V1G3 – Lineare Algebra I

Dozent:
Prof. Dr. Jan Schröer

Mitschriften von:
Tien Nguyen Thanh

WS 2021/2022
Stand: 16. Januar 2022

Inhaltsverzeichnis

1 Grundlagen

1.1 Mengen

Wir wollen uns mit einer sehr naiven, aber für unsere Zwecke ausreichenden, Mengenbegriff beschäftigen. Was eine Menge wirklich ist, erfahren wir von den Logikern und Mengentheoretikern.

Definition 1.1 (naive Menge)**.** Eine Menge M ist eine Zusammenfassung von verschiedenen Objekten, welche dann Elemente genannt werden, zu einem Objekt.

Beispiel 1.2.

- $\mathbb{N} \coloneqq \{0, 1, 2, \ldots\}$, die Menge der *natürliche Zahlen*. In dieser Vorlesung gehört die Null dazu.
- $\mathbb{Z} \coloneqq \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, die Menge der *ganze Zahlen*.
- $\mathbb{Q} \coloneqq \{a/b \mid a, b \in \mathbb{Z}, b \geq 1\}$, die Menge der *rationale Zahlen*.
- $\mathbb{R}$, die Menge der *rationalen Zahlen*.
- $\mathbb{C}$, die Menge der *komplexen Zahlen*.
- $\varnothing$, die leere Menge, die per Definition keine Elemente enthält.

Bezeichnung 1.3 (Quantoren, Mengenschreibweise, Relationen)**.** Einige häufig verwendete Symbole

- $(\ldots) \coloneqq (\ldots)$ definiert das, was links steht, durch das, was rechts steht.
- $\forall$ bedeutet „für alle“.
- $\exists$ bedeutet „es existiert“.
- Wenn M eine Menge ist, bezeichnet $|M|$ die Anzahl der Elemente in M (*Kardinalität*). Für die leere Menge ist $|\varnothing| = 0$.
- Eine Menge M heißt *n-elementig*, falls $|M| = n$ $(n \geq 0)$.
- Allgemein notieren wir Mengen bspw. durch

$$\{21, 35\} = \{x \in \mathbb{N} \mid 5 \leq x \leq 40, 7 \mid x, x \in \{7, 14, 28\}\}.$$

$\{\ \}$ sind Mengenklammern.

$|$ steht oft für „mit der Eigenschaft“. In unserem Beispiel heißt das „alle $x \in \mathbb{N}$ mit der Eigenschaft, dass ...“

, steht oft für „und“, eine logische Verknüpfung der Bedingungen bzw. Eigenschaften.

$\in$ steht für „ist Element von“. Hingegen ist $\notin$ „ist kein Element von“.

$=$ steht für „gleich“, d. h. links und rechts steht das gleiche und können gegenseitig ausgetauscht werden. Analog ist $\neq$ „ungleich“.

- $\leq, <, \geq, >$ sind „kleiner gleich“, „(echt) kleiner“, „größer gleich“, „(echt) größer“.

Bemerkung 1.4. Die Reihenfolge und Vielfachheit der Elemente in der Aufzählung von Mengen ist egal. Deshalb ist $\{1, 2, 3\} = \{2, 1, 3\} = \{1, 1, 3, 2, 3\}$.

Definition 1.5 (Teilmenge)**.** Seien A und B Mengen. Dann ist

- A eine *Teilmenge* von B, falls $x \in B$ für alle $x \in A$, geschrieben $A \subseteq B$, und
- A eine *echte Teilmenge* von B, falls $A \subseteq B$, aber $A \neq B$, geschrieben $A \subset B$.

Bemerkung 1.6. Für jede Menge M gilt $\varnothing \subseteq M$, aber $\varnothing \in M$ im Allgemeinen nicht.

Weiterhin definieren wir

Definition 1.7 (Mengenoperatoren)**.** Für Mengen A und B seien

- $A \cap B := \{x \mid x \in A, x \in B\}$ der *Durchschnitt* von A und B,
- $A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$ die *Vereinigung* von A und B,
- $A \setminus B := \{x \mid x \in A, x \notin B\}$ die *Mengendifferenz* von A und B,
- $\mathcal{P}(A) := \{U \mid U \subseteq A\}$ die *Potenzmenge* von A.

Definition 1.8 (Indexmenge)**.** Sei I eine *Indexmenge*, d. h. für jedes $i \in I$ ist A_i eine Menge. Dann sind

$$\bigcap_{i \in I} A_i := \{x \mid x \in A_i \text{ für alle } i \in I\} \qquad \text{und} \qquad \bigcup_{i \in I} A_i := \{x \mid \text{es gibt ein } i \in I \text{ mit } x \in A_i\}$$

der *Durchschnitt* bzw. *Vereinigung* der Mengen A_i über die Indexmenge I.

Beispiel 1.9.

- $\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$ ist 4-elementig.
- $\{1, 2, 3\} \cup \{2, 3\} = \{1, 2, 3\}$.
- $\{1, 2\} \setminus \{1, 3\} = \{2\}$. Die Differenzmenge $A \setminus B$ nimmt B von A weg.
- $\varnothing \cup \{1, 2\} = \{1, 2\} \neq \{\varnothing, 1, 2\} = \{\varnothing\} \cup \{1, 2\}$. Die Vereinigung mit der leeren Menge macht nichts.
- $\{\varnothing, \{1, 2, 3, 4\}\}$ ist 2-elementig, wohingegen $\{\varepsilon, 1, 2, 3, 4\}$ 5-elementig ist.

Definition 1.10 (Paar)**.** Ein *Paar* (oder *2-Tupel*) besteht aus der Angabe eines ersten Elements a und eines zweiten Elements b. Wir schreiben (a, b).

Bemerkung 1.11. Bei Paaren ist (im Gegensatz zu Mengen) die Reihenfolge wichtig. Es gilt $(a, b) = (b, a)$ genau dann, wenn $a = b$: *Achtung*: $(a, a) \neq \{a, a\} = \{a\}$.

Definition 1.12 (KARTESISCHES Produkt, Tupel)**.** Das *KARTESISCHE Produkt* zweier Mengen A und B ist $A \times B := \{(a, b) \mid a \in A, b \in B\}$.

Für Mengen $A_1, A_2, \ldots, A_n$ ist das *KARTESISCHE Produkt*

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } 1 \leq i \leq n\},$$

dessen Elemente *n-Tupel* genannt werden.

Sei A eine Menge und $n \geq 1$. Dann ist

$$A^n := \underbrace{A \times \cdots \times A}_{n \text{ mal}}$$

das *n-fache KARTESISCHE Produkt* von A.

Bemerkung 1.13. Zwei Tupel sind gleich, wenn sie gleich viele *Einträge* bzw. *Komponenten* haben und wenn an jeder Stelle die Komponenten gleich sind.

Bezeichnung 1.14. Die n-Tupel $(a_1, a_2, \ldots, a_n)$ schreiben wir oft auch senkrecht auf:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Beispiel 1.15. Sind A, B und C Mengen, dann sind die Elemente in $A \times B \times C$ 3-Tupel der Form (a, b, c), während die Elemente in $(A \times B) \times C$ 2-Tupel der Form $((a, b), c)$.

1.2 Logik

Definition 1.16 (Implikation, Äquivalenz)**.** Seien A, B und C Aussagen. Dann bedeuten

- $A \implies B$ „A impliziert B“, „aus A folgt B“,
- $A \iff B$ „A genau dann, wenn B“, „A und B sind äquivalent“, d. h. $A \implies B$ und $B \implies A$,
- $\neg A$, „nicht A“.

Zwei Schlussregeln, die wir oft verwenden werden:

Satz 1.17 (Syllogismus, Kontraposition)**.**

- *Aus $A \implies B$ und $B \implies C$ folgt $A \implies C$ (*Syllogismus*).*
- *Es gilt $A \implies B$ genau dann, wenn $\neg B \implies \neg A$ (*Kontraposition*).*

Beispiel 1.18.

$$\underbrace{\text{„Wenn es regnet,}}_{A}\ \underbrace{\text{ist die Straße nass.“}}_{B} \qquad (A \implies B)$$

ist äquivalent zu

$$\underbrace{\text{„Wenn die Straße nicht nass ist,}}_{\neg B}\ \underbrace{\text{dann regnet es nicht.“}}_{\neg A} \qquad (\neg B \implies \neg A)$$

1.2.1 Beweis durch Induktion

Für jedes natürliche $n \geq 1$ sei $A(n)$ eine Aussage. Wenn das Ziel ist, $A(n)$ für alle $n \geq 1$ zu zeigen, dann kann *vollständige Induktion* helfen. Die Beweisstrategie:

- *Induktionsanfang*: Wir zeigen, dass $A(1)$ richtig ist.
- *Induktionsschritt*: Wir nehmen an, dass $A(n)$ richtig ist. Damit beweisen wir, dass auch $A(n+1)$ richtig ist.

Das Beweisprinzip basiert auf dem Dominoeffekt: Mit dem Induktionsanfang ist $A(1)$ wahr. Mit dem Induktionsschritt folgt aus $A(1)$ auch $A(2)$. Wieder mit dem Induktionsschritt folgt aus $A(2)$ auch $A(3)$ usw. Damit haben wir die Aussagen $A(n)$ für alle $n \geq 1$ gezeigt.

Beispiel 1.19.

- Für alle $n \geq 1$ gilt $A(n)\colon \sum_{k=1}^{n}(2k-1) = n^2$.
  - *Induktionsanfang* ($n = 1$): $2 \cdot 1 - 1 = 1^2$ ist wahr und deshalb auch $A(1)$.

– *Induktionsschritt*: Es gilt

$$\sum_{k=1}^{n+1}(2k-1) = \left(\sum_{k=1}^{n}(2k-1)\right) + (2(n+1)-1) = n^2+2n+1 = (n+1)^2.$$

Dabei verwendeten wir für die zweite Gleichheit die Induktionsvoraussetzung. Folglich gilt $A(n+1)$.

- Ein falscher Induktionsbeweis: Wir behaupten, dass $A(n)$: (7 teilt 10^n) für alle $n \geq 1$ gilt.
  – *Induktionsschritt*: Angenommen $A(n)$ ist wahr, d. h. es gilt $10^n = 7a$ für ein $a \geq 1$ in $\mathbb{N}$. Dann gilt auch $10^{n+1} = 10 \cdot 10^n = 10 \cdot 7a$. Also gilt $A(n+1)$.
  – *Induktionsanfang*: Aber $A(1)$ ist falsch!

1.2.2 Beweis durch Widerspruch

Das Beweisprinzip ist, das Gegenteil der Behauptung anzunehmen und das auf einen Widerspruch mit der Voraussetzung zu führen. Folglich war die Annahme falsch und die Behauptung richtig.

Beispiel 1.20. *Behauptung*: $\sqrt{2} \notin \mathbb{Q}$.

Beweis: Angenommen $\sqrt{2} \in \mathbb{Q}$, d. h. Es gibt $a, b \in \mathbb{Z}$, $b \geq 1$ mit $\sqrt{2} = a/b$. Wir können annehmen, dass a und b teilerfremd sind (also der Bruch vollständig gekürzt ist).

Quadrieren liefert $2 = a^2/b^2 \iff 2b^2 = a^2$. Damit sind a^2 und a durch 2 teilbar, insbesondere auch a^2 durch $2 \cdot 2 = 4$ teilbar. Somit teilt 4 auch $2b^2$, also sind b^2 und b auch durch 2 teilbar (aufgrund der Eindeutigkeit der Primfaktorzerlegung). Das bedeutet, dass a und b durch 2 teilbar sind, was im Widerspruch zur Teilerfremdheit steht.

1.2.3 Gleichheit von Mengen

Bemerkung 1.21. Zwei Mengen sind *gleich*, wenn sie dieselben Elemente besitzen.

Seien A und B zwei Mengen. Um zu beweisen, dass $A = B$ ist, muss man zum Einen $A \subseteq B$ und zum Anderen $B \subseteq A$ zeigen. Der Beweis ist im Regelfall also zweiteilig!

1.3 Abbildungen

Die Idee hinter Abbildungen ist es, Mengen in Beziehung zu setzen.[1]

Definition 1.22 (Abbildung)**.** Seien X und Y Mengen. Eine *Abbildung* f von X nach Y ist eine Vorschrift, durch die jedem $x \in X$ genau ein $f(x) \in Y$ zugeordnet wird.[2]

Bemerkung 1.23. Jedes x wird genau einem $f(x)$ zugeordnet. Trotzdem ist es möglich, dass verschiedene x demselben $f(x)$ zugeordnet werden.

Bemerkung 1.24. Zwei Abbildungen sind gleich, wenn sie dieselben Definitions- und Zielmengen haben sowie elementweise bzw. punktweise gleich sind (d. h. deren Vorschrift dasselbe macht).

Bezeichnung 1.25. Wir schreiben $f\colon X \to Y$, $x \mapsto f(x)$. Dabei verwenden wir $\to$ zwischen Mengen und $\mapsto$ zwischen Elementen.

Definition 1.26 (Menge aller Abbildungen)**.** Seien X und Y Mengen. Dann ist $\mathrm{Abb}(X,Y)$ die *Menge aller Abbildungen* von X nach Y.

Beispiel 1.27. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{N}$, $x \mapsto x^2$ bildet jedes $x \in \mathbb{Z}$ auf $x^2 \in \mathbb{N}$ ab.

Definition 1.28 (Identität)**.** Sei X eine Menge. Als *Identität* von X bezeichnen wir die Abbildung $\mathrm{id}_X\colon X \to X$, $x \mapsto x$. Es gilt also $\mathrm{id}_X(x) = x$ für alle $x \in X$.

[1] Eigentlich sind es die *Relationen* die das erfüllen, wovon Abbildungen eine spezielle Form sind.

[2] Die Menge X bezeichnen wir als *Definitionsmenge* und Y als *Zielmenge*. Die Elemente aus X heißen *Urbilder* oder *Argumente*, die Elemente aus Y heißen *Zielelemente*. Die tatsächlich angenommen Werte nennen wir *Bilder* oder schlicht *Werte*, und deren Menge auch *Bild* oder *Bildmenge*.

Definition 1.29 (Komposition von Abbildungen)**.** Seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen. Dann ist

$$g \circ f\colon X \to Z, \quad x \mapsto g(f(x))$$

die *Komposition* (*Hintereinanderschaltung*, *Verkettung*) von f und g, gelesen „g verknüpft mit f“, „g komponiert mit f“, „g nach f“ oder „g Kringel f“.

Bezeichnung 1.30. Wir schreiben auch manchmal gf für $g \circ f$.

Es gilt also

$$X \xrightarrow{f} Y \xrightarrow{g} Z \ , \qquad x \longmapsto f(x) \longmapsto g(f(x)) \ .$$

Definition 1.31 (injektiv, surjektiv, bijektiv)**.** Sei $f\colon X \to Y$ eine Abbildung. Dann ist

- f *text*, falls für alle $x_1 \neq x_2$ in X gilt: $f(x_1) \neq f(x_2)$,
- f *surjektiv*, falls für jedes $y \in Y$ ein $x \in X$ existiert, sodass $f(x) = y$ ist, und
- f *bijektiv*, falls f injektiv und surjektiv ist. Dann nennen wir f eine *Bijektion*.

Definition 1.32 (Umkehrabbildung)**.** Sei $f\colon X \to Y$ eine bijektive Abbildung. Dann ist die *Umkehrabbildung* $f^{-1}\colon Y \to X$ definiert durch $f^{-1}(f(x))\colon x$ für alle $x \in X$ bzw. $f(x) \in Y$.
Es gilt dann $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$.

Umkehrabbildungen kann es nur für Bijektionen geben. Da auch f^{-1} eine Abbildung sein soll und Abbildungen jedem $y \in Y$ *genau ein* $x \in X$ zuordnet, müssen wir die Injektivität von f voraussetzen. Dann sind nämlich $f^{-1}(f(x_1))$ und $f^{-1}(f(x_2))$ für $x_1, x_2 \in X$ mit $x_1 \neq x_2$ auch unterschiedlich. Da f^{-1} von Y nach X abbilden soll, muss $f^{-1}(y)$ für alle Y definiert werden, weshalb wir die Surjektivität voraussetzen müssen. Dann gibt es für jedes $y \in Y$ ein $x \in X$ mit $y = f(x)$, sodass $f^{-1}(y) = x$ wohldefiniert[3] ist.

Auch die Komposition der Abbildung und dessen Umkehrung ergibt Sinn: $f^{-1} \circ f$ bildet von X nach Y und wieder nach X ab, und $f \circ f^{-1}$ bildet von Y nach X und wieder nach Y ab.

Beispiel 1.33.

1. $f\colon \{1,2,3\} \to \{1,2\}$ mit $1 \mapsto 1$, $2 \mapsto 1$ und $3 \mapsto 2$ ist surjektiv, aber nicht injektiv.
2. $f\colon \{1,2\} \to \{1,2,3\}$ mit $1 \mapsto 3$ und $2 \mapsto 1$ ist injektiv, aber nicht surjektiv.
3. $f\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x - 41$ ist injektiv und surjektiv, also bijektiv.
4. $f\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$ ist injektiv, aber nicht surjektiv (die ungeraden Zahlen werden nicht getroffen).
5. $f\colon \mathbb{Z} \to \mathbb{Z}$ mit $2n \mapsto n$ und $2n+1 \mapsto n$ (für $n \in \mathbb{Z}$) ist surjektiv, aber nicht injektiv.
6. Seien X und Y zwei endliche Mengen mit gleich vielen Elementen. Dann ist die Abbildung $f\colon X \to Y$ genau dann injektiv, wenn f surjektiv ist.
7. Die Abbildung $f\colon \{\text{Menschen in Bonn}\} \to \mathbb{N}$ definiert durch $x \mapsto \mathrm{Alter}(x)$ ist weder surjektiv (Menschen werden nicht beliebig alt) noch injektiv (zwei Menschen können dasselbe Alter haben).
8. Für ein fixiertes $(a,b,c,d) \in \mathbb{Q}^4$ definieren wir $f\colon \mathbb{Q}^2 \to \mathbb{Q}^2$, $(x,y) \mapsto (ax+by, cx+dy)$. Die Abbildung f ist genau dann bijektiv, wenn $ad - bc \neq 0$ gilt. Außerdem ist f genau dann injektiv, wenn f surjektiv ist. (Der Beweis dafür erfolgt später.)[4]

Ende der Vorlesung 1 am 12. Oktober 2021

[3] Der Begriff *wohldefiniert* meint, dass ein Begriff eindeutig und widerspruchsfrei definiert ist, also weder unmöglich noch mehrdeutig ist.

[4] Das ist das Matrix-Vektor-Produkt, wobei a,b,c,d die Einträge einer Matrix $A \in \mathbb{Q}^{2,2}$ ist und x,y die Einträge eines Vektors v. Dann ist A genau dann ein Isomorphismus, wenn A invertierbar ist, also $ad - bc \neq 0$. Genauso ist eine quadratische Matrix genau dann ein Monomorphismus, wenn sie ein Epimorphismus ist.

Definition 1.34. Seien M und I Mengen. Dann sei

$$M^I := \mathrm{Abb}(I, M)$$

die *Menge aller Abbildungen* $I \to M$.

Achtung: Es sind die Abbildungen von I nach M, nicht von M nach I!

Beispiel 1.35. Für $I = \{1, \dots, n\}$ ist die Abbildung $M^I \to M^n$, $f \mapsto (f(1), \dots, f(n))$ bijektiv, wobei M^n bekanntlich das n-fache kartesische Produkt bezeichnet.

Offensichtlich haben alle $f \in M^I$ dieselben Definitions- und Zielmengen. Dann sind zwei Abbildungen genau dann gleich, wenn sie für jedes Argument denselben Wert liefern, d. h. wenn die Tupel ihrer Werte gleich sind. Andersherum definiert jedes Tupel eine Abbildung, denn es gibt alle möglichen Zuordnungen $I \to M$ an.[5]

Achtung: Die hier beschriebene Abbildung bildet *Abbildungen* f auf n*-Tupel derer Werte* ab.

Definition 1.36 (Bild, Urbild einer Menge)**.** Sei $f\colon X \to Y$ eine Abbildung. Und seien $A \subseteq X$ und $B \subseteq Y$ Teilmengen. Wir bezeichnen

$$f(A) := \{f(x) \mid x \in A\} \qquad \text{und} \qquad f^{-1}(B) := \{x \mid f(x) \in B\}$$

als *Bild* von A unter f bzw. *Urbild* von B unter f. Dahingegen ist $f(X)$ das *Bild* von f. Es gilt stets $f^{-1}(Y) = X$.

Warnung: Die Schreibweise $f^{-1}(B)$ impliziert nicht, dass eine Umkehrabbildung existiert.

Bemerkung 1.37. Wir beachten, dass das nicht jedes $y \in B$ ein Urbild $\in f^{-1}(B)$ haben muss, ähnlich wie eine Abbildung nicht surjektiv sein muss. Genauso kann es mehrere Urbilder $x_1, x_2 \in f^{-1}(B)$ mit $x_1 \neq x_2$ zu einem Bild y mit $f(x_1) = f(x_2) = y$ geben, ähnlich wie eine Abbildung nicht injektiv sein muss.

Definition 1.38 (Graph)**.** Der *Graph* einer Abbildung $f\colon X \to Y$ ist

$$\Gamma(f) := \{(x, f(x)) \mid x \in X\} \subseteq X \times Y.$$

Der Graph ist also eine „Zeichnung“ der Funktion, also die Menge aller Punkte der „Ebene“, die zur Funktion „gehören“.

Bemerkung 1.39. Damit können wir den Begriff der Abbildung mengentheoretisch definieren. Seien X und Y Mengen, und sei $\Gamma \subseteq X \times Y$ (eine Relation) eine Menge von Paaren mit den folgenden Eigenschaften:

1. Für jedes $x \in X$ gibt es ein $y \in Y$ mit $(x, y) \in \Gamma$ (jedem Urbild wird ein Bild zugeordnet).

2. Falls $(x, y_1), (x, y_2) \in \Gamma$, so ist $y_1 = y_2$ (das Bild eines Urbilds ist eindeutig).

Damit definieren wir eine *Abbildung* $f_\Gamma\colon X \to Y$ durch $f_\Gamma(x) := y$ für jedes $(x, y) \in \Gamma$. Offensichtlich gilt für den Graphen $\Gamma(f_\Gamma) = \Gamma$.

1.4 Übungsaufgaben

Aufgabe 1.A (B01.A1)**.** Seien X und Y Mengen. Beweisen Sie die Äquivalenz folgender Aussagen:

(i) $X \subseteq Y$,

(ii) $X \cap Y = X$,

(iii) $X \cup Y = Y$,

(iv) $X \setminus Y = \varnothing$.

Lösung. Wegen dem Syllogismus in Satz 1.17 können wir die Äquivalenz mehrerer Aussagen effizient zeigen, indem wir im „Kreis“ schlussfolgern, z. B. (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (i).

Beweis.

[5] In fortgeschrittener Sprache: Die Abbildung ist ein *Mengenisomorphismus*, also ein bijektiver Homomorphismus, der die Mengenstruktur (auch wenn sehr banal) erhält.

1. (i) $\implies$ (ii): Wenn jedes $x \in X$ auch in Y liegt, ist die Bedingung $x \in Y$ in der Definition der Schnittmenge $X \cap Y = \{x \in X \mid x \in Y\}$ redundant. Deshalb gilt $X \cap Y = \{x \in X\} = X$.

2. (ii) $\implies$ (iii): Nach Voraussetzung müssen wir uns die Vereinigung $(X \cap Y) \cup Y$ anschauen. Da nun nach Definition der Schnittmenge $X \cap Y \subseteq Y$ gilt, erhalten wir $(X \cap Y) \cup Y = Y$.

