Lineare Algebra I

Prof. Dr. Alexander Schmidt

Wintersemester 2019/20

Kapitel 0

Grundlagen

0.1 Aussagenlogik

Naive Logik, wir verwenden die sprachliche Vorstellung ($\neq$ mathematische Logik: eigene Vorlesung)

Eine (mathematische) **Aussage** ist ein feststellender Satz, dem genau einer der Wahrheitswerte *wahr* oder *falsch* zugeordnet werden kann. So ist „Die Zahl 5 ist ungerade." eine Aussage mit dem Wahrheitswert *wahr*. Der Satz: „Das Haus hat eine schöne Farbe." ist solange keine Aussage, bis man genau präzisiert hat, welches Haus gemeint ist und welche Farben man als schön bezeichnet.

Aus einfachen Aussagen kann man durch logische Verknüpfungen kompliziertere Aussagen bilden. Den Wahrheitswert der zusammengesetzen Aussage erhält man aus den Wahrheitswerten der einzelnen Aussagen durch **Wahrheitstafeln**.

Im Folgenden seien A und B Aussagen. Wir haben die folgenden Verknüpfungen

Negation (NICHT-Verknüpfung). Symbol: $\neg$.
Wahrheitstafel:

A	$\neg A$
w	f
f	w

Konjunktion (UND-Verknüpfung). Symbol: $\wedge$.
Wahrheitstafel:

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

Disjunktion (ODER-Verknüpfung). Symbol: $\vee$.

Wahrheitstafel:

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

Beispiel 0.1. Es sei A : 7 ist eine Primzahl (w); B : 5 ist gerade (f). Dann ist
$A \wedge B$: 7 ist eine Primzahl und 5 ist gerade (f)
$A \vee B$: 7 ist eine Primzahl oder 5 ist gerade (w).

Bemerkung 0.2. Es handelt sich um ein „einschließendes“ ODER.
„Entweder A oder B“ korrespondiert zu: $(A \vee B) \wedge (\neg(A \wedge B))$.

Implikation (WENN-DANN-Verknüpfung). Symbol: $\Rightarrow$.
Wahrheitstafel:

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

Sprechweisen: Aus A folgt B. A impliziert B. A ist eine hinreichende Bedingung für B. B ist eine notwendige Bedingung für A (ist $A \Rightarrow B$ wahr, so kann A nur wahr sein, wenn auch B wahr ist).

Beispiel 0.3. Es seien m, n natürliche Zahlen.
A : m ist gerade
B : mn ist gerade.
Dann ist für alle natürlichen Zahlen m, n die Implikation $A \Rightarrow B$ wahr.

Das sehen wir durch Fallunterscheidung ein:
1.Fall: m gerade, n gerade. Dann ist A wahr, B wahr und damit $A \Rightarrow B$ wahr.
2.Fall: m gerade, n ungerade. Dann ist A wahr, B wahr und damit $A \Rightarrow B$ wahr.
3.Fall: m ungerade, n gerade. Dann ist A falsch, B wahr und damit $A \Rightarrow B$ wahr.
4.Fall: m ungerade, n ungerade. Dann ist A falsch, B falsch und damit $A \Rightarrow B$ wahr.

Äquivalenz (GENAU-DANN-WENN-Verknüpfung). Symbol: $\Leftrightarrow$.
Wahrheitstafel:

A	B	$A \Leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

Sprechweisen: A gilt genau dann, wenn B gilt. A und B sind äquivalent.

Die Aussagen $A \Leftrightarrow B$ und $(A \Rightarrow B) \wedge (B \Rightarrow A)$ sind gleichbedeutend, d.h. haben die gleiche Wahrheitstafel:

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
w	w	w	w	w	w
w	f	f	f	w	f
f	w	f	w	f	f
f	f	w	w	w	w

Beispiele 0.4. Sei a eine ganze Zahl.
1.)
$A : a - 2 > 1$
$B : a > 3$.
Die Äquivalenz $A \Leftrightarrow B$ ist für alle ganzen Zahlen a wahr.

2.)
$A : a > 0$
$B : a^2 > 0$.
Die Äquivalenz $A \Leftrightarrow B$ ist für alle ganzen Zahlen $a < 0$ falsch. Die Implikation $A \Rightarrow B$ gilt für alle ganzen Zahlen a.

Mathematische **Sätze**, **Lemmata**(=Hilfssätze) und **Korollare**(=Folgerungen) sind üblicherweise in der Form wahrer Implikationen formuliert.
Beweisen: Begründen, warum die Implikation wahr ist.
Beweismethoden für die Implikation $A \Rightarrow B$:

- Direkter Beweis: $A \Rightarrow B$
- Beweis durch Kontraposition: $\neg B \Rightarrow \neg A$
- Widerspruchsbeweis: $\neg(A \wedge \neg B)$.

Diese sind äquivalent zueinander:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	$\neg(A \wedge \neg B)$
w	w	f	f	w	w	w
w	f	f	w	f	f	f
f	w	w	f	w	w	w
f	f	w	w	w	w	w

Existenz- und Allquantor

„$A(x)$“ - Aussage, die von einer Variablen x abhängt.

„$\exists x : A(x)$“ ist gleichbedeutend mit: es existiert (mindestens) ein x, so dass $A(x)$ wahr ist.
z.B: $\exists$ natürliche Zahl n: $n > 5$. (wahr)

„$\exists!\ x : A(x)$“ ist gleichbedeutend mit: es existiert genau ein x, so dass $A(x)$ wahr ist.
z.B: $\exists!$ natürliche Zahl n: $n + 5 = 8$. (wahr)

„$\forall x : A(x)$“ ist gleichbedeutend mit: für alle x ist $A(x)$ wahr.
z.B: $\forall$ natürlichen Zahlen n: $4n$ ist gerade. (wahr)

Negation von Existenz und Allquantor

$\neg(\exists x : A(x))$ ist äquivalent zu $\forall x : \neg A(x)$.
$\neg(\forall x : A(x))$ ist äquivalent zu $\exists x : \neg A(x)$.

Beweismethoden für Existenz- und Allaussagen:

- Angabe eines Beispiels, um zu zeigen, dass eine Existenzaussage wahr ist.
  z.B.: ($\exists$ natürliche Zahl n: $n > 5$) ist wahr, denn für $n = 7$ ist $n > 5$ wahr.

- Angabe eines Gegenbeispiels, um zu zeigen, dass eine Allaussage falsch ist.
  z.B.: ($\forall$ natürlichen Zahlen n: $n \leq 5$) ist falsch, denn für $n = 7$ ist $n \leq 5$ falsch.

Allaussagen über natürliche Zahlen.[1]

Vollständige Induktion Es sei $A(n)$ eine Aussage über natürliche Zahlen und es seien die folgenden Aussagen wahr:

IA (Induktionsanfang): $A(1)$.

IS (Induktionsschritt) $\forall$ natürlichen Zahlen n: $A(n) \Rightarrow A(n+1)$.

Dann gilt: $\forall$ natürlichen Zahlen: $A(n)$.

Begründung: IA bedeutet: $A(1)$ ist wahr. IS liefert, dass $A(2)$ wahr ist, dann, dass $A(3)$ wahr ist, u.s.w. Auf diese Weise erreicht man jede natürliche Zahl.

Beispiel 0.5. Wir zeigen die Aussage:

Für alle natürlichen Zahlen n gilt $1 + \cdots + n = \frac{n(n+1)}{2}$.

mit Hilfe von vollständiger Induktion.
IA: $1 = (1 \cdot 2)/2$ (wahr).
IS: Es gelte $1 + \cdots + n = \frac{n(n+1)}{2}$. Dann gilt

$$1 + \cdots + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}.$$

[1] Natürliche Zahlen sind $1, 2, 3, \ldots$, d.h. nach unserer Konvention ist 0 keine natürliche Zahl.

0.2 Mengen

Definition 0.6 (Cantor)**.** Eine **Menge** ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen.

Diese naive Definition bringt Probleme mit sich, reicht aber für unsere Zwecke. Es gibt einen strikten, axiomatischen Zugang zur Mengenlehre.

Schreibweise für Mengen
$M = \{a, b, c, \dots\}$
z.B. $\{1, 2, 3\} = \{1, 3, 2\} = \{3, 2, 1, 1\}$
$a \in M$: a ist Element von M
$a \notin M$: a ist nicht Element von M
andere Schreibweise $M = \{A \mid B\}$ ist die Menge der Objekte der Form A, die der Bedingung B genügen, z.B. $M = \{x \mid x \in \mathbb{R},\ x \leq 5\}$ oder kürzer $M = \{x \in \mathbb{R} \mid x \leq 5\}$.

Beispiele 0.7. (Zahlbereiche)
$\mathbb{N} = \{1, 2, 3, \dots\}$ natürliche Zahlen
$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ natürliche Zahlen mit Null
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ ganze Zahlen
$\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z},\ q \in \mathbb{N},\ \frac{p}{q}$ ist gekürzter Bruch$\}$ rationale Zahlen
$\mathbb{R}$ = reelle Zahlen
$\mathbb{C}$ = komplexe Zahlen.

Definition 0.8. Die **leere Menge $\emptyset$** ist die Menge, die kein Element enthält.

Definition 0.9. Eine Menge N heißt **Teilmenge** der Menge M ($N \subset M$), wenn M alle Elemente aus N enthält.

Beispiel 0.10. • $\{1, 2\} \subset \mathbb{N}$
• die leere Menge $\emptyset$ ist Teilmenge jeder Menge.

Bemerkung 0.11. Anstelle von $N \subset M$ wird oft auch $N \subseteq M$ oder $N \subseteqq M$ geschrieben. Für uns sind diese drei Symbole vollkommen gleichwertig. Die Schreibweisen $N \subsetneq M$ oder auch $N \subsetneqq M$ oder auch $N \subsetneqq M$ bedeuten: N ist Teilmenge von M aber nicht gleich M.

Definition 0.12. Die Menge aller Teilmengen einer Menge M heißt **Potenzmenge** von M und wird mit $\mathcal{P}(M)$ bezeichnet.

Beispiele 0.13. • $M = \{0, 1\} \Longrightarrow \mathcal{P}(M) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
• ist M eine endliche Menge mit n Elementen, so ist $\mathcal{P}(M)$ eine endliche Menge mit 2^n Elementen. Dies folgt mit elementarer Kombinatorik: für jedes Element gibt es genau 2 Möglichkeiten: in der Teilmenge enthalten zu sein oder nicht.

Endlich viele (nicht notwendig endliche) Mengen werden üblicherweise durch Indizes durchnummeriert $M_1, \ldots, M_n$. Unendlich viele Mengen werden typischerweise in der Form $(M_i)_{i\in I}$ durchnummeriert, wobei I eine Menge ist, die man Ihrer Rolle wegen auch **Indexmenge** nennt. Man sagt, $(M_i)_{i\in I}$ ist eine durch I indizierte **Familie von Mengen**.

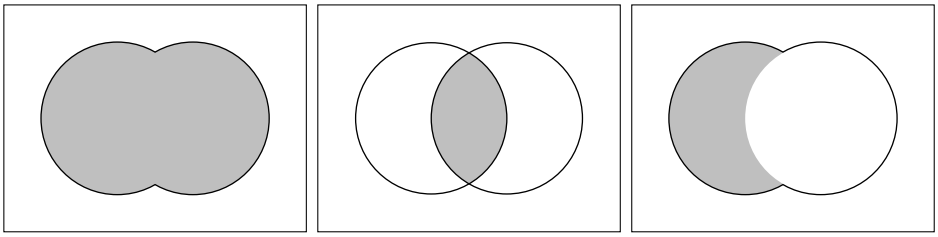
Definition 0.14. Seien K, L Teilmengen einer Menge M und $(M_i)_{i\in I}$ eine Familie von Teilmengen von M. Dann bildet man die folgenden Mengen

(i) $\bigcup\limits_{i\in I} M_i = \{m \in M \mid \text{ es gibt ein } i \in I \text{ mit } m \in M_i\}$ (Vereinigung)

(ii) $\bigcap\limits_{i\in I} M_i = \{m \in M \mid m \in M_i \text{ für alle } i \in I\}$ (Durchschnitt)

(iii) $K \smallsetminus L = \{m \in K \mid m \notin L\}$ (Komplement, auch $K - L$)

Beispiel 0.15. Vereinigung, Durchschnitt und Komplement zweier Kreisflächen.



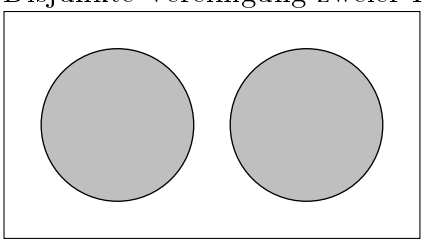
$M = \mathbb{N}$:
- $\{1, 2, 3\} - \{3, 4, 5\} = \{1, 2\}$
- $\{1, 2\} - \{1, 2, 3\} = \emptyset$

Definition 0.16. Sei $(M_i)_{i\in I}$ eine Familie von Teilmengen einer Menge M. Man sagt, M ist die **disjunkte Vereinigung** der M_i und schreibt

$$M = \dot{\bigcup_{i\in I}} M_i \quad \text{oder auch } M = \coprod_{i\in I} M_i,$$

wenn $M = \bigcup_{i\in I} M_i$ und $M_i \cap M_j = \emptyset$ für $i \neq j$ gilt.

Disjunkte Vereinigung zweier Kreisflächen:



Definition 0.17. (Produktmenge, kartesisches Produkt). Es seien $M_1, \ldots, M_n$ Mengen. Die **Produktmenge**

$$M_1 \times \cdots \times M_n$$

besteht aus allen n-Tupeln $(m_1, \ldots, m_n)$ mit $m_1 \in M_1, \ldots, m_n \in M_n$.

Beispiel 0.18. • $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ (die Punkte der reellen Ebene)
• $\mathbb{R} \times \emptyset = \emptyset$

Bemerkung 0.19. Definition 0.17 dehnt sich natürlich auf eine Familie $(M_i)_{i \in I}$ aus. Schreibweise $\prod_{i \in I} M_i$.

