.$$

□

Beispiel 3.3.39.

i.) *Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{GL}_2(R)$, also $\det(A) \in R^*$. Dann gilt:*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} := A \qquad \Longrightarrow \qquad A^{-1} = \big(\det(A)\big)^{-1} \cdot \underbrace{\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}_{\overset{(3.3.31)}{=} A^{ad}}.$$

ii.) *Sei $A \in \mathrm{GL}_n(\mathbb{R})$, und die Koeffizienten von A seien alle aus $\mathbb{Z} \subseteq \mathbb{R}$. Dann folgt sofort aus der Satz 3.3.37 (Übung!):*
Die Koeffizienten von A^{-1} liegen alle in $\mathbb{Q}$, und es gilt:

$$\det(A) \in \{\pm 1\} \quad \Longleftrightarrow \quad \text{Die Koeffizienten von } A^{-1} \text{ liegen alle in } \mathbb{Z}.$$

□

Eine direkte Konsequenz aus der Cramerschen Regel 3.3.36 ist auch der folgende Satz:

Satz 3.3.40. *(Laplacescher Entwicklungssatz)*
Sei R ein kommutativer Ring mit Eins und $A := (a_{i,j}) \in \mathrm{Mat}_n(R)$. Dann gilt:

$$\text{Entwicklung nach } i\text{-ter Zeile:} \qquad \det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{i,j} \cdot \det\big(A[i,j]\big).$$

$$\text{Entwicklung nach } j\text{-ter Spalte:} \qquad \det(A) = \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{i,j} \cdot \det\big(A[i,j]\big).$$

Somit ist die Determinante der $(n \times n)$-Matrix berechenbar mit Hilfe der Determinanten der $\big((n-1) \times (n-1)\big)$-Matrizen $A[i,j]$.

Die Terme $(-1)^{i+j} \cdot \det\big(A[i,j]\big)$ in obigen Formeln sind genau die Einträge der Transponierten der adjungierten Matrix A^{ad} von A, und ist $(b_{i,j}) := \big(A^{ad}\big)^t$, so schreiben sich obige Formeln als:

$$\text{Entwicklung nach } i\text{-ter Zeile:} \qquad \det(A) = \sum_{j=1}^{n} a_{i,j} \cdot b_{i,j}.$$

$$\textit{Entwicklung nach } j\textit{-ter Spalte:} \quad \det(A) = \sum_{i=1}^{n} a_{i,j} \cdot b_{i,j}.$$

Beweis.
Es sei $(c_{i,j}) := A^{\mathrm{ad}}$, so daß $b_{i,j} = c_{j,i}$ gilt $(*)$. Bewiesen werden die unteren beiden Entwicklungsformeln mit den Termen $b_{i,j}$ anstelle der Terme $(-1)^{i+j} \cdot \det\big(A[i,j]\big)$.

Entwicklung nach Zeilen: Die Cramersche Regel liefert die Gleichung:

$$A \cdot A^{\mathrm{ad}} = \det(A) \cdot E_n,$$

und mit der Definition $(d_{i,j}) := A \cdot A^{\mathrm{ad}}$ ergibt sich für die Koeffizienten $d_{i,i}$ auf der Diagonalen des Produktes $A \cdot A^{\mathrm{ad}}$:

$$d_{i,i} = \sum_{j=1}^{n} a_{i,j} \cdot c_{j,i} \overset{(*)}{=} \sum_{j=1}^{n} a_{i,j} \cdot b_{i,j}.$$

Andererseits gilt $A \cdot A^{\mathrm{ad}} = \det(A) \cdot E_n$, und die Diagonalelemtente $d_{i,i}$ sich gleich den Diagonalelementen von $\det(A) \cdot E_n$, also $d_{i,i} = \det(A)$. Dies liefert zusammengefaßt:

$$\det(A) = \sum_{j=1}^{n} a_{i,j} \cdot b_{i,j}.$$

Entwicklung nach Spalten: Die Cramersche Regel liefert die Gleichung:

$$A^{\mathrm{ad}} \cdot A = \det(A) \cdot E_n,$$

und mit der Definition $(d_{i,j}) := A^{\mathrm{ad}} \cdot A$ ergibt sich für die Koeffizienten $d_{j,j}$ auf der Diagonalen des Produktes $A^{\mathrm{ad}} \cdot A$:

$$d_{j,j} = \sum_{i=1}^{n} c_{j,i} \cdot a_{i,j} \overset{(R\text{ komm.})}{=} \sum_{j=1}^{n} a_{i,j} \cdot c_{j,i} \overset{(*)}{=} \sum_{i=1}^{n} a_{i,j} \cdot b_{i,j}.$$

Andererseits gilt $A^{\mathrm{ad}} \cdot A = \det(A) \cdot E_n$, und die Diagonalelemtente $d_{j,j}$ sich gleich den Diagonalelementen von $\det(A) \cdot E_n$, also $d_{j,j} = \det(A)$. Dies liefert zusammengefaßt:

$$\det(A) = \sum_{i=1}^{n} a_{i,j} \cdot b_{i,j}. \qquad \square$$

Bemerkung 3.3.41.

i.) *Der Laplacesche Entwicklungssatz ist kein effizientes Verfahren, um Determinanten zu berechnen: sein Aufwand ist in der Größenordnung von der Leibniz-Formel, denn zur Berechnung der Determinante einer $(n \times n)$-Matrix müssen n Determinanten von $\big((n-1) \times (n-1)\big)$-Matrizen berechnet werden, für diese jeweils $n-1$ Determinanten von $\big((n-2) \times (n-2)\big)$-Matrizen usw. Es ergibt sich dann auch mindestens $n!$ Multiplikationen.*

ii.) *Der Laplacesche Entwicklungssatz ist nützlich, wenn eine Matrix in einer Zeile oder einer Spalte viele Nullen enthält, da dann bei der Entwicklung nach dieser Zeile oder Spalte nur die Terme weiter berechnet werden müssen, wo der korrespondierende Eintrag in der Zeile/Spalte nicht Null ist.*

Insbesondere mit den Techniken aus Satz 3.3.22 kann eine Matrix oft so modifiziert werden, daß der günstige Fall mit vielen Nullen in einer Zeile oder Spalte auftritt.

iii.) *Lemma 3.3.4 über die Determinante einer oberen Dreiecksmatrix kann mit dem Laplaceschen Entwicklungssatz sofort induktiv bewiesen werden, indem nach der ersten Spalte entwickelt wird, die bei einer oberen Dreiecksmatrix nur im ersten/obersten Koeffizienten keine Null enthält und damit den oben angesprochenen Idealfall für den Entwicklungssatz erfüllt (Übung!). Siehe dazu auch Beispiel 3.3.42.* □

Beispiel 3.3.42.

i.) *Es sei die Telephonmatrix gegeben:*

$$A := (a_{i,j}) := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Nach dem Laplaceschen Entwicklungssatz 3.3.40 gilt für die Entwicklung von $\det(A)$ *nach der dritten Zeile:*

$$\begin{aligned} \det(A) &= \sum_{j=1}^{3} (-1)^{3+j} \cdot a_{3,j} \cdot \det\big(A[3,j]\big) \\ &= (-1)^4 \cdot 7 \cdot \det\big(A[3,1]\big) + (-1)^5 \cdot 8 \cdot \det\big(A[3,2]\big) + (-1)^6 \cdot 9 \cdot \det\big(A[3,3]\big) \\ &= 7 \cdot \underbrace{\begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix}}_{=-3} - 8 \cdot \underbrace{\begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix}}_{=-6} + 9 \cdot \underbrace{\begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix}}_{=-3} = 7 \cdot (-3) - 8 \cdot (-6) + 9 \cdot (-3) \\ &= -21 + 48 - 27 = 0. \end{aligned}$$

Die adjungierte der Telephonmatrix ist nach Beispiel 3.3.31 die Matrix:

$$A^{ad} = \begin{pmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{pmatrix} \qquad \Longrightarrow \qquad (b_{i,j}) := \big(A^{ad}\big)^t = \begin{pmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{pmatrix}.$$

Mit der Laplaceschen Formel über die Adjungierte ergibt sich dann ebenfalls beim Entwickeln nach der dritten Zeile:

$$\det(A) = \sum_{j=1}^{3} a_{3,j} \cdot b_{3,j} = 7 \cdot (-3) + 8 \cdot 6 + 9 \cdot (-3) = 0.$$

ii.) *Es sei folgende obere Dreiecksmatrix gegeben:*

$$A := \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}.$$

Wird die Determinante nach der ersten Spalte entwickelt, die nur einen Koeffizienten ungleich Null enthält, ergibt sich:

$$\det(A) = (-1)^{1+1} \cdot a \cdot \det\big(A[1,1]\big) = a \cdot \begin{vmatrix} d & e \\ 0 & f \end{vmatrix}.$$

Die Matrix $A[1,1]$ ist wieder eine obere Dreiecksmatrix, die nach der ersten Spalte entwickelt werden kann, und es folgt:

$$\det(A) = a \cdot \begin{vmatrix} d & e \\ 0 & f \end{vmatrix} = a \cdot d \cdot |f| = a \cdot d \cdot f.$$

Offensichtlich kann so jede obere Dreiecksmatrix sukzessive berechnet werden, und das Verfahren liefert per Induktion einen Beweis für Lemma 3.3.4 (Übung!).

iii.) Sei $A \in \mathrm{Mat}_n(R)$ eine obere Block-Dreiecksmatrix der Form:

$$A := \begin{pmatrix} A_1 & & & & \\ & A_2 & & * & \\ & & \ddots & & \\ & 0 & & A_{k-1} & \\ & & & & A_k \end{pmatrix} \quad \textit{mit} \quad A_i \in \mathrm{Mat}_{n_i}(R) \quad \textit{und} \quad \sum_{i=1}^{k} n_i = n.$$

Dann kann analog zum Fall von oberen Dreiecksmatrizen mit dem Laplaceschen Entwicklungssatz gezeigt werden (Übung!):

$$\det(A) = \prod_{i=1}^{k} \det(A_i). \qquad \square$$

Mit Hilfe der Cramerschen Regel kann für eine invertierbare Matrix $A \in \mathrm{GL}_n(R)$ die eindeutige Lösung des linearen Gleichungssystems

$$Az = b \qquad (\text{für } b \in R^{[n]})$$

beschrieben werden.
Die Formulierung „beschrieben werden“ ist mit Bedacht gewählt: tatsächlich liefert der folgende Satz auch ein Berechnungsverfahren für die Lösung, welches aber verlangt, $n+1$ Determinanten zu berechnen, was im allgemeinen viel aufwändiger ist als eine Lösung über den Gauß-Algorithmus oder die Inverse von A, denn natürlich ist $z = A^{-1}b$. Für diese Einschränkung muß jedoch der Gauß-Algorithmus auch Durchführbar sein, was er über Körpern aber z.B. immer ist.

Satz 3.3.43. *Sei R ein kommutativer Ring mit Eins und $A \in \mathrm{GL}_n(R)$. Weiter sei ein lineares Gleichungssystem*

$$Az = b$$

gegeben mit $b \in R^{[n]}$. Es seien $s_1, \ldots, s_n$ die Spalten von A, und für $1 \le i \le n$ sie B_i diejenige Matrix, die aus A entsteht, wenn die i-te Spalte s_i durch b ersetzt wird.

Ist dann $\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} := z$ die eindeutige Lösung des linearen Gleichungssystems $Az = b$, so gilt für die i-te Komponente z_i von z die Gleichung:

$$z_i = \det(A)^{-1} \cdot \det(B_i) \qquad (\textit{es gilt } \det(A) \in R^*).$$

Beweis.
Es sei $(c_{i,j}) := A^{\mathrm{ad}}$. Nach der Cramerschen Regel gilt $A^{-1} = \det(A)^{-1} \cdot A^{\mathrm{ad}}$, und es ist $z = A^{-1}b$. Die i-te Komponononente z_i von z berechnet sich durch:

$$\text{„}i\text{-te Zeile von } A^{-1}\text{“ mal „}b\text{“},$$

und die i-te Zeile von $A^{-1} = \det(A)^{-1} \cdot A^{\mathrm{ad}}$ hat die Form:

$$\big(\det(A)^{-1} \cdot c_{i,1}, \ldots, \det(A)^{-1} \cdot c_{i,n}\big).$$

Dies liefert dann für z_i mit $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} := b$:

$$z_i = \sum_{k=1}^{n} \big(\det(A)^{-1} \cdot c_{i,k}\big) \cdot b_k = \det(A)^{-1} \cdot \sum_{k=1}^{n} c_{i,k} \cdot b_k.$$

Für den Koeffizienten $c_{i,k}$ aus A^{ad} gilt nach Bemerkung 3.3.33 die Gleichung:

$$c_{i,k} = \det\big(A_{e_k,e_i}\big),$$

und nach Lemma 3.3.34 ist:

$$\det\big(A_{e_k,e_i}\big) = \det\begin{pmatrix} | & & | & | & | & & | \\ s_1 & \cdots & s_{i-1} & e_k & s_{i+1} & \cdots & s_n \\ | & & | & | & | & & | \end{pmatrix},$$

also insgesamt:

$$c_{i,k} = \det(s_1, \ldots, s_{i-1}, e_k, s_{i+1}, \ldots, s_n).$$

Dies liefert mit obiger dann für z_i:

$$\begin{aligned} z_i &= \det(A)^{-1} \cdot \sum_{k=1}^{n} c_{i,k} \cdot b_k \overset{(R\text{ komm.})}{=} \det(A)^{-1} \cdot \sum_{k=1}^{n} b_k \cdot c_{i,k} \\ &= \det(A)^{-1} \cdot \sum_{k=1}^{n} b_k \cdot \det(s_1, \ldots, s_{i-1}, e_k, s_{i+1}, \ldots, s_n) \\ &= \det(A)^{-1} \cdot \sum_{k=1}^{n} \det(s_1, \ldots, s_{i-1}, b_k \cdot e_k, s_{i+1}, \ldots, s_n), \end{aligned}$$

da der Faktor b_k vor der Determinante als Faktor der k-ten Spalte in die Determinante hereingezogen werden darf (Satz 3.3.22).
Aus der Linearität der Determinante in der k-ten Spalte (Satz 3.3.27) folgt dann aber mit der Gleichung $b = \sum_{k=1}^{n} b_k \cdot e_k$ letztendlich:

$$\begin{aligned} z_i &= \det(A)^{-1} \cdot \sum_{k=1}^{n} \det(s_1, \ldots, s_{i-1}, b_k \cdot e_k, s_{i+1}, \ldots, s_n) \\ &= \det(A)^{-1} \cdot \det(s_1, \ldots, s_{i-1}, \sum_{k=1}^{n} b_k \cdot e_k, s_{i+1}, \ldots, s_n) \\ &= \det(A)^{-1} \cdot \det(s_1, \ldots, s_{i-1}, b, s_{i+1}, \ldots, s_n) \\ &= \det(A)^{-1} \cdot \det(B_i). \end{aligned}$$

□

Beispiel 3.3.44. *Es sei folgendes reelle lineare Gleichungssystem gegeben:*

$$Az = b \quad \textit{mit} \quad A := \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix} \quad \textit{und} \quad b := \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

Wegen $\det(A) = 4$ *ist* A *über dem Körper* $\mathbb{R}$ *invertierbar und das Gleichungssystem hat eine eindeutige Lösung* $z := A^{-1}b$*:*

$$A^{-1} = \begin{pmatrix} 2 & -\frac{3}{4} \\ -1 & \frac{1}{2} \end{pmatrix} \quad \Longrightarrow \quad z = \begin{pmatrix} \frac{7}{4} \\ -\frac{1}{2} \end{pmatrix}.$$

Mit Hilfe der Cramerschen Regel für Gleichungssysteme in Satz 3.3.43 kann die Lösung auch mit Hilfe der dort beschriebenen Determinanten berechnet werden:

$$B_1 = \begin{array}{c} \begin{array}{cc} b & s_2 \end{array} \\ \begin{pmatrix} 2 & 3 \\ 3 & 8 \end{pmatrix} \end{array} \quad \textit{und} \quad B_2 = \begin{array}{c} \begin{array}{cc} s_1 & b \end{array} \\ \begin{pmatrix} 2 & 2 \\ 4 & 3 \end{pmatrix} \end{array} \quad \Longrightarrow \quad \det(B_1) = 7, \quad \det(B_2) = -2,$$

woraus dann für die Komponenten z_1 *und* z_2 *der Lösung* z *folgt:*

$$z_1 = \frac{\det(B_1)}{\det(A)} = \frac{7}{4} \quad \textit{und} \quad z_2 = \frac{\det(B_2)}{\det(A)} = \frac{-2}{4} = -\frac{1}{2}. \qquad \square$$

Polynome und charakteristische Polynome.

Als letzte Anwendung der Determinante soll mit ihrer Hilfe jeder quadratischen Matrix ein „charakteristisches Polynom“ zugeordnet werden. Dafür müssen zuerst einmal Polynome über einem Ring eingeführt werden.
Aus der Schule bekannt sind Polynome als Ausdrücke:

$$\sum_{i=0}^{n} a_i x^i = a_n x^n + \ldots a_1 x + a_0$$

mit den Konventionen $x^1 = x$ und $x^0 = 1$, wobei die Rolle von x als „Unbekannte“ nicht näher erläutert ist. Gemeint ist damit meist eine funktionale Betrachtung eines Polynoms, d.h. ein Ausdruck $x^2 + 1$ wird als Abbildung:

$$f\colon \mathbb{R} \longrightarrow \mathbb{R} \quad \text{mit} \quad x \mapsto x^2 + 1$$

aufgefaßt, wobei x dann die Rolle eine Funtionsvariable übernimmt. Diese funktionale Betrachtung von Polynomen bringt jedoch Probleme mit sich, wenn spezielle Körper oder Ringe (insbesondere endliche) als Definitionsbereich einer solchen Abbildung herangezogen werden. Wird zum Beispiel das Polynom/die Funktion:

$$f\colon \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \quad \text{mit} \quad x \mapsto x^2 - x$$

betrachtet, so ist dies die Nullabbildung, und gleiches gilt für jedes der Polynome $x^n - x$. Diese Ausdrücke wären dann als Abbildungen alle gleich. Dies ist jedoch nicht im Sinne der Algebra, dort soll für die formalen Polynome $x^2 - x$ und $x^3 - x$ immer gelten, daß sie verschieden sind.

Also muß nun zuersteinmal geklärt werden, was ein „formales“ Polynom im Sinne der Algebra überhaupt sein soll. Dazu seien zuersteinmal in bekannter Weise zwei Polynome $\sum_{i=0}^{n} a_i x^i$ und $\sum_{i=0}^{m} b_i x^i$ betrachtet mit $n \geq m$ und deren Summe:

$$\Big(\sum_{i=0}^{n} a_i x^i\Big) + \Big(\sum_{i=0}^{m} b_i x^i\Big) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i.$$

Es fällt auf, daß die Potenzen x^i bei dieser Rechnung keine wichtige Rolle spielen, sie sind mehr oder weniger nur Indikatoren, welche Koeffizienten miteinander verknüpft werden sollen. Die beiden Polynome könnten auch als Koeffiziententupel:

$$(a_0, a_1, a_2, \ldots, a_n) \quad \text{und} \quad (b_0, b_1, b_2, \ldots, b_m)$$

notiert und dann diese Tupel komponentenweise addiert werden - wobei hier noch das Problem der unterschiedlichen Länge der Tupel besteht. Dabei ist in obiger Tupelnotation die Reihenfolge der Koeffizienten anders gewählt als in der üblichen Polynomdarstellung

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

und dies hat den Vorteil, daß die i-ten Koeffizienten der Polynome immer an der i-ten Stelle der Tupel stehen - wobei Tupel ja in natürlicher Weise von links nach rechts gelesen werden. Werden die Tupel als Folgen betrachtet und nach rechts mit den Koeffizienten Null aufgefüllt, fällt auch das formale Problem weg, Tupel unterschiedlicher Länge zu addieren:

$$\sum_{i=0}^{n} a_i x^i \mapsto (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \quad \text{und} \quad \sum_{i=0}^{m} b_i x^i \mapsto (b_0, b_1, \ldots, b_m, 0, 0, \ldots).$$

Auch die Multiplikation zweier Polynome kann auf Tupel übertragen werden. Es gilt für das Produkt zweier Polynome:

$$\Big(\sum_{i=0}^{n} a_i x^i\Big) \cdot \Big(\sum_{i=0}^{m} b_i x^i\Big) = \sum_{i=0}^{n+m} c_i x^i \quad \text{mit} \quad c_i := \sum_{k=0}^{i} a_k b_{i-k}.$$

Aus technischen Gründen ist es ratsam, die Koeffizieneten c_i des Produktes durch eine andere Indexmenge auszudrücken:

$$\sum_{k=0}^{i} a_k b_{i-k} = \sum_{\lambda+\mu=i} a_\lambda b_\mu.$$

Mit dieser Formel wird nun die Multiplikation für Tupel definiert:

$$(a_0, a_1, \ldots) * (b_0, b_1, \ldots) := (c_0, c_1, \ldots) \quad \text{mit} \quad c_i := \sum_{\lambda+\mu=i} a_\lambda b_\mu.$$

Damit ist der Schritt vollzogen, Polynome $\sum_{i=0}^{n} a_i x^i$ mit Koeffizienten aus einen Ring R als Folgen über R zu betrachten mit der üblichen komponentenweisen Addition und einer neuen Multiplikation: und in der Folgeninterpretation tritt die ominöse Unbekannte „x“ nicht mehr auf.

Dabei sind Polynome spezielle Folgen aus dem Folgen-Modul $\prod_{i\in\mathbb{N}_0} R$, da sie nur an endlich vielen Stellen einen Koeffizient ungleich Null besitzen, und sie liegen tatsächlich schon in dem Untermodul $\bigoplus_{i\in\mathbb{N}_0} R$, der genau so definiert ist (siehe auch Definition 2.2.3).

Lemma 3.3.45. *Sei R ein kommutativer Ring mit Eins. Für zwei Folgen über R*

$$(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0} \in \prod_{i\in\mathbb{N}_0} R$$

sei eine Multiplikation definiert durch:

$$(a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0} := (c_i)_{i\in\mathbb{N}_0} \quad \textit{mit} \quad c_i := \sum_{\lambda+\mu=i} a_\lambda b_\mu.$$

Dann ist $\prod_{i\in\mathbb{N}_0} R$ mit der komponentenweise Addition und obiger Multiplikation ein kommutativer Ring mit dem Einselement

$$(1, 0, 0, \ldots).$$

Weiter gilt, daß die Teilmenge $\bigoplus_{i\in\mathbb{N}_0} R$ ein kommutativer Unterring von $\prod_{i\in\mathbb{N}_0} R$ ist, der dessen Einselement enthält.

Beweis. Siehe Lemma A.4.2 in Anhang A.4. □

Nun ist $\prod_{i\in\mathbb{N}_0} R$ auch ein R-Modul (Beispiel 2.1.4), und die Menge aller Folgen mit nur endlich vielen Einträgen ungleich Null $\bigoplus_{i\in\mathbb{N}_0} R$ ist darin ein freier R-Untermodul mit einer Basis:

$$(e_i)_{i\in\mathbb{N}_0} \quad \text{und} \quad e_i = (\delta_{i,j})_{j\in\mathbb{N}_0},$$

also denjenigen Folgen, die an genau einer Stelle eine Eins und sonst nur Nullen haben (Lemma 2.2.29).
Jede Folge $(a_i)_{i\in\mathbb{N}_0}$ aus $\bigoplus_{i\in\mathbb{N}_0} R$ läßt sich darstellen als Linearkombination:

$$(a_i)_{i\in\mathbb{N}_0} = \sum_{i\in\mathbb{N}_0} a_i \cdot e_i,$$

da nur endlich viele a_i ungleich Null sind. Es sei nun für ein Symbol „t “

$$t := e_1 = (0, 1, 0, \ldots),$$

definiert. Die spezielle Ringmultiplikation liefert für die Standard-Basis-Vektoren die Formel (Übung!):

$$e_i * e_j = e_{i+j},$$

und mit dieser wiederum ergibt sich sofort induktiv:

$$t^n = e_n.$$

Wird nun außerdem die vorherige Linearkombination $\sum_{i\in\mathbb{N}_0} a_i \cdot e_i$ nur bis zum relevanten höchsten Index

$$n := \max\big(0, \max\{k \in \mathbb{N}_0 \mid a_k \neq 0\}\big)$$

notiert, so ergibt sich für die Folge $(a_i)_{i\in I}$ eine Darstellung:

$$\sum_{i=0}^{n} a_i t^i,$$

die der ursprünglichen Notation von Polynomen mit der Unbekannten „t“ entspricht.

Für den Raum aller Folgen $\prod_{i\in\mathbb{N}_0} R$ ist das System $(e_i)_{i\in\mathbb{N}_0}$ keine Basis, so daß die Folgen nicht als deren Linearkombination geschrieben werden können. Trotzdem wird symbolisch für eine Folge:

$$\sum_{i=0}^{\infty} a_i t^i := (a_i)_{i\in\mathbb{N}_0}$$

notiert, um den Ringkontext aus Lemma 3.3.45 und die Folgenmultiplikation anzudeuten.

Definition 3.3.46. *Sei R ein kommutativer Ring mit Eins und t ein Symbol.*
Der kommutative Ring mit Eins der Folgen $\prod_{i\in\mathbb{N}_0} R$ mit den Verknüpfungen aus Lemma 3.3.45 wird mit $R[[t]]$ notiert und heißt der Potenzreihenring von R, und dessen Elemente werden als formale Potenzreihen über R bezeichnet und geschrieben als:

$$\sum_{i=0}^{\infty} a_i t^i.$$

Der kommutative Unterring mit Eins $\bigoplus_{i\in\mathbb{N}_0} R$ von $R[[t]]$ wird mit $R[t]$ notiert und heißt der Polynomring von R, und seine Elemente werden als Polynome über R beezeichnet. Polynome aus $R[t]$ werden je nach Kontext mit oder ohne Notation des Symbols geschrieben: p oder $p(t)$.
Die Null aus dem Ring $R[t]$, also die Folge mit lauter Nullen, heißt das Nullpolynom.
Für ein Polynom $p := (a_i)_{i\in\mathbb{N}_0} \in R[t]$ ist der Grad definiert durch:

$$\operatorname{grad}(p) := \begin{cases} -\infty & \text{für } p \text{ Nullpolynom,} \\ n & \text{für } p \text{ nicht das Nullpolynom und } n = \max\{k \in \mathbb{N}_0 \mid a_k \neq 0\}. \end{cases}$$

Polynome $p \in R[t]$ werden auch geschrieben in der Form:

$$p = \sum_{i=0}^{\max\left(0,\operatorname{grad}(p)\right)} a_i t^i = a_n t^n + \ldots a_1 t^1 + a_0 t^0.$$

Dabei wird in der rechten Notation t^1 als einfach als t und t^0 als „1“ oder überhaupt nicht notiert.
Der Koeffizient a_0 heißt das Absolutglied und für $n := \max\left(0, \operatorname{grad}(p)\right)$ der Koeffizient a_n der Leitkoeffizient von p.
Ist der Leitkoeffizient von p gleich Eins, so heißt das Polynom normiert.
Polynome vom Grad kleiner gleich Null werden als konstante Polynome bezeichnet, und normierte Polynome vom Grad Eins als Linearfaktoren. □

Bemerkung 3.3.47.

i.) Die Definition von Polynomen durch spezielle Folgen erlaubt eine einfachere allgemeine Notation der Summe zweier Polynome. Im einleitenden Text war noch geschrieben worden:

$$\Big(\sum_{i=0}^{n} a_i t^i\Big) + \Big(\sum_{i=0}^{m} b_i t^i\Big) = \sum_{i=0}^{m} (a_i + b_i) t^i + \sum_{i=m+1}^{n} a_i t^i,$$

da im rechten Summanden die Koeffizienten b_i für $i > m$ nicht existieren. Bei $\sum_{i=0}^{m} b_i x^i$ als Notation einer Folge sind die „oberen“ Koeffizienten per Definition

alle Null und werden in der Linearkombination $\sum_{i=0}^{m} b_i x^i$ *nur nicht notiert, und es kann einfacher geschrieben werden:*

$$\Big(\sum_{i=0}^{n} a_i t^i\Big) + \Big(\sum_{i=0}^{m} b_i t^i\Big) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) t^i.$$

ii.) In $\prod_{i\in\mathbb{N}_0} R$ *sind zwei Folgen genau dann gleich, wenn alle ihre Koeffizienten übereinstimmen (Definition 0.2.2). Damit sind die Polynome* $t^2 - t$ *und* $t^3 - t$ *aus* $\mathbb{Z}_2[t]$ *verschieden (siehe den einleitenden Text über die funktionale Interpretation von Polynomen).*

iii.) Für den kommutativen Ring mit Eins R *ist folgende Abbildung offensichtlich injektiv und sowohl ein Ringhomomorphismus als auch eine* R*-lineare Abbildung:*

$$\psi\colon R \longrightarrow R[t] \quad \textit{mit} \quad a \mapsto a = a \cdot t^0 = (a, 0, 0, \ldots) \qquad \textit{konstantes Polynom.}$$

Damit kann der Polynomring $R[t]$ *in natürlicher Weise als Ringerweiterung von* R *aufgefaßt und* $R \subseteq R[t]$ *geschrieben werden.*

iv.) Ist ein Polynom $p := \sum_{i=0}^{n} a_i t^i \in R[t]$ *gegeben, so kann für ein* $\alpha \in R$ *der Term* $\sum_{i=0}^{n} a_i \alpha^i$ *berechnet werden. Damit läßt sich via der Zuordnung:*

$$\Phi_p\colon R \longrightarrow R \quad \textit{mit} \quad \alpha \mapsto \sum_{i=0}^{n} a_i \alpha^i$$

das Polynom als Abbildung von R *nach* R *interpretieren. Dies wird dann kurz mit* $p(\alpha) := \Phi_p(\alpha)$ *bezeichnet, so daß die Notation* $p(t)$ *für das Polynom Sinn macht, um diesen funktionalen Aspekt einzubringen.*
Damit läßt sich dann eine Abbildung:

$$\Phi\colon R[t] \longrightarrow \mathrm{Abb}(R, R) \quad \textit{mit} \quad p \mapsto \Phi_p \quad \textit{bzw.}\ p \mapsto p(t)$$

aufstellen, die aber nicht injektiv sein muß, da z.B. die verschiedenen Polynome $t^n - t$ *aus* $\mathbb{Z}_2[t]$ *für alle* $n \geq 1$ *auf die Nullabbildung abgebildet werden.*
Dazu gilt folgender Satz:

Satz: Ist R *ein unendlich großer, nullteilerfreier kommutativer Ring mit Eins, so ist die Abbildung*

$$\Phi\colon R[t] \longrightarrow \mathrm{Abb}(R, R) \quad \textit{mit} \quad p \mapsto p(t)$$

ein injektiver Ringhomomorphismus und auch eine injektive R*-lineare Abbildung.*

Beweis: Zum Beispiel in [**SSAlg2**, Satz 54.6, Seite 48].

Damit ist es insbesondere über den unendlichen Körpern $\mathbb{Q}$, $\mathbb{R}$ *und* $\mathbb{C}$ *und auch über* $\mathbb{Z}$ *egal, ob Polynome als formale Objekte oder Abbildungen interpretiert werden.*
Ein Beispiel für einen unendlichen kommutativen Ring mit Nullteilern, wo obiges Φ *nicht injektiv ist, kann mit jeder unendlichen Menge* M *konstruiert werden: Dann ist der Ring* $\big(\mathcal{P}(M), \ominus, \cap\big)$ *der Potenzmenge von* M *mit der Addition „*$\ominus$*: symmetrische Differenz“ und der Multiplikation „*$\cap$*: Vereinigung“ ein unendlich großer kommutativer Ring mit Eins (die Menge* M *selbst) - siehe Beispiel 1.3.3. Dieser Ring besitzt Nullteiler, da für jedes* $A \in \mathcal{P}(M)$ *gilt:*

$$A \in \mathcal{P}(M) \quad \Longrightarrow \quad (M \setminus A) \in \mathcal{P}(M) \quad \textit{und} \quad A \cap (M \setminus A) = \emptyset, \textit{ d.h. Null.}$$

In dem Ring gilt auch $A \cap A = A$, so daß jedes $A \in \mathcal{P}(M)$ Nullstelle des Polynoms $t^2 - t$ ist und dieses Polynom also als Abbildung die Nullabbildung.

v.) *Elemente des formalen Potenzreihenringes $R[[t]]$ können nicht einfach als Abbildungen von R nach R durch Einsetzen eines $\alpha \in R$ in $\sum_{i=0}^{\infty} a_i t^i$ interpretiert werden: sind unendlich viele a_i ungleich Null und ist α kein Nullteiler, würden unendlich viele Terme $a_i \cdot \alpha^i \neq 0$ addiert, was nicht definiert ist.*
In der Analysis wird über $\mathbb{R}$ und $\mathbb{C}$ für solche Reihen ein Konvergenzbegriff definiert, so daß zumindest im „Konvergenzradius“ der Reihe diese als Funktion interpretierbar ist: aber auf einem allgemeinen Ring R kann dies nicht einfach übertragen werden (dazu muß auf R eine Topologie existieren, bzgl. der dann ein Konvergenzbegriff definiert werden kann).

vi.) *Für die Grad-Funktion im Polynomring $R[t]$ gelten folgende Aussagen, die als kleine Übung sofort aus den Definitionen folgen:*

$$\begin{aligned} \operatorname{grad}(f+g) &\leq \max\big(\operatorname{grad}(f), \operatorname{grad}(g)\big), \\ \operatorname{grad}(f \cdot g) &\leq \operatorname{grad}(f) + \operatorname{grad}(g), \end{aligned}$$

und ist R nullteilerfrei, so gilt sogar:

$$\operatorname{grad}(f \cdot g) = \operatorname{grad}(f) + \operatorname{grad}(g).$$

vii.) *Die Grad-Formel für die Multiplikation von Polynomen liefert sofort die beiden folgenden Aussagen (Übung!):*

$$R \text{ nullteilerfrei} \quad \Longleftrightarrow \quad R[t] \text{ nullteilerfrei},$$

und für einen nullteilerfreien Ring gilt:

$$R^* = \big(R[t]\big)^*.$$

viii.) *Hat ein Ring Nullteiler, so kann auch ein nicht-konstantes Polynom ein Einheit sein, wie folgendes Beispiel aus $\mathbb{Z}_4[t]$ zeigt:*

$$\begin{aligned} \big([2]_4 \cdot t + [1]_4\big)\big([2]_4 \cdot t + [1]_4\big) &= [4]_4 \cdot t^2 + \big([2]_4 + [2]_4\big) \cdot t + [1]_4 = [1]_4 \\ \Longrightarrow \quad [2]_4 \cdot t + [1]_4 &\in \big(\mathbb{Z}_4[t]\big)^*. \end{aligned}$$

ix.) *Der formale Potenzreihenring $R[[t]]$ besitzt mehr Einheiten als der Polynomring $R[t]$, denn es gilt (Übung!):*

$$\sum_{i=0}^{\infty} a_i t^i \text{ Einheit in } R[[t]] \quad \Longleftrightarrow \quad a_0 \text{ Einheit in } R. \qquad \square$$

Die Eigenschaften eines Polynomringes als Modul seien noch einmal in „aktueller“ Notation zusammengefaßt:

Satz 3.3.48. *Sei R ein kommutativer Ring mit Eins und $R[t]$ der Polynomring über R. Dann ist $R[t]$ ein freier R-Modul, und*

$$(t^i)_{i \in \mathbb{N}_0} = (1, t, t^2, t^3, \ldots)$$

eine Basis. Für $n \in \mathbb{N}_0$ sind die folgenden R-Untermoduln

$$R[t]_{|n} := \langle\, 1, t, t^2, \ldots, t^n \,\rangle = \Big\{ \sum_{i=0}^{n} a_i t^i \Big\}$$

freie Untermoduln mit der Basis $(1, t, t^2, \ldots, t^n)$*, und im Falle eines Körpers* K *gilt dann*

$$\dim_K \left(K[t]_{|n}\right) = n + 1.$$

Beweis.
Lemma 3.3.45 und Definition 3.3.46 sowie Lemma 2.2.29. □

Beispiel 3.3.49.

i.) Es seien die reellen Polynome $\mathbb{R}[t]$ *betrachtet: Dann ist die Ableitung:*

$$D\colon \mathbb{R}[t] \longrightarrow \mathbb{R}[t] \quad \textit{mit} \quad p \mapsto p'$$

eine $\mathbb{R}$*-lineare Abbildung (*$\mathbb{R}[t]$ *ist ein* $\mathbb{R}$*-Vektorraum).*
Für jedes $n \in \mathbb{N}_0$ *ist die Einschränkung dieser Abbildung:*

$$D\colon \mathbb{R}[t]_{|n} \longrightarrow \mathbb{R}[t]_{|n} \quad \textit{mit} \quad p \mapsto p'$$

wohldefiniert wegen $\operatorname{grad}(p') \leq \operatorname{grad}(p)$.

ii.) Für $a, b \in \mathbb{R}$ *mit* $a < b$ *ist die folgende Abbildung wohldefiniert und* $\mathbb{R}$*-linear, da reelle Polynome stetig und damit integrierbar sind:*

$$I_{a,b}\colon \mathbb{R}[t] \longrightarrow \mathbb{R} \quad \textit{mit} \quad p \mapsto \int_a^b p(t)\, dt.$$

iii.) Sei R *ein kommutativer Ring mit Eins und für* $n \in \mathbb{N}_0$ *der freie* R*-Modul* $R[t]_{|n}$ *mit seiner Basis* $1, t, \ldots, t^n$ *betrachtet. Von dieser Basis kann durch Zuordnung zur kanonischen Standard-Basis* $e_1, \ldots, e_{n+1}$ *des* R^{n+1} *ein Isomorphismus in den* R^{n+1} *definiert werden:*

$$t^0 \mapsto e_1, \quad t \mapsto e_2, \quad \ldots, \quad t^n \mapsto e_{n+1},$$

so daß ein Polynom durch den dadurch induzieten Isomorphismus von $R[t]_{|n}$ *nach* R^{n+1} *folgendermaßen abgebildet wird:*

$$\sum_{i=0}^{n} a_i t^i \mapsto (a_0, a_1, \ldots, a_n) \in R^{n+1}.$$

Sind Polynome $p_0, \ldots, p_n \in R[t]_{|n}$ *gegeben, so sind diese genau dann darin eine Basis, wenn die zugeordneten Tupel unter obiger Abbildung eine Basis des* R^{n+1} *sind. Um dies zu testen, kann z.B. die Determinante derjenigen Matrix* A *betrachtet werden, die aus den* $n+1$ *Zeilenvektoren des* R^{n+1} *besteht, die den* p_i *zugeordnet sind, denn es gilt:*

$$\det(A) \textit{ Einheit in } R \quad \Longleftrightarrow \quad \textit{Die Zeilen von } A \textit{ sind eine Basis des Zeilenraumes.}$$

(Die Aussage ist in Bemerkung 3.3.38 für Spaltenvektoren gezeigt, und wegen $\det(A) = \det(A^t)$ *kann sie auf Zeilen übertragen werden.)*
Werden dann zum Beispiel $t^2 + 3$*,* $t + 5$ *und* 3 *aus* $\mathbb{Z}[t]_{|2}$ *betrachtet, so haben diese unter obiger Abbilung die Bilder:*

$$t^2 + 3 \mapsto (3, 0, 1), \quad t + 5 \mapsto (5, 1, 0) \quad \textit{und} \quad 3 \mapsto (3, 0, 0),$$

und die zu testende Matrix hat die Form:

$$A := \begin{pmatrix} 3 & 0 & 1 \\ 5 & 1 & 0 \\ 3 & 0 & 0 \end{pmatrix}.$$

Es gilt $\det(A) = -3$*, so daß die Zeilen der Matrix zwar linear unabhängig sind, aber keinen Basis (*-3 *ist kein Nullteiler in* $\mathbb{Z}$*, aber auch keine Einheit).* □

Wie in Bemerkung 3.3.47 ausgeführt, kann ein Ring R kanonisch als Teilmenge seines Polynomringes $R[t]$ aufgefaßt werden (Elemente aus R als konstante Polynome), und analog können auch Matrizen über R als Matrizen über $R[t]$ betrachtet werden:

$$\mathrm{Mat}(m \times n, R) \subseteq \mathrm{Mat}\big(m \times n, R[t]\big).$$

Dann ist folgende Definiiton für die kommenden Problemstellungen wichtig:

Definition 3.3.50. *Sei* R *ein kommutativer Ring mit Eins. Weiter sei folgende Abbildung vom Matrizenring* $\mathrm{Mat}_n(R)$ *in den Polynomring* $R[t]$ *betrachtet:*

$$\chi\colon\ \mathrm{Mat}_n(R) \longrightarrow R[t] \quad \textit{mit} \quad A \mapsto \det\big(\underbrace{t \cdot E_n - A}_{\in \mathrm{Mat}_n\left(R[t]\right)}\big).$$

Dann heißt das einem $A \in \mathrm{Mat}_n(R)$ *durch* χ *zugeordnete Polynom* $\chi(A) \in R[t]$ *das charakteristische Polynom von* A *und wird auch mit* χ_A *bezeichnet.* □

Bemerkung 3.3.51.

i.) Die Abbildung χ *aus Definition 3.3.50 ist eine Abbildung zwischen den beiden Ringen* $\mathrm{Mat}_n(R)$ *und* $R[t]$*, die beide jeweils auch freie* R*-Moduln sind, aber sie ist bzgl. keiner dabei definierten Verknüpfung strukturverträglich, denn für* $A, B \in \mathrm{Mat}_n(R)$ *und* $a \in R$ *gilt:*

$$\begin{aligned} \chi(A+B) &\neq \chi(A) + \chi(B), \\ \chi(AB) &\neq \chi(A) \cdot \chi(B), \\ \chi(aA) &\neq a \cdot \chi(A). \end{aligned}$$

Zur Konstruktion von Gegenbeispielen sei der Fall $\mathrm{Mat}_2(\mathbb{Z})$ *betrachtet. Es gilt:*

$$\begin{aligned} \chi(E_2 + E_2) = \chi(2 \cdot E_2) &= \det(t \cdot E_2 - 2 \cdot E_2) = \det\big((t-2) \cdot E_2\big) \\ &= \det \begin{pmatrix} t-2 & 0 \\ 0 & t-2 \end{pmatrix} = (t-2)^2. \end{aligned}$$

Die Matrix E_2 *hat offensichtlich das charakteristische Polynom* $\chi(E_2) = (t-1)^2$*, und so folgt aus obiger Gleichung:*

$$\begin{aligned} \chi(E_2 + E_2) &= (t-2)^2 && \neq 2(t-1)^2 = (t-1)^2 + (t-1)^2 && = \chi(E_2) + \chi(E_2), \\ \chi(E_2 \cdot E_2) &= \chi(E_2) = (t-1)^2 && \neq (t-1)^4 = (t-1)^2 \cdot (t-1)^2 && = \chi(E_2) \cdot \chi(E_2), \\ \chi(2 \cdot E_2) &= (t-2)^2 && \neq 2(t-1)^2 && = 2 \cdot \chi(E_2). \end{aligned}$$

ii.) Ist $A \in \mathrm{Mat}_n(R)$ *eine obere oder untere Dreiecksmatrix mit den Diangonalelementen* $a_{i,i}$*, so ist auch* $t \cdot E_n - A$ *eine obere oder untere Dreiecksmatrix mit den Diagonalelementen* $t - a_{i,i}$*, und es folgt aus Lemma 3.3.4 über die Determinante von Dreiecksmatrizen:* $\chi_A = \prod_{i=1}^n (t - a_{i,i})$*:*

$$A = \begin{pmatrix} a_{1,1} & & & \\ & a_{2,2} & * & \\ & & \ddots & \\ & & & a_{n,n} \end{pmatrix} \implies t \cdot E_n - A = \begin{pmatrix} t - a_{1,1} & & & \\ & t - a_{2,2} & * & \\ & & \ddots & \\ & & & t - a_{n,n} \end{pmatrix}$$

$$\Longrightarrow \qquad \chi_A = \det\big(t \cdot E_n - A\big) = \prod_{i=1}^{n}(t - a_{i,i}).$$

Diese Aussage gilt insbesondere auch für Diagonalmatrizen, da diese gleichzeitig obere und untere Dreiecksmatrizen sind.

iii.) Analog zum Fall der oberen/unteren Dreiecksmatrizen sei A eine obere (oder untere) Block-Dreiecksmatrix mit Diagonalblöcken A_i wie in Beispiel 3.3.42 (oder Aufgabe 4 von Aufgabenblatt 3 LAIIa) gegeben der Form:

$$A := \begin{pmatrix} A_1 & & & & \\ & A_2 & & * & \\ & & \ddots & & \\ & 0 & & A_{k-1} & \\ & & & & A_k \end{pmatrix}.$$

Diese Blockstruktur wird in der Matrix $t \cdot E_n - A$ erhalten und es folgt sofort:

$$\det(t \cdot E_n - A) = \prod_{t=1}^{k} \det(t \cdot E_{n_i} - A_i).$$

Die Terme $\det(t \cdot E_{n_i} - A_i)$ sind dabei nichts anderes als die charakteristischen Polynome der Blöcke A_i, so daß sich dann schreiben läßt:

$$\chi_A = \prod_{i=1}^{k} \chi_{A_i}.$$

iv.) Da das charakteristische Polynom einer oberen Dreiecksmatrix nach vorheriger Bemerkung leicht zu bestimmen ist, liegt der Versuch nahe, eine Matrix A zuerst mit dem Gauß-Algorithmus in obere Dreiecksform zu bringen und dann das charakteristische Polynom zu berechnen. Folgendes Beispiel zeigt, daß dies nicht funktioniert:
Es sei folgende reelle Matrix A und ihre Zeilen-Stufen-Form nach dem ersten und den zweiten Schritt des Gauß-Algorithmus betrachtet:

$$A := \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad \rightsquigarrow \quad B := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \rightsquigarrow \quad C := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Es gilt dann für deren charakteristische Polynome:

$$\begin{aligned} \chi_A &= \det \begin{pmatrix} t-1 & -1 \\ -1 & t-2 \end{pmatrix} = (t-1)(t-2) - 2 = t^2 - 3t + 2, \\ \chi_B &= (t-1)^2 \qquad\qquad\qquad\qquad\qquad\qquad = t^2 - 2t + 1, \\ \chi_C &= (t-1)^2 \qquad\qquad\qquad\qquad\qquad\qquad = t^2 - 2t + 1. \end{aligned}$$

Die charakteristischen Polynome beider Zeilen-Stufen-Formen sind verschieden vom charakteristischen Polynom von A, so daß der Gauß-Algorithmus nicht zuerst auf A angewandt werden kann, um dann χ_A zu berechnen. Und da dies ein häufiger Fehler ist, noch einmal zur Deutlichkeit:

Der Gauß-Algorithums verträgt sich NICHT mit der Berechnung charakteristischer Polynome! □

Beispiel 3.3.52.

i.) *Sei $\alpha \in \mathbb{R}$. Dann gilt für die folgende Matrix $D_\alpha \in \mathrm{Mat}_2(\mathbb{R})$ und ihr charakteristisches Polynom $\chi_{D_\alpha} \in \mathbb{R}[t]$:*

$$D_\alpha := \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \quad \Longrightarrow \quad \begin{aligned} \chi_{D_\alpha} &= \det \begin{pmatrix} t-\cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & t-\cos(\alpha) \end{pmatrix} \\ &= t^2 - 2\cdot\cos(\alpha)\cdot t + 1. \end{aligned}$$

ii.) *Für die Telephonmatrix über $\mathbb{R}$ gilt:*

$$A := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad \Longrightarrow \quad \chi_A = \det \begin{pmatrix} t-1 & -2 & -3 \\ -4 & t-5 & -6 \\ -7 & -8 & t-9 \end{pmatrix}.$$

Wegen der Polynome (Linearfaktoren) in der Matrix fällt der Gauß-Algorithmus zur Berechnung der Determinante weg. Es könnte hier die Regel von Sarrus angewendet werden - oder in die Matrix werden durch Zeilen-/Spaltenoperationen Nullen gebracht, so daß einfacher nach einer Zeile oder Spalte entwickelt werden kann:

$$\begin{pmatrix} t-1 & -2 & -3 \\ -4 & t-5 & -6 \\ -7 & -8 & t-9 \end{pmatrix} \begin{matrix} -2 \\ + \end{matrix} \quad \rightsquigarrow \quad \begin{pmatrix} t-1 & -2 & -3 \\ -2t-2 & t-1 & 0 \\ -7 & -8 & t-9 \end{pmatrix}.$$

Entwickeln nach der zweiten Zeile liefert dann:

$$\begin{aligned} \chi_A &= 2(t+1)\cdot\det\begin{pmatrix} -2 & -3 \\ -8 & t-9 \end{pmatrix} + (t-1)\cdot\det\begin{pmatrix} t-1 & -3 \\ -7 & t-9 \end{pmatrix} \\ &= 2(t+1)\big[-2(t-9)-24\big] + (t-1)\big[(t-1)(t-9)-21\big] \\ &= -4(t+1)(t+3) + (t-1)(t^2-10t-12) \\ &= -4(t^2+4t+3) + t^3 - 10t^2 - 12t - t^2 + 10t + 12 \\ &= t^3 - 15t^2 - 18t. \end{aligned}$$

iii.) *Ein weiteres Beispiel zur Berechnung eines charakteristischen Polynoms einer reellen (3×3)-Matrix ist:*

$$A := \begin{pmatrix} 1 & -8 & -4 \\ -8 & 1 & -4 \\ -4 & -4 & 7 \end{pmatrix} \quad \Longrightarrow \quad \chi_A = \det \begin{pmatrix} t-1 & 8 & 4 \\ 8 & t-1 & 4 \\ 4 & 4 & t-7 \end{pmatrix}.$$

Zuerst die Matrix transformiert, bevor der Laplacesche Entwicklungssatz angewendet wird:

$$\begin{pmatrix} t-1 & 8 & 4 \\ 8 & t-1 & 4 \\ 4 & 4 & t-7 \end{pmatrix} \begin{matrix} -1 \\ + \end{matrix} \quad \rightsquigarrow \quad \begin{pmatrix} t-1 & 8 & 4 \\ -t+9 & t-9 & 0 \\ 4 & 4 & t-7 \end{pmatrix}.$$

Nun liefert die Entwicklung nach der zweiten Zeile:

$$\begin{aligned} \chi_A &= (t-9)\cdot\det\begin{pmatrix} 8 & 4 \\ 4 & t-7 \end{pmatrix} + (t-9)\cdot\det\begin{pmatrix} t-1 & 4 \\ 4 & t-7 \end{pmatrix} \\ &= (t-9)[8t-56-16] + (t-9)[t^2-8t+7-16] \\ &= (t-9)[8t-72] + (t-9)[t^2-8t-9] = (t-9)(t^2-81) \end{aligned}$$

$$= (t-9)(t-9)(t+9) = (t-9)^2(t+9). \qquad \square$$

Wie die obigen Beispiele von (3×3)-Matrizen zeigen, ist die Berechnung von charakteristischen Polynomen aufwendig.

Das charakteristische Polynom einer Matrix $A \in \mathrm{Mat}_n(R)$ erfüllt zumindest einige Regelmäßigkeiten, wie die folgende Aussage zeigt:

Lemma 3.3.53. *Sei R ein kommutativer Ring mit Eins und $A := (a_{i,j}) \in \mathrm{Mat}_n(R)$. Dann gilt für das charakteristische Polynom $\chi_A \in R[t]$:*

i.) χ_A ist ein normiertes Polynom vom Grad n.

ii.) Der Koeffizient c_{n-1} von t^{n-1} ist die negative Summe der Diagonalelemente von A:

$$c_{n-1} = -\sum_{i=0}^{n} a_{i,i}.$$

Die Summe der Diagonalelemente von A wird auch die Spur von A genannt und mit $\mathrm{sp}(A)$ bezeichnet, so daß mit dieser Notation gilt:

$$c_{n-1} = -\,\mathrm{sp}(A).$$

iii.) Das Absolutglied c_0 von χ_A hat die Form $c_0 = (-1)^n \cdot \det(A)$.

Zusammenfassend hat das charakteristische Polynom χ_A für $n \geq 2$ also die Gestalt:

$$\chi_A = t^n - \mathrm{sp}(A) \cdot t^{n-1} + c_{n-2} \cdot t^{n-2} + \ldots + c_1 \cdot t + (-1)^n \cdot \det(A).$$

Beweis.

$i.) + ii.)$: Die beiden Aussagen werden zusammen per Induktion über n bewiesen:

Induktionsanfang: Für $n = 1$ fallen der Koffizient c_{n-1} und c_0 zusammen, was nicht im Widerspruch zur Behauptung steht, denn es ist

$$\det(a_{1,1}) = \mathrm{sp}(a_{1,1}) = a_{1,1},$$

und für χ_A gilt:

$$\chi_A = \det(t \cdot E_1 - A) = \det(t - a_{1,1}) = t - a_{1,1}.$$

Für $n = 2$ läßt sich auch leicht errechnen:

$$\begin{aligned}\chi_A = \det(t \cdot E_2 - A) &= \det \begin{pmatrix} t - a_{1,1} & -a_{1,2} \\ -a_{2,1} & t - a_{2,2} \end{pmatrix} \\ &= (t - a_{1,1})(t - a_{2,2}) - a_{1,2}a_{2,1} \\ &= t^2 - (a_{1,1} + a_{2,2}) \cdot t + a_{1,1}a_{2,2} - a_{1,2}a_{2,1} \\ &= t^2 - \mathrm{sp}(A) \cdot t + (-1)^2 \cdot \det(A).\end{aligned}$$

Induktionsschritt, $n \geq 2$, $n - 1 \rightsquigarrow n$: Es sei definiert:

$$(\widetilde{a}_{i,j}) := \widetilde{A} := t \cdot E_n - A,$$

und es folgt dann insbesondere:

$$\widetilde{a}_{n,n} = t - a_{n,n} \quad \text{und} \quad \widetilde{A}[n,n] = t \cdot E_{n-1} - A[n,n]. \qquad (*)$$

Dann liefert der Laplacesche Entwicklungssatz 3.3.40 für χ_A durch Entwicklung von $\widetilde{A}$ nach der n-ten Zeile:

$$\chi_A = \det(t \cdot E_n - A) = \det(\widetilde{A})$$

$$\overset{(3.3.40)}{=} \sum_{j=1}^{n} (-1)^{n+j} \cdot \widetilde{a}_{n,j} \cdot \det\left(\widetilde{A}[n,j]\right)$$

$$= \widetilde{a}_{n,n} \cdot \det\left(\widetilde{A}[n,n]\right) + \sum_{j=1}^{n-1} (-1)^{n+j} \cdot \widetilde{a}_{n,j} \cdot \det\left(\widetilde{A}[n,j]\right)$$

$$\overset{(*)}{=} \underbrace{(t - a_{n,n}) \cdot \det\left(t \cdot E_{n-1} - A[n,n]\right)}_{=:T_1 \in R[t]} + \underbrace{\sum_{j=1}^{n-1} (-1)^{n+j} \cdot \widetilde{a}_{n,j} \cdot \det\left(\widetilde{A}[n,j]\right)}_{=:T_2 \in R[t]}.$$

Nun werden die Polynome T_1 und T_2 näher betrachtet.

T_1: Es gilt offensichtlich:

$$\det\left(t \cdot E_{n-1} - A[n,n]\right) = \chi_{A[n,n]},$$

und mit der Induktionsannahme folgt dann für $\chi_{A[n,n]}$:

$$\chi_{A[n,n]} = t^{n-1} - \operatorname{sp}\left(A[n,n]\right) \cdot t^{n-2} + \sum_{i=0}^{n-3} d_i t^i.$$

Dies liefert dann für das Polynom T_1:

$$T_1 = (t - a_{n,n}) \cdot \left(t^{n-1} - \operatorname{sp}\left(A[n,n]\right) \cdot t^{n-2} + \sum_{i=0}^{n-3} d_i t^i\right)$$

$$= (t - a_{n,n}) \cdot \left(t^{n-1} - \operatorname{sp}\left(A[n,n] \cdot t^{n-2}\right) + \underbrace{(t - a_{n,n}) \cdot \left(\sum_{i=0}^{n-3} d_i t^i\right)}_{=:p_1}\right.$$

$$= t^n - a_{n,n} \cdot t^{n-1} - \operatorname{sp}\left(A[n,n]\right) \cdot t^{n-1} + \underbrace{a_{n,n} \cdot \operatorname{sp}\left(A[n,n]\right) \cdot t^{n-2} + p_1}_{=:p_2}$$

$$= t^n - \left(a_{n,n} + \operatorname{sp}\left(A[n,n]\right)\right) \cdot t^{n-1} + p_2.$$

Die Gradformeln für Polynome (Bemerkung 3.3.47) liefern sofort:

$$\operatorname{grad}(p_1) \leq n - 2 \quad \Longrightarrow \quad \operatorname{grad}(p_2) \leq n - 2,$$

und mit

$$\operatorname{sp}(A) = \operatorname{sp}\left(A[n,n]\right) + a_{n,n}$$

folgt dann letztendlich für T_1:

$$T_1 = t^n - \operatorname{sp}(A) \cdot t^{n-1} + (\text{Polynom vom Grand kleiner gleich } n-2).$$

T_2: Zuerst seien die Matrizen $\widetilde{A}[n,j] \in \operatorname{Mat}_{n-1}\left(R[t]\right)$ betrachtet. In $\widetilde{A}$ sind alle Koeffizienten außerhalb der Diagonalen Konstanten (nämlich $-a_{i,j}$), und auf der Diagonalen stehen Linearfaktoren (nämlich $t - a_{i,i}$). Wird nun die n-te Zeile gestrichen und eine Spalte j mit $j \neq n$, so werden zwei der Linearfaktoren aus $\widetilde{A}$ entfernt, und $\widetilde{A}[n,j]$ enthält außer den Konstanten nur noch $n-2$ Linearfaktoren.

Dann liefern die Gradformeln aus Bemerkung 3.3.47 bei der Berechnung des Polynoms $\det\left(\widetilde{A}[n,j]\right)$ mittels der Leibniz-Formel 3.3.1 für dessen Grad mit $(b_{k,l}) := \widetilde{A}[n,j] \in \mathrm{Mat}_{n-1}\left(R[t]\right)$:

$$\begin{aligned}\operatorname{grad}\left(\det\left(\widetilde{A}[n,j]\right)\right) &= \operatorname{grad}\left(\sum_{\sigma\in S_{n-1}}\left(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n-1} b_{i,\sigma(i)}\right)\right)\\ &\leq \max_{\sigma\in S_{n-1}}\Bigg(\underbrace{\operatorname{grad}\left(\operatorname{sign}(\sigma)\cdot\prod_{i=1}^{n-1} b_{i,\sigma(i)}\right)}_{\leq n-2}\Bigg) \leq n-2, \qquad (\star)\end{aligned}$$

da im Produkt $\prod_{i=1}^{n-1} b_{i,\sigma(i)}$ höchstens $n-2$ Linearfaktoren und sonst nur Konstanten Multipliziert werden.
Damit folgt für den Grad von T_2, da die Terme $\widetilde{a}_{n,j}$ für $j \neq n$ alle Konstanten sind:

$$\begin{aligned}\operatorname{grad}(T_2) &= \operatorname{grad}\left(\sum_{j=1}^{n-1}\underbrace{(-1)^{n+j}\cdot\widetilde{a}_{n,j}\cdot\det\left(\widetilde{A}[n,j]\right)}_{\in R[t]}\right)\\ &\leq \max_{1\leq j\leq n-1}\left(\operatorname{grad}\left(\underbrace{(-1)^{n+j}\cdot\widetilde{a}_{n,j}}_{\text{Konstante}}\cdot\underbrace{\det\left(\widetilde{A}[n,j]\right)}_{(\star)\colon \operatorname{grad}\leq n-2}\right)\right) \leq n-2.\end{aligned}$$

Also ist T_2 ein Polynom mit einem Grad kleiner gleich $n-2$.
Nun folgt für χ_A die Behauptung:

$$\begin{aligned}\chi_A &= T_1 + T2\\ &= t^n - \operatorname{sp}(A)\cdot t^{n-1} + (\text{Polynom vom Grad kleiner gleich } n-2) \qquad (\leftarrow T_1)\\ &\qquad\qquad + (\text{Polynom vom Grad kleiner gleich } n-2) \qquad (\leftarrow T_2)\\ &= t^n - \operatorname{sp}(A)\cdot t^{n-1} + (\text{Polynom vom Grad kleiner gleich } n-2).\end{aligned}$$

iii.): Wird in das Polynom $\chi_A(t)$ für t der Wert Null eingesetzt, so folgt mit den Determinanteneigenschaften aus Satz 3.3.22:

$$\chi_A(0) = \det(0\cdot E_n - A) = \det\left((-1)\cdot A\right) \overset{(3.3.22)}{=} (-1)^n\cdot\det(A).$$

Offensichtlich liefert das Einsetzen der Null in ein Polynom $p(t) = \sum_{i=0}^{n} a_i\cdot t^i$ als Wert dessen Absolutglied, $p(0) = c_0$, so daß die Behauptung bewiesen ist. □

Bemerkung 3.3.54.

i.) Nach Lemma 3.3.53 ist das charakteristische Polynom einer quadratischen Matrix über einem Ring R ein normiertes Polynom in $R[t]$. Diese Aussage kann umgekehrt werden, denn jedes normierte Polynom aus $R[t]$ tritt auch als charakteristische Polynom einer Matrix auf: Sei dazu das normierte Polynom

$$p := t^n + \sum_{i=0}^{n-1} a_i\cdot t^i \in R[t]$$

gegeben, und zu p sei die folgende Matrix betrachtet:

$$A_p := \begin{pmatrix} 0 & & & & & -a_0 \\ 1 & 0 & & & & -a_1 \\ & 1 & 0 & & & -a_2 \\ & & \ddots & \ddots & & \vdots \\ & & & 1 & 0 & -a_{n-2} \\ & & & & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{Mat}_n(R).$$

Diese Matrix A_p wird mitunter auch die Begleitmatrix von A genannt.
Dann folgt für χ_{A_p} mit der Übungsaufgabe 2.b) von Aufgabenblatt 3 (LAIIa):

$$\chi_{A_p} = \det\big(t \cdot E_n - A_p\big) = \det \begin{pmatrix} t & & & & & a_0 \\ -1 & t & & & & a_1 \\ & -1 & t & & & a_2 \\ & & \ddots & \ddots & & \vdots \\ & & & -1 & t & a_{n-2} \\ & & & & -1 & t + a_{n-1} \end{pmatrix} = t^n + \sum_{i=0}^{n-1} a_i \cdot t^i.$$

ii.) *Folgende Regeln für die Spur von quadratischen Matrizen sind kleine Übungsaufgaben, und es gilt mit $\alpha \in R$, $A, B \in \mathrm{Mat}_n(R)$ und $C \in \mathrm{GL}_n(R)$:*

$$\begin{aligned} \mathrm{sp}(\alpha \cdot A) &= \alpha \cdot \mathrm{sp}(A), \\ \mathrm{sp}(A + B) &= \mathrm{sp}(A) + \mathrm{sp}(B), \\ \mathrm{sp}(AB) &= \mathrm{sp}(BA), \\ \mathrm{sp}(CAC^{-1}) &= \mathrm{sp}(A). \end{aligned}$$

Die ersten beiden Gleichungen besagen, daß die „Spur“ als folgende R-lineare Abbildung zwischen den freien R-Moduln $\mathrm{Mat}_n(R)$ und R aufgefaßt werden kann:

$$\mathrm{sp}\colon \mathrm{Mat}_n(R) \longrightarrow R \quad \textit{mit} \quad A \mapsto \textit{Summe der Diagonalelemete von } A.$$

Daß die Spur nicht verträglich mit der Matrizenmultiplikation und damit kein Ringhomomorphismus ist, zeigt folgendes Beispiel:

$$A := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \Longrightarrow \quad AB = \textit{Nullmatrix},$$

und dies liefert:

$$\mathrm{sp}(AB) = 0 \neq 1 = 1 \cdot 1 = \mathrm{sp}(A) \cdot \mathrm{sp}(B).$$

iii.) *Für eine Matrix $A \in \mathrm{Mat}_n(R)$ kann das charakteristische Polynom sofort mit Lemma 3.3.53 beschrieben werden, da es als normiertes quadratisches Polynom nur die Koeffizienten enthält, die dort näher beschrieben sind, und wegen $(-1)^2 = 1$ folgt:*

$$\chi_A = t^2 - \mathrm{sp}(A) \cdot t + \det(A).$$

Mit Matrizenkoeffizienten beschrieben lautet die Formel:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Longrightarrow \quad \chi_A = t^2 - (a + d) \cdot t + (ad - bc). \qquad \square$$

3.4. Matrizendarstellungen linearer Abbildungen

In Satz 3.1.14 wurde eine eineindeutige Beziehung zwischen Matrizen und linearen Abbildungen von Spaltenräumen ($R^{[n]}$ nach $R^{[m]}$) hergestellt durch die zueinander inversen Abbildungen:

$$\begin{aligned} \mathrm{Mat}(m \times n, R) \xrightarrow{\sim} \mathrm{Hom}_R(R^{[n]}, R^{[m]}) \quad \text{mit} \quad A \mapsto \varphi_A \colon \quad & R^{[n]} \longrightarrow R^{[m]} \\ & x \mapsto Ax, \\ \mathrm{Hom}_R(R^{[n]}, R^{[m]}) \xrightarrow{\sim} \mathrm{Mat}(m \times n, R) \qquad \text{mit} \quad \varphi \mapsto [\varphi], \end{aligned}$$

wobei die Matrix $[\varphi]$ definiert war durch den spaltenweisen Eintrag der Bilder der Standard-Basis $e_1, \ldots, e_n$ des $R^{[n]}$ unter φ:

$$[\varphi] := \begin{pmatrix} | & & | \\ \varphi(e_1) & \cdots & \varphi(e_n) \\ | & & | \end{pmatrix}.$$

Diese Zuordnungen sind sogar R-Modulisomorphismen zwischen den beiden R-Moduln $\mathrm{Hom}_R(R^{[n]}, R^{[m]})$ und $\mathrm{Mat}(m \times n, R)$, wobei insbesondere die folgende später wichtig ist:

$$[\,\cdot\,] \colon \mathrm{Hom}_R(R^{[n]}, R^{[m]}) \xrightarrow{\sim} \mathrm{Mat}(m \times n, R) \quad \text{mit} \quad \varphi \mapsto [\varphi].$$

Es ist dann möglich, Eigenschaften einer linearen Abbildung $\varphi \in \mathrm{Hom}_R(R^{[n]}, R^{[m]})$ an der Matrix $[\varphi]$ zu studieren, wobei zur Lösung der Probleme bei Matrizen (Zahlentafeln!) mitunter einfache Algorithmen zur Verfügung stehen. Folgende Tabelle listet einige Zusammenhänge zwischen φ und $[\varphi]$ auf (siehe dazu auch Lemma 3.1.17 und Satz 3.1.20):

φ:	$[\varphi]$:
injektiv	Spalten linear unabhängig
surjektiv	Spalten Erzeugendensystem des Zielraumes
bijektiv	Spalten Basis des Zielraumes
$\mathrm{im}(\varphi)$	Spalten erzeugen $\mathrm{im}(\varphi)$
$\ker(\varphi)$	Lösung des LGS: $[\varphi] \cdot z = 0$
Faser $\varphi^{-1}(b)$	Lösung des LGS: $[\varphi] \cdot z = b$
φ invertierbar	$[\varphi]$ invertierbar

Ist φ ein Endomorphismus und $[\varphi]$ damit eine quadratische Matrix, können viele der Fragestellungen bei der Matrix mit Hilfe von Determinanten gelöst werden. Und ist R ein Körper, so steht für alle Matrizen $[\varphi]$ (also auch für die Matrizendarstellungen von Nicht-Endomorphismen) bei allen Fragestellungen der Gauß-Algorithmus als Lösungshilfe zur Verfügung.