3. (iii) $\implies$ (iv): Nach Voraussetzung können wir uns $X \setminus (X \cup Y)$ anschauen. Gemäß der Definition der Vereinigung gilt stets $X \in X \cup Y$, d. h. in der Mengendifferenz nehmen wir von X mindestens alle Elemente von X weg, also ist $X \setminus (X \cup Y) = \varnothing$.

4. (iv) $\implies$ (i): Wenn nach der Differenz $X \setminus Y = \{x \in X \mid x \notin Y\}$ keine Elemente übrig bleiben, so haben alle $x \in X$ die Bedingung $x \notin Y$ nicht erfüllt, d. h. es gilt $x \in Y$ für alle $x \in X$ und damit $X \subseteq Y$. □

Eine alternative, sehr mengentheoretische, aber auch prägnante Lösung ist folgende:

Beweis.

$$
\begin{aligned}
&\text{(i)} \implies \text{(ii)}: && X = X \cap X \subseteq X \cap Y \subseteq X,\\
&\text{(ii)} \implies \text{(iv)}: && \varnothing \subseteq X \setminus Y = (X \cap Y) \setminus Y \subseteq Y \setminus Y = \varnothing,\\
&\text{(iv)} \implies \text{(iii)}: && X \cup Y = \big((X \setminus Y) \cup (X \cap Y)\big) \cup Y = (X \setminus Y) \cup \big((X \cap Y) \cup Y\big)\\
& && \quad = (X \setminus Y) \cup Y = \varnothing \cup Y = Y,\\
&\text{(iii)} \implies \text{(i)}: && X = X \cup \varnothing \subseteq X \cup Y = Y.
\end{aligned}
$$
□

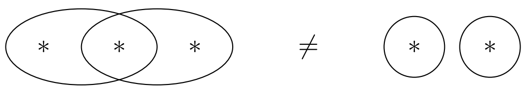
Aufgabe 1.B (B01.A2)**.** Diskutieren Sie den folgenden Induktionsbeweis:

Behauptung: Für jedes $n \geq 1$ gilt: Halten sich n Personen in einem geschlossenen Raum auf, so sind entweder alle geimpft oder alle sind ungeimpft.

Beweis mit Induktion: Der Fall $n = 1$ ist klar. Die Aussage sei nun wahr für n. Sind dann $n + 1$ Personen im Raum, so wähle eine Person aus und schicke sie hinaus. Nach Induktionsannahme haben die verbleibenden Personen denselben Impfstatus. Wir holen die ausgewählte Person wieder herein und senden eine andere Person hinaus. Die im Raum verbliebenen n haben wiederum denselben Impfstatus. Damit hat die zuerst hinaus gesandte Person denselben Impfstatus wie alle anderen im Raum befindlichen Personen. Da dies nach dem ersten Beweisschritt auch für die als zweites hinaus gesandte Person zutrifft, haben alle $n+1$ Personen denselben Impfstatus.

Lösung. Der Induktionsschritt ist eine gute Beweisstrategie, funktioniert aber nur für $n \geq 3$ und versagt bei $n = 2$.

Ein Gegenbeispiel für $n = 2$: Im Raum ist ein Geimpfter und ein Ungeimpfter. Geht eine Person raus, haben die verbleibenden Personen im Raum immer denselben Impfstatus (weil nur eine Person verbleibt). Es fehlen aber Dritte, mit denen wir zu beiden Zeitpunkten den Impfstatus der Personen, die den Raum verlassen, vergleichen können.



Aufgabe 1.C. Zeigen Sie: Für alle $n \geq 1$ gilt

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1.40}$$

Lösung. Beweis. Wir führen eine vollständige Fallunterscheidung über n durch. Dabei ist $A(n)$ (1.40).

- *Induktionsanfang*: Für $n = 1$ ist $1^2 = \frac{1}{6}(1 \cdot 2 \cdot 3)$ wahr und folglich ist auch $A(1)$ wahr.
- *Induktionsschritt*: Wenn $A(n)$ gilt, gilt auch

$$
\begin{aligned}
\sum_{k=1}^{n+1} k^2 &= (n+1)^2 + \sum_{k=1}^{n} k^2 \overset{A(n)}{=} (n+1)^2 + \frac{n(n+1)(2n+1)}{6} = \frac{n+1}{6}\big(6(n+1) + n(2n+1)\big)\\
&= \frac{n+1}{6}\big((4n+6) + n(2n+3)\big) = \frac{(n+1)(n+2)(2n+3)}{6},
\end{aligned}
$$

also ist auch $A(n+1)$ wahr. □

Alternativ können wir das auch nicht induktiv über Teleskopsummen zeigen.

Beweis. In der Summe heben sich der Minuend k^3 des Index i mit dem Subtrahenden $-(k-1)^3$ des Index $i+1$ auf. Damit gilt

$$n^3 = \sum_{k=1}^{n} \big(k^3 - (k-1)^3\big) = 3\sum_{k=1}^{n} k^2 - 3\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1 = 3\sum_{k=1}^{n} k^2 - 3\frac{n(n+1)}{2} + n$$
$$\iff \sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} = \frac{n(n+1)(2n+1)}{6}. \qquad \square$$

2 Körper

Auch *Rechenbereich* genannt. Körper verallgemeinern und abstrahieren die uns gewohnten rationalen oder reellen Zahlen und deren Rechenoperationen. Dennoch sollten wir uns ab sofort von den uns bekannten Beispielen lösen, da die in der (linearen) Algebra betrachteten Objekte sehr abstrakt werden und nicht unbedingt analog zu unserem Vorwissen funktionieren.

2.1 Körperaxiome

Axiom 2.1 (Körper)**.** Ein *Körper* ist eine Menge K zusammen mit zwei Abbildungen

$$+\colon K \times K \to K, \quad (a,b) \mapsto a+b \qquad \text{und} \qquad \cdot\colon K \times K \to K, \quad (a,b) \mapsto a \cdot b,$$

Addition bzw. *Multiplikation* genannt, sodass folgende Regeln (Axiome) gelten:

(A1) $a + (b + c) = (a + b) + c$ für alle $a, b, c \in K$ (*Assoziativität der Addition*);

(A2) $a + b = b + a$ für alle $a, b \in K$ (*Kommutativität der Addition*);

(A3) Es existiert ein Element $0 = 0_K \in K$ mit $a + 0 = a$ für alle $a \in K$ (Existenz eines *Nullelements*);

(A4) Zu jedem $a \in K$ gibt es ein $-a \in K$ mit $a + (-a) = 0$ (Existenz eines *additiven Inversen*);

(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in K$ (*Assoziativität der Multiplikation*);

(M2) $a \cdot b = b \cdot a$ für alle $a, b \in K$ (*Kommutativität der Multiplikation*);

(M3) Es existiert ein Element $1 = 1_K \in K$ mit $1 \neq 0$ und $1 \cdot a = a$ für alle $a \in K$ (Existenz eines *Einselements*);

(M4) Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein $a^{-1} \in K$ mit $a \cdot a^{-1} = 1$ (Existenz des *multiplikativen Inversen*);

(D) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ für alle $a, b, c \in K$ (*Distributivität*).

Oftmals lassen wir den Index K wie in 0_K und 1_K weg, wenn der Kontext klar ist. Manchmal schreiben wir ihn aber hinzu, um zu verdeutlichen, dass sie zum Körper K gehören.

Bemerkung 2.2. Wir setzen $1 \neq 0$ voraus, d. h. ein Körper hat mindestens zwei Elemente.[1]

Bemerkung 2.3. Dabei steht der Ausdruck $a + b$ eigentlich für $+\big((a,b)\big)$ und $a \cdot b$ für $\cdot\big((a,b)\big)$. Streng genommen müssten wir z. B. Axiom (A1) als

$$a + (b + c) = (a + c) + b \quad \longrightarrow \quad +\Big(\big(a, +\big((b,c)\big)\big)\Big) = +\Big(\big(+\big((a,b)\big), c\big)\Big)$$

und Axiom (A2) als

$$a + b = b + a \quad \longrightarrow \quad +\big((a,b)\big) = +\big((b,a)\big)$$

schreiben.

Bezeichnung 2.4. Neben diesen Axiomen führen wir noch einige Konventionen ein.

[1] Traditionell wird in der Algebra $1 \neq 0$ definiert. Es gibt aber „esoterische“ Konzepte eines einelementigen Körpers $\mathbb{F}_1$, d. h. $1 = 0$, was aber einige Körpereigenschaften verliert.

- Um Klammern zu sparen, gilt *Punktrechnung vor Strichrechnung*. Damit können wir z. B. das Distributivgesetz (D) umschreiben als $a \cdot c + b \cdot c$, ohne dass Verwirrung entsteht.
- Wir definieren $a - b := a + (-b)$ und $ab := a \cdot b$ für $a, b \in K$. Somit können wir Plusklammern und Malpunkte weglassen, wenn der Sinn dabei nicht verfälscht wird (z. B. nicht $1 \cdot 2 \neq 12$).
- Für $a, b \in K$ mit $b \neq 0$ sei
$$\frac{a}{b} := a/b := a \cdot b^{-1}.$$

Diese Regeln und Schreibweisen sind alles Konventionen und hängen nicht mit der Struktur oder den Eigenschaften eines Körper zusammen. Wir hätten genauso jede andere Konvention einführen können.

Bezeichnung 2.5. Wir definieren kurz $K^\times := K \setminus \{0\}$.

Ab sofort meinen wir mit K immer einen Körper mit den Operationen $+$ und $\cdot$, falls nicht anders spezifiziert. Manchmal schreiben wir auch $(K, +, \cdot)$ für einen Körper.

2.2 Beispiele von Körpern

Beispiel 2.6. $\mathbb{Q}$ und $\mathbb{R}$ mit den üblichen Abbildungen $+$ und $\cdot$ sind Körper.

Beispiel 2.7. $\mathbb{Z}$ ist kein Körper, da (nur) (M4) nicht erfüllt wird.

Beispiel 2.8. $\mathbb{C}$, die Menge der komplexen Zahlen mit $+$ und $\cdot$ ist ein Körper.

Beispiel 2.9. Sei $K := \{a, b\}$ mit $a \neq b$. Wir definieren die Abbildungen $+ \colon K \times K \to K$ und $\cdot \colon K \times K \to K$ durch[2]

$$\begin{aligned} a + a &= a, & a + b &= b, & b + a &= b, & b + b &= a, \\ a \cdot a &= a, & a \cdot b &= a, & b \cdot a &= a, & b \cdot b &= b. \end{aligned}$$

K erfüllt alle Axiome eines Körpers, wobei das Nullelement $0_K = a$ und das Einselement $1_K = b$ ist, also $K = \mathbb{F}_2 := \{0, 1\}$. Der Körper ist der kleinstmögliche Körper (jeder Körper muss mindestens 0 und 1 enthalten). Tatsächlich ist der Körper sogar eindeutig, was wir aber nicht beweisen werden.

Beispiel 2.10. Sei $K := \mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$.[3] Wir definieren die Abbildungen $+ \colon K \times K \to K$ und $\cdot \colon K \times K \to K$ als Einschränkung von $+ \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ und $\cdot \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (d. h. die Abbildungen sind dieselben aus $\mathbb{R}$ bis auf den kleineren Definitionsbereich). Insbesondere heißt das

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) := (a + c) + (b + d)\sqrt{2}$$

und

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) := (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Die meisten Körperaxiome sind offensichtlich erfüllt. Für (M4) stellt sich jedoch die Frage, ob $(a+b\sqrt{2})^{-1} \in K$ für alle $a + b\sqrt{2} \neq 0$ existiert. *Antwort*: Ja, denn

$$(a + b\sqrt{2}) - 1 := \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

mit

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{1}{a + b\sqrt{2}}.$$

Beachte: Die Brüche sind definiert, weil $(a/b)^2 \neq 2 \iff a^2 - 2b^2 \neq 0$ wegen $\sqrt{2} \notin \mathbb{Q}$.

[2] Die Abbildungen ähneln der Addition und Multiplikation modulo 2.

[3] Das ist eine sog. Körperadjunktion bzw. Körpererweiterung

2.3 Rechenregeln in Körpern

Lemma 2.11 (Linksdistributivität)**.** *Es gilt* $a(b+c) = ac + ac$ *für alle* $a, b, c \in K$*.*

Beweis. Es gilt $a(b+c) \overset{\text{(M2)}}{=} (b+c)a \overset{\text{(D)}}{=} ba + ca \overset{\text{(M2)}}{=} ab + ac$. □

Lemma 2.12 (Eindeutigkeit der Null)**.** *Es gibt nur ein Nullelement in einem Körper.*

Beweis. Seien $0'$ und $0''$ Nullelemente im Körper K. Dann gilt $0'' \overset{\text{(A3)}}{=} 0'' + 0' \overset{\text{(A2)}}{=} 0' + 0'' \overset{\text{(A3)}}{=} 0'$. Dabei haben wir für die erste Gleichheit die Eigenschaft $0' = 0_K$ und für die letzte Gleichheit $0'' = 0_K$ ausgenutzt. □

Lemma 2.13. *Für alle* $a \in K$ *gilt* $0a = 0$*.*

Beweis. Sei $a \in K$. Dann gelten

$$0a \overset{\text{(A3)}}{=} (0+0)a \overset{\text{(D)}}{=} 0a + 0a, \tag{2.14}$$

$$0 \overset{\text{(A4)}}{=} 0a + (-(0a)) \overset{(2.14)}{=} (0a + 0a) + (-(0a)) \overset{\text{(A1)}}{=} 0a + (0a + (-(0a))) \overset{\text{(A4)}}{=} 0a + 0 \overset{\text{(A3)}}{=} 0a.$$ □

In den Übungsaufgaben werden wir noch eine Vielzahl weiterer Regeln beweisen.

2.4 Charakteristik eines Körpers

Bezeichnung 2.15. Sei K ein Körper. Für $a \in K$ und $0 \neq m \in \mathbb{N}$ definieren wir

$$m \cdot a := \underbrace{a + a + \cdots + a}_{m \text{ mal}}.$$

Definition 2.16 (Charakteristik)**.** Wir definieren $\operatorname{char}(K)$ als die *Charakteristik* von K als

$$\operatorname{char}(K) := \begin{cases} 0 & \text{falls } m \cdot 1_K \neq 0_K \text{ für alle } m \in \mathbb{N} \setminus \{0\}, \\ \min\{m \in \mathbb{N} \setminus \{0\} \mid m \cdot 1_K = 0_K\} & \text{sonst.} \end{cases}$$

Lemma 2.17. *Sei* K *ein Körper mit* $\operatorname{char}(K) = p > 0$*. Dann ist* p *eine Primzahl.*

Beweis. Angenommen p wäre keine Primzahl, sodass es $p_1, p_2 \in \mathbb{N}$ mit $p_1, p_2 \geq 2$ und $p = p_1 p_2$ gibt. Aus der Minimalität der Charakteristik folgt $p_1 \cdot 1_K \neq 0$ und $p_2 \cdot 1_K \neq 0$. Damit gilt

$$(p_1 \cdot 1_K)(p_2 \cdot 1_K) = (p_1 p_2) \cdot 1_K = p \cdot 1_K = 0_K.$$

Aufgrund der Nullteilerfreiheit in einem Körper (s. Übungsaufgabe) gilt $p_1 \cdot 1_K = 0_K$ oder $p_2 \cdot 1_K = 0_K$, ein Widerspruch.[4] □

Ende der Vorlesung 2 am 15. Oktober 2021

[4] Die Charakteristik hat einige interessante Eigenschaften:
Aus einer positiven Charakteristik folgt sofort $a + a + \dots a = 0$. Sie hilft und zu bestimmen, wann ein Ausdruck null wird, was wichtig für das Rechnen im Körper ist (wir denken an $a + 0 = 0$, $0a = 0$ und, dass 0^{-1} nicht existiert). In diesem Kontext ist $\operatorname{char}(K) = 2$ besonders wichtig, denn in dem Fall ist $a + a = 0$ für alle $a \in K$, d. h. jedes Element ist sein eigenes additives Inverse. $\operatorname{char}(K) \neq 2$ garantiert uns die Existenz der $2 := 1 + 1$.
Jeder Teilkörper eines Körpers hat dieselbe Charakteristik wie der Körper, z. B. $\operatorname{char}(\mathbb{F}_2) = \operatorname{char}(\mathbb{F}_4) = 2$. Damit haben Körper mit gleicher Charakteristik auch eine ähnliche Struktur.
Die Charakteristik ist eigentlich für Ringe (die später folgen) definiert. All diese Eigenschaften gelten auch für Ringe.

2.5 Die Ringe $\mathbb{Z}_m$

Axiom 2.18 (Ring)**.** Ein *Ring* ist eine Menge R zusammen mit zwei Abbildungen

$$+\colon R \times R \to R, \quad (a,b) \mapsto a+b \qquad \text{und} \qquad \cdot\colon R \times R \to R, \quad (a,b) \mapsto a \cdot b$$

Addition bzw. *Multiplikation* genannt, sodass folgende Regeln (Axiome) gelten:

(A1) $a + (b + c) = (a + b) + c$ für alle $a, b, c \in R$ (*Assoziativität der Addition*);

(A2) $a + b = b + a$ für alle $a, b \in R$ (*Kommutativität der Addition*);

(A3) Es existiert ein Element $0 = 0_R \in R$ mit $a + 0 = a$ für alle $a \in R$ (Existenz eines *Nullelements*);

(A4) Zu jedem $a \in R$ gibt es ein $-a \in R$ mit $a + (-a) = 0$ (Existenz eines *additiven Inversen*);

(R1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$ (*Assoziativität der Multiplikation*);

(R2) Es existiert ein Element $1 = 1_R \in R$ mit $1 \neq 0$ und $1 \cdot a = a$ für alle $a \in R$ (Existenz eines *Einselements*);

(D) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ und $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ für alle $a, b, c \in K$ (*Distributivität*).

Definition 2.19 (kommutativer Ring)**.** Ein Ring R heißt *kommutativ*, falls zusätzlich $a \cdot b = b \cdot a$ für alle $a, b \in \mathbb{R}$ gilt.

Bemerkung 2.20. Im Vergleich zu einem Körper sind die Axiome der Addition identisch. Bei der Multiplikation fehlt lediglich die Kommutativität (M2) und die Existenz des Inversen (M4). Aufgrund der fehlenden Kommutativität werden in der Distributivität beide Multiplikationsreihenfolgen angeben, die wir auch beide nachweisen müssen.

Bemerkung 2.21. In einem Ring wird nicht verlangt, dass $1_R \neq 0_R$. Ist aber $1_R = 0_R$, so folgt daraus $a = 1_R a = 0_R a = 0_R$ für alle $a \in R$, also $R = \{0_R\}$.

Bezeichnung 2.22 (Nullring)**.** Wir nennen $R = \{0_R\}$ den trivialen[5] *Nullring*.

Wir übernehmen für Ringe alle Schreibkonventionen in bezeichnung 2.4, die wir für Körper festlegten (bis auf Brüche).

Lemma 2.23. *Seien $a, m \in \mathbb{N}$ mit $m \geq 1$. Dann existieren eindeutig bestimmte Elemente $r, q \in \mathbb{N}$ mit $0 \leq r < m$, sodass $a = qm + r$ gilt. Setze $r_m(a) := r$.*

Beweis. Zu jedem $a \in \mathbb{N}$ gibt es ein eindeutig bestimmtes $q \in \mathbb{N}$ mit $qm \leq a < (q + 1)m$. Mit $r := a - qm$ folgt die Behauptung. □

Definition 2.24 ($\mathbb{Z}$ modulo m)**.** Sei $m \in \mathbb{N}$ mit $m \geq 2$. Dann sei $\mathbb{Z}_m := \{0, 1, \ldots, m - 1\}$. Für $a, b \in \mathbb{Z}_m$ definieren wir noch Abbildungen $+$ und $\cdot$ durch $a + b := r_m(a +_{\mathbb{Z}} b)$ und $a \cdot b := r_m(a \cdot_{\mathbb{Z}} b)$. (Die Operationen in den $r_m(\ldots)$ kommen aus $\mathbb{Z}$.)

Manchmal ist es hilfreich, auch die Operatoren aus verschiedenen Mengen durch Subskripte zu unterscheiden, also $+_K$, $\cdot_R$, etc.

Lemma 2.25. *$(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring.*[6]

Beweis. Übungsaufgabe. □

Lemma 2.26. *$(\mathbb{Z}_m, +, \cdot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis. Angenommen $\mathbb{Z}_m$ ist ein Körper. Dann folgt $\operatorname{char}(\mathbb{Z}_m) = m$ aus der Definition der Addition über die Addition in $\mathbb{Z}$ (in $\mathbb{Z}$ ist $m1 = 1 + 1 + \cdots + 1 = m$). Nach Lemma 2.17 ist m eine Primzahl.

Für die Umkehrung sei nun m eine Primzahl. Zuerst zeigen wir, dass $\mathbb{Z}_m$ nullteilerfrei ist. Seien $a, b \in \mathbb{Z}_m$ mit $a \cdot b = 0 = r_m(a + b)$. Folglich wird ab von m geteilt (Rest 0). Da m eine Primzahl ist, folgt (aus dem *Lemma von* Euklid): m teilt a oder m teilt b. Weil nun $0 \leq a, b < m$ ist, muss $a = 0$ oder $b = 0$ sein. Folglich haben wir gezeigt, dass $\mathbb{Z}_m$ nullteilerfrei ist.

[5] Als *triviale* Objekte werden oft offensichtliche oder sehr einfache Objekte sowie uninteressante Randfälle bezeichnet.
[6] Ein sog. *Restklassenring modulo m*.

Nun zeigen wir, dass jedes $a \in \mathbb{Z}_m$ mit $a \neq 0$ ein multiplikatives Inverses besitzt. Für solche a definieren wir die Abbildung $\rho_a \colon \mathbb{Z}_m \to \mathbb{Z}_m$, $x \mapsto xa$. Dann ρ_a ist injektiv: Aus $xa = \rho_a(x) = \rho_a(y) = ya \iff (x-y)a = 0$ folgt aufgrund Nullteilerfreiheit $x - y = 0 \iff x = y$. Da $\mathbb{Z}_m$ endlich ist, ist ρ_a auch surjektiv.

Aus der Bijektion folgt, dass $0a, 1a, \ldots, (m-1)a$ paarweise verschieden sind (injektiv), und diese Elemente auch jedes Element aus $\mathbb{Z}_m$ repräsentiert (surjektiv), insbesondere die 1. Es gibt also ein $x \in \mathbb{Z}_m$ mit $xa = 1$. Zu jedem $a \in \mathbb{Z}_m \setminus 0$ gibt es also ein multiplikatives Inverses $x \in \mathbb{Z}_m$, sprich a ist invertierbar, was Axiom (M4) erfüllt. Die restlichen Körperaxiome folgen aus dem kommutativen Ring. □

Vom kommutativen Ring zum Körper fehlt nur noch die Existenz des multiplikativen Inversen. Hierfür haben wir alle möglichen Kandidaten für das Inverse betrachtet, also $0a, 1a, \ldots, (m-1)a$. Wir beobachten, dass diese Menge genau $\mathbb{Z}_m$ entspricht, es also eine einfache Bijektion ρ_a geben muss, die wir auch beweisen haben. Der Trick hier war zu zeigen, dass $\mathbb{Z}_m$ nullteilerfrei ist (ein gutes Zeichen, da Nullteilerfreiheit eine Körpereigenschaft ist).