Definition 0.20. Eine **Abbildung** $f : M \to N$ einer Menge M in eine Menge N ist eine Vorschrift, die jedem Element $m \in M$ genau ein(!) Element $f(m) \in N$ zuordnet.

Beispiele 0.21. • $q : \mathbb{Z} \to \mathbb{Z}\ ,\ x \longmapsto x^2$
• Ist $M \subset N$ eine Teilmenge, so gibt es die **kanonische Inklusionsabbildung** $i : M \to N$, die gegeben ist durch:

m (aufgefasst als Element von M) $\longmapsto$ m (aufgefasst als Element von N)

z.B. $\{0, 1, 2\} \xrightarrow{i} \{0, 1, 2, 3\}$. Ist $M = N$, so ist dies die sogenannte **Identitätsabbildung** $\mathrm{id} : M \to M$, $m \mapsto m$.

Definition 0.22. Zwei Abbildungen $f, g : M \to N$ heißen **gleich**, wenn $f(m) = g(m)$ für alle $m \in M$ gilt.

Beispiel 0.23. Die Abbildungen $f, g : \mathbb{R} \to \mathbb{R}$
$f(x) = x^2 + 2x + 1,\ g(x) = (x + 1)^2$ sind gleich.

Definition 0.24. Sei $f : M \to N$ eine Mengenabbildung.

(i) Für $n \in N$ heißt die Teilmenge von M

$$f^{-1}(n) = \{m \in M \mid f(m) = n\}$$

die **Urbildmenge** von n. Die Menge der $n \in N$ mit $f^{-1}(n) \neq \emptyset$ heißt das **Bild** von f. Bezeichnung: $f(M)$ oder $\mathrm{Bild}(f)$.

(ii) f heißt **injektiv**, wenn gilt $m \neq m' \Rightarrow f(m) \neq f(m')$ (äquivalent: für jedes $n \in N$ enthält $f^{-1}(n)$ höchstens ein Element).

(iii) f heißt **surjektiv**, wenn zu jedem $n \in N$ ein $m \in M$ mit $f(m) = n$ existiert (äquivalent: $f^{-1}(n) \neq \emptyset$ für alle $n \in N$).

(iv) f heißt **bijektiv** falls es surjektiv und injektiv ist. (äquivalent: $f^{-1}(n)$ enthält für jedes $n \in N$ genau ein Element).

Ist $f : M \to N$ bijektiv, so definiert man die Umkehrabbildung $f^{-1} : N \to M$ durch die Regel:

$f^{-1}(n) =$ DAS Element der Menge $f^{-1}(n)$.

(Diese Bezeichnungsdoppelung bringt in der Praxis typischerweise keine Probleme mit sich.)

Bemerkung 0.25. Sei $f : M \to N$ eine Mengenabbildung. Die Eigenschaften injektiv, surjektiv und bijektiv signalisiert man durch Modifikation des Pfeils:

$f : M \hookrightarrow N$ (injektiv), $f : M \twoheadrightarrow N$ (surjektiv), $f : M \xrightarrow{\sim} N$ (bijektiv)

Definition 0.26. Eine **Relation** R auf einer Menge M ist eine Teilmenge $R \subset M \times M$.
Sprechweise: $x, y \in M$ gehen die Relation R ein, wenn $(x, y) \in R$.
Schreibweise $x \sim_R y$.

Beispiele 0.27. 1) $M = \mathbb{R},\ R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$
2) $M = \mathbb{Z},\ R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m - n \quad \text{ist gerade}\}$
3) $M =$ die Menge der Schüler einer Schule
$R = \{(x, y) \in M \times M \mid x$ und y gehen in die gleiche Klasse$\}$

Definition 0.28. Sei M eine Menge und R eine Relation auf M. R heißt **Äquivalenzrelation** wenn die folgenden Bedingungen erfüllt sind
(Ä1) Reflexivität: $x \sim_R x$ für alle $x \in M$
(Ä2) Symmetrie: $x \sim_R y \Longrightarrow y \sim_R x$ für alle $x, y \in M$
(Ä3) Transitivität: $(x \sim_R y$ und $y \sim_R z) \Longrightarrow x \sim_R z$ für alle $x, y, z \in M$.

Beispiele 0.29. -die Relation in Beispiel 0.27, 1) ist nicht reflexiv, nicht symmetrisch, aber transitiv
-die Relationen in Beispiel 0.27, 2) und 3) sind Äquivalenzrelationen.

Bemerkung 0.30. Auf jeder Menge existiert die (nutzlose) Äquivalenzrelationen „=", d.h. $R = \{(x, y) \in M \times M \mid x = y\}$.

Typischerweise existieren auf einer Menge verschiedene Äquivalenzrelationen. So kann man z.B. auf einer Menge von Bauklötzchen die Äquivalenzrelationen „gleiche Farbe", „gleiche Größe" oder „gleiche Form" einführen.

Definition 0.31. Sei M eine nichtleere Menge und R eine Äquivalenzrelation auf M. Eine nichtleere Teilmenge $A \subset M$ heißt **Äquivalenzklasse**, wenn sie den folgenden Bedingungen genügt:

(i) $a, b \in A \Longrightarrow a \sim_R b$
(ii) $(a \in A$ und $a \sim_R b) \Longrightarrow b \in A$.

Lemma 0.32. *Ist R eine Äquivalenzrelation auf einer Menge M, so gehört jedes Element $x \in M$ zu genau einer Äquivalenzklasse. Insbesondere gilt für zwei Äquivalenzklassen A, A', dass entweder $A = A'$ oder $A \cap A' = \emptyset$.*

Mit anderen Worten: M zerfällt in die disjunkte Vereinigung der Äquivalenzklassen bzgl. R.

Beweis. 1) Es gibt eine Äquivalenzklasse die x enthält. Definiere $A := \{a \in M \mid x \sim_R a\}$. Wegen $x \sim_R x$ (Ä1) gilt $x \in A$, also $A \neq \emptyset$. Es verbleibt, die Bedingungen (i) und (ii) aus Definition 0.31 zu verifizieren.

(i) Seien $a, b \in A$. Dann gilt $x \sim_R a$ und $x \sim_R b$. Aus (Ä2) folgt $a \sim_R x$ und (Ä3) liefert $a \sim_R b$.

(ii) Sei $a \in A$ und $a \sim_R b$. Zu zeigen: $b \in A$. Nach Definition gilt $x \sim_R a$. (Ä3) liefert $x \sim_R b$, also $b \in A$.

2) Zu zeigen: ($x \in A$ und $x \in A'$) $\Longrightarrow A = A'$.
Wir zeigen $A \subset A'$. Der Nachweis von $A' \subset A$ ist aus Symmetriegründen derselbe, und wir haben die Implikation: ($A \subset A'$) und ($A' \subset A$) $\Rightarrow A = A'$.
Sei nun $a \in A$. Dann gilt wegen $x \in A$:
$a \sim_R x$. Wegen $x \in A'$ folgt $a \in A'$, also $A \subset A'$. □

Definition 0.33. Die Menge der Äquivalenzklassen einer Menge M bzgl. einer Äquivalenzrelation R heißt **Faktormenge** und wird mit M/R bezeichnet.

Beispiele 0.34. • In Beispiel 0.27 2) gibt es zwei Äquivalenzklassen

$$A_{\text{gerade}} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

und

$$A_{\text{ungerade}} = \{\dots, -3, -1, 1, 3, \dots\}$$

• In Beispiel 0.27 3) ist die Menge der Äquivalenzklassen die Menge der Schulklassen der Schule.

Hintergrund: Der Übergang zu Äquivalenzklassen soll (für ein jeweils gegebenes Problem) nicht relevante Information abstreifen. So ist für die Erstellung eines Stundenplans nur die Menge der Schulklassen relevant, nicht die (größere) Menge der Schüler.

Beispiele 0.35. • (wie man $\mathbb{Z}$ aus $\mathbb{N}$ konstruiert).
Wir betrachten die Äquivalenzrelation $\sim$ auf $\mathbb{N} \times \mathbb{N}$

$$(m, n) \sim (m', n') \Longleftrightarrow m + n' = m' + n.$$

Dann gilt $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$
(identifiziere die Äquivalenzklasse des Paares (m, n) mit der ganzen Zahl $m - n$).

• Sei $n \in \mathbb{N}$ fest gewählt. Wir sagen, dass eine ganze Zahl $x \in \mathbb{Z}$ durch n teilbar ist (und schreiben $n \mid x$), wenn ein $y \in \mathbb{Z}$ mit $x = ny$ existiert. Wir betrachten die folgende Relation auf $\mathbb{Z}$:

$$a \sim b \Longleftrightarrow n \mid (a-b).$$

Dies ist eine Äquivalenzrelation, denn
(Ä1) $a - a = 0,\ n \mid 0$, also $a \sim a$.
(Ä2) $a \sim b \Longrightarrow n \mid (a-b) \Longrightarrow n|(b-a) \Longrightarrow b \sim a$.
(Ä3) ($a \sim b$ und $b \sim c$) $\Rightarrow n \mid (a-b)$ und $n|(b-c) \Rightarrow n \mid ((a-b)+(b-c)) = (a-c) \Rightarrow a \sim c$.

Es gibt genau n verschiedene Äquivalenzklassen, die mit $\overline{0}, \overline{1}, \ldots, \overline{(n-1)}$ bezeichnet werden. Die Menge der Äquivalenzklassen heißt die Menge der **Restklassen modulo n** und wird mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Man schreibt: $a \equiv b \bmod n$, wenn a und b in der gleichen Restklasse liegen.

Definition 0.36. Sei M eine Menge und R eine Äquivalenzrelation auf M. Dann ist die **kanonische Projektion**

$$p : M \to M/R$$

definiert durch:
$m \in M$ bildet sich auf die eindeutig bestimmte Klasse $A \in M/R$ mit $m \in A$ ab.

Bemerkung 0.37. Es gilt $p^{-1}(A) = A$. Da Äquivalenzklassen per definitionem nichtleer sind, ist die kanonische Projektion eine surjektive Mengenabbildung.

Beispiel 0.38. Die Klasse 12B bestehe aus den Schülern {Albert, Berta, ...}. Für den Mathematiker IST die Klasse 12B eine Menge, nämlich 12B = {Albert, Berta, ...}. Die kanonische Projektion

$$\begin{array}{ccc} p : M & \longrightarrow & M/R \\ \uparrow & & \uparrow \\ \text{Menge der Schüler} & & \text{Menge der Schulklassen} \\ \text{der Schule} & & \text{der Schule} \end{array}$$

ordnet jedem Schüler seine Klasse zu.

$$\begin{aligned} p^{-1}(12B) &= \text{die Menge der Schüler der Klasse 12B} \\ &= \{\text{Albert, Berta,} \ldots\} \\ &= 12B. \end{aligned}$$

Definition 0.39. (Kardinalität) Sei M eine endliche Menge. Die Anzahl der Elemente von M bezeichnet man mit $\#M$ oder auch mit $\mathrm{Kard}(M)$.

Beispiele 0.40. $\#\emptyset = 0$
$\#\{2,7,9\} = 3$

Lemma 0.41. *Sei $f : M \to N$ eine Abbildung endlicher Mengen*
(i) Ist f injektiv, so gilt $\#M \leq \#N$
(ii) ist f surjektiv, so gilt $\#M \geq \#N$
(iii) ist f bijektiv, so gilt $\#M = \#N$

Beweis. trivial □

Lemma 0.42. *Sei $f : M \to M$ eine Selbstabbildung einer endlichen Menge M. Dann sind die folgenden Aussagen äquivalent*

(i) f ist injektiv
(ii) f ist surjektiv
(iii) f ist bijektiv.

Beweis. (i) $\Rightarrow$ (iii) Sei f injektiv. Dann gilt für jedes $m \in M$: $\#f^{-1}(m) \leq 1$.
Nun zerfällt M in die disjunkte Vereinigung der Urbildmengen: $M = \dot{\bigcup}_{m \in M} f^{-1}(m)$.
Daher gilt

$$\#M = \sum_{m \in M} \#f^{-1}(m) \leq \sum_{m \in M} 1 = \#M.$$

Da Links und Rechts das Gleiche steht, gilt in der Mitte Gleichheit, d.h. $\#f^{-1}(m) = 1$ für alle $m \in M$. Daher f ist bijektiv.
(ii) $\Rightarrow$ (iii) analog, hier haben wir $\#f^{-1}(m) \geq 1$ für alle m.
(iii) $\Rightarrow$ (i) und (iii) $\Rightarrow$ (ii) sind trivial. □

Die Gesamtheit aller Abbildungen einer Menge M in eine Menge N ist wieder eine Menge und wird mit $\mathrm{Abb}(M,N)$ bezeichnet.

Definition 0.43. Seien M, N, K Mengen und $f : M \to N$, $g : N \to K$ Abbildungen. Die Abbildung

$$g \circ f : M \longrightarrow K,\ m \longmapsto g(f(m))$$

heißt die **Komposition** von f und g. Die Komposition kann man als Mengenabbildung auffassen

$$\begin{array}{rccc} \circ & : & \mathrm{Abb}(M,N) \times \mathrm{Abb}(N,K) & \longrightarrow & \mathrm{Abb}(M,K) \\ & & (f,g) & \longmapsto & g \circ f. \end{array}$$

Es seien I und M Mengen und $(M_i)_{i \in I}$ die Familie von (immer gleichen) Mengen $M_i = M$ indiziert über $i \in I$. Für das I-fache Selbstprodukt von M

$$\prod_{i \in I} M_i$$

benutzt man auch die Notationen $\prod_{i \in I} M$ und M^I.