Ziel ist es nun, Matrizendarstellungen linearer Abbildungen zwischen Spaltenräumen auf Matrizendarstellungen linearer Abbildungen zwischen beliebigen Moduln zu übertragen und einem $f \colon M \longrightarrow N$ eine Matrix $[f]$ zuzuordnen. Dabei ist die Forderung „beliebige Moduln“ zu hoch gegriffen: das Matrizenkalkühl ist eng mit den Spaltenräumen verbunden, und so müssen die Moduln zu solchen isomorph sein - also freie Moduln mit endlichen Basen sein. Bei Vektorräumen ist dies keine wirkliche

Einschränkung, da alle Vektorräume eine Basis besitzen und damit freie Moduln sind - nur deren Endlichdimensionalität ist dann eine echte Voraussetzung.

Es werden also jetzt für einen kommutativen Ring R mit Eins freie R-Moduln M, N betrachtet, die jeweils eine endliche Basis besitzen. Ist dabei $B := (b_1, \ldots, b_m)$ eine Basis von M und $C := (c_1, \ldots, c_n)$ eine Basis von N, so liefern diese Basen Isomorphismen in die Spaltenräume $R^{[n]}$ und $R^{[m]}$ über die lineare Fortsetzung (2.2.31) der Basiszuordnungen:

$$b_1 \mapsto e_1, \ldots, b_m \mapsto e_m \quad \text{und} \quad c_1 \mapsto e_1, \ldots, c_n \mapsto e_n,$$

wobei $e_1, \ldots, e_m$ bzw. $e_1, \ldots, e_n$ jeweils die Standard-Basis des Spaltenraumes $R^{[m]}$ bzw. $R^{[n]}$ bezeichnet. Dies liefert dann folgendes Diagramm von R-Moduln mit Isomorphismen φ und ψ und einer linearen Abbildung $f \in \mathrm{Hom}_R(M, N)$:

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "\varphi"', "\wr"] & N \arrow[d, "\psi"', "\wr"] \\
R^{[m]} & R^{[n]}
\end{tikzcd}$$

Weil φ und ψ Isomorphismen sind, existieren Umkehrabbildungen zu ihnen und das obige Diagramm induziert ein neues, kommutatives Diagramm mit einer linearen Abbildung zwischen den Spaltenräumen:

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "\varphi"', "\wr"] & N \arrow[d, "\psi"', "\wr"] \\
R^{[m]} & R^{[n]}
\end{tikzcd}
\quad \rightsquigarrow \quad
\begin{tikzcd}
M \arrow[r, "f"] & N \arrow[d, "\psi"', "\wr"] \\
R^{[m]} \arrow[u, "\varphi^{-1}", "\wr"'] \arrow[r, dashed, "\psi \circ f \circ \varphi^{-1}"'] & R^{[n]}
\end{tikzcd}$$

Da für die Abbildung $\widetilde{f} := \psi \circ f \circ \varphi^{-1}$ zwischen den Spaltenräumen schon eine Matrizendarstellung $[\widetilde{f}]$ existiert, kann damit nun auch der Abbildung f eine Matrix zuegordnet werden:

$$f \in \mathrm{Hom}_R(M, N) \quad \rightsquigarrow \quad \widetilde{f} \in \mathrm{Hom}_R(R^{[m]}, R^{[n]}) \quad \rightsquigarrow \quad [\widetilde{f}] \in \mathrm{Mat}(n \times m, R).$$

Dabei ist zu untersuchen, ob die obige Zuordnung:

$$\mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(R^{[m]}, R^{[n]}) \quad \text{mit} \quad f \mapsto \psi \circ f \circ \varphi^{-1}$$

ein R-Modulisomorphismus ist. Dies kann mit gleichem Aufwand gleich allgemeiner beantwortet werden, ohne sich auf freie Moduln und Spaltenräume zu beschränken. Sind nämlich R-Moduln M, N und U, V gegeben mit Isomorphismen:

$$\varphi \colon M \longrightarrow U \quad \text{und} \quad \psi \colon N \longrightarrow V,$$

so kann analog zu obigen Diagrammen für ein $f \in \mathrm{Hom}_R(M, N)$ folgendes kommutative Diagramm aufgestellt werden, welches eine Zuordnung von $\mathrm{Hom}_R(M, N)$ und

$\mathrm{Hom}_R(U,V)$ liefert:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, dashed] & N \arrow[d, "\psi"', "\wr"] \\ U \arrow[u, "\varphi^{-1}", "\wr"'] \arrow[r, "\psi\circ f\circ\varphi^{-1}"'] & V \end{tikzcd} \quad \rightsquigarrow \quad \begin{array}{ccc} \mathrm{Hom}_R(M,N) & \longrightarrow & \mathrm{Hom}_R(U,V), \\ f & \mapsto & \psi\circ f\circ\varphi^{-1}. \end{array}$$

Zum Beweis, daß diese Abbildung zwischen den Homomorphismenmoduln ein R-Isomorphismus ist, muß zunächst folgende Hilfsaussage bewiesen werden:

Lemma 3.4.1. *Sei R ein kommutativer Ring mit Eins, und seien M,N,U,V jeweils R-Moduln mit R-linearen Abbildungen:*

$$\varphi\colon U \longrightarrow M, \quad f,h\colon M \longrightarrow N \quad \text{und} \quad \psi\colon N \longrightarrow V.$$

Dann gelten folgende Verknüpfungsregeln:

$$\psi\circ(f+h) = (\psi\circ f)+(\psi\circ h) \quad \text{und} \quad (f+h)\circ\varphi = (f\circ\varphi)+(h\circ\varphi).$$

Dabei ist „+“ auf den Homomorphismenmoduln definiert wie in Satz 2.1.23.

Beweis.
Die behauptete Gleichheit der Abbildungen kann jeweils auf den Modulelementen nachgerechnet werden. Für $m \in M$ gilt:

$$\begin{aligned} \big(\psi\circ(f+h)\big)(m) &= \psi\big((f+h)(m)\big) \overset{(\text{Def } f+h)}{=} \psi\big(f(m)+h(m)\big) \\ &\overset{(\psi \text{ Hom})}{=} \psi\big(f(m)\big)+\psi\big(h(m)\big) = (\psi\circ f)(m)+(\psi\circ h)(m) \\ &= \big((\psi\circ f)+(\psi\circ h)\big)(m). \end{aligned}$$

Ebenso gilt für $u \in U$:

$$\begin{aligned} \big((f+h)\circ\varphi\big)(u) &= (f+h)\big(\varphi(u)\big) \overset{(\text{Def } f+h)}{=} f\big(\varphi(u)\big)+h\big(\varphi(u)\big) \\ &= (f\circ\varphi)(u)+(h\circ\varphi)(u) = \big((f\circ\varphi)+(h\circ\varphi)\big)(u). \end{aligned}$$ □

Dies liefert nun die Aussage:

Satz 3.4.2. *Sei R ein kommutativer Ring mit Eins, und seien M,N und U,V jeweils R-Moduln mit R-Modulisomorphismen:*

$$\varphi\colon M \longrightarrow U \qquad \text{und} \qquad \psi\colon N \longrightarrow V.$$

Dann sind die beiden folgenden Abbildungen ebenfalls R-Modulisomorphismen:

$$\Phi\colon \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(U,V) \quad \text{mit} \quad f \mapsto \psi\circ f\circ\varphi^{-1},$$

$$\Psi\colon \mathrm{Hom}_R(U,V) \longrightarrow \mathrm{Hom}_R(M,N) \quad \text{mit} \quad g \mapsto \psi^{-1}\circ g\circ\varphi.$$

Weiter sind beide Abbildungen zueinander invers, d.h. es gilt:

$$\Phi = \Psi^{-1} \quad \text{und} \quad \Psi = \Phi^{-1}.$$

Für einen Isomorphismus $f \in \mathrm{Hom}_R(M,N)$ ist $\Phi(f)$ ein Isomorphismus von U nach V, und ebenso ist für einen Isomorphismus $g \in \mathrm{Hom}_R(U,V)$ auch $\Psi(g)$ ein Isomorphismus von M nach N.

Beweis.
Φ und Ψ sind wohldefinierte Abbildungen, denn die Abbildungen $\psi \circ f \circ \varphi^{-1}$ und $\psi^{-1} \circ g \circ \varphi$ haben offensichtlich die richtigen Definitions- und Wertebereiche und sind als Komposition von R-linearen Abbildungen auch wieder R-linear (Satz 2.1.22).
Nun ist zu zeigen, daß Φ und Ψ R-lineare Abbildung sind, und die jeweilige Strukturverträglichkeit mit der Addition folgt sofort aus Lemma 3.4.1:

$$\begin{aligned}
\Phi(f+\widetilde{f}) &= \psi \circ (f+\widetilde{f}) \circ \varphi^{-1} \overset{(3.4.1)}{=} \psi \circ \big((f \circ \varphi^{-1}) + (\widetilde{f} \circ \varphi^{-1})\big) \\
&\overset{(3.4.1)}{=} (\psi \circ f \circ \varphi^{-1}) + (\psi \circ \widetilde{f} \circ \varphi^{-1}) = \Phi(f) + \Phi(\widetilde{f}), \\
\Psi(g+\widetilde{g}) &= \psi^{-1} \circ (g+\widetilde{g}) \circ \varphi \overset{(3.4.1)}{=} \psi^{-1} \circ \big((g \circ \varphi) + (\widetilde{g} \circ \varphi)\big) \\
&\overset{(3.4.1)}{=} (\psi^{-1} \circ g \circ \varphi) + (\psi^{-1} \circ \widetilde{g} \circ \varphi) = \Psi(g) + \Psi(\widetilde{g}).
\end{aligned}$$

Die Verträglichkeit von Φ und Ψ mit der skalaren Multiplikation Homomorphismen folgt sofort aus deren Definition, denn es gilt für eine R-lineare Abbildung h und einen Vektor x:

$$(\lambda h)(x) = \lambda\big(h(x)\big) \qquad \text{(Satz 2.1.25)}, \tag{$*$}$$

und dann gilt wegen der R-Linearität von ψ für $u \in U$:

$$\begin{aligned}
\Phi(\lambda f)(u) &= \big(\psi \circ (\lambda f) \circ \varphi^{-1}\big)(u) = \psi\Big((\lambda f)\big(\varphi^{-1}(u)\big)\Big) \overset{(*)}{=} \psi\Big(\lambda\Big(f\big(\varphi^{-1}(u)\big)\Big)\Big) \\
&\overset{(\psi \text{ Hom})}{=} \lambda\psi\Big(\Big(f\big(\varphi^{-1}(u)\big)\Big)\Big) = \lambda\Phi(f)(u).
\end{aligned}$$

Ebenso folgt für alle $m \in M$ mit der R-Linearität von ψ^{-1}:

$$\begin{aligned}
\Psi(\lambda g)(m) &= \big(\psi^{-1} \circ (\lambda g) \circ \varphi\big)(m) = \psi^{-1}\Big((\lambda g)\big(\varphi(m)\big)\Big) \overset{(*)}{=} \psi^{-1}\Big(\lambda\Big(g\big(\varphi(m)\big)\Big)\Big) \\
&\overset{(\psi^{-1} \text{ Hom})}{=} \lambda\psi^{-1}\Big(\Big(g\big(\varphi(m)\big)\Big)\Big) = \lambda\Psi(g)(m).
\end{aligned}$$

Die beiden Abbildungen Φ und Ψ heben sich offensichtlich gegenseitig auf:

$$\begin{aligned}
\Psi\big(\Phi(f)\big) &= \Psi\big(\psi \circ f \circ \varphi^{-1}\big) = \psi^{-1} \circ \psi \circ f \circ \varphi^{-1} \circ \varphi = f, \\
\Phi\big(\Psi(g)\big) &= \Phi\big(\psi^{-1} \circ g \circ \varphi\big) = \psi \circ \psi^{-1} \circ g \circ \varphi^{-1} \circ \varphi = g,
\end{aligned}$$

und dies liefert sofort:

$$\Psi \circ \Phi = \mathrm{id}_{\mathrm{Hom}_R(M,N)}, \quad \Phi \circ \Psi = \mathrm{id}_{\mathrm{Hom}_R(U,V)} \quad \Longrightarrow \quad \Psi = \Phi^{-1} \quad \text{und} \quad \Phi = \Psi^{-1}.$$

Die Aussage über die Isomorphismen folgt sofort daraus, daß eine Komposition bijektiver Abbildungen bijektiv ist, und damit gilt:

$$\begin{aligned}
f \text{ bijektiv} \quad &\Longrightarrow \quad \psi \circ f \circ \varphi^{-1} \text{ bijektiv} \quad \Longrightarrow \quad \Phi(f) \text{ bijekitv}, \\
g \text{ bijektiv} \quad &\Longrightarrow \quad \psi^{-1} \circ g \circ \varphi \text{ bijektiv} \quad \Longrightarrow \quad \Psi(g) \text{ bijekitv}.
\end{aligned}$$

(φ, φ^{-1}, ψ und ψ^{-1} sind ja nach Voraussetzung bijektiv.) $\square$

Bemerkung 3.4.3. *Im Beweis von Satz 3.4.2 hätte nur die Linearität einer der beiden Abbildungen Φ oder Ψ gezeigt werden müssen, da später gezeigt wurde, daß beide Abbildungen zueinander invers sind: denn die mengentheoretische Inverse einer linearen Abbildung ist selbst auch linear (Satz 2.1.22).* □

Für Endomorphismenringe isomorpher Moduln gilt zusätzlich, daß die Zuordnung von Endomorphismen analog zu der in Satz 3.4.2 auch ein Ringisomorphismus ist:

Satz 3.4.4. *Sei R ein kommutativer Ring mit Eins, und es seien M, U zueinander isomorphe R-Moduln mit einem Isomorphismus $\varphi\colon M \longrightarrow U$. Dann sind die beiden von Satz 3.4.2 induzierten und zueinander inversen R-Modulisomorphismen:*

$$\Phi\colon \operatorname{End}_R(M) \longrightarrow \operatorname{End}_R(U) \quad \textit{mit} \quad f \mapsto \varphi \circ f \circ \varphi^{-1},$$
$$\Psi\colon \operatorname{End}_R(U) \longrightarrow \operatorname{End}_R(M) \quad \textit{mit} \quad g \mapsto \varphi^{-1} \circ g \circ \varphi.$$

auch Ringisomorphismen, d.h. strukturverträglich mit der Multiplikation in den Endomorphismenringen.
Beide Ringisomorphismen bilden die Einsen der Ringe aufeinander ab.
Für einen Automorphismus $f \in \mathrm{GL}_R(M)$ ist $\Phi(f)$ ein Automorphismus von U, ebenso für einen Automorphismus $g \in \mathrm{GL}_R(U)$ auch $\Psi(g)$ ein Automorphismus von M, so daß Φ und Ψ nach Einschränkung auf die jeweiligen (multiplikativen) Automorphismengruppen auch zueinander inverse Gruppenisomorphismen sind:

$$\Phi\colon \mathrm{GL}_R(M) \longrightarrow \mathrm{GL}_R(U) \quad \textit{und} \quad \Psi\colon \mathrm{GL}_R(U) \longrightarrow \mathrm{GL}_R(M).$$

Beweis.
Die Eigenschaft von Φ und Ψ, bijektiv die Endomorphismenringe aufeinander abzubilden, ist schon durch die Eigenschaft, R-Modulisomorphismen zu sein, gegeben.
Und daß beide Abbildungen die jeweils die Einsen (id_M und id_U) aufeinaner abbilden, ergibt sich sofort aus:

$$\Phi(\mathrm{id}_M) = \varphi \circ \mathrm{id}_M \circ \varphi^{-1} = \varphi \circ \varphi^{-1} = \mathrm{id}_U,$$
$$\Psi(\mathrm{id}_U) = \varphi^{-1} \circ \mathrm{id}_U \circ \varphi = \varphi^{-1} \circ \varphi = \mathrm{id}_M\,.$$

Nach Satz 3.4.2 bilden die Abbildungen Φ und Ψ jeweils Automorphismen auf Automorphismen ab, und so sind die Einschränkungen dieser Abbildungen auf die Mengen $\mathrm{GL}_R(M)$ und $\mathrm{GL}_R(U)$ wohldefiniert wegen:

$$\operatorname{im}(\Phi_{|\mathrm{GL}_R(M)}) \subseteq \mathrm{GL}_R(U) \quad \text{und} \quad \operatorname{im}(\Psi_{|\mathrm{GL}_R(U)}) \subseteq \mathrm{GL}_R(M).$$

Da sie sich nach Satz 3.4.2, auch angewendet auf Automorphismen, „gegenseitig aufheben“, d.h. es gilt:

$$\Psi\big(\Phi(f)\big) = f \quad \text{und} \quad \Phi\big(\Psi(g)\big) = g,$$

sind sie sogar Bijektionen zwischen $\mathrm{GL}_R(M)$ und $\mathrm{GL}_R(U)$.
Die beiden Abbildungen Φ und Ψ sind nach Satz 3.4.2 mit der additiven Struktur des Ringes verträglich, und so muß nur noch die Verträglichkeit mit der Multiplikation überprüft werden, wobei in den Endomorphismenringen die Multiplikation gleich der Komposition von Abbildungen ist:

$$\Phi(f \circ \widetilde{f}) = \varphi \circ (f \circ \widetilde{f}) \circ \varphi^{-1} = \varphi \circ (f \circ \underbrace{\varphi^{-1} \circ \varphi}_{=\mathrm{id}} \circ \widetilde{f}) \circ \varphi^{-1}$$
$$= (\varphi \circ f \circ \varphi^{-1}) \circ (\varphi \circ \widetilde{f} \circ \varphi^{-1}) = \Phi(f) \circ \Phi(\widetilde{f}),$$

$$\Psi(g \circ \widetilde{g}) = \varphi^{-1} \circ (g \circ \widetilde{g}) \circ \varphi = \varphi^{-1} \circ (g \circ \underbrace{\varphi \circ \varphi^{-1}}_{=\mathrm{id}} \circ \widetilde{g}) \circ \varphi$$
$$= (\varphi^{-1} \circ g \circ \varphi) \circ (\varphi^{-1} \circ \widetilde{g} \circ \varphi) = \Psi(g) \circ \Psi(\widetilde{g}). \qquad \square$$

Bemerkung 3.4.5.

i.) Im Beweis von Satz 3.4.4 braucht eigentlich nur für eine Abbildung Φ oder Ψ gezeigt werden, daß sie ein Ringhomomorphismus ist, da beide Abbildungen zueinander invers sind, und die mengentheoretische Umkehrabbildung eines Ringhomomorphismus selbst auch ein Ringhomomorphismus ist (Satz 1.3.40).

ii.) In Satz 3.4.2 wurde für R-Moduln M, N, U und V mit Isomorphismen:

$$\varphi\colon M \longrightarrow U \quad \textit{und} \quad \psi\colon N \longrightarrow V$$

gezeigt, daß die folgende Zuordnung ein Isomorphismus ist:

$$\Phi\colon \operatorname{Hom}_R(M,N) \xrightarrow{\sim} \operatorname{Hom}_R(U,V) \quad \textit{mit} \quad f \mapsto \psi \circ f \circ \varphi^{-1}.$$

Für den Fall $M = N$ und $U = V$ liefert dies eine dann einen Isomorphismus:

$$\Phi\colon \operatorname{End}_R(M) \xrightarrow{\sim} \operatorname{End}_R(U) \quad \textit{mit} \quad f \mapsto \psi \circ f \circ \varphi^{-1}.$$

Dabei sind also zwei verschiedene Isomorphismen $\varphi, \psi\colon M \longrightarrow U$ vorgegeben und liefern Diagramme:

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, dashed] & M \arrow[d, "\psi"', "\wr"] \\
U \arrow[u, "\varphi^{-1}", "\wr"'] \arrow[r, "\psi \circ f \circ \varphi^{-1}"'] & U
\end{tikzcd}$$

Diese Situation kann tatsächlich gewollt sein, aber in diesem Fall ist die Abbildung Φ aus Satz 3.4.4 kein Ringhomomorphismus, da dann in der Beweis-Gleichung:

$$\Phi(f \circ \widetilde{f}) = \psi \circ (f \circ \widetilde{f}) \circ \varphi^{-1}$$

das Einfügen von $\mathrm{id} = \varphi^{-1} \circ \varphi$ aus dem Beweis wegen $\varphi \neq \psi$ nicht hilft, Φ strukturverträglich zu machen:

$$\Phi(f \circ \widetilde{f}) = \psi \circ (f \circ \widetilde{f}) \circ \varphi^{-1} = \psi \circ f \circ \underbrace{\varphi^{-1} \circ \overset{\neq\psi}{\varphi}}_{=\mathrm{id}} \circ \widetilde{f} \circ \varphi^{-1} \neq \Phi(f) \circ \Phi(\widetilde{f}).$$

Daher wird in Satz 3.4.4 auch $\varphi = \psi$ vorausgesetzt. $\square$

Nun kann die allgemeine Situation direkt auf den konkreten Fall angewendet werden, daß M und N freie R-Moduln mit endlichen Basen sind und damit isomorph zu Spaltenräumen:

$$\varphi\colon M \longrightarrow R^{[m]} \quad \text{und} \quad \psi\colon N \longrightarrow R^{[n]}.$$

Da in der Einleitung schon spezielle Isomorphismen φ, ψ mittels Basen von M und N konstruiert wurden und diese Basen im weiteren Verlauf eine Rolle spielen, da ihre Wahl nicht kanonisch ist, seien folgende Konventionen/Notationen gemacht:

Definition 3.4.6. *Sei R ein kommutativer Ring mit Eins und M ein freier R-Modul mit einer endlichen Basis $B := (b_1, \ldots, b_m)$. Für den R-Modul $R^{[m]}$ sei die kanonische Standard-Basis bezeichnet mit:*

$$\mathcal{E}_m := (e_1, \ldots, e_m).$$

Der durch die folgende Bijektion zwischen den Basen B und $\mathcal{E}_m$:

$$b_1 \mapsto e_1, \ldots, b_m \mapsto e_m$$

induzierte R-Modulisomorphismus von M nach $R^{[n]}$ (siehe Satz 2.2.31) wird bezeichnet mit:

$$[\,\cdot\,]_B \colon M \longrightarrow R^{[m]} \quad \text{mit} \quad \sum_{i=1}^{m} a_i b_i \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Dabei wird das Bild von $x := \sum_{i=1}^{m} a_i b_i$ unter $[\,\cdot\,]_B$ auch $[x]_B$ notiert:

$$[x]_B := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Bei der Umkehrabbildung $[\,\cdot\,]_B^{-1} \colon R^{[m]} \longrightarrow M$ wird dann für das Bild eines $y \in R^{[m]}$ analog $[y]_B^{-1}$ geschrieben:

$$[y]_B^{-1} := \sum_{i=1}^{m} a_i b_i \quad \text{für} \quad y := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \in R^{[m]}.$$

Die Abbildung $[\,\cdot\,]_B$ heißt dann die Koordinatenabbildung von M bzgl. der Basis B, und für jeden Vektor $x \in M$ der Spaltenvektor $[x]_B \in R^{[m]}$ der Koordinatenvektor von x bzgl. der Basis B. □

Bemerkung 3.4.7.

i.) Sei M ein freier R-Modul mit einer Basis $B := (b_1, \ldots, b_m)$ und $x \in M$ mit $x := \sum_{i=1}^{m} a_i b_i$. In Definition 2.2.19 wird mit den „Koordinaten“ von x der Zeilenvektor $(a_1, \ldots, a_m) \in R^m$ bezeichnet, in Definition 3.4.6 der Spaltenvektor

$$[x]_B = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \in R^{[m]}$$

als „Koordinatenvektor“. Eine neue Notation ist nötig, da bei Matrizenrechnungen immer mit Spaltenvektoren gearbeitet wird.
In der Literatur wird oft einfach ein Vektor kontextabhängig als Zeilen- oder Spaltenvektor geschrieben, in diesem Skript wird dies durch obige Definition vermieden.

ii.) Ist ein freier R-Modul M mit einer Basis $B := (b_1, \ldots, b_m)$ gegeben, so ist die Koordinatenabbildung:

$$[\,\cdot\,]_B \colon M \longrightarrow R^{[m]}$$

zwar wohldefiniert, für ein $x \in M$ aber erst zu bestimmen, wenn die Linearkombination $x = \sum_{i=1}^{m} a_i b_i$ bekannt ist. Diese ist im allgemeinen aber gar nicht bekannt.

Zum Beispiel ist $(\sqrt{3}, \pi)$, $\big(\log(83), e^{\sin(29)}\big)$ *eine Basis des* $\mathbb{R}^2$, *aber die Koordinaten von* $(3, -2)$ *bezüglich dieser Basis sind nicht offensichtlich.*

iii.) *Für den Spaltenraum* $R^{[m]}$ *und dessen Standard-Basis* $\mathcal{E}_n$ *gilt offensichtlich für die Koordinatenabbildung* $[\,\cdot\,]_{\mathcal{E}_m} \colon R^{[m]} \longrightarrow R^{[m]}$:

$$x := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \sum_{i=1}^{m} a_i e_i \quad \Longrightarrow \quad [x]_{\mathcal{E}_m} = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = x \quad \Longrightarrow \quad [\,\cdot\,]_{\mathcal{E}_m} = \mathrm{id}_{R^{[m]}}\,.$$

iv.) *Für den Zeilenraum* R^m *gilt bzgl. seiner kanonischen Standard-Zeilen-Basis* $\mathcal{E}_m := (e_1, \ldots, e_m)$:

$$x := (a_1, \ldots, a_m) = \sum_{i=1}^{m} a_i e_i \quad \Longrightarrow \quad [x]_{\mathcal{E}_m} = \big[(a_1, \ldots, a_n)\big]_{\mathcal{E}_m} = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}.$$

Hier ist für die Standard-Zeilen-Basis die gleiche Bezeichnung $\mathcal{E}_m$ *gewählt wie für die Standard-Spalten-Basis. Der Koordinatenvektor des Zeilen-Vektors* x *bzgl. der Standard-Zeilen-Basis ist dann der transponierte Spaltenvektor* x^t. □

Beispiel 3.4.8.

i.) *Es sei die Basis* $B := \big((1,2),(2,1)\big)$ *des* $\mathbb{R}^2$ *gegeben. Dann hat der Vektor* $(3,3) \in \mathbb{R}^2$ *bzgl. der Basis* B *den folgenden Koordinatenvektor:*

$$(3,3) = 1 \cdot (1,2) + 1 \cdot (2,1) \quad \Longrightarrow \quad \big[(3,3)\big]_B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

ii.) *Im Polynomvektorraum* $\mathbb{Q}[t]_{|2}$ *sind* $B := (1, t, t^2)$ *und* $C := (t^2, 1, t)$ *jeweils Basen. Das Polynom* $p := 3t^2 - 2t + 7$ *hat dann bzgl. dieser Basen folgende Koordinatenvektoren:*

$$p = 3t^2 - 2t + 7 = 3 \cdot t^2 + (-2) \cdot t + 7 \cdot 1 \quad \Longrightarrow \quad [p]_B = \begin{pmatrix} 7 \\ -2 \\ 3 \end{pmatrix}, \quad [p]_C = \begin{pmatrix} 3 \\ 7 \\ -2 \end{pmatrix}.$$

iii.) *Der* $\mathbb{Z}$*-Matrizenmodul* $\mathrm{Mat}_2(\mathbb{Z})$ *hat eine Basis:*

$$B := \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

Dann gilt für die Koordinantenvektoren von Matrizen $A \in \mathrm{Mat}_2(\mathbb{Z})$ *bzgl. dieser Basis:*

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right]_B = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

iv.) *Für* $M := \{1,2,3\}$ *ist im* $\mathbb{Z}_2$*-Vektorraum* $\mathcal{P}(M)$ *das System:*

$$B := \big(\{1\}, \{2,3\}, \{1,3\}\big)$$

eine Basis, und der Vektor $\{1,2\}$ *hat bzgl. dieser folgenden Koordinatenvektor:*

$$\{1,2\} = [0]_2 \cdot \{1\} \ominus [1]_2 \cdot \{2,3\} \ominus [1]_2 \cdot \{1,3\} \quad \Longrightarrow \quad \big[\{1,2\}\big]_B = \begin{pmatrix} [0]_2 \\ [1]_2 \\ [1]_2 \end{pmatrix}. \quad \square$$

Mit dieser neuen Notation können nun die Sätze 3.4.2 und 3.4.4 sofort auf die spezielle Situation, mittels Koordinatenabbildungen in Spaltenräume zu laufen, formuliert werden:

Satz 3.4.9. *Sei R ein kommutativer Ring mit Eins, und seien M, N freie R-Moduln mit jeweils endlicher Basis. Dabei sei B eine Basis von M mit $m := |B|$, und C sei eine Basis von N mit $n := |C|$. Dann sind die folgenden Abbildungen zueinander inverse R-Modulisomorphismen:*

$$\begin{aligned} \Phi_{C,B}\colon \operatorname{Hom}_R(M,N) &\longrightarrow \operatorname{Hom}_R(R^{[m]},R^{[n]}) \quad \textit{mit} \quad f \mapsto [\,\cdot\,]_C \circ f \circ [\,\cdot\,]_B^{-1}, \\ \Psi_{C,B}\colon \operatorname{Hom}_R(R^{[m]},R^{[n]}) &\longrightarrow \operatorname{Hom}_R(M,N) \quad \textit{mit} \quad g \mapsto [\,\cdot\,]_C^{-1} \circ g \circ [\,\cdot\,]_B. \end{aligned}$$

$\Phi_{C,B}$ und $\Psi_{C,B}$ bilden dabei die Isomorphismen der jeweiligen Räume bijektiv aufeinander ab.

Beweis.
Siehe Satz 3.4.2 mit $U := R^{[m]}$ und $\varphi := [\,\cdot\,]_B$ und $V := R^{[n]}$ mit $\psi := [\,\cdot\,]_C$. □

Satz 3.4.10. *Sei R ein kommutativer Ring mit Eins und M ein freier R-Modul mit einer endlichen Basis. Dabei sei B eine Basis von M mit $m := |B|$. Dann sind die von Satz 3.4.9 induzierten zueinander inversen R-Modulisomorphismen:*

$$\begin{aligned} \Phi_{B,B}\colon \operatorname{End}_R(M) &\longrightarrow \operatorname{End}_R(R^{[m]}) \quad \textit{mit} \quad f \mapsto [\,\cdot\,]_B \circ f \circ [\,\cdot\,]_B^{-1}, \\ \Psi_{B,B}\colon \operatorname{End}_R(R^{[m]}) &\longrightarrow \operatorname{End}_R(M) \quad \textit{mit} \quad g \mapsto [\,\cdot\,]_B^{-1} \circ g \circ [\,\cdot\,]_B, \end{aligned}$$

auch Ringisomorphismen, d.h. strukturverträglich mit der Multiplikation in den Endomorphismenringen.
Beide Ringisomorphismen bilden die Einsen der Ringe aufeinander ab.
Für einen Automorphismus $f \in \mathrm{GL}_R(M)$ ist $\Phi(f)$ ein Automorphismus von $R^{[m]}$, ebenso für einen Automorphismus $g \in \mathrm{GL}_R(R^{[m]})$ auch $\Psi(g)$ ein Automorphismus von M, so daß Φ und Ψ nach Einschränkung auf die jeweiligen Automorphismengruppen auch zueinander inverse Gruppenisomorphismen sind:

$$\Phi\colon \mathrm{GL}_R(M) \longrightarrow \mathrm{GL}_R(R^{[m]}) \quad \textit{und} \quad \Psi\colon \mathrm{GL}_R(R^{[m]}) \longrightarrow \mathrm{GL}_R(M).$$

Beweis.
Siehe Satz 3.4.4 mit $U := R^{[m]}$ und $\varphi := [\,\cdot\,]_B$. □

Folgende Aussagen über die Abbildung $\Phi_{C,B}$ sind noch von Interesse:

Lemma 3.4.11. *Sei R ein kommutativer Ring mit Eins, und es seien M, N und U jeweils freie R-Moduln mit endlichen Basen. Dabei sei B eine Basis von M, C eine Basis von N und D eine Basis von U.*
Sind dann $f \in \operatorname{Hom}_R(M,N)$ und $g \in \operatorname{Hom}_R(N,U)$, so gilt für die in Satz 3.4.9 definierten Abbildungen:

$$\Phi_{D,B}(g \circ f) = \Phi_{D,C}(g) \circ \Phi_{C,B}(f).$$

Ist $f \in \operatorname{Hom}(M,N)$ ein Isomorphismus, so auch $f^{-1} \in \operatorname{Hom}_R(N,M)$, und es gilt:

$$\big(\Phi_{C,B}(f)\big)^{-1} = \Phi_{B,C}(f^{-1}) \quad \textit{und} \quad \big(\Phi_{B,C}(f^{-1})\big)^{-1} = \Phi_{C,B}(f).$$

Beweis.
Mit den Definitionen aus Satz 3.4.9 folgt sofort:

$$\begin{aligned}\Phi_{D,B}(g\circ f) &= [\,\cdot\,]_D\circ(g\circ f)\circ[\,\cdot\,]_B^{-1} = [\,\cdot\,]_D\circ(g\circ\underbrace{[\,\cdot\,]_C^{-1}\circ[\,\cdot\,]_C}_{=\mathrm{id}}\circ f)\circ[\,\cdot\,]_B^{-1}\\ &= \big([\,\cdot\,]_D\circ g\circ[\,\cdot\,]_C^{-1}\big)\circ\big([\,\cdot\,]_C\circ f\circ[\,\cdot\,]_B^{-1}\big) = \Phi_{D,C}(g)\circ\Phi_{C,B}(f).\end{aligned}$$

Für einen Isomorphismus $f\in\mathrm{Hom}_R(M,N)$ und seine Inverse $f^{-1}\in\mathrm{Hom}_R(N,M)$ gelten die Beziehungen:

$$f^{-1}\circ f=\mathrm{id}_M \quad\text{und}\quad f\circ f^{-1}=\mathrm{id}_N\,.$$

Mit $m:=|B|$, $n:=|C|$ und dem schon Bewiesenen folgt dann:

$$\begin{aligned}\mathrm{id}_{R^{[m]}} &= \Phi_{B,B}(\mathrm{id}_M) = \Phi_{B,B}(f^{-1}\circ f) = \Phi_{B,C}(f^{-1})\circ\Phi_{C,B}(f),\\ \mathrm{id}_{R^{[n]}} &= \Phi_{C,C}(\mathrm{id}_N) = \Phi_{C,C}(f\circ f^{-1}) = \Phi_{C,B}(f)\circ\Phi_{B,C}(f^{-1}),\end{aligned}$$

was wiederum sofort die behaupteten Gleichungen impliziert:

$$\big(\Phi_{C,B}(f)\big)^{-1}=\Phi_{B,C}(f^{-1}) \quad\text{und}\quad \big(\Phi_{B,C}(f^{-1})\big)^{-1}=\Phi_{C,B}(f). \qquad\square$$

Bemerkung 3.4.12. *In Satz 3.4.9 wurde für R-Moduln M und N mit Basen B und C die Abbildung:*

$$\Phi_{C,B}\colon\ \mathrm{Hom}_R(M,N)\longrightarrow\mathrm{Hom}_R(R^{[m]},R^{[n]})$$

eingeführt, bei der die Basen im Index „falsch herum“ notiert sind, denn ein darin einzusetzendes $f\in\mathrm{Hom}_R(M,N)$ bildet ja von M nach N ab und damit salopp „B nach C“. Aber die Formel in Lemma 3.4.11 macht den Sinn davon klar, denn bei:

$$\Phi_{D,C}(g)\circ\Phi_{C,B}(f)=\Phi_{D,B}(g\circ f)$$

ist die Komposition zweier Abbildungen ja auch von rechts nach links notiert. Und so gilt nun die Faustregel, daß bei obiger Komposition die „inneren Basen“ übereinstimmen müssen und die „äußeren Basen“ die Indizes der Komposition sind.
Ein weiteres Argument wäre natürlich auch die Definition von $\Phi_{C,B}$ selbst, denn in:

$$\Phi_{C,B}(f):=[\,\cdot\,]_C\circ f\circ[\,\cdot\,]_B^{-1}$$

treten die Basen ja auch in der Reihenfolge auf, wie sie bei $\Phi_{C,B}$ im Index notiert sind. $\square$

Nun sind die nötigen Schritte vollzogen, um die eingangs beschriebene Kette von Zuordnungen:

$$f\in\mathrm{Hom}_R(M,N)\quad\rightsquigarrow\quad\widetilde{f}\in\mathrm{Hom}_R(R^{[m]},R^{[n]})\quad\rightsquigarrow\quad[\widetilde{f}]\in\mathrm{Mat}(n\times m,R)$$

mit R-Modulisomorphismen zu beschreiben: Sind in den freien R-Moduln M und N Basen B und C gewählt, erfüllen folgende Abbildungen das Gewünschte:

$$\begin{array}{ccccc}\mathrm{Hom}_R(M,N) & \xrightarrow[\text{Satz 3.4.9}]{\sim} & \mathrm{Hom}_R(R^{[m]},R^{[n]}) & \xrightarrow[\text{Satz 3.1.14}]{\sim} & \mathrm{Mat}(n\times m,R),\\ f & \mapsto & \Phi_{C,B}(f) & \mapsto & \big[\Phi_{C,B}(f)\big].\end{array}$$

Dies führt dann zur endgültigen Definition einer Matrizendarstellung eines linearen Abbildung via der Verkettung von R-Modulisomorphismen:

$$[\,\cdot\,]\circ\Phi_{C,B}\colon\ \mathrm{Hom}_R(M,N)\longrightarrow\mathrm{Mat}(n\times m,R).$$

Definition 3.4.13. *Sei R ein kommutativer Ring mit Eins, und es seien M, N freie R-Moduln mit endlichen Basen. Weiter sei B eine Basis von M mit $m := |B|$ und C eine Basis von N mit $n := |N|$.*
Für $f \in \mathrm{Hom}_R(M, N)$ sei dann folgende Abbildung mit $\Phi_{C,B}$ aus Satz 3.4.9 und $[\,\cdot\,]$ aus Satz 3.1.14 definiert:

$$[\,\cdot\,]_{C,B}\colon\ \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Mat}(n \times m, R) \quad \textit{mit} \quad f \mapsto \big[\Phi_{C,B}(f)\big].$$

Die Matrix $[f]_{C,B}$ heißt die darstellende Matrix von f bzgl. der Basen B und C. □

Die Matrizen $[f]_{C,B}$ sind folgendermaßen aufgebaut:

Lemma 3.4.14. *Sei R ein kommutativer Ring mit Eins, und seien M, N jeweils freie R-Moduln mit endlichen Basen $B := (b_1, \dots b_m)$ von M und C von N mit $m = |B|$ und $n := |C|$.*
Für $f \in \mathrm{Hom}_R(M, N)$ hat die darstellende Matrix $[f]_{C,B} \in \mathrm{Mat}(n \times m, R)$ bzgl. der Basen B und C dann folgende Gestalt:

$$[f]_{C,B} = \begin{pmatrix} | & & | \\ \big[f(b_1)\big]_C & \cdots & \big[f(b_m)\big]_C \\ | & & | \end{pmatrix},$$

d.h. es werden zuerst die Bilder der Basis $b_1, \dots, b_m$ von M unter f gebildet:

$$f(b_1), \dots, f(b_m) \in N,$$

und dann die Koordinatenvektoren dieser „Bilder der Basisvektoren“ bzgl. der Basis C von N in die Spalten der Matrix gesetzt.

Für ein $x \in M$ gilt dann:

$$\big[f(x)\big]_C = [f]_{C,B} \cdot [x]_B.$$

Beweis.
Die darstellende Matrix $[f]_{C,B}$ von f bzgl. der Basen B und C ist definiert als (3.4.13):

$$[f]_{C,B} := \big[\Phi_{C,B}(f)\big].$$

Zuerst wird dabei die lineare Abbildung $f \in \mathrm{Hom}_R(M, N)$ eindeutig der linearen Abbildung $\Phi_{C,B}(f) \in \mathrm{Hom}_R(R^{[m]}, R^{[n]})$ zugeordnet mit der Vorschrift:

$$\Phi_{C,B}(f) = [\,\cdot\,]_C \circ f \circ [\,\cdot\,]_B^{-1}.$$

Danach wird dann der linearen Abbildung $\Phi_{C,B}(f)$ die Matrix $\big[\Phi_{C,B}(f)\big]$ zugeordnet, wobei für ein $\varphi \in \mathrm{Hom}_R(R^{[m]}, R^{[n]})$ die Matrix $[\varphi]$ gebildet wird, indem die Bilder $\varphi(e_1), \dots, \varphi(e_m)$ der Standard-Basisvektoren $e_1, \dots, e_m$ des $R^{[m]}$ spaltenweise in sie eingetragen werden (Satz 3.1.14):

$$[\varphi] := \begin{pmatrix} | & & | \\ \varphi(e_1) & \cdots & \varphi(e_n) \\ | & & | \end{pmatrix}.$$

Es muß also gezeigt werden, daß $\Phi_{C,B}(f)(e_i) = [f(b_i)]_C$ gilt.

Wird nun $e_1, \ldots, e_m$ in $\Phi_{C,B}(f)$ eingesetzt, um $[f]_{C,B}$ zu erhalten, folgt die Behauptung mit $[e_i]_B^{-1} = b_i$ wegen:

$$\Phi_{C,B}(f)(e_i) = \big([\,\cdot\,]_C \circ f \circ [\,\cdot\,]_B^{-1}\big)(e_i) = \Big[f\big(\underbrace{[e_i]_B^{-1}}_{b_i}\big)\Big]_C = \big[f(b_i)\big]_C.$$

Für ein $x \in M$ gilt nach folgendem kommutativen Diagramm:

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "{[\,\cdot\,]_B}"'] \arrow[dr, dashed, "\Phi_{C,B}"] & N \arrow[d, "{[\,\cdot\,]_C}"] \\
R^{[m]} \arrow[r, "\Phi_{C,B}(f)"'] & R^{[n]}
\end{tikzcd}$$

die Gleichung:

$$\big([\,\cdot\,]_C \circ f\big)(x) = \big(\Phi_{C,B}(f) \circ [\,\cdot\,]_B\big)(x) \quad \Longrightarrow \quad \big[f(x)\big]_C = \Phi_{C,B}(f)\big([x]_B\big).$$

Da für die lineare Abbildung $\Phi_{C,B}(f)$ zwischen den Spaltenräumen bzgl. ihrer Matrix $\big[\Phi_{C,B}(f)\big]$ nach Satz 3.1.14 die Gleichung:

$$\Phi_{C,B}(f)(z) \overset{(3.1.14)}{=} [\Phi_{C,B}(f)] \cdot z = [f]_{C,B} \cdot z$$

für alle $z \in R^{[m]}$ gilt, folgt unmittelbar die Behauptung:

$$\begin{aligned}
[f]_{C,B} \cdot [x]_B &= \Phi_{C,B}(f)\big([x]_B\big) = \big([\,\cdot\,]_C \circ f \circ [\,\cdot\,]_B^{-1}\big)\big([x]_B\big) \\
&= \big([\,\cdot\,]_C \circ f \circ [\,\cdot\,]_B^{-1} \circ [\,\cdot\,]_B\big)(x) = \big([\,\cdot\,]_C \circ f\big)(x) = \big[f(x)\big]_C. \qquad \square
\end{aligned}$$

Bemerkung 3.4.15.

i.) Sei $\varphi \in \mathrm{Hom}_R(R^{[n]}, R^{[m]})$. Dann hat nach Satz 3.1.14 die Matrix $[\varphi]$ als Spalten die Bilder $\varphi(e_i)$ der Standard-Basisvektoren $e_1, \ldots, e_n$ des $R^{[n]}$. Nach Lemma 3.4.14 folgt dann sofort:

$$[\varphi] = [\varphi]_{\mathcal{E}_m, \mathcal{E}_n},$$

da $[\varphi]_{\mathcal{E}_m,\mathcal{E}_n}$ die Spalten $[\varphi(e_i)]_{\mathcal{E}_m}$ für die Standard-Basisvekoten $e_1, \ldots, e_n$ des $R^{[n]}$ besitzt, und nach Bemerkung 3.4.7 für den Vektor $\varphi(e_i) \in R^{[m]}$ bzgl. der Basis $\mathcal{E}_m$ gilt: $[\varphi(e_i)]_{\mathcal{E}_m} = \varphi(e_i)$. Somit ist Definition 3.4.13 eine Verallgemeinerung der Konstruktion von Satz 3.1.14.

ii.) Sei $B := (b_1, \ldots, b_n)$ eine Basis des $R^{[n]}$. Dann gilt offensichtlich:

$$[\mathrm{id}]_{\mathcal{E}_n, B} = \begin{pmatrix} | & & | \\ b_1 & \cdots & b_n \\ | & & | \end{pmatrix},$$

denn die Spalten von $[\mathrm{id}]_{\mathcal{E}_n,B}$ sind nach Lemma 3.4.14 die Vektoren:

$$[\mathrm{id}(b_i)]_{\mathcal{E}_n} = [b_i]_{\mathcal{E}_n} \overset{(3.4.7)}{=} b_i. \qquad \square$$

Beispiel 3.4.16.

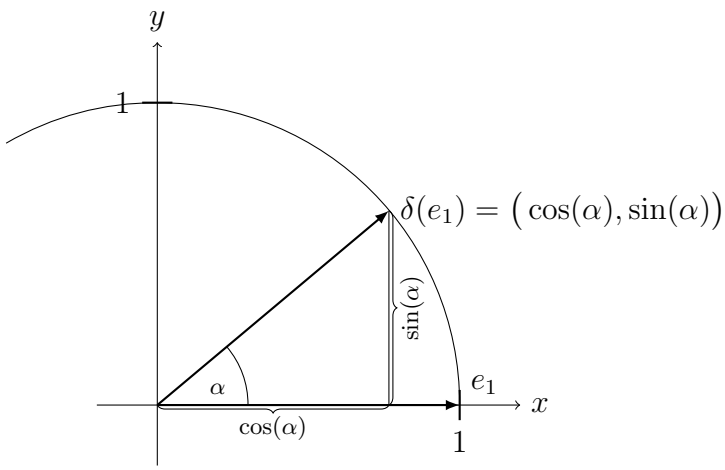
i.) Es sei der $\mathbb{R}^2$ mit der Standard-Zeilen-Basis $\mathcal{E}_2 := (e_1, e_2)$ gegeben und der folgende Endomorphismus betrachtet:

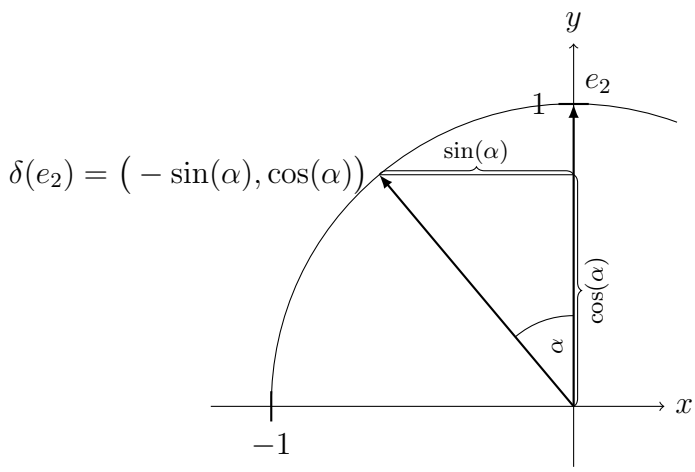
$$\delta_\alpha \colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad x \mapsto \textit{„Drehung von } x \textit{ um den Winkel } \alpha\textit{“}.$$

Für die Bilder der beiden Basisvektoren e_1 und e_2 gilt:

$$\delta(e_1) = \delta\big((1,0)\big) = \big(\cos(\alpha), \sin(\alpha)\big) \quad \textit{und} \quad \delta(e_2) = \delta\big((0,1)\big) = \big(-\sin(\alpha), \cos(\alpha)\big),$$

wie die beiden folgenden Skizzen zeigen:





Die Vektoren $\delta_\alpha(e_1), \delta_\alpha(e_2) \in \mathbb{R}^2$ haben bzgl. der Standard-Zeilen-Basis $\mathcal{E}_2$ des $\mathbb{R}^2$ nach Bemerkung 3.4.7 die Koordinatenvektoren:

$$\big[\delta_\alpha(e_1)\big]_{\mathcal{E}_2} = \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} \qquad \textit{und} \qquad \big[\delta_\alpha(e_2)\big]_{\mathcal{E}_2} = \begin{pmatrix} -\sin(\alpha) \\ \cos(\alpha) \end{pmatrix},$$

und damit gilt für die Matrizendarstellung von δ_α bzgl. der Basis $\mathcal{E}_2$ von $\mathbb{R}^2$ nach Lemma 3.4.14:

$$D_\alpha := [\delta_\alpha]_{\mathcal{E}_2,\mathcal{E}_2} = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

ii.) Es sei der Polynomvektorraum $\mathbb{R}[t]_{|3}$ gegeben mit der Basis $B := (1, t, t^2, t^3)$. Weiter sei die lineare Abbildung „Ableitung“ auf diesem Raum betrachtet, also:

$$D \colon \mathbb{R}[t]_{|3} \longrightarrow \mathbb{R}[t]_{|3} \quad \textit{mit} \quad a_3t^3 + a_2t^2 + a_1t + a_0 \mapsto 3a_3t^2 + 2a_2t + a_1.$$

Es gilt dann für die Bilder der Basisvektoren aus B:

$$D(1) = 0, \quad D(t) = 1, \quad D(t^2) = 2t \quad \textit{und} \quad D(t^3) = 3t^2.$$

Ein Polyonom $a_3t^3 + a_2t^2 + a_1t + a_0$ hat nach Beispiel 3.4.8 bzgl. der Basis B den Koordinatenvektor:

$$[a_3t^3 + a_2t^2 + a_1t + a_0]_B = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix},$$

so daß sich folgende Koordinatenvektoren für die Bilder der Basisvektoren ergeben:

$$\big[D(1)\big]_B = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \big[D(t)\big]_B = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \big[D(t^2)\big]_B = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \quad \big[D(t^2)\big]_B = \begin{pmatrix} 0 \\ 0 \\ 3 \\ 0 \end{pmatrix}.$$

Dies liefert dann nach Lemma 3.4.14 die folgende Matrizendarstellung von D bzgl. der Basis B:

$$[D]_{B,B} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

iii.) Es sei folgende Basis des $\mathbb{R}^3$ gegeben:

$$B := (b_1, b_2, b_3) := \big(\,(1,2,3),\ (4,5,6),\ (7,8,0)\big).$$

Weiter sei $\varphi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^3)$ die lineare Fortsetzung folgender Zuordnung:

$$\varphi\colon \quad (1,2,3) \mapsto (\pi, e^2, 7), \quad (4,5,6) \mapsto (0,0,0), \quad (7,8,0) \mapsto (1,1,1).$$

Mit der Standard-Zeilen-Basis $\mathcal{E}_3$ des $\mathbb{R}^3$ hat die Matrizendarstellung $[\varphi]_{\mathcal{E}_3,B}$ nach Lemma 3.4.14 und Bemerkung 3.4.7 die Form:

$$[\varphi]_{\mathcal{E}_n,B} \overset{(3.4.14)}{=} \begin{pmatrix} | & | & | \\ \big[\varphi(b_1)\big]_{\mathcal{E}_3} & \big[\varphi(b_2)\big]_{\mathcal{E}_3} & \big[\varphi(b_3)\big]_{\mathcal{E}_3} \\ | & | & | \end{pmatrix} \overset{(3.4.7)}{=} \begin{pmatrix} \pi & 0 & 1 \\ e^2 & 0 & 1 \\ 7 & 0 & 1 \end{pmatrix}.$$

iv.) Seien $B := (b_1, \ldots, b_m)$ und $C := (c_1, \ldots, c_m)$ Basen des $R^{[m]}$ für einen kommutativen Ring mit Eins. Weiter sei $\varphi \in \mathrm{End}_R(R^{[m]})$ die lineare Fortsetzung der Abbildung:

$$b_1 \mapsto c_1, \quad \ldots \quad , \quad b_m \mapsto c_m.$$

Da φ eine Basis auf eine Basis abbildet, ist es sogar ein Isomorphismus und besitzt eine Inverse φ^{-1}.
Es gelten folgende Gleichungen für Koordinatenvektoren der Basisvektoren b_i, c_i bzgl. der Basen B, C und der Standard-Basis $\mathcal{E}_m$ des $R^{[m]}$:

$$[b_i]_B = e_i, \quad [c_i]_C = e_i, \quad [b_i]_{\mathcal{E}_m} = b_i \quad \textit{und} \quad [c_i]_{\mathcal{E}_m} = c_i.$$

Es folgen daraus mit Lemma 3.4.14 sofort folgende Matrizendarstellungen von φ und φ^{-1} für den Fall $m := 2$:

$$\begin{aligned}
[\varphi]_{C,B} &= \Big(\big[\varphi(b_1)\big]_C\ \big[\varphi(b_2\big]_C\Big) &&= \Big([c_1]_C\ [c_2]_C\Big) &&= E_2,\\
[\varphi]_{\mathcal{E}_2,B} &= \Big(\big[\varphi(b_1)\big]_{\mathcal{E}_2}\ \big[\varphi(b_2)\big]_{\mathcal{E}_2}\Big) &&= \Big([c_1]_{\mathcal{E}_2}\ [c_2]_{\mathcal{E}_2}\Big) &&= C,\\
[\varphi^{-1}]_{B,C} &= \Big(\big[\varphi^{-1}(c_1)\big]_B\ \big[\varphi^{-1}(c_2)\big]_B\Big) &&= \Big([b_1]_B\ [b_2]_B\Big) &&= E_2,\\
[\varphi^{-1}]_{\mathcal{E}_2,C} &= \Big(\big[\varphi^{-1}(c_1)\big]_{\mathcal{E}_2}\ \big[\varphi^{-1}(c_2)\big]_{\mathcal{E}_2}\Big) &&= \Big([b_1]_{\mathcal{E}_2}\ [b_2]_{\mathcal{E}_2}\Big) &&= B. \qquad \square
\end{aligned}$$

Der folgende Satz faßt noch einmal die bisherigen Ergebnisse zusammen, jedoch in der neu eineführten Notation:

Satz 3.4.17. *Sei R ein kommutativer Ring mit Eins. Weiter seien M und N freie R-Moduln mit endlichen Basen $B := (b_1, \ldots, b_m)$ von M und C von N mit $m := |B|$ und $n := |C|$.*

i.) Die folgende Abbildung aus Definition 3.4.13 ist ein R-Modulisomorphismus:

$$[\,\cdot\,]_{C,B}\colon \operatorname{Hom}_R(M,N) \longrightarrow \operatorname{Mat}(n \times m, R)$$

mit der Abbildungsvorschrift:

$$f \mapsto [f]_{C,B} := \begin{pmatrix} | & & | \\ \big[f(b_1)\big]_C & \cdots & \big[f(b_m)\big]_C \\ | & & | \end{pmatrix}.$$

Für ein $x \in M$ gilt die Koordinatenvektor-Gleichung:

$$\big[f(x)\big]_C = [f]_{C,B} \cdot [x]_B.$$

Sei U ein weiterer freier R-Modul mit einer Basis D, und seien f, g lineare Abbildungen:

$$\overset{B}{M} \xrightarrow{f} \overset{C}{N} \xrightarrow{g} \overset{D}{U}.$$

Dann gilt die Matrizen-Gleichung:

$$[g \circ f]_{D,B} = [g]_{D,C} \cdot [f]_{C,B}.$$

Ist R ein Körper und $f \in \operatorname{Hom}_R(M,N)$ ein Isomorphismus, so ist $[f]_{C,B}$ invertierbar, und es gilt:

$$\big([f]_{C,B}\big)^{-1} = [f^{-1}]_{B,C}.$$

ii.) Für den Endomorphismenring $\operatorname{End}_R(M)$ ist die folgende Abbildung bzgl. einer Basis B ein R-Modulisomorphismus und ein Ringisomorphismus, der die Einsen der Ringe aufeinander abbildet:

$$[\,\cdot\,]_{B,B}\colon \operatorname{End}_R(M) \longrightarrow \operatorname{Mat}_m(R).$$

Eingeschränkt auf die Automorphismengruppe $\operatorname{GL}_R(M)$ ist diese Abbildung ein Gruppenisomorphismus:

$$[\,\cdot\,]_{B,B}\colon \operatorname{GL}_R(M) \longrightarrow \operatorname{GL}_m(R).$$

Es gelten also die folgende Regeln mit $f \in \operatorname{GL}_R(M)$:

$$[\mathrm{id}_M]_{B,B} = E_m \quad \textit{und} \quad \big([f]_{B,B}\big)^{-1} = [f^{-1}]_{B,B}.$$

iii.) Für die freien R-Moduln M und N (mit endlichen Basen) ist $\mathrm{Hom}_R(M,N)$ ein freier R-Modul mit einer endlichen Basis. Folgendes System von $m\cdot n = |B|\cdot|C|$ Abbildungen sind eine Basis von $\mathrm{Hom}_R(M,N)$:

$$\big(\varphi_{i,j}\big)_{(i,j)\in I_{n,m}} \quad \text{mit } \varphi_{i,j} \text{ lineare Fortsetzung von:} \quad b_k \mapsto \delta_{k,j}\cdot c_i = \begin{cases} 0 & \text{für } k \neq j, \\ c_i & \text{für } k = j. \end{cases}$$

Ist R ein Körper, so gilt dann insbesondere die Dimensionsformel:

$$\dim_R\big(\mathrm{Hom}_R(M,N)\big) = \dim_R(M)\cdot\dim_R(N).$$

Beweis.

i.) Die Abbildung $[\,\cdot\,]_{C,B}$ ist definiert als die Komposition:

$$[\,\cdot\,]_{C,B} \overset{(3.4.13)}{=} [\,\cdot\,]\circ\Phi_{C,B}.$$

$\Phi_{C,B}$ ist nach Satz 3.4.9 und $[\,\cdot\,]$ nach Satz 3.1.14 ein R-Modulisomorphismus, also auch deren Komposition.
Die Abbildungsvorschrift und die Koordinatenvektorgleichung sind in Lemma 3.4.14 bewiesen.
Nach Lemma 3.4.11 gilt

$$\Phi_{D,B}(g\circ f) = \Phi_{D,C}(g)\circ\Phi_{C,B}(f), \tag{$*$}$$

und mit Satz 3.1.19 gilt dann:

$$\begin{aligned}[g\circ f]_{D,B} &= \big[\Phi_{D,B}(g\circ f)\big] \overset{(*)}{=} \big[\Phi_{D,C}(g)\circ\Phi_{C,B}\big] \overset{(3.1.19)}{=} \big[\Phi_{D,C}(g)\big]\cdot\big[\Phi_{C,B}(f)\big] \\ &= [g]_{D,C}\cdot[f]_{C,B}.\end{aligned}$$

Ist $f\in\mathrm{Hom}_R(M,N)$ invertierbar, gilt dies nach Lemma 3.4.11 für $\Phi_{C,B}(f)$, und ebenso liefert dieses Lemma die Aussage $\big(\Phi_{C,B}(f)\big)^{-1} = \Phi_{B,C}(f^{-1})$. Mit der Umkehrabbildung $\Phi_{C,B}(f)^{-1}$ und Satz 3.1.19 sowie Satz 3.1.14 folgt dann:

$$\begin{aligned}\big[\Phi_{C,B}(f)\big]\cdot\big[\Phi_{B,C}(f^{-1})\big] &= \big[\Phi_{C,B}(f)\big]\cdot\big[\Phi_{C,B}(f)^{-1}\big] = \big[\Phi_{C,B}(f)\circ\Phi_{C,B}(f)^{-1}\big] \\ &= \big[\,\mathrm{id}_{R^{[n]}}\,\big] = E_n, \\ \big[\Phi_{B,C}(f^{-1})\big]\cdot\big[\Phi_{C,B}(f)\big] &= \big[\Phi_{C,B}(f)^{-1}\big]\cdot\big[\Phi_{C,B}(f)\big] = \big[\Phi_{C,B}(f)^{-1}\circ\Phi_{C,B}(f)\big] \\ &= \big[\,\mathrm{id}_{R^{[m]}}\,\big] = E_m.\end{aligned}$$