Bezeichnung 2.27 (endlicher Körper)**.** Für Primzahlen p schreiben wir auch $\mathbb{F}_p \coloneqq \mathbb{Z}_p$.

3 Vektorräume

Vektorräume sind wichtige Objekte, die in vielen Bereichen der Mathematik vorkommen. Das Ziel der linearen Algebra ist es, eine „Theorie der Vektorräume“ zu entwickeln und dabei die Eigenschaften von Vektorräumen zu erforschen.

3.1 Vektorraumaxiome

Axiom 3.1 (Vektorraum)**.** Sei K ein Körper. Ein *Vektorraum über K* oder *K-Vektorraum* ist eine Menge V zusammen mit zwei Abbildungen

$$+ \colon V \times V \to V, \quad (v_1, v_2) \mapsto v_1 + v_2 \qquad \text{und} \qquad \cdot \colon K \times V \to V, \quad (a, v) \mapsto a \cdot v,$$

Addition bzw. *Skalarmultiplikation* genannt, sodass folgende Regeln (Axiome) gelten:

(A1) $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ für alle $v_1, v_2, v_3 \in V$ (*Assoziativität der Addition*);

(A2) $v_1 + v_2 = v_2 + v_1$ für alle $v_1, v_2 \in V$ (*Kommutativität der Addition*);

(A3) Es existiert ein Element $0 = 0_V \in V$ mit $v + 0_V = v$ für alle $v \in V$ (Existenz eines *Nullelements*);

(A4) Zu jedem $v \in V$ gibt es ein $-v \in V$ mit $v + (-v) = 0$ (Existenz eines *additiven Inversen*);

(SM1) $(ab) \cdot v = a \cdot (b \cdot v)$ für alle $a, b \in K$ und $v \in V$;

(SM2) $1_K \cdot v = v$ für alle $v \in V$;

(SM3) $a \cdot (v_1 + v_2) = a \cdot v_1 + a \cdot v_2$ für alle $a \in K$ und $v_1, v_2 \in V$;

(SM4) $(a + b) \cdot v = (a \cdot v) + (b \cdot v)$ für alle $a, b \in K$ und $v \in V$.

Wir schreiben oft auch einfach V für den K-Vektorraum $(V, +, \cdot)$.

Bezeichnung 3.2. Um die Notation zu vereinfachen, legen wir $v_1 - v_2 \coloneqq v_1 + (-v_2)$, $av \coloneqq a \cdot v$ für alle $v_1, v_2, v \in V$ und $a \in K$ sowie *Punkt- vor Strichrechnung* fest.

Bezeichnung 3.3 (Vektor, Skalar, Nullvektor)**.** Die Elemente von V nennen wir *Vektoren*, die Elemente von K nennen wir *Skalare*. Das Nullelement 0_V heißt *Nullvektor* oder auch *die Null von V*.

Bemerkung 3.4. Es ist sehr wichtig, zu wissen, welchen Grundkörper K der Vektorraum hat. Dieselbe Menge V, aber über zwei verschiedene Körper K_1 und K_2, sind zwei verschiedene Vektorräume, nämlich ein K_1- und ein K_2-Vektorraum. Im Allgemeinen ist ein Vektorraum über einen anderen Körper kein Vektorraum mehr, da er z. B. nicht mehr abgeschlossen ist.

Bemerkung 3.5. Die Skalarmultiplikation multipliziert ein Skalar mit einem Vektor (wie der Name schon sagt, also kein Skalarprodukt). Wir beachten auch die Reihenfolge der Skalarmultiplikation, d. h. Skalare werden von *links* multipliziert.

Wie bei Körpern gibt es eine Vielzahl an Rechenregeln für Vektorräume, die wir in den Übungen beweisen.

3.2 Beispiele von Vektorräumen

Bezeichnung 3.6 (Nullvektorraum)**.** Sei $V := \{0\}$ über K der (triviale) *Nullvektorraum* (oft auch einfach nur $V = 0$). Addition und Skalarmultiplikation können nur auf genau eine Weise definiert werden:

$$
\begin{aligned}
+\colon V \times V \to V, &\qquad 0 + 0 \mapsto 0\\
\cdot\colon V \times V \to V, &\qquad 0 \cdot 0 \mapsto 0
\end{aligned}
$$

Beispiel 3.7. Sei K ein Körper. Dann ist K ein K-Vektorraum mit Addition und Skalarmultiplikation definiert als Addition und Multiplikation von K.

Definition 3.8 (Standardvektorraum)**.** Sei K ein Körper. Für $n \geq 1$ sei $V := K^n$ das n-fache kartesische Produkt von K. Die Elemente aus K^n schreiben wir oft als Spalten

$$
\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}
$$

mit $a_1, \dots, a_n \in K$. Wir definieren komponentenweise

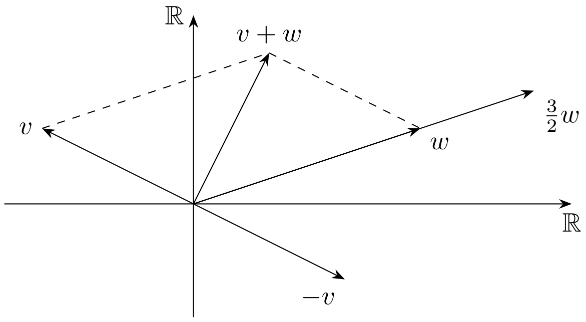
$$
+\colon V \times V \to V \quad \text{durch} \quad \left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}\right) \mapsto \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}
$$

und

$$
\cdot\colon K \times V \to V \quad \text{durch} \quad \left(a, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}\right) \mapsto \begin{pmatrix} ab_1 \\ \vdots \\ ab_n \end{pmatrix}.
$$

Dann ist $(V, +, \cdot)$ ein K-Vektorraum, der sog. *Standardvektorraum.* Wir legen $K^0 := 0$ aus K fest. Dabei stammt die komponentenweise Addition und Multiplikation aus K.

In $V = \mathbb{R}^2$ mit $K = \mathbb{R}$ können wir Addition und Skalarmultiplikation visualisieren, indem wir Vektoren als Pfeile darstellen. Addition heißt dann Aneinanderreihen von Pfeilen; Skalarmultiplikation heißt dann Strecken/Stauchen oder Änderung der Richtung von Pfeilen. Das sollte aus der Schule bekannt sein.



Ein sehr wichtiges Beispiel von Vektorräumen:

Definition 3.9 (Funktionenraum)**.** Sei K ein Körper und sei $I \neq \varnothing$ eine Menge. Wir setzen $V := K^I := \mathrm{Abb}(I, K)$ und definieren

$$
+\colon V \times V \to V, \quad (f, g) \mapsto f + g \qquad \text{und} \qquad \cdot\colon K \times V \to V, \quad (a, f) \mapsto af,
$$

punktweise durch

$$
(f + g)(x) := f(x) + g(x) \qquad \text{und} \qquad (af)(x) := a(f(x))
$$

für alle $f, g \in V$, $a \in K$, und $x \in I$.

Dann ist $(V, +, \cdot)$ ein K-Vektorraum, der sog. *(lineare) Funktionenraum.* Wir definieren $K^\varnothing = 0$ als Nullabbildung.

Dabei ist in den Definitionsgleichungen auf der linken Seite Addition und Skalarmultiplikation in V, sowie auf der rechten Seite Addition und Multiplikation in K.[1,2]

Ein noch wichtigeres Beispiel ist

Definition 3.10. Sei K ein Körper und sei $I \neq \varnothing$ eine Menge. Dann ist

$$K^{(I)} \coloneqq \{f \in K^I \mid f(x) \neq 0 \text{ für nur endlich viele } x \in I\}$$

ein K-Vektorraum, wobei wir Addition und Skalarmultiplikation von K^I benutzen. Wir definieren $K^{(\varnothing)} = 0$ als Nullabbildung.

Jede Abbildung $f \in K^{(I)}$ bildet also fast alle $x \in I$ (bis auf endlich viele) auf 0 ab.

Definition 3.11 (Teilkörper)**.** Sei $(L, +, \cdot)$ ein Körper und sei K eine Teilmenge von L, sodass die Eigenschaften

1. $0, 1 \in K$ (neutrale Elemente);
2. $a + b \in K$ für alle $a, b \in K$ (Abgeschlossenheit unter Addition);
3. $a \cdot b \in K$ für alle $a, b \in K$ (Abgeschlossenheit unter Multiplikation);
4. $-a \in K$ für alle $a \in K$ (additive Inverse) und
5. $a^{-1} \in K$ für alle $a \in K^\times$ (multiplikative Inverse)

erfüllt sind. Durch Einschränkung erhalten wir die Abbildungen

$$+\colon K \times K \to K \qquad \text{und} \qquad \cdot\colon K \times K \to K.$$

(Das ist aufgrund der Abgeschlossenheit von + und $\cdot$ garantiert, s. Punkte 2 und 3.) Wir können leicht überprüfen, dass K einen Körper bildet, und nennen K einen *Teilkörper* von L.

Beispiel 3.12. Ist K ein Teilkörper von L, so ist L ein K-Vektorraum, wobei die Skalarmultiplikation $\cdot\colon K \times L \to L$ durch Einschränkung der Multiplikation $\cdot\colon L \times L \to L$ definiert ist.

Bspw. ist der Körper $\mathbb{Q}(\sqrt{2})$ ein $\mathbb{Q}$-Vektorraum und $\mathbb{R}$ sowohl ein $\mathbb{Q}$- als auch ein $\mathbb{Q}(\sqrt{2})$-Vektorraum.

Definition 3.13 (externe direkte Summe)**.** Seien V und W zwei K-Vektorräume. Dann ist die $V \times W$ wieder ein K-Vektorraum, wobei Addition und Skalarmultiplikation komponentenweise definiert sind durch

$$(v_1, w_1) + (v_2, w_2) \coloneqq (v_1 + v_2, w_1 + w_2) \qquad \text{und} \qquad a(v, w) \coloneqq (av, aw)$$

für alle $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ und $a \in K$. Der K-Vektorraum $V \times W$ nennen wir die *(externe) direkte Summe* von V und W und schreiben $V \oplus W$.

Noch ein Beispiel aus der Analysis.

Beispiel 3.14. Sei $I = [a, b]$ ein abgeschlossenes Intervall in $\mathbb{R}$ und sei

$$C^0(I) \coloneqq \{\text{stetige Funktionen } I \to \mathbb{R}\}$$

eine Teilmenge von $\mathbb{R}^I$. Dann ist $C^0(I)$ ein $\mathbb{R}$-Vektorraum mit der Einschränkung von $+\colon \mathbb{R}^I \times \mathbb{R}^I \to \mathbb{R}^I$ und $\cdot\colon \mathbb{R} \times \mathbb{R}^I \to \mathbb{R}^I$ auf die neue Definitionsmenge $I \subset \mathbb{R}$.

Ende der Vorlesung 3 am 19. Oktober 2021

[1] An dieser Stelle fragt man sich vielleicht, warum der Standardvektorraum K^n und der Funktionenraum K^I identisch notiert werden. Das liegt daran, dass sie tatsächlich „identisch" (d. h. *isomorph*) sind, weil es eine Bijektion wie in Beispiel 1.35 gibt.

[2] Für $I = \mathbb{N}$ lässt sich auch der „unendlichdimensionale" *Folgenraum*

$$K^{\mathbb{N}} \coloneqq \{(a_1, a_2, a_3, \dots) \mid a_i \in K \text{ für alle } i \in \mathbb{N}\}$$

(wie in der Analysis) definieren.

3.3 Unterräume

Definition 3.15. Sei V ein K-Vektorraum. Eine Teilmenge U von V heißt *Unterraum* von V, falls gilt:

1. $U \neq \varnothing$;
2. $u_1 + u_2 \in U$ für alle $u_1, u_2 \in U$ (*Abgeschlossenheit bzgl. Addition*) und
3. $au \in U$ für alle $a \in K$ und $u \in U$ (*Abgeschlossenheit bzgl. Skalarmultiplikation*).

Lemma 3.16. *Sei U ein Unterraum von V. Durch Einschränkung der Addition und Skalarmultiplikation von V erhalten wir Abbildungen $+\colon U \times U \to U$ und $\cdot\colon K \times U \to U$ (was aufgrund Punkte 2 und 3 möglich ist). Dann ist U zusammen mit beiden Einschränkungen wieder ein K-Vektorraum.*

Beweis. Sei $u \in U$. Aus Punkt 3 folgen $0u = 0 \in U$ und $(-1)u = -u \in U$. Deshalb gelten die Axiome (A3) und (A4). Alle anderen Axiome folgen aus V. □

Beispiel 3.17. Die Teilmengen V und $\{0\}$ (statt $\{0\}$ schreiben wir oft nur 0) sind Unterräume von V, die sog. *trivialen Unterräume*.

Beispiel 3.18. Sei $v \in V$. Dann ist

$$U_v \coloneqq Kv \coloneqq \{av \mid a \in K\}$$

der kleinste Unterraum[3] von V, welcher v enthält.

Definition 3.19 (Gerade)**.** Ist $v \neq 0$, so nennen wir

$$U_v \coloneqq Kv \coloneqq \{av \mid a \in K\}$$

die durch v verlaufende *Gerade*.

Beispiel 3.20. Für jede Menge I ist $K^{(I)}$ ein Unterraum von K^I, denn nach Addition und Skalarmultiplikation hat jede Abbildung immer noch nur endlich viele Stellen ungleich 0.

Beispiel 3.21. Sei $I = [a, b]$ ein Intervall in $\mathbb{R}$. Dann ist $C^0(I)$ ein Unterraum von $\mathbb{R}^I$, weil sich die Stetigkeit unter Addition und Skalarmultiplikation nicht ändert.

Beispiel 3.22. Die Elemente des $\mathbb{R}$-Vektorraums $\mathbb{R}^{\mathbb{N}}$ sind die in der Analysis behandelten reellen Folgen. Die Teilmenge der konvergenten reellen Folgen ist ein Unterraum von $\mathbb{R}^{\mathbb{N}}$, da aufgrund der Grenzwertsätze die Folgen nach Addition und Skalarmultiplikation immer noch konvergieren.

Beispiel 3.23. Sei $a \in K$. Wir definieren

$$U(a) \coloneqq \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \;\middle|\; b \in K \right\}.$$

Dann ist $U(a)$ genau dann ein Unterraum von K^2, wenn $a = 0$.

Definition 3.24 (Durchschnitt, Summe)**.** Seien U_1 und U_2 Unterräume von V. Dann ist $U_1 \cap U_2$ der *Durchschnitt* von U_1 und U_2 sowie

$$U_1 + U_2 \coloneqq \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$$

die *Summe* von U_1 und U_2.

Lemma 3.25. *$U_1 \cap U_2$ und $U_1 + U_2$ sind Unterräume von V.*

Definition 3.26 (interne direkte Summe)**.** Seien U_1 und U_2 Unterräume von V. Ist $U_1 \cap U_2 = 0$, so nennen wir

$$U_1 \oplus U_2 \coloneqq U_1 + U_2$$

die *(interne) direkte Summe* von U_1 und U_2.

[3] An der Stelle müssten wir definieren, was „klein“ i. S. v. Unterräumen bedeuten soll. Hier meint der Dozent wahrscheinlich die *Dimension*, die später drankommt.

Definition 3.27 (Summe, interne direkte Summe von Familien)**.** Sei I eine Indexmenge, und für jedes $i \in I$ sei U_i ein Unterraum von V (kurz $(U_i)_{i\in I}$ eine Familie von Unterräumen von V). Die *Summe*

$$\sum_{i\in I} U_i$$

der Unterräume U_i ist die Menge aller Vektoren $v \in V$, für die es eine endliche Teilmenge $J \subseteq I$ gibt, sodass

$$v = \sum_{j\in J} u_j \qquad \text{mit } u_j \in U_j \text{ für alle } j \in J.$$

Ist

$$U_j \cap \left(\sum_{i\in I\setminus j} U_i \right) = 0 \qquad \text{für alle } j \in I,$$

so nennen wir die Summe *(interne) direkte Summe* und schreiben

$$\bigoplus_{i\in I} U_i \coloneqq \sum_{i\in I} U_i.$$

Jedes $v \in (U_i)_{i\in I}$ ist also eine Summe von endlich vielen Vektoren u_j, wobei jedes u_j von einem anderen Unterraum kommt.[4,5]

Lemma 3.28. *$\bigcup_{i\in I} U_i$ und $\sum_{i\in I} U_i$ sind Unterräume von V.*

Betrachten wir Standardvektorräume (wie z. B. $\mathbb{R}^2$), dann können wir uns Untervektorräume als z. B. den Ursprung, Geraden, Ebenen, Räume, etc. vorstellen, die den Ursprung enthalten. Insbesondere sind U_v Ursprungsgeraden. Die interne Summe zweier verschiedener Geraden in $\mathbb{R}^2$ ist $\mathbb{R}^2$ selbst; die Summe ist auch direkt, da sie nur 0 teilen.

4 Lineare Abbildungen

Die „Theorie der Vektorräume“ wird interessant, wenn wir noch Abbildungen zwischen Vektorräumen betrachten. Dabei sollen sie die Vektorraumstruktur[1] erhalten, d. h. mit der Addition und Skalarmultiplikation innerhalb des Start- und Zielvektorraums kompatibel sein. Das führt zu *linearen Abbildungen* bzw. *Homomorphismen* („Gleich-Gestalter“). Das vorläufige Ziel wird es sein, lineare Abbildungen zu verstehen.

4.1 Definition

Definition 4.1 (lineare Abbildung)**.** Seien V und W zwei K-Vektorräume. Eine Abbildung $f\colon V \to W$ heißt *linear* (oder *K-linear*), falls folgende Bedingungen gelten:

1. $f(v_1 + v_2) = f(v_1) + f(v_2)$ für alle $v_1, v_2 \in V$; und
2. $f(av) = af(v)$ für alle $v \in V$ und $a \in K$.

Dabei finden Addition und Skalarmultiplikation zwischen den Argumenten der Abbildung in V und zwischen den Bildern der Abbildung in W statt. Anders geschrieben:

$$\begin{aligned} f(v_1 +_V v_2) &= f(v_1) +_W f(v_2), \\ f(a \cdot_V v) &= a \cdot_W f(v) \end{aligned}$$

[4]Anders formuliert: Jeder Vektor v der internen Summe ist die Summe $\sum_{i\in I} u_i$ mit $u_i \in U_i$, wobei $u_i \neq 0$ nur für endlich viele u_i gilt. Vgl. mit der Definition von $K^{(I)}$.

[5]Eine witzige Eigenschaft: Für zwei Untervektorräume U und W von V gilt

$$U \times \{0\} \oplus \{0\} \times W = U \oplus W,$$

also $(u, 0) + (0, w) = (u, w)$, wobei auf der linken Seite die *interne* direkte Summe und auf der rechten Seite die *externe* direkte Summe gemeint ist. Die Vektorräume auf der linken Seite teilen sich nur den Vektor $(0, 0)$.

[1]Wichtig ist, dass die hier betrachteten Homomorphismen *Vektorraumstrukturen erhalten*, d. h. sie sind mit der Vektorraumstruktur *verträglich.* Es gibt noch viele andere Homomorphismen, wie z. B. Mengenhomomorphismen (das sind die Abbildungen), Gruppenhomomorphismen, Homomorphismen zwischen topologischen Räumen (sog. Homöomorphismen), etc.

Definition 4.2 (Homomorphismus, Endomorphismus)**.** Ist $f\colon V \to W$ linear, so nennen wir f einen *Homomorphismus*. Ist zudem $V = W$, so nennen wir f einen *Endomorphismus* (also $f\colon V \to V$).

Weiterhin definieren wir

$$\operatorname{Hom}(V, W) := \{f \in \operatorname{Abb}(V, W) \mid f \text{ ist ein Homomorphismus}\}$$

und

$$\operatorname{End}(V) := \operatorname{Hom}(V, V).$$

Definition 4.3 (Monomorphismus, Epimorphismus, Isomorphismus)**.** Sei $f\colon V \to W$ ein Homomorphismus.

- f ist ein *Monomorphismus*, falls f injektiv ist.
- f ist ein *Epimorphismus*, falls f surjektiv ist.
- f ist ein *Isomorphismus*, falls f bijektiv ist.

Definition 4.4 (isomorph)**.** Zwei K Vektorräume V und W heißen *isomorph*, falls ein Isomorphismus $f\colon V \to W$ existiert. Wir schreiben dann $V \cong W$.

Der Begriff der Isomorphie ist sehr mächtig, da er uns erlaubt, innerhalb der linearen Algebra die beiden Objekte „gleichzusetzen“, d. h. die Objekte sind zueinander äquivalent und verhalten sich auch (unter Addition und Skalarmultiplikation) gleich.[2]

Lemma 4.5. *Seien V und W zwei K-Vektorräume. Eine Abbildung $f\colon V \to w$ ist genau dann linear, wenn*

$$f(a_1 v_1 + a_2 v_2) = a_1 f(v_1) + a_2 f(v_2)$$

für alle $a_1, a_2 \in K$ und $v_1, v_2 \in V$ gilt.

Beweis. Übungsaufgabe. □

4.2 Beispiele von linearen Abbildungen

Definition 4.6 (Nullabbildung)**.** Seien V und W zwei K-Vektorräume. Die *Nullabbildung*

$$f\colon V \to W, \quad v \mapsto 0 \quad \text{für alle } v \in V$$

ist ein Homomorphismus. Wir schreiben $f = 0$.

Definition 4.7 (Identität)**.** Sei V ein K-Vektorraum. Die *Identität*

$$f\colon V \to V, \quad v \mapsto v \quad \text{für alle } v \in V$$

ist ein Homomorphismus. Wir schreiben $f = \operatorname{id}_V$.

Die Identität ist ein bijektiver Endomorphismus, also ein Isomorphismus und insbesondere ein Homomorphismus.

Beispiel 4.8.

1. Sei V ein K-Vektorraum und sei $a \in K$. Die Abbildung $f_a\colon V \to V$, $v \mapsto av$ für alle $v \in V$ ist ein Homomorphismus. Ist $a \neq 0$, d. h. $f_a \neq 0$, so ist f_a sogar ein Isomorphismus.
2. Für jeden Homomorphismus $f\colon K \to K$ gibt es ein $a \in K$ mit $f = f_a$. Für alle $\lambda \in K$ gilt nämlich $f(\lambda) = f(\lambda 1) = \lambda f(1)$. Dann können wir $a := f(1)$ setzen.
3. Die Graphen der Homomorphismen $f\colon K \to K$ sind genau die Geraden $U_v \subseteq K^2$, wobei $v = (a, b)$ mit $a \neq 0$ ist. Die Punkte des Graphen sind nämlich $(\lambda, f(\lambda)) = (\lambda, \lambda f(1)) = \lambda(1, f(1))$ für alle $\lambda \in K$. Für $a = 0$ wäre f nur auf 0 definiert.

[2] Zusätzlich definiert man einen *Automorphismus* als einen bijektiven Endomorphismus, also Isomorphismus und Endomorphismus gleichzeitig.

Beispiel 4.9. Sei K ein Körper und sei $(a,b,c,d) \in K^4$ gegeben. Die Abbildung[3]

$$f\colon K^2 \to K^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

ist ein Homomorphismus.

(Um das nachzuweisen, setzen wir einfach in die Definition linearer Abbildungen ein. Für die Addition gilt

$$f\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = \begin{pmatrix} a(x_1+x_2)+b(y_1+y_2) \\ c(x_1+x_2)+d(y_1+y_2) \end{pmatrix} = \begin{pmatrix} ax_1+by_1 \\ cx_1+dy_1 \end{pmatrix} + \begin{pmatrix} ax_2+by_2 \\ cx_2+dy_2 \end{pmatrix} = f\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}\right) + f\left(\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right).$$

Analog können wir zeigen, dass die Abbildung mit der Skalarmultiplikation kompatibel ist.)