Lemma 0.44. *Es existiert eine natürliche Bijektion*

$$\Phi: \quad \mathrm{Abb}(I, M) \xrightarrow{\sim} \prod_{i \in I} M.$$

Beweis. Die rechte Seite ist die Menge aller Tupel $(m_i)_{i \in I}$, $m_i \in M$. Die linke Seite ist die Menge der Abbildungen $f : I \to M$. Eine solche Abbildung f ist dadurch gegeben, dass man jedem $i \in I$ ein $m_i = f(i) \in M$ zuordnet. Wir definieren Φ durch die Zuordnung

$$f \in \mathrm{Abb}(I, M) \longmapsto (f(i))_{i \in I} \in \prod_{i \in I} M.$$

Da eine Abbildung f durch ihre Werte $f(i) \in M$, $i \in I$, eindeutig gegeben ist (vgl. Definition 0.22), ist Φ injektiv. Ist umgekehrt $(m_i)_{i \in I} \in \prod_{i \in I} M$ gegeben, so ist die Abbildung

$$f : I \longrightarrow M, \; i \longmapsto m_i \in M,$$

ein Urbild von $(m_i)_{i \in I}$ unter Φ. Daher ist Φ auch surjektiv. □

Kapitel 1

Gruppen, Ringe, Körper

1.1 Gruppen

Definition 1.1. Eine (binäre) **Verknüpfung** auf einer Menge M ist eine Abbildung

$$* : M \times M \to M,\ (m,n) \mapsto m * n.$$

Definition 1.2. Eine **Gruppe** $(G, *, e)$ ist eine Menge G mit einer Verknüpfung $*$ und einem ausgezeichneten Element $e \in G$, so dass

(G1) $g * (h * k) = (g * h) * k$ für alle $g, h, k \in G$ (Assoziativität)
(G2) $e * g = g$ für alle $g \in G$ (Existenz eines linksneutralen Elements)
(G3) für alle $g \in G$ existiert ein $h \in G$ mit $h * g = e$ (Existenz eines Linksinversen)

Eine Gruppe heißt **kommutativ** (oder abelsch), wenn zusätzlich gilt:

(G4) $g * h = h * g$ für alle $g, h \in G$.

Beispiele 1.3. 1) $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe.
2) $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ sind abelsche Gruppen.
3) $(\mathbb{Q} \setminus \{0\}, \bullet, 1)$ ist eine abelsche Gruppe.
4) $(\mathbb{R}_{>0}, \bullet, 1)$ ist eine abelsche Gruppe.
5) $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ ist eine abelsche Gruppe.

Wie ist die Summe von Restklassen definiert? Vorschrift: Seien $A, B \in \mathbb{Z}/n\mathbb{Z}$.
i) Wähle „Vertreter“ $a, b \in \mathbb{Z}$ von A, B, d.h. $a \in A$, $b \in B$.
ii) Bilde $a + b$ in $\mathbb{Z}$.
iii) $A + B \stackrel{df}{=} \overline{a+b}$, d.h. die Restklasse zu der $a + b$ gehört.

Damit diese Definition widerspruchsfrei ist (sprich: „$+$“ ist wohldefiniert), muss man nachweisen, dass das Ergebnis nicht von der Auswahl von a, b in Schritt i) abhängt. Das lassen wir als Übung.

6) Die **symmetrische Gruppe** $\mathfrak{S}_n$. Sei $n \in \mathbb{N}$ eine natürliche Zahl.

$\mathfrak{S}_n \stackrel{df}{=}$ die Menge aller bijektiven Abbildungen

$$\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$$

(sogenannte **Permutationen**).
$* = \circ$ Komposition (d.h. Hintereinanderausführung) von Abbildungen
$e = \mathrm{id}_{\{1,\ldots,n\}}$ die identische Abbildung.
Wir schreiben Permutationen in der Form

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

– oben stehen die Zahlen 1 bis n in der gewöhnlichen Reihenfolge.
– unten stehen die Zahlen 1 bis n in einer (evtl.) anderen Reihenfolge.

Umgekehrt definiert ein solches Diagramm eine Permutation. Wie viele gibt es? Elementare Kombinatorik:

n Möglichkeiten für die 1
$(n-1)$ Möglichkeiten für die 2
$\vdots$
1 Möglichkeit für n.

Daher gilt

$$\#\mathfrak{S}_n = n(n-1)\ldots 2 \cdot 1 = n! \ (n \text{ Fakultät}).$$

Jetzt verifizieren wir (G1) – (G3):

(G1) $g * (h * k) = g \circ (h \circ k) = (g \circ h) \circ k = (g * h) * k$.
(G2) $e * g = \mathrm{id} \circ g = g$.
(G3) ist g eine Permutation und h die inverse Abbildung g^{-1}, so gilt $h * g = g^{-1} \circ g = \mathrm{id} = e$.

Für $n \geq 3$ ist $\mathfrak{S}_n$ nicht kommutativ:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 2 & 1 & 3 & 4 & \ldots \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 1 & 3 & 2 & 4 & \ldots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 2 & 3 & 1 & 4 & \ldots \end{pmatrix}$$

aber

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 1 & 3 & 2 & 4 & \ldots \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 2 & 1 & 3 & 4 & \ldots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots \\ 3 & 1 & 2 & 4 & \ldots \end{pmatrix}$$

Satz 1.4. *Sei $G = (G, *, e)$ eine Gruppe. Dann gilt für alle $g, h, k \in G$:*

(1) Aus $g * h = g * k$ folgt $h = k$ (Linkskürzung).
(2) Aus $g * h = k * h$ folgt $g = k$ (Rechtskürzung).
(3) Es gilt $g * e = g$ (das (links)neutrale Element ist auch rechtsneutral).

(4) *Aus* $g*h=g$ *oder* $h*g=g$ *für ein* $g\in G$ *folgt* $h=e$.
(5) *Für alle* $g\in G$ *gibt es ein eindeutig bestimmtes* $g^{-1}\in G$ *mit* $g^{-1}*g=e=g*g^{-1}$.
(6) *Aus* $h*g=e$ *oder* $g*h=e$ *folgt* $h=g^{-1}$.
(7) *Es gilt* $(g^{-1})^{-1}=g$.

Beweis. (1): Sei $g*h=g*k$. Nach (G3) existiert ein $s\in G$ mit $s*g=e$. Daher gilt

$$s*(g*h)\overset{G1}{=}(s*g)*h=e*h\overset{G2}{=}h.$$

Analog:

$$s*(g*k)=(s*g)*k=e*k=k.$$

Somit folgt $h=k$.
(3): $e*g=g$ gilt nach (G2). Nach (G3) existiert ein $h\in G$ mit $h*g=e$. Daher gilt

$$h*(g*e)=(h*g)*e=e*e=e=h*g.$$

Nach (1) folgt $g*e=g$.
(5, Existenz): Nach (G3) existiert $h\in G$ mit $h*g=e$. Dann gilt

$$h*(g*h)=(h*g)*h=e*h=h\overset{(3)}{=}h*e$$

Nach (1) folgt $g*h=e$, d.h. h ist auch ein Rechtsinverses.
(2): Sei $g*k=h*k$. Sei $s\in G$ so dass $k*s=e$ (existiert nach (5)). Dann gilt

$$(g*k)*s=g*(k*s)=g*e\overset{(3)}{=}g.$$

Analog:

$$(h*k)*s=h*(k*s)=h*e=h.$$

Somit folgt $g=h$.
(4): $g*h=g\overset{(3)}{=}g*e\overset{(1)}{\Longrightarrow}h=e$, analog: $h*g=g=e*g\overset{(2)}{\Longrightarrow}h=e$.
(5, Eindeutigkeit) und (6): Seien $h,h'\in G$ mit $h*g=e=h'*g$. Mit (2) folgt $h=h'$. Daher ist g^{-1} ist eindeutig in G. Sei $h\in G$ mit $g*h=e$. Wegen $g*g^{-1}=e$ folgt mit (1) dass $h=g^{-1}$.
(7): aus $g*(g^{-1})=e$ folgt $g=(g^{-1})^{-1}$. □

Bemerkung 1.5. Für $g,h\in G$ gilt

$$(g*h)^{-1}=h^{-1}*g^{-1}.$$

Begründung: $(h^{-1}*g^{-1})*g*h=h^{-1}*e*h=e$.

1.2 Ringe

Definition 1.6. Ein **Ring** $R = (R, +, \cdot, 0_R)$ ist eine Menge R mit zwei Verknüpfungen $+, \cdot\colon R \times R \to R$ und einem ausgezeichneten Element $0_R \in R$ so dass gilt

(R1) $(R, +, 0_R)$ ist eine abelsche Gruppe.
(R2) (Assoziativität der Multiplikation) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$.
(R3) (Distributivität) $a(b + c) = ab + ac$, $(a + b)c = ac + bc$ für alle $a, b, c \in R$.

Ein **unitärer Ring** („Ring mit 1“) ist ein Tupel $R = (R, +, \cdot, 0_R, 1_R)$, so dass $(R, +, \cdot, 0_R)$ ein Ring ist und $1_R \in R$ ist ein Element für das gilt:

(R4) $1_R \cdot a = a = a \cdot 1_R$ für alle $a \in R$.

Ein Ring heißt **kommutativ**, wenn die Multiplikation kommutativ ist, also wenn

(R5) $a \cdot b = b \cdot a$ für alle $a, b \in R$ gilt.

Bemerkung 1.7. Das inverse Element von $a \in R$ bzgl. der Addition bezeichnet man mit $-a$. Ein Inverses bzgl. der Multiplikation existiert i.A. nicht. Die Eins in einem unitären Ring ist eindeutig bestimmt: Sind 1_R und $1'_R$ zwei Einselemente, so folgt $1_R = 1_R \cdot 1'_R = 1'_R$.

Beispiele 1.8. 1) $(\mathbb{Z}, +, \cdot, 0, 1)$ ist ein kommutativer Ring mit 1
2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ analog.
3) $\mathbb{Z}/n\mathbb{Z}$ ist ein kommutativer Ring mit 1. Multiplikationsvorschrift für $A \cdot B$.

(i) Wähle Repräsentanten $a \in A$, $b \in B$.
(ii) Bilde $a \cdot b$ in $\mathbb{Z}$.
(iii) $A \cdot B :=$ Klasse von $a \cdot b$.

Wie bei der Addition muss nachgewiesen werden, dass das Ergebnis unabhängig von der Auswahl in (i) ist. Wir lassen das als Übung.

4) Die Menge der geraden ganzen Zahlen ist ein kommutativer Ring ohne 1.

Lemma 1.9. *In einem Ring $R = (R, +, \cdot, 0_R)$ gelten die folgenden Aussagen*

(i) $0_R \cdot a = 0_R = a \cdot 0_R$ für alle $a \in R$
(ii) $a(-b) = -ab = (-a) \cdot b$ für alle $a, b \in R$.

Ist R unitär, so gilt

(iii) $-b = (-1_R)b$.

Beweis. (i) $0_R \cdot a + 0_R = 0_R \cdot a = (0_R + 0_R) \cdot a = 0_R a + 0_R a$. Nach Kürzen folgt $0_R = 0_R \cdot a$. Analoger Beweis für $a \cdot 0_R = 0_R$.
(ii) $0_R = a \cdot 0_R = a(b + (-b)) = ab + a(-b)$ also $-ab = a(-b)$. Die andere Aussage beweist man analog.
Ist R unitär, so setzt man in (ii) $a = 1_R$, und erhält (iii). □

Beispiel 1.10. $R = \{0\}$ mit den einzig möglichen Verknüpfungen $+$ und $\cdot$ heißt der **Nullring**. Der Nullring ist ein kommutativer Ring mit 1. (Es gilt $0_R = 0 = 1_R$). Dies ist der einzige Ring mit 1 in dem $1_R = 0_R$ gilt.
Grund: Gilt $0_R = 1_R$, so gilt für jedes $r \in R$: $r = 1_R r = 0_R r = 0_R$, d.h. R besteht aus genau einem Element.

Lemma 1.11. *Es sei $R = (R, +, \cdot, 0_R, 1_R)$ ein Ring mit 1 und $R^\times \subset R$ die Menge aller Elemente in R die sowohl ein Links- als auch ein Rechtsinverses bzgl. Multiplikation haben, d.h.*

$$R^\times = \{r \in R \mid \exists s, t \in R : sr = 1_R = rt\}.$$

Dann ist $\{R^\times, \cdot, 1_R\}$ eine Gruppe. Man nennt $R^\times$ die **Einheitengruppe** *von R.*

Beweis. Wir müssen zunächst zeigen, dass die Multiplikation nicht aus $R^\times$ hinausführt. Seien also $r, r' \in R^\times$ und s, s', t, t' mit $sr = 1 = rt$, $s'r' = 1 = r't'$. Dann gilt

$$(s's)(rr') = s'(sr)r' = s'1r' = s'r' = 1 \quad \text{und}$$
$$(rr')(t't) = r(r't')t = r1t = rt = 1.$$

Daher gilt $rr' \in R^\times$. Wir weisen nun die Gruppenaxiome (G1)–(G3) nach. G1, also die Assoziativität der Multiplikation, folgt aus den Axiomen für Ringe (R2). $1 \in R^\times$ ist ein neutrales Element, also gilt G2. Bleibt zu zeigen, dass für $r \in R^\times$ ein $r' \in R^\times$ mit $r'r = 1$ existiert. Nach Definition existiert ein $s \in R$ mit $sr = 1$ und wir müssen einsehen, dass $s \in R^\times$ gilt. s hat offensichtlich ein Rechtsinverses, nämlich r. Aber r ist auch linksinvers zu s. Dies sieht man so. Wähle $t \in R$ mit $rt = 1$. Dann gilt:

$$s = s(rt) = (sr)t = t.$$

Hieraus folgt: $rs = rt = 1$. □

Bemerkung 1.12. Angenommen es gilt $0_R \in R^\times$. Dann existiert ein $r \in R$ mit $0_R r = 1_R$ und es folgt $0_R = 0_R r = 1_R$, d.h. R ist der Nullring.

Wir werden es zunächst nur mit kommutativen Ringen zu tun haben. Besonders einfache Ringe sind Körper (siehe nächster Abschnitt).