Wenn $n=m$ gilt, folgt daraus sofort:

$$\big[\Phi_{C,B}(f)\big]\cdot\big[\Phi_{B,C}(f^{-1})\big] = E_n = \big[\Phi_{B,C}(f^{-1})\big]\cdot\big[\Phi_{C,B}(f)\big],$$

also:

$$[f]_{C,B}\cdot[f^{-1}]_{B,C} = E_n = [f^{-1}]_{B,C}\cdot[f]_{C,B} \quad\Longrightarrow\quad \big([f]_{C,B}\big)^{-1} = [f^{-1}]_{B,C}.$$

Die Aussage $n=m$ kann für einen Körper R daraus gefolgert werden, daß $\Phi_{C,B}(f)$ dann ein Isomorphismus der endlichdimensionalen R-Vektorräume $R^{[m]}$ und $R^{[n]}$ ist und aus Satz 2.2.61 dann Dimensionsgleichheit und damit $n=m$ folgt:

$$R^{[m]}\cong R^{[n]} \quad\overset{2.2.61}{\Longleftrightarrow}\quad \dim_R(R^{[m]}) = \dim_R(R^{[n]} \quad\overset{2.2.49}{\Longleftrightarrow}\quad m=n.$$

ii.) Die Abbildung $[\,\cdot\,]_{B,B}$ ist die Komposition der beiden Abbildungen $[\,\cdot\,]$ aus Satz 3.1.20 und $\Phi_{B,B}$ aus Satz 3.4.10. Beide Abbildungen erfüllen nach diesen Sätzen die behaupteten Eigenschaften, so daß sie auch für deren Komposition gelten.

iii.) Nach Satz 3.1.14 hat der R-Modul $\mathrm{Hom}_R(R^{[m]}, R^{[n]})$ eine Basis $(\psi_{i,j})_{(i,j)\in I_{n,m}}$:

$$\psi_{i,j}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}\right) = x_j e_i.$$

Wird darauf der Isomorphismus $\Psi_{C,B}\colon \mathrm{Hom}_R(R^{[m]}, R^{[n]}) \longrightarrow \mathrm{Hom}_R(M,N)$ aus Satz 3.4.9 angewendet, die Umkehrabbildung von $\Phi_{C,B}$, so bildet dieser Isomorphismus die Basis $(\psi_{i,j})_{(i,j)\in I_{n,m}}$ auf eine Basis in $\mathrm{Hom}_R(M,N)$ ab. Dabei gilt für die Basisvektoren b_i von M:

$$\begin{aligned}\Psi_{C,B}(\psi_{i,j})(b_k) &= \big([\,\cdot\,]_C^{-1} \circ \psi_{i,j} \circ [\,\cdot\,]_B\big)(b_k) = \Big[\psi_{i,j}\big([b_k]_B\big)\Big]_C^{-1} \\ &= \big[\psi_{i,j}(e_k)\big]_C^{-1} = [\delta_{k,j}\cdot e_i]_C^{-1} = \delta_{k,j}\cdot c_i = \varphi_{i,j}(b_k).\end{aligned}$$

Da $\Psi_{C,B}(\psi_{i,j})$ und $\varphi_{i,j}$ auf einer Basis von M übereinstimmen, sind die beiden Abbildungen gleich und damit ist wie behauptet $(\varphi_{i,j})$ eine Basis von $\mathrm{Hom}_R(M,N)$.
Die Aussage über die Dimension von $\mathrm{Hom}_R(M,N)$ folgt sofort aus der Größe des Systems $(\varphi_{i,j})_{(i,j)\in I_{n,m}}$ wegen $|I_{n,m}| = n\cdot m$. □

Nun ist jeder linearen Abbildung $f \in \mathrm{Hom}_R(M,N)$ zwischen freien R-Moduln M und N mit endlichen Basen B von M und C von M eine Matrix $[f]_{C,B}$ zugordnet, und es kann der Zusammenhang zwischen f und $[f]_{C,B}$ betrachtet werden (siehe auch die Einleitung des Abschnitts):

Satz 3.4.18. *Sei R ein kommutativer Ring mit Eins, und seien M und N jeweils freie R-Moduln mit endlichen Basen $B := (b_1,\dots,b_m)$ und $C := (c_1,\dots,c_n)$. Weiter sei $f \in \mathrm{Hom}_R(M,N)$ gegeben.*
Dann gilt für f und seine darstellende Matrix $[f]_{C,B} \in \mathrm{Mat}(n\times m, R)$ bzgl. der Basen B und C folgender Zusammenhang:

i.) Es gelten folgende Äquivalenzen:

$$\begin{aligned} f \text{ injektiv} &\iff \text{Spalten von } [f]_{C,B} \text{ linear unabhängig,} \\ f \text{ surjektiv} &\iff \text{Spalten von } [f]_{C,B} \text{ erzeugen den } R^{[n]}, \\ f \text{ bijektiv} &\iff \text{Spalten von } [f]_{C,B} \text{ sind Basis des } R^{[n]}. \end{aligned}$$

ii.) Ist $y \in \mathrm{im}(f)$, so gilt für seine Faser $f^{-1}(y)$:

$$f^{-1}(y) = \Big[\big\{\text{Lösung des LGS: } [f]_{C,B}\cdot z = [y]_C\big\}\Big]_B^{-1}.$$

Insbesondere gilt dann für $\ker(f)$, d.h. die Faser $f^{-1}(0)$:

$$\ker(f) = \Big[\big\{\text{Lösung des homogenen LGS: } [f]_{C,B}\cdot z = 0\big\}\Big]_B^{-1}.$$

Ist dabei $x_1,\dots,x_k$ eine Basis des Lösungsraumes des LGS $[f]_{C,B}\cdot z = 0$, so ist $[x_1]_B^{-1},\dots,[x_k]_B^{-1}$ eine Basis von $\ker(f)$.

iii.) Es gilt $\operatorname{rg}(f) = \operatorname{rg}\big([f]_{C,B}\big)$*, das Bild von* f *hat die Form:*

$$\operatorname{im}(f) = \Big[\langle\, \textit{Spalten von } [f]_{C,B}\,\rangle\Big]_C^{-1},$$

und für eine Basis $y_1, \ldots, y_s$ *des Erzeugnisses der Spalten von* $[f]_{C,B}$ *ist das System von* $[y_1]_C^{-1}, \ldots, [y_s]_C^{-1}$ *eine Basis von* $\operatorname{im}(f)$*.*

Beweis.

i.) Es gilt $[\,\cdot\,]_{C,B} = [\,\cdot\,] \circ \Phi_{C,B}$ und $\Phi_{C,B} = [\,\cdot\,]_C \circ f \circ [\,\cdot\,]_B^{-1}$, wobei die Koordinatenabbildungen $[\,\cdot\,]_B$ und $[\,\cdot\,]_C$ R-Isomorphismen sind. Damit gilt offensichtlich:

$$\begin{aligned} f \text{ injektiv} \quad &\Longleftrightarrow \quad \Phi_{C,B}(f) \text{ injektiv}, \\ f \text{ surjektiv} \quad &\Longleftrightarrow \quad \Phi_{C,B}(f) \text{ surjektiv}, \\ f \text{ bijektiv} \quad &\Longleftrightarrow \quad \Phi_{C,B}(f) \text{ bijektiv}, \end{aligned}$$

da die Komposition von injektiven/surjektiven/bijektiven Abbildungen wieder injektiv/surjektiv/bijektiv ist (Lemma 0.4.11) und die beiden Koordinatenabbildungen alle drei Bedingungen erfüllen.
Nach Satz 3.1.14 und Lemma 3.1.17 gilt dann für die Spaltenraum-Abbildung $\Phi_{C,B}(f)$:

$$\begin{aligned} \Phi_{C,B}(f) \text{ injektiv} \quad &\Longleftrightarrow \quad \text{Spalten von } [f]_{C,B} \text{ linear unabhängig}, \\ \Phi_{C,B}(f) \text{ surjektiv} \quad &\Longleftrightarrow \quad \text{Spalten von } [f]_{C,B} \text{ erzeugen den } R^{[n]}, \\ \Phi_{C,B}(f) \text{ bijektiv} \quad &\Longleftrightarrow \quad \text{Spalten von } [f]_{C,B} \text{ sind Basis des } R^{[n]}. \end{aligned}$$

Dies liefert zusammen mit obiger Tabelle die gewünschte Aussage.

ii.) Zur Berechnung der Faser $f^{-1}(y)$ sei folgendes kommutative Diagramm betrachtet:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "{[\,\cdot\,]_B}"'] & N \arrow[d, "{[\,\cdot\,]_C}"] \\ R^{[m]} \arrow[r, "\widetilde{f} := \Phi_{C,B}(f)"'] & R^{[n]} \end{tikzcd}$$

Es reicht nun zu zeigen, daß gilt:

$$f^{-1}(y) = \Big[\widetilde{f}^{-1}\big([y]_C\big)\Big]_B^{-1},$$

denn die Faser von $\widetilde{f}^{-1}\big([y]_C\big)$ ist genau die Lösungsmenge des linearen Gleichungssystems $[f]_{C,B} \cdot z = [y]_C$. Dies liefern dann die folgenden Äquivalenzen:

$$\begin{aligned} x \in f^{-1}(y) \quad &\overset{\text{Def Faser}}{\Longleftrightarrow} \quad f(x) = y \\ &\overset{[\,\cdot\,]_C \text{ Iso}}{\Longleftrightarrow} \quad \big[f(x)\big]_C = [y]_C \\ &\overset{[\,\cdot\,]_C \circ f = \widetilde{f} \circ [\,\cdot\,]_B}{\Longleftrightarrow} \quad \widetilde{f}\big([x]_B\big) = [y]_C \\ &\overset{\text{Def Faser}}{\Longleftrightarrow} \quad [x]_B \in \widetilde{f}^{-1}\big([y]_C\big) \\ &\overset{[\,\cdot\,]_B \text{ Iso}}{\Longleftrightarrow} \quad x \in \Big[\widetilde{f}^{-1}\big([y]_C\big)\Big]_B^{-1}. \end{aligned}$$

Der Isomorphismus $[\,\cdot\,]_B^{-1}$ bildet also die Fasern $f^{-1}(y)$ und $\widetilde{f}^{-1}\big([y]_C\big)$ aufeinander ab, und damit auch die Kerne der beiden Abbildungen, da natürlich $[0]_C = 0$ gilt. Isomorphismen bilden aber auch Basen auf Basen ab, so daß für eine Basis $x_1, \ldots, x_k$ von $\ker(\widetilde{f})$ dann $[x_1]_B^{-1}, \ldots, [x_k]_B^{-1}$ eine Basis ist von $\ker(f) = \big[\ker(\widetilde{f})\big]_B^{-1}$.

iii.) Für die Bilder von f und $\widetilde{f}$ gilt:

$$\begin{aligned} y \in \operatorname{im}(f) \quad &\overset{\text{Def im}(f)}{\Longleftrightarrow} \quad \exists x \in M : f(x) = y \\ &\overset{[\,\cdot\,]_C \text{ Iso}}{\Longleftrightarrow} \quad \exists x \in M : \big[f(x)\big]_C = [y]_C \\ &\overset{[\,\cdot\,]_C \circ f = \widetilde{f} \circ [\,\cdot\,]_B}{\Longleftrightarrow} \quad \exists x \in M : \widetilde{f}\big([x]_B\big) = [y]_C \\ &\overset{[\,\cdot\,]_B \text{ Iso}}{\Longleftrightarrow} \quad \exists z \in R^{[m]} : \widetilde{f}(z) = [y]_C \\ &\overset{\text{Def im}(\widetilde{f}}{\Longleftrightarrow} \quad [y]_C \in \operatorname{im}(\widetilde{f}). \end{aligned}$$

Die Anwendung des Isomorphismus $[\,\cdot\,]_C^{-1}$ auf diese Aussage liefert dann sofort:

$$\operatorname{im}(f) = \big[\operatorname{im}(\widetilde{f})\big]_C^{-1}.$$

Das Bild von $\widetilde{f}$ ist das Erzeugnis der Spalten von $[f]_{C,B}$, so daß alle Aussagen sofort folgen. □

Beispiel 3.4.19.

i.) Es sei folgende Basis des $\mathbb{R}^3$ gegeben:

$$B := (b_1, b_2, b_3) := \big(\,(1,2,3),\ (4,5,6),\ (7,2,0)\big).$$

Weiter sei $\varphi \in \operatorname{End}_{\mathbb{R}}(\mathbb{R}^3)$ die lineare Fortsetzung folgender Zuordnung:

$$\varphi\colon \quad (1,2,3) \mapsto (1,1,1), \quad (4,5,6) \mapsto (0,0,0), \quad (7,8,0) \mapsto (1,1,1).$$

Mit der Standard-Zeilen-Basis $\mathcal{E}_3$ des $\mathbb{R}^3$ hat die Matrizendarstellung $[\varphi]_{\mathcal{E}_3,B}$ nach Lemma 3.4.14 und Bemerkung 3.4.7 die Form:

$$[\varphi]_{\mathcal{E}_n,B} \overset{(3.4.14)}{=} \begin{pmatrix} | & | & | \\ \big[\varphi(b_1)\big]_{\mathcal{E}_3} & \big[\varphi(b_2)\big]_{\mathcal{E}_3} & \big[\varphi(b_3)\big]_{\mathcal{E}_3} \\ | & | & | \end{pmatrix} \overset{(3.4.7)}{=} \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Die spezielle Zeilen-Stufen-Form von $[\varphi]_{\mathcal{E}_3,B}$ *ist nach zwei Zeilen-Operationen erreicht und hat die Form:*

$$[\varphi]_{\mathcal{E}_3,B} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Daraus lassen sich sofort Basen des Kerns und des Bildes der von $[\varphi]_{\mathcal{E}_3,B}$ *induzierten linearen Abbildung, nämlich* $\Phi_{\mathcal{E}_3,B}(\varphi)$*, ablesen (nach Satz 3.2.25 und Satz 3.2.28):*

$$\textit{Basis des Kerns:} \quad v_1 := \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}, \quad v_2 := \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix},$$

$$\textit{Basis des Bildes:} \quad w := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Mit Satz 3.4.18 ergibt sich dann für die Abbildung φ*:*

$$\textit{Basis von } \ker(\varphi)\textit{:} \quad [v_1]_B^{-1} = -b_2 = \begin{pmatrix} -4 \\ -5 \\ -6 \end{pmatrix}, \quad [v_2]_B^{-1} = b_1 - b_3 = \begin{pmatrix} -6 \\ 0 \\ 3 \end{pmatrix},$$

$$\textit{Basis von } \operatorname{im}(\varphi)\textit{:} \quad [w]_{\mathcal{E}_3}^{-1} = w = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

ii.) Es sei wie in Beispiel 3.4.16 der Polynomvektorraum $\mathbb{R}[t]_{|3}$ *gegeben mit der Basis* $B := (1, t, t^2, t^3)$ *und die die lineare Abbildung „Ableitung“ auf diesem Raum:*

$$D\colon \mathbb{R}[t]_{|3} \longrightarrow \mathbb{R}[t]_{|3} \quad \textit{mit} \quad a_3t^3 + a_2t^2 + a_1t + a_0 \mapsto 3a_3t^2 + 2a_2t + a_1.$$

Die Matrizendarstellung von D *bzgl. der Basis* B *ist dann:*

$$[D]_{B,B} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Die Matrix $[D]_{B,B}$ *hat fast spezielle Zeilen-Stufen-Form (alle Nicht-Null-Einträge müssen noch auf Eins normiert werden), und schon aus* $[D]_{B,B}$ *können alle relevanten Daten über die von ihr induzierte lineare Abbildung* $\Phi_{B,B}(D)$ *abgelesen werden:*

$$\textit{Basis des Kerns:} \quad v := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$\textit{Basis des Bildes:} \quad w_1 := \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad w_2 := \begin{pmatrix}0\\2\\0\\0\end{pmatrix}, \quad w_3 := \begin{pmatrix}0\\0\\3\\0\end{pmatrix}.$$

Im $\mathbb{R}$-Vektorraum $\mathbb{R}[t]_{|3}$ können die Vektoren w_1, w_2, w_3 auf die Standard-Basisvektoren e_1, e_2, e_3 normiert werden, die dann auch eine Basis des Bildes sind, so daß sich sofort ergibt:

$$\begin{aligned} \textit{Basis von } \ker(D)\textit{:} &\quad [v]_B^{-1} = 1, \\ \textit{Basis von } \operatorname{im}(D)\textit{:} &\quad [e_1]_B^{-1}, [e_2]_B^{-1}, [e_3]_B^{-1} = 1, t, t^2. \end{aligned}$$

Damit ergeben sich für die Ableitung D bzgl. der Polynome bis zum Grad Drei die (schon bekannten) Ergebnisse:

Die konstanten Polynome liegen im Kern der Ableitung,

Die Polynome bis zum Grad Zwei liegen im Bild der Ableitung. □

Der letzte Teil des Satzes 3.4.17 hat einen interessanten Spezialfall. Ist M ein freier R-Modul mit einer Basis $B := (b_1, \ldots, b_m)$, so ist $\operatorname{Hom}_R(M, R)$ ein freier R-Modul mit einer Basis:

$$\varphi_{1,1}, \ldots, \varphi_{1,m} \quad \text{mit} \quad \varphi_{1,j}(b_k) = \delta_{k,j} \cdot 1_R = \delta_{k,j},$$

wobei als Basis C von R hier die Eins von R gewählt wurde (siehe Satz 3.4.17). Wird dabei eine einfachere Indizierung gewählt, kann die Basis auch geschrieben werden als:

$$\varphi_1, \ldots, \varphi_m \quad \text{mit} \quad \varphi_j(b_k) = \delta_{k,j} = \delta_{j,k}. \tag{3.4.20}$$

Die Basis $(\varphi_j)_{1 \le j \le m}$ des Moduls $\operatorname{Hom}_R(M)$ ist unmittelbar aus der Basis B von M konstruiert. Dies gibt Anlaß zur folgenden Definition:

Definition 3.4.21. *Sei R ein kommutativer Ring mit Eins und M ein R-Modul. Dann heißt der Modul $\operatorname{Hom}_R(M, R)$ der Dualraum von M und wird notiert mit:*

$$M^* := \operatorname{Hom}_R(M, R).$$

Ist M ein freier Modul mit einer Basis $B := (b_1, \ldots, b_n)$, dann heißt die daraus konstruierte Basis von M^* (siehe Satz 3.4.17 und insbesondere die Konstruktion 3.4.20) die duale Basis zu B und wird bezeichnet mit:

$$B^* := (b_1^*, \ldots, b_m^*) \quad \textit{mit} \quad b_j^*(b_k) = \delta_{k,j}.$$ □

Bemerkung 3.4.22.

i.) Ist R ein kommutativer Ring mit Eins und M ein freier R-Modul mit einer endlichen Basis B, so liefert Satz 3.4.17 sofort, daß sein Dualraum M^* ein freier R-Modul ist mit einer Dual-Basis B^* der gleichen Mächtigkeit. Dies wiederum liefert die Existenz eines R-Modulisomorphismus von M nach M^*:

$$M \xrightarrow{\sim} M^* \quad \textit{mit} \quad b_i \mapsto b_i^* \textit{ für alle } b_i \in B.$$

ii.) Nicht jeder freie Modul ist isomorph zu seinem Dualraum: Es gilt zum Beispiel der Satz:

Satz: *Sei K ein Körper und V ein K-Vektorraum mit einer Basis $(v_i)_I$, d.h. es gilt $V \cong \bigoplus_I K$ (siehe Satz 2.2.61). Dann ist der Dualrraum V^* isomorph zum K-Vektorraum $\prod_I K$:*

$$V \cong \bigoplus_I K \quad \Longrightarrow \quad V^* \cong \prod_I K.$$

Beweis: *Zum Beispiel in* [**BrLAI**, Satz 6.67, Seite 315].

Zum Beispiel für den Polynomvektorraum $\mathbb{R}[t]$ und den Ring der formalen Potenzeireihen $\mathbb{R}[[t]]$ gelten die Isomorphien:

$$\mathbb{R}[t] \cong \bigoplus_{\mathbb{N}_0} \mathbb{R} \quad \textit{und} \quad \mathbb{R}[[t]] \cong \prod_{\mathbb{N}_0} \mathbb{R},$$

so daß die formalen Potenzreihen (bis auf Isomorphie) den Dualraum des Polyomvektorraumes bilden, und deren Dimensionen sind verschieden, denn es gilt:

$$\dim_{\mathbb{R}}\big(\mathbb{R}[t]\big) \textit{ ist abzählbar unendlich} \quad \textit{und} \quad \dim_{\mathbb{R}}\big(\mathbb{R}[[t]]\big) \textit{ überabzählbar unendlich.}$$

iii.) *Für $n \in \mathbb{N}$ und einen kommutativen Ring mit Eins R gilt:*

$$\big(\mathbb{R}^{[n]}\big)^* \cong \mathrm{Mat}(1 \times n, R) \stackrel{!}{=} R^n,$$

denn die $(1 \times n)$-Matrizen und Zeilenvektoren der Länge n können kanonisch identifiziert werden. □

Beispiel 3.4.23.

i.) *Sei M ein R-Modul mit einer Basis $B = (b_1, b_2, b_3)$. Dann enthält die zu B duale Basis B^* des $M^* = \mathrm{Hom}_R(M, R)$ die drei Abbildungen b_1^*, b_2^*, und b_3^*, die lineare Fortsetzungen der folgenden Basiszuordnungen sind:*

$$b_1^*\colon \begin{array}{l} b_1 \mapsto 1 \\ b_2 \mapsto 0 \\ b_3 \mapsto 0 \end{array}, \qquad b_2^*\colon \begin{array}{l} b_1 \mapsto 0 \\ b_2 \mapsto 1 \\ b_3 \mapsto 0 \end{array}, \qquad b_3^*\colon \begin{array}{l} b_1 \mapsto 0 \\ b_2 \mapsto 0 \\ b_3 \mapsto 1 \end{array}.$$

ii.) *Es sei der $\mathbb{R}$-Vektorraum $\mathcal{C}^0(\mathbb{R})$ der stetigen Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ betrachtet. Weiter sei $[a, b] \subseteq \mathbb{R}$ ein Intervall, und es sei die folgende Funktion definiert:*

$$I_{a,b}\colon \mathcal{C}^0(\mathbb{R}) \longrightarrow \mathbb{R} \quad \textit{mit} \quad f \mapsto \int_a^b f(x)\,dx.$$

$I_{a,b}$ ist eine lineare Abbildung (siehe z.B. auch Beispiel 2.1.18) und damit ein Element aus $\mathrm{Hom}_{\mathbb{R}}\big(\mathcal{C}^0(\mathbb{R}), \mathbb{R}\big)$, dem Dualraum von $\mathcal{C}^0(\mathbb{R})$, d.h. es gilt:

$$I_{a,b} \in \Big(\mathcal{C}^0(\mathbb{R})\Big)^*.$$

Damit liefert jedes Intervall $[a, b] \subseteq \mathbb{R}$ über obige Definition ein Element $I_{a,b}$ des Dualraumes von $\mathcal{C}^0(\mathbb{R})$.

iii.) *Es sei wieder der $\mathbb{R}$-Vektorraum $\mathcal{C}^0(\mathbb{R})$ betrachtet, und für $x_0 \in \mathbb{R}$ sei die folgende Auswertungs-Funktion definiert:*

$$p_{x_0}\colon \mathcal{C}^0(\mathbb{R}) \longrightarrow \mathbb{R} \quad \textit{mit} \quad f \mapsto f(x_0).$$

Die Abbildung p_{x_0} ist linear wegen:

$$p_{x_0}(f+g) \stackrel{(Def\ p_{x_0})}{=} (f+g)(x_0) \stackrel{(Def\ f+g)}{=} f(x_0) + g(x_0) \stackrel{(Def\ p_{x_0})}{=} p_{x_0}(f) + p_{x_0}(g)$$

und:

$$p_{x_0}(\lambda f) \overset{(Def\, p_{x_0})}{=} (\lambda f)(x_0) \overset{(Def\, \lambda f)}{=} \lambda\big(f(x_0)\big) \overset{(Def\, p_{x_0})}{=} \lambda p_{x_0}(f).$$

Damit liefert jeder Punkt $x_0 \in \mathbb{R}$ mit obiger Definition ein Element p_{x_0} aus dem Dualraum von $\mathcal{C}^0(\mathbb{R})$. □

Im allgemeinen ist es bei einer gegebenen Basis in einem freien Modul nicht klar, wie ein Vektor als Linearkombination davon geschrieben werden kann. Ist jedoch eine endliche Basis B im Modul M bekannt, kann leicht jedes $\varphi \in M^*$ als Linearkombination der dualen Basis B^* zu B von M^* ausgedrückt werden:

Lemma 3.4.24. *Sei R ein kommutativer Ring mit Eins und M ein freier R-Modul mit einer Basis $B := (b_1, \ldots, b_m)$. Weiter sei $B^* := (b_1^*, \ldots, b_m^*)$ die duale Basis zu B von M^*. Dann hat ein $\varphi \in M^*$ bzgl. der Basis B^* folgende Linearkombinationsdarstellung:*

$$\varphi = \sum_{i=1}^{m} \varphi(b_i) \cdot b_i^*.$$

Beweis.
Da zwei Abbildungen aus $M^* = \mathrm{Hom}_R(M, R)$ genau dann gleich sind, wenn sie auf der Basis B von M übereinstimmen, braucht die behauptete Identität nur auf den b_k nachgeprüft zu werden:

$$\Big(\sum_{i=1}^{m} \varphi(b_i) \cdot b_i^*\Big)(b_k) = \sum_{i=1}^{m} \varphi(b_i) \cdot \underbrace{b_i^*(b_k)}_{=\delta_{i,k}} = \varphi(b_k). \qquad \square$$

Sind zwei R-Moduln M und N gegeben, so induziert eine lineare Abbildung

$$f\colon M \longrightarrow N$$

immer eine linenare Abbildung zwieschen den Dualräumen, denn für jedes $\varphi \in N^*$ ist die Abbildung $\varphi \circ f$ eine Abbildung aus M^*, wie folgendes Diagramm zeigt:

$$\begin{tikzcd}
M \arrow[r, "f \in \mathrm{Hom}_R(M,N)"] \arrow[dr, "\varphi \circ f \in M^*"'] & N \arrow[d, "\varphi \in N^*"] \arrow[dl, dashed, bend right] \\
& R
\end{tikzcd}$$

Lemma 3.4.25. *Sei R ein kommutativer Ring mit Eins, und seien M, N jeweils R-Moduln. Dann ist für $f \in \mathrm{Hom}_R(M, N)$ die folgende Abbildung eine R-linear Abbildung:*

$$f^*\colon N^* \longrightarrow M^* \quad \textit{mit} \quad \varphi \mapsto \varphi \circ f.$$

Diese Abbildung f^* wird auch die duale Abbildung von f genannt.

Beweis.
$f^*(\varphi+\psi) = f^*(\varphi) + f^*(\psi)$: Lemma 3.4.1.
$f^*(\lambda\varphi) = \lambda f^*(\varphi)$: Diese Gleichung kann für alle $m \in M$ verifiziert werden:

$$\begin{aligned} f^*(\lambda\varphi)(n) &= \big((\lambda\varphi)\circ f\big)(m) = (\lambda\varphi)\big(f(m)\big) = \lambda\Big(\varphi\big(f(m)\big)\Big) \\ &= \lambda\big((\varphi\circ f)(m)\big) = \lambda\big(f^*(\varphi)(m)\big) = \big(\lambda f^*(\varphi)\big)(m). \end{aligned}$$ □

Bemerkung 3.4.26. *Das Konzept der Dualräume wird in diesem Skript nicht weiter vertieft. Es folgen einige Aussagen über die duale Abbildung, deren Beweis jeweils eine nützliche (kleine) Übung ist:*

i.) Für zwei R-lineare Abbilungen $f, g\colon M \longrightarrow N$ gilt:

$$(f+g)^* = f^* + g^* \quad \textit{und} \quad (\lambda f)^* = \lambda(f^*).$$

Damit ist die folgende Zuordnung eine R-lineare Abbildung:

$$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(N^*, M^*) \quad \textit{mit} \quad f \mapsto f^*.$$

ii.) Für lineare Abbildungen $f \in \mathrm{Hom}_R(M,N)$ und $g \in \mathrm{Hom}_R(N,U)$ gilt:

$$(g\circ f)^* = f^* \circ g^*.$$

iii.) Ist K ein Körper und $f\colon V \longrightarrow W$ ein Vektorraumhomomorphismus, so gilt:

$$\begin{aligned} f \textit{ injektiv} \quad &\Longrightarrow \quad f^* \textit{ surjektiv}, \\ f \textit{ surjektiv} \quad &\Longrightarrow \quad f^* \textit{ injektiv}. \end{aligned}$$ □

Basiswechsel.

Für eine lineare Abbildung zwischen freien R-Moduln

$$f\colon M \longrightarrow N$$

mit endlichen Basen jeweils gleicher Größe $B, \widetilde{B}$ von M und $C, \widetilde{C}$ von N können verschiedene Matrizendarstellungen

$$[f]_{C,B} \quad \text{und} \quad [f]_{\widetilde{C},\widetilde{B}}$$

betrachtet werden, die in Abhängigkeit von den gewählten Basen natürliche völlig verschiedene Einträge haben.

Beispiel 3.4.27. *Der folgende Endomorphismus des $\mathbb{R}^2$:*

$$f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad (x,y) \mapsto (x+2y,\ -x+4y)$$

hat bzgl. der Basen:

$$\mathcal{B} := \big((2,1),\ (1,1)\big), \quad \mathcal{C} := \big((4,2),\ (3,3)\big) \quad \textit{und} \quad \mathcal{E}_2$$

die folgenden Matrizendarstellungen (Übung!):

$$[f]_{\mathcal{E}_2,\mathcal{E}_2} = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}, \quad [f]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \quad \textit{und} \quad [f]_{\mathcal{C},\mathcal{B}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$ □

Die folgende Aussage beschreibt, wie die einzelnen Matrizendarstellungen voneinander abhängen:

Lemma 3.4.28. *Sei R ein kommutativer Ring mit Eins, und seien M, N freie R-Moduln mit endlichen Basen jeweils gleicher Größe $\mathcal{B}, \widetilde{\mathcal{B}}$ von M und $\mathcal{C}, \widetilde{\mathcal{C}}$ von N. Dann gilt für die Matrizendarstellungen von $f \in \mathrm{Hom}_R(M, N)$ bzgl. dieser Basen:*

$$[f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}} = [\mathrm{id}_N]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot [\mathrm{id}_M]_{\mathcal{B},\widetilde{\mathcal{B}}}.$$

Für die Koordinatenvektoren von Vektoren $x \in M$ und $y \in N$ bzgl. dieser Basen gilt:

$$[x]_{\widetilde{\mathcal{B}}} = [\mathrm{id}_M]_{\widetilde{\mathcal{B}},\mathcal{B}} \cdot [x]_{\mathcal{B}} \quad \textit{und} \quad [y]_{\widetilde{\mathcal{C}}} = [\mathrm{id}_N]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [y]_{\mathcal{C}}.$$

Beweis.
Nach Satz 3.4.17 gilt:

$$\begin{aligned}[\mathrm{id}_N]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot [\mathrm{id}_M]_{\mathcal{B},\widetilde{\mathcal{B}}} &\overset{(3.4.17)}{=} [\mathrm{id}_N \circ f]_{\widetilde{\mathcal{C}},\mathcal{B}} \cdot [\mathrm{id}_M]_{\mathcal{B},\widetilde{\mathcal{B}}} = [f]_{\widetilde{\mathcal{C}},\mathcal{B}} \cdot [\mathrm{id}_M]_{\mathcal{B},\widetilde{\mathcal{B}}} \\ &\overset{(3.4.17)}{=} [f \circ \mathrm{id}_M]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}} = [f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}.\end{aligned}$$

Analog folgt aus Satz 3.4.17 für die Koordinatenvektoren bei Basiswechsel:

$$\begin{aligned}[\mathrm{id}_M]_{\widetilde{\mathcal{B}},\mathcal{B}} \cdot [x]_{\mathcal{B}} &\overset{(3.4.17)}{=} [\mathrm{id}_M(x)]_{\widetilde{\mathcal{B}}} = [x]_{\widetilde{\mathcal{B}}}, \\ [\mathrm{id}_N]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [y]_{\mathcal{C}} &\overset{(3.4.17)}{=} [\mathrm{id}_N(y)]_{\widetilde{\mathcal{C}}} = [y]_{\widetilde{\mathcal{C}}}.\end{aligned}$$

□

Bemerkung 3.4.29.

i.) Die Bedingung in Lemma 3.4.28, daß die Basen $\mathcal{B}, \widetilde{\mathcal{B}}$ und die Basen $\mathcal{C}, \widetilde{\mathcal{C}}$ jeweils gleiche Länge haben sollen, ist eigentlich überflüssig, da in einen freien R-Modul alle Basen die gleiche Länge haben. Dies wurde bisher aber nur für den Fall von Vektorräumen, also freien Moduln über Körpern, bewiesen. Daher die zusätzliche, eigentlich obsolete Einschränkung.

ii.) Die Basiswechselmatrizen $[\mathrm{id}_{Raum}]_{Basis,Basis}$ sind im allgemeinen nicht bekannt. Daher kann noch nicht aus einer Matrizendarstellung von f die bzgl. einer anderen Basis mit der Formel aus Lemma 3.4.28 berechnet werden. Die Formel liefert also nur, daß beide Matrizendarstellungen von f durch Matrizenprodukte mit invertierbaren Matrizen $[\mathrm{id}_M]_{\widetilde{\mathcal{C}},\mathcal{C}}$ und $[\mathrm{id}_N]_{\mathcal{B},\widetilde{\mathcal{B}}}$ zusammenhängen.

iii.) Die Formel aus Lemma 3.4.28 kann mit Hilfe der Rechenformeln aus Satz 3.4.17 sofort aufgestellt werden - sie folgt aber auch aus den schon vorher betrachteten kommutativen Diagrammen für Matrizendarstellungen von linearen Abbildungen: Es sind folgende zwei Diagramme gegeben für die Matrizendarstellungen $[f]_{\mathcal{C},\mathcal{B}}$ und $[f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}$:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "{[\,\cdot\,]_{\mathcal{B}}}"'] & N \arrow[d, "{[\,\cdot\,]_{\mathcal{C}}}"] \\ R^{[m]} \arrow[r, "\Phi_{\mathcal{C},\mathcal{B}}(f)"'] & R^{[n]} \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "f"] \arrow[d, "{[\,\cdot\,]_{\widetilde{\mathcal{B}}}}"'] & N \arrow[d, "{[\,\cdot\,]_{\widetilde{\mathcal{C}}}}"] \\ R^{[m]} \arrow[r, "\Phi_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}(f)"'] & R^{[n]} \end{tikzcd}$$

$$\rightsquigarrow [f]_{\mathcal{C},\mathcal{B}} \qquad\qquad \rightsquigarrow [f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}$$

Die beiden Diagramme können verbunden werden, wenn zwischen M und M die Identitätsabbildung id_M und zwieschen N und N die Identitätsabbildung id_N eingefügt wird, und es ergibt sich folgendes kommutative Diagramm:

$$\begin{tikzcd}
R^{[m]} \arrow[rrr, "\rightsquigarrow [f]_{\mathcal{C},\mathcal{B}}", "\Phi_{\mathcal{C},\mathcal{B}}(f)"'] \arrow[dddd, "\Phi_{\mathcal{B},\widetilde{\mathcal{B}}}(\mathrm{id}_M)", "\rightsquigarrow [\mathrm{id}_M]_{\mathcal{B},\widetilde{\mathcal{B}}}"'] & & & R^{[n]} \arrow[dddd, "\Phi_{\widetilde{\mathcal{C}},\mathcal{C}}(\mathrm{id}_N)", "\rightsquigarrow [\mathrm{id}_N]_{\widetilde{\mathcal{C}},\mathcal{C}}"'] \\
& M \arrow[ul, "{[\,\cdot\,]_{\mathcal{B}}}"] \arrow[r, "f"] & N \arrow[ur, "{[\,\cdot\,]_{\mathcal{C}}}"'] \arrow[d, "\mathrm{id}_N"] & \\
& M \arrow[u, "\mathrm{id}_M"] \arrow[r, "f"] & N \arrow[dr, "{[\,\cdot\,]_{\widetilde{\mathcal{C}}}}"] & \\
R^{[m]} \arrow[ur, "{[\,\cdot\,]_{\widetilde{\mathcal{B}}}}"'] \arrow[rrr, "\Phi_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}(f)", "\rightsquigarrow [f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}"'] & & & R^{[n]}
\end{tikzcd}$$

Dies liefert dann die behauptete Beziehung zwischen den verschiedenen Matrizendarstellungen von f:

$$\Phi_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}}(f) = \Phi_{\widetilde{\mathcal{C}},\mathcal{C}}(\mathrm{id}_N) \circ \Phi_{\mathcal{C},\mathcal{B}}(f) \circ \Phi_{\mathcal{B},\widetilde{\mathcal{B}}}(\mathrm{id}_M) \implies [f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}} = [\mathrm{id}_N]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot [\mathrm{id}_M]_{\mathcal{B},\widetilde{\mathcal{B}}}. \quad \square$$

Beispiel 3.4.30. *Der Endomorphismus des $\mathbb{R}^2$ aus Beispiel 3.4.27:*

$$f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad (x,y) \mapsto (x+2y,\ -x+4y)$$

hat bzgl. der Basen:

$$\mathcal{B} := \big((2,1),\ (1,1)\big), \quad \mathcal{C} := \big((4,2),\ (3,3)\big) \quad \textit{und} \quad \mathcal{E}_2$$

die folgenden Matrizendarstellungen:

$$[f]_{\mathcal{E}_2,\mathcal{E}_2} = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}, \quad [f]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \quad \textit{und} \quad [f]_{\mathcal{C},\mathcal{B}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Mit Lemma 3.4.28 folgen dann unter anderem folgende Beziehungen:

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = [f]_{\mathcal{B},\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{B},\mathcal{E}_2} \cdot [f]_{\mathcal{E}_2,\mathcal{E}_2} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{B},\mathcal{E}_2} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [f]_{\mathcal{C},\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{C},\mathcal{E}_2} \cdot [f]_{\mathcal{E}_2,\mathcal{E}_2} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{C},\mathcal{E}_2} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}}.$$

$\square$

In dem vorherigen Beispiel sind alle Abbdildungen schon zwischen Spalten- bzw. Zeilen-Räumen definiert, vor allem die Identitätsabbildungen, und in diesem Fall ist es möglich, eine Matrizendarstellung der Identitätsabbildung zu berechnen. Dazu sei das folgende Lemma betrachtet:

Lemma 3.4.31. *Sei R ein kommutativer Ring mit Eins und $\mathcal{B} := (b_1, \ldots, b_m)$ und $\mathcal{C} := (c_1, \ldots, c_n)$ Basen des Spaltenraumes $R^{[m]}$. Weiter seien B und C diejenigen Matrizen aus $\mathrm{GL}_m(R)$, deren Spalten genau die Vektoren der Basen $\mathcal{B}$ und $\mathcal{C}$ sind:*

$$B := \begin{pmatrix} | & & | \\ b_1 & \cdots & b_m \\ | & & | \end{pmatrix} \quad \textit{und} \quad C := \begin{pmatrix} | & & | \\ c_1 & \cdots & c_m \\ | & & | \end{pmatrix}$$

Dann hat die Identitätsabbildung id *des $R^{[m]}$ folgende Matrizendarstellungen:*

$$[\mathrm{id}]_{\mathcal{E}_m,\mathcal{B}} = B, \quad [\mathrm{id}]_{\mathcal{E}_m,\mathcal{C}} = C \quad \textit{und} \quad [\mathrm{id}]_{\mathcal{C},\mathcal{E}_m} = C^{-1},$$

woraus dann folgt:

$$[\mathrm{id}]_{\mathcal{C},\mathcal{B}} = [\mathrm{id}]_{\mathcal{C},\mathcal{E}_m} \cdot [\mathrm{id}]_{\mathcal{E}_m,\mathcal{B}} = C^{-1}B.$$

Für einen Vektor $x \in R^{[m]}$ gilt damit:

$$[x]_{\mathcal{C}} = [\mathrm{id}]_{\mathcal{C},\mathcal{B}} \cdot [x]_{\mathcal{B}} = (C^{-1}B) \cdot [x]_{\mathcal{B}}.$$

Beweis.
Nach Bemerkung 3.4.15 gelten die Gleichungen:

$$[\mathrm{id}]_{\mathcal{E}_m,\mathcal{B}} = B \quad \text{und} \quad [\mathrm{id}]_{\mathcal{E}_m,\mathcal{C}} = C,$$

woraus dann mit Satz 3.4.17 folgt:

$$[\mathrm{id}]_{\mathcal{C},\mathcal{E}_m} = [\mathrm{id}^{-1}]_{\mathcal{C},\mathcal{E}_m} \overset{(3.4.17)}{=} \left([\mathrm{id}]_{\mathcal{E}_m,\mathcal{C}}\right)^{-1} = C^{-1}.$$

Satz 3.4.17 liefert dann sofort:

$$[\mathrm{id}]_{\mathcal{C},\mathcal{E}_m} \cdot [\mathrm{id}]_{\mathcal{E}_m,\mathcal{B}} \overset{(3.4.17)}{=} [\mathrm{id} \circ \mathrm{id}]_{\mathcal{C},\mathcal{B}} = [\mathrm{id}]_{\mathcal{C},\mathcal{B}} \quad \Longrightarrow \quad [\mathrm{id}]_{\mathcal{C},\mathcal{B}} = C^{-1}B.$$

Mit Lemma 3.4.28 gilt dann letztendlich auch:

$$[x]_{\mathcal{C}} \overset{(3.4.28)}{=} [\mathrm{id}]_{\mathcal{C},\mathcal{B}} \cdot [x]_{\mathcal{B}} = (C^{-1}B) \cdot [x]_{\mathcal{B}}. \qquad \square$$

Bemerkung 3.4.32. *Die Aussage läßt sich leicht auf den Falle von Zeilenräumen übertragen: Ist $\mathcal{B} := (b_1, \ldots, b_m)$ eine des R^m, so werden in die Matrix $[\mathrm{id}_{R^m}]_{\mathcal{E}_m,\mathcal{B}}$ die Zeilenvektoren $b_1, \ldots, b_m$ spaltenweise eingetragen. Zum Beispiel hat dann bzgl. der Basen:*

$$\mathcal{B} := \big((1,3,4),\ (0,1,7),\ (8,2,1)\big) \quad \textit{und} \quad \mathcal{E}_3$$

des $\mathbb{R}^3$ die Identitätsabbildung $[\mathrm{id}_{\mathbb{R}^3}]$ folgende Matrizendarstellung:

$$[\mathrm{id}_{\mathbb{R}^3}]_{\mathcal{E}_3,\mathcal{B}} = \begin{pmatrix} 1 & 0 & 8 \\ 3 & 1 & 2 \\ 4 & 7 & 1 \end{pmatrix}. \qquad \square$$

Mit Lemma 3.4.33 kann die allgemeine Formulierung aus Lemma 3.4.28 dann für den speziellen Fall der Spaltenräume präzisiert werden:

LEMMA 3.4.33. *Sei R ein kommutativer Ring mit Eins und $f \in \mathrm{Hom}_R(R^{[m]}, R^{[n]})$. Es seien $\mathcal{B}, \widetilde{\mathcal{B}}$ Basen des $R^{[m]}$ und $\mathcal{C}, \widetilde{\mathcal{C}}$ Basen des $R^{[n]}$ jeweils gleicher Länge, und $B, \widetilde{B}$ und $C, \widetilde{C}$ die jeweiligen Matrizen aus $\mathrm{GL}_m(R)$ und $\mathrm{GL}_n(R)$, die spaltenweise aus den Basen zusammengesetzt sind (siehe auch Lemma 3.4.31). Dann gilt für die Matrizendarstellung von f bzgl. dieser Basen:*

$$[f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}} = [\mathrm{id}]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot [\mathrm{id}]_{\mathcal{B},\widetilde{\mathcal{B}}} = (\widetilde{C}^{-1}C) \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot (B^{-1}\widetilde{B}).$$

BEWEIS.
Lemma 3.4.28 liefert die Gleichung:

$$[f]_{\widetilde{\mathcal{C}},\widetilde{\mathcal{B}}} = [\mathrm{id}]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot [\mathrm{id}]_{\mathcal{B},\widetilde{\mathcal{B}}},$$

und Lemma 3.4.31 die Gleichung:

$$[\mathrm{id}]_{\widetilde{\mathcal{C}},\mathcal{C}} \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot [\mathrm{id}]_{\mathcal{B},\widetilde{\mathcal{B}}} = (\widetilde{C}^{-1}C) \cdot [f]_{\mathcal{C},\mathcal{B}} \cdot (B^{-1}\widetilde{B}). \qquad \square$$

BEMERKUNG 3.4.34. *Bezüglich der Forderung, daß die Basen $\mathcal{B}, \widetilde{\mathcal{B}}$ und $\mathcal{C}, \widetilde{\mathcal{C}}$ die gleiche Länge haben sollen, siehe Bemerkung 3.4.29.* $\square$

BEISPIEL 3.4.35. *Es sei wieder der Endomorphismus des $\mathbb{R}^2$ aus Beispiel 3.4.30 betrachtet:*

$$f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \textit{mit} \quad (x,y) \mapsto (x+2y,\ -x+4y)$$

Dazu seien auch wider die gleichen Basen gegeben:

$$\mathcal{B} := \big((2,1),\ (1,1)\big), \quad \mathcal{C} := \big((4,2),\ (3,3)\big).$$

Die in Beispiel 3.4.30 aufgestellten Gleichungen:

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = [f]_{\mathcal{B},\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{B},\mathcal{E}_2} \cdot [f]_{\mathcal{E}_2,\mathcal{E}_2} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{B},\mathcal{E}_2} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [f]_{\mathcal{C},\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{C},\mathcal{E}_2} \cdot [f]_{\mathcal{E}_2,\mathcal{E}_2} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}} = [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{C},\mathcal{E}_2} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \cdot [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}}$$

können mit Lemma 3.4.31 bzw. Lemma 3.4.33 weiter aufgelöst werden. Es ist:

$$B := [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{E}_2,\mathcal{B}} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \textit{und} \quad C^{-1} := [\mathrm{id}_{\mathbb{R}^2}]_{\mathcal{C},\mathcal{E}_2} = \begin{pmatrix} 4 & 3 \\ 2 & 3 \end{pmatrix}^{-1} = \frac{1}{6} \cdot \begin{pmatrix} 3 & -3 \\ -2 & 4 \end{pmatrix},$$

und es folgt:

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{6} \cdot \begin{pmatrix} 3 & -3 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}. \qquad \square$$

Matrizendarstellungen von Endomorphismen.

Die bisher allgemein behandelte Situation (lineare Abbildungen zwischen verschiedenen freien Moduln) soll nun speziell für Endomorphismen eines freien Moduls bzw. Vektorraumes betrachtet werden. Dabei werden von einem Endomorphismen $f \in \mathrm{End}_R(M)$ jeweils nur Matrizendarstellungen der Form $[f]_{\mathcal{B},\mathcal{B}}$ bzgl. *einer* Basis betrachet, nicht allgemeine der Form $[f]_{\mathcal{C},\mathcal{B}}$ bzgl. zweier Basen von M, da da bei der Darstellung bzgl. einer Basis die Ringstruktur auf dem Endomorphismenring respektiert wird, d.h die Verknüpfung von zwei Endomorphismen:

$$[f]_{\mathcal{B},\mathcal{B}} \cdot [g]_{\mathcal{B},\mathcal{B}} = [f \circ g]_{\mathcal{B},\mathcal{B}}$$

(siehe auch Bemerkung 3.4.5). Zuerst werden die allgemeinen Aussagen für den speziellen Fall noch einmal zusammenfassend notiert:

Satz 3.4.36. *Sei R ein kommutativer Ring mit Eins und M ein freier R-Modul mit endlichen Basen $\mathcal{B}, \mathcal{C}$ gleicher Länge. Dann gilt nach Lemma 3.4.28 für die Matrizendarstellungen von $f \in \mathrm{End}_R(M)$ bzgl. dieser Basen:*

$$[f]_{\mathcal{C},\mathcal{C}} = [\mathrm{id}_M]_{\mathcal{C},\mathcal{B}} \cdot [f]_{\mathcal{B},\mathcal{B}} \cdot [\mathrm{id}_M]_{\mathcal{B},\mathcal{C}},$$

und wegen $[\mathrm{id}_M]_{\mathcal{B},\mathcal{C}} = [\mathrm{id}_M]_{\mathcal{C},\mathcal{B}}^{-1}$ folgt insbesondere mit $S := [\mathrm{id}_M]_{\mathcal{C},\mathcal{B}}$:

$$[f]_{\mathcal{C},\mathcal{C}} = S \cdot [f]_{\mathcal{B},\mathcal{B}} \cdot S^{-1}.$$

Für den Spezialfall des Spaltenraumes $R^{[n]}$ seien $\mathcal{B}$, $\mathcal{C}$ Basen des $R^{[n]}$ der Länge n und B, C diejenigen Matrizen aus $\in \mathrm{GL}_n(R)$, die spaltenweise aus den Basen zusammengesetzt sind (siehe auch Lemma 3.4.31). Dann gilt für die Matrizendarstellung von $f \in \mathrm{End}_R(R^{[n]})$ bzgl. dieser Basen mit Lemma 3.4.33 und obiger Formel:

$$[f]_{\mathcal{C},\mathcal{C}} = [\mathrm{id}]_{\mathcal{C},\mathcal{B}} \cdot [f]_{\mathcal{B},\mathcal{B}} \cdot [\mathrm{id}]_{\mathcal{B},\mathcal{C}} = (C^{-1}B) \cdot [f]_{\mathcal{B},\mathcal{B}} \cdot (B^{-1}C).$$

Mit $S := [\mathrm{id}]_{\mathcal{C},\mathcal{B}} = (C^{-1}B) \in \mathrm{GL}_n(R)$ folgt dann analog zur obigen allgemeinen Aussage:

$$[f]_{\mathcal{C},\mathcal{C}} = S \cdot [f]_{\mathcal{B},\mathcal{B}} \cdot S^{-1}.$$ □

Diese spezielle Form des Basiswechsels bei Matrizendarstellungen von Endomorphismen trägt eine eigene Bezeichnung:

Definition 3.4.37. *Sei R ein kommutativer Ring mit Eins. Zwei quadratische Matrizen $B, C \in \mathrm{Mat}_n(R)$ heißen konjugiert, wenn es ein $S \in \mathrm{GL}_n(R)$ gibt mit:*

$$C = SBS^{-1}.$$

Zwei Endomorphismen $\varphi, \psi \in \mathrm{End}_R(M)$ eines R-Moduls M heißen konjugiert, wenn es ein $\xi \in \mathrm{GL}_R(M)$ gibt mit:

$$\varphi = \xi \circ \psi \circ \xi^{-1}.$$ □

Satz 3.4.36 liefert sofort, daß zwei Matrizendarstellungen eines Endomorphismus zu verschiedenen Basen konjugierte Matrizen sind - und auch die Umkehrung davon gilt, wie die folgende Aussage zeigt:

LEMMA 3.4.38. *Sei R ein kommutativer Ring mit Eins, und seien $B, C \in \mathrm{Mat}_n(R)$ zwei quadratische Matrizen. Dann sind folgende beide Aussagen äquivalent:*

i.) B und C sind konjugiert.

ii.) Es gibt ein $f \in \mathrm{End}_R(R^{[n]})$ und Basen $\mathcal{B}$ und $\mathcal{C}$ des $R^{[n]}$, so daß für B und C gilt:

$$B = [f]_{\mathcal{B},\mathcal{B}} \quad \text{und} \quad C = [f]_{\mathcal{C},\mathcal{C}}.$$

BEWEIS.

i.) $\Longrightarrow$ *ii.)*: Seien B und C konjugiert und $S \in \mathrm{GL}_n(R)$ mit $C = SBS^{-1}$. Die Spalten von S sind nach Bemerkung 3.3.38 eine Basis des $R^{[n]}$, und diese sei mit $\mathcal{S}$ bezeichnet. Weiter sei f der von C induzierte Endomorphismus φ_C des $R^{[n]}$. Dann gilt mit Satz 3.1.14 und Bemerkung 3.4.15:

$$[f]_{\mathcal{E}_n,\mathcal{E}_n} \overset{(\mathrm{Def})}{=} [\varphi_C]_{\mathcal{E}_n,\mathcal{E}_n} \overset{(3.4.15)}{=} [\varphi_C] \overset{(3.1.14)}{=} C,$$

so daß C die Matrizendarstellung von f bzgl. der Basis $\mathcal{E}_n$ ist. Mit $S = [\mathrm{id}]_{\mathcal{E}_n,\mathcal{S}}$ folgt dann sofort, daß B die Matrizendarstellung von f bzgl. der Basis $\mathcal{S}$ ist:

$$[f]_{\mathcal{S},\mathcal{S}} = [\mathrm{id}]_{\mathcal{S},\mathcal{E}_n} \cdot [f]_{\mathcal{E}_n,\mathcal{E}_n} \cdot [\mathrm{id}]_{\mathcal{E}_n,\mathcal{S}} = S^{-1}CS = B.$$

Mit $f := \varphi_C$, $\mathcal{B} := \mathcal{S}$ und $\mathcal{C} := \mathcal{E}_n$ ist die Behauptung also bewiesen.

ii.) $\Longrightarrow$ *i.)*: Satz 3.4.36. □

Damit sind konjugierte Matrizen bzgl. ihrer Interpretation als Abbildungsdarstellungen „gleich“, da sie als verschiedene Zahlenschemata zur Darstellung ein und derselben Abbildung aufgefaßt werden können. Deshalb ist es für das Studium von Endomorphismen nur wichtig, die quadratischen Matrizen „bis auf Konjugation“ zu untersuchen.

Dabei ist die Relation „konjugiert sein“ für Matrizen eine Äquivalenzrelation, wie folgendes Lemma zeigt, so daß die Menge $\mathrm{Mat}_n(R)$ in disjunkte Teilmengen (Äquivalenzklassen) jeweils zueinander konjugierter Matrizen zerfällt:

LEMMA 3.4.39. *Sei R ein kommutativer Ring mit Eins. Weiter sei für Matrizen $B, C \in \mathrm{Mat}_n(R)$ definiert:*

$$B \sim C \qquad :\Longleftrightarrow \qquad \exists S \in \mathrm{GL}_n(R) : C = SBS^{-1}.$$

Diese Relation „B und C sind konjugiert“ ist eine Äquivalenzrelation auf $\mathrm{Mat}_n(R)$, und die zugehörigen Äquivalenzklassen werden die Konjugationsklassen genannt.

BEWEIS.

reflexiv: Für $B \in \mathrm{Mat}_n(R)$ gilt: $B = E_n \cdot B \cdot E_n^{-1}$, so daß $B \sim B$ folgt.

symmetrisch: Gilt $B \sim C$, so gibt es ein $S \in \mathrm{GL}_n(R)$ mit $C = SBS^{-1}$, und da mit S auch S^{-1} in $\mathrm{GL}_n(R)$ liegt, gilt:

$$S^{-1}C\big(S^{-1}\big)^{-1} = B \qquad \Longrightarrow \qquad C \sim B.$$

transitiv: Seien $B, C, D \in \mathrm{Mat}_n(R)$ mit $B \sim C$ und $C \sim D$ und $S, T \in \mathrm{GL}_n(R)$, so daß gilt:

$$C = SBS^{-1} \quad \text{und} \quad D = TCT^{-1}.$$

Es folgt dann:

$$D = TCT^{-1} = T(SBS^{-1})T^{-1} = (TS)B(TS)^{-1},$$

und da mit $S, T \in \mathrm{GL}_n(R)$ auch $TS \in \mathrm{GL}_n(R)$ gilt, liefert dies $C \sim D$. $\square$

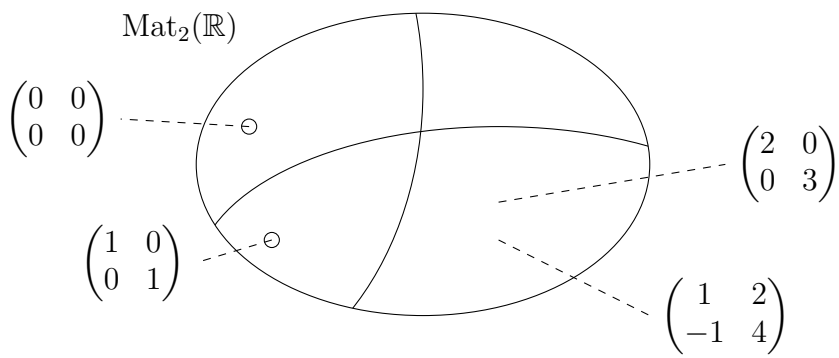
Bemerkung 3.4.40.

i.) Zwei Konjugationsklassen von $\mathrm{Mat}_n(R)$ *sind immer einelementig, denn es gilt für alle* $S \in \mathrm{GL}_n(R)$*:*

$$\textit{Nullmatrix} = S \cdot \textit{Nullmatrix} \cdot S^{-1},$$
$$\textit{Einheitsmatrix} = S \cdot \textit{Einheitsmatrix} \cdot S^{-1}.$$

ii.) Für einen Körper K *ist es möglich, alle Konjugationsklassen von* $\mathrm{Mat}_n(K)$ *zu beschreiben - und dies ist Thema von LA IIb. Bei Ringen ist dies i.a. nicht möglich. Schon beim scheinbar einfachen Ring* $\mathbb{Z}$ *ist eine Beschreibung aller Klassen von* $\mathrm{Mat}_2(\mathbb{Z})$ *nicht einfach, für größere Matrizen über* $\mathbb{Z}$ *existiert noch keine Klassifikation.* $\square$

Beispiel 3.4.41. *i.) Im Falle der* (2×2)*-Matrizen über* $\mathbb{R}$ *liefern Beispiel 3.4.35 und Bemerkung 3.4.40 folgende Skizze:*



Die Konjugations-/Äquivalenzklasse von der Nullmatrix und der Einheitsmatrix sind nach Bemerkung 3.4.40 einelementig, die beiden aufgeführten Matrizen nach Beispiel 3.4.35 in einer Klasse.

ii.) Sei K *ein Körper und* $A \in \mathrm{Mat}_2(K)$*. Dann gilt (Übung!):*

$$A \neq 0, A^2 = 0 \quad \Longleftrightarrow \quad A \sim \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Damit bilden alle Matrizen mit der Eigenschaft $A \neq 0, A^2 = 0$ *in* $\mathrm{Mat}_2(K)$ *eine Konjugationsklasse und die Matrix* $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ *ein Repräsentant dieser Klasse.*

iii.) Für den Ring $\mathbb{Z}$ *gilt vorherige Klassifikationsaussage nicht. Es gilt zwar:*

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

aber die Matrix $\left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right)$ *ist nicht konzugiert zu* $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ *mit einem* $S \in \mathrm{GL}_2(\mathbb{Z})$*. Es gilt dabei folgende Aussage über* $\mathbb{Z}$*(Übung!):*

$$\begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} \sim_{\mathbb{Z}} \begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix} \qquad \Longleftrightarrow \qquad |n| = |m|.$$

Über dem Körper $\mathbb{Q}$ *sind beide Matrizen nach vorheriger Aussage konjugiert, da sie da ja beide zu der Matrix* $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ *mit einem* $S \in \mathrm{GL}_2(\mathbb{Q})$ *konjugiert sind.*

Damit zerfällt die $\mathbb{Q}$-Konjugationsklasse über $\mathbb{Z}$ in viele Klassen, da zur Konjugation über $\mathbb{Z}$ weniger invertierbare Matrizen zum Konjugieren zur Verfügung stehen. $\square$

Die Frage, ob zwei gegebene Matrizen $B, C \in \mathrm{Mat}_n(R)$ konjugiert sind oder nicht, ist nicht leicht zu klären. Der Ansatz, ein $S \in \mathrm{GL}_n(R)$ zu finden, welches $C = SBS^{-1}$ erfüllt, ist kaum praktikabel. Selbst nach der Äquivalenzumformung:

$$C = SBS^{-1} \qquad \Longleftrightarrow \qquad CS = SB$$

wäre ein Gleichungssystem mit n^2 Variablen (den Einträgen von S) zu lösen, was nur für kleine n und spezielle Matrizen B, C wie in Beispiel 3.4.41 Sinn macht.
Der Lösungsweg (zumindest über Körpern) wird sein, gewisse Kenngrößen von Matrizen herauszuarbeiten, die sich bei der Konjugation nicht ändern - sogenannte Konjugationsinvarianten - und im Idealfall mit Hilfe dieser Konjugationsinvarianten dann zu entscheiden, ob die Matrizen konjugiert sind oder nicht.
Eine Reihe von Konjugationsinvarianten liefert die folgende Aussage:

Lemma 3.4.42. *Sei R ein kommutativer Ring mit Eins, und seien $B, C \in \mathrm{Mat}_n(R)$ quadratische Matrizen, die zueinander konjugiert sind, d.h. $C = SBS^{-1}$ mit einem $S \in \mathrm{GL}_n(R)$. Dann gelten folgende Implikation:*

$$B \sim C \qquad \Longrightarrow \qquad \begin{cases} \det(B) = \det(C), \\ \chi_B = \chi_C, \\ \mathrm{sp}(B) = \mathrm{sp}(C). \end{cases}$$

Ist R ein Körper und B nicht die Nullmatrix, so gilt auch:

$$B \sim C \qquad \Longrightarrow \qquad \mathrm{rg}(B) = \mathrm{rg}(C).$$

Beweis.

$\det(B) = \det(C)$: Nach dem Determinantenmultiplikationssatz 3.3.8 foglt sofort:

$$\begin{aligned} C = SBS^{-1} \qquad \Longrightarrow \qquad \det(C) &= \det(SBS^{-1}) \\ &= \det(S) \cdot \det(B) \cdot \det(S^{-1}) \\ &= \det(S) \cdot \det(S^{-1}) \cdot \det(B) \\ &= \det(B), \end{aligned}$$

da im kommutativen Ring $\det(B) \cdot \det(S^{-1}) = \det(S^{-1}) \cdot \det(B)$ gilt (Bemerkung 3.3.9) und natürlich $\det(S) \cdot \det(S^{-1}) = 1$ aus $SS^{-1} = E_n$ folgt.

$\chi_B = \chi_C$: Mit den Matrizenmultiplikationsregeln aus Satz 3.1.8 und der vorherigen Aussage $(*)$ gilt für die charakteristischen Polynome $\chi_B(t), \chi_C(t) \in R[t]$:

$$\begin{aligned} \chi_C(t) &= \det(t \cdot E_n - C) \\ &= \det(t \cdot SE_nS^{-1} - SBS^{-1}) \\ &= \det\left(S(t \cdot E_n - B)S^{-1}\right) \\ &\overset{(*)}{=} \det(t \cdot E_n - B) \\ &= \chi_B(t). \end{aligned}$$

$\mathrm{sp}(B) = \mathrm{sp}(C)$: Bemerkung 3.3.54.

$\operatorname{rg}(B) = \operatorname{rg}(C)$: Nach Satz 3.2.21 ändert sich der Rang einer Matrix nicht, wenn sie mit invertierbaren Matrizen multipliziert wird. Dann gilt sofort:

$$\operatorname{rg}(B) = \operatorname{rg}(SB) = \operatorname{rg}\left((SB)S^{-1}\right) = \operatorname{rg}(C). \qquad \square$$

Bemerkung 3.4.43. *Die in Lemma 3.4.42 aufgeführten Konjugationsinvarianten können nicht allgemein klären, ob zwei gegebene Matrizen konjugiert sind oder nicht!*

- *Ist bei zwei Matrizen mindestens eine der Konjugationsinvarianten verschieden, so können sie nicht konjugiert sein.*
- *Sind alle in Lemma 3.4.42 aufgeführten Konjugationsinvarianten gleich, so müssen die Matrizen trotzdem nicht konjugiert sein!*

Damit kann höchstens entschieden werden, ob Matrizen nicht *konjugiert sind.*

Für ein von Matrizen, die nicht konjugiert sind, wo aber alle Konjugationsinvarianten aus Lemma 3.4.42 übereinstimmen, sei betrachtet:

$$B := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2 \quad \textit{und} \quad C := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Für die Konjugationsinvarianten der beiden Matrizen gilt:

$$\begin{aligned} \det(B) &= 1 = \det(C), \\ \chi_B &= t^2 - 2t + 1 = \chi_C, \\ \operatorname{sp}(B) &= 2 = \operatorname{sp}(C), \\ \operatorname{rg}(B) &= 2 = \operatorname{rg}(C). \end{aligned}$$

Jedoch ist B als Einheitsmatrix nur zu sich selbst konjugiert und zu damit zu keiner anderen Matrix - und insbesondere auch nicht zu C.