Beispiel 4.10. Die Abbildung $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ ist kein Homomorphismus bzw. nicht $\mathbb{R}$-linear, denn z. B. gilt $16 = f(2+2) \neq f(2) + f(2) = 8$.

Warnung: In der linearen Algebra gibt es viele verschiedene Nullen. Z. B. seien V und W zwei K-Vektorräume. 0 kann nun die Null 0_K in K, die Null 0_V in V, die Null 0_W in W, die Nullabbildung $0\colon V \to W$ oder der triviale Unterraum $\{0\}$ sein.

4.3 Erste Eigenschaften linearer Abbildungen

Für das restliche Kapitel seien V und W zwei K-Vektorräume.

Lemma 4.11. *Sei $f\colon V \to W$ ein Homomorphismus. Dann gilt $f(0) = 0$.*

Beweis. Es gibt zwei Möglichkeiten, die Aussage zu beweisen.

Erster Beweis: Es gilt

$$f(0) \overset{\text{(A3)}}{=} f(0+0) \overset{\text{Hom.}}{=} f(0) + f(0).$$

Daraus folgt

$$0 \overset{\text{(A4)}}{=} f(0) - f(0) = (f(0)+f(0)) - f(0) \overset{\text{(A1)}}{=} f(0) + (f(0) - f(0)) \overset{\text{(A4)}}{=} f(0) + 0 \overset{\text{(A3)}}{=} f(0).$$

Zweiter Beweis: Für die Nullen $0_K \in K$, $0_V \in V$ und $0_W \in W$ gilt mit der Rechenregel $0v = 0$

$$f(0_V) = f(0_K 0_V) \overset{\text{Hom.}}{=} 0_K f(0_V) = 0_W. \qquad \square$$

Der zweite Beweis ist zwar kürzer, ist aber weniger elementar.

Lemma 4.12. *Sei $f\colon V \to W$ ein Isomorphismus. Dann ist die Umkehrabbildung $f^{-1}\colon W \to V$ wieder ein Isomorphismus.*

Beweis. Aus den Eigenschaften von Bijektionen wissen wir, dass f^{-1} existiert und auch bijektiv ist. Wir müssen noch zeigen, dass f^{-1} linear ist.

Weil f bijektiv ist, ist jedes $w \in W$ von der Form $f(v) = w$ für ein eindeutig bestimmtes $v \in V$. Dann gelten für alle $v, v_1, v_2 \in V$ und $a \in K$

$$f^{-1}(f(v_1) + f(v_2)) = f^{-1}(f(v_1 + v_2)) = v_1 + v_2 = f^{-1}(f(v_1)) + f^{-1}(f(v_2))$$

und

$$f^{-1}(a(f(v))) = f^{-1}(f(av)) = av = af^{-1}(f(v)).$$

Folglich ist f^{-1} linear. $\square$

Lemma 4.13. *Seien $f\colon U \to V$ und $g\colon V \to W$ Homomorphismen. Dann ist die Komposition $g \circ f\colon U \to W$ auch ein Homomorphismus.*

Beweis. Wir verwenden Lemma 4.5. Für alle $a_1, a_2 \in K$ und $v_1, v_2 \in V$ gilt

$$\begin{aligned}(g \circ f)(a_1 u_2 + a_2 u_2) = g(f(a_1 u_1 + a_2 u_2)) &\overset{\text{Hom. } f}{=} g(a_1 f(u_1) + a_2 f(u_2)) \\ &\overset{\text{Hom. } g}{=} a_1 g(f(u_1)) + a_2 g(f(u_2)) = a_1 (g \circ f)(u_1) + a_2 (g \circ f)(u_2).\end{aligned} \qquad \square$$

[3] Das ist das Matrix-Vektor-Produkt.

Ende der Vorlesung 4 am 22. Oktober 2021

Lemma 4.14. *Für alle $f, g \in \operatorname{Hom}(V, W)$ und $a \in K$ definieren wir Abbildungen (Addition und Skalarmultiplikation eines Funktionenraums)*

$$f + g \colon V \to W, \quad v \mapsto f(v) + g(v) \qquad \text{und} \qquad af \colon V \to W, \quad v \mapsto a(f(v)).$$

Dann ist $(\operatorname{Hom}(V, W), +, \cdot)$ *ein K-Vektorraum*

Beweis.

- Zuerst müssen wir zeigen, dass die Addition und Skalarmultiplikation auf $\operatorname{Hom}(V, W)$ abgeschlossen ist, d. h., dass $f + g$ und af linear sind. Dafür können wir leicht überprüfen, dass

$$(f + g)(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (f + g)(v_1) + \lambda_2 (f + g)(v_2)$$

für alle $v_1, v_2 \in V$ und $\lambda_1, \lambda_2 \in K$ gilt.

- Die Axiome (A1) und (A2) in $\operatorname{Hom}(V, W)$ folgen aus den Axiomen (A1) und (A2) in W.
- Der Nullvektor in $\operatorname{Hom}(V, W)$ (Axiom (A3)) ist die Nullabbildung $0 \colon V \to W$, ein Homomorphismus.
- Für jedes $f \in \operatorname{Hom}(V, W)$ definieren wir $-f \colon V \to W$, $v \mapsto -(f(v))$ als das additive Inverse. Wir sehen leicht, dass $-f \in \operatorname{Hom}(V, W)$. Dann gilt

$$(f + (-f))(v) = f(v) + (-(f(v))) = 0 \qquad \text{für alle } v \in V.$$

Also gilt Axiom (A4) in $\operatorname{Hom}(V, W)$.

- Für alle $f, g \in \operatorname{Hom}(V, W)$, $a \in K$ und $v \in V$ gilt

$$\begin{aligned}(a(f + g))(v) = a((f + g)(v)) = a(f(v) + g(v)) &\underset{\text{in } W}{\overset{\text{(SM3)}}{=}} a(f(v)) + a(g(v)) \\ &= (af)(v) + (ag)(v) = (af + ag)(v).\end{aligned}$$

Also gilt Axiom (SM3) in $\operatorname{Hom}(V, W)$.

- Den Nachweis der Axiome (SM1), (SM2) und (SM4) können wir ähnlich führen. □

Lemma 4.15. *Sei $f \colon V \to W$ ein Homomorphismus.*

1. *Existiert ein Homomorphismus $g \colon W \to V$ mit $g \circ f = \mathrm{id}_V$, so ist f ein Monomorphismus.*
2. *Existiert ein Homomorphismus $g \colon W \to V$ mit $f \circ g = \mathrm{id}_W$, so ist f ein Epimorphismus.*

Beweis. Übungsaufgabe. □

Bemerkung 4.16. Die Umkehrung der beiden Aussagen in Lemma 4.15 gilt auch. Der Beweis dazu erfolgt später.[4]

4.4 Lineare Abbildungen und affine Geraden

Definition 4.17 (Restklasse modulo U)**.** Sei V ein K-Vektorraum und sei U ein Unterraum von V sowie $v \in V$. Dann ist die *Restklasse von v modulo U* definiert als die Menge

$$v + U \coloneqq \{v + u \mid u \in U\}.$$

Das entspricht dem Unterraum U, aber verschoben um v.[5]

Zur Erinnerung: Wir definierten $U_v \coloneqq \{av \mid a \in K\}$ für $v \in V$.

[4] Wir werden sehen, dass das mit der Invertierbarkeit von Matrizen zu tun hat, wobei g ein Produkt von Elementarmatrizen ist.
[5] Die Namensgebung entstammt der Zahlentheorie. Ähnlich sind alle $w \in U$ in der Restklasse $v + U$ enthalten, und v ist ein Repräsentant dieser Äquivalenzklasse (definiert durch $v \sim w :\iff (v - w) \in U$).

Definition 4.18 (affine Gerade)**.** Für alle $v, w \in V$ sei

$$L_{v,w} \coloneqq \{u_{v,w}(a) \coloneqq av + (1-a)w \mid a \in K\}.$$

Falls $v \neq w$, nennen wir $L_{v,w}$ die durch v und w verlaufende *affine Gerade*. Falls $v = w$ ist $L_{v,w} = \{v\}$.

Bemerkung 4.19.

1. Für $a = 1$ und $a = 0$ erhalten wir $v \in L_{v,w}$ bzw. $w \in L_{v,w}$.
2. Im Allgemeinen ist $L_{v,w}$ kein Unterraum von V. Bspw. fehlt der Nullvektor.

Lemma 4.20. *Seien $v, w \in V$. Es gilt für alle affinen Geraden*

$$L_{v,w} = w + U_{v-w}.$$

Beweis. Es gilt für alle $a \in K$

$$u_{v,w}(a) = av + (1-a)w = w + a(v-w).$$

Folglich bestehen die affine Gerade und die Restklasse aus denselben Elementen. □

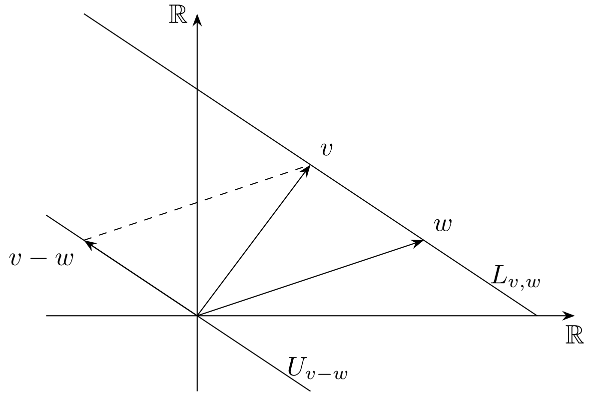


Abbildung 4.1: Affine Gerade $L_{v,w}$ in $\mathbb{R}^2$. U_{v-w} geht durch 0, während $L_{v,w}$ eine Verschiebung von U_{v-w} um w ist. $L_{v,w}$ und U_{v-w} sind dementsprechend parallel.

Für einen Homomorphismus $f\colon V \to W$ gilt nun

$$f(u_{v,w}(a)) = f(av + (1-a)w) = a(f(v)) + (1-a)(f(w)) = u_{f(v),f(w)}(a).$$

Damit bildet f affine Geraden wieder auf affine Geraden ab (falls $f(v) \neq f(w)$). Die Bildgerade unter f kann aber rotiert oder parallel verschoben worden sein. Durch Einschränkung erhalten wir Abbildungen

$$f_{v,w}\colon L_{v,w} \to L_{f(v),f(w)}, \quad u_{v,w}(a) \mapsto u_{f(v),f(w)}(a)$$

und

$$f_{v-w}\colon U_{v-w} \to U_{f(v)-f(w)}, \quad a(v-w) \mapsto a(f(v) - f(w))$$

mit $a \in K$.

Bemerkung 4.21.

1. Für $v \neq w$ mit $f(v) \neq f(w)$ sind $f_{v,w}$ und f_{v-w} beide bijektiv. In diesem Fall werden die *parallelen* affinen Geraden U_{v-w} und $L_{v,w}$ wieder auf die *parallelen* affinen Geraden $U_{f(v)-f(w)}$ und $L_{f(v),f(w)}$ abgebildet.
2. Für $v \neq w$, aber $f(v) = f(w)$ ist $L_{f(v),f(w)} = \{f(v)\}$ und $U_{f(v)-f(w)} = 0$.

4.5 Kern und Bild

Definition 4.22 (Kern, Bild)**.** Sei $f\colon V \to W$ ein Homomorphismus. Dann ist

$$\mathrm{Kern}(f) \coloneqq \{v \in V \mid f(v) = 0\} \subseteq V$$

der *Kern* von f, und

$$\mathrm{Bild}(f) \coloneqq \{f(v) \mid v \in V\} \subseteq W$$

das *Bild* von f.

Der Kern ist im Prinzip die Menge aller „Nullstellen" von f. Es gilt nämlich per Definition[6]

$$\mathrm{Kern}(f) = f^{-1}(0).$$

Lemma 4.23. *Sei $f\colon V \to W$ ein Homomorphismus. Dann gelten:*

1. $\mathrm{Kern}(f)$ *ist ein Unterraum von V.*
2. $\mathrm{Bild}(f)$ *ist ein Unterraum von W.*
3. $\mathrm{Kern}(f) = 0$ *genau dann, wenn f ein Monomorphismus ist.*
4. $\mathrm{Bild}(f) = W$ *genau dann, wenn f ein Epimorphismus ist.*

Beweis.

1. Wegen $f(0) = 0$ liegt 0 in $\mathrm{Kern}(f)$. Damit ist $\mathrm{Kern}(f) \neq \varnothing$.
   Für alle $a \in K$ und $v, v_1, v_2 \in \mathrm{Kern}(f)$ gilt aufgrund Linearität
   $$f(v_1 + v_2) = f(v_1) + f(v_2) = 0 + 0 = 0 \qquad \text{und} \qquad f(av) = af(v) = a0 = 0.$$
   Folglich liegen alle $v_1 + v_2$ und av in $\mathrm{Kern}(f)$, also ist $\mathrm{Kern}(f)$ unter Addition und Skalarmultiplikation abgeschlossen. $\mathrm{Kern}(f)$ ist ein Unterraum von V.
2. Wegen $f(0) = 0$ liegt $f(0)$ in $\mathrm{Bild}(f)$. Damit ist $\mathrm{Bild}(f) \neq \varnothing$.
   Seien $w, w_1, w_2 \in \mathrm{Bild}(f)$, d. h. es gibt $v, v_1, v_2 \in V$ mit $f(v) = w$, $f(v_1) = w_1$ und $f(v_2) = w_2$. Für alle $a \in K$ und $w, w_1, w_2 \in \mathrm{Bild}(f)$ gelten aufgrund Linearität
   $$w_1 + w_2 = f(v_1) + f(v_2) = f(v_1 + v_2) \qquad \text{und} \qquad aw = af(v) = f(av).$$
   Folglich gibt es zu jeden $w_1 + w_2$ und aw Urbilder, weshalb $w_1 + w_2$ und aw in $\mathrm{Bild}(f)$ liegen. Also ist $\mathrm{Bild}(f)$ unter Addition und Skalarmultiplikation abgeschlossen und $\mathrm{Bild}(f)$ ein Unterraum von W.
3. Sei f injektiv und sei $v \in \mathrm{Kern}(f)$. Dann gilt
   $$f(v) = 0 = f(0),$$
   und aus der Injektivität folgt $v = 0$. Also ist $\mathrm{Kern}(f) = 0$.
   Ist f nicht injektiv, so gibt es $v_1 \neq v_2$ in V mit $f(v_1) = f(v_2)$. Dann gilt aufgrund Linearität
   $$f(v_1 - v_2) = f(v_1) - f(v_2) = 0.$$
   Somit ist $v_1 - v_2 \in \mathrm{Kern}(f)$, aber $v_1 - v_2 \neq 0$ und damit $\mathrm{Kern}(f) \neq 0$.
4. Das folgt unmittelbar aus den Definitionen. □

Lemma 4.24. *Sei $f\colon V \to W$ ein Homomorphismus und sei $b \in \mathrm{Bild}(f)$. Dann ist $f^{-1}(b)$ genau dann ein Unterraum von V, wenn $b = 0$.*

[6] Eine alternative Charakterisierung des Kerns: Sei $f\colon V \to W$ ein Homomorphismus. Für alle $v, w \in V$ ir definieren die Äquivalenzrelation $v \sim w :\iff f(v) = f(w)$. Dabei folgt aus der Linearität

$$v \sim w \iff f(v) = f(w) \iff f(v) - f(w) = f(v - w) = 0$$

Damit zerfällt V in Restklassen modulo $\mathrm{Kern}(f)$.

Beweis. Zur Rückrichtung: Ist $b = 0$, dann ist $f^{-1}(b) = \mathrm{Kern}(f)$, was nach Lemma 4.23 ein Unterraum von V ist.

Zur Hinrichtung: Ist $b \neq 0$, dann folgt $0 \notin f^{-1}(b)$ aus $f(0) = 0$ (andernfalls wäre $f(0) = b \neq 0$). Damit ist $f^{-1}(b)$ kein Vektorraum und insbesondere kein Unterraum von V, weil der Nullvektor fehlt. □

Lemma 4.25. *Sei $f\colon V \to W$ ein Homomorphismus und seien $b \in \mathrm{Bild}(f)$ und $v \in f^{-1}(b)$. Dann gilt*

$$f^{-1}(b) = v + f^{-1}(0) = v + \mathrm{Kern}(f).$$

Das bedeutet, dass ein Urbild $v \in f^{-1}(b)$ ausreicht, um die gesamte Urbildmenge zu beschreiben. Das wird noch wichtig, wenn wir lineare Gleichungssysteme lösen werden.

Beweis. Sei $x \in v + \mathrm{Kern}(f)$, also $x = v + u$ mit $u \in \mathrm{Kern}(f)$. Wir haben

$$f(x) = f(v + u) = f(v) + f(u) = b + 0 = b.$$

Also gilt $x \in f^{-1}(b)$ für alle x und daher $v + \mathrm{Kern}(f) \subseteq f^{-1}(b)$.

Sei nun $x \in f^{-1}(b)$. Es gelten

$$x = (v - v) + x = v + (x - v)$$

und

$$f(-v) = f((-1)v) = -f(v) = -b.$$

Daraus folgt

$$f(x - v) = f(x) + f(-v) = b - b = 0$$

und daher $x - v \in \mathrm{Kern}(f)$, d. h. $x = v + (x - v) \in v + \mathrm{Kern}(f)$ für alle x. Somit gilt $f^{-1}(b) \subseteq v + \mathrm{Kern}(f)$ und letztendlich $f^{-1}(b) = v + \mathrm{Kern}(f)$. □

5 Matrizenrechnung

5.1 Definition einer Matrix

Zur Erinnerung: Sei K ein Körper und $n \geq 1$. Dann ist K^n (das n-fache kartesische Produkt) die Menge aller n-Tupel der Form

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \qquad \text{mit } a_i \in K \text{ für alle } 1 \leq i \leq n.$$

Wir werden fast immer mit der *informellen* Definition von Matrizen arbeiten, die anschaulicher und praktischer ist.

Definition 5.1 (Matrix (informell))**.** Seien $m, n \geq 1$ natürliche Zahlen. Eine $(m \times n)$-*Matrix* (mit *Einträgen in* K) ist eine Anordnung von Elementen $a_{ij} \in K$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$ in Form eines Rechtecks/einer Tabelle

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Auch sehen wir die Indizes mit Kommata getrennt, also $a_{i,j}$, um z. B. $a_{1,37}$ und $a_{13,7}$ auseinanderzuhalten.

Bezeichnung 5.2 (Menge der Matrizen, Zeile, Spalte, Eintrag)**.** Mit $K^{m,n}$ bezeichnen wir die *Menge aller* $(m \times n)$*-Matrizen.* Die m-Tupel

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

nennen wir die j*-te Spalte* von A, und die n-Tupel

$$(a_{i1}, a_{i2}, \dots, a_{in})$$

nennen wir die i*-te Zeile* von A. Für alle $1 \leq i \leq m$ und $1 \leq j \leq n$ nennen wir $A_{ij} := a_{ij}$ den ij*-ten Eintrag* von A.

Bemerkung 5.3. Es ist sehr wichtig, dass wir sowohl in der Größe $m \times n$ als auch in den Indizes von a_{ij} *zuerst die Zeile, dann die Spalte* schreiben. Genauso ist die Anordnung der Einträge wichtig; vertauschen wir zwei Einträge, erhalten wir eine andere Matrix.

Beispiel 5.4.

$$A = \begin{pmatrix} 1 & \pi & \sqrt{2} \\ 0 & -1 & 0 \end{pmatrix} \in \mathbb{R}^{2,3}$$

ist eine (2×3)-Matrix mit Einträgen in $\mathbb{R}$.

Nun zur *formalen* Definition, die wir kaum benutzen werden. Es ist aber recht einfach, alle Beweise und Aussagen in die formale Definition zu überführen.

Definition 5.5 (Matrix (formal))**.** Für $s \geq 1$ sei $I_s := \{1, 2, \dots, s\}$. Wir setzen

$$K^{m,n} := K^{I_m \times I_n} = \operatorname{Abb}(I_m \times I_n, K).$$

Die Elemente von $K^{m,n}$ nennen wir $(m \times n)$*-Matrizen* (mit *Einträgen in* K).

Eine Matrix A ist also die Abbildung[1]

$$A\colon I_m \times I_n \to K, \quad (i,j) \mapsto a_{ij}.$$

Bezeichnung 5.6. Statt

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in K^{m,n}$$

schreiben wir auch

$$A = (a_{ij}) \in K^{m,n}.$$

Manchmal ist es sinnvoll, die Notation (a_{ij}) statt A zu wählen.

Definition 5.7 (Nullmatrix)**.** Sei $A = (a_{ij}) \in K^{m,n}$ eine Matrix mit $a_{ij} = 0$ für alle i, j. Wir schreiben dann $A = 0_{m,n} = 0$ und nennen sie die *Nullmatrix* in $K^{m,n}$.

Für $m = 0$ oder $n = 0$ beschreibt $K^{m,n} := K^{I_m \times I_n} = K^{\varnothing}$ mit $I_0 := \varnothing$ die Menge der Matrizen, die keine Zeilen oder Spalten haben. In dem Fall enthält $K^{m,n}$ genau ein Element, die *leere Matrix* oder auch *Nullmatrix*, die wir wieder mit 0 oder $0_{m,n}$ bezeichnen.

Bezeichnung 5.8. Für $m, n \geq 0$ definieren wir

$$M_{m,n}(K) := K^{m,n} \qquad \text{und} \qquad M_n(K) := K^{n,n}$$

für rechteckige bzw. quadratische Matrizen.

Mit der Schreibweise $M_{m,n}(K)$ wollen wir die Ringstruktur der Menge der Matrizen betonen (was wir noch zeigen), während wir mit $K^{m,n}$ die Vektorraumstruktur betonen möchten.

Ende der Vorlesung 5 am 26. Oktober 2021

[1] Die Definition erinnert an die Schreibweise von Familien, $A = (a_{ij})_{(i,j) \in I_m \times I_n}$.

5.2 Operationen auf Matrizen

Definition 5.9 (Addition)**.** Seien $m, n \geq 1$. Seien $A = (a_{ij})$ und $B = (b_{ij})$ Matrizen in $K^{m,n}$. Die *Summe* von A und B ist

$$A + B \coloneqq (a_{ij} + b_{ij}) = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

und die Abbildung

$$+\colon K^{m,n} \times K^{m,n} \to K^{m,n}, \quad (A, B) \mapsto A + B$$

heißt *Addition von Matrizen.*

Definition 5.10 (Skalarmultiplikation)**.** Seien $m, n \geq 1$. Seien $a \in K$ und $A = (a_{ij}) \in K^{m,n}$. Die *Skalarmultiplikation* von a und B ist

$$a \cdot A \coloneqq aA \coloneqq (aa_{ij}) = \begin{pmatrix} aa_{11} & aa_{12} & \cdots & aa_{1n} \\ aa_{21} & aa_{22} & \cdots & aa_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ aa_{m1} & aa_{m2} & \cdots & aa_{mn} \end{pmatrix}$$

und die Abbildung

$$\cdot\colon K \times K^{m,n} \to K^{m,n}, \quad (a, A) \mapsto aA$$

heißt *Skalarmultiplikation für Matrizen.*

Merke: Addition und Skalarmultiplikation erfolgen komponentenweise.