1.3 Körper

Definition 1.13. Ein **Körper** K ist ein kommutativer unitärer Ring $(K, +, \cdot, 0_K, 1_K)$, in dem gilt

$$K^\times = K \smallsetminus \{0_K\}.$$

In Worten: K ist nicht der Nullring (sonst wäre $0_K \in K^\times$) und jedes von Null verschiedene Element besitzt ein Inverses bzgl. Multiplikation.

Beispiele 1.14. 1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ mit den üblichen Operationen sind Körper.
2) $\mathbb{Z}$ ist kein Körper (nur 1 und -1 haben ein Inverses).

Lemma 1.15. *In einem Körper K gilt*

$$a \cdot b = 0_K \Longrightarrow (a = 0_K \text{ oder } b = 0_K)$$

Beweis. Angenommen $a \neq 0_K$. Dann existiert ein $a^{-1} \in K$ mit $a^{-1}a = 1_K$. Es folgt $b = 1_K \cdot b = a^{-1}ab = a^{-1}0_K = 0_K$. □

Lemma 1.16. *Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.*

Beweis. $\mathbb{Z}/p\mathbb{Z}$ ist ein kommutativer Ring mit 1. Es genügt zu zeigen, dass jede von 0 verschiedene Restklasse ein Inverses bzgl. Multiplikation besitzt. In anderen Worten ist zu zeigen:

Für jedes $A \in \mathbb{Z}/p\mathbb{Z}$, $A \neq \overline{0}$, ist die $\overline{1}$ im Bild der Abbildung:

$$A\cdot\ : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \quad B \mapsto AB.$$

Wir zeigen sogar, dass $A\cdot$ surjektiv ist. Da $\mathbb{Z}/p\mathbb{Z}$ endlich ist, genügt es nach 0.42 zu zeigen, dass $A\cdot$ injektiv ist.
Angenommen es gäbe Restklassen $B, C \in \mathbb{Z}/p\mathbb{Z}$ mit $AB = AC$. Zu zeigen: $B = C$. Seien $a, b, c \in \mathbb{Z}$ Vertreter von A, B und C. Wegen $A \neq 0$ gilt $p \nmid a$. Wegen $AB = AC$ gilt $ab \equiv ac \bmod p \Rightarrow a(b-c) \equiv 0 \bmod p \Rightarrow p \mid a(b-c)$.
Weil p Primzahl ist und $p \nmid a$ folgt $p \mid (b-c)$, also $b \equiv c \bmod p$ also $B = C$. Also ist die Abbildung: $\cdot A : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ injektiv, also surjektiv, insbesondere liegt $\overline{1}$ im Bild. □

Bemerkung 1.17. Ist $n \in \mathbb{N}$ keine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ *kein* Körper.

Beweis. Für $n = 1$ ist $\mathbb{Z}/n\mathbb{Z}$ der Nullring. Nun sei $n > 1$ und keine Primzahl. Dann existieren $a, b \in \mathbb{N}$ mit $1 < a, b < n$ und $ab = n$. Für die Restklassen bedeutet dies $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ aber $\bar{a}\bar{b} = \overline{ab} = \bar{n} = \bar{0}$. Dies steht im Widerspruch zu Lemma 1.15. Also ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper. □

Wie man am Beispiel $\mathbb{Z}/p\mathbb{Z}$ sieht, kann es in einem Körper passieren, dass $\underbrace{1_K + \cdots + 1_K}_{p\text{-mal}} = 0_K$ gilt.

Definition 1.18. Sei K ein Körper. Die kleinste natürliche Zahl n mit

$$\underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} = 0_K \text{ (in } K)$$

heißt die **Charakteristik** von K. Notation $\mathrm{char}(K)$. Gibt es eine solche Zahl nicht, setzt man $\mathrm{char}(K) = 0$.

Bemerkungen 1.19. 1) Es gilt $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) \geq 2$ (wegen $1_K \neq 0_K$).
2) die Körper $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben die Charakteristik 0
3) $\mathbb{Z}/p\mathbb{Z}$ hat die Charakteristik p.

Satz 1.20. *Die Charakteristik eines Körpers ist entweder gleich* 0 *oder eine Primzahl.*

Beweis. Sei $\mathrm{char}(K) \neq 0$, also $\mathrm{char}(K) = n \geq 2$. Wäre n keine Primzahl, so gäbe es $a, b \in \mathbb{N}$, $1 < a, b < n$ mit $ab = n$. Dann gilt

$$\underbrace{(1_K + \cdots + 1_K)}_{a\text{-mal}} \cdot \underbrace{(1_K + \cdots + 1_K)}_{b\text{-mal}} = \underbrace{(1_K + \cdots + 1_K)}_{n\text{-mal}} = 0.$$

Nach Lemma 1.15 folgt $\underbrace{(1_K + \cdots + 1_K)}_{a\text{-mal}} = 0_K$ oder $\underbrace{(1_K + \cdots + 1_K)}_{b\text{-mal}} = 0_K$. Dies widerspricht der Minimalität von n. □

Für uns wird (außer recht spät) die Charakteristik keine Rolle spielen. Solange es keine Arbeit macht, werden wir jede Annahme an die Charakteristik vermeiden.

1.4 Homomorphismen

Homomorphismen = Strukturerhaltende Abbildungen.

Definition 1.21. Seien $(G, *_G, e_G)$ und $(H, *_H, e_H)$ Gruppen. Eine Abbildung $f : G \to H$ heißt **Gruppenhomomorphismus**, wenn für alle $g, g' \in G$ gilt

$$f(g *_G g') = f(g) *_H f(g').$$

Sind $(R, +_R, \cdot_R, 0_R)$ und $(S, +_S, \cdot_S, 0_S)$ Ringe, so heißt eine Abbildung $f : R \to S$ **Ringhomomorphismus**, wenn für alle $a, b \in R$ gilt

$$f(a +_R b) = f(a) +_S f(b),\ \ f(a \cdot_R b) = f(a) \cdot_S f(b).$$

Ein Ringhomomorphismus $f : R \to S$ von Ringen mit 1 $(R, +_R, \cdot_R, 0_R, 1_R)$ und $(S, +_S, \cdot_S, 0_S, 1_S)$ heißt **unitär** (oder Homomorphismus von Ringen mit 1), wenn zusätzlich gilt: $f(1_R) = 1_S$.
Eine Abbildung von Körpern heißt **Körperhomomorphismus**, wenn sie ein unitärer Ringhomomorphismus ist.

Definition 1.22. Ein Gruppen-(Ring-, Körper-)homomorphismus heißt Gruppen-(Ring-, Körper-) **Isomorphismus**, wenn er **bijektiv** ist. Zwei Gruppen (Ringe, Körper) heißen **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt.

Bemerkung 1.23. Die inverse Abbildung f^{-1} zu einem Gruppen- (Ring-, Körper-) Isomorphismus ist wieder ein Gruppen-(Ring-, Körper-)Isomorphismus (!).

Lemma 1.24. *Sei $f : (G, *_G, e_G) \to (H, *_H, e_H)$ ein Gruppenhomomorphismus. Dann gilt*

(i) $f(e_G) = e_H$,
(ii) $f(g^{-1}) = f(g)^{-1}$ *für alle* $g \in G$.

Beweis. (i) Es gilt $e_G *_G e_G = e_G$, also

$$f(e_G) *_H f(e_G) = f(e_G *_G e_G) = f(e_G) = f(e_G) *_H e_H.$$

Kürzen ergibt $f(e_G) = e_H$.
(ii) $e_H \overset{(i)}{=} f(e_G) = f(g * g^{-1}) = f(g) \cdot f(g^{-1})$. Daher gilt $f(g)^{-1} = f(g^{-1})$. □

Beispiele 1.25.

- Ist $(G, *, e)$ eine Gruppe, so ist die Identität $\mathrm{id} : G \to G$ ein Gruppenisomorphismus.
- Sind $(G, *_G, e_G)$, $(H, *_H, e_H)$ Gruppen, so ist der **triviale** Homomorphismus $f : G \to H$, $f(g) = e_H$ für alle $g \in G$, ein Gruppenhomomorphismus.
- Sei $n \in \mathbb{N}$. Die Restklassenabbildung (kanonische Projektion)

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad a \longmapsto \overline{a},$$

  ist ein surjektiver, unitärer Ringhomomorphismus.
- Die Inklusionen $\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Körperhomomorphismen.
- Die Exponentialabbildung

$$\begin{array}{ccc} (\mathbb{R}, +, 0) & \longrightarrow & (\mathbb{R}_{>0}, \cdot, 1) \\ t & \longmapsto & e^t \end{array}$$

  ist ein Gruppenisomorphismus.
- Sei $n \in \mathbb{N}$. Die Abbildung

$$\begin{array}{c} \mathfrak{S}_n \longrightarrow \mathfrak{S}_{n+1} \\ \begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix} \longmapsto \begin{pmatrix} 1 & \dots & n, & n+1 \\ \pi(1) & \dots & \pi(n), & n+1 \end{pmatrix} \end{array}$$

  ist ein injektiver Gruppenhomomorphismus.

Definition 1.26. Eine Teilmenge H einer Grupppe $G = (G, *, e)$ heißt **Untergruppe**, wenn sie mit der von G geerbten Struktur eine Gruppe ist, d.h.

(i) $e \in H$
(ii) $h, h' \in H \Rightarrow h * h' \in H$
(iii) $h \in H \Rightarrow h^{-1} \in H$.

Bemerkung. Ist $H \neq \varnothing$, so folgt (i) schon aus (ii) und (iii).

Lemma 1.27. *Sei H eine Untergruppe von G. Die Relation*

$$g \sim_H g' \Longleftrightarrow g^{-1} * g' \in H$$

ist eine Äquivalenzrelation auf G.

Beweis. Reflexivität: $g \sim_H g$ weil $g^{-1} * g = e \in H$.
Symmetrie: $g \sim_H g' \Rightarrow g^{-1} * (g') \in H \Rightarrow (g')^{-1} * g = (g^{-1} * g')^{-1} \in H \Rightarrow g' \sim_H g$.
Transitivität: $g \sim g'$ und $g' \sim g'' \Rightarrow g^{-1} * g'' = g^{-1} * g' * (g')^{-1} * g'' \in H \Rightarrow g \sim_H g''$. □

Bemerkung 1.28. Die Äquivalenzklasse eines Elements $g \in G$ besteht aus allen $g' \in G$ der Form $g * h$ mit $h \in H$. Bezeichnung: gH. Die Menge aller Äquivalenzklassen wird mit G/H bezeichnet (die **Linksnebenklassen** zu H).

Definition 1.29. Sei $f : G \to H$ ein Gruppenhomomorphismus. Der **Kern** von f ist die Teilmenge

$$\mathrm{Kern}(f) = \{g \in G \mid f(g) = e_H\}.$$

Im Englischen heißen Kern und Bild *kernel* und *image*. Man verwendet oft auch die englischen Bezeichnungen $\ker(f)$ und $\mathrm{im}(f)$.

Lemma 1.30. *Sei $f : G \to H$ ein Gruppenhomomorphismus.*

(i) $\mathrm{Kern}(f)$ *ist eine Untergruppe von G.*
(ii) $\mathrm{Bild}(f)$ *ist eine Untergruppe von H.*
(iii) *f ist injektiv* $\Longleftrightarrow \mathrm{Kern}(f) = \{e_G\}$.
(iv) *f ist surjektiv* $\Longleftrightarrow \mathrm{Bild}(f) = H$.

Beweis. (i) $f(e_G) = e_H \Rightarrow e_G \in \mathrm{Kern}(f)$.
$g, g' \in \mathrm{Kern}(f) \Rightarrow f(g * g') = f(g) * f(g') = e_H$ also $g * g' \in \mathrm{Kern}(f)$.
Aus 1.24 (ii) folgt für $g \in \mathrm{Kern}(f)$, dass $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$, also $g^{-1} \in \mathrm{Kern}(f)$.

(ii) $f(e_G) = e_H \Rightarrow e_H \in \mathrm{Bild}(f)$.
Seien $h, h' \in \mathrm{Bild}(f)$ und $g, g' \in G$ mit $f(g) = h$, $f(g') = h'$. Dann gilt $f(g * g') = f(g) * f(g') = h * h'$, also $h * h' \in \mathrm{Bild}(f)$.
Ist $h = f(g) \in \mathrm{Bild}(f)$, so gilt $h^{-1} = f(g^{-1}) \in \mathrm{Bild}(f)$.

(iii) ($\Longrightarrow$) Sei f injektiv. Für $g \in \mathrm{Kern}(f)$ gilt $f(e_G) = e_H = f(g) \Rightarrow g = e_G$, also $g = e_G$, d.h. $\mathrm{Kern}(f) = \{e_G\}$
($\Longleftarrow$) Sei nun $\mathrm{Kern}(f) = \{e_G\}$ und $g, g' \in G$ mit $f(g) = f(g')$. Dann gilt

$$f(g * (g')^{-1}) = f(g) * f(g')^{-1} = e_H,$$

also $g * (g')^{-1} \in \mathrm{Kern}(f) = \{e_G\}$. Es folgt $g = g'$.

(iv) ist trivial. □

Bemerkung 1.31. Jeder Gruppenhomomorphismus $f : G \to H$ induziert einen surjektiven Gruppenhomomorphismus $F : G \twoheadrightarrow \text{Bild}(f)$ durch $F(g) = f(g) \in \text{Bild}(f)$.

Notation: Von jetzt an lassen wir das $*$-Zeichen weg und schreiben gh für $g * h$ („Juxtaposition“).

Lemma 1.32. *Sei G eine* kommutative *Gruppe und $H \subset G$ eine Untergruppe.*

(i) *die Menge G/H der Linksnebenklassen zu H wird durch die Verknüpfung*

$$(gH)(g'H) = (gg')H$$

zu einer kommutativen Gruppe.