Zur Klassifikation von Matrizen bis auf Konjugation müssen also noch bessere Konjugationsinvarianten gefunden werden! $\square$

Beispiel 3.4.44. *Die folgenden Matrizen aus* $\operatorname{Mat}_2(\mathbb{R})$ *sind nach Beispiel 3.4.35 konjugiert:*

$$D := \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \quad \textit{und} \quad F := \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}.$$

Deren Konjugationsinvarianten aus Lemma 3.4.42 müssen dann übereinstimmen, und tatsächlich gilt:

$$\begin{aligned} \det(D) &= 6 = \det(F), \\ \chi_D &= t^2 - 5t + 6 = \chi_F, \\ \operatorname{sp}(D) &= 5 = \operatorname{sp}(F), \\ \operatorname{rg}(D) &= 2 = \operatorname{rg}(F). \end{aligned} \qquad \square$$

Da die Determinante und das charakteristische Polynom einer Matrix konjugationsinvariant sind und Matrizendarstellungen von Endomorphismen bzgl. gleichgroßer Basen konjugiert sind, lassen sich beide Begriffe von Matrizen auf abstrakte Endomorphismen übertragen:

Satz 3.4.45. *Sei K ein Körper und V ein endlichdimensionaler K-Vektorraum. Dann besitzt jedes $\varphi \in \mathrm{End}_K(V)$ eine Matrizendarstellung, da V eine endliche Basis besitzt, und es gilt::*

i.) Alle Matrizendarstellungen $[\varphi]_{B,B}$ von φ bzgl. irgendeiner Basis B haben die gleiche Determinante.

ii.) Alle Matrizendarstellungen $[\varphi]_{B,B}$ von φ bzgl. irgendeiner Basis B haben das gleiche charakteristische Polynom.

Damit kann jedem Endomorphismus eines endlichdemensionalen K-Vektorraumes eine Determinante und ein charakteristisches Polynom zugeordnet werden, in dem für $\varphi \in \mathrm{End}_K(V)$ bzgl. einer beliebig gewählten Basis B von V definiert wird:

$$\det(\varphi) := \det\big([\varphi]_{B,B}\big) \quad \textit{und} \quad \chi_\varphi := \chi_{[\varphi]_{B,B}}.$$

Beweis.
Der endlich-dimensionale K-Vektorraum V ist ein freier Modul, da jeder Vektorraum eine Basis besitzt (Satz 2.2.43), und zwei gewählte Basen $\mathcal{B}$ und $\mathcal{C}$ sind darin von gleicher Länge (nämlich der Dimension von V, Satz 2.2.46). Dann sind nach Satz 3.4.36 die Matrizendarstellungen $[\varphi]_{\mathcal{B},\mathcal{B}}$ und $[\varphi]_{\mathcal{C},\mathcal{C}}$ konjugiert und haben nach Lemma 3.4.42 die gleiche Determinante und das gleiche charakteristische Polynom. □

Bemerkung 3.4.46. *Es ist möglich, Satz 3.4.45 für freie Moduln mit endlichen Basen zu erweitern, und damit auch die Definition von Determinante und charakteristischen Polynom für Endomorphismen solcher Module, wenn in solchen Moduln alle Basen die gleiche Länge haben. Dies ist tatsächlich der Fall, aber nicht im Skript bewiesen. Daher hier die Einschränkung auf den Fall von Vektorräumen.* □

Es soll noch einmal das Beispiel 3.4.35 betrachtet werden: der Endomorphismus

$$f\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \quad \text{mit} \quad (x,y) \mapsto (x+2y,\ -x+4y)$$

hat bzgl. der Basen

$$\mathcal{B} := \big((2,1),\ (1,1)\big) \quad \text{und} \quad \mathcal{E}_2$$

zueinander konjugierte Matrizendarstellungen

$$B := [f]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \quad \text{und} \quad C := [f]_{\mathcal{E}_2,\mathcal{E}_2} = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix},$$

wobei die Matrix B eine besonders einfache Gestalt hat und eine Diagonalmatrix ist. Dazu sei folgende Definition gemacht:

Definition 3.4.47. *Sei R ein kommutativer Ring mit Eins und M ein freier R-Modul. Ein Endomorphismus $\varphi \in \mathrm{End}_R(M)$ heißt diagonalisierbar, wenn es eine endliche Basis $\mathcal{B}$ von M gibt, so daß die Matrizendarstellung $[f]_{\mathcal{B},\mathcal{B}}$ eine Diagonalmatrix ist.*
Eine Matrix $A \in \mathrm{Mat}_n(R)$ heißt diagonalisierbar, wenn sie konjugiert zu einer Diagonalmatrix ist. □

Bemerkung 3.4.48. *Nach Lemma 3.4.38 können zwei konjugierte Matrizen als Matrizendarstellung eines Endomorphismus zu verschiedenen Basen aufgefaßt werden, so daß direkt aus obiger Definition für eine Matrix A folgt:*

$$A \text{ ist diagonalisierbar} \quad \Longleftrightarrow \quad \begin{array}{l} A \text{ ist die Matrizendarstellung einer diago-} \\ \text{nalisierbaren Abbildung.} \end{array}$$

Dies erklärt den Zusammenhang des Diagonalisierbarkeitsbegriffs für Endomorphismen und Matrizen. □

Eine Diagonalmatrix D mit den Diagonaleinträgen $d_1, \dots d_n$ hat die Eigenschaft, daß für die Standard-Basisvektoren $e_1, \dots, e_n$ gilt:

$$D \cdot e_i = d_i \cdot e_i,$$

d.h. der Vektor e_i wird nur mit dem Faktor d_i multipliziert. Hat der Endomorphismus f bzgl. einer Basis $\mathcal{B}$ die Matrizendarstellung $[f]_{\mathcal{B},\mathcal{B}} = D$, so gilt für den Vektor $v_i := [e_i]_{\mathcal{B}}^{-1}$ nach Satz 3.4.17:

$$[f(v_i)]_B = [f]_{\mathcal{B},\mathcal{B}} \cdot [v_i]_{\mathcal{B}} = D \cdot e_i = d_i \cdot e_i \quad \overset{[\,\cdot\,]_{\mathcal{B}}}{\Longrightarrow} \quad f(v_i) = d_i \cdot v_i.$$

Insbesondere ist der Vektor v_i nicht Null, da er das Bild von $e_i \neq 0$ unter dem Isomorphismus $[\,\cdot\,]_{\mathcal{B}}$ ist. Es gibt also einen nicht-trivialen Vektor, der von der Abbildung f um den Faktor d_i gestreckt wird. Der Nullvektor erfüllt diese Eigenschaft bzgl. jeden Streckungsfaktors λ, es gilt immer $f(0) = 0 = \lambda \cdot 0$, daher hier die Betonung auf die Existenz eines nicht-trivialen Vektors!
Hat v die Eigenschaft, durch den Endomorphismus f um den Faktor λ gestreckt zu werden, so erfüllt er die folgende Äquivalenz:

$$f(v) = \lambda v \quad \Longleftrightarrow \quad (f - \lambda \cdot \mathrm{id})(v) = 0. \tag{3.4.49}$$

Damit liegt v also im Kern des Endomorphismus $f - \lambda \cdot \mathrm{id}$, was eine nützliche Beschreibung ist, da Kerne von linearen Abbildungen wohlbekannte Objekte sind. Dies führt zur folgenden Definition:

Definition 3.4.50. *Sei K ein Körper, V ein K-Vektorraum und $\varphi \in \mathrm{End}_K(V)$. Ein $\lambda \in K$ heißt Eigenwert von φ, falls gilt:*

$$\ker(\varphi - \lambda \cdot \mathrm{id}_V) \neq \{0\}.$$

Ist λ ein Eigenwert von φ, so heißen alle Vektoren aus $\ker(\varphi - \lambda \cdot \mathrm{id}_V)$ Eigenvektoren von φ zum Eigenwert λ. Der Untervektorraum $\ker(\varphi - \lambda \cdot \mathrm{id}_V) \subseteq V$ heißt der Eigenraum von φ zum Eigenwert λ (oder auch kurz: Eigenraum zu λ). Der Eigenraum von φ zum Eigenwert λ wird auch notiert mit:

$$\mathrm{Eig}(\varphi, \lambda) := \ker(\varphi - \lambda \cdot \mathrm{id}), \qquad \textit{kurz auch: } V_\lambda := \mathrm{Eig}(\varphi, \lambda).$$

Ist $A \in \mathrm{Mat}_n(K)$, so heißt λ ein Eigenwert zu A, wenn das homogene lineare Gleichungssystem

$$(A - \lambda E_n)z = 0$$

nicht-triviale Lösungen hat. Ist λ ein Eigenwert zu A, so heißen alle Lösungsvektoren des homogenen linearen Gleichungssystems $(A - \lambda E_n)z = 0$ Eigenvektoren von A zum Eigenwert λ. Der Lösungsraum des linearen Gleichungssystems $(A - \lambda E_n)z = 0$ im $K^{[n]}$ heißt auch der Eigenraum von A zum Eigenwert λ (oder auch kurz: Eigenraum zu λ). Der Eigenraum von A zum Eigenwert λ wird auch notiert mit:

$$\mathrm{Eig}(A, \lambda) := \ker(A - \lambda \cdot \mathrm{id}).$$ □

Bemerkung 3.4.51.

i.) *Die Definition des Eigenraumes eines Endomorphismus f wurde von der Äquivalenz 3.4.49 inspiriert:*

$$f(v) = \lambda v \quad \Longleftrightarrow \quad (f - \lambda \cdot \mathrm{id})(v) = 0,$$

d.h. es werden diejenigen Vektoren gesucht, die von f um den Faktor λ gestreckt werden. Natürlich wäre es auch möglich gewesen, obige Äquivalenz folgendermaßen aufzustellen:

$$f(v) = \lambda v \quad \Longleftrightarrow \quad (\lambda \cdot \mathrm{id} - f)(v) = 0.$$

Da natürlich folgende Gleichung besteht (Übung!):

$$\ker(f - \lambda \cdot \mathrm{id}) = \ker(\lambda \cdot \mathrm{id} - f),$$

ist es völlig egal, welche Variante zur Definition von $\mathrm{Eig}(f, \lambda)$ verwendet wird.

ii.) *Mit der Äquivalenz 3.4.49 ergibt sich folgende äquivalente geometrische Definition von Eigenwerten und Eigenvektoren eines Endomorphismus $\varphi \in \mathrm{End}_K(V)$:*

- *λ ist ein Eigenwert von φ, wenn es einen Nicht-Nullvektor $v \in V$ gibt, der von φ um den Faktor λ gesteckt wird:*

$$\varphi(v) = \lambda \cdot v.$$

- *Eigenvektoren zu λ sind genau diejenigen Vektoren, die von φ um den Faktor λ gestreckt werden.*

Analog läßt sich für eine Matrix $A \in \mathrm{Mat}_n(K)$ formulieren:

- *λ ist ein Eigenwert von A, wenn es einen Nicht-Nullvektor $x \in K^{[n]}$ gibt, der multipliziert mit A das λ-fache von sich ergibt:*

$$Ax = \lambda x.$$

- *Eigenvektoren zu λ sind genau diejenigen Vektoren, die multipliziert mit A das λ-fache von sich ergeben.*

iii.) *Die geometrische Interpretation von Eigenwerten und Eigenvektoren beantwortet sofort die Frage, ob jeder Endomorphismus Eigenwerte besitzt: Nein! Wird in der Ebene $\mathbb{R}^2$ um den Winkel α gedreht und gilt $\alpha \notin \{0°, 180°\}$, so wird kein Vektor auf ein Vielfaches von sich abgebildet (Die Drehung um $\alpha = 180°$ jedoch bildet einen Vektor v auf $-v$ ab!).*

iv.) *Zwei Werte aus K haben eine besondere Interpretation, falls sie als Eigenwert eines $\varphi \in \mathrm{End}_K(V)$ auftregen:*

$\lambda = 1$: *Ist Eins ein Eigenwert von φ, so sind die Eigenvektoren von φ zum Eigenwert Eins Fixpunkte von φ:*

$$\varphi(v) = 1 \cdot v \quad \Longleftrightarrow \quad \varphi(v) = v.$$

$\lambda = 0$: *Ist Null ein Eigenwert von φ, so sind die Eigenvektoren von φ zum Eigenwert Null die Elemente des Kerns von φ:*

$$\varphi(v) = 0 \cdot v = 0 \quad \Longleftrightarrow \quad v \in \ker(\varphi).$$

Dies liefert sofort zwei anschauliche Aussagen:

A1: Ein Endomorphismus hat genau dann den Eigenwert Eins, wenn er nicht-triviale Fixpunkte hat.

A2: Ein Endomorphismus hat genau dann den Eigenwert Null, wenn er einen nicht-trivialen Kern hat.

v.) *Ist eine Matrix $A \in \mathrm{Mat}_n(K)$ gegben, so induziert diese einen Endomorphismus $\varphi_A \in \mathrm{End}_K(K^{[n]})$ mit $\varphi_A(x) = Ax$ für alle $x \in K^{[n]}$. In diesem Fall sind die Lösung des homogenen linearen Gleichungssystems $Az = 0$ und der Kern von φ_A die gleiche Menge. Dies gilt dann natürlich analog für die Matrix $A - \lambda \cdot E_n$ und den davon induzierten Endomorphismus $\varphi_{A-\lambda\cdot E_n}$, und mit Satz 3.1.20 folgt:*

$$\begin{aligned}\mathrm{Eig}(A,\lambda) &\overset{(Def)}{=} \text{Lösung von: } (A-\lambda\cdot E_n)z = 0\\ &= \ker(\varphi_{(A-\lambda\cdot E_n)})\\ &\overset{(3.1.20)}{=} \ker(\varphi_A - \lambda\cdot \mathrm{id})\\ &\overset{(Def)}{=} \mathrm{Eig}(\varphi_A,\lambda).\end{aligned}$$

Insbesondere haben A und φ_A die selben Eigenwerte.

vi.) *Die Definitionen von Eigenwerten und Eigenvektoren in Definition 3.4.50 sind dort auf Vektorraumendomorphismen beschränkt. Tatsächlich könnten die Begriffe auch auch Modulendomorphismen erweitert werden. Für spätere Aussagen und Berechnungen ist es aber nützlich, diese Begriffe nur in Körpern zu betrachten.*
Insbesonder bei Ringen mit Nullteilern treten Phänomene auf, die der geometrischen Anschauung von Eigenwerten/Eigenvektoren zuwiderlaufen. Im $\mathbb{Z}_4$-Modul $\mathbb{Z}_4$ gilt dazu zum Beispiel für die Identitätsabbildung:

$$\mathrm{id}_{\mathbb{Z}_4}\left([2]_4\right) = [2]_4 = [1]_4 \cdot [2]_4 = [3]_4 \cdot [2]_4,$$

so daß der Vektor $[2]_4$ Eigenvektor zu den verschiedenen Eigenwerten $[1]_4$ und $[3]_4$ wäre - und insbesondere $[3]_4$ ein Eigenwert der Identität.
Bei freien Moduln über Integritätsringen, z.B. dem $\mathbb{Z}$-Modul $\mathbb{Z}^{[n]}$, macht die Erweiterung jedoch Sinn. □

Es ergibt sich sofort folgende nützliche Beschreibung der Diagonalisierbarkeit von Endomorphismen und Matrizen:

Satz 3.4.52. *Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum.*

i.) *Für $\varphi \in \mathrm{End}_K(V)$ und eine Basis $\mathcal{B} := (b_1, \ldots, b_n)$ von V gilt:*

$$[\varphi]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix} \iff \text{Der } i\text{-te Basisvektor } b_i \text{ ist ein Eigenvektor von } \varphi \text{ zum Eigenwert } \lambda_i.$$

Daraus folgt sofort folgende Formulierung:

$$\varphi \text{ ist diagonalisierbar} \iff V \text{ enthält eine Basis aus Eigenvektoren von } \varphi.$$

ii.) *Für eine Matrix $A \in \mathrm{Mat}_n(K)$ und eine Basis $\mathcal{B} := (b_1, \ldots, b_n)$ des $K^{[n]}$ gilt, wenn B diejenige Matrix ist, deren Spalten aus den Basisvektoren b_i besteht:*

$$B^{-1}AB = \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix} \iff \text{Der } i\text{-te Basisvektor } b_i \text{ ist ein Eigenvektor von } A \text{ zum Eigenwert } \lambda_i.$$

Daraus folgt sofort folgende Formulierung:

$$A \text{ ist diagonalisierbar} \iff K^{[n]} \text{ enthält eine Basis aus Eigenvektoren von } A.$$

Beweis.

i.) Es braucht nur die erste Äquivalenz der Aussage bewiesen werden, da die zweite Äquivalenz eine direkte Folgerung aus der ersten ist.

„$\Rightarrow$“: In der Matrix $[\varphi]_{\mathcal{B},\mathcal{B}}$ steht in der i-ten Spalte nach Lemma 3.4.14 der Koordinatenvektor $[\varphi(b_i)]_{\mathcal{B}}$. Nach Voraussetzung an $[\varphi]_{\mathcal{B},\mathcal{B}}$ ist dies der Spaltenvektor $\lambda_i \cdot e_i$, und es folgt wie behauptet:

$$[\varphi(b_i)]_{\mathcal{B}} = \lambda_i \cdot e_i \qquad \Longrightarrow \qquad \varphi(b_i) = [\lambda_i \cdot e_i]_{\mathcal{B}}^{-1} = \lambda_i \cdot b_i.$$

„$\Leftarrow$“: Gilt $\varphi(b_i) = \lambda_i \cdot b_i$, so folgt für den i-ten Spaltenvektor $[\varphi(b_i)]_{\mathcal{B}}$ von $[\varphi]_{\mathcal{B},\mathcal{B}}$ sofort:

$$[\varphi(b_i)]_{\mathcal{B}} = [\lambda_i \cdot b_i]_{\mathcal{B}} = \lambda_i \cdot [b_i]_{\mathcal{B}} = \lambda_i \cdot e_i.$$

Damit sind die Spalten von $[\varphi]_{\mathcal{B},\mathcal{B}}$ von der behaupteten Form.

ii.) Es braucht nur die erste Äquivalenz der Aussage bewiesen werden, da die zweite Äquivalenz eine direkte Folgerung aus der ersten ist.

„$\Rightarrow$“: Sei D die vorgegebene Diagonalmatrix mit den Diagonalelementen $\lambda_1, \ldots, \lambda_n$. Dann gilt:

$$B^{-1}AB = D \qquad \Longleftrightarrow \qquad AB = BD.$$

Da $b_1, \ldots, b_n$ die Spalten von B sind, entpricht das Produkt $A \cdot b_i$ dann dem Produkt $B \cdot d_i$, wenn d_i die i-te Spalte von D ist, und wegen $d_i = \lambda_i \cdot e_i$ folgt sofort wie gewünscht:

$$A \cdot b_i = B \cdot d_i = B \cdot (\lambda_i \cdot e_i) = \lambda_i \cdot (B \cdot e_i) = \lambda_i \cdot b_i,$$

da das Produkt einer Matrix mit den Standard-Basisvektor e_i genau deren i-te Spalte ergibt (siehe auch Lemma 3.1.6 zur Interpretation der Matrizenmultiplikation).

„$\Leftarrow$“: Wird das Matrizenprodukt wie in Lemma 3.1.6 betrachtet, ergibt sich aus der Gleichung $B^{-1}B = E_n$ sofort für den Spaltenvektor b_i von B die Gleichung $B^{-1} \cdot b_i = e_i$. Es gilt nach Voraussetzung $A \cdot b_i = \lambda_i \cdot b_i$, und es folgt:

$$(B^{-1}A) \cdot b_i = B^{-1}(\lambda_i \cdot b_i) = \lambda_i \cdot (B^{-1} \cdot b_i) = \lambda_i \cdot e_i.$$

Die Matrix $B^{-1}AB$ kann spaltenweise konstruiert werden, indem $B^{-1}A$ an die Spalten b_i von B multipliziert wird, und obige Aussage liefern:

$$B^{-1}A \cdot b_i = B^{-1} \cdot (\lambda_i b_i) = \lambda_i \cdot (B \cdot b_i) = \lambda_i \cdot e_i.$$

Also enthält das Produkt $B^{-1}AB$ die Spalten $\lambda_1 \cdot e_1, \ldots, \lambda_n \cdot e_n$, was genau der behaupteten Diagonalform entspricht. □

Bisher gibt es noch keine Möglichkeit, von einem gegebenen Endomorphismus oder einer gegebenen Matrix die Eigenwerte zu berechnen, denn es ist ja nicht ersichtlich, für welche Werte $\lambda \in K$ z.B. ein Gleichungssystem $(A - \lambda \cdot E_n)z = 0$ nicht-triviale Lösungen hat. „Systematisches durchprobieren“ mit allen Körperelementen ist sicher kein gehbarer Weg. Dabei ist auch gar nicht klar, ob und wieviele Eigenwerte eine gegebene Matrix (oder ein Endomorphismus) überhaupt hat.

Folgende Aussage gibt ein Mittel in die Hand, die Eigenwerte von Endomorphismen und Matrizen zu bestimmen und theoretische Aussagen über sie zu machen:

Satz 3.4.53. *Sei K ein Körper und V ein endlich-dimemsionaler K-Vektorraum.*

i.) Für $\varphi \in \mathrm{End}_K(V)$ und $\lambda \in K$ sind äquivalent:
- *a.) λ ist ein Eigenwert von φ.*
- *b.) Der Endomorphismus $\varphi - \lambda \cdot \mathrm{id}$ ist nicht injektiv/surjektiv/bijektiv.*
- *c.) λ ist eine Nullstelle des charakteristischen Polynoms χ_φ.*

ii.) Für eine Matrix $A \in \mathrm{Mat}_n(K)$ und $\lambda \in K$ sind äquivalent:
- *a.) λ ist ein Eigenwert von A.*
- *b.) Das homogene lineare Gleichungssystem $(A - \lambda E_n)z = 0$ hat nicht-triviale Lösungen.*
- *c.) λ ist Nullstelle des charakteristischen Polynoms χ_A.*

Insbesondere gilt dann, wenn A eine Matrizendarstellung von φ ist:

$$\lambda \text{ ist Eigenwert von } \varphi \quad \Longleftrightarrow \quad \lambda \text{ ist Eigenwert von } A.$$

Beweis.

i.) Es gilt folgende die Behauptung umfassende Kette von Äquivalenzen:

$$\begin{aligned}
& \lambda \text{ ist Eigenwert von } \varphi \\
\overset{3.4.50}{\Longleftrightarrow} \quad & \ker(\varphi - \lambda \cdot \mathrm{id}) \neq \{0\} \\
\overset{2.1.27}{\Longleftrightarrow} \quad & \text{Der Endomorphismus } \varphi - \lambda \cdot \mathrm{id} \text{ ist nicht injektiv} \\
\overset{2.2.60}{\Longleftrightarrow} \quad & \text{Der Endomorphismus } \varphi - \lambda \cdot \mathrm{id} \text{ ist nicht surjektiv} \\
\overset{2.2.60}{\Longleftrightarrow} \quad & \text{Der Endomorphismus } \varphi - \lambda \cdot \mathrm{id} \text{ ist nicht bijektiv} \\
\overset{*_1}{\Longleftrightarrow} \quad & \det(\varphi - \lambda \cdot \mathrm{id}) = 0 \\
\Longleftrightarrow \quad & \det(\lambda \cdot \mathrm{id} - \varphi) = 0 \\
\overset{*_2}{\Longleftrightarrow} \quad & \chi_\varphi(\lambda) = 0
\end{aligned}$$

Dabei gelten die Äquivalenzen $(*_1)$ und $(*_2)$ aus folgenden Gründen:

$*_1$: Ist $\mathcal{B}$ eine Basis von V, so gilt nach Satz 3.4.17

$$\varphi - \lambda \cdot \mathrm{id} \text{ nicht bijektiv} \quad \Longleftrightarrow \quad [\varphi - \lambda \cdot \mathrm{id}]_{\mathcal{B},\mathcal{B}} \text{ nicht invertierbar.}$$

Eine quadratische Matrix über einem Körper ist genau dann nicht invertierbar, wenn ihre Determinante Null ist (Satz 3.3.22), und da die Determinante eines Endomorphismus über eine seiner Matrizendarstellungen definiert ist, gilt die behauptete Äquivalenz.

$*_2$: Die Äquivalenz ist klar für eine Matrizendarstellung von $\lambda \cdot \mathrm{id} - \varphi$ (Definition des charakteristischen Polynoms einer Matrix 3.3.50), und da für einen Endomoprhismus die Determinante und das charakteristische Polynom über eine Matrizendarstellung definiert sind (Satz 3.4.45), überträgt sich die Äquivalenz auf den behaupteten Fall.

ii.) Es gilt folgende die Behauptung umfassende Kette von Äquivalenzen:

$$\begin{aligned}
& \lambda \text{ ist Eigenwert von } A \\
\overset{3.4.50}{\Longleftrightarrow} \quad & (A - \lambda \cdot E_n)z = 0 \text{ hat nicht-triviale Lösungen} \\
\overset{\star}{\Longleftrightarrow} \quad & A - \lambda \cdot E_n \text{ ist nicht invertierbar}
\end{aligned}$$

$$\begin{aligned} &\overset{3.3.22}{\Longleftrightarrow} && \det(A - \lambda \cdot E_n) = 0 \\ &\Longleftrightarrow && \det(\lambda \cdot E_n - A) = 0 \\ &\overset{3.3.50}{\Longleftrightarrow} && \chi_A(\lambda) = 0 \end{aligned}$$

Die Äquivalenz ($\star$) folgt daraus, daß die Invertierbarkeit einer quadratischen Matrix B äquivalent ist zu der Bijektivität des induzierten Endomorphismus φ_B (Satz 3.1.20) und damit zu dessen Injektivität (Lemma 2.2.60), und die Lösungsmenge des homogenen Gleichungssystems $Bz = 0$ zum Kern von φ_B in Korrespondez steht. Dann ergibt sich die Behauptung aus:

$$\begin{aligned} Bz = 0 \text{ hat nicht-triviale Lösungen} \quad &\Longleftrightarrow \quad \ker(\varphi_B) \neq \{0\} \\ &\Longleftrightarrow \quad \varphi_B \text{ nicht injektiv} \\ &\Longleftrightarrow \quad \varphi_B \text{ nicht bijektiv} \\ &\Longleftrightarrow \quad B \text{ nicht invertierbar.} \end{aligned}$$

Da das charakteristische Polynom von φ mit dem jeder seiner Matrizendarstellungen per Definition übereinstimmt, folgt die letzte Äquivalenzaussage sofort aus den vorherigen Ergebnissen, da Eigenwerte jeweils Nullstellen der charakteristischen Polynome sind. □

Bemerkung 3.4.54.

i.) *Der Eigenraum eines Endomorphismus φ zu einem Eigenwert λ wurde durch $\ker(\varphi - \lambda \cdot \mathrm{id})$ definiert. Beim Beweis, daß die Eigenwerte von φ den Nullstellen seines charakteristischen Polynoms χ_φ entsprechen, wurde dann zu der Abbildung $\lambda \cdot \mathrm{id} - \varphi$ gewechselt, da dies zur Definition von charakteristischen Polynomen paßt. Wegen*

$$\ker(\varphi - \lambda \cdot \mathrm{id}) = \ker(\lambda \cdot \mathrm{id} - \varphi)$$

(siehe auch Bemerkung 3.4.51) wäre es möglich, die Definition der Eigenräume umzustellen und sie den charakteristischen Polynomen anzupassen - allerdings ist die hier gewählte Form gerade beim Rechnen praktischer. Obige Gleichung erlaubt aber jedem, die ihm genehmere Form zu wählen.
Beim charakteristischen Polynom kann in der Definition nicht einfach von der gewählten Form $\det(t \cdot E_n - A)$ auf $\det(A - t \cdot E_n)$ gewechselt werden, da sonst bei ungeradem n das Polynom mit „-1“ multipliziert wird und nicht mehr normiert ist, denn es gilt:

$$\det(t \cdot E_n - A) = (-1)^n \cdot \det(A - t \cdot E_n).$$

ii.) *Satz 3.4.53 liefert für konjugierte Matrizen B und C sofort, daß sie die gleichen Eigenwerte besitzen, denn diese sind ja die Nullstellen der charakteristischen Polynome χ_B und χ_C, die nach Lemma 3.4.42 konjugationsinvariant sind und damit gleich.*

iii.) *Das charakteristische Polynom einer Matrix aus $\mathrm{Mat}_n(K)$ hat den Grad n (Lemma 3.3.53), und da Polynome vom Grad n über einem Körper K höchstens n Nullstellen haben können, ist damit die Anzahl der Eigenwerte einer $(n \times n)$-Matrix beschränkt durch deren Größe.*

Ebenso kann ein Endomorphismus eines n-dimensionalen Vektorraumes nicht mehr als n Eigenwerte haben, da sein charakteristisches Polynom als das einer seiner Matrizendarstellungen definiert ist, die auch eine $(n \times n)$-Matrix ist.
Im folgenden Satz 3.4.56 wird diese Abschätzung für die Anzahl der Eigenwerte auch ohne das charakteristische Polynom bewiesen.

iv.) Es sei K ein Körper und $p \in K[t]$ ein normiertes Polynom, welches in Linearfaktoren zerfalle:

$$p := t^n + c_{n-1} \cdot t^{n-1} + \ldots + c_1 \cdot t + c_0 \quad \textit{und} \quad p = \prod_{i=1}^{n} (t - \alpha_i).$$

Dann lassen sich die Koeffizienten c_i durch die Nullstellen α_i ausdrücken, und es gilt insbesondere (Übung! Per Induktion):

$$p = t^n + \big(\underbrace{-(\alpha_1 + \ldots + \alpha_n)}_{=c_{n-1}}\big) \cdot t^{n-1} + \ldots + c_1 \cdot t + \underbrace{(-1)^n \cdot \alpha_1 \cdots \alpha_n}_{=c_0}, \qquad (*)$$

d.h. der Koeffizient c_{n-1} ist die negative Summe der Nullstellen von p, und das Absolutglied c_0 das Produkt aller Nullstellen mit dem Vorzeichen $(-1)^n$.
Ist nun eine Matrix $A \in \mathrm{Mat}_n(K)$ gegeben mit dem charakteristischem Polynom χ_A, und zerfällt dieses in Linearfaktoren:

$$\chi_A = \prod_{i=1}^{n} (t - \lambda_i),$$

so gilt nach Lemma 3.3.53:

$$\chi_A = t^n - \mathrm{sp}(A) \cdot t^{n-1} + \ldots + c_1 \cdot t + (-1)^n \cdot \det(A),$$

und mit obiger Gleichung $(*)$ folgt:

$$\mathrm{sp}(A) = \sum_{i=1}^{n} \lambda_i \quad \textit{und} \quad \det(A) = \prod_{i=1}^{n} \lambda_i.$$

Da nach Satz 3.4.53 die Nullstellen λ_i des charakteristischen Polynoms χ_A genau die Eigenwerte von A sind, läßt sich dann salopp formulieren:

> *Die Spur von A ist die Summe seiner Eigenwerte.*
>
> *Die Determinante von A ist das Produkt seiner Eigenwerte.*

Bei dieser saloppen Formulierung muß darauf geachtet werden, daß unter den λ_i Eigenwerte mehrfach vorkommen können, so daß obige plakative Aussage immer „mit Vielfachheit“ der Nullstelle zu interpretieren ist.
Auch ist die Voraussetzung, daß χ_A in Linearfaktoren zerfällt, was nicht bei jedem charakteristischen Polynom erfüllt ist. Zum Beispiel hat die Matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ das charakteristische Polynom t^2+1, und über $\mathbb{Q}$ und $\mathbb{R}$ hat dies keine Nullstellen und zerfällt somit nicht in Linearfaktoren.

v.) Das charakteristische Polynom einer Diagonalmatrix D mit den Diagonalelementen $d_1, \ldots, d_n$ ist nach Bemerkung 3.3.51 ein Produkt von Linearfaktoren $(t - d_i)$:

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \quad \Longrightarrow \quad \chi_D = \prod_{i=1}^{n} (t - d_i).$$

Ist φ ein diagonalisierbarer Endolmorphismus, so gibt es eine Matrizendarestellung von φ von der Form D, und das charakteristische Polynom von φ ist ein Produkt Linearfaktoren:

$$\varphi \text{ diagonalisierbar} \quad \Longrightarrow \quad \chi_\varphi \text{ zerfällt in Linearfaktoren.}$$

Ist A eine diagonalisierbare Matrix, so kann sie in eine Matrix der Form D konjugiert werden, und da das charakteristische Polynom von A konjugationsinvariant ist, gilt $\chi_A = \chi_D$ und χ_A ist ein Produkt von Linearfaktoren:

$$A \text{ diagonalisierbar} \quad \Longrightarrow \quad \chi_A \text{ zerfällt in Linearfaktoren.}$$

vi.) *Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Für ein $\varphi \in \mathrm{End}_K(V)$ gilt nach Satz 3.4.53:*

$$\varphi \text{ hat den Eigenwert } 0 \quad \Longleftrightarrow \quad \varphi \text{ ist nicht injektiv/surjektiv/bijektiv.}$$

φ ist genau dann nicht injektiv/surjektiv/bijektiv, wenn $\det(\varphi) = 0$ gilt (siehe Satz 3.3.22 und Lemma 2.2.60).
Weiter hat φ genau dann den Eigenwert 0, wenn für das charakteristische Polynom χ_φ gilt: $\chi_\varphi(0) = 0$, denn ein Polynom $p := c_n \cdot t^n + \ldots c_1 \cdot t + c_0$ hat genau dann 0 als Nullstelle, wenn das Absolutglied c_0 gleich Null ist wegen $p(0) = c_0$.
Somit sind folgende Aussagen äquivalent:

- *φ hat den Eigenwert 0.*
- *φ ist nicht injektiv/surjektiv/bijektiv.*
- $\det(\varphi) = 0$.
- *χ_φ hat kein Absolutglied (bzw. es ist Null).* □

Beispiel 3.4.55.

i.) *Es sei K ein Körper und $A \in \mathrm{Mat}_n(K)$ eine obere oder untere Dreiecksmatrix mit Diagonalelementen $d_1, \ldots, d_n$. Dann gilt nach Beispiel 3.3.52:*

$$A = \begin{pmatrix} d_1 & & & \\ & d_2 & * & \\ & & \ddots & \\ & & & d_n \end{pmatrix} \quad \Longrightarrow \quad \chi_A = \det\big(t \cdot E_n - A\big) = \prod_{i=1}^{n} (t - d_i).$$

Nach Satz 3.4.53 sind die Eigenwerte von A genau die Nullstellen von χ_A und damit die Diagonalelemente von A:

> *Bei einer oberen/unteren Dreiecksmatrix entsprechen deren Diagonalelemente den Eigenwerten der Matrix.*

ii.) *Ist $A \in \mathrm{Mat}_2(\mathbb{R})$, so gilt für deren chararkteristisches Polynom $\chi_A \in \mathbb{R}[t]$:*

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Longrightarrow \quad \chi_A = t^2 - (a+d) \cdot t + (ad - bc).$$

(Siehe auch Bemerkung 3.3.54.)
Für ein normiertes quadratisches Polynom $t^2 + p \cdot t + q \in \mathbb{R}[t]$ liefert die sogenannte pq-Formel für dessen Nullstellen:

$$t_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}.$$

Es existieren genau dann (reelle) Nullstellen, wenn die Diskriminante des Polynoms nicht negativ ist:

$$t_{1/2} \in \mathbb{R} \text{ existieren} \quad \Longleftrightarrow \quad p^2 - 4q \geq 0.$$

Dann hat A genau dann Eigenwerte, wenn gilt:

$$(a+d)^2 - 4(ad - bc) \geq 0 \quad \Longleftrightarrow \quad (a-d)^2 + 4bc \geq 0.$$

iii.) Es sei $D_\alpha \in \mathrm{Mat}_2(\mathbb{R})$ die Matrizendarstellung der Drehung im $\mathbb{R}^2$ um den Winkel α bzgl. der Standardbasis (siehe Beispiel 3.4.16):

$$D_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Nach Beispiel 3.3.52 gilt:

$$\chi_{D_\alpha} = t^2 - 2 \cdot \cos(\alpha) \cdot t + 1.$$

Es existieren genau dann reelle Eigenwerte, wenn die Diskriminante von χ_{D_α} nicht negativ ist, d.h. wenn gilt:

$$\big(-2\cos(\alpha)\big)^2 - 4 \geq 0 \quad \Longleftrightarrow \quad 4\cos^2(\alpha) \geq 4. \quad \Longleftrightarrow \quad \cos^2(\alpha) \geq 1.$$

Wegen $\cos(\alpha) \in [-1, 1]$ gilt $\cos^2(\alpha) \leq 1$, so daß obige Ungleichung nur erfüllt ist, wenn gilt:

$$\cos^2(\alpha) = 1 \quad \Longleftrightarrow \quad \cos(\alpha) = \pm 1 \quad \Longleftrightarrow \quad \alpha \in \{\, k\pi \mid k \in \mathbb{Z} \,\}.$$

Die relevanten Winkel in Grad sind dann:

$$\alpha \in \{0^\circ, 180^\circ\},$$

was auch schon bei den geometrischen Überlegungen in Bemerkung 3.4.51 das Ergebnis war.

iv.) Nach Beispiel 3.4.44 gilt für die folgende Matrix $F \in \mathrm{Mat}_2(\mathbb{R}$:

$$F := \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \quad \Longrightarrow \quad \chi_F = t^2 - 5t + 6.$$

Die pq-Formel liefert die folgenden beiden Nullstellen von χ_F:

$$t_{1/2} = \frac{5 \pm \sqrt{5^2 - 4 \cdot 6}}{2} = \frac{5 \pm 1}{2} \quad \Longrightarrow \quad t \in \{2, 3\}.$$

Also hat F die Eigenwerte 2 und 3. □

Satz 3.4.56. *Sei K ein Körper und V ein eindlich-dimensionaler K-Vektorraum.*

i.) Es sei $\varphi \in \mathrm{End}_K(V)$, und $\lambda_1, \ldots, \lambda_k$ seien paarweise verschiedene Eigenwerte. Dann gilt:

a.) Sind $v_1, \ldots, v_k$ Eigenvektoren zu λ_i mit $v_i \neq 0$, so sind $v_1, \ldots, v_k$ linear unabhängig. Insbesondere folgt $k \leq \dim_K(V)$, d.h. es gibt höchstens so viele verschiedene Eigenwerte von $\varphi \in \mathrm{End}_K(V)$ wie die Dimension von V.

b.) Sind für $1 \leq i \leq k$ die Vektoren $v_{i,1}, \ldots, v_{i,r_i}$ jeweils linear unabhängige in den Eigenräumen $\mathrm{Eig}(\varphi, \lambda_i)$, so sind all diese Vektoren zusammen linear unabhängig:

$$\underbrace{v_{1,1}, \ldots, v_{1,r_1}}_{\text{l.u. Vektoren zu } \lambda_1}, \ldots, \underbrace{v_{k,1}, \ldots, v_{k,r_k}}_{\text{l.u. Vektoren zu } \lambda_k} \qquad \text{linear unabhängig in } V.$$

Insbesondere gilt damit:

$$\sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(\varphi, \lambda_i)\big) \leq \dim_K(V).$$

c.) Seien $\lambda_1, \ldots, \lambda_k$ alle Eigenwerte von φ. Dann folgt:

$$\varphi \text{ diagonalisierbar} \quad \Longleftrightarrow \quad \sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(\varphi, \lambda_i)\big) = \dim_K(V).$$

Im Falle der Diagonalisierbarkeit kann dann eine Eigenvektorbasis von V aus den Eigenvektorbasen der Eigenräume $\operatorname{Eig}(\varphi, \lambda_i)$ zusammengesetzt werden.

ii.) Sei $A \in \operatorname{Mat}_n(K)$, und es seien $\lambda_1, \ldots, \lambda_k$ paarweise verschiedene Eigenwerte zu A. Dann gilt:

a.) Sind für $1 \leq i \leq k$ die Vektoren $v_{i,1}, \ldots, v_{i,r_i}$ jeweils linear unabhängig in den Eigenräumen $\operatorname{Eig}(A, \lambda_i)$, so sind all diese Vektoren zusammen linear unabhängig:

$$\underbrace{v_{1,1}, \ldots, v_{1,r_1}}_{\text{l.u. Vektoren zu } \lambda_1}, \ldots, \underbrace{v_{k,1}, \ldots, v_{k,r_k}}_{\text{l.u. Vektoren zu } \lambda_k} \qquad \text{linear unabhängig in } K^{[n]}.$$

Insbesondere gilt dann:

$$\sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(A, \lambda_i)\big) \leq n,$$

und es gibt es höchstens n verschiedene Eigenwerte von A.

b.) Seien $\lambda_1, \ldots, \lambda_k$ alle Eigenwerte von A. Dann folgt:

$$A \text{ diagonalisierbar} \quad \Longleftrightarrow \quad \sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(A, \lambda_i)\big) = n.$$

Im Falle der Diagonalisierbarkeit kann dann eine Eigenvektorbasis des $K^{[n]}$ aus den Eigenvektorbasen der Eigenräume $\operatorname{Eig}(A, \lambda_i)$ zusammengesetzt werden.

Beweis.

i.) a.) Der Beweis wird per Induktion über die Anzahl k der paarweise verschiedenen Eigenwerte geführt:

Induktionsanfang $k = 1$: Der Vektor v_1 ist wegen $v_1 \neq 0$ ein einelementiges linear unabhängiges System (Beispiel 2.2.25).

Induktionsschritt $k \rightsquigarrow k+1$: Es seien nun $k+1$ paarweise verschiedene Eigenwerte $\lambda_1, \ldots, \lambda_{k+1}$ von φ gegeben und Eigenvektoren $v_1, \ldots, v_{k+1}$ mit $v_i \neq 0$, und es sei

$$\sum_{i=1}^{k+1} \alpha_i v_i = 0. \tag{$*$}$$

Es ist zu zeigen, daß daraus $\alpha_i = 0$ für alle $1 \leq i \leq k+1$ folgt.

Die Gleichug $(*)$ kann mit λ_{k+1} multipliziert werden, und es folgt:

$$\sum_{i=1}^{k+1} \alpha_i v_i = 0 \quad \Longrightarrow \quad \lambda_{k+1} \cdot \sum_{i=1}^{k+1} \alpha_i v_i = 0 \quad \Longrightarrow \quad \sum_{i=1}^{k+1} \lambda_{k+1} \alpha_i v_i = 0. \qquad (\star_1)$$

Andererseits folgt aus $\varphi(0) = 0$ und $\varphi(v_i) = \lambda_i v_i$:

$$0 = \varphi(0) = \varphi\Big(\sum_{i=1}^{k+1} \alpha_i v_i\Big) = \sum_{i=1}^{k+1} \alpha_i \varphi(v_i) = \sum_{i=1}^{k+1} \alpha_i \lambda_i v_i \quad \Longrightarrow \quad \sum_{i=1}^{k+1} \lambda_i \alpha_i v_i = 0. \quad (\star_2)$$

Die Differenz der beiden Gleichungen $(\star_1)$ und $(\star_2)$ ergibt dann:

$$\sum_{i=1}^{k+1} \lambda_{k+1} \alpha_i v_i - \sum_{i=1}^{k+1} \lambda_i \alpha_i v_i = 0 \quad \Longrightarrow \quad \sum_{i=1}^{k} (\lambda_{k+1} - \lambda_i) \alpha_i v_i = 0,$$

da die $(k+1)$-ten Terme in den Summen der linken Differenz beide gleich $\lambda_{k+1}\alpha_{k+1}v_{k+1}$ sind. Auf die Summe:

$$\sum_{i=1}^{k} (\lambda_{k+1} - \lambda_i) \alpha_i v_i = 0$$

kann dann die Induktionsannahme angewendet werden und es folgt für alle $1 \leq i \leq k$ dann $(\lambda_{k+1} - \lambda_i)\alpha_i = 0$. Wegen $\lambda_{k+1} - \lambda_i \neq 0$ (alle Eigenwerte paarweise verschieden!) gilt im nullteilerfreien Körper K:

$$\underbrace{(\lambda_{k+1} - \lambda_i)}_{\neq 0} \alpha_i v_i = 0 \quad \Longrightarrow \quad \alpha_i = 0.$$

Sind $\alpha_1, \ldots, \alpha_k$ alle Null, so folgt für den Koeffizienten α_{k+1} dann:

$$\alpha_{k+1} v_{k+1} = \sum_{i=1}^{k+1} \alpha_i \overset{(\star)}{=} 0 \quad \overset{v_{k+1} \neq 0}{\Longrightarrow} \quad \alpha_{k+1} = 0.$$

Damit ist die Induktion beendet und die Aussage des Satzes bewiesen, daß die Eigenvektoren zu paarweise verschiedenen Eigenwerten linear unabhängig sind (alles keine Nullvektoren!).
Da es per Definition zu jedem Eigenwert einen Nicht-Null-Eigenvektor gibt, existiert zu k paarweise verschiedenen Eigenvektoren dann auch ein linear unabhängiges System der Größe k, und da die Größe linear unabhängiger Systeme nach oben durch die Dimension des Raumes beschränkt ist, folgt $k \leq \dim_K(V)$.

b.) Es sei gegeben:

$$\sum_{i=1}^{k} \sum_{j=1}^{r_i} \alpha_{i,j} v_{i,j} = 0.$$

Zu zeigen ist, daß dann alle $\alpha_{i,j}$ Null sein müssen. Sei dazu betrachtet:

$$w_i := \sum_{j=1}^{r_i} \alpha_{i,j} v_{i,j} \quad \Longrightarrow \quad \sum_{i=1}^{k} w_i = 0. \qquad (\star)$$

Angenommen, $w_{j_1}, \ldots, w_{j_s}$ wären dabei keine Nullvektoren. Nach dem ersten Teil des Satzes wären sie dann linear unabhängig, würden aber nach $(\star)$ eine

nicht-triviale Linearkombination der Null liefern. Dies ist nicht möglich, so daß alle w_i Null sein müssen.
Dies liefert dann aber sofort für $1 \leq i \leq k$:

$$w_i = 0 \quad \Longrightarrow \quad \sum_{j=1}^{r_i} \alpha_{i,j} v_{i,j} = 0 \quad \overset{v_{i,1},\ldots,v_{i,r_i}\ \text{l.u.}}{\Longrightarrow} \quad \alpha_{i,j} = 0 \text{ für } 1 \leq j \leq r_i.$$

Dann sind aber wie gewünscht alle $\alpha_{i,j}$ gleich Null, und das Gesamtsystem aller $v_{i,j}$ ist linear unabhängig.
Die Abschätzung $\sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(\varphi, \lambda_i)\big) \leq \dim_K(V)$ folgt unmittelbar, da aus linear unabhängigen Systemen der verschiedenen Eigenräume ein linear unabhängiges System des Gesamtraumes zusammengesetzt werden kann.

c.) „$\Rightarrow$“: Es ist nur die Abschätzung $\dim_K(V) \leq \sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(\varphi, \lambda_i)\big)$ zu zeigen, da die Umkehrung nach vorheriger Aussage immer gilt.
Ist φ diagonalisierbar, gibt es nach Satz 3.4.52 eine Basis von V aus Eigenvektoren von φ. Sind darin jeweils n_i (linear unabhängige) Eigenvektoren aus dem Eigenraum V_{λ_i}, so folgt die gesuchte Abschätzung aus:

$$\dim_K(V) = n = \sum_{i=1}^{k} n_i \leq \sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(\varphi, \lambda_i)\big).$$

„$\Leftarrow$“: Basen aus den Eigenräumen V_{λ_j} können nach dem vorherigen Teil des Satzes zu einem linear unabhängigen System in V zusammengesetzt werden. Die Gleichung:

$$\dim_K(V) = \sum_{i=1}^{k} \dim_K \big(\operatorname{Eig}(\varphi, \lambda_i)\big)$$

liefert dann, daß das aus den Eigenvektor-Basen der Eigenräume zusammengesetzte linear unabhängige System in V schon ein maximales System und damit eine Basis aus Eigenvektoren von V ist.

ii.) Nach Bemerkung 3.4.51 haben die Matrix $A \in \operatorname{Mat}_n(K)$ und der induzierte Endomorphismus $\varphi_A \in \operatorname{End}_K(K^{[n]})$ die selben Eigenwerte, und es gilt die Gleichung:

$$\operatorname{Eig}(A, \lambda) = \operatorname{Eig}(\varphi_A, \lambda).$$

Damit übertragen sich alle Ergebnisse über φ_A aus dem ersten Teil des Satzes sofort auf die Aussagen über A. □

Bemerkung 3.4.57.

i.) Aus Satz 3.4.56 folgt sofort für ein $\varphi \in \operatorname{End}_K(V)$ mit $n := \dim_K(V)$:

$$\varphi \text{ hat } n \text{ verschiedene Eigenwerte} \quad \Longrightarrow \quad \varphi \text{ ist diagonalisierbar.}$$

Ebenso gilt für ein ein $A \in \operatorname{Mat}_n(K)$:

$$A \text{ hat } n \text{ verschiedene Eigenwerte} \quad \Longrightarrow \quad A \text{ ist diagonalisierbar.}$$

In beiden Fällen muß die Summe der Dimensionen der Eigenräume gleich n sein, da jeder Eigenraum per Definition mindestens die Dimension Eins hat:

$$\sum_{i=1}^{k} \underbrace{\dim\big(\operatorname{Eig}(\varphi,\lambda_i)\big)}_{\geq 1} \geq k,$$

und mit $\sum_{i=1}^{k} \dim\big(\operatorname{Eig}(\varphi,\lambda_i)\big) \leq n$ und $k = n$ folgt dann das Kriterium aus Satz 3.4.56:

$$\sum_{i=1}^{k} \dim\big(\operatorname{Eig}(\varphi,\lambda_i)\big) = n = \dim_K(V) \quad \Longleftrightarrow \quad \varphi \text{ ist diagonalisierbar.}$$

(Die Argumentation für A läuft analog.)

ii.) *Offensichtlich ist vorherige Bedingung für die Diagonalisierbarkeit nur hinreichend und nicht notwendig: denn die Identität bzw. die Einheitsmatrix sind beide diagonalisierbar, haben aber nur einen Eigenwert, nämlich die Eins.*

iii.) *Das Diagonalisierbarkeitskriterium aus Satz 3.4.56 mit der Eigenraumdimensionssumme kann auch folgendermaßen formuliert werden: Da für $\varphi \in \operatorname{End}_K(V)$ mit dem Rangsatz 2.2.59 formuliert werden kann:*

$$\dim_K\big(\operatorname{Eig}(\varphi,\lambda_i)\big) = \dim_K\big(\ker(\varphi - \lambda\cdot\mathrm{id})\big) = \dim_K(V) - \operatorname{rg}(\varphi - \lambda\cdot\mathrm{id}),$$

läßt sich mit Satz 3.4.56 formulieren:

$$\varphi \text{ diagonalisierbar} \quad \Longleftrightarrow \quad \sum_{i=1}^{k}\Big(\dim_K(V) - \operatorname{rg}(\varphi - \lambda_i\cdot\mathrm{id})\Big) = \dim_K(V).$$

Analog folgt dann für eine Matrix $A \in \operatorname{Mat}_n(K)$:

$$A \text{ diagonalisierbar} \quad \Longleftrightarrow \quad \sum_{i=1}^{k}\Big(n - \operatorname{rg}(A - \lambda_i\cdot E_n)\Big) = n. \qquad \square$$

Die vorherigen Sätze ermöglichen es ein Programm aufzustellen, wie eine gegebene Matrix $A \in \operatorname{Mat}_n(K)$ auf Diagonaliserbarkeit getestet und eine Matrix C konstruiert werden kann, so daß $C^{-1}AC$ eine Diagonalmatrix ist. Deren Diagonalelemente sind dann die Eigenwerte von A, und die Spalten von C die dazu passenden Eigenvektoren.

Test auf Diagonalisierbarkeit:

- Bestimme das charakteristische Polynom χ_A von A und dessen Nullstellen $\lambda_1,\ldots,\lambda_k$. Dies ergibt die Eigenwerte von A (Satz 3.4.53).
- Gilt $k = n$, so ist A diagonalisierbar (Bemerkung 3.4.57).
- Bei $k < n$ bestimme für jedes λ_i den Rang von $A - \lambda_i\cdot E_n$. Dann ist A genau dann diagonalierbar, falls gilt (Bemerkung 3.4.57):

$$n = \sum_{i=1}^{k}\big(n - \operatorname{rg}(A - \lambda_i\cdot E_n)\big).$$

Konstruktion der konjugierenden Matrix C:

- Bestimme für jedes λ_i eine Basis der Lösung des homogenen Gleichungssystems $(A - \lambda_i\cdot E_n)z = 0$: dies ist dann ein Basis des Eigenraumes $\operatorname{Eig}(A,\lambda_i)$.

- Alle Basen der Räume $\mathrm{Eig}(A, \lambda_i)$ ergeben eine Eigenvektorbasis des $K^{[n]}$ zu A (Satz 3.4.56), und werden diese Basisvektoren spaltenweise in eine Matrix C geschrieben, so ergibt sich (Satz 3.4.52):

$$C^{-1}AC = \text{Diagonalmatrix}.$$

Das i-te Diagonalelement ist dabei der Eigenwert zum i-ten Spaltenvektor von C.

Beispiel 3.4.58.

i.) Es sei folgende Matrix aus Beispiel 3.4.55 betrachtet:

$$F := \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}.$$

Das charakteristische Polynom von F ist:

$$\chi_F = t^2 - 5t + 6 = (t-2)(t-3),$$

und somit hat F die Eigenwerte 2 und 3. Da F „genügend“ Eigenwerte hat (soviel wie möglich, d.h. entsprechend seiner Größe), ist F diagonalisierbar. Zur Bestimmung einer Eigenraumbasis zur Konstruktion von C mit:

$$C^{-1}FC = \textit{Diagonalmatrix}$$

müssen Basen der Eigenräume $\mathrm{Eig}(F, 2)$ und $\mathrm{Eig}(F, 3)$ gefunden werden, also Basen der Lösungen der homogenen Gleichungssysteme:

$$(F - 2E_2)z = 0 \qquad \textit{und} \qquad (F - 3E_2)z = 0.$$

$(F - 2E_2)z = 0$: *Um eine Basis der Lösung von $(F - 2E_2)z = 0$ zu finden, kann $F - 2E_2$ in spezielle Zeilen-Stufen-Form gebracht werden, um aus dieser ein Basis abzulesen:*

$$F - 2E_2 = \begin{pmatrix} -1 & 2 \\ -1 & 2 \end{pmatrix} \quad \rightsquigarrow \quad \underbrace{\begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix}}_{\textit{sp. ZSF}} \quad \rightsquigarrow \quad \underbrace{v_1 = \begin{pmatrix} -2 \\ -1 \end{pmatrix}}_{\textit{Basisvektor}}.$$

$(F - 3E_2)z = 0$: *Um eine Basis der Lösung von $(F - 3E_2)z = 0$ zu finden, kann $F - 3E_2$ in spezielle Zeilen-Stufen-Form gebracht werden, um aus dieser ein Basis abzulesen:*

$$F - 3E_2 = \begin{pmatrix} -2 & 2 \\ -1 & 1 \end{pmatrix} \quad \rightsquigarrow \quad \underbrace{\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}}_{\textit{sp. ZSF}} \quad \rightsquigarrow \quad \underbrace{v_1 = \begin{pmatrix} -1 \\ -1 \end{pmatrix}}_{\textit{Basisvektor}}.$$

Nun kann die konjugierende Matrix C spaltenweise aus den Basisvektoren der Eigenräume zusammengesetzt werden:

$$C := \begin{pmatrix} -2 & -1 \\ -1 & -1 \end{pmatrix},$$

und es ergibt sich:

$$C^{-1}FC = \begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Dabei braucht die letzte Rechnung $C^{-1}FC$ nicht ausgeführt werden, da die Eigenwerte der Diagonalmatrix ja per Konstruktion von C schon feststehen (Satz 3.4.52).

ii.) Es sei folgende Matrix $A \in \mathrm{Mat}_3(\mathbb{R})$ betrachtet:

$$A := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Bei einer oberen Dreiecksmatrix stehen die Eigenwerte auf der Diagonalen (Beispiel 3.4.55), so daß das charakteristische Polynom χ_A nicht berechnet werden muß. Die Eigenwerte sind 1 und 2, und da deren Anzahl kleiner als Drei ist, kann nicht auf Diagonalisierbarkeit geschlossen werden.
Es müssen nun die Ränge der folgenden Matrizen berechnet werden:

$$A - 1 \cdot E_3 = A - E_3 \qquad \text{und} \qquad A - 2 \cdot E_3.$$

Zur Rangberechnung muß die jeweilige Matrix noch nicht in spezielle Zeilen-Stufen-Form gebracht werden, es reicht, eine „allgemeine“ Zeilen-Stufen-Form zu bestimmen:

$$A - E_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \rightsquigarrow \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

$$A - 2E_3 = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \rightsquigarrow \qquad \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Es tritt also beide Male der Rang Zwei auf, und das Rang-Kriterium aus Bemerkung 3.4.57 liefert:

$$\underbrace{\big(3 - \mathrm{rg}(A - E_3)\big)}_{\dim\left(\mathrm{Eig}(A,1)\right)} + \underbrace{\big(3 - \mathrm{rg}(A - 2E_3)\big)}_{\dim\left(\mathrm{Eig}(A,2)\right)} = (3-2) + (3-2) = 2 < 3,$$

also ist die Matrix A nicht diagonalisierbar.

iii.) Es sei folgende Matrix $B \in \mathrm{Mat}_3(\mathbb{R})$ betrachtet:

$$B := \begin{pmatrix} -7 & 4 & -4 \\ -12 & 7 & -6 \\ 0 & 0 & 1 \end{pmatrix}.$$

Als erstes muß das charakteristische Polynom von B berechnet werden, um die Eigenwerte von B zu erhalten, und es gilt:

$$\chi_B = t^3 - t^2 - t + 1 = (t-1)^2(t+1).$$

Die Eigenwerte sind -1 und 1, und da deren Anzahl kleiner als Drei ist, kann nicht auf Diagonalisierbarkeit geschlossen werden.
Es müssen nun die Ränge der folgenden Matrizen berechnet werden:

$$B - 1 \cdot E_3 = B - E_3 \qquad \text{und} \qquad B - (-1) \cdot E_3 = B + E_3.$$

Zur Rangberechnung muß die jeweilige Matrix noch nicht in spezielle Zeilen-Stufen-Form gebracht werden, es reicht, eine „allgemeine“ Zeilen-Stufen-Form

zu bestimmen:

$$B - E_3 = \begin{pmatrix} -8 & 4 & -4 \\ -12 & 6 & -6 \\ 0 & 0 & 0 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} -8 & 4 & -4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

$$B + E_3 = \begin{pmatrix} -6 & 4 & -4 \\ -12 & 8 & -6 \\ 0 & 0 & 2 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} -6 & 4 & -4 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Das Rang-Kriterium aus Bemerkung 3.4.57 liefert:

$$\underbrace{\big(3 - \mathrm{rg}(B - E_3)\big)}_{\dim\left(\mathrm{Eig}(B,1)\right)} + \underbrace{\big(3 - \mathrm{rg}(B + E_3)\big)}_{\dim\left(\mathrm{Eig}(B,-1)\right)} = (3-1) + (3-2) = 3,$$

also ist die Matrix B diagonalisierbar. Zur Bestimmung einer Eigenraumbasis zur Konstruktion von C mit:

$$C^{-1}BC = \textit{Diagonalmatrix}$$

müssen Basen der Eigenräume $\mathrm{Eig}(B,1)$ *und* $\mathrm{Eig}(B,-1)$ *gefunden werden, also Basen der Lösungen der homogenen Gleichungssysteme:*

$$(B - E_3)z = 0 \qquad \textit{und} \qquad (B + E_3)z = 0.$$

$(B - E_3)z = 0$: *Um eine Basis der Lösung von $(B - E_3)z = 0$ zu finden, kann $B - E_3$ in spezielle Zeilen-Stufen-Form gebracht werden, um aus dieser ein Basis abzulesen:*

$$B - E_3 = \begin{pmatrix} -8 & 4 & -4 \\ -12 & 6 & -6 \\ 0 & 0 & 0 \end{pmatrix} \quad \rightsquigarrow \quad \underbrace{\begin{pmatrix} 1 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{\textit{sp. ZSF}} \quad \rightsquigarrow \quad \underbrace{v_1 = \begin{pmatrix} \frac{1}{2} \\ -1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} -\frac{1}{2} \\ 0 \\ -1 \end{pmatrix}}_{\textit{Basisvektoren}}.$$

$(B + E_3)z = 0$: *Um eine Basis der Lösung von $(B + E_3)z = 0$ zu finden, kann $B + E_3$ in spezielle Zeilen-Stufen-Form gebracht werden, um aus dieser ein Basis abzulesen:*

$$B + E_3 = \begin{pmatrix} -6 & 4 & -4 \\ -12 & 8 & -6 \\ 0 & 0 & 2 \end{pmatrix} \quad \rightsquigarrow \quad \underbrace{\begin{pmatrix} 1 & -\frac{2}{3} & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}}_{\textit{sp. ZSF}} \quad \rightsquigarrow \quad \underbrace{v_1 = \begin{pmatrix} -\frac{2}{3} \\ -1 \\ 0 \end{pmatrix}}_{\textit{Basisvektor}}.$$

Nun kann die konjugierende Matrix C spaltenweise aus den Basisvektoren der Eigenräume zusammengesetzt werden - dabei werden die einzelnen Basisvektoren mit geeigneten Faktoren versehen, um ganzzahlige Einträge zu erhalten:

$$C := \begin{pmatrix} 1 & -1 & -2 \\ -2 & 0 & -3 \\ 0 & -2 & 0 \end{pmatrix}.$$

und es ergibt sich:

$$C^{-1}BC = \frac{1}{14} \cdot \begin{pmatrix} 6 & -4 & -3 \\ 0 & 0 & -7 \\ -4 & -2 & 2 \end{pmatrix} \cdot \begin{pmatrix} -7 & 4 & -4 \\ -12 & 7 & -6 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -2 \\ -2 & 0 & -3 \\ 0 & -2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Dabei braucht die letzte Rechnung $C^{-1}BC$ nicht ausgeführt werden, da die Eigenwerte der Diagonalmatrix ja per Konstruktion von C schon feststehen (Satz 3.4.52). □

Es soll noch untersucht werden, wann zwei Diagonalmatrizen zueinander konjugiert sind:

Lemma 3.4.59. *Sei K ein Körper, und seien $A, B \in \mathrm{Mat}_n(K)$ Diagonalmatrizen mit:*

$$A := \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \qquad \text{und} \qquad B := \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix}.$$

Die Matrizen A und B sind genau dann konjugiert ($A \sim B$), wenn die Diagonalelemente von A und B durch eine Permutation ineinander überführbar sind:

$$A \sim B \quad \Longleftrightarrow \quad \exists \pi \in S_n : a_i = b_{\pi(i)}.$$

Für $\sigma \in S_n$ sei $\varphi_\sigma \in \mathrm{End}_K(K^{[n]})$ der durch die Basiszuordnung $e_i \mapsto e_{\sigma(i)}$ definierte Endomorphismus. Weiter sei $P_\sigma \in \mathrm{Mat}_n(K)$ die σ durch den folgenden Gruppenmonomorphismus zugeordnete Matrix (siehe Aufgabe 4, Aufgabenblatt 1, LAIIa):

$$\Psi \colon S_n \longrightarrow \mathrm{GL}_n(K) \quad \text{mit} \quad \sigma \mapsto P_\sigma := [\varphi_\sigma].$$

Dann gilt mit obigem $\pi \in S_n$, welches die Diagonalelemete ineinander überführt:

$$a_i = b_{\pi(i)} \text{ für alle } i \quad \Longleftrightarrow \quad A = P_\pi^{-1} B P_\pi = P_{\pi^{-1}} B P_\pi.$$

Dabei hat die Matrix P_π die Form:

$$P_\pi = \begin{pmatrix} | & & | \\ e_{\pi(1)} & \cdots & e_{\pi(m)} \\ | & & | \end{pmatrix}.$$

Beweis.
Zuerst wird das Produkt $P_{\pi^{-1}} B P_\pi$ betrachtet: Für die Standard-Basisvektoren e_i gilt dabei mit $P_\sigma e_i = e_{\sigma(i)}$:

$$P_{\pi^{-1}} B P_\pi e_i \overset{(\text{Def } P_\pi)}{=} P_{\pi^{-1}} B e_{\pi(i)} \overset{(\text{Def } B)}{=} P_{\pi^{-1}} b_{\pi(i)} e_{\pi(i)} = b_{\pi(i)} P_{\pi^{-1}} e_{\pi(i)} \overset{(\text{Def } P_{\pi^{-1}})}{=} b_{\pi(i)} e_i.$$

Damit hat die i-te Spalte von $P_{\pi^{-1}} B P_\pi$ die Form $b_{\pi(i)} e_i$, und es folgt mit $A e_i = a_i e_i$ unmittelbar die Äquivalenz:

$$a_i = b_{\pi(i)} \text{ für alle } i \quad \Longleftrightarrow \quad A = P_{\pi^{-1}} B P_\pi.$$

Da die Abbildung Ψ ein Gruppenhomomorphismus ist, gilt:

$$E_n = \Psi(\mathrm{id}) = \Psi(\pi \circ \pi^{-1}) = P_\pi \cdot P_{\pi^{-1}} \quad \Longrightarrow \quad P_\pi^{-1} = P_{\pi^{-1}},$$

und es folgt die zweite Behauptung des Satzes:

$$a_i = b_{\pi(i)} \text{ für alle } i \quad \Longleftrightarrow \quad A = P_\pi^{-1} B P_\pi = P_{\pi^{-1}} B P_\pi.$$

Damit ist auch schon bewiesen:

$$a_i = b_{\pi(i)} \text{ für alle } i \quad \Longrightarrow \quad A \sim B,$$

und es muß nur die Umkehrung dieser Implikation gezeigt werden.