Lemma 5.11. *$(K^{m,n}, +, \cdot)$ ist ein K-Vektorraum.*

Beweis. Für den Beweis müssten wir die Vektorraumaxiome nachrechnen, die sich aber unmittelbar aus den Körperaxiomen ergeben. Der Nullvektor ist die Nullmatrix $0_{m,n} \in K^{m,n}$. Für $m = 0$ oder $n = 0$ ist $K^{m,n}$ als $\{0_{m,n}\}$ definiert, was der Nullvektorraum ist. □

Definition 5.12 (Produkt)**.** Seien $m, n, p \geq 1$ und seien $A = (a_{ij}) \in K^{m,n}$ und $B = (b_{jk}) \in K^{n,p}$ Matrizen. Das *Produkt* von A und B ist

$$A \cdot B \coloneqq AB \coloneqq (c_{ik}) \in K^{m,p} \qquad \text{mit} \qquad c_{ik} \coloneqq \sum_{j=1}^{n} a_{ij} b_{jk}$$

und die Abbildung

$$\cdot\colon K^{m,n} \times K^{n,p} \to K^{m,p}, \quad (A, B) \mapsto AB$$

heißt *Multiplikation von Matrizen.*

Bemerkung 5.13.

1. Bei der Matrixmultiplikation müssen wir auf die richtigen Größen der Matrizen achten: A ist eine $(m \times n)$-Matrix, B ist eine $(n \times p)$-Matrix und AB ist eine $(m \times p)$-Matrix. Der erste „Faktor" muss also genauso viele Spalten haben wie der zweite „Faktor" Zeilen hat.

2. Der ik-te Eintrag des Produkts ist das Matrixprodukt

$$c_{ik} = (a_{i1}, \ldots, a_{in}) \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix}.$$

   Merke: *i-te Zeile mal k-te Spalte.*

Beispiel 5.14.

1. $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

2. $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$.

3. Das Produkt einer $(1 \times n)$-Matrix (*Zeilenvektor*) und einer $(n \times 1)$-Matrix (*Spaltenvektor*) ist eine (1×1)-Matrix (Skalar):
$$\underbrace{(a_1, \ldots, a_n)}_{\in K^{1,n}} \cdot \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_{\in K^{n,1}} = \left(\sum_{j=1}^{n} a_j b_j \right) \in K^{1,1}.$$

4. Sei $K = \mathbb{Q}$. Dann gilt
$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 3 \\ 0 & 1 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 & 3 \\ 0 & 3 & 7 & 1 \end{pmatrix}.$$

Bemerkung 5.15. Für beliebige Matrizen A und B kann das Produkt AB existieren, aber das Produkt BA hingegen möglicherweise nicht (das hängt von der Größe der Matrizen ab). Für quadratische Matrizen gilt aber im Allgemeinen $AB \neq BA$ (vgl. Punkte 1 und 2 sehen). Für quadratische Matrizen $A, B \neq 0$ kann $AB = 0$ sein (s. Punkt 1).

5.3 Rechenregeln für Matrizen

Lemma 5.16 (Assoziativität). *Seien $A = (a_{ij}) \in K^{m,n}$, $B = (b_{jk}) \in K^{n,p}$ und $C = (c_{kl}) \in K^{p,q}$. Dann gilt*
$$A(BC) = (AB)C.$$

Beweis. Aus der Definition folgen
$$A(BC) = A \cdot \left(\left(\sum_{k=1}^{p} b_{jk} c_{kl} \right)_{jl} \right) = \left(\left(\sum_{j=1}^{n} \sum_{k=1}^{p} a_{ij} b_{jk} c_{kl} \right)_{il} \right)$$
und
$$(AB)C = \left(\left(\sum_{j=1}^{n} a_{ij} b_{jk} \right)_{ik} \right) \cdot C = \left(\left(\sum_{k=1}^{p} \sum_{j=1}^{n} a_{ij} b_{jk} c_{kl} \right)_{il} \right).$$
Mit der Kommutativität der Addition (A2) in K folgt die Gleichheit. □

Lemma 5.17 (Linksdistributivität). *Für alle $A = (a_{ij}) \in K^{m,n}$, $B = (b_{jk})$ und $C = (c_{jk})$ in $K^{n,p}$ gilt*
$$A(B + C) = AB + AC.$$

Beweis. Es gelten
$$(A(B + C))_{ik} = (a_{i1}, \ldots, a_{1n}) \cdot \begin{pmatrix} b_{1k} + c_{1k} \\ \vdots \\ b_{nk} + c_{nk} \end{pmatrix} = \sum_{j=1}^{n} a_{ij}(b_{jk} + c_{jk})$$
und
$$(AB + AC)_{ik} = (a_{i1}, \ldots, a_{1n}) \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix} + (a_{i1}, \ldots, a_{1n}) \cdot \begin{pmatrix} c_{1k} \\ \vdots \\ c_{nk} \end{pmatrix} = \sum_{j=1}^{n} a_{ij} b_{jk} + \sum_{j=1}^{n} a_{ij} c_{jk}.$$
Wenden wir die Distributivität (Axiom (D)) in K an, erhalten wir die Gleichheit. □

Lemma 5.18 (Rechtsdistributitvität). *Für alle $A = (a_{ij})$, $B = (b_{ij})$ in $K^{m,n}$ und $C = (c_{jk}) \in K^{n,p}$ gilt*
$$(A + B)C = AC + BC.$$

Beweis. Der Beweis erfolgt analog zur Linksdistributivität. □

Definition 5.19 (Einheitsmatrix)**.** Für $n \geq 1$ sei

$$E_n \coloneqq \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \in K^{n,n}$$

die *Einheitsmatrix* in $K^{n,n}$, also

$$E_n \coloneqq (a_{ij}) \in K^{n,n} \qquad \text{mit} \qquad a_{ij} = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{sonst.} \end{cases}$$

Für $n = 0$ sei $E_0 = 0_n$.

Die Einheitsmatrix ist immer quadratisch.
Einträge, die null sind, lassen wir einfach weg, um die Matrix übersichtlicher zu gestalten.

Lemma 5.20 (Einselement)**.** *Für alle $A \in K^{m,n}$ gilt*

$$E_m A = A = A E_n.$$

Beweis. Das können wir durch einfaches Nachrechnen mithilfe der Definition der Matrixmultiplikation überprüfen. Aufgrund der Nullen in einer Zeile bzw. Spalte werden alle Einträge bis auf eines mit 0 multipliziert; diese Summanden fallen dann raus. □

Die Einsen in der Einheitsmatrix greifen jeweils genau eine Zeile bzw. Spalte „heraus".

Lemma 5.21. *Für alle $a \in K$, $A \in K^{m,n}$ und $B \in K^{n,p}$ gilt*

$$a(AB) = (aA)B = A(aB).$$

Beweis. Dies können wir wieder durch einfaches Nachrechnen überprüfen, wobei wir die Definition der Skalarmultiplikation für Matrizen un der Matrixmultiplikation anwenden und die Axiome in K verwenden müssen. □

Lemma 5.22 (Ring der quadratischen Matrizen)**.** $(M_n(K), +, \cdot)$ *ist ein Ring.*

Beweis. Die Axiome (A1) bis (A4) für Ringe folgen aus Axiomen (A1) bis (A4) in K und $-(a_{ij}) = (-a_{ij})$ für Matrizen $(a_{ij}) \in M_n(K)$, da die Matrixaddition von komponentenweise definiert wurde. Axiom (R1) ist Lemma 5.16. Axiom (R2) ist Lemma 5.20. Axiom (D) sind Lemmata 5.17 und 5.18. □

Bemerkung 5.23. Beispiel 5.14 zeigt, dass der Ring $M_2(K)$ (oder allgemein $M_n(K)$ für $n \geq 2$) <u>nicht</u> kommutativ und <u>nicht</u> nullteilerfrei ist.
Spezialfälle: $M_1(K) \cong K$ ist ein Körper. $M_0(K)$ ist der Nullring.

Axiom 5.24 (Algebra)**.** Sei K ein Körper. Ein Ring $(R, +, \cdot)$ zusammen mit einer Abbildung (*Skalarmultiplikation*)

$$*\colon K \times R \to R, \quad (a, r) \mapsto a * r$$

heißt *K-Algebra*, falls folgende Axiome gelten:

(AL1) $(R, +, *)$ ist ein K-Vektorraum;

(AL2) $a * (r \cdot s) = (a * r) \cdot s = r \cdot (a * s)$ für alle $a \in K$ und $r, s \in R$.[2]

Bezeichnung 5.25. Wir schreiben auch $ar \coloneqq a * r$ und $rs \coloneqq r \cdot s$.

Achtung: Wir haben hier drei Multiplikationen: Die Körpermultiplikation $\cdot_K$, die Ringmultiplikation $\cdot_R$ und die Skalarmultiplikation $*$. Welche Multiplikation gemeint ist, sehen wir anhand der Art der Elemente, die verknüpft werden. Genauso haben wir zwei Additionen: Die Körperaddition $+_K$ und die Ringaddition $+_R$.

[2] Eine alternative Definition: Eine *K-Algebra* A ist ein Vektorraum $(A, +, *)$, zusammen mit einer K-bilinearen Verknüpfung $\cdot\colon A \times A \to A$, d. h. für $\cdot$ gelten Axiom (D) für Ringe und Axiom (AL2).

Lemma 5.26 (Algebra der quadratischen Matrizen). *$M_n(K)$ ist eine K-Algebra, wobei $+$ die Addition von Matrizen, $\cdot$ die Multiplikation von Matrizen und $*$ die Skalarmultiplikation von Matrizen ist.*

Beweis. Wir haben gerade gezeigt, dass $M_n(K)$ ein Ring ist.

Um Axiom (AL1) zeigen, müssen wir die Vektorraumaxiome zeigen: Axiome (A1) bis (A4) für Vektorräume folgen direkt aus Axiome (A1) bis (A4) für Ringe. Axiome (SM1) bis (SM4) können wir einfaches durch Nachrechnen und Anwenden der Distributivität in K zeigen.

Axiom (AL2) ist Lemma 5.21. □

5.4 Matrizen als lineare Abbildungen

Nun sehen wir, warum wir den Begriff einer Matrix überhaupt einführten, nämlich um lineare Abbildungen übersichtlich darzustellen.

Definition 5.27 (Matrixabbildung). Sei $A = (a_{ij}) \in K^{m,n}$ eine Matrix. Wir definieren eine Abbildung, die wir ebenfalls mit A bezeichnen, durch

$$A\colon K^n \to K^m, \quad v \mapsto A(v) \coloneqq A \cdot v,$$

wobei $A \cdot v$ das Produkt der $(m \times n)$-Matrix A mit der $(n \times 1)$-Matrix v ist. (Hier haben wir $K^n = K^{n,1}$ identifiziert.) Die Abbildung $A\colon K^n \to K^m$ heißt *Matrixabbildung*.[3]

Lemma 5.28. *Die Matrixabbildung $A\colon K^n \to K^m$ ist K-linear.*

Beweis. Seien $A \in K^{m,n}$ und $v_1, v_2 \in K^n$. Dann folgt aus Lemma 5.17

$$A(v_1 + v_2) = A \cdot (v_1 + v_2) = A \cdot v_1 + A \cdot v_2 = A(v_1) + A(v_2).$$

Für $a \in K$ und $v \in V$ folgt aus Lemma 5.21

$$A(av) = A \cdot (av) = a(A \cdot v) = a(A(v)).$$ □

Damit liefern Matrixabbildungen viele neue Beispiele für Homomorphismen (auf Standardvektorräumen).

Beispiel 5.29.

1. Die Einheitsmatrix E_n liefert die Identität $\mathrm{id}_{K^n}\colon K^n \to K^n$.
2. Die Matrix $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in M_2(K)$ liefert die Abbildung
$$A\colon K^2 \to K^2, \quad \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} b \\ -a \end{pmatrix}.$$
Für $K = \mathbb{R}$ können wir uns das so vorstellen: A dreht jeden Vektor in $\mathbb{R}^2$ um einen rechten Winkel im Uhrzeigersinn.[4]
3. Beispiel 4.9 ist die Matrixabbildung
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\colon K^2 \to K^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Satz 5.30. *Seien $A \in K^{m,n}$ und $B \in K^{n,p}$ sowie $A\colon K^n \to K^m$ bzw. $B\colon K^p \to K^n$ die entsprechenden Matrixabbildungen. Dann gilt*
$$A \cdot B = A \circ B,$$
wobei $A \cdot B$ das Matrixprodukt und $A \circ B$ die Komposition von Abbildungen ist.

Bemerkung 5.31. Das ist genau der Grund, warum die Matrixmultiplikation so definiert wurde! Aus dem Satz folgt auch, dass wir für gewöhnlich (der Konvention für Abbildung entsprechend) Matrixprodukte von rechts nach links auswerten. Die tatsächliche Multiplikationsreihenfolge ist aber egal (genauso wie $(g \circ f)(x) = g(f(x))$).

[3] Auch bekannt als *Matrix-Vektor-Produkt*.

[4] Eine sog. *Rotationsmatrix* $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ für $\theta = -\frac{1}{2}\pi$.

$$\begin{tikzcd} K^p \arrow[r, "B"] \arrow[rr, bend right, "A\circ B"'] & K^n \arrow[r, "A"] & K^m \end{tikzcd}$$

Beweis. Nach Lemma 5.16 gilt für alle $v \in K^p$

$$(A \cdot B)(v) = (A \cdot B) \cdot v = A \cdot (B \cdot v) = A(B(v)) = (A \circ B)(v). \qquad \square$$

5.5 Die Standardbasis von Standardvektorräumen

Definition 5.32 (Standardbasisvektor)**.** Sei $n \geq 1$. Für alle $1 \leq i \leq n$ sei

$$e_i^{(n)} \coloneqq e_i \coloneqq \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n \qquad \text{mit } a_j \coloneqq \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{sonst,} \end{cases}$$

der *i-te Standardbasisvektor* oder auch *i-te Einheitsvektor* von K^n.

Lemma 5.33. *Für jedes $v \in K^n$ gibt es eindeutig bestimmte $a_1, \ldots, a_n \in K$ mit $v = \sum_{i=1}^n a_i e_i$.*

Beweis. Zur Existenz: Es gilt

$$\sum_{i=1}^n a_i e_i = \begin{pmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_2 \\ \vdots \\ 0 \end{pmatrix} \cdots + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \eqqcolon v.$$

Zur Eindeutigkeit: Angenommen, es gibt zwei Darstellungen

$$\sum_{i=1}^n a_i e_i = v = \sum_{i=1}^n b_i e_i$$

von v. Daraus folgt

$$\sum_{i=1}^n (a_i - b_i) e_i = \begin{pmatrix} a_1 - b_1 \\ \vdots \\ a_n - b_n \end{pmatrix} = 0,$$

was genau dann möglich ist, wenn $a_i - b_i = 0 \iff a_i = b_i$ für alle i ist. $\square$

Definition 5.34 (Standardbasis)**.** Wir nennen $\{e_1, e_2, \ldots, e_n\} \subseteq K^n$ die *Standardbasis* von K^n.

Ende der Vorlesung 6 am 29. Oktober 2021

Lemma 5.35. *Seien $f, g \in \operatorname{Hom}(K^n, K^m)$. Dann gilt $f = g$ genau dann, wenn $f(e_i) = g(e_i)$ für alle $1 \leq i \leq n$.*

Zwei Homomorphismen sind demnach genau dann gleich, wenn sie in den Standardbasisvektoren übereinstimmen.

Beweis. Gemäß Lemma 5.33 gibt es für jedes $v \in K^n$ Skalare $a_1, \ldots, a_n \in K$ mit $v = \sum_{i=1}^n a_i e_i$.
Seien $f, g \in \operatorname{Hom}(K^n, K^m)$. Gilt $f(e_i) = g(e_i)$ für alle $1 \leq i \leq n$, so folgt aus der Linearität

$$f(v) = \sum_{i=1}^n a_i f(e_i) = \sum_{i=1}^n a_i g(e_i) = g(v).$$

Gilt hingegen $f = g$, also $f(v) = g(v)$ für alle $v \in K^n$, so ist natürlich auch $f(e_i) = g(e_i)$ mit $e_i \in K^n$. $\square$

Die allgemeine Definition einer *Basis* eines K-Vektorraums (und wie mächtig dieser Begriff ist) erfahren wir später.

5.6 $K^{m,n}$ und $\mathrm{Hom}(K^n, K^m)$

Satz 5.36. *Für $m, n \geq 0$ gilt*

$$K^{m,n} \cong \mathrm{Hom}(K^n, K^m).$$

Beweis. Wir definieren die Abbildung

$$\eta\colon K^{m,n} \to \mathrm{Hom}(K^n, K^m), \quad A \mapsto \eta(A),$$

die definiert ist durch

$$(\eta(A))(v) := A(v) = A \cdot v \qquad \text{für alle } v \in K^n.$$

η ordnet also jeder Matrix A die Abbildung $\eta(A)$ zu. Wir wollen zeigen, dass η ein Isomorphismus ist.

- η ist wohldefiniert, also $\eta(A) \in \mathrm{Hom}(K^n, K^m)$: Nach Definition ist $\eta(A)$ die Matrixabbildung $A\colon K^n \to K^m$ zur Matrix A. Lemma 5.28 sagt, dass Matrixabbildungen K-linear sind.
- η ist K-linear: Für alle $A_1, A_2 \in K^{m,n}$, $a_1, a_2 \in K$ und $v \in K^n$ gilt mittels der Rechenregeln für Matrizen
$$\begin{aligned}[\eta(a_1A_1 + a_2A_2)](v) &= (a_1A_1 + a_2A_2) \cdot v = a_1(A_1 \cdot v) + a_2(A_2 \cdot v)\\ &= a_1[(\eta(A_1))(v)] + a_2[(\eta(A_2))(v))] = [a_1(\eta(A_1)) + a_2(\eta(A_2))](v).\end{aligned}$$
- η ist ein Monomorphismus: Betrachten wir eine Matrix $A = (a_{ij}) \in K^{m,n}$. Für $1 \leq j \leq n$ ist
$$Ae_j = A(e_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$
die j-te Spalte von A. Sind also zwei Matrizen $A \neq B$ in $K^{m,n}$ verschieden, so muss es eine Spalte j geben, in der sie nicht übereinstimmen, also $(\eta(A))(e_j) = A(e_j) \neq B(e_j) = (\eta(B))(e_j)$. Ferner folgt aus Lemma 5.35, dass dann auch $\eta(A) \neq \eta(B)$ gilt. Also ist η injektiv.
- η ist ein Epimorphismus: Sei $f \in \mathrm{Hom}(K^m, K^n)$ ein Homomorphismus. Zu jedem f definieren wir eine Matrix
$$A_f := (a_{ij}) \in K^{m,n} \qquad \text{durch} \qquad A(e_j) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} := f(e_j) \quad \text{für alle } 1 \leq j \leq n.$$
Per unserer Definition folgt dann $A(e_j) = f(e_j)$ für alle $1 \leq j \leq n$ und daher nach Lemma 5.35 auch $A_f = f$. Folglich finden wir zu jedem Homomorphismus $f = A_f$ eine Matrix $\eta^{-1}(f) = A_f$. Also ist η surjektiv.

□

Einer der wichtigsten Aussagen in der linearen Algebra:

Korollar 5.37. *Alle Abbildungen in* $\mathrm{Hom}(K^n, K^m)$ *sind Matrixabbildungen.*
Für $m = 0$ oder $n = 0$ gilt $\mathrm{Hom}(K^m, K^n) = \{0\}$, *wobei* $0\colon K^n \to K^m$ *die Nullabbildung ist.*

Ab sofort werden wir Homomorphismen in Standardvektorräumen und Matrixabbildungen „synonym“ verwenden und unterscheiden oft nicht mehr zwischen $K^{n,m}$ und $\mathrm{Hom}(K^n, K^m)$. Statt $\eta(A)$ wie im Beweis von Satz 5.36 schreiben wir nur noch A und meinen damit sowohl die Matrix $A \in K^{m,n}$ als auch die Matrixabbildung $A\colon K^n \to K^m$.

5.7 Elementarmatrizen und Zeilen- und Spaltenumformungen

Definition 5.38 (Elementarmatrix Typ (I))**.** Für $1 \leq i, j \leq m$ mit $i \neq j$ und $a \in K$ definieren wir eine quadratische Matrix

$$T_{ij}^{(m)}(a) \coloneqq T_{ij}(a) = (t_{pq}) \in K^{m,m} \qquad \text{durch} \qquad t_{pq} \coloneqq \begin{cases} 1 & \text{falls } p = q, \\ a & \text{falls } (p,q) = (i,j), \\ 0 & \text{sonst.} \end{cases}$$

Wir nennen diese Art von Matrizen *Elementarmatrizen vom Typ (I).*

Die Matrizen sind Einheitsmatrizen, wobei genau ein Skalar $a \in K$ irgendwo in den freien Einträgen liegt (d. h. nicht auf der Hauptdiagonale).

Beispiel 5.39.

$$T_{25}^{(6)}(a) = \begin{pmatrix} 1 &&&&& \\ & 1 &&& a & \\ && 1 &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& 1 \end{pmatrix}, \qquad T_{52}^{(6)}(a) = \begin{pmatrix} 1 &&&&& \\ & 1 &&&& \\ && 1 &&& \\ &&& 1 && \\ & a &&& 1 & \\ &&&&& 1 \end{pmatrix}.$$

Definition 5.40 (Elementarmatrix Typ (II))**.** Für $1 \leq i \leq m$ und $b \in K^\times$ definieren wir eine quadratische Matrix

$$D_i^{(m)}(b) \coloneqq D_i(b) = (d_{pq}) \in K^{m,m} \qquad \text{durch} \qquad d_{pq} \coloneqq \begin{cases} 1 & \text{falls } p = q \neq i, \\ b & \text{falls } p = q = 1, \\ 0 & \text{sonst.} \end{cases}$$

Wir nennen diese Art von Matrizen *Elementarmatrizen vom Typ (II).*

Diese Matrizen sind Einheitsmatrizen, wobei genau ein Skalar $b \in K^\times$ (also $b \neq 0$) eine Eins auf der Hauptdiagonale ersetzt.

Beispiel 5.41.

$$D_3^{(6)} = \begin{pmatrix} 1 &&&&& \\ & 1 &&&& \\ && b &&& \\ &&& 1 && \\ &&&& 1 & \\ &&&&& 1 \end{pmatrix}.$$

Definition 5.42 (Elementarmatrix Typ (III))**.** Für $1 \leq i \neq j \leq m$ definieren wir eine quadratische Matrix

$$E_{ij}^{(m)} \coloneqq E_{ij} = (e_{pq}) \in K^{m,m} \qquad \text{durch} \qquad e_{pq} \coloneqq \begin{cases} 1 & \text{falls } i \neq p = q \neq j, \\ 1 & \text{falls } (p,q) = (i,j), \\ 1 & \text{falls } (p,q) = (j,1), \\ 0 & \text{sonst.} \end{cases}$$

Wir nennen diese Art von Matrizen *Elementarmatrizen vom Typ (III).*

Bemerkung 5.43.

1. Aufgrund der Symmetrie gilt $E_{ij}^{(m)} = E_{ji}^{(m)}$.

2. *Achtung*: Die Elementarmatrix $E_{ij}^{(m)}$ ist nicht die Einheitsmatrix E_m, denn wir haben zwei Indizes i und j.

Die Matrizen sind Elementarmatrizen, wobei aber zwei Einträge auf der Hauptdiagonale null sind, dafür aber in einem Quadrat in den beiden anderen Ecken die fehlenden Einsen stehen.