(ii) *Die kanonische Projektion $p : G \to G/H$ ist ein surjektiver Gruppenhomomorphismus und es gilt*

$$\text{Kern}(p) = H.$$

Bemerkung 1.33. G/H heißt die **Faktorgruppe** von G nach H.

Beweis. (i) Wir müssen nachweisen, dass die Verknüpfung wohldefiniert ist, d.h. gilt $g_1H = g_2H$ und $g_1'H = g_2'H$, so folgt $(g_1g_1') = (g_2g_2')H$.
Wir wissen: $g_1^{-1}g_2 \in H$ und $(g_1')^{-1}g_2' \in H$. Es ist H Untergruppe in G und G ist kommutativ. Also gilt

$$\begin{aligned}(g_1g_1')^{-1}(g_2g_2') &= ((g_1')^{-1}g_1^{-1})(g_2g_2') \\ &= ((g_1')^{-1}g_2')(g_1^{-1}g_2) \in H.\end{aligned}$$

Die Gültigkeit der Gruppenaxiome wird von G geerbt, z.B. gilt $e_{G/H} = e_GH$.

(ii) Die kanonische Projektion ist surjektiv nach 0.37. Dass p ein Homomorphismus ist, folgt direkt aus der Definition der Verknüpfung auf G/H. Schließlich gilt

$$\begin{aligned}\text{Kern}(p) &= \{g \in G \mid p(g) = e_{G/H}\} \\ &= \{g \in G \mid g \sim_H e_G\} \\ &= \{g \in G \mid e_G^{-1}g \in H\} = \{g \in G \mid g \in H\} = H.\end{aligned}$$

□

Bemerkung 1.34. Ist G nicht kommutativ, so ist die Verknüpfung auf G/H nur unter bestimmten Bedingungen an H wohldefiniert.

Definition 1.35. Sei $(R, +_R, 0_R, \cdot_R)$ ein Ring und $S \subset R$ eine Teilmenge. S heißt **Unterring** (oder **Teilring**), wenn S mit den von R geerbten Strukturen ein Ring ist, d.h.
• $0_R \in S$ und $(S, +_R, 0_R)$ ist eine Untergruppe von $(R, +_R, 0_R)$, d.h. $(s_1, s_2 \in S \Rightarrow s_1 + s_2 \in S$ und $s \in S \Rightarrow -s \in S)$
• mit $s_1, s_2 \in S$ liegt $s_1 \cdot s_2$ in S.
Ist R unitär, so heißt S **unitärer Unterring** von R wenn S ein Unterring ist, unitär ist, und es gilt $1_S = 1_R$.

Beispiele 1.36. • $\mathbb{Z}$ ist ein unitärer Unterring von $\mathbb{Q}$.
• $2\mathbb{Z} = \{a \in \mathbb{Z} \mid a \text{ ist gerade}\}$ ist ein (nicht-unitärer) Unterring in $\mathbb{Z}$
• $\mathbb{R} \times \mathbb{R}$ mit komponentenweiser Addition und Multiplikation ist ein unitärer Ring. $\mathbb{R} \times \{0\} \subset \mathbb{R} \times \mathbb{R}$ ist ein Unterring, ist unitär, aber kein unitärer Unterring weil: $1_{\mathbb{R}\times\mathbb{R}} = (1,1)$, aber $1_{\mathbb{R}\times\{0\}} = (1,0)$.

Definition 1.37. Ein **Unterkörper** eines Körpers ist ein unitärer Unterring, der selbst Körper ist.

Beispiel 1.38. $\mathbb{Q}$ ist Unterkörper von $\mathbb{R}$ und $\mathbb{C}$ und $\mathbb{R}$ ist Unterkörper von $\mathbb{C}$.

Lemma 1.39. *Ist*

$$f : (R, +_R, 0_R, \cdot_R) \longrightarrow (S, +_S, 0_S, \cdot_S)$$

ein Ringhomomorphismus, so gilt

$$f(0_R) = 0_S,\ f(-a) = -f(a),\ a \in R.$$

Beweis. Der Ringhomomorphismus f induziert einen Homomorphismus der „unterliegenden“ Gruppen $f : (R, +_R, 0_R) \to (S, +_S, 0_S)$. Das Ergebnis folgt aus 1.24. □

Bemerkung 1.40. • Kern(f) ist ein Unterring in R, der i.A. nicht unitär ist, auch wenn R unitär ist.
• Bild(f) ist ein Unterring in S. Sind R und S unitär, und f ein unitärer Ringhomomorphismus, so ist Bild(f) ein unitärer Teilring.

Lemma 1.41. *Sei $f : (R, +_R, 0_R, \cdot_R, 1_R) \longrightarrow (S, +_S, 0_S, \cdot_S, 1_S)$ ein unitärer Ringhomomorphismus. Dann gilt $f(R^\times) \subset S^\times$ und die induzierte Abbildung*

$$(R^\times, \cdot, 1_R) \longrightarrow (S^\times, \cdot, 1_S)$$

zwischen den Einheitengruppen ist ein Gruppenhomomorphismus.

Beweis. Sei $r \in R^\times$ und $s \in R^\times$ sein (Rechts-, wie Links-) Inverses. Dann gilt

$$f(s)f(r) = f(sr) = f(1_R) = 1_S, \quad \text{und}$$

$$f(r)f(s) = f(rs) = f(1_R) = 1_S.$$

Also gilt $f(r) \in S^\times$. Die induzierte Abbildung $R^\times \to S^\times$ ist ein Gruppenhomomorphismus, weil f ein Ringhomomorphismus ist. □

Satz 1.42. *Seien $K = (K, +_K, \cdot_K, 0_K, 1_K)$ und $L = (L, +_L, \cdot_L, 0_L, 1_L)$ Körper und $f : K \to L$ ein Körperhomomorphismus. Dann gilt*

(i) *f ist injektiv,*

(ii) $char(K) = char(L)$,

(iii) $\mathrm{Bild}(f)$ *ist ein Unterkörper von* L.

Beweis. (i) Nach 1.30 genügt es zu zeigen, dass $\mathrm{Kern}(f) = \{0_K\}$ gilt. Sei $a \in \mathrm{Kern}(f)$, $a \neq 0$. Dann existiert $a^{-1} \in K$ und es gilt

$$1_L = f(1_K) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) = 0_L \cdot f(a^{-1}) = 0_L.$$

Wegen $1_L \neq 0_L$ ist dies ein Widerspruch, weshalb ein solches a nicht existiert. Es folgt $\mathrm{Kern}(f) = \{0_K\}$.
(ii) Aus (i) folgt

$$\underbrace{1_K + \cdots + 1_K}_{n\text{-mal}} = 0_K \iff f(1_K) + \cdots + f(1_K) = 0_L$$
$$\iff \underbrace{1_L + \cdots + 1_L}_{n\text{-mal}} = 0_L.$$

Direkt nach der Definition der Charakteristik folgt $\mathrm{char}(K) = \mathrm{char}(L)$.
(iii) $\mathrm{Bild}(f)$ ist ein unitärer Teilring von L. Zu zeigen: ist $y \in \mathrm{Bild}(f)$, $y \neq 0_L$, so gilt $y^{-1} \in \mathrm{Bild}(f)$. Sei nun $y = f(x)$. Wegen $f(0_K) = 0_L$ gilt $x \neq 0_K$, also $x \in K^\times$. Nach 1.41 ist $f : K^\times \to L^\times$ ein Gruppenhomomorphismus. Nach 1.24 (ii) folgt $f(x^{-1}) = f(x)^{-1} = y^{-1}$, also $y^{-1} \in \mathrm{Bild}(f)$. □

Bemerkung 1.43. Die induzierte Abbildung $F : K \to f(K), x \mapsto f(x) \in f(K)$, ist also ein Körperisomorphismus und man identifiziert K mit $f(K)$.
Sprechweise: Der Körper K ist über f in L eingebettet. I.A. kann es mehrere Einbettungen von K nach L geben (!)

Sind $f : G_1 \to G_2$ und $g : G_2 \to G_3$ Grupppenhomomorphismen, so auch die Verknüpfung

$$g \circ f : G_1 \longrightarrow G_3.$$

Gleiches gilt für Ring- und Körperhomomorphismen.

Definition 1.44. Sei G eine Gruppe. Ein Gruppenhomomorphismus $f : G \to G$ heißt **Gruppenendomorphismus**. Ist f bijektiv, so heißt f **Gruppenautomorphismus**.
Die analoge Sprechweise benutzt man für Ringe und Körper.
Bezeichnung: $\mathrm{End}(G)$, $\mathrm{End}(R)$, $\mathrm{End}(K)$ bzw. $\mathrm{Aut}(G)$, $\mathrm{Aut}(R)$, $\mathrm{Aut}(K)$.

Lemma 1.45. *Sei G eine Gruppe (R ein Ring, K ein Körper). Dann ist* $\mathrm{Aut}(G)$ $(\mathrm{Aut}(R), \mathrm{Aut}(K))$ *mit der Verknüpfung*

$$\begin{array}{ccc} \mathrm{Aut}(G) \times \mathrm{Aut}(G) & \longrightarrow & \mathrm{Aut}(G) \\ (f, g) & \longmapsto & g \circ f \end{array}$$

(analog für $\mathrm{Aut}(R)$, $\mathrm{Aut}(K)$*) eine Gruppe.*

Beweis. Wohldefiniertheit: Mit f und g ist auch $g \circ f$ bijektiv.
- Assoziativität: $h \circ (g \circ f) = h \circ g \circ f = (h \circ g) \circ f$
- neutrales Element: id_G
- Inverses. Mit f ist auch f^{-1} ein Gruppenautomorphismus und es gilt

$$f \circ f^{-1} = \mathrm{id}_G \,.$$

□

Bemerkung 1.46. Ist $R = (R, +_R, \cdot_R, 0_R)$ ein Ring, so muss man zwischen den Gruppen $\mathrm{Aut}(R, +_R, \cdot_R, 0_R)$ (Ringautomorphismen) und $\mathrm{Aut}(R, +_R, 0_R)$ (Gruppenautomorphismen) unterscheiden. Die erste Gruppe ist eine Untergruppe der zweiten.

Kapitel 2

Vektorräume

2.1 Klassische Vektorrechnung

Die Erfordernisse der Analysis führen zur Erweiterung von $\mathbb{Q}$ zu den reellen Zahlen $\mathbb{R}$.

Veranschaulichung: reelle Zahl $\hat{=}$ Punkt auf der Zahlengeraden.
Nach Festlegung eines Koordinatenkreuzes ($\hat{=}$ 0-Punkt und zwei zueinander senkrechter „Einheitsvektoren“ können wir jeden Punkt der Ebene als Paar reeller Zahlen schreiben. Entsprechend: Punkte des Raumes $\hat{=}$ Tripeln reeller Zahlen

Allgemeiner: Sei $n \in \mathbb{N}$

Definition 2.1. Ein n-Tupel $(x_1, \ldots, x_n)$ reeller Zahlen heißt **Punkt oder Vektor des n-dimensionalen Raumes.** Die Zahlen $x_1, \ldots, x_n$ heißen die **Komponenten** des Vektors $(x_1, \ldots, x_n)$. Die Gesamtheit solcher n-Tupel wird mit $\mathbb{R}^n$ bezeichnet. Es heißt $0_{\mathbb{R}^n} := (0, \ldots, 0)$ der **Nullvektor**.

In der Schulmathematik ist stets $n = 2$ oder 3 und die Terminologie verschieden. Dort versteht man unter einem Vektor eine Äquivalenzklasse von Pfeilen $\overrightarrow{AB}$ (in der Ebene oder im Raum) bezüglich der Äquivalenzrelation „gleiche Richtung und gleiche Länge“. Jede Äquivalenzklasse hat einen kanonischen Vertreter, nämlich den mit $A = 0_{\mathbb{R}^n}$. Wir identifizieren hier den Vektor einfach mit der Pfeilspitze $B = (x_1, \ldots, x_n)$ seines eindeutig bestimmten Vertreters der Form $\overrightarrow{0_{\mathbb{R}^n}B}$. Das heißt, bei uns gibt es nur noch die sogenannten „Ortsvektoren“, also solche, deren Anfangspunkt der Koordinatenursprung ist. Diese werden stets mit ihrer Pfeilspitze, also einem Punkt gleichgesetzt. Punkte und Vektoren sind also für uns Synonyme. Je nach Situation werden wir den einen oder den anderen Standpunkt bevorzugen. Wenn wir z.B. über den Abstand zwischen Vektoren sprechen, denken wir an Punkte, reden wir über den Winkel zwischen Vektoren, denken wir an Pfeile.
Was kann man mit Vektoren machen?

I: Vektoraddition
$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$

II: Skalarmultiplikation
$\alpha \in \mathbb{R}$ (ein sogenannter „Skalar“)
$x = (x_1, \ldots, x_n) \in \mathbb{R}^n$
$\alpha \cdot x = (\alpha x_1, \ldots, \alpha x_n)$

III: Skalarprodukt
$x = (x_1, \ldots, x_n) \in \mathbb{R}^n$
$y = (y_1, \ldots, y_n) \in \mathbb{R}^n$
$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n \in \mathbb{R}$
heißt das (Standard-)Skalarprodukt von x und y.