Sei also $A \sim B$. Nach Lemma 3.4.38 gibt es dann ein $f \in \mathrm{End}_K(K^{[n]})$ und Basen $\mathcal{V} := (v_1, \ldots, v_n)$ und $\mathcal{W} := (w_1, \ldots, w_n)$ des $K^{[n]}$ mit:

$$A = [f]_{\mathcal{V},\mathcal{V}} \quad \text{und} \quad B = [f]_{\mathcal{W},\mathcal{W}},$$

und nach Satz 3.4.52 sind die Basisvektoren v_i Eigenvektoren zu den Eigenwerten a_i und die Basisvektoren w_i Eigenvektoren zu den Eigenwerten b_i. Die Eigenwerte und Eigenräume von f, A und B sind alle gleich (Bemerkung 3.4.51).
Seien $\lambda_1, \ldots, \lambda_k$ die paarweise verschiedenen Eigenwerte von f, A und B, und r_i sei die Anzahl der Basisvektoren in $\mathcal{V}$ zum Eigenwert λ_i und s_i die entsprechende Anzahl der Basisvektoren in $\mathcal{W}$. Es soll nun $r_i = s_i$ für $1 \leq i \leq s_i$ gezeigt werden.
Dabei gelten bzgl. der beiden Basen $\mathcal{V}, \mathcal{W}$ des $K^{[n]}$ die Gleichungen:

$$\sum_{i=1}^{k} r_i = n = \sum_{i=1}^{k} s_i,$$

und wegen der Diagonalisierbarkeit von f, A, B enbenso:

$$n = \sum_{i=1}^{k} \dim_K \big(\mathrm{Eig}(f, \lambda_i)\big)$$

wegen:

$$\dim_K \big(\mathrm{Eig}(A, \lambda_i)\big) = \dim_K \big(\mathrm{Eig}(f, \lambda_i)\big) = \dim_K \big(\mathrm{Eig}(B, \lambda_i)\big).$$

Dies liefert dann die beiden Abschätzungen:

$$n = \sum_{i=1}^{k} r_i \leq \sum_{i=1}^{k} \dim_K \big(\mathrm{Eig}(f, \lambda_i)\big) = n \quad \Longrightarrow \quad r_i = \dim_K \big(\mathrm{Eig}(f, \lambda_i)\big)$$

$$n = \sum_{i=1}^{k} s_i \leq \sum_{i=1}^{k} \dim_K \big(\mathrm{Eig}(f, \lambda_i)\big) = n \quad \Longrightarrow \quad s_i = \dim_K \big(\mathrm{Eig}(f, \lambda_i)\big),$$

die zusammengefaßt $r_i = s_i$ ergeben.
Nun sind in den Basen $\mathcal{V}$ und $\mathcal{W}$ zu jedem der Eigenwerte λ_i gleichviele Basisvektoren enthalten, die dann mit einer Bijektion $\pi \in S_n$ jeweils einander zugeordnet werden können. Diese Zuordnung von Basisvektoren liefert dann aber die gewünschte Zuordnung der Diagonalelemente der Matrizen A und B, da der i-te Basis-/Eigenvektor mit dem i-ten Eigen-/Diagonalwert der Matrix korrespondiert. □

Beispiel 3.4.60. *Es seien folgende Diagonalmatrizen gegeben:*

$$A := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \quad \textit{und} \quad B := \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

*Die Diagonalelemente können durch die Permutation $\pi := (1432)$ ineinander überführt werden: dabei ist π eine Permutation der Diagonal**stellen**, nicht der Diagonal**werte**! Es gilt:*

$$a_1 = b_4 = b_{\pi(1)}, \quad a_2 = b_1 = b_{\pi(2)}, \quad a_3 = b_2 = b_{\pi(3)} \quad \textit{und} \quad a_4 = b_3 = b_{\pi(4)}.$$

Es folgt dann mit Lemma 3.4.59 und $\pi^{-1} = (1234)$*:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} = A = P_{\pi^{-1}} B P_\pi = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

□

Klassifikation von $\mathrm{Mat}_2(\mathbb{C})$ **bis auf Konjugation.**

Mit den bisherigen Ergebnissen ist es nun möglich, die (2×2)-Matrizen über dem Körper $\mathbb{C}$ vollständig bis auf Konjugation zu klassifizieren. Dazu kurz einige Worte zu den (aus der Analyisvorlesung bekannten) komplexen Zahlen $\mathbb{C}$.
Die Zahlenmengen:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

zeichnen sich dadurch aus, daß die nächstgrößere Menge aus der vorhergehenden konstruiert werden kann, indem ein „mathematischer Mangel“ behoben wird, wie im folgenden grob skizziert:

$\mathbb{Z}$ zu $\mathbb{Q}$: Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring, in dem nicht alle Elemente ein multiplikatives Inverses besitzen. Dies wird durch eine formale Konstruktion von „Brüchen“ behoben, so daß zu $\mathbb{Z}$ dann die Inversen $\frac{1}{z}$ für $z \neq 0$ hinzugefügt werden, und dies dann insgesamt den Körper $\mathbb{Q}$ der Brüche von $\mathbb{Z}$ ergibt.
Also wird $\mathbb{Z}$ „algebraisch“ erweitert, um multiplikative Inverse zu bekommen, und der Körper $\mathbb{Q}$ ist in diesem Sinne vollständig/perfekt.

$\mathbb{Q}$ zu $\mathbb{R}$: Die Erweiterung von $\mathbb{Q}$ nach $\mathbb{R}$ kann topologisch motiviert werden, in dem zu $\mathbb{Q}$ alle „fiktiven“ Grenzwerte von rationalen Cauchy-Folgen hinzugefügt werden wie zum Beispiel die eulersche Zahl:

$$e = \sum_{i=0}^{\infty} \frac{1}{i!}.$$

(Der Grenzwert einer Reihe ist auch der Grenzwert einer Folge: der Partialsummenfolge). Zwar läßt sich eine reelle Zahlen wie $\sqrt{2}$ auch algebraisch motivieren als Nullstelle des rationalen Polynoms $t^2 - 2$, welche dann zu $\mathbb{Q}$ hinzugefügt wird, aber so können nicht alle Hinzufügungen motiviert werden (e und π zum Beispiel sind nicht als Nullstellen rationaler Polynome konstruierbar), so daß die topologische Motivation umfassender ist. Der Körper $\mathbb{R}$ ist dann in dem Sinne vollständig/perfekt, daß jede Cauchy-Folge darin einen Grenzwert enthält.

$\mathbb{R}$ zu $\mathbb{C}$: $\mathbb{R}$ ist algebraisch nicht vollständig/perfekt, da nicht für alle Polynome sämtliche Nullstellen in $\mathbb{R}$ existieren (z.B. für $t^2 + 1$). Der Schritt von $\mathbb{R}$ nach $\mathbb{C}$ ist, genau diesen Mangel zu beheben, und alle Nullstellen reeller Polynome hinzuzufügen. $\mathbb{C}$ ist dann in diesem Sinne vollstängig/perfekt, daß jedes komplexe Polynom alle seine Nullstellen in $\mathbb{C}$ enthält bzw. über $\mathbb{C}$ in Linearfaktoren zerfällt.

Wird nun eine Matrix $A \in \mathrm{Mat}_2(\mathbb{C})$ betrachtet, so zerfällt deren charakteristisches Polynom $\chi_A \in \mathbb{C}[t]$ in Linearfaktoren:

$$\chi_A = (t - \lambda_1) \cdot (t - \lambda_2) \overset{(3.3.54)}{=} t^2 - \mathrm{sp}(A) \cdot t + \det(A) \overset{(3.4.54)}{=} t^2 - (\lambda_1 + \lambda_2) \cdot t + (\lambda_1 \cdot \lambda_2).$$

Es können nun zuersteinmal zwei Fälle unterschieden werden:

Fall A, $\lambda_1 \neq \lambda_2$: Dann ist A nach Bemerkung 3.4.57 diagonalisierbar (n verschiedene Eigenwerte, $n := 2$), und es folgt:

$$A \sim \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Fall B, $\lambda_1 = \lambda_2$: Es sei $\lambda := \lambda_1 = \lambda_2$, und es gilt dann:

$$\chi_A = (t-\lambda)^2 = t^2 - \mathrm{sp}(A) \cdot t + \det(A) = t^2 - 2\lambda \cdot t + \lambda^2. \tag{3.4.61}$$

Hier sind wiederum zwei Fälle zu unterscheiden:

$A - \lambda \cdot E_2 = 0$: Dann gilt $A = \lambda \cdot E_2$ und somit insbesondere:

$$A \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

$A - \lambda \cdot E_2 \neq 0$: Es ist eine Übungsaufgabe, dann zu zeigen, daß die folgende Gleichung gilt:

$$(A - \lambda \cdot E_2)^2 = 0.$$

(Ein möglicher Ansatz wäre, für $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ die Identitäten 3.4.61 auszunutzen, um $(A - \lambda \cdot E_2)^2$ zu berechnen.) Für $B := A - \lambda \cdot E_2$ gilt dann mit Bemerkung 3.4.41 (siehe auch Aufgabe 2.b, Übungsblatt 6, LAIIa):

$$B \neq 0, B^2 = 0 \quad \Longrightarrow \quad B \sim \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Dies liefert dann sofort:

$$\begin{aligned} SBS^{-1} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad &\Longrightarrow \quad S(A - \lambda \cdot E_2)S^{-1} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &\Longrightarrow \quad SAS^{-1} - \lambda \cdot E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &\Longrightarrow \quad SAS^{-1} = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \\ &\Longrightarrow \quad A \sim \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}. \end{aligned}$$

Damit ist für jede Matrix $A \in \mathrm{Mat}_2(\mathbb{C})$ eine spezielle Matrix angegeben, zu der sie konjugiert ist, und die drei Prototypen:

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \quad \lambda \cdot E_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix},$$

sind offensichtlich nicht zueinander konjugiert (entweder haben sie unterschiedliche Eigenwerte, oder die beiden Typen mit gleichen Eigenwerten sind nicht konjugiert, da $\lambda \cdot E_2$ nicht „wegkonjugiert“ werden kann).

Zusammengefaßt liefert dies folgende Beschreibung der Konjugationsklassen von $\mathrm{Mat}_2(\mathbb{C})$:

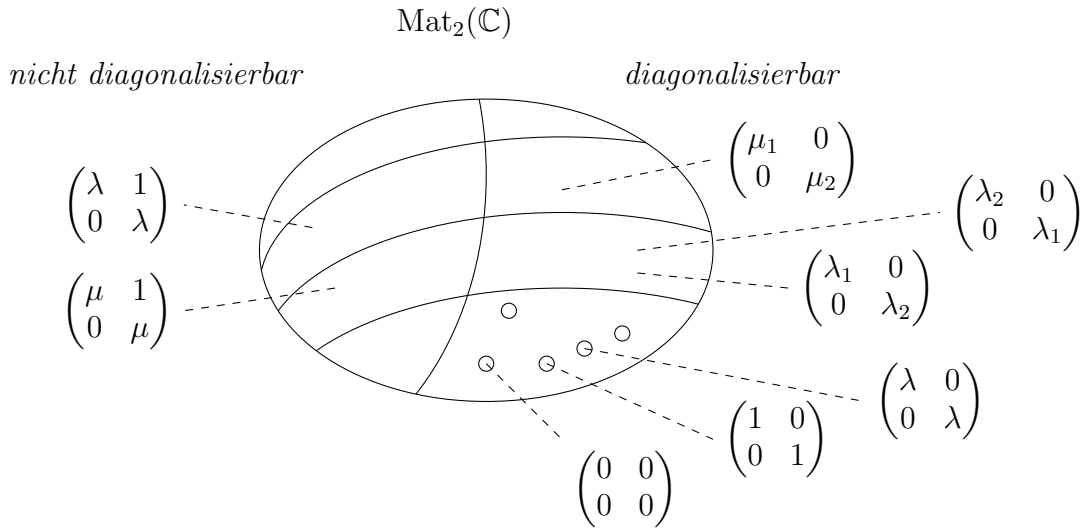
Bemerkung 3.4.62. *Jede Matrix* $A \in \mathrm{Mat}_2(\mathbb{C})$ *ist konjugiert zu genau einer der Matrizen des Types:*

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \quad \lambda \cdot E_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix},$$

wobei das charakteristische Polynom χ_A *die folgende Form hat:*

$$\chi_A = (t - \lambda_1)(t - \lambda_2) \quad \textit{oder} \quad \chi_A = (t - \lambda)^2.$$

Die Diagonalmatrix $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ *ist dabei nur bis auf Vertauschung der Diagonalelemente eindeutig. Die Konjugationsklassen der Matrizen* $\lambda \cdot E_2$ *sind offensichtlich einelementig. Dies führt zu folgender Skizze:*



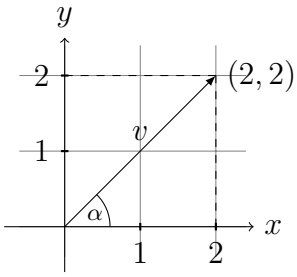
$\square$

KAPITEL 4

Euklidische Vektorräume

4.1. Euklidische Vektorräume

Bisher wurden Vektorräume und Moduln als „algebraische Strukturen“ betrachtet: als eine abelsche Gruppe, auf der ein Ring oder Körper operiert (dies ist die formale algebraische Sprechweise für die Definition 2.1.7 eines R-Moduls M via eines Ringhomorphismus $\Psi\colon R \longrightarrow \mathrm{End}(M)$ mit $\Psi(1_R) = \mathrm{id}_M$).
Zumindest in den $\mathbb{R}$-Vektorräumen $\mathbb{R}^2$ und $\mathbb{R}^3$, der „Ebene“ und dem „Raum“, ist schon bekannt, daß mit Vektoren nicht nur „algebraisch gerechnet“(d.h. Vektoren addiert oder gestreckt), sondern darin auch Geometrie betrieben wird. Geometrie in dem Sinne, daß es für Vektoren einen anschaulichen Längenbegriff gibt, Winkel zwischen Vektoren und, wenn die „Endpunkte“ von Vektoren als Punkte in der Ebene bzw. dem Raum aufgefaßt werden, auch ein Abstand zwischen diesen Punkten. Zum Beispiel ist aus der Schule bekannt:



Der Vektor $v := (2,2) \in \mathbb{R}^2$ hat die euklidische Länge:

$$|v| = \sqrt{2^2 + 2^2} = \sqrt{8} = 2\sqrt{2},$$

und den Winkel $\alpha = 45°$ zur x-Achse.

Zur Berechnung der Länge von v in obigem Beispiel wurde der Satz des Pythagoras in einem der durch gestrichelte Linien angedeuteten Dreiecke verwendet.

Es soll nun die anschauliche Geometrie in $\mathbb{R}^2$ und $\mathbb{R}^3$ auf beliebige Vektorräume verallgemeinert werden. Dabei ist jedoch zu beachten, daß dies nur bei speziellen Grundkörpern Sinn machen kann, denn z.B. über den endlichen Körpern $\mathbb{Z}_p$ widerspricht ein „Vielfaches“ eines Vektors jeder geometrischen Anschauung.
Tatsächlich wird im wesentlichen Geometrie in Vektorräumen über $\mathbb{R}$ und $\mathbb{C}$ betrieben, wobei salopp folgende Begriffsbildung gilt:

Vektorraum mit Geometrie über $\mathbb{R}$:	$\rightsquigarrow$	euklidischer Vektorraum.
Vektorraum mit Geometrie über $\mathbb{C}$:	$\rightsquigarrow$	unitärer Vektorraum.

In beiden Fällen wird die Geometrie mit Hilfe eines noch zu definierenden „Skalarproduktes“ abstrakt eingeführt, wobei sich die Definitonen eines Skalarproduktes über $\mathbb{R}$ und $\mathbb{C}$ wesentlich unterscheiden: dies wird hier nicht ausgeführt und sich auf den reellen Fall beschränkt.
Ist jedoch einmal ein Skalarprodukt gegeben, sind viele Konstruktionen und Ergebnisse in euklidischen und unitären Räumen analog/gleich.

Der Weg, mit einem Skalarprodukt in einem reellen Vektorraum Geometrie zu definieren, wird in zwei Schritten ablaufen:

$$\text{Skalarprodukt} \quad \rightsquigarrow \quad \text{Längenbegriff} \quad \rightsquigarrow \quad \text{Abstandsbegriff.}$$

Ein Längenbegriff in Vektorräumen ist wesentlich und kann auch unabhängig von einem Skalarprodukt durch eine „Norm“ definiert werden, und ein Abstandsbegriff ist in noch viel allgemeineren Situationen als nur in Vektorräumen von Interesse und wird dann unabhängig von Skalarprodukten durch eine „Metrik“ realisiert. So wird der Weg dann in neuer Sprechweise sein:

$$\text{Skalarprodukt} \quad \rightsquigarrow \quad \text{Norm} \quad \rightsquigarrow \quad \text{Metrik.}$$

Daß beide Begriffe (Norm/Metrik) in euklidischen Vektorräumen mit Hilfe eines Skalarproduktes realisiert werden, verleiht ihnen besondere Strukturverträglichkeit und liefert im Endeffekt einen topologischen Vektorraum - worauf hier nicht näher eingegangen wird.
Zunächst sei ein formaler Abstandsbegriff, eine Metrik, definiert:

Definition 4.1.1. *Sei M eine nicht-leere Menge. Eine Abbildung:*

$$d\colon M \times M \longrightarrow \mathbb{R}_0^+$$

heißt Metrik auf M, wenn folgende drei Bedingungen erfüllt sind:

$$\begin{aligned} \textit{Definitheit:} \quad & d(x,y) = 0 \quad \Longleftrightarrow \quad x = y. \\ \textit{Symmetrie:} \quad & d(x,y) = d(y,x). \\ \textit{Dreiecksungleichung:} \quad & d(x,z) \leq d(x,y) + d(y,z). \end{aligned}$$

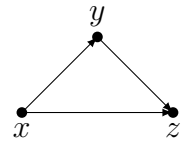
Dann wird (M,d) als metrischer Raum bezeichnet, und $d(x,y)$ als der Abstand zwischen $x, y \in M$. □

Bemerkung 4.1.2.

i.) Obige Definition eines „metrischen Raumes“ verlangt nur eine Abstandsfunktion/Metrik auf einer Menge, die selbst überhaupt keine Struktur zu tragen braucht.

ii.) Wird der Abstand zwischen zwei Punkten anschaulich interpretiert als „der Weg, der zwischen zwei Punkten zurückgelegt werden muß“, so sind die drei Forderungen an einen Abstandsbegriff/eine Metrik ebenfalls sehr anschaulich:

Definitheit:	*Sind Start- und Endpunkt gleich, so braucht kein Weg zwischen ihnen zurückgelegt werden, und ist bei einem Weg keine Strecke zurückzulegen, sind Start- und Endpunkt gleich.*
Symmetrie:	*Die Distanz zwischen zwei Punkten ist richtungsungabhängig, d.h. der Weg von x nach y ist genauso lang wie der von y nach x.*
Dreiecksungleichung:	*Die direkte Verbindung von x nach z ist kürzer, als einen Umweg über einen Punkt y zu nehmen.*



iii.) Auf jeder Menge M existiert die folgende triviale Metrik (Übung!):

$$d\colon M \times M \longrightarrow \mathbb{R}_0^+ \quad \textit{mit} \quad (x,y) \mapsto \begin{cases} 0 & \textit{für } x = y, \\ 1 & \textit{für } x \neq y. \end{cases}$$

In dieser Metrik hat ein Punkt zu jedem anderen Punkt den Abstand Eins. Dies zeigt, wie schwach die Forderungen an eine Metrik sind, denn mit dieser Metrik verbindet sich natürlich keine vernünftige Anschauung.

iv.) In metrischen Räumen können zwei wesentliche Begriffe definiert werden:
- *Konvergente Folgen.*
- *Stetige Funktionen.*

Nötig dazu ist die Definition einer Umgebung um Punkt $x \in M$ mit Hilfe eines ε-Balles $B_\varepsilon(x)$ für $\varepsilon > 0$:

$$B_\varepsilon(x) := \{\, y \in M \mid d(x,y) < \varepsilon \,\}.$$

Definition: Sei (M,d) ein metrischer Raum. Eine Folge $(x_i)_{i\in\mathbb{N}_0}$ in M heißt konvergent gegen einen Punkt x, falls gilt:

$$(x_i)_{i\in\mathbb{N}_0} \to x \quad \Longleftrightarrow \quad \textit{Für jedes } \varepsilon > 0 \textit{ liegen fast alle Folgenglieder in } B_\varepsilon(x).$$

Dabei bedeutet „fast alle“ im mathematischen Sinne: „alle bis auf endlich viele“. Dann läßt sich auch formaler schreiben:

$$(x_i)_{i\in\mathbb{N}_0} \to x \quad \Longleftrightarrow \quad \forall \varepsilon > 0\ \exists N_\varepsilon \in \mathbb{N} : d(x,x_i) < \varepsilon \textit{ für } i \geq N_\varepsilon.$$

Definition: Seien (M,d_1) und (N,d_2) metrische Räume. Dann heißt eine Abbildung $f\colon M \longrightarrow N$ stetig im Punkt x, falls gilt:

$$f \textit{ stetig in } x \quad \Longleftrightarrow \quad \textit{Für jedes } \varepsilon > 0 \textit{ gibt es ein } \delta > 0 \textit{ mit } f\big(B_\delta(x)\big) \subseteq B_\varepsilon\big(f(x)\big).$$

Auch dieses läßt sich formaler schreiben als:

$$f \textit{ stetig in } x \quad \Longleftrightarrow \quad \forall \varepsilon > 0\ \exists \delta > 0 : d_1(x,y) < \delta \implies d_2\big(f(x), f(y)\big) < \varepsilon.$$

v.) Auf einer Menge können viele verschiedene Metriken existieren: somit ist eine Aussage über den Abstand zweier Punkte immer nur im Kontext einer vorgegebenen Metrik möglich. □

Als nächstes wird auf $\mathbb{R}$-Vektorräumen ein abstrakter Längenbegriff eingeführt:

Definition 4.1.3. *Sei V ein $\mathbb{R}$-Vektorraum. Eine Abbildung:*

$$\|\cdot\|\colon V \longrightarrow \mathbb{R}_0^+$$

heißt Norm, wenn sie folgende drei Bedingungen erfüllt:

$$\begin{aligned} \textit{Definitheit:} \quad & \|x\| = 0 \quad \Longleftrightarrow \quad x = 0. \\ \textit{Homogenität:} \quad & \|\alpha \cdot x\| = |\alpha| \cdot \|x\|. \\ \textit{Dreiecksungleichung:} \quad & \|x+y\| \leq \|x\| + \|y\|. \end{aligned}$$

Dann wird $\big(V, \|\cdot\|\big)$ als normierter Vektorraum bezeichnet, und $\|x\|$ die Länge von $x \in V$.
Ein Vektor $x \in V$ heißt normiert, falls er die Länge Eins hat: $\|x\| = 1$. □

Bemerkung 4.1.4.

i.) Aus der Homogenität einer Norm folgt sofort:

$$\|-x\| = \|(-1)\cdot x\| = |-1|\cdot\|x\| = \|x\|,$$

was der Vorstellung entspricht, daß die Länge eines Vektors nicht davon abhängen soll, in welche Richtung er zeigt.

ii.) Auf einem Vektorraum können verschiedene Normen existieren. Die Länge eines Vektors ist somit immer nur im Kontext einer gewählten Norm definiert. □

Beispiel 4.1.5.

i.) Im $\mathbb{R}^{[n]}$ bzw. im $\mathbb{R}^n$ gibt es für jedes $p \in \mathbb{N}$ die sogenannte p-Norm:

$$\|x\|_p := \sqrt[p]{\textstyle\sum_{i=1}^n |x_i|^p},$$

wobei die x_i die Komponenten des Spalten- oder Zeilenvektors x sind (siehe z.B. [**BlAn1**, Seite 229-230] *für die Definition und den Beweis der Dreiecksungleichung mit Hilfe der Minkowski-Ungleichung).*

ii.) Im $\mathbb{R}^{[n]}$ bzw. im $\mathbb{R}^n$ gibt es die sogenannte Maximums-Norm:

$$\|x\|_\infty := \max(|x_i|),$$

wobei die x_i wieder die Komponenten des Spalten- oder Zeilenvektors x sind. Die Maximums-Norm hängt durch folgende Aussage mit den p-Normen zusammen:

$$\text{Für } x \in \mathbb{R}^{[n]} \text{ bzw. } x \in \mathbb{R}^n \text{ gilt:} \quad \lim_{p\to\infty} \|x\|_p = \|x\|_\infty.$$

iii.) Ist auf dem $\mathbb{R}^{[n]}$ eine Norm $\|\cdot\|$ gegeben, so induziert diese auf dem Matrizenraum $\mathrm{Mat}_n(\mathbb{R})$ eine Norm durch:

$$\|A\|_{ind} := \max_{x\neq 0} \frac{\|Ax\|}{\|x\|} = \max_{\|x\|=1} \|Ax\|.$$

Dazu muß natürlich zuerst einmal gezeigt werden, daß $\max_{\|x\|=1}\|Ax\|$ überhaupt existiert. Dies liegt daran, daß die von einer Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ induzierte Abbildung $\varphi_A \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^{[n]})$ stetig ist und ebenso die Norm-Abbildung $\|\cdot\|$ von $\mathbb{R}^{[n]}$ nach $\mathbb{R}$, und die Menge aller Vektoren mit der Länge Eins in $\mathbb{R}^{[n]}$ kompakt (siehe die $(n-1)$-te Einsheitsphäpre S^{n-1} in Definition 4.1.17).
Dann ist folgende Komposition von stetigen Abbildungen stetig:

$$\|\cdot\| \circ \varphi_A \colon \mathbb{R}^{[n]} \longrightarrow \mathbb{R},$$

und auf der kompakten Einheitsphäre $S^{n-1} \subseteq \mathbb{R}^{[n]}$ nimmt sie ein Maximum an und es gilt:

$$\|A\|_{ind} := \max_{\|x\|=1} \|Ax\| = \max\big((\|\cdot\| \circ \varphi_A)_{|_{S^{n-1}}}\big).$$ □

Wesentlich ist, daß eine gewählte Norm schon eine Metrik induziert, so daß mit einem Längen- auch gleich ein Abstandsbegriff in einem Vektorraum gegeben ist:

Lemma 4.1.6. *Sei $\big(V, \|\cdot\|\big)$ ein normierter $\mathbb{R}$-Vektorraum. Dann induziert die Norm $\|\cdot\|$ eine Metrik auf V durch:*

$$d_{\|\cdot\|} \colon V \times V \longrightarrow \mathbb{R}_0^+ \quad \text{mit} \quad (x,y) \mapsto \|x-y\|.$$

Die Metrik $d_{\|\cdot\|}$ heißt auch die von $\|\cdot\|$ induzierte Metrik auf V.

Beweis.
Es sind für $d_{\|\cdot\|}$ die drei Eigenschaften einer Metrik aus Definition 4.1.1 zu zeigen:

Definitheit: Es gilt für $x, y \in V$:

$$d_{\|\cdot\|}(x,y) = 0 \quad \overset{\text{(Def)}}{\Longleftrightarrow} \quad \|x-y\| = 0 \overset{(\|\cdot\| \text{ definit})}{\Longleftrightarrow} x - y = 0 \quad \Longleftrightarrow \quad x = y.$$

Symmetrie: Mit Bemerkung 4.1.4 folgt sofort:

$$d_{\|\cdot\|}(x,y) \overset{\text{(Def)}}{=} \|x-y\| \overset{(4.1.4)}{=} \|y-x\| \overset{\text{(Def)}}{=} d_{\|\cdot\|}(y,x).$$

Dreiecksungleichung: Für $x, y, z \in V$ gilt:

$$\begin{aligned} d_{\|\cdot\|}(x,z) &\overset{\text{(Def)}}{=} \|x-z\| = \|(x-y)+(y-z)\| \overset{\text{DrUngl}}{\leq} \|x-y\| + \|y-z\| \\ &\overset{\text{(Def)}}{=} d_{\|\cdot\|}(x,y) + d_{\|\cdot\|}(y,z). \end{aligned}$$

□

Bemerkung 4.1.7.

i.) Nach Lemma 4.1.6 induziert jede Norm auf einem Vektorraum eine Metrik, aber auf jedem Vektorraum gibt es mindestens eine Metrik, die nicht von einer Norm abgeleitet ist!
Ist V ein $\mathbb{R}$-Vektorraum mit einer Norm $\|\cdot\|$, so erfüllt die davon induzierte Metrik $d_{\|\cdot\|}$ für $v \neq 0$ wegen $\|v\| \neq 0$ die Gleichung:

$$d_{\|\cdot\|}(3v,v) = \|3v-v\| = \|2v\| = 2\cdot\|v\| \neq \|v\| = \|2v-v\| = d_{\|\cdot\|}(2v,v).$$

Die triviale Metrik aus Bemerkung 4.1.2:

$$d(x,y) = \begin{cases} 0 & \text{für } x = y, \\ 1 & \text{für } x \neq y, \end{cases}$$

liefert aber wegen $3v \neq v$ und $2v \neq v$:

$$d(3v,v) = 1 = d(2v,v),$$

so daß sie nicht von einer Norm induziert sein kann.

ii.) Auf den reellen Zahlen $\mathbb{R}$ ist die Betragsfunktion $|\cdot|$ eine Norm, und diese induziert nach Lemma 4.1.6 folgende Metrik auf $\mathbb{R}$:

$$d(x,y) := |x-y|.$$

Dann hat ein ε-Ball um ein $x \in \mathbb{R}$ bzgl. dieser Metrik die Form:

$$B_\varepsilon(x) = \{\, y \in \mathbb{R} \mid |x-y| < \varepsilon \,\}.$$

Eine Folge $(x_i)_{i\in\mathbb{N}_0}$ in $\mathbb{R}$ konvergiert dann in diesem metrischen Raum gegen x, falls gilt:

$$\begin{aligned} (x_i)_{i\in\mathbb{N}_0} \to x \quad &\Longleftrightarrow \quad \text{Für jedes } \varepsilon > 0 \text{ liegen fast alle Folgenglieder in } B_\varepsilon(x) \\ &\Longleftrightarrow \quad \forall \varepsilon > 0\ \exists N \in \mathbb{N} : d(x,x_i) < \varepsilon \text{ für } i \geq N \\ &\Longleftrightarrow \quad \forall \varepsilon > 0\ \exists N \in \mathbb{N} : |x-x_i| < \varepsilon \text{ für } i \geq N. \end{aligned}$$

Die letzte Zeile ist die übliche Definition einer konvergenten Folge in Analysis I. Wird eine Abbildung $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ betrachtet und jeweils in $\mathbb{R}$ die vom Betrag (Norm) induzierte Metrik, so ist f stetig in einem Punkt $x \in \mathbb{R}$, falls gilt:

$$\begin{aligned} f \text{ stetig in } x \quad &\Longleftrightarrow \quad \text{Für jedes } \varepsilon > 0 \text{ gibt es ein } \delta > 0 \text{ mit } f\big(B_\delta(x)\big) \subseteq B_\varepsilon\big(f(x)\big) \\ &\Longleftrightarrow \quad \forall \varepsilon > 0\ \exists \delta > 0 : d(x,y) < \delta \implies d\big(f(x), f(y)\big) < \varepsilon \end{aligned}$$

$$\iff \quad \forall \varepsilon > 0\ \exists \delta > 0 : |x - y| < \delta \implies |f(x) - f(y)| < \varepsilon.$$

Die letzte Zeile ist die übliche Definition der ε-δ-Stetigkeit von f in x. □

Nun wird das Skalarprodukt eines reellen Vektorraumes definiert, aus dem dann später eine Norm und damit auch Metrik abgeleitet werden können:

Definition 4.1.8. *Sei V ein $\mathbb{R}$-Vektorraum. Eine symmetrische Bilinearform (siehe 3.3.24):*

$$\langle \cdot, \cdot \rangle \colon V \times V \longrightarrow \mathbb{R}$$

heißt Skalarprodukt auf V, wenn sie zusätzlich auch positiv definit ist, d.h. wenn gilt:

$$\langle v, v \rangle > 0 \text{ für alle } v \neq 0.$$

Dann wird $\big(V, \langle \cdot, \cdot \rangle\big)$ als euklidischer Vektorraum bezeichnet. □

Bemerkung 4.1.9.

i.) *Das „Skalarprodukt“ zweier Vektoren ist* kein *Vektor, und damit ist es keine innere Verknüpfung auf dem Vektorraum, auch wenn sein Name es nahelegt. Zwischen Vektoren ist nur eine Addition definiert, keine Multiplikation!*

ii.) *Da $\langle \cdot, \cdot \rangle$ eine Bilinearform ist, gilt für alle Vektoren $x \in V$:*

$$\langle 0, x \rangle = \langle x, 0 \rangle = 0,$$

da für den Nullvektor gilt:

$$0_V = 0_{\mathbb{R}} \cdot 0_V \quad \implies \quad \langle 0_V, x \rangle = \langle 0_{\mathbb{R}} \cdot 0_V, x \rangle = 0_{\mathbb{R}} \cdot \langle 0_V, x \rangle = 0_{\mathbb{R}}.$$

iii.) *Die positive Definitheit von $\langle \cdot, \cdot \rangle$ liefert sofort für alle $x \in V$ die Ungleichung:*

$$\langle x, x \rangle \geq 0,$$

und es gilt folgende Äquivalenz:

$$\langle x, x \rangle = 0 \quad \iff \quad x = 0.$$

iv.) *Ist der Grundkörper $\mathbb{C}$, so werden nicht „Bilinearformen“ verwendet, um ein Skalarprodukt zu definieren, sondern sogenannte „Sesquilinearformen“. Eine Bilinearform:*

$$b(\cdot\,, \cdot) \colon V \times V \longrightarrow \mathbb{R}$$

ist in zwei Kompoenenten linear (d.h. verträglich mit der Addition und skalaren Multiplikation), eine Sesquilinearform:

$$s(\cdot\,, \cdot) \colon W \times W \longrightarrow \mathbb{C}$$

nur $1\frac{1}{2}$-fach linear, nämlich verträglich mit der Addition in beiden und der skalaren Multiplikation in einer *Komponente - in der anderen Komponente werden Skalare komplex konjugiert herausgezogen.*
Auch die Forderung der Symmetrie ändert sich im komplexen Fall zur Forderung „hermitesch“ zu sein, d.h. ein vertauschen der Einträge in der Sesquilinearform liefert den komplex konjugierten Wert:

$$s(x, y) = \overline{s(y, x)}.$$

Eine allgemeine Betrachtung von Sesquilinearformen findet sich zum Beispiel in [**BrLAII**]. □

Beispiel 4.1.10.

i.) Für den Spaltenraum $\mathbb{R}^{[n]}$ ist folgende Abbildung ein Skalarprodukt (Übung!):

$$\mathbb{R}^{[n]} \times \mathbb{R}^{[n]} \longrightarrow \mathbb{R} \quad \textit{mit} \quad \left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right) \mapsto \sum_{i=1}^{n} x_i \cdot y_i.$$

Dieses Skalarprodukt wird das Standard-Skalarprodukt auf dem $\mathbb{R}^{[n]}$ genannt. (Siehe auch Beispiel 3.3.26 und Definition 4.1.17.)

ii.) Für den Zeilenraum $\mathbb{R}^n$ ist folgende Abbildung ein Skalarprodukt (Übung!):

$$\mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R} \quad \textit{mit} \quad \big((x_1, \ldots, x_n),\ (y_1, \ldots, y_n)\big) \mapsto \sum_{i=1}^{n} x_i \cdot y_i.$$

Dieses Skalarprodukt wird das Standard-Skalarprodukt auf dem $\mathbb{R}^n$ genannt. (Siehe auch Beispiel 3.3.26 und Definition 4.1.17.)

iii.) Auf dem $\mathbb{R}^2$ ist folgende Abbildung ein Skalarprodukt (Übung!):

$$\mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R} \quad \textit{mit} \quad \big((x_1, x_2),\ (y_1, y_2)\big) \mapsto 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + 5x_2y_2.$$

iv.) Es sei folgende Teilmenge der reellen Folgen $\prod_{i\in\mathbb{N}_0} \mathbb{R}$ definiert:

$$\ell^2 := \{\, (x_i)_{i\in\mathbb{N}_0} \mid \sum_{i=0}^{\infty} |x_i|^2 < \infty \,\} \subseteq \prod_{i\in\mathbb{N}_0} \mathbb{R}.$$

Es ist eine leichte Übung zu zeigen, daß diese Teilmenge das Untervektorraum-Kritierium 2.1.13 erfüllt und damit ein $\mathbb{R}$-Vektorraum ist.
Auf ℓ^2 ist folgende Abbildung ein Skalarprodukt:

$$\langle\, \cdot, \cdot \,\rangle \colon \ell^2 \times \ell^2 \longrightarrow \mathbb{R} \quad \textit{mit} \quad \big((x_i)_{i\in\mathbb{N}_0}, (y_i)_{i\in\mathbb{N}_0}\big) \mapsto \sum_{i\in\mathbb{N}_0} x_i y_i.$$

Die obige Reihe konvergiert und $\langle\, \cdot, \cdot \,\rangle$ ist damit wohldefiniert, denn es gilt:

$$(x_i)_{i\in\mathbb{N}_0}, (y_i)_{i\in\mathbb{N}_0} \in \ell^2 \quad \Longrightarrow \quad x := \sum_{i\in\mathbb{N}_0} |x_i|^2 < \infty, \quad y := \sum_{i\in\mathbb{N}_0} |y_i|^2 < \infty,$$

und mit:

$$0 \leq \big(|x_i| - |y_i|\big)^2 = |x_i|^2 - 2|x_i||y_i| + |y_i|^2 \implies 2|x_iy_i| = 2|x_i||y_y| \leq |x_i|^2 + |y_i|^2 \quad (*)$$

folgt sofort die absolute Konvergenz und damit Konvergenz der Reihe:

$$\sum_{i\in\mathbb{N}_0} |x_iy_i| \leq \sum_{i\in\mathbb{N}_0} 2|x_iy_i| \overset{(*)}{\leq} \sum_{i\in\mathbb{N}_0} |x_i|^2 + \sum_{i\in\mathbb{N}_0} |y_i|^2 = x + y < \infty.$$

Daß $\langle\, \cdot, \cdot \,\rangle$ bilinear, symmetrisch und positiv definit ist, folgt sofort aus den Rechenregeln für Reihen und dessen Definition (Übung!).

v.) Sei $[a, b] \subseteq \mathbb{R}$ mit $a < b$ ein Intervall. Dann ist folgende Abbildung ein Skalarprodukt auf dem Raum $\mathcal{C}^0(\mathbb{R})$ der stetigen Abbildungen von $\mathbb{R}$ (Übung!):

$$\mathcal{C}^0(\mathbb{R}) \times \mathcal{C}^0(\mathbb{R}) \longrightarrow \mathbb{R} \quad \textit{mit} \quad (f, g) \mapsto \int_a^b f(x) \cdot g(x)\, dx.$$

(Siehe auch Beispiel 3.3.26.) □

Nun soll, wie bereits angekündigt, aus einem Skalarprodukt eine Norm auf dem Vektorraum abgeleitet werden. Um bei der Konstruktion die Dreiecksungleichung zu zeigen, ist die folgende Cauchy-Schwarzesche Ungleichung von Nutzen, die auch später zur Konstruktion/Definition von Winkeln zwischen Vektoren von gebraucht wird:

LEMMA 4.1.11. *(Cauchy-Schwarzsche Ungleichung)*
Sei $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ ein euklidischer Vektorraum. Dann gilt für alle $x, y \in V$:

$$\langle x, y\rangle^2 \leq \langle x, x\rangle \cdot \langle y, y\rangle.$$

Insbesondere folgt dann für alle $x, y \in V$:

$$|\langle x, y\rangle| \leq \sqrt{\langle x, x\rangle} \cdot \sqrt{\langle y, y\rangle}.$$

BEWEIS.
Zum Beweis der Formel:

$$\langle x, y\rangle^2 \leq \langle x, x\rangle \cdot \langle y, y\rangle$$

werden die beiden Fälle $x = 0$ und $x \neq 0$ separat untersucht:

$x = 0$: Bei der Bilinearform $\langle\,\cdot,\cdot\,\rangle$ gilt für alle $y \in V$ nach Bemerkung 4.1.9 die Gleichung:

$$\langle 0, y\rangle = \langle y, 0\rangle = 0.$$

Weiter gilt nach Bemerkung 4.1.9 für alle $y \in V$ die Ungleichung $\langle y, y\rangle \geq 0$, so daß zusammenfassend folgt:

$$\underbrace{\langle 0, y\rangle^2}_{=0} \leq \underbrace{\langle 0, 0\rangle}_{=0} \cdot \underbrace{\langle y, y\rangle}_{\geq 0}.$$

$x \neq 0$: Zuerst wird für alle $\alpha, \beta \in \mathbb{R}$ die aus der positiven Definitheit von $\langle\,\cdot,\cdot\,\rangle$ und Bemerkung 4.1.9 folgende Ungleichung:

$$0 \leq \langle \alpha x + \beta y, \alpha x + \beta y\rangle$$

betrachtet, und aus der Bilinearität von $\langle\,\cdot,\cdot\,\rangle$ folgt dann sofort:

$$\begin{aligned} 0 \leq \langle \alpha x + \beta y, \alpha x + \beta y\rangle &= \langle \alpha x, \alpha x\rangle + \langle \alpha x, \beta y\rangle + \langle \beta y, \alpha x\rangle + \langle \beta y, \beta y\rangle \\ &= \alpha^2 \cdot \langle x, x\rangle + \alpha\beta \cdot \langle x, y\rangle + \beta\alpha \cdot \langle y, x\rangle + \beta^2 \cdot \langle y, y\rangle. \end{aligned}$$

Da $\langle\,\cdot,\cdot\,\rangle$ symmetrisch ist und $\mathbb{R}$ kommutativ, können in der untersten Zeile die mittleren Terme zusammengefaßt werden, und es ergibt sich zusammengefaßt die Abschätzung:

$$0 \leq \alpha^2 \cdot \langle x, x\rangle + 2\alpha\beta \cdot \langle x, y\rangle + \beta^2 \cdot \langle y, y\rangle. \tag{$*$}$$

Diese Abschätzung gilt für alle $\alpha, \beta \in \mathbb{R}$, also auch für die beiden geschickt gewählten Werte:

$$\alpha := -\langle x, y\rangle \quad \text{und} \quad \beta := \langle x, x\rangle.$$

Dies eingesetzt in die Ungleichung $(*)$ ergibt:

$$0 \leq \big(-\langle x, y\rangle\big)^2 \cdot \langle x, x\rangle + 2\big(-\langle x, y\rangle \cdot \langle x, x\rangle\big) \cdot \langle x, y\rangle + \big(\langle x, x\rangle\big)^2 \cdot \langle y, y\rangle.$$

Wegen der positiven Definitheit von $\langle\,\cdot,\cdot\,\rangle$ und $x \neq 0$ gilt $\langle x, x\rangle > 0$, so daß die obige Ungleichung durch $\langle x, x\rangle$ geteilt werden darf, und es folgt:

$$\begin{aligned} 0 \leq \langle x, y\rangle^2 - 2\langle x, y\rangle^2 + \langle x, x\rangle \cdot \langle y, y\rangle &= -\langle x, y\rangle^2 + \langle x, x\rangle \cdot \langle y, y\rangle \\ \Longrightarrow \quad \langle x, y\rangle^2 &\leq \langle x, x\rangle \cdot \langle y, y\rangle. \end{aligned}$$

Da alle Terme obiger Ungleichung größer gleich Null sind, darf auf die Ungleichung die (streng monotone) Wurzelfunktion angewendet werden, und es folgt daraus die Ungleichung:

$$\sqrt{\langle x,y\rangle^2} \leq \sqrt{\langle x,x\rangle \cdot \langle y,y\rangle}.$$

Wegen der positiven Definitheit des Skalarproduktes sind die Faktoren unter der rechten Wurzel beide größer gleich Null, so daß der Wurzelausdruck auseinandergezogen werden kann, und mit Eigenschaft $\sqrt{\alpha^2} = |\alpha|$ für alle $\alpha \in \mathbb{R}$ folgt letztendlich die behauptete Formel:

$$|\langle x,y\rangle| \leq \sqrt{\langle x,x\rangle} \cdot \sqrt{\langle y,y\rangle}. \qquad \square$$

Nun kann mit Hilfe des Skalarproduktes eine Norm definiert werden:

Satz 4.1.12. *Sei $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ ein euklidischer Vektorraum. Dann induziert das Skalarprodukt $\langle\,\cdot,\cdot\,\rangle$ eine Norm (und damit auch eine Metrik, siehe Lemma 4.1.6) auf V durch:*

$$\|\cdot\|_{\langle\,\cdot,\cdot\,\rangle} \colon V \longrightarrow \mathbb{R}_0^+ \quad \textit{mit} \quad x \mapsto \sqrt{\langle x,x\rangle}.$$

Beweis.
Es sind für $\|\cdot\|_{\langle\,\cdot,\cdot\,\rangle}$ die drei Eigenschaften einer Norm aus Definition 4.1.3 nachzuprüfen:

Definitheit: Es gilt für $x \in V$:

$$\|x\|_{\langle\,\cdot,\cdot\,\rangle} = 0 \quad \overset{\text{(Def)}}{\Longleftrightarrow} \quad \sqrt{\langle x,x\rangle} = 0 \quad \Longleftrightarrow \quad \langle x,x\rangle = 0 \quad \overset{(4.1.9)}{\Longleftrightarrow} \quad x = 0.$$

Homogenität:

$$\|\alpha x\|_{\langle\,\cdot,\cdot\,\rangle} \overset{\text{(Def)}}{=} \sqrt{\langle \alpha x, \alpha x\rangle} = \sqrt{\alpha^2 \cdot \langle x,x\rangle} = |\alpha| \cdot \sqrt{\langle x,x\rangle} \overset{\text{(Def)}}{=} |\alpha| \cdot \|x\|_{\langle\,\cdot,\cdot\,\rangle}.$$

Dreiecksungleichung: Nach Bemerkung 4.1.9 sind die Terme $\langle x,x\rangle$, $\langle y,y\rangle$ größer gleich Null, und es gilt:

$$\langle x,x\rangle = \big(\sqrt{\langle x,x\rangle}\big)^2 \quad \text{und} \quad \langle y,y\rangle = \big(\sqrt{\langle y,y\rangle}\big)^2. \tag{$\star$}$$

Damit und mit der Cauchy-Schwarzschen Ungleichung 4.1.11 läßt sich dann zeigen:

$$\begin{aligned}
\big(\|x+y\|_{\langle\,\cdot,\cdot\,\rangle}\big)^2 &\overset{\text{(Def)}}{=} \langle x+y, x+y\rangle \\
&= \langle x,x\rangle + 2\underbrace{\langle x,y\rangle}_{\leq|\langle x,y\rangle|} + \langle y,y\rangle \\
&\leq \langle x,x\rangle + 2|\langle x,y\rangle| + \langle y,y\rangle \\
&\overset{4.1.11}{\leq} \langle x,x\rangle + 2 \cdot \sqrt{\langle x,x\rangle} \cdot \sqrt{\langle y,y\rangle} + \langle y,y\rangle \\
&\overset{(\star)}{=} \Big(\sqrt{\langle x,x\rangle} + \sqrt{\langle y,y\rangle}\Big)^2 \\
&\overset{\text{(Def)}}{=} \big(\|x\|_{\langle\,\cdot,\cdot\,\rangle} + \|y\|_{\langle\,\cdot,\cdot\,\rangle}\big)^2,
\end{aligned}$$

also zusammengefaßt:

$$\big(\|x+y\|_{\langle\,\cdot,\cdot\,\rangle}\big)^2 \quad \leq \big(\|x\|_{\langle\,\cdot,\cdot\,\rangle} + \|y\|_{\langle\,\cdot,\cdot\,\rangle}\big)^2.$$

Nun kann die Wurzelfunktion auf die Ungleichung angewendet werden, da die quadrierten Zahlen $\|x+y\|_{\langle\cdot,\cdot\rangle}$ und $\|x\|_{\langle\cdot,\cdot\rangle} + \|y\|_{\langle\cdot,\cdot\rangle}$ beide größer gleich Null sind, und es ergibt sich die gesuchte Abschätzung:

$$\|x+y\|_{\langle\cdot,\cdot\rangle} \leq \|x\|_{\langle\cdot,\cdot\rangle} + \|y\|_{\langle\cdot,\cdot\rangle}. \qquad \square$$

Bemerkung 4.1.13. *Nun läßt sich die Cauchy-Schwarzsche Ungleichung in einen euklidischen Vektorraum $\big(V, \langle\cdot,\cdot\rangle\big)$ für $x, y \in V$ auch folgendermaßen formulieren:*

$$|\langle x, y\rangle| \leq \|x\|_{\langle\cdot,\cdot\rangle} \cdot \|y\|_{\langle\cdot,\cdot\rangle}. \qquad \square$$

Damit sind nun in einem euklidischen Vektorraum $\big(V, \langle\cdot,\cdot\rangle\big)$ über das Skalarprodukt $\langle\cdot,\cdot\rangle$ eine induzierte Norm, und damit eine induzierte Metrik definiert:

$$\underbrace{\langle\cdot,\cdot\rangle}_{\text{Skalarprodukt}} \overset{4.1.12}{\rightsquigarrow} \underbrace{\|\cdot\|_{\langle\cdot,\cdot\rangle}}_{\text{Norm}} \overset{4.1.6}{\rightsquigarrow} \underbrace{d_{\|\cdot\|_{\langle\cdot,\cdot\rangle}}}_{\text{Metrik}}$$

$$\text{mit} \qquad d_{\|\cdot\|_{\langle\cdot,\cdot\rangle}}(x,y) := \|x-y\|_{\langle\cdot,\cdot\rangle} := \sqrt{\langle x-y, x-y\rangle}.$$

Dabei wird in Zukunft die Notation verkürzt, da der Kontext meist klar ist:

Definition 4.1.14. *Sei $\big(V, \langle\cdot,\cdot\rangle\big)$ ein euklidischer Vektorraum. Im folgenden wird, wenn nicht explizit anders vermerkt, als Norm in V immer die vom Skalarprodukt induzierte Norm verwendet (Satz 4.1.12) und kurz notiert mit:*

$$\|x\| := \sqrt{\langle x, x\rangle}.$$

Als Metrik wird, wenn nicht explizit anders vermerkt, immer die von dieser Norm induzierte Metrik verwendet und kurz notiert mit:

$$d(x,y) := \sqrt{\langle x-y, x-y\rangle}. \qquad \square$$

Bemerkung 4.1.15. *Sei $\big(V, \langle\cdot,\cdot\rangle\big)$ ein euklidischer Vektorraum. Dann liefern die vorhergehenden Betrachtungen:*

$$\begin{aligned} & V \text{ euklidischer Vektorraum} & & \\ \Longrightarrow\ & V \text{ normierter Vektorraum} & \rightsquigarrow\ & \text{Längenbegriff} \\ \Longrightarrow\ & V \text{ metrischer Raum} & \rightsquigarrow\ & \text{Abstandsbegriff.} \end{aligned}$$

Insbesondere existieren in einem metrischen Raum die wesentlichen Begriffe (siehe Bemerkung 4.1.2):

$$\text{konvergente Folgen} \quad \text{und} \quad \text{stetige Abbildungen.} \qquad \square$$

Beispiel 4.1.16.

i.) Es sei der $\mathbb{R}^2$ mit dem Standard-Skalarprodukt betrachtet:

$$\langle (x_1, x_2),\ (y_1, y_2)\rangle := x_1 y_1 + x_2 y_2.$$

Dann gilt für die Standard-Basisvektoren bzgl. der induzierten Norm und Metrik:

$$\|(1,0)\| = \sqrt{\langle (1,0),(1,0)\rangle} = \sqrt{1^2+0^2} = 1.$$

$$\|(0,1)\| = \sqrt{\langle (0,1),(0,1)\rangle} = \sqrt{0^2+1^2} = 1.$$

$$d\big((1,0),\ (0,1)\big) = \|(1,0)-(0,1)\| = \|(1,-1)\| = \sqrt{1^2+(-1)^2} = \sqrt{2}.$$

ii.) Es sei der $\mathbb{R}^2$ mit dem folgendem Skalarprodukt betrachtet (siehe auch Beispiel 4.1.10):

$$\langle (x_1, x_2),\ (y_1, y_2)\rangle := 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + 5x_2y_2.$$

Dann gilt für die Standard-Basisvektoren bzgl. der induzierten Norm und Metrik:

$$\begin{aligned}
\|(1,0)\| &= \sqrt{\langle (1,0),(1,0)\rangle} = \sqrt{2\cdot 1\cdot 1 + 3\cdot 1\cdot 0 + 3\cdot 0\cdot 1 + 5\cdot 0\cdot 0} = \sqrt{2}.\\
\|(0,1)\| &= \sqrt{\langle (0,1),(0,1)\rangle} = \sqrt{2\cdot 0\cdot 0 + 3\cdot 0\cdot 1 + 3\cdot 1\cdot 0 + 5\cdot 1\cdot 1} = \sqrt{5}.\\
d\big((1,0),\ (0,1)\big) &= \|(1,0)-(0,1)\| = \|(1,-1)\| = \sqrt{\langle (1,-1),(1,-1)\rangle}\\
&= \sqrt{2\cdot 1\cdot 1 + 3\cdot 1\cdot (-1) + 3\cdot (-1)\cdot 1 + 5\cdot (-1)\cdot (-1)} = \sqrt{1} = 1.
\end{aligned}$$

iii.) Es der der Raum der stetigen reellen Funktionen $\mathcal{C}^0(\mathbb{R})$ mit dem folgenden Skalarprodukt betrachtet (siehe auch Beispiel 4.1.10):

$$\langle f, g\rangle := \int_0^\pi f(x)\cdot g(x)\ dx.$$

Dann gilt für die Länge des Vektors $\sin(x) \in \mathcal{C}^0(\mathbb{R})$:

$$\begin{aligned}
\|\sin(x)\| &= \sqrt{\langle \sin(x), \sin(x)\rangle}\\
&= \sqrt{\int_0^\pi \sin^2(x)\ dx}\\
&= \sqrt{\Big[\frac{x}{2} - \frac{\sin(2x)}{4}\Big]_0^\pi}\\
&= \sqrt{\Big(\frac{\pi}{2} - \frac{\sin(2\pi)}{4}\Big) - \Big(\frac{0}{2} - \frac{\sin(2\cdot 0)}{4}\Big)}\\
&= \sqrt{\frac{\pi}{2}}.
\end{aligned}$$

□

Häufig wird der Spalten-Raum $\mathbb{R}^{[n]}$ oder der Zeilen-Raum $\mathbb{R}^n$ zusammen mit dem Standard-Skalarprodukt und der davon induzierten Norm betrachtet, und so sei definiert:

Definition 4.1.17. *Auf dem Spalten-Raum $\mathbb{R}^{[n]}$ bzw. dem Zeilen-Raum $\mathbb{R}^n$ sei mit $\langle\,\cdot,\cdot\,\rangle_2$ jeweils das Standard-Skalarprodukt bezeichnet (siehe auch Beispiel 4.1.10):*

$$\langle \begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}, \begin{pmatrix} y_1\\ \vdots\\ y_n\end{pmatrix}\rangle_2 := \sum_{i=1}^n x_i\cdot y_i. \quad \text{bzw.} \quad \big\langle (x_1,\dots,x_n),\ (y_1,\dots,y_n)\big\rangle_2 := \sum_{i=1}^n x_i\cdot y_i.$$

Die vom Standard-Skalarprodukt $\langle\,\cdot,\cdot\,\rangle_2$ induzierte Norm in den jeweiligen Räumen heißt euklidische Norm und wird auch mit dem Index „Zwei“ gekennzeichnet:

$$\|x\|_2 := \sqrt{\langle x, x\rangle_2} \quad \text{für } x \in \mathbb{R}^{[n]} \text{ bzw. } x \in \mathbb{R}^n.$$

Die n-te Einheitskugel in $\mathbb{R}^{[n]}$ bzw. $\mathbb{R}^n$ ist die Menge:

$$D^n := \{\, x \mid \|x\|_2 \le 1 \,\} \quad \text{für } x \in \mathbb{R}^{[n]} \text{ bzw. } x \in \mathbb{R}^n,$$

und die $(n-1)$-te Einheitsphäre im jeweiligen Raum die Menge:

$$S^{n-1} := \{\, x \mid \|x\|_2 = 1 \,\} \quad \text{für } x \in \mathbb{R}^{[n]} \text{ bzw. } x \in \mathbb{R}^n. \qquad \square$$

Bemerkung 4.1.18.

i.) *Bei der euklidischen Norm ist die Notation des Index „Zwei“ in $\|x\|_2$ üblich, da es im $\mathbb{R}^{[n]}$ bzw. $\mathbb{R}^n$ für jedes $p \in \mathbb{N}$ die sogenannte p-Norm:*

$$\|x\|_p := \sqrt[p]{\textstyle\sum_{i=1}^n |x_i|^p}$$

gibt, und die euklidische Norm dann die spezielle 2-Norm ist. Beim Standard-Skalarprodukt ist die Index-Notation unüblich, da es nicht analog p-Skalarprodukte gibt. Meist werden nur die Klammern „$\langle \cdot, \cdot \rangle$“ geschrieben, die in diesem Skript aber allgemein für Skalarprodukte verwendet werden. Der Begriff „Standard-Skalarprodukt“ ist zwar eindeutig und macht die Situation klar, trotzdem wird im folgenden für dieses die Notation $\langle \cdot, \cdot \rangle_2$ verwendet, um noch einmal explizit darauf hinzuweisen, daß ein spezielles Skalarprodukt verwendet wird.

ii.) *Die n-te Einheitsphäre ist eine Teilmenge des $\mathbb{R}^{[n+1]}$ bzw. $\mathbb{R}^{n+1}$, die n-te Einheitskugel liegt im $\mathbb{R}^{[n]}$ bzw. $\mathbb{R}^n$.*

iii.) *Im Spalten-Raum $\mathbb{R}^{[n]}$ wird für die beiden Spaltenvektoren $x, y \in \mathbb{R}^{[n]}$ das Standard-Skalarprodukt auch geschrieben als:*

$$\langle x, y \rangle_2 = x^t \cdot y,$$

wobei beide Vektoren kanonisch als Matrizen aufgefaßt werden.

iv.) *Im Zeilen-Raum $\mathbb{R}^n$ kann mit vorheriger Interpretation von Vektoren $x, y \in \mathbb{R}^n$ als Matrizen das Standard-Skalarprodukt auch geschrieben werden als:*

$$\langle x, y \rangle_2 = x \cdot y^t,$$

wobei diese Notation unüblich ist. Meist werden dann die Vektoren $x, y \in \mathbb{R}^n$ als Spaltenvektoren notiert, um zu obiger Schreibweise $x^t \cdot y$ zu kommen. $\square$

Orthogonalität.

Als nächstes wird in euklidischen Räumen „Orthogonalität“ defininiert, d.h. wann zwei Vektoren „senkrecht aufeinander stehen“, was anschaulich im $\mathbb{R}^2$ bedeutet, daß ein Winkel von 90° oder 270° zwischen ihnen besteht. Nun wird Orthogonalität mit Hilfe des Skalarproduktes definiert, denn Winkel sind bisher gar nicht bekannt.
Zwar werden anschließend auch allgemein Winkel zwischen Vektoren definiert, so daß die Vorgenhensweise, erst über „senkrecht stehen“ und dann über Winkel zu reden, unsinnig erscheint. Der Grund für die Vorgenhensweise liegt darin, daß das Konzept von Orthogonalität auch im allgemeineren Kontext als in euklidischen Vektorräumen definiert werden kann - Winkel jedoch nicht.

Definition 4.1.19. *Sei $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ ein euklidischer Vektorraum. Zwei Vektoren x, y aus V heißen orthogonal oder senkrecht zueinander, falls gilt:*

$$\langle x, y\rangle = 0.$$

Sind x, y orthogonal, so wird dies auch notiert mit $x \perp y$.
Ist $(v_i)_{i\in I}$ ein System von Vektoren, so heißt dies orthogonal (oder auch Orthogonalsystem), wenn alle Vektoren des Systems paarweise orthogonal zueinander sind:

$$v_i \perp v_j \text{ für alle } i, j \in I \text{ mit } i \neq j.$$

Ein orthogonales System $(v_i)_{i\in I}$ heißt orthonormal (oder auch Orthonormalsystem), wenn alle Vektoren darin normiert sind, d.h. es gilt $\|v_i\| = 1$ für alle $i \in I$.
Eine Basis $(v_i)_{i\in I}$ von V heißt Orthogonalbasis, falls sie auch ein Orthogonalsystem ist, und Orthonormalbasis, falls sie auch ein Orthonormalsystem ist. □

Bemerkung 4.1.20.

i.) Für einen Vektor $v \neq 0$ eines euklidischen Vektorraumes gilt offensichtlich:

$$\frac{v}{\|v\|} := \tfrac{1}{\|v\|} \cdot v \text{ hat die Länge Eins,}$$

denn es folgt sofort aus der Definitheit und Homogenität der Norm:

$$\big\|\tfrac{1}{\|v\|} \cdot v\big\| \overset{(Homog.)}{=} \big|\underbrace{\tfrac{1}{\|v\|}}_{>0}\big| \cdot \|v\| = \tfrac{1}{\|v\|} \cdot \|v\| = 1.$$

ii.) Für einen Vektor v eines euklidischen Vektorraumes gilt offensichtlich:

$$v \text{ normiert} \overset{\text{Def 4.1.19}}{\iff} \|v\| = 1 \overset{\text{Def 4.1.14}}{\iff} \sqrt{\langle v, v\rangle} = 1 \iff \langle v, v\rangle = 1.$$

iii.) Ist $(v_i)_{i\in I}$ eine Basis eines euklidischen Vektorraumes, so folgt aus vorheriger Aussage sofort:

$$(v_i)_{i\in I} \text{ ist eine Orthonormalbasis} \iff \langle v_i, v_j\rangle = \delta_{i,j} := \begin{cases} 0 & \text{für } i \neq j, \\ 1 & \text{für } i = j. \end{cases}$$

iv.) Ist $(v_i)_{i\in I}$ eine Orthonormalbasis eines euklidischen Vektorraumes, so gilt für das Skalarprodukt zweier Basisvektoren:

$$\langle v_i, v_j\rangle = \delta_{i,j}.$$

Insbesondere liefert dies für eine Linearkombination $\sum_{i\in I} \alpha_i v_i$ dann:

$$\langle v_k, \sum_{i\in I} \alpha_i v_i\rangle = \sum_{i\in I} \alpha_i \underbrace{\langle v_k, v_i\rangle}_{=\delta_{i,j}} = \alpha_k. \qquad (*)$$

Jeder Vektor x des Raumes läßt sich als Linearkombination der Orthonormalbasis $(v_i)_{i\in I}$ schreiben, und mit der Gleichung $(*)$ folgt dann sofort:

$$x = \sum_{i\in I} \langle v_i, x\rangle \cdot v_i.$$

Insbesondere bei einer endlichen Orthonormalbasis $v_1, \ldots, v_n$ kann damit die Linearkombination $x = \sum_{i=1}^n \alpha_i v_i$ von gegebenen x aus „zurückgerechnet“ werden, indem alle n Koeffizienten $\alpha_1, \ldots, \alpha_n$ über die Skalarprodukte $\langle v_i, x\rangle$ bestimmt werden.