Beispiel 5.44.

$$E_{14}^{(6)} = E_{41}^{(m)} = \begin{pmatrix} 0 & \cdots & \cdots & 1 & & \\ \vdots & 1 & & \vdots & & \\ \vdots & & 1 & \vdots & & \\ 1 & \cdots & \cdots & 0 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}.$$

Den Typenbegriff der Elementarmatrizen werden wir aber nicht so häufig benutzen.[5]

Lemma 5.45. *Die Matrixabbildungen $T_{ij}^{(m)}(a)$, $D_i^{(m)}(b)$ und $E_{ij}^{(m)}$ mit $a \in K$ und $b \in K^\times$ sind Isomorphismen.*

Beweis. Es gilt

$$\begin{aligned} T_{ij}^{(m)}(a) \cdot T_{ij}^{(m)}(-a) &= E_m = T_{ij}^{(m)}(-a) \cdot T_{ij}^{(m)}(a), \\ D_i^{(m)}(b) \cdot D_i^{(m)}(b^{-1}) &= E_m = D_i^{(m)}(b^{-1}) \cdot D_i^{(m)}(b), \\ E_{ij}^{(m)} \cdot E_{ij}^{(m)} &= E_m. \end{aligned}$$

Mit Lemma 4.15 folgt aus den linken und rechten Seiten der Gleichungen, dass die Elementarmatrizen Epimorphismen bzw. Monomorphismen sind.

(Die Gleichungen können wir durch geschicktes nachrechnen überprüfen: Sei $A \coloneqq T_{ij}^{(m)}(a) - E_m$. Daraus folgt auch $T_{ij}^{(m)}(-a) = E_m - A$. Daher gilt

$$\begin{aligned} T_{ij}(a) \cdot T_{ij}(-a) = (E_m + A)(E_m - A) &= E_m E_m - E_m A + A E_m - AA = E_m - AA = E_m \\ &= E_m E_m + E_m A - A E_m - AA = (E_m - A)(E_m + A) = T_{ij}(-a) \cdot T_{ij}(a), \end{aligned}$$

wobei $AA = 0_m$. Ähnlich können wir $B \coloneqq D_i^{(m)}(b) - E_m$ und $B' \coloneqq D_i^{(m)}(b^{-1}) - E_m$ definieren. Dann gilt

$$D_i^{(m)}(b) \cdot D_i^{(m)}(b^{-1}) = (E_m + B)(E_m + B') = E_m + B + B' + BB'.$$

Schauen wir und den Eintrag in (i, i) an, sehen wir

$$1 + B_{ii} + B'_{ii} + B_{ii} B'_{ii} = 1 + (b - 1) + (b^{-1} - 1) + (b - 1)(b^{-1} - 1) = 1.$$

Also gilt mit $BB' = B'B$ (Kommutativität der Multiplikation in K)

$$D_i^{(m)}(b) \cdot D_i^{(m)}(b^{-1}) = E_m = (E_m + B')(E_m + B) = D_i^{(m)}(b^{-1}) \cdot D_i^{(m)}(b).$$

Zuletzt sei $C \coloneqq E_{ij} - E_m$. Dann gilt

$$E_{ij} \cdot E_{ij} = (E_m + C)(E_m + C) = E_m + 2C + CC = E_m,$$

wobei tatsächlich $2C = -CC$ gilt; das müsste man leider einfach nachrechnen.) □

Lemma 5.46 (Zeilenoperationen)**.** *Seien $A \in K^{m,n}$, $a \in K$ und $b \in K^\times$. Dann bilden die Elementarmatrizen die sog.* Zeilenoperationen vom Typ (I), (II) oder (III) *oder* elementare Zeilenumformungen*, wenn sie von links multipliziert werden.*

1. *$T_{ij}^{(m)}(a) \cdot A$ entsteht aus A, wenn wir zur i-ten Zeile von A das a-fache der j-ten Zeile von A addieren.*
2. *$D_i^{(m)}(b) \cdot A$ entsteht aus A, wenn wir die i-te Zeile von A mit b multiplizieren.*
3. *$E_{ij}^{(m)} \cdot A$ entsteht aus A, wenn wir die i-te und j-te Zeile von A vertauschen.*

Beweis. Das ist pure Rechnung. Wieder hilft die Zerlegung $T_{ij}(a) = E_m + B$, $D_i(b) = E_m + C$ und $E_{ij} = E_m + D$. □

[5] Die Menge aller Elementarmatrizen der Größe m über K spannen die *allgemeine lineare Gruppe* $\mathrm{GL}_n(K)$, die Menge aller invertierbaren Matrizen in K^n, auf. Den Begriff der allgemeinen linearen Gruppe werden wir aber später betrachten.

Lemma 5.47. *Die Zeilenoperationen vom Typ (III) können wir durch Verknüpfung von Zeilenoperationen vom Typ (I) und Typ (II) erhalten.*

Beweis. Es gilt z. B.

$$E_{ij} = D_j(-1) \cdot T_{ij}(1) \cdot T_{ji}(-1) \cdot T_{ij}(1).$$

Sei $A \in K^{m,m}$. E_{ij} vertauscht die i te und j te Zeile. Bezeichnen wir die Zeilen mit Zeilenvektoren z_i und z_j, dann gilt

$$\begin{cases} z_i \\ z_j \end{cases} \xrightarrow{T_{ij}(1)} \begin{cases} z_i + z_j \\ z_j \end{cases} \xrightarrow{T_{ji}(-1)} \begin{cases} z_i + z_j \\ z_j - z_i - z_j = -z_i \end{cases} \xrightarrow{T_{ij}(1)} \begin{cases} z_i + z_j - z_i = z_j \\ -z_i \end{cases} \xrightarrow{D_j(-1)} \begin{cases} z_j \\ z_i \end{cases}. \qquad \square$$

Analog definieren wir Spaltenoperationen.

Definition 5.48 (Spaltenoperationen)**.** Sei $A \in K^{n,m}$. Dann sind

$$A \cdot T_{ij}^{(m)}(a), \qquad A \cdot D_j^{(m)}(b) \qquad \text{und} \qquad A \cdot E_{ij}^{(m)}$$

die *elementaren Spaltenoperationen vom Typ (I), (II) bzw. (III).*

5.8 Gauß-Algorithmus

Nun kommen wir zu einer der Ursprünge der linearen Algebra: Das Lösen von linearen Gleichungssystemen. Hierfür entwickeln wir die Theorie rund um den *Gauss-Algorithmus*. Der Algorithmus war eigentlich schon vor Gauß bekannt (antikes China). Im Gegensatz zu vielen anderen Vorlesungen zur linearen Algebra machen wir das mit genügend Theorie, und nicht gleich in der ersten Vorlesung.

5.8.1 Reduzierte Zeilenstufenform

Definition 5.49 (reduzierte Zeilenstufenform)**.** Eine Matrix $B = (b_{ij}) \in K^{m,n}$ ist in *reduzierter Zeilenstufenform*, falls folgendes gilt:

1. $B = 0$. Oder:
2. Es existieren ein Zeilenindex $1 \leq r \leq \min(m, n)$ und Spaltenindizes $1 \leq j_1 < j_2 < \cdots < j_r \leq n$, sodass folgende Bedingungen erfüllt sind:
   (a) Für alle Zeilen $1 \leq k \leq r$ gilt $b_{kj} = 0$ für alle $j < j_k$. (In Worten: Für die ersten r Zeilen sind die ersten $j_k - 1$ Einträge der k ten Zeile alles null.)
   (b) Für alle Zeilen $1 \leq k \leq r$ gilt
   $$b_{ij_k} = \begin{cases} 1 & \text{falls } i = k, \\ 0 & \text{sonst.} \end{cases}$$
   (In Worten: Für die ersten r Zeilen ist der Eintrag in der j_k ten Spalte Eins, und alle anderen Einträge der j_k-ten Spalte sind null. Die Spalten sind also „Standardbasisvektoren“ e_k.)[6]
   (c) Für alle Zeilen $r + 1 \leq k \leq m$ gilt $b_{kj} = 0$ für alle $1 \leq j \leq n$. (In Worten: Die restlichen $m - r$ Zeilen sind alles Nullen, also ein großer Nullblock.)

Bezeichnung 5.50 (Zeilenstufenindizes)**.** Wir nennen die Menge der Indizes

$$\mathcal{I}(B) := \begin{cases} \{j_1, \ldots, j_r\} & \text{falls } B \neq 0, \\ \varnothing & \text{sonst.} \end{cases}$$

Zeilenstufenindizes. Zudem definieren wir das Komplement

$$\mathcal{K}(B) := \{1, \ldots, n\} \setminus \mathcal{I}(B).$$

Eine Matrix in reduzierter Zeilenstufenform ist also von der Form

[6] Sind die Einträge b_{ij_k} nicht normiert und sind in derselben Spalte über dem Eintrag nicht alles Nullen, so bezeichnet man diese Form als (nicht reduzierte) *Zeilenstufenform*

$$
\begin{array}{cccccccccccccccccccc|c}
1 & & & j_1 & & & & j_2 & & & & j_3 & & & & & j_r & & & n & \\
\hline
0 & \cdots & 0 & 1 & \star & \cdots & \star & 0 & \star & \cdots & \star & 0 & \star & \cdots & \star & & 0 & \star & \cdots & \star & 1 \\
 & & & & & & & 1 & \star & \cdots & \star & 0 & \star & \cdots & \star & & 0 & \star & \cdots & \star & 2 \\
 & & & & & & & & & & & 1 & \star & \cdots & \star & & 0 & \star & \cdots & \star & 3 \\
 & & & & & & & & & & & & & & & \cdots & 0 & \star & \cdots & \star & 4 \\
 & & & & & & & 0 & & & & & & & & & \vdots & \vdots & & \vdots & \vdots \\
 & & & & & & & & & & & & & & & & 0 & \star & \cdots & \star & r-1 \\
 & & & & & & & & & & & & & & & & 1 & \star & \cdots & \star & r \\
\hline
 & & & & & & & & & & & & & & & & & & & & r+1 \\
 & & & & & & & 0 & & & & & & & & & & & & & \vdots \\
 & & & & & & & & & & & & & & & & & & & & m
\end{array}
$$

Dabei stehen die für beliebige Einträge aus K.

Bemerkung 5.51. Es gilt $\mathcal{I}(B) = \varnothing$ genau dann, wenn $B = 0$. Es gilt $\mathcal{K}(B) = \varnothing$ genau dann, wenn $B = E_n$ oder wenn

$$
B = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ \hline & 0 & \end{pmatrix}.
$$

Beispiel 5.52. Die Matrix

$$
B = \begin{pmatrix}
0 & 1 & b_{13} & b_{14} & 0 & b_{16} & 0 & 0 & b_{19} & b_{1,10} \\
0 & 0 & 0 & 0 & 1 & b_{26} & 0 & 0 & b_{29} & b_{2,10} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & b_{39} & b_{3,10} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_{49} & b_{4,10} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \in K^{6,10}
$$

ist in reduzierter Zeilenstufenform, wobei $r = 4, \mathcal{I}(B) = \{j_1, j_2, j_3, j_4\} = \{2, 5, 7, 8\}$ und $\mathcal{K}(B) = \{1, 3, 4, 6, 9, 10\}$.

5.8.2 Gauß-Algorithmus

Satz 5.53. *Sei $A = (a_{ij}) \in K^{m,n}$. Dann gibt es Elementarmatrizen $T_1, \dots, T_t$, sodass $B \coloneqq T_t \cdots T_2 T_1 A$ in reduzierter Zeilenstufenform ist.*

Definition 5.54. Entsteht die Matrix B durch Anwendung von elementaren Zeilenoperationen aus A, so nennen wir B eine *reduzierte Zeilenstufenform von A*.

Beweis. Wir beweisen diesen Satz durch die Angabe eines rekursiven Algorithmus bzw. beweisen die Aussage induktiv.

Falls $A = 0$, dann ist A bereits in reduzierter Zeilenstufenform und der Algorithmus stoppt.

Sei also $a \neq 0$ und wir setzen $A^{(0)} = (a_{ij}^{(0)}) \coloneqq A$. Sei

$$
j_1 \coloneqq \min\{1 \leq s \leq n \mid \text{es gibt ein } 1 \leq p \leq m \text{ mit } a_{ps}^{(0)} \neq 0\},
$$

d. h. wir wählen als ersten Zeilenstufenindex die linkste Spalte von A ungleich null. Insbesondere sind alle Spalten links von j_1 alles null und unter Zeilenoperationen bleiben sie null. Nun wählen wir ein $1 \leq p \leq m$, sodass eben $a_{pj_1}^{(0)} \neq 0$ ist.

Weiterhin setzen wir

$$
C^{(0)} = (c_{ij}^{(0)}) \coloneqq D_1((a_{pj_1}^{(0)})^{-1}) \cdot E_{1p} \cdot A^{(0)}.
$$

Hierbei haben wir die Zeile von a_{pj_1} in die erste Zeile geholt und den Eintrag normiert, also $c_{1j_1}^{(0)} = 1$. Nun setzen wir

$$
A^{(1)} = (a_{ij}^{(1)}) \coloneqq T_{m1}(-c_{mj_1}^{(0)}) \cdots T_{21}(-c_{2j_1}^{(0)}) \cdot C^{(0)},
$$

d. h. für die zweite Zeile nehmen wir den Eintrag $c_{2j_1}^{(0)}$ der j_1-ten Spalte, und addieren das $-c_{2j_1}^{(0)}$-fache der ersten Zeile auf die zweite Zeile. Wegen $c_{1j_1}^{(0)} = 1$, ist nun $a_{2j_1}^{(1)} = 0$. Das machen wir für alle restlichen Zeilen genauso. Folglich sind alle Einträge der j_1-ten Spalte ausgelöscht bis auf $a_{1j_1}^{(1)} = 1$. Die ersten j_1 Spalten sind also in der richtigen Form.

Nun definieren wir induktiv Matrizen $A^{(k)}$ und $C^{(k)}$ sowie $j_1 < \cdots < j_k$ aus $\mathbb{N}$ wie folgt: Angenommen $A^{(k-1)} = (a_{ij}^{(k-1)})$ und $j_1 < \cdots < j_k$ sind für ein $k \geq 2$ bereits definiert.

Wir setzen

$$j_k \coloneqq \min\{j_k < s \leq n \mid \text{es gibt ein } k \leq p \leq m \text{ mit } a_{ps}^{(k-1)\neq 0}\}.$$

Hierbei handelt es sich um den k ten Zeilenstufenindex j_k, sodass, wenn wir die ersten $k-1$ Zeilen ignorieren, die j_k-te Spalte die linkste der Matrix ungleich null ist. Das bedeutet, dass Zwischen Zeilen k und m und Spalten 1 und $j_k - 1$ alles null ist.

Gibt es ein solches j_k nicht, so ist $A^{(k-1)}$ bereits in reduzierter Zeilenstufenform (wir sind auf den großen Nullblock gestoßen) und der Algorithmus stoppt.

Wir nehmen an, dass ein j_k existiert. Wir wählen ein $k \leq p \leq m$, sodass eben $a_{pj_k}^{(k-1)} \neq 0$ ist.

Wir setzen

$$C^{(k-1)} = (c_{ij}^{(k-1)}) \coloneqq D_k((a_{pj_k}^{(k-1)})^{-1}) \cdot E_{kp} \cdot A^{(k-1)}.$$

Hier haben wir die Zeile von $a_{pj_k}^{(k-1)}$ in die k-te Zeile geholt und den Eintrag normiert, also $c_{kj_k}^{(k-1)} = 1$. Weiterhin setzen wir

$$A^{(k)} = (a_{ij}^{(k)}) \coloneqq T_{mk}(-c_{mj_k}^{(k-1)}) \cdots T_{k+1,k}(-c_{k+1,j_k}^{(k-1)}) \cdot T_{k-1,k}(-c_{k-1,j_k}^{(k-1)}) \cdots T_{1k}(-c_{1j_k}^{(k-1)}) \cdot C^{(k-1)}.$$

Hier löschen wir jeden Eintrag der j_k-ten Spalte aus bis auf $a_{kj_k}^{(k)} = 1$. Dabei blieben die ersten $j_k - 1$ Spalten unverändert, weil in der k-te Zeile die ersten $j_k - 1$ Einträge null sind.

Wir sehen dass nach jedem Schritt $k \geq 1$ die $(k \times n)$-Matrix der ersten k Zeilen von $A^{(k)}$ und die $(m \times j_k)$-Matrix der ersten j_k Spalten von $A^{(k)}$ in reduzierter Zeilenstufenform sind.

Nach spätestens $k = \min(m, n)$ Schritten stoppt der Algorithmus, denn dann gibt es keine Zeilen und Spalten mehr. Per Induktion ist also $B = A^{(k)}$ in reduzierter Zeilenstufenform. $\square$

Der Algorithmus im Beweis ist der *Gauss-Algorithmus*.[7]

Algorithmus 5.1 Gauss-Algorithmus.

input: Matrix $A \in K^{m,n}$.
output: Matrix $B \in K^{m,n}$, die reduzierter Zeilenstufenform von A.

```
if A = 0 then
    return A
```

Beispiel 5.55. Sei

$$A = \begin{pmatrix} 0 & 2 & -1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & -2 & 2 & 0 \end{pmatrix} \in \mathbb{Q}^{3,4}.$$

Der Gauß-Algorithmus liefert schrittweise folgende Matrizen:

$$\xrightarrow{E_{12}} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 2 & -1 & 1 \\ 1 & -2 & 2 & 0 \end{pmatrix} \qquad \xrightarrow{T_{31}(-1)} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 2 & -1 & 1 \\ 0 & -2 & 1 & -1 \end{pmatrix}$$

$$\xrightarrow{D_2(\frac{1}{2})} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & -2 & 1 & -1 \end{pmatrix} \qquad \xrightarrow{T_{32}(2)} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix} \eqqcolon B.$$

Natürlich können wir die reduzierte Zeilenstufenform intelligenter konstruieren, nicht so wie der Gauß-Algorithmus es vorschreibt.

[7] Das ist nicht ganz korrekt. Der hier beschriebene Algorithmus ist der sog. Gauß-Jordan-*Algorithmus*, der eine reduzierte Zeilenstufenform liefert. Verzichten wir darauf, die Einträge zu normieren und alle Einträge der j_k-ten Spalte über der k-ten Zeile auszulöschen, erhalten wir das *gaussche Eliminationsverfahren*, was nur eine (nicht reduzierte) Zeilenstufenform liefert.

- Es ist einfacher, wenn wir bei Typ (III) Operationen eine Zeile auswählen, in der der Eintrag in der $a_{pj_k} = 1$ ist. Dann können wir auf die Matrix C verzichten.
- Wir müssen nicht notwendigerweise die Typ (III) Operationen anwenden. Manchmal ist es sinnvoller, sie so zu lassen und Brüche zu vermeiden.
- Um zu große Einträge zu vermeiden, empfiehlt es sich, alle Zeilen (wenn möglich) durch Typ (II) Operationen zu „kürzen“, sodass die Einträge noch ganzzahlig bleiben.

Später werden wir noch zeigen, dass die reduzierte Zeilenstufenform einer Matrix sogar eindeutig ist.

Ende der Vorlesung 7 am 02. November 2021

5.9 Kerne von Matrixabbildungen

Definition 5.56 (Basisvektoren des Kerns)**.** Sei $B = (b_{ij}) \in K^{m,n}$ in reduzierter Zeilenstufenform. Für $\mathcal{I}(B) = \{j_1 < \cdots < j_r\}$ und $j \in \mathcal{K}(B)$ definieren wir

$$L_j^B := \begin{pmatrix} \ell_{1j} \\ \vdots \\ \ell_{nj} \end{pmatrix} \in K^n \qquad \text{durch} \qquad \ell_{kj} := \begin{cases} 1 & \text{falls } k = j, \\ -b_{sj} & \text{falls } k = j_s \text{ mit } j_s \in \mathcal{I}(B) \text{ und } j_s < j, \\ 0 & \text{sonst.} \end{cases}$$

Das L steht für Lösung.

Beispiel 5.57. Wir betrachten wieder die Matrix

$$B = \begin{pmatrix} 0 & 1 & b_{13} & b_{14} & 0 & b_{16} & 0 & 0 & b_{19} & b_{1,10} \\ 0 & 0 & 0 & 0 & 1 & b_{26} & 0 & 0 & b_{29} & b_{2,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & b_{39} & b_{3,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_{49} & b_{4,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in K^{6,10}$$

aus Beispiel 5.52, die in reduzierter Zeilenstufenform mit $\mathcal{I}(B) = \{2, 5, 7, 8\}$ ist. Die Vektoren $L_j^B \in K^{10}$ mit $j \in \mathcal{K}(B) = \{1, 3, 4, 6, 9, 10\}$ sind

$$L_1^B = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad L_3^B = \begin{pmatrix} 0 \\ -b_{13} \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad L_4^B = \begin{pmatrix} 0 \\ -b_{14} \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad L_6^B = \begin{pmatrix} 0 \\ -b_{16} \\ 0 \\ 0 \\ -b_{26} \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad L_9^B = \begin{pmatrix} 0 \\ -b_{19} \\ 0 \\ 0 \\ -b_{29} \\ 0 \\ -b_{39} \\ -b_{49} \\ 1 \\ 0 \end{pmatrix}, \quad L_{10}^B = \begin{pmatrix} 0 \\ -b_{1,10} \\ 0 \\ 0 \\ -b_{2,10} \\ 0 \\ -b_{3,10} \\ -b_{4,10} \\ 0 \\ 1 \end{pmatrix}.$$

Die Vektoren L_j^B haben so viele Einträge wie es Spalten in B gibt. Dabei ist der j-te Eintrag 1 und die Einträge darüber kommen aus der j-ten Spalte von B. Die verteilen wir auf die Zeilenstufenindizes $\mathcal{I}(B)$.

Bemerkung 5.58. Die L_j^B sind gerade so definiert, dass $BL_j^B = 0$ gilt.

Wir wissen aus Korollar 5.37, dass wir jede Matrix $B \in K^{m,n}$ als Matrixabbildung $B\colon K^n \to K^m$ auffassen können. Damit können wir sinnvoll den Kern definieren.

Satz 5.59 (Basis des Kerns)**.** *Sei $B \in K^{m,n}$ in reduzierter Zeilenstufenform.*

1. *Es gilt*

$$\operatorname{Kern}(B) = \left\{ \sum_{j \in \mathcal{K}(B)} a_j L_j^B \;\middle|\; a_j \in K \right\}.$$

Falls $\mathcal{K}(B) = \varnothing$, ist $\operatorname{Kern}(B) = 0$.

2. Aus
$$\sum_{j\in\mathcal{K}(B)} a_j L_j^B = \sum_{j\in\mathcal{K}(B)} b_j L_j^B \qquad \textit{mit } a_j, b_j \in K$$
folgt $a_j = b_j$ *für alle* $j \in \mathcal{K}(B)$.

(In fortgeschrittener Sprache: Die Menge $\{L_j^B \mid j \in \mathcal{K}(B)\}$ *ist eine Basis von* $\operatorname{Kern}(B)$*.)*

Beweis. Sei B in reduzierter Zeilenstufenform mit $\mathcal{I}(B) = \{j_1 < \cdots < j_r\}$ und $\mathcal{K}(B) = \{1, \ldots, n\} \setminus \mathcal{I}(B)$.