Besonderheit für $n = 3$

IV: Vektorprodukt (oder Kreuzprodukt)
$x = (x_1, x_2, x_3) \in \mathbb{R}^3$, $y = (y_1, y_2, y_3) \in \mathbb{R}^3$
$x \times y = (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1) \in \mathbb{R}^3$

Elementare Eigenschaften:

(V1) $(x + y) + z = x + (y + z)$ für alle $x, y, z \in \mathbb{R}^n$ (Assoziativität)

(V2) $0_{\mathbb{R}^n} + x = x$ für alle $x \in \mathbb{R}^n$ (neutrales Element)

(V3) $x + y = y + x$ für alle $x, y \in \mathbb{R}^n$ (Kommutativität)

(V4) $\alpha \cdot \underbrace{(\beta \cdot x)}_{\in \mathbb{R}^n} = \underbrace{(\alpha \cdot \beta)}_{\in \mathbb{R}} \cdot x$ für alle $\alpha, \beta \in \mathbb{R}, x \in \mathbb{R}^n$
(Verträglichkeit der Multiplikationen)

(V5) $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$, für alle $\alpha, \beta \in \mathbb{R}$, $x \in \mathbb{R}^n$
(erstes Distributivgesetz)

(V6) $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$, für alle $\alpha \in \mathbb{R}$, $x, y \in \mathbb{R}^n$
(zweites Distributivgesetz)

(V7) (Wirkung der $0 \in \mathbb{R}$): $0 \cdot x = 0_{\mathbb{R}^n}$ für $x \in \mathbb{R}^n$

(V8) (Wirkung der $1 \in \mathbb{R}$): $1 \cdot x = x$, $x \in \mathbb{R}^n$.

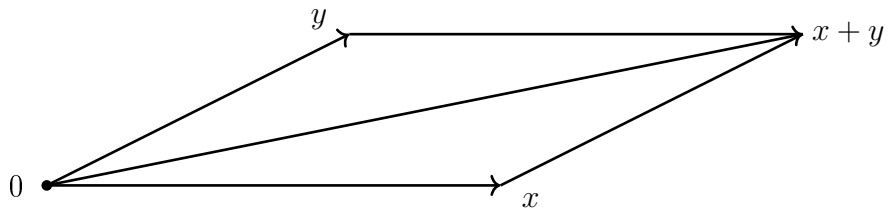
Alle diese Eigenschaften folgen komponentenweise aus den bekannten Rechenregeln für reelle Zahlen.

Konventionen:

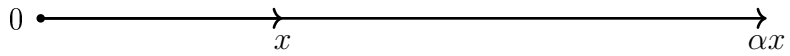
- Punkt geht vor Strichrechnung
  $\alpha \cdot x + \beta \cdot y = (\alpha \cdot x) + (\beta \cdot y)$
- Das Zeichen „+“ wird sowohl für die Addition reeller Zahlen, als auch für die Addition von Vektoren benutzt.
- Das Zeichen „·“ wird sowohl für die Multiplikation in $\mathbb{R}$, als auch für die Skalarmultultiplikation benutzt.
  Man läßt den Punkt oft weg: $\alpha\beta = \alpha \cdot \beta$, $\alpha x = \alpha \cdot x$
- (V1) und (V4) erlauben es, Ausdrücke wie $x + y + z$ oder $\alpha\beta x$ ohne Klammern zu schreiben.
- Oft bezeichnet man $0_{\mathbb{R}^n} \in \mathbb{R}^n$ einfach nur mit 0.

Geometrische Veranschaulichung:

$x + y \mathrel{\hat{=}}$ Komposition von Vektoren



$\alpha x =$ Streckung um den Faktor α



Eigenschaften des Skalarprodukts: Für alle $x, y, z \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$ gilt

(S1) $\underset{\substack{\uparrow \\ (\text{„+“ im } \mathbb{R}^n)}}{\langle x + y, z\rangle} = \underset{\substack{\uparrow \\ (\text{„+“ in } \mathbb{R})}}{\langle x, z\rangle + \langle y, z\rangle}$ (Distributivität)

(S2) $\alpha\langle x, y\rangle = \langle \alpha x, y\rangle$ (Homogenität)

(S3) $\langle x, y\rangle = \langle y, x\rangle$ (Symmetrie)

(S4) Positive Definitheit: $\langle x, x\rangle > 0$ wenn $x \neq 0_{\mathbb{R}^n}$

(S1) – (S3) sind offensichtlich, (S4) folgt daraus, dass Quadrate nichtnegativ sind und aus $x_1^2 + \cdots + x_n^2 = 0 \Leftrightarrow x_1 = \ldots = x_n = 0$.

Definition 2.2. $x \in \mathbb{R}^n$: $\|x\| \stackrel{df}{=} \sqrt{\langle x, x\rangle}$ heißt die **Norm** von x.

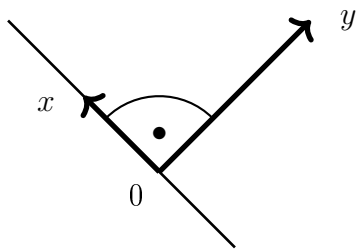
Geometrische Interpretation: $\|x\|$ ist der Abstand von x (als Punkt aufgefasst) vom Nullpunkt bzw. wenn man x als Pfeil auffasst, seine Länge.

Bemerkung 2.3. Es gilt $\|\alpha x\| = |\alpha|\,\|x\|$, $\alpha \in \mathbb{R}$, $x \in \mathbb{R}^n$.

Definition 2.4. (Standardabstand im $\mathbb{R}^n$) Seien $x, y \in \mathbb{R}^n$. Dann heißt $d(x,y) \stackrel{df}{=} \|x - y\|$ der **Abstand** zwischen x und y.

Definition 2.5. (Orthogonalität) Zwei Vektoren $x, y \in \mathbb{R}^n$ heißen **orthogonal** (Notation: $x \perp y$), wenn $\langle x, y\rangle = 0$ gilt.

Definition 2.5 ist auf die folgende Weise geometrisch begründet. Es seien $x, y \neq 0_{\mathbb{R}^n}$. Dann spannen x und y eine Ebene auf und in dieser bilden x und y genau dann einen rechten Winkel, wenn der Lotpunkt von y auf die Gerade durch 0 und x gerade der Ursprung 0 ist, d.h. 0 ist derjenige Punkt auf der Geraden mit dem kleinsten Abstand zu y.



Mit anderen Worten: es muss $\|y - \lambda x\| > \|y\|$ für alle $\lambda \neq 0$ gelten. Das ist äquivalent zu $\|y - \lambda x\|^2 > \|y\|^2$. Nun gilt

$$\|y - \lambda x\|^2 = \langle y - \lambda x, y - \lambda x\rangle = \|y\|^2 + \lambda^2\|x\|^2 - 2\lambda\langle x, y\rangle.$$

Die Ungleichung ist daher äquivalent zu

$$\|x\|^2 > \frac{2}{\lambda}\langle x, y\rangle \quad \text{für alle } \lambda \neq 0,$$

was offensichtlich genau dann richtig ist, wenn $\langle x, y\rangle = 0$ gilt.

Satz 2.6 (Satz des Pythagoras)**.** *Sind $x, y \in \mathbb{R}^n$ orthogonal (zueinander), so gilt*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Beweis.

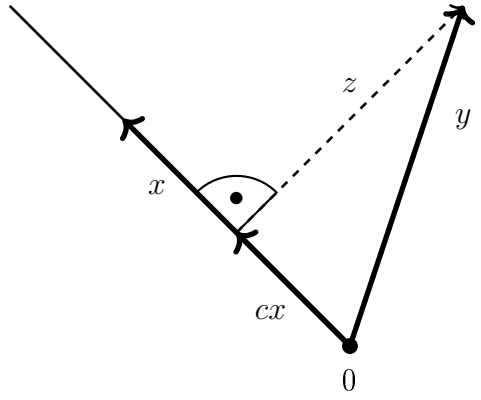
$$\begin{aligned} \|x + y\|^2 = \langle x + y, x + y\rangle &= \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle \\ &= \|x\|^2 + \|y\|^2 \end{aligned}$$

□

Satz 2.7. *(Orthogonalprojektion) Sei $x \in \mathbb{R}^n$, $x \neq 0$. Dann gibt es zu jedem $y \in \mathbb{R}^n$ ein eindeutig bestimmtes $z \in \mathbb{R}^n$ und eine eindeutig bestimmte reelle Zahl $c \in \mathbb{R}$ so dass gilt*

$$x \perp z \quad \text{und} \quad y = cx + z.$$

Es gilt $c = \frac{\langle y,x\rangle}{\|x\|^2}$ und $z = y - \frac{\langle y,x\rangle}{\|x\|^2}x$.



Beweis. Eindeutigkeit: Es seien $z \in \mathbb{R}^n$, $c \in \mathbb{R}$ mit der beschriebenen Eigenschaft. Dann gilt

$$\begin{aligned} \langle y, x\rangle = \langle cx + z, x\rangle &= \langle cx, x\rangle + \langle z, x\rangle \\ &= c\|x\|^2. \end{aligned}$$

Wegen $\|x\| \neq 0$ folgt $c = \frac{\langle y,x\rangle}{\|x\|^2}$. Daher ist c eindeutig. Weiter gilt $y = cx + z$, also $z = y - cx$ und daher ist auch z eindeutig bestimmt.

Existenz: Eine einfache Rechnung zeigt, dass die oben angegebenen c und z die gewünschten Eigenschaften haben

(ii) $cx + z = cx + (y - cx) = y$

(i) $\langle z, x\rangle = \langle y - cx, x\rangle$
$= \langle y, x\rangle - c\langle x, x\rangle$
$= \langle y, x\rangle - \frac{\langle y,x\rangle}{\|x\|^2}\langle x, x\rangle = 0$ □

Satz 2.8. *(Schwarzsche Ungleichung) Für $x, y \in \mathbb{R}^n$ gilt*

$$|\langle x, y\rangle| \leq \|x\| \cdot \|y\|.$$

Beweis. Für $x = 0$ sind beide Seiten 0. Sei $x \neq 0$ und $c \in \mathbb{R}$, $z \in \mathbb{R}^n$ wie in Satz 2.7, d.h. $y = z + cx$. $\langle z, x\rangle = 0$. Dann gilt

$$\begin{aligned} \|y\|^2 = \langle y, y\rangle &= \langle z + cx, z + cx\rangle \\ &= c^2\|x\|^2 + \|z\|^2 \\ &\geq c^2\|x\|^2 \\ &= \left(\frac{\langle y, x\rangle}{\|x\|^2}\right)^2 \|x\|^2 \\ &= \frac{(\langle x, y\rangle)^2}{\|x\|^2} \end{aligned}$$

Das Ziehen der Quadratwurzel liefert das Gewünschte. □

Satz 2.9. *(Dreiecksungleichung) Für $x, y \in \mathbb{R}^n$ gilt*

$$\|x+y\| \leq \|x\| + \|y\|.$$

Beweis.

$$\begin{array}{rcl} \|x+y\|^2 & = & \langle x+y, x+y\rangle = \|x\|^2 + 2\langle x,y\rangle + \|y\|^2 \\ & \leq & \|x\|^2 + 2|\langle x,y\rangle| + \|y\|^2 \\ \text{(Schwarz)} & \leq & \|x\|^2 + 2\|x\|\,\|y\| + \|y\|^2 \\ & = & (\|x\| + \|y\|)^2. \end{array}$$

□

Bemerkung 2.10. Der Name Dreiecksungleichung kommt daher, dass für drei Punkte $x, y, z \in \mathbb{R}^n$ folgt

$$\begin{array}{rcl} d(x,z) = \|x-z\| & = & \|(x-y)+(y-z)\| \\ & \leq & \|x-y\| + \|y-z\| \\ & = & d(x,y) + d(y,z). \end{array}$$

$n = 3$. Wir erinnern uns an das Kreuzprodukt für $x, y \in \mathbb{R}^3$

$$x \times y = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1).$$

Eigenschaften: Für $x, y, z \in \mathbb{R}^3$, $\alpha \in \mathbb{R}$ gilt

(1) Additivität im ersten Argument:

$$(x+y) \times z = x \times z + y \times z$$

(2) Homogenität im ersten Argument:

$$(\alpha x) \times y = \alpha(x \times y)$$

(3) Antisymmetrie: $x \times y = -y \times x$

Orthogonalität:

(4) $x \times y \perp x,\ x \times y \perp y$
(5) $x \times x = 0$.

Diese Eigenschaften rechnet man leicht nach. Mittels (3) folgen direkt auch

(1') $x \times (y+z) = x \times y + x \times z$
(2') $x \times (\alpha y) = \alpha(x \times y)$.

Bemerkung 2.11. Das Kreuzprodukt im $\mathbb{R}^3$ ist ein Beispiel für eine Operation, die weder kommutativ, noch assoziativ ist.

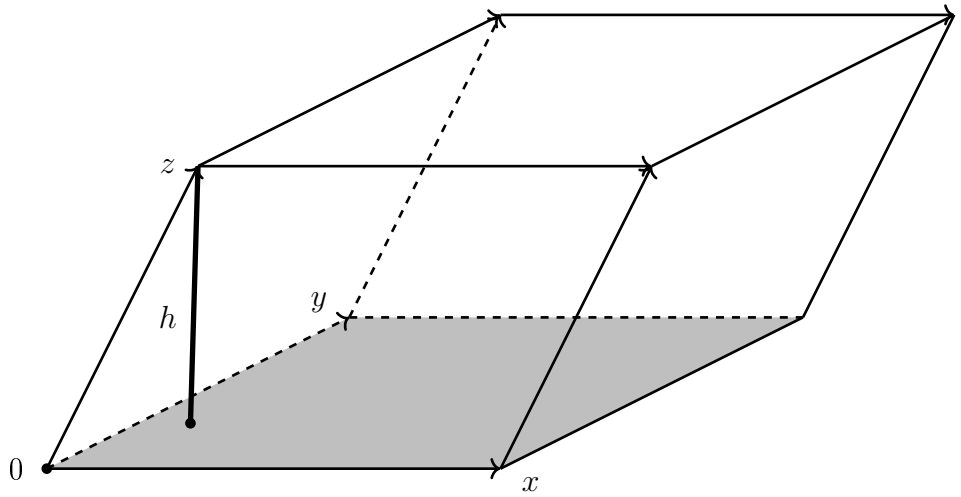
$$\begin{aligned} \bullet (1,0,0) \times (0,1,0) &= (0,0,1) \\ (0,1,0) \times (1,0,0) &= (0,0,-1) \end{aligned}$$

$$\begin{aligned} \bullet \big((1,0,0) \times (1,0,0)\big) \times (0,1,0) &= (0,0,0) \times (0,1,0) = (0,0,0) \\ (1,0,0) \times \big((1,0,0) \times (0,1,0)\big) &= (1,0,0) \times (0,0,1) = (0,-1,0) \end{aligned}$$

Geometrische Deutung:
Zwei Vektoren im $\mathbb{R}^3$ spannen ein **Parallelogramm** auf, dessen Flächeninhalt wir mit $\mathrm{vol}(x,y)$ bezeichnen.[1] Schulwissen:

$$\mathrm{vol}(x,y) = \|x \times y\|. \tag{6}$$

Drei Vektoren $x, y, z \in \mathbb{R}^3$ spannen ein **Parallelotop** (Spat) auf.