Normalerweise ist es nicht klar, wie die Koeffizienten eines Vektors bzgl. einer gegebenen Basis berechnet werden können. □

Beispiel 4.1.21.

i.) Im $\mathbb{R}^n$ ist die Standard-Basis $e_1, \ldots, e_n$ bzgl. des Standard-Skalarproduktes (siehe 4.1.10) eine Orthonormalbasis, denn es gilt:

$$\langle e_i, e_j \rangle = \big\langle (\delta_{i,k})_{1\le k\le n}, (\delta_{j,k})_{1\le k\le n} \big\rangle = \sum_{i=k}^{n} \delta_{i,k} \cdot \delta_{j,k} = \delta_{i,j}.$$

Die Aussage gilt analog für die Standard-Basis $e_1, \ldots, e_n$ und das Standard-Skalarprodukt im $\mathbb{R}^{[n]}$.

ii.) Der Polynomvektorraum $\mathbb{R}[t]_{|2}$ ist zusammen mit dem Skalarprodukt (siehe auch Beispiel 4.1.10):

$$(p, q) \mapsto \int_{-1}^{1} p(t) \cdot q(t)\, dt$$

ein euklidischer Vektorraum. Die folgenden drei Polynome sind offensichtlich eine Basis (Übung!):

$$L_0(t) := 1, \quad L_1(t) := t \quad \text{und} \quad L_2(t) := \tfrac{1}{2}(3t^2 - 1).$$

Diese Vektoren sind gleichzeitig ein Orthogonalsystem, also eine Orthogonalbasis, denn es gilt (Übung!):

$$\langle L_i(t), L_j(t) \rangle = 0 \text{ für } i \neq j.$$

Ein Beispiel sei vorgeführt:

$$\langle L_1(t), L_2(t) \rangle = \int_{-1}^{1} t \cdot \tfrac{1}{2}(3t^2 - 1)\, dt = \tfrac{1}{2} \cdot \int_{-1}^{1} 3t^3 - t\, dt = \tfrac{1}{2} \cdot \left[\tfrac{3}{4}t^4 - \tfrac{1}{2}t^2\right]_{-1}^{1} = \tfrac{1}{2} \cdot 0 = 0.$$

Die Polynome $L_i(t)$ heißen Legendre-Polynome und sie folgen einem allgemeinen Bildungsgesetz, welches für jeden Grad n ein Polynom $L_n(t)$ zu erzeugen, so daß $L_0(t), \ldots, L_n(t)$ eine Orthogonalbasis von $\mathbb{R}[t]_{|n}$ sind. □

Bemerkung 4.1.20 zeigt die Nützlichkeit von Orthonormalbasen - die Frage ist, ob solche in jedem euklidischen Vektorraum existieren. Es wird nun gezeigt, wie im Falle eines endlich-dimensionalen euklidischen Vektorraumes aus einer gegebenen (beliebigen) Basis eine Orthonormalbasis konstruiert werden kann (durch das Gram-Schmidtsche Orthogonalisierungsverfahren 4.1.23); vorher muß noch folgende Hilfsaussage gezeigt werden:

Lemma 4.1.22. *Sei $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ ein euklidischer Vektorraum und $(v_i)_{i\in I}$ ein orthogonales System mit $v_i \neq 0$ für alle $i \in I$. Dann ist das System $(v_i)_{i\in I}$ linear unabhängig.*

Beweis.
Es ist zu zeigen, daß gilt:

$$\sum_{i\in I} \alpha_i v_i = 0 \quad \Longrightarrow \quad \alpha_i = 0 \text{ für alle } i \in I.$$

Für den Koeffizienten α_k folgt mit obiger Linearkombination, da das Skalarprodukt $\langle\,\cdot,\cdot\,\rangle$ bilinear ist und nach Voraussetzung $\langle v_k, v_i\rangle = 0$ für $k \neq i$ gilt:

$$0 = \langle v_k, 0\rangle = \langle v_k, \sum_{i\in I} \alpha_i v_i\rangle = \sum_{i\in I} \alpha_i \cdot \underbrace{\langle v_k, v_i\rangle}_{=\,0 \text{ für } i\neq k} = \alpha_k \cdot \langle v_k, v_k\rangle.$$

Wegen der Voraussetzung $v_k \neq 0$ ist wegen der positiven Definitheit von $\langle\,\cdot,\cdot\,\rangle$ dann $\langle v_k, v_k\rangle \neq 0$, und es folgt $\alpha_k = 0$. Damit müssen alle Koeffizienten Null sein und das System damit linear unabhängig. □

Nun kann gezeigt werden, wie in einem endlich-dimensionalen euklidischen Vektorraum aus einer gegebenen Basis eine Orthogonal- und Orthonormalbasis konstruiert werden kann. Damit ist dann implizit auch ein Existenzbeweis von Orhogonalbasen im endlich-dimensionalen Fall gegeben:

Satz 4.1.23. *(Gram-Schmidtsches Orthogonalisierungsverfahren)*
Sei $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ ein endlich-dimensionaler euklidischer Vektorraum und $v_1, \ldots, v_n$ eine Basis von V. Es seien definiert:

$$w_1 := v_1 \qquad \text{und} \qquad w_i := v_i - \sum_{j=1}^{i-1} \frac{\langle w_j, v_i\rangle}{\langle w_j, w_j\rangle} \cdot w_j \quad \text{für } 2 \leq i \leq n.$$

Dann liegt w_i im von $v_1, \ldots, v_i$ erzeugten Unterraum und es gilt $w_i \neq 0$, und damit insbesondere $\langle w_i, w_i\rangle \neq 0$ für alle $1 \leq i \leq n$, so daß obige Formel wohldefiniert ist. Außerdem erfüllen die konstruierten Vektoren w_i die Bedingung:

$$w_1, \ldots, w_n \text{ ist eine Orthogonalbasis von } V.$$

Der oben beschriebenen Algorithmus, aus der gegebenen Basis eine Orthogonalbasis zu konstruieren, heißt Gram-Schmidtsches Orthogonalisierungsverfahren.

Sind $v_1, \ldots, v_k$ schon ein orthogonales System, so gilt $w_i = v_i$ für $1 \leq i \leq k$, d.h. der Algorithmus verändert dann die ersten k Vektoren nicht.

Weiter gilt:

$$q_i := \frac{w_i}{\|w_i\|} \qquad \Longrightarrow \qquad q_1, \ldots, q_n \text{ ist eine Orthonormalbasis von } V.$$

Beweis. Es seien für $1 \leq j < i \leq n$ folgende Abkürzungen definiert:

$$s_{j,i} := \frac{\langle w_i, v_j\rangle}{\langle w_i, w_i\rangle} \qquad \Longrightarrow \qquad w_i = v_i - \sum_{j=1}^{i-1} s_{j,i} \cdot w_j.$$

Da $v_1, \ldots, v_n$ eine Basis ist, gilt vor allem $v_i \neq 0$ für alle $1 \leq i \leq n$ (sonst wäre das System nicht linear unabhängig), und es gibt keine nicht-trivialen Linearkombinationen der Null mit Vektoren aus dieser Basis.
Es wird nun per Induktion bewiesen, daß w_i im Erzeugnis von $v_1, \ldots, v_i$ liegt und $w_i \neq 0$ gilt:

Induktionsanfang $i = 1$: Es ist per Definition $w_1 = v_1$, und wegen $v_1 \neq 0$ folgt die Behauptung für $i = 1$.

Induktionsschritt $(i-1) \rightsquigarrow i$: Nach der Induktionsannahme sind dann die konstruierten Vektoren $w_1, \ldots, w_{i-1}$ eine Linearkombination von $v_1, \ldots, v_{i-1}$, und es folgt sofort aus der Definition von w_i:

$$w_i = v_i - \sum_{j=1}^{i-1} s_{j,i} \cdot \underbrace{w_j}_{\substack{\text{LK von} \\ v_1,\ldots,v_j}} = v_i - \big(\text{Linearkombination von } v_1, \ldots, v_{i-1}\big).$$

Also ist w_i eine Linearkombination von $v_1, \ldots, v_i$, und da diese Linearkombination nicht-trivial ist (der Koeffizient von v_i ist Eins), kann w_i nicht der Nullvektor sein.

Es wird nun per Induktion über $2 \leq i \leq n$ gezeigt, daß die konstruierten Vektoren $w_1, \ldots, w_i$ paarweise orthogonal zueinander sind (für $i = 1$ ist nichts zu zeigen):

Induktionsanfang $i = 2$: w_2 ist orthogonal zu w_1, denn es gilt:

$$\begin{aligned}
\langle w_1, w_2 \rangle &= \langle w_1, v_2 - s_{1,2} \cdot w_1 \rangle \\
&= \langle w_1, v_2 \rangle - s_{1,2} \cdot \langle w_1, w_1 \rangle \\
&= \langle w_1, v_2 \rangle - \frac{\langle w_1, v_2 \rangle}{\langle w_1, w_1 \rangle} \cdot \langle w_1, w_1 \rangle \\
&= 0.
\end{aligned}$$

Induktionsschritt: $(i-1) \rightsquigarrow i$: Nach der Induktionsannahme gilt $\langle w_k, w_j \rangle = 0$ für $1 \leq k \neq j \leq i-1$, und es bleibt zu zeigen, daß alle w_k mit $1 \leq k \leq i-1$ zu w_i orthogonal sind:

$$\begin{aligned}
\langle w_k, w_i \rangle &= \langle w_k, v_i - \sum_{j=1}^{i-1} s_{j,i} \cdot w_j \rangle \\
&= \langle w_k, v_i \rangle - \sum_{j=1}^{i-1} s_{j,i} \cdot \underbrace{\langle w_k, w_j \rangle}_{= 0 \text{ für } k \neq j} \\
&= \langle w_k, v_i \rangle - s_{k,i} \cdot \langle w_k, w_k \rangle \\
&= \langle w_k, v_i \rangle - \frac{\langle w_k, v_i \rangle}{\langle w_k, w_k \rangle} \cdot \langle w_k, w_k \rangle \\
&= 0.
\end{aligned}$$

Also sind also alle w_i ungleich Null und paarweise orthogonal zueinander, so daß dann aus Lemma 4.1.22 ihre lineare Unabhängigkeit folgt. Wegen ihrer Anzahl sind sie sogar ein maximal linear unabhängiges System und damit eine Basis, also insgesamt wie behauptet eine Orthogonalbasis.

Nun wird per Induktion über $k \geq 2$ gezeigt, daß für orthogonale Startvektoren $v_1, \ldots, v_k$ der Algorithmus die Vektoren nicht ändert und $w_i = v_i$ für $1 \leq i \leq k$ gilt:

Induktionsanfang $k = 2$: Es gilt per Defintion $w_1 = v_1$, und für $\langle v_1, v_2 \rangle = 0$ folgt:

$$w_2 = v_2 - \frac{\overbrace{\langle w_1, v_2 \rangle}^{=\langle v_1, v_2 \rangle = 0}}{\langle w_1, w_1 \rangle} \cdot w_1 = v_2.$$

Induktionsschritt $(k-1) \rightsquigarrow k$: Ist $v_1, \ldots, v_k$ ein orthogonales System, so natürlich auch $v_1, \ldots, v_{k-1}$. Nach der Induktionsvoraussetzung gilt somit für $1 \leq j \leq k-1$ jeweils $w_j = v_j$. So folgt mit der Voraussetzung $\langle v_j, v_k \rangle = 0$ für $1 \leq j \leq k$ auch noch:

$$w_k = v_k - \sum_{j=1}^{k-1} \frac{\langle w_j, v_k \rangle}{\langle w_j, w_j \rangle} \cdot w_j = v_k - \sum_{j=1}^{k-1} \frac{\overbrace{\langle v_j, v_k \rangle}^{=0}}{\langle w_j, w_j \rangle} \cdot w_j = v_k.$$

Zu guter Letzt gilt nach Bemerkung 4.1.20:

$$\|q_i\| = \Big\| \frac{w_i}{\|w_i\|} \Big\| = 1,$$

also sind die Vektoren $q_1, \ldots, q_n$ alle normiert und auch orthogonal, d.h. eine Orthonormalbasis. □

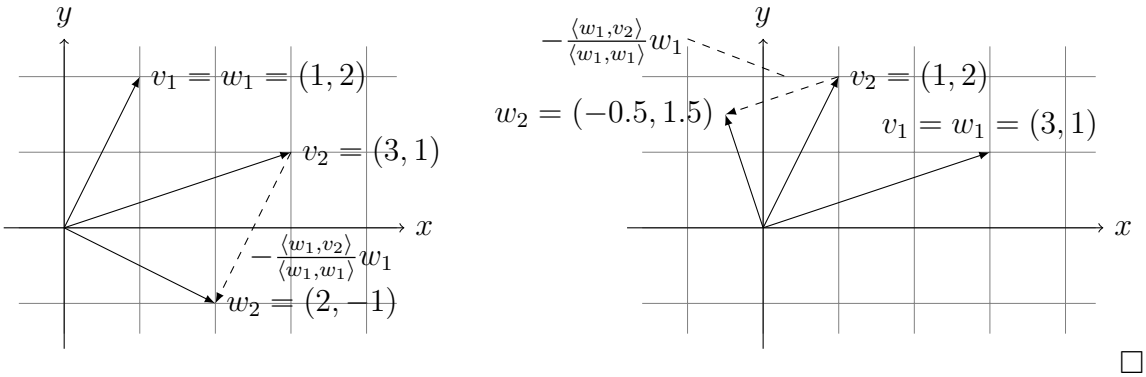
Bemerkung 4.1.24.

i.) Das Ergebnis des Gram-Schmidtschen Orthogonalisierungsverfahrens hängt bei einer gegebenen Basis von der Reihenfolge der Vektoren ab, wie folgendes Beispiel im $\mathbb{R}^2$ mit dem Standard-Skalarprodukt zeigt:

$$(1,2),(3,1) \quad \rightsquigarrow \quad (1,2),(3,1) - \tfrac{\langle (1,2),(3,1) \rangle_2}{\langle (1,2),(1,2) \rangle_2}(1,2) = (3,1) - \tfrac{5}{5}(1,2) \ = (2,-1).$$

$$(3,1),(1,2) \quad \rightsquigarrow \quad (3,1),(1,2) - \tfrac{\langle (3,1),(1,2) \rangle_2}{\langle (3,1),(3,1) \rangle_2}(3,1) = (1,2) - \tfrac{5}{10}(3,1) = (-0.5, 1.5).$$

ii.) Im Zweidimensionalen kann auch graphisch betrachtet werden, wie das Gram-Schmidtsche Verfahren die zwei gegebenen Vektoren v_1, v_2 zu Vektoren w_1, w_2 orthogonalisiert: der erste Vektor wird beibehalten, und der zweite Vektor wird parallel zum ersten auf dessen Senkrechte projeziert ($w_2 := v_2 - \frac{\langle w_1, v_2 \rangle}{\langle w_1, w_1 \rangle} w_1$):



□

Das Gram-Schmidtsche Orthogonalisierungsverfahren liefert sofort folgende Aussagen:

Satz 4.1.25.

i.) In einem endlich-dimensionalen euklidischen Vektorraum kann jedes Orthogonalsystem, das keinen Nullvektor enthält, zu einer Orthogonalbasis ergänzt werden.

ii.) Jeder endlich-dimensionale euklidische Vektorraum hat eine Orthogonalbasis.

iii.) In einem endlich-dimensionalen euklidischen Vektorraum kann jedes orthonormale System zu einer Orthonormalbasis ergänzt werden.

iv.) Jeder endlich-dimensionale euklidische Vektorraum hat eine Orthonormalbasis.

Beweis.

i.) Ist $v_1, \ldots, v_k$ ein orthogonales System ohne einen Nullvektor, so ist es nach Lemma 4.1.22 linear unabhängig, und kann nach dem Basisergänzungssatz 2.2.43 zu einer Basis von V ergänzt werden.
Mit dem Gram-Schmidtschen Ortogonalisierungsverfahren 4.1.23 kann aus dieser Basis eine Orthogonalbasis gewonnnen werden, wobei das Verfahren die schon paarweise senkrechten Vektoren $v_1, \ldots, v_k$ nicht verändert. Somit ist die konstruierte Basis dann sogar eine Basisergänzung des vorgegebenen orthogonalen Systems.

ii.) Jeder Vektorraum hat eine Basis, und mit dem Gram-Schmidtschen Orthogonalisierungsverfahren 4.1.23 kann daraus eine Orthogonalbasis konstruiert werden.

iii.) Ein orthonormales System $v_1, \ldots, v_k$ enthält keinen Nullvektor ($\|0\| \neq 1$), und somit ist es insbesondere ein orthogonales System ohne Nullvektor. Nach vorheriger Aussage kann dies zu einer Orthogonalbasis erweitert werden, und diese liefert nach Normierung eine Orthonormalbasis, die immer noch die ursprünglichen Vektoren $v_1, \ldots, v_k$ enthält, dieses System also erweitert.

iv.) Jeder Vektorraum hat nach vorheriger Aussage eine Orthogonalbasis, und diese liefert nach Normierung eine Orthonormalbasis. □

Bemerkung 4.1.26. *Die Aussagen aus Satz 4.1.25 können nicht auf unendliche euklidische Vektorräume übertragen werden!*

i.) Im euklidischen Vektorraum ℓ^2 aus Beispiel 4.1.10 ist folgendes unendliche System von Vektoren ein Orthonormalsystem:

$$S := (e_0, e_1, e_2, \ldots, e_i, \ldots)_{i \in \mathbb{N}_0} \quad \textit{mit} \quad e_i := (0, \ldots, 0, \underset{i}{1}, 0, \ldots),$$

also e_i die Folge, die nur an der i-ten Stelle eine Eins und sonst nur Nullen enthält.
Das Orthonormalsystem S ist kein Erzeugendensystem von ℓ^2, da die Folge:

$$\left(\tfrac{1}{n}\right)_{n \in \mathbb{N}_0} \in \ell^2$$

keine Linearkombination der Vektoren aus S sein kann. Es kann leicht gezeigt werden, daß für alle $v \in \ell^2$ gilt (Übung!):

$$v \perp e_i \textit{ für alle } i \in \mathbb{N}_0 \quad \Longrightarrow \quad v = 0.$$

Damit kann das Orthonormalsystem S nicht orthogonal und somit nicht orthonormal erweitert werden, und insbesondere also nicht zu einer Orthonormalbasis ergänzt werden.

ii.) Der Raum ℓ^2 besitzt überhaupt keine Orthonormalbasis. Ein Beweis davon kann in folgenden Schritten geführt werden:

- *Angenommen, $(v_i)_{i \in I}$ wäre eine Orthonormalbasis von ℓ^2. Dann kann mit Hilfe des maximalen Orthonormalsystems S gezeigt werden, daß I eine abzählbare Menge ist: jedes e_i ist eine Linearkombination von endliche vielen Basisvektoren v_j, und somit S (abzählbar) insgesamt von abzählbar vielen v_j. Nicht verwendete Basisvektoren wären orthogonal zu S, was dessen Maximalität widerspräche, so daß es nicht mehr Elemente in der Basis geben kann als die abzählbar vielen zur Erzeugung von S verwendeten.*

- *Angenommen, $(v_i)_{i\in I}$ wäre eine abzählbare Orthonormalbasis von ℓ^2. In einem euklidischen (normierten) Raum können konvergente Reihen erklärt werden, und folgende Reihe bzgl. der Orthonormalbasis $(v_i)_{i\in I}$ wäre dann konvergent:*
$$x := \sum_{i\in I} \tfrac{1}{i} v_i.$$
x hat dann mit v_i das Skalarprodukt $\frac{1}{i}$ (dazu muß die Stetigkeit des Skalarproduktes gezeigt werden), also mit allen Basisvektoren ein Skalarprodukt ungleich Null.
Da x aber auch durch endlich viele Basisvektoren der Orthonormalbasis $(v_i)_{i\in I}$ erzeugt werden kann, hat es mit allen nicht verwendeten Basisvektoren das Skalarprodukt Null, im Widerspruch zur Konstruktion von x.

Die obige Beweisskizze läßt sich zu folgen Aussagen verallgemeinern:

Satz 1: *Ein euklidischer Vektorraum kann höchstens eine endliche oder eine überabzählbare Orthonormalbasis besitzen.*

Satz 2: *Besitzt ein euklischer Vektorraum ein maximales abzählbares Orthonormalsystem, welches keine Basis ist, so besitzt er keine Orthonormalbasis.*

□

Beispiel 4.1.27. *Es folgen Beispiele, wie mit Hilfe des Gram-Schmidtschen Orthogonalisierungsverfahrens Basen in Orthogonal- und Orthonormalbasen transformiert werden können:*

i.) Ist $\big(V, \langle\cdot,\cdot\rangle\big)$ ein euklidischer Vektorraum mit einer Basis v_1, v_2, v_3, so liefert das Gram-Schmidtsche Verfahren 4.1.23 folgende Orthogonalbasis:
$$w_1 := v_1, \quad w_2 := v_2 - \frac{\langle w_1, v_2\rangle}{\langle w_1, w_1\rangle}\cdot w_1 \quad \textit{und} \quad w_3 := v_3 - \frac{\langle w_1, v_3\rangle}{\langle w_1, w_1\rangle}\cdot w_1 - \frac{\langle w_2, v_3\rangle}{\langle w_2, w_2\rangle}\cdot w_2.$$
Eine Orthonormalbasis ergibt sich dann durch normieren:
$$q_1 := \tfrac{1}{\|w_1\|}\cdot w_1, \quad q_2 := \tfrac{1}{\|w_2\|}\cdot w_2, \quad \textit{und} \quad q_3 := \tfrac{1}{\|w_3\|}\cdot w_3 \quad \textit{mit} \quad \|w_i\| := \sqrt{\langle w_i, w_i\rangle}.$$

ii.) Im $\mathbb{R}^3$ sei folgende Basis gegeben:
$$(1,1,0), \quad (0,1,1) \quad \textit{und} \quad (1,0,1).$$
Das Gram-Schmidtsche Orthogonalisierungsverfahren 4.1.23 transformiert diese dann bzgl. des Standard-Skalarproduktes in folgende Orthogonalbasis:
$$\begin{aligned}
w_1 &:= (1,1,0),\\
w_2 &:= (0,1,1) - \frac{\langle (1,1,0),(0,1,1)\rangle_2}{\langle (1,1,0),(1,1,0)\rangle_2}\cdot(1,1,0) = (0,1,1) - \tfrac{1}{2}\cdot(1,1,0) = (-\tfrac{1}{2},\tfrac{1}{2},1),\\
w_3 &:= (1,0,1) - \frac{\langle (1,1,0),(1,0,1)\rangle_2}{\langle (1,1,0),(1,1,0)\rangle_2}\cdot(1,1,0) - \frac{\langle (-\frac{1}{2},\frac{1}{2},1),(1,0,1)\rangle_2}{\langle (-\frac{1}{2},\frac{1}{2},1),(-\frac{1}{2},\frac{1}{2},1)\rangle_2}\cdot(-\tfrac{1}{2},\tfrac{1}{2},1)\\
&= (1,0,1) - \tfrac{1}{2}\cdot(1,1,0) - \tfrac{\frac{1}{2}}{\frac{3}{2}}\cdot(-\tfrac{1}{2},\tfrac{1}{2},1)\\
&= (1,0,1) - (\tfrac{1}{2},\tfrac{1}{2},0) - (-\tfrac{1}{6},\tfrac{1}{6},\tfrac{1}{3})\\
&= (\tfrac{2}{3},-\tfrac{2}{3},\tfrac{2}{3}).
\end{aligned}$$

iii.) Es sei im $\mathbb{R}^2$ das folgende Skalarprodukt gegeben (siehe Beispiel 4.1.10):

$$\langle (x_1, x_2), (y_1, y_2) \rangle := 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + 5x_2y_2.$$

Dann liefert das Gram-Schmidtsche Orthogonalisierungsverfahren für die Basis $(1,0), (0,1)$ des $\mathbb{R}^2$ folgende Orthogonalbasis:

$$w_1 := (1,0),$$
$$w_2 := (0,1) - \frac{\langle (1,0),(0,1) \rangle}{\langle (1,0),(1,0) \rangle} \cdot (1,0) = (0,1) - \tfrac{3}{2} \cdot (1,0) = (-\tfrac{3}{2}, 1).$$

Die Vektoren w_1, w_2 haben die Längen:

$$\|w_1\| := \sqrt{\langle (1,0),(1,0) \rangle} = \sqrt{2} \quad \textit{und} \quad \|w_2\| := \sqrt{\langle (-\tfrac{3}{2},1),(-\tfrac{3}{2},1) \rangle} = \sqrt{\tfrac{1}{2}} = \tfrac{1}{\sqrt{2}}.$$

Die liefert dann folgende aus der Standard-Basis konstruierte Orthonormalbasis:

$$q_1 := \frac{1}{\|w_1\|} \cdot w_1 = \tfrac{1}{\sqrt{2}} \cdot (1,0) \quad \textit{und} \quad q_2 := \frac{1}{\|w_2\|} \cdot w_2 = \sqrt{2} \cdot (-\tfrac{3}{2}, 1) = (-\tfrac{3}{\sqrt{2}}, \sqrt{2}). \quad \square$$

Aus dem Gram-Schmidtschen Orthogonalisierungsverfahren läßt sich für invertierbare Matrizen $A \in \mathrm{GL}_n(\mathbb{R})$, deren Spalen ja eine Basis des $\mathbb{R}^{[n]}$ sind, eine sogenannte QR-Zerlegung herleiten, die für numerische Verfahren wichtig ist:

Satz 4.1.28. *(QR-Zerlegung)*
Sei $A \in \mathrm{GL}_n(\mathbb{R})$. Dann gibt es Matrizen $Q, R \in \mathrm{GL}_n(\mathbb{R})$, so daß gilt:

i.) $A = QR$.
ii.) Die Spalten von Q sind eine Orthonormalbasis des $\mathbb{R}^{[n]}$ bzgl. des Standard-Skalarproduktes $\langle \cdot, \cdot \rangle_2$.
iii.) R ist eine obere Dreiecksmatrix.

Beweis.
Da A eine invertierbare Matrix ist, sind die Spalten von A eine Basis des $\mathbb{R}^{[n]}$. Seien $v_1, \ldots, v_n \in \mathbb{R}^{[n]}$ die Spalten von A. Dann kann auf die Basis $v_1, \ldots, v_n$ das Gram-Schmidtsche Orthogonalisierungsverfahren angewendet werden, und dies liefert eine Orthogonalbasis $w_1, \ldots, w_n$, wobei gilt:

$$w_i = v_i - \sum_{j=1}^{i-1} s_{j,i} \cdot w_j \quad \text{mit} \quad s_{j,i} := \frac{\langle w_j, v_i \rangle_2}{\langle w_j, w_j \rangle_2}.$$

Diese Gleichung kann umgestellt werden zu:

$$v_i = w_i + \sum_{j=1}^{i-1} s_{j,i} \cdot w_j, \tag{$*$}$$

so daß die Spalten der Matrix A eine Linearkombination der konstruierten Orthogonalbasis $w_1, \ldots, w_n$ sind. Dies liefert sofort eine Darstellung:

$$A = OS,$$

wenn in der Matrix O spaltenweise die Orthogonalbasis $w_1, \ldots, w_n$ eingetragen wird und in der i-ten Spalte von S die Koeffizienten der Linearkombinationsdarstellung

von v_i in $(*)$:

$$O := \begin{pmatrix} | & & | \\ w_1 & \cdots & w_n \\ | & & | \end{pmatrix} \qquad \text{und} \qquad S := \begin{pmatrix} 1 & s_{1,2} & s_{1,3} & & & s_{1,n} \\ 0 & 1 & s_{2,3} & & & s_{2,n} \\ 0 & 0 & 1 & & & s_{3,n} \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & & & 1 & s_{n-1,n} \\ 0 & 0 & & & & 1 \end{pmatrix}.$$

Nach Lemma 3.1.6 ist O mal die i-te Spalte von S eine Linearkombination der Spalten von O mit den Koeffizienten aus der i-ten Spalte von S, und dies liefert nach $(*)$ dann die i-te Spalten von A.
Es sei nun D die Diagonalmatrix mit den Diagonaleinträgen $\|w_1\|_2, \ldots, \|w_n\|_2$. Da $w_1, \ldots, w_n$ alle ungleich Null sind (Verfahren von Gram-Schmidt), gilt auch $\|w_i\|_2 \neq 0$ für alle $1 \leq i \leq n$, und die Diagonalmatrix D ist inverterierbar wegen:

$$\det(D) = \prod_{i=1}^{n} \|w_i\|_2 \neq 0.$$

Dann gilt offensichtlich:

$$A = OS = O(D^{-1}D)S = \underbrace{(OD^{-1})}_{=:Q}\underbrace{DS}_{=:R}.$$

Die Multiplikation der Matrix S mit der Diagonalmatrix D von links multipliziert alle Zeilen von S mit den entsprechenden Diagonaleinträgen von D (dies folgt mit $D = \prod_{i=1}^{n} D_i\big(\|w_i\|_2\big)$ und Satz 3.2.7), so daß vor allem die obere Dreicksgestalt von S nicht verändert wird und R eine obere Dreiecksmatrix ist.
Die Multiplikation von O mit der Diagonalmatrix D^{-1} von rechts multipliziert alle Spalten von O mit den entsprechenden Diagonaleinträgen von D^{-1} (analoge Argumentation wie oben), so daß die Spalten $w_1, \ldots, w_n$ durch deren Längen geteilt und damit normiert werden. Somit enthält die Matrix Q spaltenweise genau die Orthonormalbasis $q_1 \ldots, q_n$ mit $q_i := \frac{w_i}{\|w_i\|_2}$, die im Gram-Schmidtschen Orthogonalisierungsverfahren konstruiert wurde:

$$\begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ q_1 & \cdots & q_n \\ | & & | \end{pmatrix} \underbrace{\begin{pmatrix} \|w_1\|_2 & & & & \\ & \ddots & & & \\ & & \|w_n\|_2 & & \end{pmatrix} \begin{pmatrix} 1 & s_{1,2} & & & s_{1,n} \\ 0 & 1 & & & s_{2,n} \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & & 1 & s_{n-1,n} \\ 0 & 0 & & & 1 \end{pmatrix}}_{=R}.$$

□

Bemerkung 4.1.29.

i.) Der Determinantenmultiplikationssatz 3.3.8 liefert sofort, daß bei der QR-Zerlegung eines invertierbaren A auch die Matrizen Q und R invertierbar sind, denn es gilt:

$$\begin{aligned} A \in \mathrm{GL}_n(\mathbb{R}) \quad &\Longleftrightarrow \quad \det(A) \neq 0 \\ &\Longrightarrow \quad 0 \neq \det(A) = \det(QR) = \det(Q) \cdot \det(R) \end{aligned}$$

$$\begin{aligned} &\Longrightarrow \quad \det(Q), \det(R) \neq 0 \\ &\Longleftrightarrow \quad Q, R \in \mathrm{GL}_n(\mathbb{R}). \end{aligned}$$

ii.) *Die QR-Zerlegung ist eindeutig, denn für zwei Zerlegungen $A = QR = \widetilde{Q}\widetilde{R}$ gilt wegen der Invertierbarkeit aller vorkommenden Matrizen:*

$$QR = \widetilde{Q}\widetilde{R} \quad \Longrightarrow \quad \widetilde{Q}^{-1}Q = \widetilde{R}R^{-1},$$

und kann gezeigt werden, daß $\widetilde{Q}^{-1}Q$ wieder als Spalten eine Orthonormalbasis des $\mathbb{R}^{[n]}$ bzgl. des Standard-Skalarproduktes enthält und $\widetilde{R}R^{-1}$ eine obere Dreiecksmatrix ist. Weiter kann gezeigt werden, daß $\widetilde{Q}^{-1}Q$ die Determinante Eins hat und daraus dann $\widetilde{Q}^{-1}Q = E_n$ folgt, was letztendlich $Q = \widetilde{Q}$ und $R = \widetilde{R}$ impliziert.

iii.) *Ist $A \in \mathrm{GL}_n(R)$, so sind seine Spalten $v_1, \ldots, v_n$ eine Basis des $\mathbb{R}^{[n]}$ (siehe z.B. Bemerkung 3.3.38). Nach dem Beweis von Satz 4.1.28 liefert das Gram-Schmidtsche Orthogonalisierungsverfahren eine QR-Zerlegung, wo in Q die aus $v_1, \ldots, v_n$ transformierte Orthonormalmatrix $q_1, \ldots, q_n$ steht und in R die Koeffizienten aus dem Gram-Schmidt-Verfahren, zeilenweise multipliziert mit der Norm der Orthogonalbasis $w_1, \ldots, w_n$, die im Verfahren zuerst berechnet wurde. Ist nun nur eine QR-Zerlegung $A = QR$ gegeben, so entsteht wegen der Eindeutigkeit der QR-Zerlegung diese genau aus dem Gram-Schmidt-Verfahren, und aus den beiden Matrizen Q und R können alle Zwischenschritte herausgelesen werden:*

a.) *Die Diagonalelemente $r_{i,i}$ von R enthalten die Längen der Orthogonalbasis w_i, d.h. $r_{i,i} = \|w_i\|_2$.*

b.) *$w_1, \ldots, w_n$ ergeben sich durch $\|w_i\|_2 \cdot q_i$.*

c.) *Wird in der Matrix R jede Zeile durch ihr Diagonalelement geteilt, so sind danach deren Einträge genau die Terme*

$$s_{j,i} := \frac{\langle w_j, v_i \rangle_2}{\langle w_j, w_j \rangle_2},$$

die beim Berechnen der Orthogonalbasis $w_1, \ldots, w_n$ aus der in A spaltenweise gegebenen Basis $v_1, \ldots, v_n$ auftreten:

$$w_i := v_i - \sum_{j=1}^{i-1} s_{j,i} w_j.$$

Siehe dazu auch die LR-Zerlegung einer Matrix (3.2.38):

LR-Zerlegung: *Die LR-Zerlegung $A = LR$ beschreibt den Gauß-Algorithmus, mit dem die Matrix A in eine Zeilen-Stufen-Form (obere Dreiecksgestalt) R gebracht wird, und die im Algorithmus auftretenden Koeffizienten des Verfahrens sind in L kodiert.*

QR-Zerlegung: *Die QR-Zerlegung $A = QR$ beschreibt das Gram-Schmidtsche Orthogoanlisierungsverfahren, mit dem die Basis aus den Spalten von A in eine Orthonormalbasis transformiert wird, die in den Spalten von Q steht, und die im Algorithmus auftretenden Koeffizienten sind in R kodiert.* □

Beispiel 4.1.30. *Es sei folgende reelle Matrix gegeben:*

$$A := \begin{pmatrix} 1 & 4 & -1 \\ 2 & 3 & -2 \\ 0 & -1 & -6 \end{pmatrix}.$$

Es gilt $\det(A) = 30$, *so daß* $A \in \mathrm{GL}_3(\mathbb{R})$ *gilt. Es soll nun für* A *bzgl. des Standard-Skalarproduktes im* $\mathbb{R}^{[3]}$ *mit:*

$$\langle \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \rangle_2 = x_1y_1 + x_2y_2 + x_3y_3$$

eine QR-Zerlegung mit Hilfe des Gram-Schmidtschen Orthogonalisierungsverfahrens konstruiert werden.
Die Spalten von A *seien mit* v_1, v_2, v_3 *bezeichnet. Sie bilden eine Basis des* $\mathbb{R}^{[3]}$, *so daß sie mit Hilfe des Gram-Schmidtschen Orthogonalisierungsverfahren 4.1.23 in eine Orthogonalbasis* w_1, w_2, w_3 *des* $\mathbb{R}^{[3]}$ *umgewandelt werden können:*

$$w_1 := v_1, \quad w_2 := v_2 - s_{1,2} \cdot w_1, \quad w_3 := v_3 - s_{1,3} \cdot w_1 - s_{2,3} \cdot w_2 \quad \textit{mit} \quad s_{i,j} := \frac{\langle w_i, v_j \rangle_2}{\langle w_i, w_i \rangle_2}.$$

Schrittweise Berechnung führt zu:

$$w_1 = v_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \quad \Longrightarrow \quad s_{1,2} = \frac{\langle w_1, v_2 \rangle_2}{\langle w_1, w_1 \rangle_2} = \frac{1 \cdot 4 + 2 \cdot 3 + 0 \cdot (-1)}{1^2 + 2^2 + 0^2} = \frac{10}{5} = 2,$$

$$w_2 = v_2 - s_{1,2} \cdot w_1 = \begin{pmatrix} 4 \\ 3 \\ -1 \end{pmatrix} - 2 \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} \quad \Longrightarrow$$

$$s_{1,3} = \frac{\langle w_1, v_3 \rangle_2}{\langle w_1, w_1 \rangle_2} = \frac{1 \cdot (-1) + 2 \cdot (-2) + 0 \cdot (-6)}{5} = \frac{-5}{5} = -1,$$

$$s_{2,3} = \frac{\langle w_2, v_3 \rangle_2}{\langle w_2, w_2 \rangle_2} = \frac{2 \cdot (-1) + (-1) \cdot (-2) + (-1) \cdot (-6)}{2^2 + (-1)^2 + (-1)^2} = \frac{6}{6} = 1$$

$$w_3 = v_3 - s_{1,3} \cdot w_1 - s_{2,3} \cdot w_2 = \begin{pmatrix} -1 \\ -2 \\ -6 \end{pmatrix} - (-1) \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \\ -5 \end{pmatrix}.$$

Aus der Orthogonalbasis w_1, w_2, w_3 *kann dann durch Normieren eine Orthonormalbasis* q_1, q_2, q_3 *konstruiert werden:*

$$q_i := \frac{1}{\|w_i\|_2} \cdot w_i \quad \textit{mit} \quad \|w_i\|_2 = \sqrt{\langle w_i, w_i \rangle_2}.$$

Es ergibt sind dann als Orthonormalbasis q_1, q_2, q_3:

$$\begin{array}{rcl} \|w_1\|_2 & = & \sqrt{5} \\ \|w_2\|_2 & = & \sqrt{6} \\ \|w_3\|_2 & = & \sqrt{30} \end{array} \quad \Longrightarrow \quad q_1 = \begin{pmatrix} \frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \\ 0 \end{pmatrix}, \; q_2 = \begin{pmatrix} \frac{2}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \end{pmatrix}, \; q_3 = \begin{pmatrix} -\frac{2}{\sqrt{30}} \\ \frac{1}{\sqrt{30}} \\ -\frac{5}{\sqrt{30}} \end{pmatrix}.$$

Das Gram-Schmidt-Verfahren liefert mit seinen Koeffizienten $s_{i,j}$ die folgende Zerlegung von A:

$$A = OS \quad \textit{mit} \quad O := \begin{pmatrix} | & | & | \\ w_1 & w_2 & w_3 \\ | & | & | \end{pmatrix} \quad \textit{und} \quad S := \begin{pmatrix} 1 & s_{1,2} & s_{1,3} \\ 0 & 1 & s_{2,3} \\ 0 & 0 & 1 \end{pmatrix}.$$

Die QR-Zerlegung von A ergibt sich dann aus der Formel $A = OD^{-1}DS$ mit der Diagonalmatrix D, die jeweils $\|w_i\|_2$ auf der Diagonalen enthält:

$$\begin{aligned} A &= \underbrace{\begin{pmatrix} | & | & | \\ w_1 & w_2 & w_3 \\ | & | & | \end{pmatrix}}_{=O} \cdot \underbrace{\begin{pmatrix} \frac{1}{\|w_1\|_2} & & \\ & \frac{1}{\|w_2\|_2} & \\ & & \frac{1}{\|w_3\|_2} \end{pmatrix}}_{=D^{-1}} \cdot \underbrace{\begin{pmatrix} \|w_1\|_2 & & \\ & \|w_2\|_2 & \\ & & \|w_3\|_2 \end{pmatrix}}_{=D} \cdot \underbrace{\begin{pmatrix} 1 & s_{1,2} & s_{1,3} \\ 0 & 1 & s_{2,3} \\ 0 & 0 & 1 \end{pmatrix}}_{=S} \\ &= \underbrace{\begin{pmatrix} | & | & | \\ q_1 & q_2 & q_3 \\ | & | & | \end{pmatrix}}_{=OD^{-1}=:Q} \cdot \underbrace{\begin{pmatrix} \|w_1\|_2 & \|w_1\|_2 \cdot s_{1,2} & \|w_1\|_2 \cdot s_{1,3} \\ 0 & \|w_2\|_2 & \|w_2\|_2 \cdot s_{2,3} \\ 0 & 0 & \|w_3\|_2 \end{pmatrix}}_{=DS=:R}. \end{aligned}$$

Hierbei sind die Spalten von Q genau die Orthonormalbasis q_1, q_2, q_3. Alle Werte eingesetzt ergeben dann endgültig:

$$\underbrace{\begin{pmatrix} 1 & 4 & -1 \\ 2 & 3 & -2 \\ 0 & -1 & -6 \end{pmatrix}}_{A} = \underbrace{\begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{6}} & -\frac{2}{\sqrt{30}} \\ \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{30}} \\ 0 & -\frac{1}{\sqrt{6}} & -\frac{5}{\sqrt{30}} \end{pmatrix}}_{Q} \cdot \underbrace{\begin{pmatrix} \sqrt{5} & 2\sqrt{5} & -\sqrt{5} \\ 0 & \sqrt{6} & \sqrt{6} \\ 0 & 0 & \sqrt{30} \end{pmatrix}}_{R}. \qquad \square$$

Oft ist es wichtig, für einen Vektor die Menge aller Vektoren zu betrachten, die orthogonal zu ihm sind - und verallgemeinernd für einen Untervektorraum alle Vektoren, die auf allen Unterraumvektoren senkrecht stehen. Dazu sei definiert:

Definition 4.1.31. *Sei V ein euklidischer Vektorraum und $U \subseteq V$ ein Untervektorraum. Dann heißt die Menge der Vektoren, die jeweils zu allen Vektoren von U orthogonal sind, das orthogonale Komplement von U und wird notiert mit:*

$$U^\perp := \{\, v \in V \mid v \perp u \textit{ für alle } u \in U \,\}.$$

Ist $W \subseteq V$ ein weiterer Untervektorraum, und sind alle Vektoren aus U und W jeweils paarweise orthongonal, so heißen beide Unterräume orthogonal zueinander und es wird notiert:

$$U \perp W \quad \Longleftrightarrow \quad u \perp w \textit{ für alle } u \in U, w \in W. \qquad \square$$

Zueinander orthogonale Untervektorraume haben die Eigenschaft, daß linear unabhängige Systeme aus ihnen zu einem linear unabhängigen System zusammengesetzt werden können:

LEMMA 4.1.32. *Sei $\big(V, \langle\cdot,\cdot\rangle\big)$ ein euklidischer Vektorraum. Weiter seien $U, W \subseteq V$ Untervektorräume mit $U \perp W$. Dann gilt:*

i.) $U \cap W = \{0\}$.

ii.) *Sind $u_1, \ldots, u_k$ linear unabhängig in U und $w_1, \ldots, w_r$ linear unabhängig in W, so sind:*

$$u_1, \ldots, u_k, w_1, \ldots, w_r \text{ linear unabhängig in } V.$$

BEWEIS.

i.) Sei $v \in U \cap W$. Für $u \in U$ und $w \in W$ gilt wegen $U \perp W$ nach Definition 4.1.31 $u \perp w$, also $\langle u, w\rangle = 0$. Da v in U und W liegt, folgt somit:

$$v \perp v \quad \Longrightarrow \quad \langle v, v\rangle = 0 \quad \overset{Definitheit}{\Longrightarrow} \quad v = 0.$$

ii.) Es ist zu zeigen:

$$\sum_{i=1}^{k} \alpha_i u_i + \sum_{j=1}^{r} \beta_j w_j = 0 \quad \Longrightarrow \quad \alpha_i, \beta_j = 0.$$

Dabei gilt:

$$\sum_{i=1}^{k} \alpha_i u_i + \sum_{j=1}^{r} \beta_j w_j = 0 \quad \Longrightarrow \quad \underbrace{\sum_{i=1}^{k} \alpha_i u_i}_{\in U} = \underbrace{\sum_{j=1}^{r} (-\beta_j) w_j}_{\in W} \in U \cap W = \{0\},$$

und die lineare Unabhängigkeit der Teilsysteme $u_1, \ldots, u_k$ und $w_1, \ldots, w_r$ liefert dann sofort $\alpha_i = 0$ und $\beta_j = 0$. □

Für das orthogonale Komplement eines Unterraumes gelten folgende wesentliche Eigenschaften:

LEMMA 4.1.33. *Sei $\big(V, \langle\cdot,\cdot\rangle\big)$ ein endlich-dimensionaler euklidischer Vektorraum. Weiter sei $U \subseteq V$ ein Untervektorraum. Dann gilt:*

i.) *$U^\perp$ ist ein Untervektorraum.*

ii.) $U \perp U^\perp$.

iii.) $U \cap U^\perp = \{0\}$.

iv.) *Sind $u_1, \ldots, u_k$ linear unabhängig in U und $v_1, \ldots, v_r$ linear unabhängig in $U^\perp$, so sind:*

$$u_1, \ldots, u_k, v_1, \ldots, v_r \text{ linear unabhängig in } V.$$

v.) $\dim_{\mathbb{R}}(U) + \dim_{\mathbb{R}}(U^\perp) = \dim_{\mathbb{R}}(V)$.

vi.) *Jedes $x \in V$ besitzt eine eindeutige Summenzerlegung $x = u + \widetilde{u}$ mit $u \in U$ und $\widetilde{u} \in U^\perp$.*

vii.) $(U^\perp)^\perp = U$.

Beweis.

i.) Für $x, y \in U^\perp$ ist nach dem Untervektorraumkriterium 2.1.13 zu zeigen, daß $\alpha x + \beta y$ für alle $\alpha, \beta \in \mathbb{R}$ in $U^\perp$ liegt. Für alle $u \in U$ gilt wegen $x, y \in U^\perp$:

$$\langle u, x\rangle = \langle u, y\rangle = 0,$$

und so folgt:

$$\langle u, \alpha x + \beta y\rangle = \alpha \cdot \langle u, x\rangle + \beta \cdot \langle u, y\rangle = 0,$$

so daß $\alpha x + \beta y$ in $U^\perp$ liegt.

ii.) $U \perp U^\perp$ gilt nach Definition 4.1.31.

iii.) $U \cap U^\perp = \{0\}$ folgt aus $U \perp U^\perp$ und Lemma 4.1.32.

iv.) Diese Aussage folgt ebenso wegen $U \perp U^\perp$ aus Lemma 4.1.32.

v.) Sei $u_1, \ldots, u_k$ eine Basis von U. Diese kann durch Vektoren $x_1, \ldots, x_r$ zu einer Basis von V ergänzt werden. Durch das Gram-Schmidtsche Orthogonalisierungsverfahren 4.1.23 kann aus dieser eine Orthogonalbasis von V:

$$\widetilde{u}_1, \ldots, \widetilde{u}_k, \widetilde{x}_1, \ldots, \widetilde{x}_r$$

konstruiert werden, so daß $\widetilde{u}_1, \ldots, \widetilde{u}_k$ im Erzeugnis von $u_1, \ldots, u_k$ liegen, also in U. Aus Dimensionsgründen ist dann $\widetilde{u}_1, \ldots, \widetilde{u}_k$ ein maximal linear unabhängiges System in U und damit eine Basis von U.
Es muß jetzt noch gezeigt werden, daß $\widetilde{x}_1, \ldots, \widetilde{x}_r$ eine Basis von $U^\perp$ ist: Nach Konstruktion liegen all diese Vektoren in $U^\perp$ und sind somit ein linear unabhängiges System in $U^\perp$. Wäre es nicht maximal linear unabhängige in $U^\perp$, so könnte es um einen Vektor $x \in U^\perp$ verlängert werden, und nach vorheriger Aussage wäre dann:

$$\underbrace{\widetilde{u}_1, \ldots, \widetilde{u}_k}_{\text{l.u. in } U}\underbrace{\widetilde{x}_1, \ldots, \widetilde{x}_r, x}_{\text{l.u. in } U^\perp}$$

wegen $U \perp U^\perp$ linear unabhängig in V. Dies ist jedoch ein Widerspruch dazu, daß schon:

$$\widetilde{u}_1, \ldots, \widetilde{u}_k, \widetilde{x}_1, \ldots, \widetilde{x}_r$$

eine Basis von V ist, so daß es kein ergänzendes x mehr geben kann und $\widetilde{x}_1, \ldots, \widetilde{x}_r$ schon in $U^\perp$ maximal linear unabhängig ist und damit eine Basis.
Die Dimensionsformel ist dann klar.

vi.) Nach der vorherigen Dimensionsformel und der Zusammensetzbarkeit von linear unabhängigen Systemen aus U und $U^\perp$ folgt sofort, daß eine Basis $u_1, \ldots, u_k$ aus U und eine Basis $v_1, \ldots, v_r$ aus $U^\perp$ zusammengesetzt eine Basis von V ergeben. Dies liefert sofort, daß jedes $x \in V$ eine eindeutige Zerlegung $x = u + \widetilde{u}$ mit $u \in U$ und $\widetilde{u} \in U^\perp$ besitzt:

$$x = \underbrace{\sum_{i=1}^{k} \alpha_i u_i}_{=:u} + \underbrace{\sum_{j=1}^{r} \beta_j v_j}_{=:\widetilde{u}}.$$

vii.) Offensichtlich gilt nach Definition 4.1.31 die Beziehung $U \subseteq (U^\perp)^\perp$. Die Gleichheit gilt nach der vorherigen Dimensionsformel:

$$\dim_{\mathbb{R}}(U) + \dim_{\mathbb{R}}(U^\perp) = \dim_{\mathbb{R}}(V) = \dim_{\mathbb{R}}(U^\perp) + \dim_{\mathbb{R}}\left((U^\perp)^\perp\right)$$

$$\Longrightarrow \quad \dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}\left((U^\perp)^\perp\right) \quad \overset{2.2.53}{\Longrightarrow} \quad U = (U^\perp)^\perp. \qquad \square$$

Bemerkung 4.1.34. *In Lemma 4.1.33 sind eine Aussagen über das orthogonale Komplement eines Unterraumes eines endlich-dimensionalen euklidischen Vektorraumes gemacht, und die ersten vier gelten offensichtlich auch, wenn der Unterraum in einem unendlich-dimensionalen euklidischen Vektorraum liegt.*
Die anderen Aussagen über das orthogonale Komplement eines Unterraumes aus Lemma 4.1.33 gelten nicht unbedingt im Fall eines unendlich-dimensionalen Vektorraumes: Sei dazu wieder der unendlich-dimensionale euklidische Raum ℓ^2 aus Beispiel 4.1.10 betrachtet. Es sei darin der von:

$$S := (e_0, e_1, e_2, \ldots, e_i, \ldots)_{i\in\mathbb{N}_0} \quad \textit{mit} \quad e_i := (0, \ldots, 0, \underset{i}{1}, 0, \ldots)$$

erzeugte Unterraum $U := \langle S\rangle$ betrachtet. S ist nach Bemerkung 4.1.26 ein maximal linear unabhängiges orthogonales System, so daß $U^\perp = \{0\}$ folgt. Damit gilt vor allem:

$$(U^\perp)^\perp = (\{0\})^\perp = \ell^2,$$

aber nach Bemerkung 4.1.26 ist S kein Erzeugendensystem von ℓ^2 und damit:

$$U \subsetneq (U^\perp)^\perp.$$

Im endlich-dimensionalen Fall gilt nach Lemma 4.1.33 immer $U = (U^\perp)^\perp$.
Auch hat nicht jedes $x \in \ell^2$ eine eindeutige Zerlegung $x = u + \widetilde{u}$ mit $u \in U$ und $\widetilde{u} \in U^\perp$, denn wegen $U^\perp = \{0\}$ gibt es für jedes $x \notin U$ gar keine solche Zerlegung. Da $U \subsetneq \ell^2$ gilt, existieren auch solche $x \notin U$. □

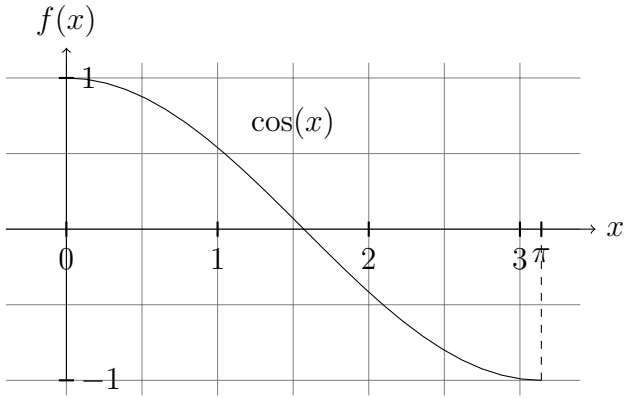
Es soll jetzt noch, wie angekündigt, in euklidischen Räumen für zwei Vektoren ein Winkel zwischen ihnen erklärt werden. Sei dazu ein euklidischer Vektorraum $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ betrachtet. Für $x, y \in V$ mit $x, y \neq 0$ gilt nach der Cauchy-Schwarzschen Ungleichung 4.1.11 bzw. Bemerkung 4.1.13:

$$|\langle x, y\rangle| \leq \|x\| \cdot \|y\| \quad \overset{\|x\|,\|y\|\neq 0}{\Longrightarrow} \quad \frac{|\langle x, y\rangle|}{\|x\| \cdot \|y\|} \leq 1,$$

was wiederum äquivalent ist zu der Aussage:

$$-1 \leq \frac{\langle x, y\rangle}{\|x\| \cdot \|y\|} \leq 1. \tag{4.1.35}$$

Jeder Zahl $\gamma \in [-1, 1]$ ist genau ein $\alpha \in [0, \pi]$ zugeordnet mit $\gamma = \cos(\alpha)$:



Dies führt dann zu der Definition:

Definition 4.1.36. *Sei $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ ein euklidischer Vektorraum. Dann ist für zwei Vektoren $x, y \in V$ mit $x, y \neq 0$ der Winkel definiert durch Gleichung 4.1.35, d.h. die eindeutig bestimmte Zahl $\alpha_{x,y} \in [0, \pi]$ mit:*

$$\cos(\alpha_{x,y}) = \frac{\langle x, y\rangle}{\|x\| \cdot \|y\|}. \qquad \square$$

Bemerkung 4.1.37.

i.) Wegen der Symmetry des Skalarproduktes gilt für den Winkel zwischen zwei Vektoren x, y nach Definition 4.1.36:

$$\frac{\langle x, y\rangle}{\|x\| \cdot \|y\|} = \frac{\langle y, x\rangle}{\|y\| \cdot \|x\|} \qquad \Longrightarrow \qquad \alpha_{x,y} = \alpha_{y,x}.$$

ii.) In einem euklidischen Vektorraum $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ gilt für $x, y \neq 0$ wegen:

$$x, y \neq 0 \qquad \Longleftrightarrow \qquad \|x\|, \|y\| \neq 0$$

die Äquivalenzenkette:

$$x \perp y \quad \overset{4.1.19}{\Longleftrightarrow} \quad \langle x, y\rangle = 0 \quad \overset{x,y\neq 0}{\Longleftrightarrow} \quad \frac{\langle x, y\rangle}{\|x\| \cdot \|y\|} = 0 \quad \overset{4.1.36}{\Longleftrightarrow} \quad \cos(\alpha_{x,y}) = 0$$

$$\overset{\alpha_{x,y}\in[0,\pi]}{\Longleftrightarrow} \quad \alpha_{x,y} = \tfrac{\pi}{2} \qquad \Longleftrightarrow \qquad \alpha_{x,y} = 90^\circ.$$

Damit verträgt sich die Definition von Orthogonalität bzw. „senkrecht stehen“ über das Skalarprodukt in Definition 4.1.19 mit der aus der Schule im $\mathbb{R}^2$ bekannten Definition über den Winkel.

iii.) Für zwei Vektoren x, y eines euklidischen Vektorraumes $\big(V, \langle\,\cdot,\cdot\,\rangle\big)$ liefern die Eigenschaften des Skalarproduktes sofort die Gleichung:

$$\|x + y\|^2 = \langle x + y, x + y\rangle = \langle x, x\rangle + 2 \cdot \langle x, y\rangle + \langle y, y\rangle = \|x\|^2 + \|y\|^2 + 2 \cdot \langle x, y\rangle. \quad (*)$$

Für $x, y \neq 0$ gilt nach der Definiton des Winkels in 4.1.36:

$$\langle x, y\rangle = \cos(\alpha_{x,y}) \cdot \|x\| \cdot \|y\|,$$

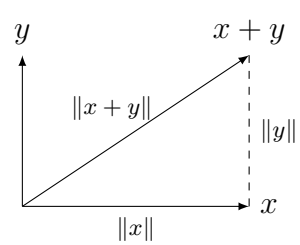
und dies liefert zusammen mit der Gleichung $(*)$ sofort für die Vektoren $x, y \neq 0$ den sogennanten Cosinus-Satz:

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2 \cdot \cos(\alpha_{x,y}) \cdot \|x\| \cdot \|y\|.$$

Für $x \perp y$ gilt dann nach der vorherigen Äquivalenzenkette $\cos(\alpha_{x,y}) = 0$, und es folgt eine Aussage, die aus der Schule im $\mathbb{R}^2$ zusammen mit dem Standard-Skalarprodukt als Satz von Pythagoras bekannt ist:

$$x \perp y \qquad \Longrightarrow \qquad \|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Skizze:



$\square$

Matrizendarstellung von Bilinearformen.

Wie bei linearen Abbildungen können auch bei Bilinearformen Matrizen zu deren Beschreibung herangezogen werden. Dazu wird zuerst, analog wie zu den linearen Abbildungen in Lemma 2.2.13 gezeigt, daß Bilinearformen durch ihre Bilder auf einer Basis eindeutig festgelegt sind:

LEMMA 4.1.38. *Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum und $v_1, \ldots, v_n$ eine Basis von V. Sind dann zwei Bilinearformen:*

$$b_1, b_2 \colon V \times V \longrightarrow \mathbb{R}$$

gegeben, so gilt:

$$b_1 = b_2 \qquad \Longleftrightarrow \qquad b_1(v_i, v_j) = b_2(v_1, v_j) \quad \text{für alle } 1 \leq i, j \leq n.$$

BEWEIS.

„$\Rightarrow$“: Trivial.

„$\Leftarrow$“: Es seien $x, y \in V$ gegeben mit

$$x := \sum_{i=1}^{n} \alpha_i v_i \quad \text{und} \quad y := \sum_{j=1}^{n} \beta_j v_j.$$

Dann folgt aus den Eigenschaften einer Bilinearform:

$$\begin{aligned} b_1(x, y) &= b_1\big(\sum_{i=1}^{n} \alpha_i v_i, y\big) = \sum_{i=1}^{n} b_1\big(\alpha_i v_i, y\big) = \sum_{i=1}^{n} \alpha_i \cdot b_1(v_i, y) \\ &= \sum_{i=1}^{n} \alpha_i \cdot b_1\big(v_i, \sum_{j=1}^{n} \beta_j v_j\big) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j b_1(v_i, v_j) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j b_2(v_i, v_j) = b_2\big(\sum_{i=1}^{n} \alpha_i v_i, \sum_{j=1}^{n} \beta_j v_j\big) = b_2(x, y). \end{aligned}$$

□

Für $\dim_{\mathbb{R}}(V) := n$ gibt es n^2 Basisvektortupel (v_i, v_j) auf denen eine Bilinearform $b \colon V \times V \longrightarrow \mathbb{R}$ eindeutig festgelegt ist, und diese können in einer $(n \times n)$-Matrix angeordnet werden, um b zu beschreiben:

DEFINITION 4.1.39. *Sei V ein $\mathbb{R}$-Vektorraum mit einer Basis $B := (v_1, \ldots, v_n)$ und $b \colon V \times V \longrightarrow \mathbb{R}$ eine Bilinearform. Dann ist die darstellende Matrix von b bzgl. der Basis B definiert durch:*

$$_B[b]_B := \begin{pmatrix} b(v_1, v_1) & \ldots & b(v_1, v_n) \\ \vdots & & \vdots \\ b(v_n, v_1) & \ldots & b(v_n, v_n) \end{pmatrix} \in \mathrm{Mat}_n(\mathbb{R}).$$

Die Menge aller Bilienarformen auf V sei notiert mit:

$$Bil_{\mathbb{R}}(V) := \{\, b \colon V \times V \longrightarrow \mathbb{R} \mid b \text{ Bilinearform} \,\}.$$

□

Bemerkung 4.1.40.

i.) Die Menge $Bil_{\mathbb{R}}(V)$ aller Bilinearformen auf dem $\mathbb{R}$-Vektorraum V trägt auch eine $\mathbb{R}$-Vektorraumstruktur: Eine Bilinearformen $b\colon V \times V \longrightarrow \mathbb{R}$ ist ja auch eine Abbildung, also gilt:

$$Bil_{\mathbb{R}}(V) \subseteq \mathrm{Abb}(V \times V, \mathbb{R}),$$

und es ist leicht zu zeigen, daß $Bil_{\mathbb{R}}(V)$ ein $\mathbb{R}$-Untervektorraum des $\mathbb{R}$-Vektorraumes $\mathrm{Abb}(V \times V, \mathbb{R})$ ist.
Für $b_1, b_2 \in Bil_{\mathbb{R}}(V)$, $\alpha \in \mathbb{R}$ und $x, y \in V$ sind dabei die Verknüpfungen auf dem $\mathbb{R}$-Vektorraum $Bil_{\mathbb{R}}(V)$ definiert durch (siehe auch Bemerkung 2.1.3):

$$(b_1 \oplus b_2)(x, y) := b_1(x, y) + b_2(x, y) \quad \text{und} \quad (\alpha \bullet b_1)(x, y) := \alpha \cdot b_1(x, y).$$

Die Vektorraumstruktur auf $Bil_{\mathbb{R}}(V)$ spielt im weiteren Verlauf keine Rolle.

ii.) Sei V ein $\mathbb{R}$-Vektorraum, und es sei B eine Basis von V. Mittlerweile gibt es drei „Klammer-Ausdrücke“, die bezüglich B Objekte darstellen:

$[x]_B \in \mathbb{R}^{[n]}$:	*Koordinatendarstellung eines $x \in V$, Definition 3.4.6,*
$[\varphi]_{B,B} \in \mathrm{Mat}_n(\mathbb{R})$:	*Matrizendarstellung eines Endomorphismus $\varphi \in \mathrm{End}_{\mathbb{R}}(V)$, Definition 3.4.13,*
${}_B[b]_B \in \mathrm{Mat}_n(\mathbb{R})$:	*Matrizendarstellung einer Bilinearform $b \in Bil_{\mathbb{R}}(V)$, Definition 4.1.39.*

□

Beispiel 4.1.41. *Es sei im $\mathbb{R}^2$ folgende Bilinearform gegeben (das Skalarprodukt aus Beispiel 4.1.10):*

$$b\big((x_1, x_2), (y_1, y_2)\big) := 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + 5x_2y_2.$$

Dann hat b bzgl. der Standard-Basis $\mathcal{E}_2 := (e_1, e_2)$ des $\mathbb{R}^2$ folgende Matrizendarstellung:

$${}_{\mathcal{E}_2}[b]_{\mathcal{E}_2} = \begin{pmatrix} b(e_1, e_1) & b(e_1, e_2) \\ b(e_2, e_1) & b(e_2, e_2) \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}.$$

Bezüglich der Basis $B := (v_1, v_2) := \big((1, 1), (0, 1)\big)$ hat b die Matrizendasrstellung:

$${}_B[b]_B = \begin{pmatrix} b(v_1, v_1) & b(v_1, v_2) \\ b(v_2, v_1) & b(v_2, v_2) \end{pmatrix} = \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}.$$

□

Andersherum kann bei gegebener Basis $B := (v_1, \ldots, v_n)$ von V einer quadratischen Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ eine Bilinearform zugeordnet werden mit Hilfe der Koordinatenabbildung aus Definition 3.4.6:

$$[\cdot]_B\colon V \longrightarrow \mathbb{R}^{[n]} \quad \text{mit} \quad \sum_{i=1}^{n} a_i v_i \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

wie folgende Aussage zeigt:

Lemma 4.1.42. *Sei V ein $\mathbb{R}$-Vektorraum und $B := (v_1, \ldots, v_n)$ eine Basis. Weiter sei $A \in \mathrm{Mat}_n(\mathbb{R})$. Dann ist folgende durch A induzierte Abbildung eine Bilinearform auf V:*

$$b_A\colon V \times V \longrightarrow \mathbb{R} \quad \text{mit} \quad (x, y) \mapsto [x]_B^t \cdot A \cdot [y]_B,$$

wobei $[x]_B^t$ ein Zeilenvektor ist, der transponierte Spaltenvektor $[x]_B$.