1. Für ein beliebiges
$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$
im Kern sei
$$\begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} := B(a).$$
Wir sehen sofort, dass $c_k = 0$ für alle $r + 1 \leq k \leq m$, denn diese Zeilen bilden den Nullblock. Für alle $1 \leq s \leq r$ gilt hingegen
$$c_s = (0, \ldots, 0, 1, b_{s,j_s+1}, \ldots, b_{sn}) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_{j_s} + \sum_{j=j_s+1}^{n} b_{sj} a_j = a_{j_s} + \sum_{\substack{j\in\mathcal{K}(B) \\ j>j_s}} b_{sj} a_j.$$
Für die letzte Gleichheit haben wir den Fakt ausgenutzt, dass in den Spalten der Zeilenstufenindizes nach j_s nur Nullen stehen. Nun gilt $B(a) = 0$ genau dann, wenn
$$c_s = 0 \iff a_{j_s} = -\sum_{\substack{j\in\mathcal{K}(B) \\ j>j_s}} b_{sj} a_j \qquad \text{für alle } 1 \leq s \leq r.$$
Tatsächlich erfüllen alle
$$a = \sum_{j\in\mathcal{K}(B)} a_j L_j^B$$
diese Bedingung. Begründung: Für $j \in \mathcal{K}(B)$ ist der j-te Eintrag von $\sum_{j\in\mathcal{K}(B)} a_j L_j^B$ gleich a_j, denn von allen Vektoren ist der j-te Eintrag nur von L_j^B gleich Eins, sonst Null. Für $j_s \in \mathcal{I}(B)$ ist der j_s-te Eintrag gleich
$$-\sum_{\substack{j\in\mathcal{K}(B) \\ j>j_s}} b_{sj} a_j,$$
s. Definition 5.56 der L_j^B.

   Umgekehrt liegt auch jedes L_j^B und aufgrund Linearität auch jede Summe der Form $\sum_{j\in\mathcal{K}(B)} a_j L_j^B$ mit $a_j \in K$ in $\operatorname{Kern}(B)$. Folglich sind beide Mengen gleich.

2. Sei nun
$$\sum_{j\in\mathcal{K}(B)} a_j L_j^B = \sum_{j\in\mathcal{K}(B)} b_j L_j^B$$
mit $a_j, b_j \in K$. Wie eben gezeigt, ist für $j \in \mathcal{K}(B)$ der j-te Eintrag der linken Seite gleich a_j, und der rechten Seite gleich b_j, also $a_j = b_j$. Wie eben gezeigt, hängen die anderen Einträge nur von den a_j bzw. b_j ab, also auch $a_{j_s} = b_{j_s}$ für alle $j_s \in \mathcal{I}(B)$. □

Lemma 5.60. *Seien* $A \in K^{m,n}$ *eine Matrix und* $T \in K^{m,m}$ *eine Elementarmatrix. Dann gilt*
$$\operatorname{Kern}(A) = \operatorname{Kern}(TA).$$

Beweis. Für alle $v \in \text{Kern}(A)$ gilt $A(v) = 0$, also auch $(TA)(v) = 0$ und damit $v \in \text{Kern}(AT)$. Umgekehrt sei nun $v \in \text{Kern}(TA)$, also $(TA)(v) = T(A(v)) = 0$. Weil T ein Isomorphismus (Lemma 5.45) ist, ist es auch insbesondere injektiv, sodass wegen $T(0) = 0$ auch $A(v) = 0$ gelten muss. Folglich ist $v \in \text{Kern}(A)$ und daher $\text{Kern}(A) = \text{Kern}(TA)$. □

Korollar 5.61 (Bestimmung des Kerns)**.** *Sei $A \in K^{m,n}$ und sei B eine reduzierte Zeilenstufenform von A. Dann gilt*

$$\text{Kern}(A) = \text{Kern}(B).$$

Das bedeutet, dass der Gauß-Algorithmus ein explizites Verfahren zur Konstruktion einer Basis von $\text{Kern}(A)$ *liefert.*

Satz 5.62. *Sei $A \in K^{m,n}$ und sei B eine reduzierte Zeilenstufenform von A. Sei zudem $\mathcal{K}(B) = \{1, \dots, n\} \setminus \mathcal{I}(B) = \{i_1 < \cdots < i_{n-r}\}$. Dann ist die Abbildung*

$$f\colon K^{n-r} \to \text{Kern}(A), \qquad \sum_{k=1}^{n-r} a_k e_k \mapsto \sum_{k=1}^{n-r} a_k L_{i_k}^B$$

ein Isomorphismus von Vektorräumen.[8]

Beweis. Die Linearität von f können wir aus einer einfachen Rechnung und dem Distributivgesetz folgern.

Aus Satz 5.59 folgt, dass jeder Vektor in $\text{Kern}(A)$ in der Form $\sum_{k=1}^{n-r} a_k L_{i_k}^B$ darstellbar ist, sodass wir gemäß Lemma 5.33 ein passendes Urbild $\sum_{k=1}^{n-r} a_k e_k$ finden können. Also ist f surjektiv.

Satz 5.59 und Lemma 5.33 implizieren auch die Injektivität von f, denn die Summendarstellungen der Vektoren aus K^{n-r} bzw. $\text{Kern}(A)$ sind eindeutig. □

5.10 Bilder von Matrixabbildungen

Das Bild einer Matrixabbildung ist oft viel leichter als den Kern zu bestimmen.

Lemma 5.63. *Sei $A \in K^{m,n}$ und sei $\{e_1, \dots, e_n\}$ die Standardbasis von K^n. Dann gilt*

$$\text{Bild}(A) = \left\{ \sum_{j=1}^{n} a_j A(e_j) \;\middle|\; a_j \in K \right\}.$$

Die $A(e_j)$ sind die Spalten von A.

Beweis. Sei $w \in \text{Bild}(A)$ beliebig. Per Definition gibt es ein

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$

mit $A(v) = w$. Gemäß Lemma 5.33 gilt $v = \sum_{j=1}^{n} a_j e_j$. Daraus folgern wir

$$w = A(v) = A\left(\sum_{j=1}^{n} a_j e_j\right) = \sum_{j=1}^{n} a_j A(e_j).$$

Umgekehrt ist $A(e_j) \in \text{Bild}(A)$ für jedes $1 \leq j \leq n$. Weil $\text{Bild}(A)$ ein Unterraum ist (Lemma 4.23), ist $\text{Bild}(A)$ unter Addition und Skalarmultiplikation abgeschlossen und es gilt $\sum_{j=1}^{n} a_j A(e_j) \in \text{Bild}(A)$ für alle $a_j \in K$. Daraus folgt die Gleichheit beider Mengen. □

Definition 5.64 (reduzierte Spaltenstufenform)**.** Eine Matrix $B \in K^{m,n}$ ist in *reduzierter Spaltenstufenform*, falls die transponierte Matrix B^T in reduzierter Zeilenstufenform ist.

[8] Das folgt schon daraus, dass die lineare Hülle der beiden Basen dieselbe Dimension besitzen.

Bemerkung 5.65. Für $A \in K^{m,n}$ gibt es Elementarmatrizen $T_1, \dots, T_t \in K^{n,n}$, sodass $T_t \cdots T_1 A^T$ in reduzierter Zeilenstufenform ist. Aus den Gesetzen zur Transposition folgt, dass

$$\left(T_t \cdots T_1 A^T\right)^T = A T_1^T \cdots T_t^T$$

in reduzierter Spaltenstufenform ist. Dabei ist die transponierte Matrix T^T einer Elementarmatrix T wieder eine Elementarmatrix. Somit können wir auch jede Matrix A in reduzierte Spaltenstufenform bringen.

Satz 5.66. *Sei $B \in K^{m,n}$ in reduzierter Spaltenstufenform und sei $r = |\mathcal{I}(B^T)|$.*

1. *Es gilt*

$$\operatorname{Bild}(B) = \left\{ \sum_{j=1}^{r} a_j B(e_j) \;\middle|\; a_j \in K \right\}.$$

   Falls $B = 0$ die leere Matrix ist, ist $\operatorname{Bild}(B) = 0$.

2. *Aus*

$$\sum_{j=1}^{r} a_j B(e_j) = \sum_{j=1}^{r} b_j B(e_j) \qquad \textit{mit } a_j, b_j \in K$$

   folgt $a_j = b_j$ für alle $1 \le j \le r$.

(In fortgeschrittener Sprache: Die Menge $\{B(e_j) \mid 1 \le j \le r\}$ ist eine Basis von $\operatorname{Bild}(B)$*.)*

Beweis. Seien B in reduzierter Spaltenstufenform und $\mathcal{I}(B) = \{j_1 < \cdots < j_r\}$ die Spaltenstufenindizes.

1. Für alle $r + 1 \le j \le m$ ist die j-te Spalte von B gleich Null, d. h. $B(e_j) = 0$ und damit

$$\sum_{j=1}^{r} a_j B(e_j) = \sum_{j=1}^{n} a_j B(e_j) \qquad \text{für alle } a_j \in K.$$

   Der Rest folgt aus Lemma 5.63.

2. Für $j_s \in \mathcal{I}(B^T)$ ist der j_s-te Eintrag von $\sum_{j=1}^{r} a_j B(e_j)$ gleich a_j, da in der j_s-ten Zeile von B genau eine Eins in Spalte s steht. Daraus folgt sofort die Behauptung. □

Lemma 5.67. *Seien $A \in K^{m,n}$ eine Matrix und $T \in K^{n,n}$ eine Elementarmatrix. Dann gilt*

$$\operatorname{Bild}(A) = \operatorname{Bild}(AT).$$

Beweis. Weil T ein Isomorphismus ist (Lemma 5.45), ist T auch surjektiv, also $T(K^n) = K^n$ und damit $\operatorname{Bild}(A) = \operatorname{Bild}(AT)$. □

Korollar 5.68 (Bestimmmung des Bildes)**.** *Sei $A \in K^{m,n}$ und sei B eine reduzierte Spaltenstufenform von A. Dann gilt*

$$\operatorname{Bild}(A) = \operatorname{Bild}(B).$$

Das bedeutet, dass der Gauß-Algorithmus ein explizites Verfahren zur Konstruktion einer Basis von $\operatorname{Bild}(A)$ *liefert.*

Ende der Vorlesung 8 am 05. November 2021

5.11 Invertierbare Matrizen

Definition 5.69 (invertierbar)**.** Sei R ein Ring. Ein Element $r \in R$ ist

1. *linksinvertierbar*, falls es ein $s \in R$ gibt mit $sr = 1$,
2. *rechtsinvertierbar*, falls es ein $t \in R$ gibt mit $rt = 1$, und
3. *invertierbar*, falls r sowohl rechts- als auch linksinvertierbar ist.

Lemma 5.70. *Sei R ein Ring und sei $r \in R$ invertierbar. Dann gelten:*

1. *Es gibt ein eindeutiges Element $r^{-1} \in R$ mit $rr^{-1} = r^{-1}r = 1$.*
2. *Falls $rs = 1$ gilt für ein $s \in R$, so gilt $s = r^{-1}$.*
3. *Falls $rs = 1$ gilt für ein $s \in R$, so gilt $s = r^{-1}$.*
4. *r^{-1} ist invertierbar mit $(r^{-1})^{-1} = r$.*

Beweis. 1. Da r invertierbar ist, existieren $s, t \in R$ mit $rs = 1$ und $tr = 1$. Es gilt dann

$$s = 1s = (tr)s = t(rs) = t1 = t.$$

Nun setzen wir $r^{-1} := s = t$.

2. Sei $r^{-1} \in R$ mit $r^{-1}r = 1$ (Punkt 1). Angenommen es gilt $rp = 1$ für ein $p \in R$. Dann gilt

$$p = 1p = \big(r^{-1}r\big)p = r^{-1}(rp) = r^{-1}1 = r^{-1}.$$

3. Sei $r^{-1} \in R$ mit $rr^{-1} = 1$ (Punkt 1). Angenommen es gilt $qr = 1$ für ein $a \in R$. Dann gilt

$$q = q1 = q\big(rr^{-1}\big) = (qr)r^{-1} = 1r^{-1} = r^{-1}.$$

4. Das folgt direkt aus Punkt 1. □

Bezeichnung 5.71 (Inverse)**.** Wir nennen r^{-1} das *Inverse* von r. (Umgekehrt ist auch r das Inverse von r^{-1}.)

Bemerkung 5.72. Es gibt Ringe, in der nicht jedes Element ein Inverses besitzt. *Beispiel*: Wir betrachten den Ring $(\mathrm{End}_K(K^{\mathbb{N}}), +, \circ)$ der Endomorphismen auf dem Folgenraum $K^{\mathbb{N}}$ unter Addition $+$ und Komposition $\circ$. Wir definieren den Links- und Rechtsshift

$$\begin{aligned} f &\in \mathrm{End}_K(K^{\mathbb{N}}), \quad f\colon (x_1, x_2, x_3, \dots) \mapsto (x_2, x_3, x_4, \dots),\\ g &\in \mathrm{End}_K(K^{\mathbb{N}}), \quad g\colon (x_1, x_2, x_3, \dots) \mapsto (0, x_1, x_2, \dots). \end{aligned}$$

Dann gilt zwar $f \circ g = \mathrm{id}_{K^{\mathbb{N}}}$ (die Null wird wieder vernichtet), aber es gibt kein $h \in \mathrm{End}_K^(K^{\mathbb{N}})$ mit $h \circ f = \mathrm{id}_{K^{\mathbb{N}}}$ (denn $(x_2, x_3, x_4, \dots)$ enthält keine Information über x_1). Es gibt sogar mehrere Rechtsinverse zu f, da die 0 beliebig gewählt wurde:

$$g_a \in \mathrm{End}_K(K^{\mathbb{N}}), \qquad g_a\colon (x_1, x_2, x_3, \dots) \mapsto (a, x_1, x_2, \dots) \qquad \text{für alle } a \in K.$$

Satz 5.73. *Sei $A \in K^{m,n}$. Dann sind folgende Aussagen äquivalent:*

1. *A ist ein Isomorphismus.*
2. *$m = n$ und es gibt Elementarmatrizen $T_1, \dots, T_t \in K^m$ mit $T_t \cdots T_1 A = E_n$.*
3. *$m = n$ und es gibt Elementarmatrizen $T_1, \dots, T_t \in K^n$ mit $AT_1 \dots T_t = E_m$.*
4. *$m = n$ und A ist invertierbar.*
5. *$m = n$ und E_n ist die reduzierter Zeilenstufenform von A.*

Beweis.

- Aus Punkt 1 folgt Punkt 2: Sei A ein Isomorphismus. Nach Satz 5.53 gibt es Elementarmatrizen $T_1, \dots, T_t$, sodas $B \coloneqq T_t \cdots T_1 A$ in reduzierter Zeilenstufenform ist.

  Sei $r \coloneqq |\mathcal{I}(B)|$. Wäre $r < n$, so ist $\mathcal{K}(B) \neq \varnothing$ und es gibt Vektoren L_j^B, also $\mathrm{Kern}(B) = \mathrm{Kern}(A) \neq 0$. Aus Lemma 4.23 folgt aber, dass A kein Monomorphismus sein kann, was dem Isomorphismus widerspricht. Folglich ist $r = n$. Es kann also nur noch $B = E_n$ oder

$$B = \left(\begin{array}{ccc} 1 & & \\ & \ddots & \\ & & 1 \\ \hline & & \\ & 0 & \\ & & \end{array}\right).$$

  Weil A und die Elementarmatrizen Isomorphismen sind, ist auch B ein Isomorphismus damit ein Epimorphismus und daher $\mathrm{Bild}(B) = K^m$. Wäre $m > n$, so ist B von der zweiten Form und wir sehen leicht, dass die Standardbasisvektoren $e_{n+1}, \dots, e_m \notin \mathrm{Bild}(B) = K^m$ liegen, Widerspruch!

  Folglich ist $m = n$ und $B = E_n$. Insbesondere ist E_n die einzige reduzierte Zeilenstufenform von A.

- Punkte 2 und 3 sind äquivalent: Für Elementarmatrizen sind folgende Gleichungen äquivalent:

$$T_t \cdots T_1 A = E_n, \tag{5.74}$$
$$A = T_1^{-1} \cdots T_t^{-1}, \tag{5.75}$$
$$A T_1 \cdots T_1 = E_n. \tag{5.76}$$

  Wir wissen, dass Elementarmatrizen invertierbar sind (Lemma 5.45). Somit folgt (5.74) aus (5.75) durch Multiplikation mit $T_1^{-1} \cdots T_t^{-1}$ von links, und (5.75) aus (5.74) durch Multiplikation mit $T_t \cdots T_1$ von links. Analog sind (5.75) und (5.76) äquivalent, also auch (5.74) und (5.76).

- Aus Punkte 2 und 3 folgt Punkt 4: Die Produkte der Elementarmatrizen $B, C \in M_n(K)$ erfüllen $AB = E_n = CA$. Also hat A Links- und Rechtsinverse.

- Aus Punkt 4 folgt Punkt 5: Wenn A invertierbar ist, gibt es Matrizen $B, C \in M_n(K)$ mit $AB = E_n = CA$. Aus Lemma 4.15 folgt, dass A sowohl ein Mono- als auch ein Epimorphismus ist und deshalb ein Isomorphismus ist.

- Punkte 2 und 5 sind äquivalent: Zur Hinrichtung: Die Eindeutigkeit folgt aus dem Beweis zu Punkt 1. Zur Rückrichtung: Das ist die Definition. □

Folgende Aussage ist sehr schön und sehr wichtig.[9]

Korollar 5.77. *Sei K ein Körper. Für $m, n \geq 0$ gilt*

$$K^m \cong K^n \iff m = n.$$

Beweis. Ist $K^m \cong K^n$, dann gibt es einen Isomorphismus $A \in K^{m,n}$, woraus $m = n$ folgt. Ist hingegen $m = n$, so ist $A = E_n = \mathrm{id}_{K^n}$ ein Isomorphismus zwischen K^m und K^n. □

Korollar 5.78 (Praktische Berechnung inverser Matrizen)**.** *Sei $A \in M_n(K)$ invertierbar. Der Gauß-Algorithmus liefert Elementarmatrizen $T_1, \dots, T_t$ mit $T_t \cdots T_1 A = E_n$. Dann gilt*

$$A^{-1} = T_t \cdot T_1 \qquad \text{und} \qquad A = T_1^{-1} \cdot T_t^{-1}.$$

Bemerkung 5.79. Wir haben hier die *invertierbaren* Matrizen charakterisiert. Dennoch gibt es (notwendigerweise) nichtquadratische Matrizen, die nur Links-, aber keine Rechtsinversen besitzen oder andersherum.

Definition 5.80 (allgemeine lineare Gruppe)**.** Für $n \geq 1$ sei

$$\mathrm{GL}_n(K) \coloneqq \{A \in M_n(K) \mid A \text{ ist invertierbar}\}$$

die *allgemeine lineare Gruppe* vom Grad n über einem Körper K.

[9] Wir können das auch später durch lineare Fortsetzung mittels Basisvektoren zeigen.

Korollar 5.81. *Jedes $A \in \mathrm{GL}_n(K)$ ist ein Produkt von Elementarmatrizen vom Typ (I) und (II).*

Korollar 5.82. *Für alle $A \in \mathrm{GL}_n(K)$ gilt $A^{-1} \in \mathrm{GL}_n(K)$ und $(A^{-1})^{-1} = A$.*

Satz 5.83. *Für $A \in M_n(K)$ sind äquivalent:*

1. *A ist ein Isomorphismus.*
2. *A ist ein Monomorphismus.*
3. *A ist ein Epimorphismus.*

Beweis. Aus Punkt 1 folgen per Definition Punkte 2 und 3.

- Aus Punkt 2 folgt Punkt 1: Sei A ein Monomorphismus. Seien $T_1, \dots, T_t$ Elementarmatrizen, sodass $B = T_t \cdot T_1 A$ eine reduzierter Zeilenstufenform von A ist. Da $T_t \cdot T_1$ ein Iso- und A ein Monomorphismus ist, ist auch B ein Monomorphismus. Damit ist $\mathrm{Kern}(B) = 0$ (Lemma 4.23) und somit $\mathcal{K}(B) = \varnothing$ und $\mathcal{I}(B) = n$. Weil B quadratisch ist, haben wir $B = E_n$. Nach Satz 5.73 ist A ein Isomorphismus.
- Aus Punkt 3 folgt Punkt 1: Sei A ein Epimorphismus. Wieder seien $T_1, \dots, T_t$ Elementarmatrizen, sodass $B = T_t \cdot T_1 A$ eine reduzierter Zeilenstufenform von A ist. Da $T_t \cdot T_1$ ein Iso- und A ein Epimorphismus ist, ist auch B ein Epimorphismus, also $\mathrm{Bild}(B) = K^n$. Wäre $|\mathcal{I}(B)| < n$, so ist mindestens die letzte Zeile von B gleich Null, weil B quadratisch ist. Mit Lemma 5.63 schließen wir aber, dass der Standardbasisvektor $e_n \notin \mathrm{Bild}(B)$, ein Widerspruch zu $\mathrm{Bild}(B) = K^n$. Daher ist $\mathcal{I}(B) = n$ und, weil B quadratisch ist, $B = E_n$. Nach 5.73 ist A ein Isomorphismus. □

Bemerkung 5.84.

1. Ein alternativer Beweis ergibt sich durch Benutzung der Transposition. Angenommen wir haben gezeigt, dass wenn A ein Monomorphismus ist, dann A ein Isomorphismus ist.

   Sei nun A ein Epimorphismus. Daraus folgt, dass A^T ein Monomorphismus ist. Mit dem gerade Gezeigtem ist A^T ein Isomorphismus, also auch A selbst, was zu zeigen war.

2. Es gibt K-Vektorräume V und $f, g \in \mathrm{End}(V)$, sodass
   - f ein Monomorphismus, aber kein Isomorphismus, und
   - g ein Epimorphismus, aber kein Isomorphismus ist

   (S. Bemerkung 5.72).

Bezeichnung 5.85. Seien $A = (a_{ij}) \in K^{m,n}$ und $B = (b_{ij}) \in K^{m,l}$ Matrizen. Wir definieren

$$[A|B] := \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & b_{11} & \cdots & b_{1l} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} & b_{m1} & \cdots & b_{ml} \end{array}\right) \in K^{m,n+l},$$

wobei dessen linker $(m \times n)$-Block A und dessen rechter $(m \times l)$-Block B ist.

Bemerkung 5.86 (Trick zur Berechnung von Inversen). Sei $A \in K^{n,n}$. Dann liefert der Gauß-Algorithmus Elementarmatrizen $T_1, \dots, T_t$ mit $T_t \cdots T_1 A = E_n$. Anschließend müssen wir das möglicherweise aufwändige Produkt $T_t \cdots T_1 = A^{-1}$ berechnen, um das Inverse zu bestimmen.

Um das zu vermeiden, definieren wir

$$C := [A|E_n] \in K^{n,2n}.$$

Wenden wir die Elementarmatrizen auf C an, gilt

$$T_t \cdots T_1 C = [E_n|A^{-1}],$$

weil die Zeilenoperationen keine Spalten miteinander verrechnen. Die Matrix $[E_n|A^{-1}]$ ist die reduzierte Zeilenstufenform von C.

Statt also den Gauß-Algorithmus auf A anzuwenden und dann das Produkt $T_t \cdots T_1$ zu berechnen, ist es einfacher, wenn wir den Gauß-Algorithmus gleich auf $C = [A|E_n]$ anwenden und das Inverse dann daraus ablesen.