Das Volumen bezeichnen wir mit $\mathrm{vol}(x,y,z)$.

Satz 2.12. *Es gilt*

$$\mathrm{vol}(x,y,z) = |\langle x \times y, z\rangle|.$$

Beweis. Nach (4) steht $x \times y$ senkrecht auf der Fläche des von x und y aufgespannten Parallelogramms. Schulwissen:

$$\mathrm{vol}(x,y,z) = \mathrm{vol}(x,y) \cdot h$$

wobei h die Höhe von z über der von x und y aufgespannten Ebene ist.
Schreiben wir $z = c \cdot (x \times y) + w$ mit $\langle x \times y, w\rangle = 0$ (Orthogonalprojektion 2.7), so gilt

[1] Das Parallelogramm kann auch zu einer Strecke oder einem Punkt entarten, dann ist der Flächeninhalt Null.

$$h = \|c \cdot (x \times y)\| = |c| \cdot \|x \times y\| = \frac{|\langle z, x \times y\rangle|}{\|x \times y\|^2} \cdot \|x \times y\| = \frac{|\langle z, x \times y\rangle|}{\|x \times y\|}.$$

Es ergibt sich daher

$$\begin{aligned} \mathrm{vol}(x, y, z) &= \mathrm{vol}(x, y) \cdot \frac{|\langle z, x \times y\rangle|}{\|x \times y\|} \\ &= \|x \times y\| \cdot \frac{|\langle z, x \times y\rangle|}{\|x \times y\|} \\ &= |\langle x \times y, z\rangle|. \end{aligned}$$

□

Dies motiviert die

Definition 2.13. Das **Spatprodukt** (= Determinante) dreier Vektoren $x, y, z \in \mathbb{R}^3$ ist die reelle Zahl $\langle x \times y, z\rangle$ („Volumen mit Vorzeichen“).

Bemerkung 2.14. Explizit erhält man

$$\langle x \times y, z\rangle = x_1y_2z_3 + x_2y_3z_1 + x_3y_1z_2 - x_1y_3z_2 - x_2y_1z_3 - x_3y_2z_1.$$

2.2 Definition eines Vektorraums

Sei R ein unitärer Ring.

Definition 2.15. Ein (unitärer Links-)**Modul** über R ist eine abelsche Gruppe $(M, +_M, 0_M)$ mit einer Operation

$$R \times M \to M, \quad (a, m) \mapsto a \cdot m,$$

so dass für alle $a, b \in R$, $v, w \in M$ gilt
(M1) $a \cdot (b \cdot v) = (a \cdot b) \cdot v$
(M2) $(a + b) \cdot v = a \cdot v + b \cdot v$
(M3) $a \cdot (v + w) = a \cdot v + a \cdot w$
(M4) $1_R \cdot v = v$.

Die rechten Seiten von (M2) und (M3) sind so zu interpretieren, dass Punkt- vor Strichrechnung geht. Man lässt die Punkte typischerweise weg und schreibt av für $a \cdot v$.

Definition 2.16. Ein Modul über einem Körper K heißt ***K*-Vektorraum**.

Beispiele 2.17. 1) $\{0\}$ mit der offensichtlichen (und einzig möglichen) Operation ist ein K-Vektorraum.
2) $(K, +_K, 0_K)$ mit der Operation $K \times K \to K$, $(a, v) \mapsto av$, ist ein K-Vektorraum.
3) $K^n = \underbrace{K \times \cdots \times K}_{n\text{-mal}}$ wird zum K-Vektorraum durch

$$(v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n)$$

und $a(v_1, \ldots, v_n) = (av_1, \ldots, av_n)$.
4) $\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum. Allgemeiner: Ist L ein Körper und $K \subset L$ ein Unterkörper, so wird L durch die Operation $K \times L \to L$, $(k, l) \mapsto kl$ zum K-Vektorraum.
5) Die Menge $C^n(\mathbb{R}, \mathbb{R})$ der n-mal stetig differenzierbaren reellwertigen Funktionen auf $\mathbb{R}$ $(0 \leq n \leq \infty)$ ist ein $\mathbb{R}$-Vektorraum durch

Addition: $(f_1 + f_2)(x) = f_1(x) + f_2(x)$.
Skalarmultiplikation: $(af)(x) = af(x)$.

Von jetzt an sei K ein fixierter Körper, den wir manchmal von der Notation ausschließen.

Lemma 2.18. *Sei V ein K-Vektorraum. Dann gilt für alle $v \in V$, $a \in K$:*

(i) $0_K \cdot v = 0_V$,

(ii) $(-1)_K v = -v$,

(iii) $a \cdot 0_V = 0_V$.

Beweis. (i) $0_V + 0_K \cdot v = 0_K \cdot v = (0_K + 0_K)v = 0_K \cdot v + 0_K \cdot v$. Jetzt kürzen.
(ii) $0_V = 0_K \cdot v = (1_K + (-1)_K) \cdot v = v + (-1_K)v$.
(iii) $0_V + a \cdot 0_V = a \cdot 0_V = a \cdot (0_V + 0_V) = a \cdot 0_V + a \cdot 0_V$. Jetzt kürzen. □

Definition 2.19. Es seien V, W K-Vektorräume. Ein Gruppenhomomorphismus

$$f : V \to W$$

heißt **(*K*-)lineare Abbildung** oder **(*K*-)Vektorraumhomomorphismus**, wenn $f(ax) = af(x)$ für alle $x \in V$ gilt. Die Menge der linearen Abbildungen von V nach W wird mit $\mathrm{Hom}_K(V, W)$ bezeichnet.

Weitere Notationen:

$\mathrm{End}_K(V) = \mathrm{Hom}_K(V, V)$ (Endomorphismen)
$\mathrm{GL}(V) = \mathrm{Aut}_K(V) = \{\varphi \in \mathrm{End}_K(V) \mid \varphi \text{ ist Isomorphismus}\}$ (Automorphismen)

Beispiele linearer Abbildungen.

1) $K^n \to K^1 = K,\ (a_1, \ldots, a_n) \mapsto a_1$.

2) $\mathbb{R}^n \to \mathbb{R},\ x \mapsto \langle x, y\rangle$ für ein festes $y \in \mathbb{R}^n$.

3) $K^n \to K^{2n},\ (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n, a_1, \ldots, a_n)$.

4) $C^0(\mathbb{R}, \mathbb{R}) \to \mathbb{R},\ f \mapsto \int_0^1 f(x)dx$.

5) $n \geq 1$:

$$\begin{array}{rcl} C^n(\mathbb{R}, \mathbb{R}) & \longrightarrow & C^{n-1}(\mathbb{R}, \mathbb{R}) \\ f & \longmapsto & f' = \frac{df}{dx} \quad \text{(Ableitung)}. \end{array}$$

Definition 2.20. Eine Teilmenge V eines Vektorraumes W heißt **Untervektorraum**, wenn sie mit den von W geerbten Strukturen ein Vektorraum ist, d.h.

(i) V ist Untergruppe von W
(ii) $v \in V \Rightarrow a \cdot v \in V$ für alle $a \in K$.

Beispiel 2.21. $V = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ ist ein Untervektorraum des $\mathbb{R}^3$.

Lemma 2.22. *Sei $f : V \to W$ eine (K-)lineare Abbildung. Dann gilt*

(i) $\mathrm{Kern}(f) \subset V$ *ist Untervektorraum,*

(ii) $\mathrm{Bild}(f) \subset W$ *ist Untervektorraum.*

Beweis. $\mathrm{Kern}(f)$ und $\mathrm{Bild}(f)$ sind Untergruppen nach 1.30. Für $v \in \mathrm{Kern}(f)$ gilt $f(av) = af(v) = a \cdot 0_W = 0_W$, also $av \in \mathrm{Kern}(f)$ für alle $a \in K$. Für $w = f(v) \in \mathrm{Bild}(f)$ gilt $a \cdot w = a \cdot f(v) = f(a \cdot v) \in \mathrm{Bild}(f)$. □

2.3 Operationen auf Vektorräumen

1) Seien U, V K-Vektorräume und M eine Menge.

(a) $\mathrm{Abb}(M, V)$ wird zum Vektorraum durch

$$(f_1 + f_2)(m) = f_1(m) + f_2(m), \quad (af)(m) = a(f(m))$$

neutrales Element: $e(m) = 0_V$ für alle $m \in M$ („Nullabbildung"), Bezeichnung: $0 \in \mathrm{Abb}(M, V)$

(b) $\mathrm{Hom}_K(U, V) \subset \mathrm{Abb}(U, V)$ ist ein Untervektorraum, weil:

– 0 ist eine lineare Abbildung
– f_1, f_2 linear $\Rightarrow f_1 + f_2$ linear
– $a \in K$, f linear $\Rightarrow af$ linear.

Spezialfall: $V = K$

Definition 2.23. Es heißt

$$U^* := \mathrm{Hom}_K(U, K)$$

der **Dualraum** zu U, seine Elemente heißen **Linearformen** auf U.

Ist $f : U \to V$ eine lineare Abbildung, so ist die **duale Abbildung**

$$f^* : V^* \longrightarrow U^*,\ \varphi \longmapsto \varphi \circ f,$$

linear (!). Die Abbildung

$$\begin{array}{rccc} * : \mathrm{Hom}_K(U,V) & \longrightarrow & \mathrm{Hom}_K(V^*,U^*) \\ f & \longmapsto & f^* \end{array}$$

ist linear (!). Die Abbildung

$$U \longrightarrow (U^*)^*\ ,\ u \longmapsto (f \mapsto f(u)),$$

ist linear (!) und heißt die **Auswertungsabbildung**.

(c) das kartesische Produkt $U \times V$ wird durch $(u_1, v_1)+(u_2, v_2) = (u_1+u_2, v_1+v_2)$ und $a(u, v) = (au, av)$ zu einem K-Vektorraum.
Alternative Bezeichnung: $U \oplus V$ (die *direkte* Summe).

2) Seien $U_1, U_2 \subset V$ Untervektorräume.

(a): $U_1 \cap U_2$ ist ein Untervektorraum in V.

(b): $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1,\ u_2 \in U_2\}$ ist ein Untervektorraum in V.

Lemma 2.24. *Die natürliche Abbildung*

$$\varphi : U_1 \oplus U_2 \to U_1 + U_2, \quad (u_1, u_2) \longmapsto u_1 + u_2,$$

ist linear und surjektiv. Gilt $U_1 \cap U_2 = \{0\}$, so ist φ ein Isomorphismus.

Beweis. • φ ist linear. Seien $u_1, v_1 \in U_1,\ u_2, v_2 \in U_2$ und $a \in K$:

$$\begin{aligned} &\varphi((u_1, u_2) + (v_1, v_2)) = \varphi((u_1 + v_1, u_2 + v_2)) \\ &= u_1 + v_1 + u_2 + v_2 = (u_1 + u_2) + (v_1 + v_2) \\ &= \varphi((u_1, u_2)) + \varphi((v_1, v_2)). \end{aligned}$$

$$\begin{aligned} &\varphi(a(u_1, u_2)) = \varphi(au_1, au_2)) = \\ &au_1 + au_2 = a(u_1 + u_2) = a\varphi((u_1, u_2)). \end{aligned}$$

• Die Surjektivität folgt aus der Definition von $U_1 + U_2$.

• Sei $U_1 \cap U_2 = \{0\}$ und $(u_1, u_2) \in \mathrm{Kern}(\varphi)$. Dann gilt $u_1 + u_2 = 0 \Rightarrow u_1 = -u_2$. Folglich $u_1 \in U_2$, $u_2 \in U_1$, also $u_1, u_2 \in U_1 \cap U_2 = \{0\} \Rightarrow (u_1, u_2) = (0, 0)$. Daher gilt $\mathrm{Kern}(\phi) = \{0\}$ und die Injektivität von φ folgt aus 1.30 (iii). □

3) Sei $U \subset V$ ein Untervektorraum. Die Faktorgruppe V/U der Nebenklassen $v+U$ von V modulo U wird ein K-Vektorraum durch

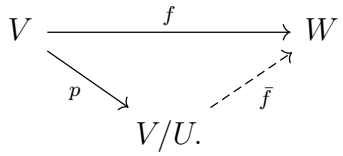
$$a \cdot (v+U) = a \cdot v + U.$$

Unabhängigkeit von der Auswahl: Ist $v_1+U = v_2+U$, so gilt $v_1-v_2 \in U$. Folglich: $av_1 - av_2 = a(v_1-v_2) \in U$ und daher $av_1 + U = av_2 + U$.

V/U heißt der **Faktorvektorraum**. Die kanonische Projektion $p : V \to V/U$ ist linear.

Satz 2.25. *(Universelle Eigenschaft des Faktorraums). Sei $U \subset V$ ein Untervektorraum und $p : V \to V/U$ die kanonische Projektion. Dann gilt:*

Zu jeder linearen Abbildung $f : V \to W$ mit $U \subset \mathrm{Kern}(f)$ gibt es eine eindeutig bestimmte lineare Abbildung $\bar{f} : V/U \to W$ mit $f = \bar{f} \circ p$.