Beweis.
Der Term $[x]_B^t \cdot A \cdot [y]_B$ ist ein Matrizenprodukt, und alle Eigenschaften einer Bilinearform von b_A lassen sich direkt aus den Eigenschaften des Matrizenproduktes in Satz 3.1.8 ablesen. □

Beispiel 4.1.43.

i.) Es sei folgende reelle Matrix gegeben:

$$A := \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$$

Im $\mathbb{R}^2$ sei weiter die Standard-Basis $\mathcal{E}_2 := (e_1, e_2)$ betrachtet. Für $(x, y) \in \mathbb{R}^2$ gilt dann:

$$[(x, y)]_{\mathcal{E}_2} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

Dann hat die durch A induzierte Bilinearform $b_A \in Bil_{\mathbb{R}}(\mathbb{R}^2)$ auf den Vektoren $(1, 3)$ und $(2, -1)$ den Wert:

$$\begin{aligned} b_A\big((1,3),\,(2,-1)\big) := [(1,3)]_{\mathcal{E}_2}^t \cdot A \cdot [(2,-1)]_{\mathcal{E}_2} &= \begin{pmatrix} 1 \\ 3 \end{pmatrix}^t \cdot \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \end{pmatrix} = 4. \end{aligned}$$

ii.) Allgemein gilt für die vorher gegebene Matrix A:

$$\begin{aligned} b_A\big((x_1,x_2),\,(y_1,y_2)\big) := [(x_1,x_2)]_{\mathcal{E}_2}^t \cdot A \cdot [(y_1,y_2)]_{\mathcal{E}_2} &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \cdot \begin{pmatrix} 2y_1 + 3y_2 \\ 3y_1 + 5y_2 \end{pmatrix} \\ &= 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + 5x_2y_2. \end{aligned}$$

Dies ist das Skalarprodukt aus Beispiel 4.1.10. □

Als nächstes wird gezeigt, daß die beiden Zuordnungen invers zueinander sind:

Satz 4.1.44. *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und B eine Basis von V. Dann sind die folgenden beiden Abbildungen invers zueinander:*

$$\begin{aligned} \Phi_B\colon Bil_{\mathbb{R}}(V) &\longrightarrow \mathrm{Mat}_n(\mathbb{R}) \quad \textit{mit} \quad b \mapsto {}_B[b]_B, \\ \Psi_B\colon \mathrm{Mat}_n(\mathbb{R}) &\longrightarrow Bil_{\mathbb{R}}(V) \quad \textit{mit} \quad A \mapsto b_A. \end{aligned}$$

Damit gilt insbesondere für alle $x, y \in V$ mit der Koordinatendarstellung bzgl. B:

$$b(x, y) = [x]_B^t \cdot {}_B[b]_B \cdot [y]_B,$$

und für jede Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ gilt:

$$b(x, y) = [x]_B \cdot A \cdot [y]_B \textit{ für alle } x, y \quad \Longrightarrow \quad A = {}_B[b]_B.$$

Beweis.
Es ist zuerst zu zeigen, daß gilt:

$$\Psi_B \circ \Phi_B = \mathrm{id}_{\mathrm{Bil}_{\mathbb{R}}(V)} \quad \text{und} \quad \Phi_B \circ \Psi_B = \mathrm{id}_{\mathrm{Mat}_n(\mathbb{R})}\,.$$

$\Psi_B \circ \Phi_B = \mathrm{id}_{\mathrm{Bil}_{\mathbb{R}}(V)}$: Für $b \in \mathrm{Bil}_{\mathbb{R}}(V)$ ist zu zeigen:

$$\underbrace{b_{{}_B[b]_B}}_{=(\Psi_B\circ\Phi_B)(b)} = b.$$

Nach Lemma 4.1.38 sind die Bilinearformen b und $b_{{}_B[b]_B}$ schon gleich, wenn sie auf allen Tupeln (v_i, v_j) der Basis $B := (v_1, \ldots, v_n)$ übereinstimmen.
Es gilt dabei $[v_i]_B = e_i$ mit dem i-ten Standard-Basisvektor e_i des $\mathbb{R}^{[n]}$, und bzgl. dieser Standard-Basisvektoren des $\mathbb{R}^{[n]}$ folgt für eine Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ aus der Interpretation des Matrizenproduktes aus Lemma 3.1.6:

$$e_i^t \cdot A \cdot e_j = a_{i,j} \quad \text{mit} \quad A := (a_{i,j}).$$

Dies liefert dann mit ${}_B[b]_B = \big(b(v_i, v_j)\big)$ wie gewünscht:

$$b_{{}_B[b]_B}(v_i, v_j) = [v_i]_B^t \cdot {}_B[b]_B \cdot [v_j]_B = e_i^t \cdot {}_B[b]_B \cdot e_j = b(v_i, v_j).$$

$\Phi_B \circ \Psi_B = \mathrm{id}_{\mathrm{Mat}_n(\mathbb{R})}$: Es ist für $A := (a_{i,j}) \in \mathrm{Mat}_n(\mathbb{R})$ zu zeigen:

$$\underbrace{{}_B[b_A]_B}_{=(\Phi_B\circ\Psi_B)(A)} = A.$$

Wieder wird ausgenutzt, daß für A bzgl. der Standard-Basisvektoren des $\mathbb{R}^{[n]}$ die Gleichung $e_i^t \cdot A \cdot e_j = a_{i,j}$ gilt, und mit $[v_i]_B = e_i$ folgt dann sofort:

$${}_B[b_A]_B = \big(b_A(v_i, v_j)\big) = \big([v_i]_B^t \cdot A \cdot [v_j]_B\big) = \big(e_i^t \cdot A \cdot e_j\big) = (a_{i,j}) = A.$$

Die behauptete Gleichung $b(x, y) = [x]_B^t \cdot {}_B[b]_B \cdot [y]_B$ folgt sofort aus der vorher gezeigten Identität $b = b_{{}_B[b]_B}$, und die letzte Implikation gilt dann wegen der Injektivität von Ψ_B. □

Bemerkung 4.1.45. *Nach Satz 4.1.44 können also nach Wahl einer Basis in V alle Bilinearformen aus $Bil_{\mathbb{R}}(V)$ eineindeutig mit den quadratischen Matrizen $\mathrm{Mat}_n(\mathbb{R})$ identifierziert werden - die wiederum nach Satz 3.4.17 via Basiswahl eineindeutig die Endomorphismen von V beschreiben:*

$$Bil_{\mathbb{R}}(V) \xrightarrow[4.1.44]{\text{Basiswahl } B} \mathrm{Mat}_n(\mathbb{R}) \xleftarrow[3.4.17]{\text{Basiswahl } B} \mathrm{End}_R(V).$$

Ein $A \in \mathrm{Mat}_n(\mathbb{R})$ kann also je nach Situation als Beschreibung $A = {}_B[b]_B$ einer Bilinearform b auf V aufgefaßt werden oder als Beschreibung $[\varphi]_{B,B}$ eines Endomorphismus φ von V. □

Mit den bisherigen Ergebnissen ist es leicht, den Zusammenhang zwischen den Matrizendarstellungen einer Bilienarform bzgl. verschiedener Basen zu beschreiben:

Satz 4.1.46. *Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum, b eine Bilinearform auf V, und es seien B und C Basen von V. Dann gilt für die Matrizendarstellungen von b bzgl. dieser Basen:*

$${}_C[b]_C = [\mathrm{id}]_{B,C}^t \cdot {}_B[b]_B \cdot [\mathrm{id}]_{B,C}.$$

Beweis.
Es folgt für alle $x, y \in V$ mit $[v]_C = [\mathrm{id}(v)]_C = [\mathrm{id}]_{C,B} \cdot [v]_B$:

$$\begin{aligned}
[x]_B^t \cdot {}_B[b]_B \cdot [y]_B &\overset{(4.1.44)}{=} b(x,y) \overset{(4.1.44)}{=} b(x,y)[x]_C^t \cdot {}_C[b]_C \cdot [y]_C \\
&= \big([\mathrm{id}]_{C,B} \cdot [x]_B\big)^t \cdot {}_C[b]_C \cdot \big([\mathrm{id}]_{C,B} \cdot [y]_B\big) \\
&\overset{(3.3.35)}{=} \big([x]_B^t \cdot [\mathrm{id}]_{C,B}^t\big) \cdot {}_C[b]_C \cdot \big([\mathrm{id}]_{C,B} \cdot [y]_B\big) \\
&= [x]_B^t \cdot \Big([\mathrm{id}]_{C,B}^t \cdot {}_C[b]_C \cdot [\mathrm{id}]_{C,B}\Big) \cdot [y]_B.
\end{aligned}$$

Die Eindeutigkeitsaussage in Satz 4.1.44, daß es genau ein $A \in \mathrm{Mat}_n(\mathbb{R})$ gibt mit $b(x,y) = [x]_B^t \cdot A \cdot [y]_B$, liefert dann sofort die Behauptung. □

Bemerkung 4.1.47. *Die Basiswechsel haben bei Matrizendarstellungen von Endomorphismen und Bilinearformen verschiedene Formen:*

- *Bei einen Endomorphismus $\varphi \in \mathrm{End}_{\mathbb{R}}(V)$ gilt für den Zusammenhang der Matrizendarstellungen bzgl. Basen B und C nach Satz 3.4.36:*

$$[\varphi]_{C,C} = [\mathrm{id}]_{B,C}^{-1} \cdot [\varphi]_{B,B} \cdot [\mathrm{id}]_{B,C}.$$

- *Bei einer Bilinearform $b \in Bil_{\mathbb{R}}(V)$ gilt für den Zusammenhang der Matrizendarstellungen bzgl. Basen B und C nach Satz 4.1.46:*

$${}_C[b]_C = [\mathrm{id}]_{B,C}^t \cdot {}_B[b]_B \cdot [\mathrm{id}]_{B,C}.$$

Es wird also einmal eine Basiswechselmatrix und ihre Inverse, und einmal eine Basiswechselmatrix und ihre Transponierte verwendet, um die jeweiligen Matrizendarstellungen ineinander zu transformieren. □

Beispiel 4.1.48. *In Beispiel 4.1.41 wurde die folgende Bilinearform auf dem $\mathbb{R}^2$:*

$$b\big((x_1,x_2),\,(y_1,y_2)\big) := 2x_1y_1 + 3x_1y_2 + 3x_2y_1 + 5x_2y_2$$

bzgl. der Basen $\mathcal{E}_2$ und $B := \big((1,1),\,(0,1)\big)$ dargestellt, und es ergab sich:

$${}_{\mathcal{E}_2}[b]_{\mathcal{E}_2} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \qquad \textit{und} \qquad {}_B[b]_B = \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}.$$

Die Basiswechselmatrix $[\mathrm{id}]_{\mathcal{E}_2,B}$ ergibt sich leicht durch den spaltenweisen *Eintrag der Basis B in eine Matrix:*

$$[\mathrm{id}]_{\mathcal{E}_2,B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

und die Basiswechselformel aus Satz 4.1.46 liefert sofort:

$${}_B[b]_B = [\mathrm{id}]_{\mathcal{E}_2,B}^t \cdot {}_{\mathcal{E}_2}[b]_{\mathcal{E}_2} \cdot [\mathrm{id}]_{\mathcal{E}_2,B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^t \cdot \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}. \qquad \square$$

DEFINITION 4.1.49. *Eine Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ heißt symmetrisch, falls sie gleich ihrer transponierten ist, d.h. wenn gilt:*

$$A = A^t \quad \text{bzw.} \quad a_{i,j} = a_{j,i} \text{ für alle } i, j \text{ mit } (a_{i,j}) := A.$$

Eine symmetrische Matrix $A \in \mathrm{Mat}_n(\mathbb{R})$ heißt positiv definit, falls für alle $x \in \mathbb{R}^{[n]}$ mit $x \neq 0$ gilt:

$$x^t A x > 0.$$

Die Menge aller symmetrischen Matrizen wird bezeichnet mit:

$$Sym_n(\mathbb{R}) := \{\, A \in \mathrm{Mat}_n(\mathbb{R}) \mid A^t = A \,\}. \qquad \square$$

BEMERKUNG 4.1.50.

i.) Ist $A \in \mathrm{Mat}_n(\mathbb{R})$ symmetrisch, so gilt für $x, y \in \mathbb{R}^{[n]}$ bzgl. des Standard-Skalarproduktes:

$$\langle x, Ay \rangle_2 \overset{(4.1.18)}{=} x^t A y \overset{(x^t A y \in \mathbb{R})}{=} (x^t A y)^t \overset{(3.3.35)}{=} y^t A^t (x^t)^t \overset{(A^t = A)}{=} y^t A x$$
$$\overset{(4.1.18)}{=} \langle y, Ax \rangle_2. \overset{(\langle \cdot, \cdot \rangle \text{ sym})}{=} \langle Ax, y \rangle_2.$$

ii.) Offensichtlich gilt:

$$Sym_n(\mathbb{R}) \subseteq \mathrm{Mat}_n(\mathbb{R}) \text{ ist ein Untervektorraum.} \qquad \square$$

SATZ 4.1.51. *Sei $A \in \mathrm{Mat}_n(\mathbb{R})$ eine symmetrische Matrix. Dann gibt es eine Matrix $S \in \mathrm{GL}_n(\mathbb{R})$ und eine Diagonalmatrix D mit:*

$$S^t A S = D.$$

BEWEIS. TBA. $\square$

LEMMA 4.1.52. *Sei $A \in \mathrm{Mat}_n(\mathbb{R})$ eine symmetrische Matrix. Dann gilt:*

i.) A besitzt einen Eigenwert $\lambda \in \mathbb{R}$.

ii.) Wird der Spalten-Raum $\mathbb{R}^{[n]}$ mit dem Standard-Skalarprodukt $\langle \cdot, \cdot \rangle_2$ und der daraus abgeleiteten euklidischen Norm $\| \cdot \|_2$ betrachtet, so gilt für die folgende stetige Funktion (Polynom in n Variablen):

$$q_A \colon \mathbb{R}^n \longrightarrow \mathbb{R} \quad \text{und} \quad x \mapsto \langle x, Ax \rangle_2$$

bzgl. der kompakten $(n-1)$-ten Einheitssphäre:

$$S^{n-1} := \{\, x \in \mathbb{R}^{[n]} \mid \|x\|_2 = 1 \} \subseteq \mathbb{R}^{[n]},$$

daß $\max(q_{A|_{S^n}})$ der größte Eigenwert von A ist, und jedes $v \in S^n \subseteq \mathbb{R}^{[n]}$, in dem q_A sein Maximum annimmt, ein Eigenvektor zu diesem Eigenwert:

$$\max(q_{A|_{S^{n-1}}}) = q_A(v) = \langle v, Av \rangle_2.$$

Beweis.
Offensichtlich muß nur die zweite Aussage bewiesen werden, da sie eine Verschärfung der ersten Aussage ist. Dazu wird zunächst folgende Hilfsaussage gezeigt:

Hilfssatz: Sei $A \in \mathrm{Mat}_n(\mathbb{R})$ eine symmetrische Matrix und

$$q_A \colon \mathbb{R}^n \longrightarrow \mathbb{R} \quad \text{mit} \quad x \mapsto \langle x, Ax\rangle_2.$$

Weiter sei $v \in S^{n-1}$ so, daß die stetige Abbildung q_A darin ein Maximum auf dem Kompaktum $S^{n-1} \subseteq \mathbb{R}^n$ annimmt. Dann gilt für $w \in S^{n-1}$ bzgl. des Standard-Skalarproduktes $\langle\,\cdot,\cdot\,\rangle_2$:

$$v \perp w \quad \Longrightarrow \quad Av \perp w.$$

Beweis des Hilfssatzes: Sei $\alpha \in]0,1]$, $\beta_\alpha := \sqrt{1-\alpha^2}$ und $x_\alpha := \beta_\alpha v + \alpha w$. Es gilt:

$$v, w \in S^{n-1} \overset{\text{Def } S^{n-1}}{\Longrightarrow} \|v\|_2 = \|w\|_2 = 1 \overset{4.1.20}{\Longrightarrow} \langle v, v\rangle_2 = \langle w, w\rangle_2 = 1,$$

und mit $\beta_\alpha^2 + \alpha^2 = 1$ und $\langle v, w\rangle_2 = 0$ wegen $v \perp w$ folgt $x_\alpha \in S^{n-1}$:

$$\|x_\alpha\|_2 = \sqrt{\langle x_\alpha, x_\alpha\rangle_2} = \sqrt{\langle \beta_\alpha v + \alpha w, \beta_\alpha v + \alpha w\rangle_2} = \sqrt{\beta_\alpha^2 \cdot \langle v, v\rangle_2 + \alpha^2 \cdot \langle w, w\rangle_2} = 1.$$

Nun gilt nach der Wahl von v wegen $x_\alpha \in S^{n-1}$ die Ungleichung:

$$q_A(v) \geq q_A(x_\alpha) \quad \Longrightarrow \quad \langle v, Av\rangle_2 \geq \langle x_\alpha, Ax_\alpha\rangle_2. \tag{$*_1$}$$

Da $\langle\,\cdot,\cdot\,\rangle_2$ und A symmetrisch sind, gilt:

$$\langle \beta_\alpha v, \alpha Aw\rangle_2 \overset{(\langle\cdot,\cdot\rangle_2 \text{ sym.})}{=} \langle \alpha Aw, \beta_\alpha v\rangle_2 \overset{(4.1.50)}{=} \langle \alpha w, \beta_\alpha Av\rangle_2, \tag{$*_2$}$$

so daß für $\langle x_\alpha, Ax_\alpha\rangle_2$ folgt:

$$\begin{aligned}
\langle x_\alpha, Ax_\alpha\rangle_2 &= \langle \beta_\alpha v + \alpha w, A(\beta_\alpha v + \alpha w)\rangle_2 \\
&= \langle \beta_\alpha v, \beta_\alpha Av\rangle_2 + \langle \alpha w, \beta_\alpha Av\rangle_2 + \underbrace{\langle \beta_\alpha v, \alpha Aw\rangle_2}_{=\langle \alpha w, \beta_\alpha Av\rangle_2 \ (*_2)} + \langle \alpha w, \alpha Aw\rangle_2 \\
&= \beta_\alpha^2 \cdot \langle v, Av\rangle_2 + 2\alpha\beta_\alpha \cdot \langle w, Av\rangle_2 + \alpha^2 \cdot \langle w, Aw\rangle_2.
\end{aligned} \tag{$*_3$}$$

Zusammengefaßt liefern dann $(*_1)$ und $(*_3)$, da Ungleichungen durch $\alpha > 0$ geteilt werden dürfen:

$$\begin{aligned}
& \langle v, Av\rangle_2 \geq \beta_\alpha^2 \cdot \langle v, Av\rangle_2 + 2\alpha\beta_\alpha \cdot \langle w, Av\rangle_2 + \alpha^2 \cdot \langle w, Aw\rangle_2 \\
\Longrightarrow \quad & \langle v, Av\rangle_2 - \underbrace{\beta_\alpha^2}_{=1-\alpha^2} \cdot \langle v, Av\rangle_2 \geq 2\alpha\beta_\alpha \cdot \langle w, Av\rangle_2 + \alpha^2 \cdot \langle w, Aw\rangle_2 \\
\Longrightarrow \quad & \alpha^2 \cdot \langle v, Av\rangle_2 \geq 2\alpha\beta_\alpha \cdot \langle w, Av\rangle_2 + \alpha^2 \cdot \langle w, Aw\rangle_2 \\
\Longrightarrow \quad & \alpha^2 \cdot \big(\langle v, Av\rangle_2 - \langle w, Aw\rangle_2\big) \geq 2\alpha\beta_\alpha \cdot \langle w, Av\rangle_2 \\
\overset{\alpha>0}{\Longrightarrow} \quad & \alpha \cdot \big(\langle v, Av\rangle_2 - \langle w, Aw\rangle_2\big) \geq 2\beta_\alpha \cdot \langle w, Av\rangle_2.
\end{aligned} \tag{$*_4$}$$

Sei $\varepsilon \in \{\pm 1\}$. Dann folgt aus $w \in S^{n-1}$ und $v \perp w$ sofort $\varepsilon w \in S^{n-1}$ und $v \perp \varepsilon w$, so daß die Abschätzung $(*_4)$ auch für εw hergeleitet werden kann:

$$\alpha \cdot \big(\langle v, Av\rangle_2 - \langle \varepsilon w, A(\varepsilon w)\rangle_2\big) \geq 2\beta_\alpha \cdot \langle \varepsilon w, Av\rangle_2. \tag{$*_5$}$$

Dabei gelten die Identitäten:

$$\varepsilon \cdot \langle w, Av\rangle_2 = \langle \varepsilon w, Av\rangle_2 \quad \text{und} \quad \langle w, Aw\rangle_2 = \big\langle \varepsilon w, A(\varepsilon w)\big\rangle_2,$$

und mit $\varepsilon := \operatorname{sign}\big(\langle w, Av\rangle_2\big)$ und $\widetilde{w} := \varepsilon w$ folgt aus $(*_4)$ und $(*_5)$ dann die Ungleichungskette:

$$\alpha \cdot \underbrace{\big(\langle v, Av\rangle_2 - \langle w, Aw\rangle_2\big)}_{=:K_{v,w}} \geq 2\beta_\alpha \cdot \langle \widetilde{w}, Av\rangle \geq 0, \tag{$*_6$}$$

wobei $K_{v,w}$ eine von v und w abhängige Konstante größer gleich Null ist.
Die Ungleichungskette $(*_6)$ gilt für alle $\alpha \in]0,1]$. In der Ungleichungskette $(*_6)$ kann nun der Grenzwert für $\alpha \to 0$ gebildet werden, wobei dann $\beta_\alpha \to 1$ gilt, und es folgt letztendlich:

$$0 \geq 2 \cdot \langle \widetilde{w}, Av\rangle_2 \geq 0 \quad \Longrightarrow \quad \langle \widetilde{w}, Av\rangle_2 = 0.$$

Zu guter letzt liefert dies die gewünschte Hilfsaussage:

$$0 = \langle \widetilde{w}, Av\rangle_2 \overset{\text{(s.o.)}}{=} \varepsilon \cdot \langle w, Av\rangle_2 \quad \Longrightarrow \quad \langle w, Av\rangle_2 = 0 \quad \Longrightarrow \quad Av \perp w.$$

Nachdem der Hilfsatz bewiesen ist, wird nun gezeigt, daß ein $v \in S^{n-1}$, auf dem $q_{A|_{S^{n-1}}}$ sein Maximum annimmt, ein Eigenvektor zum Eigenwert $\max(q_{A|_{S^{n-1}}})$ ist. Sei dazu U das orthogonale Komplement des von v erzeugten Unterraumes: $U := \langle v\rangle^\perp$. Nach dem Hilfssatz gilt für alle $w \in U \cap S^{n-1}$ wegen $w \perp v = 0$:

$$w \perp Av = 0 \quad \Longrightarrow \quad \langle w, Av\rangle_2 = 0,$$

so daß für alle $u \in U$ folgt:

$$\langle u, Av\rangle_2 = \|u\|_2 \cdot \langle \underbrace{\tfrac{1}{\|u\|_2} \cdot u}_{\in U \cap S^{n-1}}, Av\rangle_2 = \|u\|_2 \cdot 0 = 0 \quad \Longrightarrow \quad Av \in U^\perp.$$

und da nach Lemma 4.1.33 $U^\perp = \langle v\rangle$ gilt, ist Av ein Vielfaches von v: $Av = \lambda v$ mit $\lambda \in \mathbb{R}$. Für λ folgt dann wegen $\|v\|_2 = 1 \implies \langle v, v\rangle_2 = 1$:

$$Av = \lambda v \quad \Longrightarrow \quad \langle v, Av\rangle_2 = \langle v, \lambda v\rangle_2 = \lambda \cdot \langle v, v\rangle = \lambda,$$

so daß $\langle v, Av\rangle_2 = q_A(v)$ ein Eigenwert von A mit dem Eigenvektor v ist (wegen $\|v\|_2 = 1$ ist natürlich $v \neq 0$).
Es muß jetzt nur noch gezeigt werden, daß der Eigenwert $\langle v, Av\rangle = q_A(v)$ der größte Eigenwert von A ist. Sei dazu μ ein weiterer Eigenwert von A, und $x \neq 0$ ein Eigenvektor. Dann ist auch $\widetilde{x} := \frac{1}{\|x\|_2} x \in S^{n-1}$ ein Eigenvektor zum Eigenwert μ, und es gilt:

$$q_A(\widetilde{x}) = \langle \widetilde{x}, A\widetilde{x}\rangle_2 = \langle \widetilde{x}, \mu\widetilde{x}\rangle_2 = \mu \cdot \langle \widetilde{x}, \widetilde{x}\rangle_2 = \mu,$$

d.h. μ liegt im Bild von $q_{A|_{S^{n-1}}}$ und ist daher kleiner gleich dessen Maximum, also:

$$\mu \leq \max(q_{A|_{S^{n-1}}}) = q_A(v). \qquad \square$$

Satz 4.1.53. *Sei $A \in \mathrm{GL}_n(\mathbb{R})$. Dann sind folgende Aussagen äquivalent:*

i.) Die Spalten von A sind eine Orthonormalbasis des $\mathbb{R}^{[n]}$ bzgl. des Standard-Skalarproduktes $\langle \cdot, \cdot \rangle_2$.
ii.) Die Zeilen von A sind eine Orthonormalbasis des $\mathbb{R}^{[n]}$ bzgl. des Standard-Skalarproduktes $\langle \cdot, \cdot \rangle_2$.
iii.) $A^{-1} = A^t$.

Beweis. TBA. $\square$

Definition 4.1.54. *Eine Matrix $A \in \mathrm{GL}_n(\mathbb{R})$ heißt orthogonale Matrix, falls sie eine und damit alle der äquivalenten Bedingungen aus Satz 4.1.53 erfüllt, d.h. wenn z.B. gilt:*

$$A^t = A^{-1}. \qquad \square$$

Satz 4.1.55. *(Hauptachsentransformationssatz)*
Sei $A \in \mathrm{Mat}_n(\mathbb{R})$ eine symmetrische Matrix. Dann gilt:

i.) A ist diagonalisierbar.

ii.) Für die Eigenräume $\mathrm{Eig}(A, \lambda_1), \ldots, \mathrm{Eig}(A, \lambda_k)$ von A gilt:

$$\mathrm{Eig}(A, \lambda_i) \perp \mathrm{Eig}(A, \lambda_j) \quad \text{für} \quad i \neq j.$$

iii.) Es gibt eine Basis aus Eigenvektoren von A, die bzgl. des Standard-Skalarproduktes $\langle \cdot, \cdot \rangle_2$ des $\mathbb{R}^{[n]}$ eine Orthonormalbasis ist.

iv.) Es gibt eine Matrix $S \in \mathrm{GL}_n(\mathbb{R})$ mit $S^{-1} = S^t$ und eine Diagonalmatrix D, so daß gilt:

$$S^{-1}AS = S^tAS = D.$$

Dabei sind die Diagonaleinträge von D die Eigenwerte von A.
Dies wird auch formuliert als:

„A ist diagonalisierbar durch eine orthogonale Matrix“.

Beweis. TBA. $\square$

Satz 4.1.56. *Sei $A \in \mathrm{Mat}_n(\mathbb{R})$ eine symmetrische Matrix. Dann sind äquivalent:*

i.) A ist positiv definit.

ii.) Alle Eigenwerte von A sind positiv, d.h. es gilt:

$$\lambda \text{ Eigenwert von } A \quad \Longrightarrow \quad \lambda > 0.$$

iii.) Für das charakteristische Polynom $\chi_A(t) := t^n + \sum_{i=0}^{n-1} a_i t^i$ gilt:

$$(-1)^{n-i} \cdot a_i > 0.$$

Beweis. TBA. $\square$

Bemerkung 4.1.57.

i.) Sei $A \in \mathrm{Mat}_2(\mathbb{R})$ symmetrisch. Nach Bemerkung 3.3.54 gilt (für jede (2×2)-Matrix):

$$\chi_A(t) = t^2 - \mathrm{sp}(A) \cdot t + \det(A),$$

und mit Satz 4.1.56 folgt dann sofort:

$$A \text{ positiv definit} \quad \Longleftrightarrow \quad \mathrm{sp}(A) > 0, \quad \det(A) > 0.$$

ii.) Sei $A := \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathbb{R})$ symmetrisch. Dann ist es eine leichte Übung zu zeigen:

$$ac - b^2 > 0, \quad a + c > 0 \quad \Longleftrightarrow \quad ac - b^2 > 0, \quad a > 0,$$

und es folgt sofort mit $\mathrm{sp}(A) = a + c$ und $\det(A) = ac - b^2$ aus vorheriger Aussage:

$$A \text{ positiv definit} \quad \Longleftrightarrow \quad a > 0, \quad \det(A) > 0.$$

Dieses Kriterium für die positive Definitheit einer (2×2)-Matrix ist ein Spezialfall des Hauptminoren-Kriteriums, das hier nicht bewiesen wird:

Satz: *Sei* $A \in \mathrm{Mat}_n(\mathbb{R})$ *eine symmetrische Matrix, und es seien* $A_1, \ldots, A_n$ *die Untermatrizen mit:*

$$A_i := \begin{pmatrix} a_{1,1} & \ldots & a_{1,i} \\ \vdots & & \vdots \\ a_{i,1} & \ldots & a_{i,i} \end{pmatrix} \in \mathrm{Mat}_k(\mathbb{R}) \qquad \textit{mit} \qquad A := \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{pmatrix} \in \mathrm{Mat}_n(\mathbb{R}).$$

Die A_i *sind also die* $(i \times i)$*-Blöcke links oben in der Matrix* A*, und insbesondere* $A_1 = (a_{i,i})$ *und* $A_n = A$*. Dann gilt:*

$$A \textit{ positiv definit} \quad \Longleftrightarrow \quad \det(A_i) > 0 \textit{ für } 1 \leq i \leq n. \qquad \square$$

ANHANG A

Lineare Algebra I und IIa

A.1. Allgemeines Assoziativ- und Kommutativgesetz

Es wird nun gezeigt, daß in assoziativen algebraischen Strukturen $(M, *)$ das „allgemeine Assoziativgesetz“ für beliebig große (endliche) Klammerausdrücke gilt und damit die Klammern in Verknüpfungen weggelassen werden können. Dazu muß ersteinmal für algebraische Strukturen $(M, *)$ formalisert werden, was überhaupt die Verknüpfung mehrerer Elemente sein soll:

Definition A.1.1. *Sei $(M, *)$ eine algebraische Struktur, und seien $a_1, \ldots, a_n \in M$. Dann ist für $n \in \mathbb{N}$ eine n-stellige innere Verknüpfung $P\colon M^n \longrightarrow M$ rekursiv definiert durch:*

$$\begin{aligned} n = 1: &\quad P(a_1) := a_1 \\ n \geq 2: &\quad P(a_1, \ldots, a_n) = Q(a_1, \ldots, a_i) * \widetilde{Q}(a_{i+1}, \ldots, a_n) \\ &\quad \text{mit } i, j \in \mathbb{N},\ i + j = n \text{ und einer } i\text{-stelligen Verknüpfung } Q \\ &\quad \text{und einer } j\text{-stelligen Verknüpfung } \widetilde{Q}. \end{aligned}$$

Mit $\mathcal{V}_n(M)$ ist die Menge aller n-stelligen inneren Verknüpfungen auf M bezeichnet. Die n-stellige innere Standardverknüpfung $P_{St}^{(n)}$ ist rekursiv definiert durch:

$$\begin{aligned} n = 1: &\quad P_{St}^{(1)}(a_1) := a_1. \\ n \geq 2: &\quad P_{St}^{(n)}(a_1, \ldots, a_n) := P_{St}^{(n-1)}(a_1, \ldots, a_{n-1}) * P_{St}^{(1)}(a_n) \\ &\qquad\qquad\qquad\qquad\qquad\qquad = P_{St}^{(n-1)}(a_1, \ldots, a_{n-1}) * a_n. \end{aligned}$$

□

Bemerkung A.1.2.

i.) Sei $(M, *)$ eine algebraische Struktur. Dann gilt:

$$\mathcal{V}_1(M) = \{\mathrm{id}_M\} = \{P_{St}^{(1)}\} \quad \text{und} \quad \mathcal{V}_2(M) = \{(a_1, a_2) \mapsto a_1 * a_2\} = \{P_{St}^{(2)}\}.$$

Für $n = 3$ gibt es folgende Fallunterscheidung:

„$*$“ *assoziativ* $\quad\Longrightarrow\quad \mathcal{V}_3(M) = \{P_{St}^{(3)}\}$,

„$*$“ *nicht assoziativ* $\quad\Longrightarrow\quad \mathcal{V}_3(M) = \{P_{St}^{(3)}, (a_1, a_2, a_3) \mapsto a_1 * (a_2 * a_3)\}$.

ii.) Für $n = 2$ ist die Definition einer „zweistelligen“ inneren Verknüpfung exakt die Definition einer inneren Verknüpfung aus Definition 1.1.1. □

Ziel ist nun zu zeigen, daß in einer assoziativen algebraischen Struktur $(M, *)$ für alle $n \in \mathbb{N}$ die Aussage $\mathcal{V}_n(M) = \{P_{St}^{(n)}\}$ gilt (siehe den assoziativen Fall $n = 3$ in Bemerkung A.1.2), also jedwede Klammerung bei Verknüpfungen von mehreren Elementen das gleiche Ergebnis liefert und damit eine Klammerung auch weggelassen werden kann. Ein wichtiger Schritt dahin ist:

LEMMA A.1.3. *Sei $(M,*)$ eine assoziative algebraische Struktur. Weiter sei $n \geq 2$, und es seien $a_1, \ldots, a_n \in M$. Dann gilt für alle $1 \leq i < n$ mit $j := n - i$:*

$$P_{St}^{(n)}(a_1, \ldots, a_n) = P_{St}^{(i)}(a_1, \ldots, a_i) * P_{St}^{(j)}(a_{i+1}, \ldots, a_n).$$

BEWEIS. Der Beweis wird durch Induktion über n geführt.

Induktionsanfang $n = 2$: Es ist nur der Fall $i = j = 1$ zu betrachten:

$$P_{St}^{(2)}(a_1, a_2) \overset{\text{(Def)}}{=} P_{St}^{(1)}(a_1) * P_{St}^{(1)}(a_2).$$

Induktionsschritt $n \rightsquigarrow n+1$: Es ist für alle $1 \leq i \leq n$ mit $j := n+1-i$ zu zeigen:

$$P_{St}^{(n+1)}(a_1, \ldots, a_{n+1}) = P_{St}^{(i)}(a_1, \ldots, a_i) * P_{St}^{(j)}(a_{i+1}, \ldots, a_{n+1}).$$

Der Fall $i = n$ ist nichts anderes als die rekursive Definition von $P_{St}^{(n+1)}$ aus Definition A.1.1.
Für $i < n$ gilt $j - 1 = n - i \in \mathbb{N}$ und $n = i + (j-1)$, und es folgt per Induktion:

$$\begin{aligned} P_{St}^{(n+1)}(a_1, \ldots, a_{n+1}) &\overset{\text{(Def)}}{=} P_{St}^{(n)}(a_1, \ldots, a_n) * a_{n+1} \\ &\overset{\text{(IAnn)}}{=} \left(P_{St}^{(i)}(a_1, \ldots, a_i) * P_{St}^{(j-1)}(a_{i+1}, \ldots, a_n)\right) * a_{n+1} \\ &\overset{\text{(Ass)}}{=} P_{St}^{(i)}(a_1, \ldots, a_i) * \left(P_{St}^{(j-1)}(a_{i+1}, \ldots, a_n) * a_{n+1}\right) \\ &\overset{\text{(Def)}}{=} P_{St}^{(i)}(a_1, \ldots, a_i) * P_{St}^{(j)}(a_{i+1}, \ldots, a_{n+1}) \end{aligned}$$ □

Nun kann leicht das allgemeine Assoziativgesetz für assoziative algebraische Strukturen $(M,*)$ formuliert werden:

SATZ A.1.4. *(Allgemeines Assoziativgesetz)*
Sei $(M,*)$ eine assoziative algebraische Struktur. Dann ist $\mathcal{V}_n(M) = \{P_{St}^{(n)}\}$, d.h. alle möglichen Klammerungen in Verknüpfungen von n Elementen aus M liefern das gleiche Ergebnis.

BEWEIS.
Der Beweis wird durch Induktion über n geführt:

Induktionsanfang $n = 1$: Bemerkung A.1.2.

Induktionsschritt $n \rightsquigarrow n+1$: Sei $P \in \mathcal{V}_{n+1}(M)$. Nach Definition A.1.1 gibt es dann $i, j \in \mathbb{N}$ mit $i + j = n + 1$ und

$$P(a_1, \ldots, a_{n+1}) = Q(a_1, \ldots, a_i) * \widetilde{Q}(a_{i+1}, \ldots, a_{n+1}),$$

wobei Q eine i-stellige und $\widetilde{Q}$ eine j-stellige innere Verknüpfung auf M ist mit $i, j \leq n$. Nach der Induktionsannahme gilt $Q = P_{St}^{(i)}$ und $\widetilde{Q} = P_{St}^{(j)}$, und aus Lemma A.1.3 folgt dann sofort:

$$P(a_1, \ldots, a_{n+1}) = P_{St}^{(i)}(a_1, \ldots, a_i) * P_{St}^{(j)}(a_{i+1}, \ldots, a_{n+1}) \overset{\text{(A.1.3)}}{=} P_{St}^{(n+1)}(a_1, \ldots, a_{n+1}).$$ □

Bemerkung A.1.5. *Für die Menge $|\mathcal{V}_n(M)|$ gilt folgende Abschätzung:*

$$|\mathcal{V}_n(M)| = \sum_{i=1}^{n-1} |\mathcal{V}_i(M)| \cdot |\mathcal{V}_{n-i}(M)| \leq \frac{(2n-2)!}{n!(n-1)!}.$$

Dabei ist $\frac{(2n-2)!}{n!(n-1)!} = \frac{1}{n}\binom{2n-2}{n-1}$ die Anzahl der möglichen Klammerungen für n Elemente aus einer algebraischen Struktur $(M, *)$.
Ein Beweis findet sich im z.B. im Skript [**PanDM**, Seite 6–8]. □

Damit kann nun in einer assoziativen algebraischen Struktur $(M, *)$ die Verknüpfung von mehreren Elementen definiert werden:

Definition A.1.6. *Sei $(M, *)$ eine assoziative algebraische Struktur. Dann wird für n Elemente $a_1, \ldots, a_n \in M$ deren Verknüpfung definiert durch:*

$$\prod_{i=1}^{n} a_i := P_{St}^{(n)}(a_1, \ldots, a_n) \qquad \text{(salopp auch: } a_1 * \cdots * a_n := \prod_{i=1}^{n} a_i\text{).}$$

Bei Verwendung des Verknüpfungssymbols „+ “ wird die Verknüpfung von $a_1, \ldots, a_n$ mit $\sum_{i=1}^{n} a_i$ notiert. □

Es kann auch ein allgemeines Kommutativgesetz für kommutative und assoziative algebraische Strukturen $(M, *)$ per Induktion bewiesen werden. Dabei ermöglicht die Assoziativität, wie vorher gesehen, ersteinmal eine vernünftige Definition eines Produktes mehrerer Elemente, für das dann ein allgemeines Kommutativgesetz gezeigt werden kann.

Satz A.1.7. *(Allgemeines Kommutativgesetz)*
Sei $(M, *)$ eine kommutative und assoziative algebraische Struktur. Weiter seien $a_1, \ldots, a_n \in M$. Dann gilt für alle $f \in S_n$:

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{f(i)}.$$

Beweis. Der Beweis wird durch Induktion über n geführt:

Induktionsanfang $n = 1$: Klar, denn es gibt nur $f = \mathrm{id}$.

Induktionsschritt $n \rightsquigarrow n+1$: Sei $f \in S_{n+1}$. Dann gibt es ein $k \in \{1, \ldots, n+1\}$ mit $f(k) = n+1$.

Ist $k = n+1$, d.h. $f(n+1) = n+1$, so gilt $\tilde{f} := f|_{\{1,\ldots,n\}} \in S_n$, und es folgt sofort aus der Induktionsannahme:

$$\prod_{i=1}^{n+1} a_{f(i)} = \Big(\prod_{i=1}^{n} a_{f(i)}\Big) * a_{f(n+1)} = \Big(\prod_{i=1}^{n} a_{\tilde{f}(i)}\Big) * a_{n+1} \overset{\text{(IAnn)}}{=} \Big(\prod_{i=1}^{n} a_i\Big) * a_{n+1} = \prod_{i=1}^{n+1} a_i.$$

Ist $k < n+1$, so gilt:

$$\prod_{i=1}^{n+1} a_{f(i)} = \Big(\prod_{i=1}^{k} a_{f(i)}\Big) * \Big(\prod_{i=k+1}^{n+1} a_{f(i)}\Big) \overset{\text{(Komm)}}{=} \Big(\prod_{i=k+1}^{n+1} a_{f(i)}\Big) * \Big(\prod_{i=1}^{k} a_{f(i)}\Big)$$

$$\overset{f(k)=n+1}{=} \Big(\prod_{i=k+1}^{n+1} a_{f(i)}\Big) * \Big(\Big(\prod_{i=1}^{k-1} a_{f(i)}\Big) * a_{f(k)}\Big) \overset{\text{(Ass)}}{=} \Big(\prod_{i=k+1}^{n+1} a_{f(i)} * \prod_{i=1}^{k-1} a_{f(i)}\Big) * a_{n+1}$$

$$\overset{\text{(Komm)}}{=} \Big(\prod_{i=1}^{k-1} a_{f(i)} * \prod_{i=k+1}^{n+1} a_{f(i)}\Big) * a_{n+1} = \Big(\prod_{\substack{i=1\\ i\neq k}}^{n+1} a_{f(i)}\Big) * a_{n+1}.$$

Es sei folgende Abbildung definiert:

$$\varphi\colon \{1,\dots,n\} \longrightarrow \{1,\dots,n\} \quad \text{mit} \quad i \mapsto \begin{cases} f(i) & \text{für } i < k, \\ f(i+1) & \text{für } i \geq k. \end{cases}$$

Dann ist $\varphi \in S_n$ und $\prod\limits_{\substack{i=1\\ i\neq k}}^{n+1} a_{f(i)} = \prod\limits_{i=1}^{n} a_{\varphi(i)}$, und es folgt per Induktion:

$$\prod_{i=1}^{n+1} a_{f(i)} = \Big(\prod_{\substack{i=1\\ i\neq k}}^{n+1} a_{f(i)}\Big) * a_{n+1} = \Big(\prod_{i=1}^{n} a_{\varphi(i)}\Big) * a_{n+1} \overset{\text{(IAnn)}}{=} \Big(\prod_{i=1}^{n} a_i\Big) * a_{n+1} = \prod_{i=1}^{n+1} a_i. \quad \square$$

A.2. Potenzgesetze in Monoiden

Als nächstes sollen Potenzen in Monoiden definiert und Rechengesetze dazu hergeleitet werden:

Definition A.2.1. *Sei $(M,*)$ ein Monoid mit dem neutralen Element e. Für $a \in M$ und $n \in \mathbb{N}_0$ sei die n-te Potenz definiert als:*

$$a^0 := e \quad \textit{und} \quad a^n := \prod_{i=1}^{n} a \textit{ für } n \in \mathbb{N}.$$

Ist a invertierbar, so sei für $n < 0$ definiert:

$$a^n := (a^{-1})^{|n|}.$$

Wird die Verknüpfung „$+$“ benutzt, so wird für $n \in \mathbb{N}_0$ (oder auch $n \in \mathbb{Z}$) die n-te Potenz von a als n-fache Verknüpfung von a mit sich selbst mit $n \bullet a$ geschrieben. $\square$

Bemerkung A.2.2.

i.) In den Gruppen $(\mathbb{Z},+)$, $(\mathbb{Q},+)$ und $(\mathbb{R},+)$ stimmt dann für $n \in \mathbb{Z}$ und a aus einer der Gruppen $n \bullet a$ mit dem Produkt $n \cdot a$, der „normalen“ Multiplikation mit n, überein. Allerdings muß dabei auf die Reihenfolge der „Faktoren“ geachtet werden, denn es ist zwar $3 \bullet \pi = \pi + \pi + \pi$ definiert, aber nicht $\pi \bullet 3$.
In $(\mathbb{Z},+)$ gibt es gar keinen Unterschied zwischen „$\bullet$“ und „$\cdot$“. Es gilt für alle $a, b \in \mathbb{Z}$:

$$a \bullet b = b \bullet a = a \cdot b = b \cdot a.$$

ii.) Für ein invertierbares Element a in einem Monoid gilt dann für $k \in \mathbb{Z}$ und $\varepsilon_k := \operatorname{sign}(k)$:

$$a^k = (a^{\varepsilon_k})^{|k|}. \qquad \square$$

Lemma A.2.3. *Sei $(M,*)$ ein Monoid mit dem neutralen Element e und $a \in M$ invertierbar. Dann gilt für $k \in \mathbb{Z}$:*

$$a^{-k} = (a^{-1})^k = (a^k)^{-1}.$$

Insbesondere gilt dann $a^k * a^{-k} = e$ für alle $k \in \mathbb{Z}$.

Beweis. Sei e das neutrale Element in M. Dann ist $a^0 = e$ für alle $a \in M$ und $e^{-1} = e$, so daß für $k = 0$ die Gleichungen gelten.

$a^{-k} = (a^{-1})^k$:

$k > 0$: Dies ist Definition A.2.1.

$k < 0$: Die Gleichung folgt aus Lemma 1.1.25:

$$(a^{-1})^k \overset{(A.2.1)}{=} \left((a^{-1})^{-1}\right)^{-k} \overset{(1.1.25)}{=} a^{-k}.$$

$(a^{-1})^k = (a^k)^{-1}$:

$k > 0$: Die Behauptung wird per Induktion über k gezeigt:

Induktionsanfang $k = 1$: klar.

Induktionsschritt $k \rightsquigarrow k + 1$: Es gilt:

$$(a^{-1})^{k+1} \overset{(A.2.1)}{=} (a^{-1})^k * a^{-1} \overset{(IAnn)}{=} (a^k)^{-1} * a^{-1} \overset{(1.1.25)}{=} (a * a^k)^{-1} = (a^{k+1})^{-1}.$$

$k < 0$: Es folgt:

$$(a^{-1})^k \overset{(A.2.1)}{=} \left((a^{-1})^{-1}\right)^{-k} \overset{(-k>0)}{=} \left((a^{-1})^{-k}\right)^{-1} \overset{(A.2.1)}{=} (a^k)^{-1}.$$ □

Definition A.2.4. *Sei $(M, *)$ eine Halbgruppe. $a, b \in M$ kommutieren, falls gilt:*

$$a * b = b * a.$$ □

Lemma A.2.5. *Sei $(M, *)$ ein Monoid, und $a, b \in M$ kommutieren. Dann gilt für alle $n, m \in \mathbb{N}_0$:*

$$a^n * b^m = b^m * a^n.$$

Falls a und b invertierbar sind, gilt diese Aussage für alle $n, m \in \mathbb{Z}$.

Beweis. Für $n = 0$ oder $m = 0$ ist die Aussage klar.

$n, m \in \mathbb{N}$: Zuerst wird die Aussage für $m = 1$, also $a^n * b = b * a^n$ per Induktion über n gezeigt:

Induktionsanfang $n = 1$: klar.

Induktionsschritt $n \rightsquigarrow n + 1$: Es gilt:

$$a^{n+1} * b = a^n * (a * b) = a^n * (b * a) = (a^n * b) * a \overset{(IAnn)}{=} (b * a^n) * a = b * a^{n+1}.$$

Nun wird die Aussage $a^n * b^m = b^m * a^n$ für beliebiges $n \in \mathbb{N}$ per Induktion über m gezeigt:

Induktionsanfang $m = 1$: Dies ist genau die vorherige Aussage.

Induktionsschritt $m \rightsquigarrow m + 1$: Es gilt:

$$a^n * b^{m+1} = a^n * (b^m * b) = (a^n * b^m) * b \overset{(IAnn)}{=} (b^m * a^n) * b = b^m * (a^n * b)$$
$$\overset{(s.o.)}{=} b^m * (b * a^n) = b^{m+1} * a^n.$$

Nun zu dem Fall, daß a und b invertierbar sind: zuerst wird gezeigt, daß dann a^{ε_1} und b^{ε_2} für alle $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ kommutieren.

$(\varepsilon_1, \varepsilon_2) = (1, 1)$: Dies ist die Voraussetzung über a und b.

$(\varepsilon_1, \varepsilon_2) = (-1, -1)$: Es gilt:

$$a^{-1} * b^{-1} \overset{(1.1.25)}{=} (b * a)^{-1} \overset{(Vor)}{=} (a * b)^{-1} \overset{(1.1.25)}{=} b^{-1} * a^{-1}.$$

$(\varepsilon_1, \varepsilon_2) = (-1, 1)$: Es gilt:

$$\left.\begin{aligned} (a^{-1} * b) * (a * b^{-1}) &\overset{(\text{Vor})}{=} a^{-1} * (a * b) * b^{-1} = e \\ (a * b^{-1}) * (a^{-1} * b) &\overset{(-1,-1)}{=} a * (a^{-1} * b^{-1}) * b = e \end{aligned}\right\} \Longrightarrow a^{-1} * b = (a * b^{-1})^{-1} = b * a^{-1}.$$

$(\varepsilon_1, \varepsilon_2) = (1, -1)$: Es gilt:

$$\left.\begin{aligned} (a * b^{-1}) * (a^{-1} * b) &\overset{(-1,-1)}{=} a * (a^{-1} * b^{-1}) * b = e \\ (a^{-1} * b) * (a * b^{-1}) &\overset{(\text{Vor})}{=} a^{-1} * (a * b) * b^{-1} = e \end{aligned}\right\} \Longrightarrow a * b^{-1} = (a^{-1} * b)^{-1} = b^{-1} * a.$$

Für den allgemeinen Fall $n, m \in \mathbb{Z}$ sei nun gesetzt:

$$\varepsilon_n := \operatorname{sign}(n) \quad \text{und} \quad \varepsilon_m := \operatorname{sign}(m) \qquad \Longrightarrow \qquad a = \left(a^{\varepsilon_n}\right)^{|n|} \quad \text{und} \quad b = \left(b^{\varepsilon_m}\right)^{|m|}.$$

Es gilt $|n|, |m| \in \mathbb{N}_0$, und a^{ε_n} und b^{ε_m} kommutieren nach vorheriger Aussage, so daß folgt:

$$a^n * b^m = \left(a^{\varepsilon_n}\right)^{|n|} * \left(b^{\varepsilon_m}\right)^{|m|} = \left(b^{\varepsilon_m}\right)^{|m|} * \left(a^{\varepsilon_n}\right)^{|n|} = b^m * a^n. \qquad \square$$

Satz A.2.6. *(Potenzgesetze) Sei $(M, *)$ ein Monoid.*

i.) Dann gilt für $a \in M$ und $n, m \in \mathbb{N}_0$:

$$a^n * a^m = a^{n+m}.$$

Ist a invertierbar, so gilt die Aussage für alle $n, m \in \mathbb{Z}$.

ii.) Falls $a, b \in M$ kommutieren, so folgt für alle $n, m \in \mathbb{N}_0$:

$$a^n * b^n = (a * b)^n.$$

Sind a und b beide invertierbar, so gilt die Aussage für alle $n, m \in \mathbb{Z}$.

iii.) Für $a \in M$ und $n, m \in \mathbb{N}_0$ gilt:

$$(a^n)^m = a^{n \cdot m}.$$

Ist a invertierbar, so gilt die Aussage für alle $n, m \in \mathbb{Z}$.

Beweis.

i.) Zuerst wird die Gleichung $a^n * a^m = a^{n+m}$ untersucht.

$n = 0$ oder $m = 0$: Klar.

$n, m > 0$: Die Aussage ist ein Spezialfall des allgemeinen Assoziativgesetzes (1.1.8) mit $a_i := a$:

$$a^n * a^m = \left(\prod_{i=1}^{n} a\right) * \left(\prod_{i=1}^{m}\right) \overset{(1.1.8)}{=} \prod_{i=1}^{n+m} a = a^{n+m}.$$

$n, m < 0$: Es gilt $-n, -m > 0$, und es folgt damit aus dem vorherigen Fall:

$$a^n * a^m = (a^{-1})^{-n} * (a^{-1})^{-m} \overset{(\text{s.o.})}{=} (a^{-1})^{-n-m} = a^{n+m}.$$

$n > 0, m < 0$: Sei $r := n + m$. Dann sind folgende Fälle zu betrachten:

$r \geq 0$: Es gilt $r \geq 0$ und $-m > 0$, und es folgt aus den vorherigen Betrachtungen:

$$a^n * a^m = a^{r+(-m)} * a^m \overset{\substack{r \geq 0 \\ -m > 0}}{=} (a^r * a^{-m}) * a^m = a^r * (a^{-m} * a^m) \overset{(A.2.3)}{=} a^r = a^{n+m}.$$

$r < 0$: Es gilt $r < 0$ und $-n < 0$, und es folgt aus den vorherigen Betrachtungen:

$$a^n * a^m = a^n * a^{-n+r} \overset{\substack{-n<0 \\ r\leq 0}}{=} a^n * (a^{-n} * a^r) = (a^n * a^{-n}) * a^r \overset{(A.2.3)}{=} a^r = a^{n+m}.$$

$n < 0, m > 0$: Weil a mit sich selbst kommutiert, gilt dies nach Lemma A.2.5 auch für a^n und a^m mit $n, m \in \mathbb{Z}$, und es folgt:

$$a^n * a^m = a^m * a^n \overset{\substack{m>0 \\ n<0 \\ \text{s.o.}}}{=} a^{m+n} = a^{n+m}.$$

Damit ist die Aussage $a^n * a^m = a^{n+m}$ für alle Fälle bewiesen.

ii.) Nun zu der Gleichung $(a * b)^n = a^n * b^n$.
$n = 0$: Klar.
$n > 0$: Die Aussage wird per Induktion über n bewiesen:
Induktionsanfang $n = 1$: Klar.
Induktionsschritt $n \rightsquigarrow n + 1$: Da mit a und b auch a und b^n für alle $n \in \mathbb{N}$ kommutieren (Lemma A.2.5), folgt sofort:

$$(a * b)^{n+1} \overset{(\text{Def})}{=} (a * b)^n * (a * b) \overset{(\text{IAnn})}{=} a^n * b^n * a * b \overset{(A.2.5)}{=} a^n * a * b^n * b = a^{n+1} * b^{n+1}.$$

$n < 0$: Mit a und b kommutieren nach Lemma A.2.5 auch a^{-1} und b^{-1}, so daß die Aussage aus dem obigen Fall folgt:

$$(a * b)^n = \left((a * b)^{-1}\right)^{-n} \overset{(A.2.5)}{=} (a^{-1} * b^{-1})^{-n} \overset{\substack{A.2.5 \\ \text{s.o.}}}{=} (a^{-1})^{-n} * (b^{-1})^{-n} = a^n * b^n.$$

Damit ist die Aussage $(a * b)^n = a^n * b^n$ für alle $n \in \mathbb{N}$ bewiesen.

iii.) Nun zu der Aussage $(a^n)^m = a^{n \cdot m}$. Sie wird in Abhängigkeit von m bewiesen, wobei n aus $\mathbb{N}_0$ oder $\mathbb{Z}$ zugelassen ist, je nachem ob a invertierbar ist oder nicht.
$m = 0$: Klar.
$m > 0$: Die Aussage wird per Induktion über m bewiesen:
Induktionsanfang $m = 1$: Klar.
Induktionsschritt $m \rightsquigarrow m + 1$: Es gilt:

$$(a^n)^{m+1} = (a^n)^m * a^n \overset{(\text{IAnn})}{=} a^{n \cdot m} * a^n \overset{\text{i.)}}{=} a^{n \cdot m + n} = a^{n \cdot (m+1)}.$$

$m < 0$: Es gilt mit $-m > 0$:

$$(a^n)^m = \left((a^n)^{-1}\right)^{-m} \overset{(A.2.3)}{=} (a^{-n})^{-m} \overset{\substack{-m>0 \\ \text{i.)}}}{=} a^{(-n)\cdot(-m)} = a^{n \cdot m}.$$

Damit sind alle Potenzgesetze in allen Fällen bewiesen. □

A.3. Die symmetrische Gruppe S_n

Dieser Abschnitt enthält einige vollständige Beweise von Aussagen des Skriptes, die wegen ihrer Länge bzw. wegen ihres technischen Aufwandes vorher nur skizziert oder ganz weggelassen wurden.

Satz A.3.1. *Es sei $M := \{1, \dots, n\}$, $\sigma \in S_n$ und $\sigma \neq \mathrm{id}_M$. Dann existieren eindeutig bestimmte zyklische Permutationen $\sigma_1, \dots, \sigma_k \in S_n$ mit paarweise disjunkten Trägermengen $T_1, \dots, T_k \subseteq M$, so daß sich σ als Produkt der σ_i schreiben läßt:*

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_k.$$

Da zyklische Permutationen mit disjunkten Trägern kommutieren (siehe Bemerkung 0.4.26), ist dieses Produkt nur bis auf die Reihenfolge der σ_i eindeutig.
Wird bzgl. σ die Äquivalenzrelation aus Lemma 1.1.33 betrachtet, so entsprechen die Trägermengen T_i denjenigen Äquivalenzklassen, die keinen Fixpunkt von σ enthalten.

Beweis. Zuerst wird gezeigt, daß es passende σ_i überhaupt gibt, und danach deren Eindeutigkeit.

Existenz der σ_i: Es sei auf der Menge $M = \{1, \dots, n\}$ bzgl. σ die Äquivalenzrelation aus Lemma 1.1.33 betrachtet. Aus den Äquivalenzklassen dieser Relation wird nun eine Zerlegung von σ in ein Produkt von zyklischen Permutationen hergeleitet, die per Konstruktion alle geforderten Bedingungen erfüllt.
Da die Menge M endlich ist, existieren nur endlich viele Äquivalenzklassen, und es seien $T_1, \dots, T_k$ diejenigen Klassen davon mit mehr als nur einem Element. Da alle T_i nach Lemma 1.1.33 invariant sind unter σ, können folgende Permutationen $\sigma_1, \dots \sigma_k \in S_n$ definiert werden:

$$\text{Für } 1 \leq i \leq k \text{ sei} \qquad \sigma_i(j) := \begin{cases} \sigma(j) & \text{für } j \in T_i, \\ j & \text{sonst,} \end{cases}$$

also $\sigma_{i|_{T_i}} = \sigma_{|_{T_i}}$ und $\sigma_{i|_{M \setminus T_i}} = \mathrm{id}_{M \setminus T_i}$.
Jedes σ_i bewegt per Definition nur die Äquivalenzklasse T_i und verhält sich darauf wie σ, und da alle Punkte außerhalb der Klassen $T_1, \dots, T_k$ Fixpunkte sind, ergibt sich sofort die Zerlegung:

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_k.$$

Es bleibt zu zeigen, daß jedes σ_i eine zyklische Permutationen mit der jeweiligen Trägermenge T_i ist. Um Mehrfachindizes zu vermeiden, sei für ein gewähltes i bezeichnet: $f := \sigma_i$ und $T := T_i$.
Für $x \in T$ gilt $T = [x]$, und es sei die folgende Folge betrachtet:

$$x, f(x), f^2(x), f^3(x) \dots$$

Da die Menge T endlich ist, muß es $r, s \in \mathbb{N}_0$ geben mit $r < s$ und $f^r(x) = f^s(x)$, und es folgt:

$$f^r(x) = f^s(x) \implies f^{-r}\big(f^r(x)\big) = f^{-r}\big(f^s(x)\big) \implies x = f^0(x) = f^{s-r}(x)$$

mit $s - r \in \mathbb{N}$. Also ist die Menge $\{\, m \in \mathbb{N} \mid f^m(x) = x \,\}$ nicht leer. Ist $t \in \mathbb{N}$ ihr Minimimum, so folgt aus der vorherigen Implikation:

$$x, f(x), f^2(x), \dots, f^{t-1}(x) \text{ sind paarweise verschieden} \quad \text{und} \quad f^t(x) = x.$$

Offensichtlich gilt nach der Äquivalenzrelation $\{x, f(x), \dots, f^{t-1}(x)\} \subseteq [x]$, und wenn sogar die Gleichheit beider Mengen gilt, ist f eine zyklische Permutation mit der Trägermenge $[x]$ bzw. T.
Für ein $y \in [x]$ gilt $y = f^s(x)$ mit einem $s \in \mathbb{Z}$. Nach der Division mit Rest gibt es $q, r \in \mathbb{Z}$ mit $s = q \cdot t + r$ und $0 \leq r < t$. Ist $s < 0$, so folgt wegen $t > 0$ dann

$q < 0$. Sei $\tilde{t} := \operatorname{sign}(q) \cdot t$. Es gilt dann $q \cdot t = |q| \cdot \tilde{t}$, und aus $f^t(x) = x$ und damit $f^{-t}(x) = x$ folgt $f^{\tilde{t}}(x) = x$ und letztendlich:

$$f^{q \cdot t}(x) = f^{\tilde{t} \cdot |q|} = (f^{\tilde{t}})^{|q|}(x) = \underbrace{f^{\tilde{t}}\Big(f^{\tilde{t}}\Big(\dots\big(\underbrace{f^{\tilde{t}}(x)}_{=x}\big)\Big)\Big)}_{|q| \text{ mal}} = x.$$

Diese Gleichung liefert dann wie gewünscht wegen $0 \leq r \leq t-1$:

$$y = f^s(x) = f^{q \cdot t + r}(x) = (f^r \circ f^{q \cdot t})(x) = f^r\big(f^{q \cdot t}(x)\big) = f^r(x) \in \big\{x, f(x), \dots, f^{t-1}(x)\big\}.$$

Damit gilt die gesuchte Inklusion $[x] \subseteq \{x, f(x), \dots, f^{t-1}(x)\}$, und der Existenzbeweis ist erbracht.