5.12 Beispiele

5.12.1 Berechnung einer inversen Matrix

Sei

$$A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & -2 \\ 0 & -1 & 1 \end{pmatrix} \in \mathbb{Q}^{3,3}.$$

Der Gauß-Algorithmus liefert schrittweise die folgenden Matrizen:

$$\begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & -2 \\ 0 & -1 & 1 \end{pmatrix} \xrightarrow{D_1(\frac{1}{2})} \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 1 & 2 & -2 \\ 0 & -1 & 1 \end{pmatrix} \xrightarrow{T_{21}(-1)} \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & \frac{5}{2} & -2 \\ 0 & -1 & 1 \end{pmatrix} \xrightarrow{D_2(\frac{2}{5})} \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 1 & -\frac{4}{5} \\ 0 & -1 & 1 \end{pmatrix}$$

$$\xrightarrow{T_{32}(1)} \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 1 & -\frac{4}{5} \\ 0 & 0 & \frac{1}{5} \end{pmatrix} \xrightarrow{D_3(5)} \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 1 & -\frac{4}{5} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{T_{23}(\frac{4}{5})} \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{T_{12}(\frac{1}{2})} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Weil das Ergebnis E_3 ist, ist A invertierbar. Es folgt, dass

$$A^{-1} = T_{12}(\tfrac{1}{2}) \cdot T_{23}(\tfrac{4}{5}) \cdot D_3(5) \cdot T_{32}(1) \cdot D_2(\tfrac{2}{5}) \cdot T_{21}(-1) \cdot D_1(\tfrac{1}{2}).$$

Um dieses Produkt nicht ausrechnen zu müssen, wenden wir den Trick aus Bemerkung 5.86 an. Wir bilden eine (3×6)-Matrix $C := [A|E_3]$, deren linker (3×3)-Block gleich A und rechter (3×3)-Block gleich B ist. Dann ist

$$T_{12}(\tfrac{1}{2}) \cdot T_{23}(\tfrac{4}{5}) \cdot D_3(5) \cdot T_{32}(1) \cdot D_2(\tfrac{2}{5}) \cdot T_{21}(-1) \cdot D_1(\tfrac{1}{2}) \cdot [A|E_3] = [E_3|A^{-1}].$$

Sei also

$$C = [A|E_3] = \left(\begin{array}{ccc|ccc} 2 & -1 & 0 & 1 & 0 & 0 \\ 1 & 2 & -2 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 \end{array}\right) \in \mathbb{Q}^{3,6}.$$

Der Gauß-Algorithmus (mit den gleichen Operationen) liefert schrittweise folgende Matrizen

$$C = [A|E_3] \left(\begin{array}{ccc|ccc} 2 & -1 & 0 & 1 & 0 & 0 \\ 1 & 2 & -2 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{D_1(\frac{1}{2})} \left(\begin{array}{ccc|ccc} 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 1 & 2 & -2 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{T_{21}(-1)} \left(\begin{array}{ccc|ccc} 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{5}{2} & -2 & -\frac{1}{2} & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{D_2(\frac{2}{5})} \left(\begin{array}{ccc|ccc} 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -\frac{4}{5} & -\frac{1}{5} & \frac{2}{5} & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{T_{32}(1)} \left(\begin{array}{ccc|ccc} 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -\frac{4}{5} & -\frac{1}{5} & \frac{2}{5} & 0 \\ 0 & 0 & \frac{1}{5} & -\frac{1}{5} & \frac{2}{5} & 1 \end{array}\right) \xrightarrow{D_3(5)} \left(\begin{array}{ccc|ccc} 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -\frac{4}{5} & -\frac{1}{5} & \frac{2}{5} & 0 \\ 0 & 0 & 1 & -1 & 2 & 5 \end{array}\right)$$

$$\xrightarrow{T_{23}(\frac{4}{5})} \left(\begin{array}{ccc|ccc} 1 & -\frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 & -1 & 2 & 4 \\ 0 & 0 & 1 & -1 & 2 & 5 \end{array}\right) \xrightarrow{T_{12}(\frac{1}{2})} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 & 2 & 4 \\ 0 & 0 & 1 & -1 & 2 & 5 \end{array}\right) = [E_3|A^{-1}]$$

Also gilt

$$A^{-1} = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 2 & 4 \\ -1 & 2 & 5 \end{pmatrix}$$

5.12.2 Invertierbare 2×2-Matrizen

Proposition 5.87. *Sei $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K^{2,2}$. Dann ist A invertierbar genau dann, wenn $ad - bc \neq 0$ gilt.*[10] *In diesem Fall ist*

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in K^{2,2}.$$

[10] Das ist die *Determinante*, die wir später noch behandeln werden.

Beweis.

Fall 1 ($a \neq 0$). Wir wenden den Gauß-Algorithmus an und erhalten

$$D_1(a^{-1})A = \begin{pmatrix} 1 & a^{-1}b \\ c & d \end{pmatrix}, \qquad T_{21}(-c)D_1(a^{-1})A = \begin{pmatrix} 1 & a^{-1}b \\ 0 & d - a^{-1}bc \end{pmatrix} =: B.$$

Wir sehen, dass $d - a^{-1}bc \neq 0 \iff ad - bc \neq 0$.

Fall 2a ($a \neq 0$ und $ad - bc = 0$). In diesem Fall erhalten wir

$$\begin{pmatrix} 1 & a^{-1}b \\ 0 & d - a^{-1}bc \end{pmatrix}^T \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0.$$

Gäbe es also ein Inverses B^{-1}, würde

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = E_n \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \left(\left(B^{-1}\right)^T B^T \right) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \left(B^{-1}\right)^T \left(B^T \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \left(B^{-1}\right)^T 0 = 0$$

gelten, ein Widerspruch. Folglich sind B und somit auch A nicht invertierbar.

Fall 2b ($a \neq 0$ und $ad - bc \neq 0$). In diesem Fall setzen wir den Gauß-Algorithmus fort und erhalten

$$T_{12}(-a^{-1}b)D_2((d - a^{-1}bc)^{-1})T_{21}(-c)D_1(a^{-1})A = E_2.$$

Also ist A invertierbar mit

$$A^{-1} = T_{12}(-a^{-1}b)D_2((d - a^{-1}bc)^{-1})T_{21}(-c)D_1(a^{-1}) = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Fall 2 ($a = 0$ und $c = 0$). In diesem Fall erhalten wir

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0.$$

Gäbe es also ein Inverses A^{-1}, würde

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = E_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left(A^{-1}A\right) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A^{-1} \left(A \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = A^{-1}0 = 0$$

gelten, ein Widerspruch. Folglich ist A nicht invertierbar.

Fall 3 ($a = 0$ und $c \neq 0$). Offenbar ist A genau dann invertierbar, wenn

$$E_{12}A = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

invertierbar ist. Nach Satz 5.73 gibt es dann Elementarmatrizen $T_1, \ldots, T_t$, sodass $T_t \cdots T_1(E_{12}A) = E_n$. Dann ist aber auch $A^{-1} = T_t \cdots T_1 E_{12}$.

Dieser Fall erfolgt analog zu Fall Fall 1, sodass $E_{12}A$ genau dann invertierbar ist, wenn $cb - da \neq 0 \iff ad - bc \neq 0$ mit

$$(E_{12}A)^{-1} = \frac{1}{cb - da} \begin{pmatrix} b & -d \\ -a & c \end{pmatrix} \iff A^{-1} = \frac{1}{cb - da} \begin{pmatrix} b & -d \\ -a & c \end{pmatrix} E_{12} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Nach vollständiger Fallunterscheidung sehen wir, dass A genau dann invertierbar ist, wenn $ad - bc \neq 0$ gilt. $\square$

Ende der Vorlesung 9 am 09. November 2021

5.13 Übungsaufgaben

Definition 5.88 (Transponierte)**.** Sei

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in K^{m,n}.$$

Die *Transponierte* A^T von A ist definiert durch

$$A^T := (a_{ji}) = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nm} \end{pmatrix} \in K^{n,m}.$$

Der Eintrag a_{ij} in der i-ten Zeile und j-ten Spalte von A wird also zum Eintrag der j-ten Zeile und i-ten Spalte von A^T.

Lemma 5.89. *Für alle $A \in K^{l,m}$ und $B \in K^{m,n}$ gilt*

$$(AB)^T = B^T A^T.$$

Lemma 5.90. *Sei $A \in K^{m,n}$ eine Matrix und sei A^T die Transponierte von A. Dan gelten:*

1. *A ist genau dann ein Monomorphismus, wenn A^T ein Epimorphismus ist.*
2. *A ist genau dann ein Epimorphismus, wenn A^T ein Monomorphismus ist.*
3. *A ist genau dann ein Isomorphismus, wenn A^T ein Isomorphismus ist.*

6 Lineare Gleichungssysteme

Mit ausreichend formaler Theorie kommen wir nun zur eine der Hauptanwendungsgebiete der linearen Algebra: *lineare Gleichungssysteme.*

6.1 Definition eines Linearen Gleichungssystems

Definition 6.1 (lineares Gleichungssystem, Variable, Koeffizient)**.** Ein *lineares Gleichungssystem* besteht aus m Gleichungen der Form

$$\begin{matrix} a_{11}X_1 + a_{12}X_2 & + \ldots + a_{1n}X_n & = b_1 \\ a_{21}X_1 + a_{22}X_2 & + \ldots + a_{2n}X_n & = b_2 \\ \vdots \qquad\quad \vdots & \vdots & \vdots \\ a_{m1}X_1 + a_{m2}X_2 & + \ldots + a_{mn}X_n & = b_m \end{matrix} \qquad \text{mit } a_{ij}, b_i \in K \tag{6.2}$$

wobei $X_1, \ldots, X_n$ *Variablen* oder *Unbekannte* und die a_{ij} *Koeffizienten* genannt werden.

Die Variablen stehen für Platzhalter, sodass, wenn wir Werte dafür einsetzen, Gleichungen in K entstehen.

Definition 6.3 (Matrixschreibweise, Koeffizientenmatrix)**.** Mittels der Matrixmultiplikation können wir (6.2) kürzer schreiben:

$$Ax = b,$$

wobei

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in K^{m,n}$$

die *Koeffizientenmatrix* von (6.2) und

$$x \coloneqq \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} \in K^m \qquad \text{und} \qquad b \coloneqq \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m$$

ist.

Definition 6.4 (Lösung, Lösungsmenge)**.** Ein Vektor

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$$

ist eine *Lösung* von (6.2), falls

$$\begin{aligned} a_{11}v_1 + a_{12}v_2 &+ \ldots + a_{1n}v_n &= b_1 \\ a_{21}v_1 + a_{22}v_2 &+ \ldots + a_{2n}v_n &= b_2 \\ \vdots \qquad\quad \vdots \;&\quad \vdots &\vdots\; \\ a_{m1}v_1 + a_{m2}v_2 &+ \ldots + a_{mn}v_n &= b_m \end{aligned}$$

gilt. Die *Lösungsmenge* des linearen Gleichungssystems (6.2) definieren wir als

$$\mathcal{L}(A, b) \coloneqq \{v \in K^n \mid v \text{ ist eine Lösunge von } (6.2)\}.$$

Definition 6.5 ((in-)homogen, erweiterte Koeffizientenmatrix)**.** Das lineare Gleichungssystem $Ax = b$ heißt *homogen*, falls $b = 0$, und andernfalls *inhomogen*.

Die Matrix

$$[A|b] \coloneqq \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right) \in K^{m,n+1}$$

ist die *erweiterte Koeffizientenmatrix* von (6.2).

Lemma 6.6. *Sei $Ax = b$ ein lineares Gleichungssystem mit $A \in K^{m,n}$ und $b \in K^m$. Dann gilt*

$$\mathcal{L}(A, b) = \{v \in K^n \mid A(v) = b\} = A^{-1}(b).$$

Beweis. Das folgt sofort aus Definition 6.4. □

Bezeichnung 6.7 (Lösbarkeit)**.** Ein Gleichungssystem $Ax = b$ ist

- *lösbar*, falls $\mathcal{L}(A, b) \neq \varnothing$,
- *eindeutig lösbar*, falls $|\mathcal{L}(A, b)| = 1$, und
- *unlösbar*, falls $\mathcal{L}(A, b) = \varnothing$.

6.2 Lösungsverfahren

Lemma 6.8. *Sei $T \in K^{m,m}$ eine Elementarmatrix und sei $[A|b] \in K^{m,n+1}$ die erweiterte Koeffizientenmatrix. Sei*

$$[A'|b'] \coloneqq \left(\begin{array}{ccc|c} a'_{11} & \cdots & a'_{1n} & b'_1 \\ \vdots & \ddots & \vdots & \vdots \\ a'_{m1} & \cdots & a'_{mn} & b'_m \end{array}\right) \coloneqq T \cdot [A|b].$$

Dann gilt

$$\mathcal{L}(A', b') = \mathcal{L}(A, b).$$

Beweis. Sei

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n.$$

Dann gilt die Aussage für Elementarmatrizen $T = T_{ij}(\lambda)$ vom Typ (I) mit $i \neq j$ und $\lambda \in K^\times$. Für alle $1 \leq i, j \leq m$ mit $i \neq j$ und $\lambda \in K$ ist

$$\sum_{k=1}^{n} a_{ik} v_k = b_i \qquad \text{und} \qquad \sum_{k=1}^{n} a_{jk} v_k = b_j$$

in $Ax = b$ äquivalent zu

$$\sum_{k=1}^{n} (a_{ik} + \lambda a_{jk}) v_k = b_i \qquad \text{und} \qquad \sum_{k=1}^{n} a_{jk} v_k = b_j$$

in $A'x = b'$.

Für Elementarmatrizen $T = D_i(\lambda)$ vom Typ (II) ist

$$\sum_{k=1}^{n} a_{ik} v_k = b_i$$

in $Ax = b$ äquivalent zu

$$\sum_{k=1}^{n} \lambda a_{ik} v_k = \lambda b_i$$

in $A'x = b'$ für alle $1 \leq i \leq m$ und $\lambda \in K^\times$.

Für Elementarmatrizen vom Typ (III) ist das auch klar wegen Lemma 5.47. Letztendlich erhalten Elementarmatrizen nur die Lösungsmenge. □

Bemerkung 6.9. Ist $[A|b]$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems, so können wir wegen 5.53 und Lemma 6.8 o. B. d. A. annehmen, dass A bereits in reduzierter Zeilenstufenform ist.

Satz 6.10 (Lösung eines linearen Gleichungssystems)**.** *Sei $Ax = b$ ein lineares Gleichungssystem mit A in reduzierter Zeilenstufenform und $\mathcal{I}(A) = \{j_1 < \cdots < j_r\}$. Dann gelten:*

1. *Falls $b_k \neq 0$ für ein $r + 1 \leq k \leq m$ gilt, so ist $Ax = b$ unlösbar, d. h. $\mathcal{L}(A, b) = \varnothing$.*
2. *Angenommen es gilt $0 = b_{r+1} = \cdots = b_m$. Wir definieren*

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n \qquad \textit{durch} \qquad v_k := \begin{cases} b_s & \textit{falls } k = j_s \textit{ für ein } 1 \leq s \leq r, \\ 0 & \textit{sonst.} \end{cases}$$

Dann gilt

$$\mathcal{L}(A, b) = v + \mathcal{L}(A,0) = v + \operatorname{Kern}(A).$$

Wir sehen also, dass $\mathcal{L}(A, b)$ eine Restklasse modulo $\operatorname{Kern}(A)$ ist. Dabei ist v gerade so konstruiert, sodass $Av = b$ bzw. $v \in A^{-1}(b)$ gilt.

Beweis.

1. Seien $w \in K^n$ und

$$\begin{pmatrix} w'_1 \\ \vdots \\ w'_m \end{pmatrix} := A(w).$$

Weil für $r + 1 \leq k \leq m$ die k-te Zeile von A gleich Null ist, ist nach Multiplikation $0 = w'_{r+1} = \cdots = w'_m$. Nun gibt es aber ein $b_k \neq 0$ für ein $r + 1 \leq k \leq m$. Folglich ist $Aw \neq b$ für alle $w \in K^n$.

2. Seien nun $0 = b_{r+1} = \cdots = b_m$ und v wie oben definiert. Weil v nur Einträge bei den Zeilenstufenindizes hat, und weil A in der k-ten Zeile ($1 \leq k \leq r$) von allen Spalten $\mathcal{I}(A)$ genau bei j_k eine Eins hat, gilt $A(v) = b$. Der Rest folgt aus Lemma 4.25. □

Korollar 6.11 (Lösbarkeit)**.** *Sei $A \in K^{m,n}$ in reduzierter Zeilenstufenform mit $|\mathcal{I}(A)| = r$, und sei $b \in K^m$. Dann ist das lineare Gleichungssystem $Ax = b$ genau dann lösbar, wenn $0 = b_{r+1} = \cdots = b_m$ gilt.*

Korollar 6.12 (eindeutige Lösbarkeit)**.** *Sei $A \in K^{m,n}$ in reduzierter Zeilenstufenform mit $|\mathcal{I}(A)| = r$, und sei $b \in K^m$. Dann ist das lineare Gleichungssystem $Ax = b$ genau dann eindeutig lösbar, wenn $0 = b_{r+1} = \cdots = b_m$ und* $\operatorname{Kern}(A) = 0$ *gilt.*

6.3 Beispiele

Beispiel 6.13. Sei $K = \mathbb{Q}$ und sei

$$[A|b] := \begin{pmatrix} 0 & 0 & 2 & 4 & -6 & 1 & -1 & 0 \\ 2 & 1 & 1 & 0 & -1 & 0 & 1 & 2 \\ 2 & 1 & 0 & -2 & 2 & 1 & 1 & 6 \\ 4 & 2 & 0 & -4 & 4 & 1 & 1 & 8 \\ 2 & 1 & 0 & -2 & 2 & -3 & 1 & -6 \end{pmatrix} \in \mathbb{Q}^{5,8}$$

Der Gauß-Algorithmus liefert

$$[B|c] = \begin{pmatrix} 1 & \frac{1}{2} & 0 & -1 & 1 & 0 & 0 & 1 \\ & & 1 & 2 & -3 & 0 & 0 & -1 \\ & & & & & 1 & 0 & 3 \\ & & & & & & 1 & 1 \\ & & & & & & & 0 \end{pmatrix},$$

wobei B in reduzierter Zeilenstufenform ist. An der letzten Spalte c sehen wir, dass das lineare Gleichungssystem lösbar ist ($c_5 = 0 = b_{5j}$ für alle $1 \leq j \leq 9$). Es gelten $\mathcal{I}(B) = \{1, 3, 6, 7\}$, $\mathcal{K}(B) = \{2, 4, 5\}$ und

$$L_2^B = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad L_4^B = \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad L_5^B = \begin{pmatrix} -1 \\ 0 \\ 3 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad \in \mathbb{Q}^7.$$

Zudem ist der Kern von B

$$\operatorname{Kern}(B) = \operatorname{Kern}(A) = \mathcal{L}(A, 0) = \{a_2 L_2^B + a_4 L_4^B + a_5 L_5^B \mid a_2, a_4, a_5 \in K\}$$

und eine Lösung von $Bx = c$ ist

$$v := \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 3 \\ 1 \end{pmatrix} \in \mathbb{Q}^7,$$

also $Bv = c$ und damit auch $Av = b$. Demnach ist die Lösungsmenge

$$\mathcal{L}(A, b) = v + \mathcal{L}(A, 0).$$

Beispiel 6.14. Für $a, b, c \in \mathbb{Q}$ sei

$$A = \begin{pmatrix} 1 & a & b \\ c & b & a \end{pmatrix} \in \mathbb{Q}^{2,3}.$$

Wir wollen das homogene lineare Gleichungssystem $Ax = 0$ in Abhängigkeit von a, b, c lösen. Weil unter Zeilenoperationen die Nullspalte in $[A|0]$ unverändert bleibt, können wir sie weglassen.

Wir fangen einfach an, den Gauß-Algorithmus anzuwenden:

$$\begin{pmatrix} 1 & a & b \\ c & b & a \end{pmatrix} \xrightarrow{T_{21}(-c)} \begin{pmatrix} 1 & a & b \\ 0 & b-ca & a-cb \end{pmatrix}.$$

Nun erfolgt eine vollständige Fallunterscheidung.

Fall 1 ($b - ca \neq 0$). Wir erhalten

$$\xrightarrow{D_2((b-ca)^{-1})} \begin{pmatrix} 1 & a & b \\ 0 & 1 & \dfrac{a-cb}{b-ca} \end{pmatrix} \xrightarrow{T_{12}(-a)} \begin{pmatrix} 1 & 0 & b - a\dfrac{a-cb}{b-ca} \\ 0 & 1 & \dfrac{a-cb}{b-ca} \end{pmatrix}.$$

Als *Basis* von $\mathrm{Kern}(A)$ erhalten wir

$$L_3^B = \begin{pmatrix} -b + a\dfrac{a-cb}{b-ca} \\ -\dfrac{a-cb}{b-ca} \\ 1 \end{pmatrix}$$

und daher $\mathcal{L}(A, 0) = \{a_3 L_3^B \mid a_3 \in \mathbb{Q}\}$.

Fall 2 ($b - ca = 0$ und $a - cb \neq 0$). Dann erhalten wir

$$\begin{pmatrix} 1 & a & b \\ 0 & 0 & a-cb \end{pmatrix} \xrightarrow{D_2((a-cb)^{-1})} \begin{pmatrix} 1 & a & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Als *Basis* von $\mathrm{Kern}(A)$ erhalten wir

$$L_2^B = \begin{pmatrix} -a \\ 1 \\ 0 \end{pmatrix}$$

und daher $\mathcal{L}(A, 0) = \{a_2 L_2^B \mid a_2 \in \mathbb{Q}\}$.

Fall 3 ($b - ca = 0$ und $a - cb = 0$). Wir erhalten die reduzierte Zeilenstufenform

$$\begin{pmatrix} 1 & a & b \\ 0 & 0 & 0 \end{pmatrix}.$$

Als *Basis* von $\mathrm{Kern}(A)$ erhalten wir

$$L_2^B = \begin{pmatrix} -a \\ 1 \\ 0 \end{pmatrix}, \qquad L_3^B = \begin{pmatrix} -b \\ 0 \\ 1 \end{pmatrix},$$

und daher $\mathcal{L}(A, 0) = \{a_2 L_2^B + a_3 L_3^B \mid a_2, a_3 \in \mathbb{Q}\}$.

7 Lineare Unabhängigkeit, Basen und Dimension

7.1 Linearkombinationen und lineare Hüllen

Definition 7.1 (Linearkombination)**.** Sei V ein K-Vektorraum. Seien $v_1, \ldots, v_m \in V$. Dann ist $v \in V$ eine *Linearkombination von* $v_1, \ldots, v_m$, falls es $a_1, \ldots, a_m \in K$ gibt mit

$$v = a_1 v_1 + \cdots + a_m v_m.$$

Beispiel 7.2.

1. Für alle $v_1, \dots, v_m \in V$ ist $0 \in V$ eine Linearkombination von $v_1, \dots, v_m$, denn $0 = 0v_1 + \dots + 0v_m$.
2. Jeder Vektor $v \in K^n$ ist eine Linearkombination der Standardbasisvektoren $e_1, \dots, e_n$ von K^n (Lemma 5.33).
3. Seien $v_1 = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, $v_2 = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ und $v_3 = \left(\begin{smallmatrix}-1\\1\end{smallmatrix}\right)$ in $\mathbb{Q}^2$. Dann gilt
$$\begin{pmatrix}2\\1\end{pmatrix} = 2v_1 + 1v_2 + 0v_3 = 3_v1 + 0v_2 + 1v_3.$$
Achtung: Linearkombinationen müssen also nicht immer eindeutig sein.
4. Sei $A \in K^{m,n}$ eine Koeffizientenmatrix und $b \in K^n$. Das Gleichungssystem $Ax = b$ ist genau dann lösbar, wenn b eine Linearkombination der Spalten $A(e_1), \dots, A(e_n)$ von A ist, also $b \in \mathrm{Bild}(A)$. Für alle $v \in K^n$ gilt nämlich
$$Ax = v_1 A(e_1) + \dots + v_n A(e_n).$$

Ende der Vorlesung 10 am 12. November 2021