Eindeutigkeit der σ_i: Es sei eine Produktzerlegung

$$\sigma = \pi_1 \circ \dots \circ \pi_r$$

gegeben mit zyklischen Permutationen π_i und paarweise disjunkten Trägern S_i. Es reicht zu zeigen, daß die Träger S_i mit den Äquivalenzklassen aus der Relation des Existenzbeweises übereinstimmen, denn dann müssen die π_i genau den vorher konstruierten zyklischen Permutationen σ_i entsprechen. Damit gäbe es nur eine mögliche Zerlegung.

Sei also für ein gewähltes i der Träger S_i von π_i betrachtet, und zur Vermeidung von Multiindezes $S := S_i$ und $\pi := \pi_i$ gesetzt. Weiter sei $S := \{a_1, \dots, a_s\}$. Es reicht zu zeigen, daß $S = [a_1]$ gilt, denn dann ist der Träger gleich einer Äquivalenzklasse.

Nach der Voraussetzung gilt $\sigma^j(a_1) = \pi^j(a_1)$ für $0 \leq j \leq s$, so daß sofort $S \subseteq [a_1]$ folgt, und es bleibt nur die umgekehrte Inklusion zu zeigen.

Dazu sei $y \in [a_1]$ gewählt. Dann gibt es nach der Definition der Äquivalenzrelation ein $j \in \mathbb{Z}$ mit $y = \sigma^j(a_1)$, und für $j \geq 0$ ist sofort klar, daß $y \in S$ gilt.

Für $j < 0$ sei folgendes betrachtet: Da alle π paarweise miteinander kommutieren, gilt nach Satz 1.1.32 für alle $j \in \mathbb{Z}$:

$$\sigma^j = \pi_1^j \circ \dots \circ \pi_r^j.$$

Nach Bemerkung 0.4.26 haben für alle $1 \leq i \leq r$ die zyklischen Permutationen π_i und ihre jeweilige zyklische Inverse π_i^{-1} jeweils die gleiche Trägermenge S_i, und diese ist somit invariant unter π_i^j für alle $j \in \mathbb{Z}$. Insbesondere gilt dann:

$$y = \sigma^j(a_1) = \pi^j(a_1) \in S. \qquad \square$$

Lemma A.3.2. *Für jedes $n \in \mathbb{N}$ ist die folgende Abbildung ein Gruppenhomomorphismus von S_n in die multiplikative Gruppe $\{\pm 1\}$:*

$$\operatorname{sign}\colon S_n \longrightarrow \{\pm 1\} \quad \textit{mit} \quad \sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Dann wird $\operatorname{sign}(\sigma)$ das Signum von σ genannt.

Beweis. Es seien zuerst für ein $\sigma \in S_n$ folgende Mengen betrachtet:

$$\begin{aligned} I &:= \{\, (i,j) \mid 1 \le i < j \le n \,\}, \\ J &:= \{\, (i,j) \mid 1 \le i \le j \le n,\ \sigma(i) < \sigma(j) \,\}, \\ F &:= \{\, (i,j) \mid 1 \le i \le j \le n,\ \sigma(i) > \sigma(j) \,\}. \end{aligned}$$

Es folgt sofort $I = J \dot\cup F$, da für $(i,j) \in I$ immer $\sigma(i) \neq \sigma(j)$ gilt (wegen σ injektiv und $i \neq j$). Weiter sei folgende Abbildung betrachtet:

$$f_\sigma \colon I \longrightarrow I \quad \text{mit} \quad (i,j) \mapsto \begin{cases} \big(\sigma(i), \sigma(j)\big) & \text{falls } \sigma(i) < \sigma(j), \\ \big(\sigma(j), \sigma(i)\big) & \text{falls } \sigma(i) > \sigma(j). \end{cases}$$

Die Abbildung ist wohldefiniert, da σ eine Bijektion ist (d.h. $\sigma(i) \neq \sigma(j)$ für $i < j$), und eine kleine Fallunterscheidung für $f_\sigma\big((i,j)\big) = f_\sigma\big((l,k)\big)$ zeigt, daß f_σ injektiv und wegen $|I| < \infty$ damit sogar eine Bijektion auf I ist. Es folgt sofort:

$$I = f_\sigma(I) = f_\sigma(J) \dot\cup f_\sigma(F).$$

Es ist nun zu zeigen, daß „sign“ wohldefiniert ist, d.h. $\operatorname{sign}(\sigma) \in \{\pm 1\}$ gilt, und daß „sign“ ein Homomorphismus ist:

$\operatorname{sign}(\sigma) \in \{\pm 1\}$: Es gilt:

$$\begin{aligned} \prod_{1 \le i < j \le n} \sigma(j) - \sigma(i) &= \Big(\prod_{\substack{1 \le i < j \le n \\ \sigma(i) < \sigma(j)}} \sigma(j) - \sigma(i) \Big) \cdot \Big(\prod_{\substack{1 \le i < j \le n \\ \sigma(i) > \sigma(j)}} \sigma(j) - \sigma(i) \Big) \\ &= \Big(\prod_{(i,j) \in J} \sigma(j) - \sigma(i) \Big) \cdot \Big(\prod_{(i,j) \in F} (-1) \cdot \big(\sigma(i) - \sigma(j)\big) \Big) \\ &= \Big(\prod_{(l,k) \in f_\sigma(J)} (k - l) \Big) \cdot \Big(\prod_{(l,k) \in f_\sigma(F)} (-1) \cdot (k - l) \Big) \\ &\overset{(*)}{=} (-1)^{|F|} \prod_{1 \le l < k \le n} (k - l) \quad = \quad (-1)^{|F|} \prod_{1 \le i < j \le n} (j - i). \end{aligned}$$

Bei der Gleichung $(*)$ wurde $I = f_\sigma(I) = f_\sigma(J) \dot\cup f_\sigma(F)$ benutzt und die Beziehung $|f_\sigma(F)| = |F|$ (wegen f_σ injektiv). Aus dieser Herleitung ergibt sich sofort:

$$\operatorname{sign}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\prod\limits_{1 \le i < j \le n} \sigma(j) - \sigma(i)}{\prod\limits_{1 \le i < j \le n} j - i} = (-1)^{|F|} \in \{\pm 1\}.$$

„sign“ Homomorphismus: Es ist für $\tau, \sigma \in S_n$ zu zeigen, daß gilt:

$$\operatorname{sign}(\tau \circ \sigma) = \operatorname{sign}(\tau) \cdot \operatorname{sign}(\sigma).$$

Nach der Definition von „sign“und einer kleinen Erweiterung folgt:

$$\begin{aligned} \operatorname{sign}(\tau \circ \sigma) &= \prod_{1 \le i < j \le n} \frac{\tau\big(\sigma(j)\big) - \tau\big(\sigma(i)\big)}{j - i} = \prod_{1 \le i < j \le n} \frac{\tau\big(\sigma(j)\big) - \tau\big(\sigma(i)\big)}{\sigma(j) - \sigma(i)} \cdot \frac{\sigma(j) - \sigma(i)}{j - i} \\ &= \prod_{1 \le i < j \le n} \frac{\tau\big(\sigma(j)\big) - \tau\big(\sigma(i)\big)}{\sigma(j) - \sigma(i)} \cdot \underbrace{\prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}}_{\operatorname{sign}(\sigma)}. \end{aligned}$$

Es bleibt also zu zeigen, daß gilt:

$$\prod_{1\le i<j\le n} \frac{\tau\big(\sigma(j)\big)-\tau\big(\sigma(i)\big)}{\sigma(j)-\sigma(i)} = \operatorname{sign}(\tau).$$

Dazu sei betrachtet:

$$\begin{aligned}
\prod_{1\le i<j\le n} \frac{\tau\big(\sigma(j)\big)-\tau\big(\sigma(i)\big)}{\sigma(j)-\sigma(i)} &= \prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}} \frac{\tau\big(\sigma(j)\big)-\tau\big(\sigma(i)\big)}{\sigma(j)-\sigma(i)} \cdot \prod_{\substack{1\le i<j\le n\\ \sigma(i)>\sigma(j)}} \frac{\tau\big(\sigma(j)\big)-\tau\big(\sigma(i)\big)}{\sigma(j)-\sigma(i)} \\
&\overset{(*)}{=} \prod_{(i,j)\in J} \frac{\tau\big(\sigma(j)\big)-\tau\big(\sigma(i)\big)}{\sigma(j)-\sigma(i)} \cdot \prod_{(i,j)\in F} \frac{\tau\big(\sigma(i)\big)-\tau\big(\sigma(j)\big)}{\sigma(i)-\sigma(j)} \\
&= \prod_{(l,k)\in f_\sigma(J)} \frac{\tau(k)-\tau(l)}{k-l} \cdot \prod_{(l,k)\in f_\sigma(F)} \frac{\tau(k)-\tau(l)}{k-l} \\
&\overset{(\star)}{=} \prod_{1\le l<k\le n} \frac{\tau(k)-\tau(l)}{k-l} = \operatorname{sign}(\tau).
\end{aligned}$$

Bei der Gleichung $(*)$ wurde im rechten Produkt jeweils der Nenner und der Zähler mit -1 multipliziert, und bei $(\star)$ wurde die eingangs hergeleitete Indexmengenzerlegung benutzt:

$$f_\sigma(J) \,\dot\cup\, f_\sigma(F) = f_\sigma(I) = I. \qquad \square$$

Um Lemma 1.2.46 zu beweisen, müssen zuerst zwei Hilfsaussagen gezeigt werden:

Lemma A.3.3. *Sei $\sigma \in S_n$ eine zyklische Permutation mit $\sigma := (a_1 \ldots a_k)$. Dann kann das k-Zykel $(a_1 \ldots a_k)$ als Produkt von $k-1$ Zykeln der Länge 2 geschrieben werden, und insbesondere in der folgenden Form:*

$$(a_1 \ldots a_k) = (a_1\, a_2)(a_2\, a_3)\cdots(a_{k-1}\, a_k) = \prod_{i=1}^{k-1}(a_i\, a_{i+1}).$$

Beweis.
Der Beweis wird durch Induktion über $k \ge 2$ geführt:

Induktionsanfang $k=2$: Trivial.
Induktionsschritt $k \rightsquigarrow k+1$: Zuerst wird folgende Aussage gezeigt:

$$\underbrace{(a_1 \ldots a_k\, a_{k+1})}_{=:\sigma} = \underbrace{(a_1 \ldots a_k)}_{=:\pi}\underbrace{(a_k\, a_{k+1})}_{=:\tau}. \qquad (\star)$$

Die obigen Abbildungen sind offensichtlich für $i \notin \{a_1, \ldots, a_{k+1}\}$ gleich, da dann i in keinen Träger enthalten ist.
Auch für $i \in \{a_1, \ldots, a_{k-1}\}$ ist die Aussage klar, denn dann ist i nicht im Träger von τ enthalten und es gilt $\sigma(i) = \pi(i)$.
Also ist nur der Fall $i \in \{a_k, a_{k+1}\}$ zu untersuchen, und es folgt:

$$\begin{aligned}
\sigma(a_k) &= a_{k+1} \quad &&\text{und} \quad &&(\pi\circ\tau)(a_k) = \pi\big(\tau(a_k)\big) &&= \pi(a_{k+1}) = a_{k+1}, \\
\sigma(a_{k+1}) &= a_1 \quad &&\text{und} \quad &&(\pi\circ\tau)(a_{k+1}) = \pi\big(\tau(a_{k+1})\big) &&= \pi(a_k) \quad = a_1.
\end{aligned}$$

Damit ist die Zerlegung $\sigma = \pi \circ \tau$ gezeigt, und es folgt mit der Induktionsannahme:

$$(a_1 \ldots a_k\, a_{k+1}) \overset{(\star)}{=} (a_1 \ldots a_k)(a_k\, a_{k+1}) \overset{\text{(IAnn)}}{=} \Big(\prod_{i=1}^{k-1}(a_i\, a_{i+1})\Big) = \prod_{i=1}^{k}(a_i\, a_{i+1}). \qquad \square$$

Lemma A.3.4. *Sei $\sigma \in S_n$ eine zyklische Permutation mit $\sigma := (a_1 \ldots a_k)$. Dann gilt für $\tau \in S_n$:*

$$\tau \circ \sigma \circ \tau^{-1} = \big(\tau(a_1) \ldots \tau(a_k)\big).$$

Beweis.
Es ist zu zeigen, daß die Abbildungen $\tau \circ \sigma \circ \tau^{-1}$ und $\big(\tau(a_1) \ldots \tau(a_k)\big)$ für alle $i \in \{1 \ldots, n\}$ übereinstimmen.
Sei zuerst $i \in \{\tau(a_1), \ldots, \tau(a_k)\}$. Dann gibt es ein $1 \leq l \leq k$ mit $i = \tau(a_l)$, und es folgt:

$$(\tau \circ \sigma \circ \tau^{-1})(i) = \tau\Big(\sigma\Big(\tau^{-1}\big(\tau(a_l)\big)\Big)\Big) \qquad = \tau\big(\sigma(a_l)\big) = \begin{cases} \tau(a_{l+1}) & \text{für } l < k, \\ \tau(a_1) & \text{für } l = k. \end{cases}$$

$$\big(\tau(a_1) \ldots \tau(a_k)\big)(i) = \big(\tau(a_1) \ldots \tau(a_k)\big)\big(\tau(a_l)\big)) \qquad = \begin{cases} \tau(a_{l+1}) & \text{für } l < k, \\ \tau(a_1) & \text{für } l = k. \end{cases}$$

Sei nun $i \notin \{\tau(a_1), \ldots, \tau(a_k)\}$. Dann ist $\tau^{-1}(i) \notin \{a_1, \ldots, a_k\}$, und es folgt:

$$(\tau \circ \sigma \circ \tau^{-1})(i) = \tau\Big(\sigma\big(\underbrace{\tau^{-1}(i)}_{\text{Fixpunkt von } \sigma}\big)\Big) = \tau\big(\tau^{-1}(i)\big) = i = \big(\tau(a_1) \ldots \tau(a_k)\big)(i). \qquad \square$$

Nun kann die Aussage aus Lemma 1.2.46 bewiesen werden:

Lemma A.3.5. *Sei $\sigma \in S_n$ eine zyklische Permutation. Dann gilt:*

$$\sigma = (a_1\, a_2 \ldots a_k) \qquad \Longrightarrow \qquad \operatorname{sign}(\sigma) = (-1)^{k-1}.$$

Daraus folgt insbesondere für eine beliebige Permutation $f \in S_n$ und eine Produktdarstellung $f = \sigma_1 \circ \cdots \circ \sigma_r$ mit zyklischen Permutationen $\sigma_1, \ldots, \sigma_r$ (mit nicht notwendigerweise disjunkten Trägern) durch die Homomorphismus-Eigenschaft von „sign“:

$$f = \underbrace{(a_{1,1} \ldots a_{1,k_1})}_{\textit{Zykeldarst. } \sigma_1}\underbrace{(a_{2,1} \ldots a_{2,k_2})}_{\textit{Zykeldarst. } \sigma_2} \cdots \underbrace{(a_{r,1} \ldots a_{r,k_r})}_{\textit{Zykeldarst. } \sigma_r} \qquad \Longrightarrow \qquad \operatorname{sign}(f) = \prod_{i=1}^{r}(-1)^{k_i - 1}.$$

Beweis.
Nach Lemma A.3.3 kann der Zykel $(a_1 \ldots a_k)$ zerlegt werden in das Produkt:

$$(a_1 \ldots a_k) = (a_1\, a_2)(a_2\, a_3) \cdots (a_{k-1}\, a_k) = \prod_{i=1}^{k-1}(a_i\, a_{i+1}),$$

und da die Abbildung „sign“ ein Gruppenhomomorphismus ist (Lemma A.3.2), folgt mit $\tau_i := (a_i\, a_{i+1})$:

$$\operatorname{sign}\big(\sigma\big) = \operatorname{sign}\Big(\prod_{i=1}^{k-1}\tau_i\Big) = \prod_{i=1}^{k-1}\operatorname{sign}\big(\tau_i\big). \qquad (\star)$$

Für jedes $\tau := (a\,b) \in S_n$ und $\eta := (1\,2) \in S_n$ gibt es nach Lemma A.3.4 ein $\pi \in S_n$ mit $\pi \circ (a\,b) \circ \pi^{-1} = (1\,2)$, denn wegen $\pi \circ (a\,b) \circ \pi^{-1} = \big(\pi(a)\,\pi(b)\big)$ kann π folgendermaßen gewählt werden:

$$\begin{array}{llllll} a,b \in \{1,2\} & \Longrightarrow & \pi := \mathrm{id} & a,b \notin \{1,2\} & \Longrightarrow & \pi := (1\,a)(2\,b), \\ a = 1, b \neq 2 & \Longrightarrow & \pi := (2\,b), & a = 2, b \neq 1 & \Longrightarrow & \pi := (1\,b), \\ b = 1, a \neq 2 & \Longrightarrow & \pi := (2\,a), & b = 2, a \neq 1 & \Longrightarrow & \pi := (1\,a). \end{array}$$

Der Gruppenhomomorphismus „sign“ erfüllt für $\sigma, \pi \in S_n$:

$$\mathrm{sign}(\sigma) = \mathrm{sign}(\pi \circ \sigma \circ \pi^{-1}),$$

da die Gruppe $\big(\{\pm 1\}, \cdot\big)$ und damit der Wertebereich der Abbildung „sign“ eine abelsche Gruppe ist, woraus dann mit obiger Gleichung $\pi \circ (a\,b) \circ \pi^{-1} = (1\,2) = \eta$ für alle τ_i folgt:

$$\mathrm{sign}(\tau_i) = \mathrm{sign}(\eta).$$

Dies liefert zusammen mit der Gleichung $(\star)$ dann:

$$\mathrm{sign}(\sigma) = \prod_{i=1}^{k-1} \mathrm{sign}(\tau_i) = \prod_{i=1}^{k-1} \mathrm{sign}(\eta) = \big(\mathrm{sign}(\eta)\big)^{k-1}.$$

Es muß also nur noch gezeigt werden, daß $\mathrm{sign}(\eta) = (-1)$ gilt. Sei dazu die Definition der Abbildung „sign“ für ein $\theta \in S_n$ betrachtet (Lemma A.3.2):

$$\begin{aligned} \mathrm{sign}(\theta) &:= \prod_{1 \le i < j \le n} \frac{\theta(j) - \theta(i)}{j - i} \\ &= \underbrace{\prod_{1 < j \le n} \frac{\theta(j) - \theta(1)}{j - 1}}_{i=1} \cdot \underbrace{\prod_{2 < j \le n} \frac{\theta(j) - \theta(2)}{j - 2}}_{i=2} \cdot \underbrace{\prod_{3 \le i < j \le n} \frac{\theta(j) - \theta(i)}{j - i}}_{i \ge 3}. \end{aligned}$$

Gilt nun $\theta := \eta = (1\,2)$, so ist das Produkt für $i \ge 3$ gleich Eins, da Zähler und Nenner übereinstimmen. Es folgt also:

$$\mathrm{sign}(\eta) = \underbrace{\prod_{1 < j \le n} \frac{\eta(j) - 2}{j - 1}}_{i=1} \cdot \underbrace{\prod_{2 < j \le n} \frac{\eta(j) - 1}{j - 2}}_{i=2}.$$

Wird nun im linken Produkt $(i = 1)$ noch der Faktor für $j = 2$ herausgezogen, so ergibt sich wegen $\eta(j) = j$ für $3 \le j$:

$$\mathrm{sign}(\eta) = \underbrace{\frac{1-2}{2-1}}_{(i,j)=(1,2)} \cdot \prod_{2 < j \le n} \frac{j-2}{j-1} \cdot \prod_{2 < j \le n} \frac{j-1}{j-2} = \frac{1-2}{2-1} = -1. \qquad \square$$

Insbesondere folgt nun aus dem Lemma A.3.5, daß die Abbildung „sign“ für Zykeldarstellungen von Permutationen wohldefiniert ist.

A.4. Determinanten

Satz A.4.1. *(Determinantenmultiplikationssatz)*
Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann gilt für $A, B \in \mathrm{Mat}_n(R)$:

$$\det(AB) = \det(A) \cdot \det(B).$$

Beweis.
Es werden die beiden Terme $\det(AB)$ udn $\det(A)\cdot\det(B)$ explizit berechnet und verglichen. Sei dazu $(a_{i,j}) := A$, $(b_{i,j}) := B$ und $(c_{i,j}) := C := AB$. Dabei gilt dann für die Koeffizienten des Matrizenproduktes $c_{i,j}$:

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}.$$

$\det(AB)$: Es gelten folgende Gleichungen, wobei einzelne Umformungen am Ende der Rechnung näher erläutert sind:

$$\begin{aligned}
\det(AB) = \det(C) &= \sum_{\lambda\in S_n}\Big(\operatorname{sign}(\lambda)\cdot\prod_{i=1}^{n} c_{i,\lambda(i)}\Big)\\
&= \sum_{\lambda\in S_n}\left(\operatorname{sign}(\lambda)\cdot\prod_{i=1}^{n}\Big(\sum_{k=1}^{n} a_{i,k}b_{k,\lambda(i)}\Big)\right)\\
&\overset{(\star_1)}{=} \sum_{\lambda\in S_n}\left(\operatorname{sign}(\lambda)\cdot\sum_{(k_1,\dots,k_n)\in I_n^n}\Big(\prod_{i=1}^{n} a_{i,k_i}b_{k_i,\lambda(i)}\Big)\right)\\
&= \sum_{(k_1,\dots,k_n)\in I_n^n}\left(\sum_{\lambda\in S_n}\Big(\operatorname{sign}(\lambda)\cdot\prod_{i=1}^{n} a_{i,k_i}b_{k_i,\lambda(i)}\Big)\right)\\
&\overset{(\star_2)}{=} \sum_{\substack{(k_1,\dots,k_n)\in I_n^n\\ k_i\neq k_j}}\left(\sum_{\lambda\in S_n}\Big(\operatorname{sign}(\lambda)\cdot\prod_{i=1}^{n} a_{i,k_i}b_{k_i,\lambda(i)}\Big)\right)\\
&\overset{(\star_3)}{=} \sum_{\sigma\in S_n}\left(\sum_{\lambda\in S_n}\Big(\operatorname{sign}(\lambda)\cdot\prod_{i=1}^{n} a_{i,\sigma(i)}b_{\sigma(i),\lambda(i)}\Big)\right).
\end{aligned}$$

Erläuterungen zu einzelnen Umformungen:
$\star_1$: Es gilt folgende Aussage für $1\le m\le n$:

$$\prod_{i=1}^{m}\Big(\sum_{k=1}^{n} a_{i,k}b_{k\lambda(i)}\Big) = \sum_{k_1,\dots,k_m\in I_n^m}\Big(\prod_{i=1}^{m} a_{i,k_i}b_{k_i,\lambda(i)}\Big).$$

Diese wird nun per Induktion über m bewiesen:
Induktionsanffang $m=1$: Es gilt offensichtlich wegen $I_n=\{1,\dots,n\}$ die Gleichung:

$$\sum_{k=1}^{n} a_{1,k}b_{k,\lambda(1)} = \sum_{k_1\in I_n} a_{1,k_1}b_{k_1,\lambda(1)}.$$

Induktionsschritt $m\mapsto m+1$: Es gilt:

$$\prod_{i=1}^{m+1}\Big(\sum_{k=1}^{n} a_{i,k}b_{k,\lambda(i)}\Big) = \left(\prod_{i=1}^{m}\Big(\sum_{k=1}^{n} a_{i,k}b_{k,\lambda(i)}\Big)\right)\cdot\underbrace{\Big(\sum_{k=1}^{n} a_{m+1,k}b_{k,\lambda(m+1)}\Big)}_{i=m+1}$$

$$\overset{\text{(IAnn)}}{=} \left(\sum_{(k_1,\dots,k_m)\in I_n^m} \Big(\prod_{i=1}^m a_{i,k_i} b_{k_i,\lambda(i)} \Big) \right) \cdot \Big(\sum_{k=1}^n a_{m+1,k} b_{k,\lambda(m+1)} \Big)$$

$$= \sum_{k=1}^n \left(\sum_{(k_1,\dots,k_m)\in I_n^m} \Big[\Big(\prod_{i=1}^m a_{i,k_1} b_{k_i,\lambda(i)} \Big) \cdot a_{m+1,k} b_{k,\lambda(m+1)} \Big] \right)$$

$$= \sum_{(k_1,\dots,k_{m+1})\in I_n^{m+1}} \Big(\prod_{i=1}^{m+1} a_{i,k_i} b_{k_i,\lambda(k_i)} \Big).$$

Mit $m := n$ folgt dann die behauptete Umformung.

$\star_2$: Im kommutativen Ring R gilt:

$$\sum_{\lambda\in S_n} \Big(\operatorname{sign}(\lambda) \cdot \prod_{i=1}^n a_{i,k_i} b_{k_i,\lambda(k_i)} \Big) = \Big(\prod_{i=1}^n a_{i,k_i} \Big) \cdot \left(\sum_{\lambda\in S_n} \Big(\operatorname{sign}(\lambda) \cdot \prod_{i=1}^n b_{k_i,\lambda(k_i)} \Big) \right),$$

da in dem Produkt der a_{i,k_i} der Laufindex λ nicht vorkommt.
Es sei nun $B(k_1,\dots,k_n)$ diejenige $(n\times n)$-Matrix, deren i-te Zeile die k_i-te Zeile von B ist. Dann gilt mit der Leibnizformel:

$$\sum_{\lambda\in S_n} \Big(\operatorname{sign}(\lambda) \cdot \prod_{i=1}^n b_{k_i,\lambda(k_i)} \Big) = \det\big(B(k_1,\dots,k_n)\big),$$

und obige Formel lautet dann:

$$\sum_{\lambda\in S_n} \Big(\operatorname{sign}(\lambda) \cdot \prod_{i=1}^n a_{i,k_i} b_{k_i,\lambda(k_i)} \Big) = \Big(\prod_{i=1}^n a_{i,k_i} \Big) \cdot \det\big(B(k_1,\dots,k_n)\big).$$

Sind nun in $(k_1,\dots,k_n)$ zwei Indizes gleich, so hat $B(k_1,\dots,k_n)$ zwei gleiche Zeilen, und es gilt nach Lemma 3.3.7 dann $\det\big(B(k_1,\dots,k_n)\big) = 0$.
Somit können alle Terme, in denen $(k_1,\dots,k_n)$ nicht paarweise verschiedene Einträge enthält, wegfallen.

$\star_3$: Die Menge aller Tupel $(k_1,\dots,k_n) \in I_n^n$ mit paarweise verschiedenen Einträgen sind genau die Tupel $\big((\sigma(1),\dots,\sigma(n)\big)$ mit $\sigma \in S_n$.

$\det(A)\cdot\det(B)$: Es gelten folgende Gleichungen, wobei einzelne Umformungen am Ende der Rechnung näher erläutert sind:

$$\det(A)\cdot\det(B) = \left(\sum_{\sigma\in S_n} \Big(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^n a_{i,\sigma(i)} \Big) \right) \cdot \left(\sum_{\pi\in S_n} \Big(\operatorname{sign}(\pi) \cdot \prod_{i=1}^n b_{i,\pi(i)} \Big) \right)$$

$$\overset{(*_1)}{=} \sum_{\sigma\in S_n} \left(\sum_{\pi\in S_n} \Big[\operatorname{sign}(\sigma) \cdot \Big(\prod_{i=1}^n a_{i,\sigma(i)} \Big) \cdot \operatorname{sign}(\pi) \cdot \Big(\prod_{i=1}^n b_{i,\pi(i)} \Big) \Big] \right)$$

$$\overset{(*_2)}{=} \sum_{\sigma\in S_n} \left(\sum_{\pi\in S_n} \Big(\underbrace{\operatorname{sign}(\sigma)\cdot\operatorname{sign}(\pi)}_{=\operatorname{sign}(\sigma\circ\pi)} \cdot \prod_{i=1}^n a_{i,\sigma(i)} \cdot \prod_{i=1}^n b_{i,\pi(i)} \Big) \right)$$

$$\overset{(*_3)}{=} \sum_{\sigma\in S_n} \left(\sum_{\pi\in S_n} \Big(\operatorname{sign}(\sigma\circ\pi) \cdot \prod_{i=1}^n a_{i,\sigma(i)} \cdot \prod_{i=1}^n b_{\sigma(i),\sigma(\pi(i))} \Big) \right)$$

$$= \sum_{\sigma\in S_n}\left(\sum_{\pi\in S_n}\left(\operatorname{sign}(\underbrace{\sigma\circ\pi}_{=:\lambda})\cdot\prod_{i=1}^{n} a_{i,\sigma(i)}b_{\sigma(i),\sigma\circ\pi(i)}\right)\right)$$

$$\overset{(*_4)}{=} \sum_{\sigma\in S_n}\left(\sum_{\lambda\in S_n}\left(\operatorname{sign}(\lambda)\cdot\prod_{i=1}^{n} a_{i,\sigma(i)}b_{\sigma(i),\lambda(i)}\right)\right).$$

Erläuterungen zu einzelnen Umformungen:

$*_1$: Für zwei endliche Indexmengen U, V kann folgende Gleichung per Induktion über $|U|$ leicht bewiesen werden (mit x_u, y_v aus einem kommutativen Ring):

$$\Big(\sum_{u\in U} x_u\Big)\cdot\Big(\sum_{v\in V} y_v\Big) = \sum_{u\in U}\Big(\sum_{v\in V} x_u y_v\Big).$$

Mit $U := V := S_n$, $u := \sigma$, $v := \pi$ sowie

$$x_\sigma := \operatorname{sign}(\sigma)\cdot\prod_{k=1}^{n} a_{i,\sigma(i)} \quad \text{und} \quad y_\pi := \operatorname{sign}(\pi)\cdot\prod_{k=1}^{n} b_{i,\pi(i)}$$

ergibt sich die Umformung.

$*_2$: Die Elemente $\operatorname{sign}(\sigma)$, $\operatorname{sign}(\pi)$, $a_{i,\sigma(i)}$ und $b_{i,\pi(i)}$ liegen im kommutativen Ring R, so daß die Reihenfolge der Faktoren in den Produkte vertauscht werden darf.

$*_3$: Für jedes $\sigma \in S_n$ gilt

$$\prod_{i=1}^{n} b_{i,\pi(i)} = \prod_{i=1}^{n} b_{\sigma(i),\sigma(\pi(i))},$$

da nur die Reihenfolge der Faktoren $b_{i,\pi(i)}$ aus dem kommutativen Ring R durch σ permutiert wird.

$*_4$: Es gilt $\{\sigma\circ\pi | \pi\in S_n\} = \sigma S_n = S_n$, so daß der Indexwechsel in der inneren Summe möglich ist.

Nach den Umformungen ergibt sich für $\det(AB)$ und $\det(A)\cdot\det(B)$ der gleiche Term, so daß beide Ausdrücke übereinstimmen. □

Lemma A.4.2. *Sei R ein kommutativer Ring mit Eins. Für zwei Folgen über R*

$$(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0} \in \prod_{i\in\mathbb{N}_0} R$$

sei eine Multiplikation definiert durch:

$$(a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0} := (c_i)_{i\in\mathbb{N}_0} \quad \textit{mit} \quad c_i := \sum_{\lambda+\mu=i} a_\lambda b_\mu.$$

Dann ist $\prod_{i\in\mathbb{N}_0} R$ mit der komponentenweise Addition und obiger Multiplikation ein kommutativer Ring mit dem Einselement

$$(1, 0, 0, \ldots).$$

Weiter gilt, daß die Teilmenge $\bigoplus_{i\in\mathbb{N}_0} R$ ein kommutativer Unterring von $\prod_{i\in\mathbb{N}_0} R$ ist, der dessen Einselement enthält.

Beweis.

$\left(\prod_{i\in\mathbb{N}_0} R, +, *\right)$ kommutativer Ring mit Eins: $\prod_{i\in\mathbb{N}_0} R$ ist ein Ring bzgl. komponentenweiser Addition und komponentenweiser Multiplikation (Beispiel 1.3.3), und damit vor allem bzgl. der hier betrachteten komponentenweisen Addition eine abelsche Gruppe.

Es muß also noch gezeigt werden, daß $\prod_{i\in\mathbb{N}_0} R$ bzgl. der „neuen“ Multiplikation „$*$“ ein Monoid ist (mit dem behaupteten Einselement) und die Distributivgesetze gelten.

„$*$“ assoziativ: Es seien drei Folgen $(a_i), (b_i)$ und (c_i) aus $\prod_{i\in\mathbb{N}_0} R$ gegeben. Es seien definiert:

$$(d_i)_{i\in\mathbb{N}_0} := (a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0} \quad\Longrightarrow\quad d_i = \sum_{\lambda+\mu=i} a_\lambda b_\mu,$$

$$(e_i)_{i\in\mathbb{N}_0} := (b_i)_{i\in\mathbb{N}_0} * (c_i)_{i\in\mathbb{N}_0} \quad\Longrightarrow\quad e_i = \sum_{\mu+\nu=i} b_\mu c_\nu.$$

Dann gelten folgende Rechnungen für das Assoziativgesetz:

$$\begin{aligned}\big((a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0}\big) * (c_i)_{i\in\mathbb{N}_0} &= (d_i)_{i\in\mathbb{N}_0} * (c_i)_{i\in\mathbb{N}_0} = \Big(\sum_{\kappa+\nu=i} d_\kappa c_\nu\Big)_{i\in\mathbb{N}_0}\\ &= \Big(\sum_{\kappa+\nu=i} \underbrace{\Big(\sum_{\lambda+\mu=\kappa} a_\lambda b_\mu\Big)}_{=d_\kappa} c_\nu\Big)_{i\in\mathbb{N}_0} = \Big(\sum_{\lambda+\mu+\nu=i} (a_\lambda b_\mu) c_\nu\Big)_{i\in\mathbb{N}_0}\end{aligned}$$

und

$$\begin{aligned}(a_i)_{i\in\mathbb{N}_0} * \big((b_i)_{i\in\mathbb{N}_0} * (c_i)_{i\in\mathbb{N}_0}\big) &= (a_i)_{i\in\mathbb{N}_0} * (e_i)_{i\in\mathbb{N}_0} = \Big(\sum_{\lambda+\kappa=i} a_\lambda e_\kappa\Big)_{i\in\mathbb{N}_0}\\ &= \Big(\sum_{\lambda+\kappa=i} a_\lambda \underbrace{\Big(\sum_{\mu+\nu=\kappa} b_\mu c_\nu\Big)}_{=e_\kappa}\Big)_{i\in\mathbb{N}_0} = \Big(\sum_{\lambda+\mu+\nu=i} a_\lambda (b_\mu c_\nu)\Big)_{i\in\mathbb{N}_0}.\end{aligned}$$

Da in R das Assoziativgesetz für die Multiplikation gilt, ist $(a_\lambda b_\mu)c_\nu = a_\lambda(b_\mu c_\nu)$ in jedem Summanden und das Assoziativgesetz gilt auch für „$*$“.

$(1, 0, 0, \ldots)$ Einselement: Es sei $(e_i)_{i\in\mathbb{N}_0}$, d.h. es gilt $e_0 = 1$ und $e_i = 0$ für $i > 0$. Dann gilt für eine Folge $(a_i)_{i\in\mathbb{N}_0}$ und ein $k \in \mathbb{N}_0$:

$$\sum_{\lambda+\mu=k} e_\lambda a_\mu = e_0 a_k = a_k = a_k e_0 = \sum_{\lambda+\mu=k} a_\mu e_\lambda, \qquad (\star)$$

und es folgt:

$$(e_i)_{i\in\mathbb{N}_0} * (a_i)_{i\in\mathbb{N}_0} = \Big(\sum_{\lambda+\mu=i} e_\lambda a_i\Big)_{i\in\mathbb{N}_0} \overset{(\star)}{=} (a_i)_{i\in\mathbb{N}_0} \overset{(\star)}{=} \Big(\sum_{\mu+\lambda=i} a_\mu e_\lambda\Big)_{i\in\mathbb{N}_0} = (a_i)_{i\in\mathbb{N}_0} * (e_i)_{i\in\mathbb{N}_0}.$$

Distributivgesetze: Es seien $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0}$ und $(c_i)_{i\in\mathbb{N}_0}$ aus $\prod_{i\in\mathbb{N}_0} R$ gegeben. Dann folgen die Distributivgesetze $D1$ und $D2$ aus:

$$\begin{aligned}(a_i)_{i\in\mathbb{N}_0} * \big((b_i)_{i\in\mathbb{N}_0} + (c_i)_{i\in\mathbb{N}_0}\big) &= (a_i)_{i\in\mathbb{N}_0} * (b_i + c_i)_{i\in\mathbb{N}_0}\\ &= \Big(\sum_{\lambda+\mu=i} a_\lambda (b_\mu + c_\mu)\Big)_{i\in\mathbb{N}_0}\end{aligned}$$

$$
\begin{aligned}
&= \Big(\sum_{\lambda+\mu=i} (a_\lambda b_\mu + a_\lambda c_\mu) \Big)_{i\in\mathbb{N}_0} \\
&= \Big(\sum_{\lambda+\mu=i} a_\lambda b_\mu + \sum_{\lambda+\mu=i} a_\lambda c_\mu \Big)_{i\in\mathbb{N}_0} \\
&= \Big(\sum_{\lambda+\mu=i} a_\lambda b_\mu \Big)_{i\in\mathbb{N}_0} + \Big(\sum_{\lambda+\mu=i} a_\lambda c_\mu \Big)_{i\in\mathbb{N}_0} \\
&(a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0} + (a_i)_{i\in\mathbb{N}_0} * (c_i)_{i\in\mathbb{N}_0}. \qquad (D1)
\end{aligned}
$$

$$
\begin{aligned}
\big((b_i)_{i\in\mathbb{N}_0} + (c_i)_{i\in\mathbb{N}_0}\big) * (a_i)_{i\in\mathbb{N}_0} &= (b_i + c_i)_{i\in\mathbb{N}_0} * (a_i)_{i\in\mathbb{N}_0} \\
&= \Big(\sum_{\lambda+\mu=i} (b_\lambda + c_\lambda) * a_\mu) \Big)_{i\in\mathbb{N}_0} \\
&= \Big(\sum_{\lambda+\mu=i} (b_\lambda a_\mu + c_\lambda a_\mu) \Big)_{i\in\mathbb{N}_0} \\
&= \Big(\sum_{\lambda+\mu=i} b_\lambda a_\mu + \sum_{\lambda+\mu=i} c_\lambda a_\mu \Big)_{i\in\mathbb{N}_0} \\
&= \Big(\sum_{\lambda+\mu=i} b_\lambda a_\mu \Big)_{i\in\mathbb{N}_0} + \Big(\sum_{\lambda+\mu=i} c_\lambda a_\mu \Big)_{i\in\mathbb{N}_0} \\
&(b_i)_{i\in\mathbb{N}_0} * (a_i)_{i\in\mathbb{N}_0} + (c_i)_{i\in\mathbb{N}_0} * (a_i)_{i\in\mathbb{N}_0}. \qquad (D2)
\end{aligned}
$$

„$*$“ kommutativ: Wegen $a_\lambda b_\mu = b_\mu a_\lambda$ gilt für zwei Folgen $(a_i)_{i\in\mathbb{N}_0}$ und $(b_i)_{i\in\mathbb{N}_0}$:

$$
(a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0} = \Big(\sum_{\lambda+\mu=i} a_\lambda b_\mu \Big) = \Big(\sum_{\lambda+\mu=i} b_\mu a_\lambda \Big) = \Big(\sum_{\mu+\lambda=i} b_\mu a_\lambda \Big) = (b_i)_{i\in\mathbb{N}_0} * (a_i)_{i\in\mathbb{N}_0}.
$$

$\bigoplus_{i\in\mathbb{N}_0} R$ Unterring: Es ist zu zeigen, daß $\bigoplus_{i\in\mathbb{N}_0} R$ bzgl. der komponentenweise Addition eine Untergruppe ist, was nach Lemmma 2.2.9 gilt, und daß $\bigoplus_{i\in\mathbb{N}_0} R$ bzgl. der Multiplikation „$*$“ abgeschlossen ist. Dazu muß für zwei Folgen $(a_i)_{i\in\mathbb{N}_0}$ und $(b_i)_{i\in\mathbb{N}_0}$, die nur endlich viele Koeffizienten a_i bzw. b_i ungleich Null haben, auch das Produkt

$$
(c_i)_{i\in\mathbb{N}_0} := (a_i)_{i\in\mathbb{N}_0} * (b_i)_{i\in\mathbb{N}_0}
$$

nur endlich viele Koeffizienten c_i ungleich Null enthält (diese Bedingung an die Koeffizienten ist genau die Definition der Teilmenge $\bigoplus_{i\in\mathbb{N}_0} R$ von $\prod_{i\in\mathbb{N}_0} R$: siehe Definition 2.2.3).

Sei dazu α der höchste Index mit $a_i \neq 0$ und β der höchste Index mit $b_i \neq 0$. Dann gilt für alle $k > \alpha + \beta$:

$$
\begin{aligned}
\lambda + \mu = k \text{ und } \lambda < \alpha \quad &\Longrightarrow \quad \mu > \beta, \\
\lambda + \mu = k \text{ und } \mu < \beta \quad &\Longrightarrow \quad \lambda > \alpha,
\end{aligned}
$$

und so folgt für die Koeffizienten c_k mit $k > \alpha + \beta$:

$$
c_k = \sum_{\lambda+\mu=k} a_\lambda b_\mu = 0.
$$

Damit sind höchstens die Koeffizienten c_k mit $k \leq \alpha + \beta$ in $(c_i)_{i\in\mathbb{N}_0}$ ungleich Null, also nur endlich viele.

Offensichtlich liegt $(1, 0, 0, \ldots)$ in $\bigoplus_{i \in \mathbb{N}_0} R$, und die Kommutativität der Multiplikation überträgt sich aus dem Oberring. $\square$

Literaturverzeichnis

[BlAn1] Christian Blatter, *Analysis 1*, Springer Verlag, 1991, vierte Auflage.

[BrLAI] Egbert Brieskorn, *Lineare Algebra und analytische Geometrie I*, Vieweg, 1983.

[BrLAII] Egbert Brieskorn, *Lineare Algebra und analytische Geometrie II*, Vieweg, 1985.

[FAn1] Otto Forster, *Analysis 1*, Vieweg, 1976.

[GMZ] H.-D. Ebbinghaus et al., *Zahlen*, Grundwissen Mathematik 1, Springer-Verlag, 1983.

[LaMR] T. Y. Lam, *Lectures on Modules and Rings*, Springer, 1999.

[MAC] Georg Cantor, *Beiträge zu Begründung der transfiniten Mengenlehre*, Mathematische Annalen, Volume 46 Nummer 4, 1895, Seite 481–512.

[PanDM] Alois Panholzer, *Diskrete Methoden*, Vorlesungsskript Sommersemester 2011, TU Wien.

[RALA] Steven Roman, *Advanced Linear Algebra*, Springer Verlag, Graduate Texts in Mathematics 135, 1992.

[RSV] H.-J. Reiffen, G. Scheja, U. Vetter, *Algebra*, B.I. Wissenschaftsverlag, 1984, 2te Auflage.

[SSAlg1] G. Scheja, U. Storch, *Lehrbuch der Algebra Teil 1*, B. G. Teubner Stuttgart, 1980.

[SSAlg2] G. Scheja, U. Storch, *Lehrbuch der Algebra Teil 2*, B. G. Teubner Stuttgart, 1988.

[SSAlg3] G. Scheja, U. Storch, *Lehrbuch der Algebra Teil 2*, B. G. Teubner Stuttgart, 1981.

[WAn1] Rolf Walter, *Einführung in die Analysis 1*, de Gruyter, 2007.

Index

$(A)_{i,j}$, 168
$(a)_R$, 90
$(n-1)$-te Einheitsphäre, 334
A^t, 232
B^A, 19
D^n, 333
$D_i^{(n)}(\alpha)$, 188
E_n, 169
G/U, 50
$I_{m,n}$, 168
LR-Zerlegung, 214
$L_{i,j}^{(n)}(\lambda)$, 188
M^*, 288
$P_{St}^{(n)}$, Anh. 1
$P_{i,j}^{(n)}$, 188
QR-Zerlegung, 342
$R[[t]]$, 257
$R[t]$, 257
$R[t]_{,_n}$259
R^*, 84
$R^{[n]}$, 177
$S(M)$, 19
S^{n-1}, 334
S_n, 19
  Signum, 66, Anh. 9
$U * g$, 50
V_λ, 302
$[\,\cdot\,]_B$, 274
$[\,\cdot\,]_{C,B}$, 278
$[\varphi]$, 179
$\mathrm{Abb}(A,B)$, 19
$\mathrm{Aut}(M)$, 62
$\mathrm{Aut}_R(M)$, 115
$\mathrm{Aut}_{\mathrm{Ring}}(R)$, 95
$\mathrm{Eig}(A,\lambda)$, 302
$\mathrm{Eig}(\varphi,\lambda)$, 302
$\mathrm{End}(M)$, 62
$\mathrm{End}_R(M)$, 115
$\mathrm{End}_{\mathrm{Ring}}(R)$, 95
$\mathrm{GL}_R(M)$, 115
$\mathrm{GL}_n(R)$, 177
$\mathrm{Hom}(M,N)$, 62
$\mathrm{Hom}_R(M,N)$, 115
$\mathrm{Hom}_{\mathrm{Ring}}(R,S)$, 95
$\mathrm{Mat}(m\times n,R)$, 168
$\mathrm{Mat}_n(R)$, 177
$\mathrm{SL}_n(R)$, 224
$\alpha_{x,y}$, 350
χ_φ, 301
$\Gamma B30D\cdot\Gamma B30D_2$, 333
$\Gamma B30Dx\Gamma B30D_\infty$, 326
$\Gamma B30Dx\Gamma B30D_p$, 326
$\mathrm{h}A\,g\,B$, 47
$\mathrm{h}A\,x_i \mid i\in I\,B$, 134
$\mathrm{h}A\,x_i\,B_{i\in I}$, 134
$\mathrm{h}A\,\cdot,\cdot\,B_2$, 333
$\delta_{i,j}$, 144
$\mathrm{diag}(A)$, 168
ℓ^2, 329
ℓ_g, 46
$\emptyset$, 6
$\mathrm{graph}(f)$, 11
$\mathrm{im}(f)$, 11
κ_g, 64
$\mathbb{Z}_n,+)$, 60
$\mathcal{E}_m$, 274
$\mathcal{P}(M)$, 6
$\mathcal{V}_n(M)$, Anh. 1
$\mathrm{ord}(g)$, 47
det, 218
$\det(A)$, 218
$\det(\varphi)$, 301
$\dim_K(V)$, 159
$\ker(\varphi)$, 71, 99, 123
$\mathrm{rg}(\varphi)$, 164
$\mathrm{rg}_{\mathrm{Spalte}}(A)$, 200
$\mathrm{rg}_{\mathrm{Zeile}}(A)$, 200
sign, 10
$\mathrm{sp}(A)$, 264
$\mathrm{Bil}_{\mathbb{R}}(V)$, 351
$\mathrm{Sym}_n(\mathbb{R})$, 356
ε-Ball, 325
φ_A, 178
$e_k^{I,R}$, 144
$g * U$, 50
n-fach multilineare Abbildung, 240

n-fache Multilinearform, 240
n-te Einheitskugel, 333
p-Norm, 326
${}_B[b]_B$, 351
., 240
Äquivalenz, 3
Äquivalenzklasse, 7
Äquivalenzrelation, 7
überabzählbar, 18

Abbildung, 11
  im, 11
  bijektiv, 14
  Bild, 11
  bilinear, 240
  Definitionsbereich, 11
  Einbettung, 63
  Einschränkung, 20
  Faser, 13
  Gleichheit, 12
  graph, 11
  Gruppenautomorphismus, 63
  Gruppenendomorphismus, 63
  Gruppenepimorphismus, 63
  Gruppenhomomorphismus, 63
  Gruppenisomorphismus, 63
  Gruppenmonomorphismus, 63
  Homomorphismus, 62
  Identität, 14
  injektiv, 14
  inverse, 17
  Körperhomomorphismus, 95
  lineare Abbildung, 115
  multilinear, 240
    alternierend, 240
    symmetrisch, 240
  Ringhomomorphismus, 95
  strukturerhaltend, 62
  strukturverträglich, 62
  surjektiv, 14
  Umkehrabbildung, 17
  Urbild, 13
  Wertebereich, 11
Abbildungen
  Komposition, 16
abgeschlossen, 26, 111
Absolutglied, 257
Abstand, 324
abzählbar, 18
adjungierte Matrix, 243
allgemeine lineare Gruppe, 115
alternierende Gruppe, 222
alternierende Multilinearform, 240
Assoziativgesetz, 27
  allgemeines, 28, Anh. 2
Austauschsatz, 157
Automorphismus, 62

Basis, 140
Basisauswahlsatz, 156
Basisergänzungssatz, 157
Begleitmatrix, 267
Betrag, 10
bijektiv, 14
Bild, 11
Bilienarform
  darstellende Matrix, 351
bilineare Abbildung, 240

Cauchy-Schwarzsche Ungleichung, 330
charakteristische Polynom, 261
Cosinus-Satz, 350
Cramersche Regel, 246

darstellende Matrix, 278, 351
Definitheit, 324, 325
Definitionsbereich, 11
Determinante, 218
Determinanten
  Regel von Sarrus, 221
  Sarrussche Regel, 221
Determinantenmultiplikantionssatz, 223, Anh. 13
Diagonale, 168
Diagonalelemente, 168
diagonalisierbar, 301
Diagonalmatrix, 169
Differenzmenge, 6
Dimension, 159
  endlich, 159
  unendlich, 159
disjunkt, 7
Distributivgesetze, 79
Division mit Rest, 10
Dreiecksungleichung, 324, 325
duale Abbildung, 290
duale Basis, 288
Dualraum, 288

Eigenraum, 302
Eigenvektoren, 302
Eigenwert, 302
Einbettung, 62
eindliche Menge, 18
Einheit, 84
Einheitengruppe, 84, 92
Einheitsmatrix, 169
Eins, 29, 79
Einschränkung, 20
Element, 5
  inverses, 29, 30
  invertierbar, 29
  neutrales, 29

Potenzen, 33, Anh. 4
Elementarmatrix, 168
Elemente
kommutieren, 34, Anh. 5
Endomorphismen
Eigenvektoren, 303
Eigenwerte, 303
Endomorphismenring, 122
Endomorphismus, 62
charakteristisches Polynom, 301
Determinante, 301
diagonalisierbar, 301
Epimorphismus, 62
Erweiterung, 139
Erzeugendensystem, 137
minimal, 139
Erzeugnis, 134, 136
eucklidischer Vektorraum, 328
euklidische Norm, 333
Eulersche φ-Funktion, 92

Faktorgruppe, 58
Faser, 13
Fasern, 13
Fixpunkt, 19
Folge
Konvergenz, 325
formale Potenzreihe, 257
freier Modul, 156
Funktion, 11
Stetigkeit, 325

Gauß-Algorithmus, 193
general linear group, 177
Grad, 257
Gram-Schmidtsches
Orthogonalisierungsverfahren, 337
Graph, 11
Gruppe, 31
abelsche, 31
Einbettung, 63
Element
Ordnung, 47
Faktorgruppe, 58
Gruppenautomorphismus, 63
Gruppenendomorphismus, 63
Gruppenepimorphismus, 63
Gruppenhomomorphismus, 63
Gruppenisomorphismus, 63
Gruppenmonomorphismus, 63
Homomorphie-Satz
Version I, 73
Version II, 75
Homomorphismus
Projektion, 66
kommutative, 31
Linksmultiplikation, 46
Linksnebenklasse, 50
Repräsentant, 50
Normalteiler, 56
Operation, 65
Quotientengruppe, 58
Projektion, 66
Rechtsnebenklasse, 50
Untergruppe, 31
Erzeuger, 47
erzeugt, 47
zyklisch, 47
Zentrum, 228
zyklisch, 47
Gruppen
Konjugationsklassen, 64
Operation
Orbit, 65
Gruppenhomomorphismus, 62

Halbgruppe, 31
kommutative, 31
Halbgruppenhomomorphismus, 62
Hauptachsentransformationsatz, 359
Hauptideal, 90
Hauptminoren-Kriterium, 359
Homogenität, 325
Homomorphie-Satz für Gruppen Version II, 75
Homomorphie-Satz für Moduln und Vektorräume Version II, 125
Homomorphie-Satz für Ringe Version II, 101
Homomorphie-Satz Version I, 73, 100, 124
Homomorphismus
Gruppe, 63
Körper, 95
Körperhomomorphismus, 95
Kern, 71, 99, 123
Modul, 115
Ring, 95
Ringhomomorphismus, 95
Vektorraum, 115

Ideal, 89
Hauptideal, 90
maximal, 91
Identitität, 14
Implikation, 3
Induktion
vollständige, 23
Induktionsanfang, 23
Induktionsannahme, 24
Induktionsschritt, 23
Induktionsanfang, 23
Induktionsannahme, 24
Induktionsschritt, 23

induzierte Metrik, 326
injektiv, 14
Integritätsring, 83
invariant, 19
Inverse, 17
inverse Abbildung, 17
invertierbarer Matrix, 177
isomorph, 63, 115
Isomorphismus, 62

Körper, 87
  Körperhomomorphismus, 95
kanonische Basis, 145
kartesische Produkt, 6
Kern, 123
  Gruppenhomomorpismus, 71
  Ringhomomorphismus, 99
Klassifikation
  zyklische Gruppen, 77
Koeffizienten, 168
Koeffizientensystem, 134
kommutativer Ring, 80
Kommutativgesetz, 27
  allgemeines, 29, Anh. 3
Komposition, 15
kongruent, 60
Konjugation, 64
Konjugationsinvariante, 299
Konjugationsklasse, 297
Konjugationsklassen, 64
konjugiert, 296
konstante Polynome, 257
konvergent, 325
Koordinaten, 140
Koordinatenabbildung, 274
Koordinatenraum, 177
Koordinatenvektor, 274
Kroneckersymbol, 144

Länge, 325
Lagrange, Satz von, 53
Laplacescher Entwicklungssatz, 249
leere Menge, 6
Leibniz-Formel, 219
Leitkoeffizient, 257
linear abhängig, 142
linear unabhängig, 142
Lineare Abbildung, 115
lineare Abbildung
  Endomorphismus
    charakteristisches Polynom, 301
    Determinante, 301
  lineare Fortsetzung, 147
  Rang, 164
Lineare Abbildungen
  Eigenvektoren, 303
  Eigenwerte, 303
lineare Abbildungen
  Rangsatz, 164
lineare Fortsetzung, 147
lineare Gleichung, 129
  Koeffizienten, 129
  Lösung, 129
  Unbekannte, 129
lineare Hülle, 134
lineares Gleichungssystem, 129
  homogen, 129
  inhomogen, 129
  Koeffizienten, 129
  Lösung, 129
  rechte Seite, 129
lineares Gleichunssystem
  Gleichungen, 129
Linearfaktoren, 257
Linearkombination, 134, 136
Linksmultiplikation, 46, 85
Linksmultiplikaton, 107
Linksnebenklasse, 50
Logik
  Äquivalenz, 4
  Implikation, 4

Mächtigkeit von Mengen, 18
Matrix, 168
  charakteristisches Polynom, 261
  Determinante, 219
  diagonalisierbar, 301
  Diagonalmatrix, 169
  Einheitsmatrix, 169
  Elementarmatrix, 169
  invertierbar, 177
  Koeffizient, 169
  Konjugationsinvariante, 299
  Konjugationsklasse, 297
  konjugiert, 296
  quadratisch, 168
  Rang, 203
  Spaltenindex, 169
  Spaltenrang, 200
  spezielle Zeilen-Stufen-Form, 187
  symmetrisch, 356
  Zeilen-Stufen-Form, 187
    spezielle, 187
  Zeilenindex, 169
  Zeilenrang, 200
Matrizen
  Eigenvektoren, 303
  Eigenwerte, 303
Matrizenprodukt, 171
Matrizenring, 177
maximal linear unabhängiges System, 151
Maximums-Norm, 326

Menge, 5
  überabzählbar, 18
  abzählbar, 18
  Differenzenmenge, 7
  disjunkt, 7
  Element, 6
  endlich, 18
  kartesisches Produkt, 7
  leere, 6
  Mächtigkeit, 18
  Minimum, 10
  Ordnung, 18
  Permutation, 19
  Potenzmenge, 6
  Relation, 7
  Schnittmenge, 7
  symmetrische Differenz, 82
  Teilmenge, 6
    echte, 6
  unendlich, 18
  Vereinigungsmenge, 7
Metrik, 324
  Abstand, 324
  Definitheit, 324
  Dreiecksungleichung, 324
  Symmetrie, 324
metrischer Raum, 324
  Konvergenz, 325
  Stetigkeit, 325
minimales Erzeugendensystem, 139
Modul, 105, 108
  Basis, 140
  Endomorphismenring, 122
  Erzeugendensystem, 137
    minimal, 139
  frei, 156
  Homomorphismus
    Kern, 123
    Projektion, 119
  isomorph, 115
  lineare Abbildung, 115
    Kern, 123
    Projektion, 119
  Linksmultiplikation, 107
  Modulhomomorphismus, 115
    Kern, 123
  Quotientenmodul
    Projektion, 119
  Skalare, 105
  skalare Multplikation, 105
  Untermodul, 111
  Vektoraddition, 105
  Vektoren, 105
Modulhomomorphismus, 115
  Kern, 123
Moduln
  Homomorphie-Satz
    Version II, 125
modulo, 60
Modulstruktur, 108
Monoid, 31
  kommutativer, 31
  Potenzgesetze, 34, Anh. 6
  Untermonoid, 31
Monoidhomomorphismus, 62
Monomorphismus, 62
Moudl
  Nullvektor, 105
Multilinearform, 240
  alternierend, 240
  symmetrisch, 240

Nebenklasse
  Linksnebenklasse, 50
    Repräsentant, 50
  Rechtsnebenklasse, 50
    Repräsentant, 50
  Repräsentant, 50
Norm, 325
  Definitheit, 325
  Dreiecksungleichung, 325
  euklidisch, 334
  Homogenität, 325
  Länge, 325
  normiert, 325
Normalteiler, 56
normiert, 257, 325
Null, 29, 79
Nullmatrix, 168
Nullpolynom, 257
Nullteiler, 83
nullteilerfrei, 83
Nullvektor, 105

obere Dreiecksmatrix, 212
Obersystem, 139
Operation, 65
  Gruppe, 65
Orbit, 65
Ordnung, 18
orthogonal, 335, 346
Orthogonalbasis, 335
orthogonale Komplement, 346
orthogonale Matrix, 359
Orthogonalsystem, 335
orthonormal, 335
Orthonormalbasis, 335
Orthonormalsystem, 335

Permutation, 19
  Signum, 66, Anh. 9

Träger, 20
Zykel, 20
zyklisch, 20
Permutationen, 19
Polynom, 257
charakteristisches, 261
Polynom:Absolutglied, 257
Polynom:Grad, 257
Polynom:konstantes Polynom, 257
Polynom:Leitkoeffizient, 257
Polynom:Linearfaktor, 257
Polynomring, 257
positiv definit, 328, 356
Potenzen, 33, Anh. 4
Potenzgesetze, 34, Anh. 6
Potenzmenge, 6
Potenzreihenring, 257
Projektion
kanonische, 66, 97, 119
Punkt-vor-Strich-Regelung, 80

Quotienmodul
Projektion, 119
Quotienring
Projektion, 97
Quotientengruppe, 58
Projektion, 66
Quotientenmodul, 113
Quotientenring, 90
Quotientenvektorraum, 113
Quotienvektorraum
Projektion, 119

Rang, 164, 203
Rangsatz, 164
Rechtsnebenklasse, 50
reflexiv, 7
Regel von Sarrus, 221
Relation, 7
Äquivalenzklasse, 7
Repräsentant, 7
Äquivalenzrelation, 7
reflexiv, 7
symmetrisch, 7
transitiv, 7
Repräsentant, 7, 50
Repräsentantensystem
vollständig, 8
Restklasse, 60
Restklassengring, 92
Restklassengruppe, 60
kongruent, 60
modulo, 60
Ring, 79
Distributivgesetze, 80
Einheit, 84
Einheitengruppe, 84
Hauptideal, 90
Homomorphismus
Kern, 71, 99
Projektion, 97
Ideal, 89
Hauptideal, 90
Integritätsring, 83
Linksmultiplikation, 85
mit Eins, 79
Nullteiler, 83
Punkt-vor-Strich-Regelung, 80
Quotientenrin
Projektion, 97
Ringhomomorphismus, 95
Kern, 71, 99
Unterring, 87
Ringe
Homomorphie-Satz
Version I, 100, 124
Version II, 101

Sarrussche Regel, 221
Satz von Pythagoras, 350
Schiefkörper, 87
Schnittmenge, 6
senkrecht, 335
Signum, 10, 66, Anh. 9
Skalare, 105
skalare Multiplikation, 105
Skalarprodukt, 328
Spaltenindex, 168
Spaltenrang, 200
Spaltenraum, 177
Spaltenvektor, 168
Spaltenvektoren, 177
Spann, 134
spezielle Zeilen-Stufen-Form, 187
Spur, 264
Stammfunktion, 127
Standard-Basis, 145
Standard-Skalarprodukt, 329
stetig, 325
Struktur
abgeschlossen, 26
algebraisch, 26
algebraische, 26
Unterstruktur, 26
assoziative, 27
Gruppe, 31
abelsche, 31
kommutative, 31
Untergruppe, 31
Halbgruppe, 31
kommutative, 31
Unterhalbgruppe, 31

Körper, 87
kommutative, 27
Monoid, 31
kommutativer, 31
Untermonoid, 31
Ring, 80
Distributivgesetze, 80
Eins, 80
kommutativ, 80
Null, 80
Punkt-vor-Strich-Regelung, 80
Stufen, 187
surjektiv, 14
Symmetrie, 324
symmetrisch, 7
symmetrische Differenz, 82
Symmetrische Gruppe, 19
symmetrische Matrix, 356
symmetrische Multilinearform, 240
System, 132

Teilmenge, 5
echte, 6
Teilsystem, 139
Träger, 20
transitiv, 7
Transponierte, 232
transponierte Matrix, 232

Umkehrabbildung, 17
unendliche Menge, 18
untere Dreiecksmatrix, 212
Untermodul, 111
Unterraum
orthogonal, 346
Unterring, 87
Unterstruktur, 26
Untervektorraum, 111
Urbild, 13

Vektoraddition, 105
Vektoren, 105
Vektorräume
Homomorphie-Satz
Version II, 125
Vektorraum, 105, 108
Basis, 140
Dimension, 159
endlich, 159
unendlich, 159
Endomorphismenring, 122
Erzeugendensystem, 137
minimal, 139
Homomorphismus
Kern, 123
Projektion, 119
isomorph, 115
lineare Abbildung, 115
Kern, 123
Projektion, 119
Linksmultiplikation, 107
Nullvektor, 105
Quotientenvektorraum
Projektion, 119
Skalare, 105
skalare Multplikation, 105
Untervektorraum, 111
Vektoraddition, 105
Vektoren, 105
Vektorraumhomomorphismus, 115
Kern, 123
Vektorraumhomomorphismus, 115
Kern, 123
Rang, 164
Vereinigungsmenge, 6
Verknüpfung
äußere, 104
Assoziativgesetz
allgemeines, 28, Anh. 2
innere, 26
n-stellig, Anh. 1
n-stellige Standardverknüpfung, Anh. 1
n-stelliges Produkt, 28, Anh. 3
Assoziativgesetz, 27
Eins, 29
inverses Element, 29, 30
Kommutativgesetz, 27
kommutieren, 34, Anh. 5
neutrales Element, 29
Null, 29
Kommutativgesetz
allgemeines, 29, Anh. 3
vollständige Induktion, 23

Wertebereich, 11
Winkel, 350

Zahl
sign, 10
Signum, 10
Zahlen, 9
Betrag, 10
Division mit Rest, 10
ganze, 9
Grundrechenarten, 9
natürliche, 9
Ordnung, 9
rationale, 9
relle, 9
Zeilen-Stufen-Form, 187
Zeilenindex, 168
Zeilenrang, 200

Zeilenraum, 177
Zeilenvektor, 168
Zeilenvektoren, 177
Zentrum, 227
Zykel, 20
zyklisch, 20