Beweis. Existenz: Definiere $\bar{f}(v+U) = f(v)$.
Wohldefiniertheit: Gilt $v_1 + U = v_2 + U$, so gilt $v_1 - v_2 \in U \subset \mathrm{Kern}(f)$. Daher gilt

$$\begin{aligned} f(v_1) = f(v_1) - f(v_1 - v_2) &= f(v_1 - v_1 + v_2) \\ &= f(v_2). \end{aligned}$$

Eindeutigkeit: Seien $\bar{f}_1$ und $\bar{f}_2$ zwei solche Abbildungen und $v+U \in V/U$ beliebig. Z.z. $\bar{f}_1(v+U) = \bar{f}_2(v+U)$. Wegen $f(v) = \bar{f}_1(p(v)) = \bar{f}_1(v+U)$ und $f(v) = \bar{f}_2(p(v)) = \bar{f}_2(v+U)$ gilt $\bar{f}_1(v+U) = \bar{f}_2(v+U)$. □

Korollar 2.26. *Seien $U \subset V$ Vektorräume und W ein weiterer Vektorraum. Dann gibt es einen natürlichen Isomorphismus von Vektorräumen*

$$F : \{\varphi \in \mathrm{Hom}_K(V,W) \mid U \subset \mathrm{Kern}(\varphi)\} \xrightarrow{\sim} \mathrm{Hom}_K(V/U, W)$$

Beweis. Der Definitionsbereich von F ist, wie man leicht nachprüft, ein Untervektorraum von $\mathrm{Hom}_K(V,W)$. Die Abbildung F ist durch die Universaleigenschaft des Faktorraums gegeben (2.25), d.h. $F(\varphi) =: \psi$ ist die eindeutig bestimmte Abbildung mit $\psi(v+U) = \varphi(v) \in W$ für alle $v \in V$. Dass F linear ist, folgt direkt aus der Definition.
Um zu zeigen, dass F ein Isomorphismus ist, genügt es, eine Umkehrabbildung anzugeben. Sei $p : V \to V/U$ die kanonische Projektion und für $\psi : V/U \to W$ setze $G(\psi) = \psi \circ p : V \to W$. Dann gilt $U \subset \mathrm{Kern}(G(\psi))$, sowie $F \circ G(\psi) = \psi$ und $G \circ F(\varphi) = \varphi$ für alle φ und ψ. □

Korollar 2.27. *Sei $f : V \to W$ eine lineare Abbildung. Dann gibt es einen natürlichen Isomorphismus*

$$\big(W/\operatorname{Bild}(f)\big)^* \cong \operatorname{Kern}(f^* : W^* \to V^*).$$

Beweis. $\big(W/\operatorname{Bild}(f)\big)^* = \operatorname{Hom}_K(W/\operatorname{Bild}(f), K)$
und

$$\begin{aligned} \operatorname{Kern} f^* &= \{\varphi : W \longrightarrow K \mid f^*(\varphi) = 0\} \\ &= \{\varphi : W \longrightarrow K \mid \varphi \circ f = 0\} \\ &= \{\varphi : W \longrightarrow K \mid \operatorname{Bild}(f) \subset \operatorname{Kern}(\varphi)\}. \end{aligned}$$

Die Aussage folgt aus 2.26 (mit $U = \operatorname{Bild}(f)$ und $W = K$). □

Satz 2.28. *(Homomorphiesatz für lineare Abbildungen). Seien V, W Vektorräume und $f : V \to W$ eine lineare Abbildung. Dann gibt es einen natürlichen Vektorraumisomorphismus*

$$F : V/\operatorname{Kern}(f) \xrightarrow{\sim} \operatorname{Bild}(f)$$

mit der Eigenschaft $f = i \circ F \circ p$. Hier bezeichnet $p : V \to V/\operatorname{Kern}(f)$ die kanonische Projektion und $i : \operatorname{Bild}(f) \to W$ die Inklusion.

Beweis. Nach 2.25 erhalten wir eine lineare Abbildung $\overline{f} : V/\operatorname{Kern}(f) \to W$ mit $\overline{f}(v + \operatorname{Kern}(f)) = f(v)$, d.h. $f = \overline{f} \circ p$.
• $\overline{f}$ ist injektiv, da $\overline{f}(v + \operatorname{Kern}(f)) = 0 \Rightarrow f(v) = 0 \Rightarrow v \in \operatorname{Kern}(f) \Rightarrow v + \operatorname{Kern}(f) = 0 + \operatorname{Kern}(f)$.
• das Bild von $\overline{f}$ ist gleich $\operatorname{Bild}(f)$ (klar).
Damit können wir $\overline{f}$ in der Form $\overline{f} = i \circ F$ mit $F : V/\operatorname{Kern}(f) \to \operatorname{Bild}(f)$ schreiben. Da $\overline{f}$ injektiv ist, ist auch F injektiv. Außerdem ist F nach Konstruktion surjektiv (vgl. 1.31). Daher ist F ein Isomorphismus und es gilt $f = \overline{f} \circ p = i \circ F \circ p$. □

4) Unendliche Familien
Seien $(U_i)_{i \in I}$ Vektorräume. Das kartesische Produkt

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

wird (analog zum Produkt zweier Vektorräume) durch komponentenweise Addition und Skalarmultiplikation zu einem Vektorraum.

Notation: Ist I eine Indexmenge und sind $(a_i)_{i \in I}$ Objekte die durch I indiziert sind, so sagt man, dass eine Eigenschaft „für fast alle $i \in I$“ erfüllt ist, wenn es eine endliche Teilmenge $J \subset I$ gibt, so dass für alle $i \in I \setminus J$ das Objekt a_i die Eigenschaft hat.

Beispiel 2.29. Fast alle natürlichen Zahlen sind größer als 10.

Definition 2.30 (Direkte Summe)**.**

$$\bigoplus_{i\in I} U_i := \{(u_i)_{i\in I} \mid u_i = 0 \text{ für fast alle } i \in I\}$$

heißt die **direkte Summe** der Vektorräume U_i.

Es ist $\bigoplus_{i\in I} U_i$ ein Untervektorraum in $\prod_{i\in I} U_i$. Ist I endlich, so gilt $\bigoplus_{i\in I} U_i = \prod_{i\in I} U_i$. Ist die Indexmenge I endlich und nicht-leer nimmt man sich typischerweise eine bijektive Abbildung $I \xrightarrow{\sim} \{1,\dots,n\}$ und schreibt $\bigoplus_{i\in I} U_i = \bigoplus_{i=1}^{n} U_i$, und analog für die anderen Operationen.

Konventionen: $\bigoplus_{i\in\emptyset} U_i = \{0\} = \prod_{i\in\emptyset} U_i$.

Sei nun $(U_i)_{i\in I}$ eine Familie von Untervektorräumen eines Vektorraums V. Dann haben wir die Untervektorräume **Durchschnitt** und **Summe**

$$\bigcap_{i\in I} U_i = \{u \mid u \in U_i \text{ für alle } i\}$$

$$\sum_{i\in I} U_i = \left\{ \sum_{i\in I} u_i \mid u_i \in U_i \text{ für alle } i, \text{ und } u_i = 0 \text{ f. f. a. } i \right\}$$

Wegen der Bedingung $u_i = 0$ f.f.a. i ist die scheinbar unendliche Summe nur eine endliche Summe und darum überhaupt erst definiert.

Konventionen:

$$\sum_{i\in\emptyset} U_i = \{0\}, \quad \bigcap_{i\in\emptyset} U_i = V.$$

Wir haben gesehen, dass $\mathrm{Hom}_K(V,W)$ wieder eine Vektorraumstruktur trägt. Insbesondere ist es eine abelsche Gruppe bzgl. $+$. Ist $V = W$, so definieren wir auf $\mathrm{Hom}_K(V,V) = \mathrm{End}_K(V)$ eine Multiplikation durch $\circ$ (Komposition).

Lemma 2.31 (Endomorphismenring)**.** *Mit den oben erklärten Operationen ist* $(\mathrm{End}_K(V), +, \circ, 0, \mathrm{id}_V)$ *ein unitärer Ring. Die Abbildung*

$$K \to \mathrm{End}_K(V),\ a \longmapsto a \cdot \mathrm{id}_V,$$

ist ein unitärer Ringhomomorphismus. Durch die Operation

$$\begin{array}{rcl} \mathrm{End}_K(V) \times V & \longrightarrow & V, \\ (f, v) & \longmapsto & f(v) \end{array}$$

wird V zu einem (unitären, links) $\mathrm{End}_K(V)$*-Modul .*

Beweis. Wir verifizieren die Ringaxiome für $(\mathrm{End}_K(V), +, \circ, 0, \mathrm{id}_V)$. Zunächst ist $\circ$ assoziativ. Weiter gilt $g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$ wegen

$$\begin{aligned}(g \circ (f_1 + f_2))(v) &= g((f_1 + f_2)(v)) = g(f_1(v) + f_2(v)) \\ &= g(f_1(v)) + g(f_2(v)) \\ &= g \circ f_1(v) + g \circ f_2(v) = (g \circ f_1 + g \circ f_2)(v).\end{aligned}$$

Analog $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$. Also ist $\mathrm{End}_K(V)$ ein Ring in dem id_V offenbar ein 1-Element ist. Dass die Abbildung $K \to \mathrm{End}_K(V),\ a \mapsto a \cdot \mathrm{id}_V$, ein Ringhomomorphismus ist, liest man leicht an den Definitionen ab. Die gegebene Operation macht V zu einem $\mathrm{End}_K(V)$-Modul weil:

(M1) $g \cdot (f \cdot v) = g(f(v)) = (g \circ f)(v) = (g \cdot f)(v)$.
(M2) $(f + g) \cdot v = (f + g)(v) = f(v) + g(v) = f \cdot v + g \cdot v$
(M3)

$$\begin{aligned}f \cdot (v + w) &= f(v + w) = f(v) + f(w) \\ &= f \cdot v + f \cdot w.\end{aligned}$$

(M4) $1_{\mathrm{End}_K(V)} \cdot v = \mathrm{id}_V(v) = v$. □

2.4 Basen

Erinnerung an Lemma 0.44: Eine über eine Indexmenge I indizierte Familie $(m_i)_{i \in I}$ von Elementen einer Menge M ist nichts weiter als eine Abbildung $m : I \to M$ und wir schreiben $m(i) = m_i \in M$ und $m = (m_i)_{i \in I} \in M^I$.

Sprechweise: $(m_i)_{i \in I}$ ist ein **System von Elementen in** M.

Definition 2.32. Ein System von Skalaren $(\alpha_i)_{i \in I} \in K^I$ heißt **endlich**, wenn $\alpha_i = 0$ für fast alle i gilt. Die Menge aller endlichen Systeme von Skalaren wird mit

$$K^{(I)}$$

bezeichnet.

Bemerkung 2.33. Sei V ein K-Vektorraum, $(v_i)_{i \in I}$ ein System von Vektoren in V und $(\alpha_i)_{i \in I} \in K^{(I)}$ ein endliches System von Skalaren. Dann gilt $\alpha_i v_i = 0$ für fast alle i, so dass man der Summe

$$\sum_{i \in I} \alpha_i v_i$$

einen Sinn geben kann.

Definition 2.34. Sei V ein K-Vektorraum, I eine Indexmenge und $v = (v_i)_{i \in I}$ ein System von Vektoren in V. Der Untervektorraum

$$\mathrm{Lin}((v_i)_{i \in I}) = \left\{ \sum_{i \in I} \alpha_i v_i \mid (\alpha_i)_{i \in I} \in K^{(I)} \right\}$$

heißt die **lineare Hülle** des Systems $(v_i)_{i\in I}$. Jeder Vektor $v \in \mathrm{Lin}((v_i)_{i\in I})$ heißt **Linearkombination** der v_i. Man nennt $\mathrm{Lin}((v_i)_{i\in I})$ auch den von den Vektoren $(v_i)_{i\in I}$ **aufgespannten** Untervektorraum.

Bemerkung 2.35. Setzt man $U_i = Kv_i := \{\alpha v_i \mid \alpha \in K\}$, so gilt

$$\mathrm{Lin}((v_i)_{i\in I}) = \sum_{i\in I} U_i.$$

Definition 2.36. Sei $(v_i)_{i\in I}$ ein System von Vektoren eines Vektorraums V.

(i) $(v_i)_{i\in I}$ heißt **Erzeugendensystem** von V, wenn $\mathrm{Lin}((v_i)_{i\in I}) = V$ gilt.

(ii) $(v_i)_{i\in I}$ heißt **linear unabhängig**, wenn für jedes endliche System von Skalaren $(\alpha_i)_{i\in I} \in K^{(I)}$ die Implikation

$$\sum_{i\in I} \alpha_i v_i = 0 \implies \alpha_i = 0 \text{ für alle } i$$

gilt.

(iii) $(v_i)_{i\in I}$ heißt **Basis** von V, wenn es zu jedem Vektor $v \in V$ ein eindeutig bestimmtes endliches System von Skalaren $(\alpha_i)_{i\in I} \in K^{(I)}$ mit $v = \sum_{i\in I} \alpha_i v_i$ gibt.

Lemma 2.37. *Ein System von Vektoren $(v_i)_{i\in I}$ ist genau dann eine Basis von V wenn es ein Erzeugendensystem und linear unabhängig ist.*

Beweis. Sei $(v_i)_{i\in I}$ eine Basis. Da jeder Vektor als Linearkombination der v_i darstellbar ist, gilt $\mathrm{Lin}((v_i)_{i\in I}) = V$, d.h. $(v_i)_{i\in I}$ ist ein Erzeugendensystem. Ist nun $(\alpha_i)_{i\in I} \in K^{(I)}$ ein endliches System von Skalaren mit $\sum_{i\in I} \alpha_i v_i = 0$, so gilt wegen $\sum_{i\in I} 0 \cdot v_i = 0$ und der Eindeutigkeit der Darstellung: $\alpha_i = 0$ für alle $i \in I$.

Sei nun $(v_i)_{i\in I}$ ein Erzeugendensystem. Dann ist jeder Vektor Linearkombination der $(v_i)_{i\in I}$. Z.z: ist das System $(v_i)_{i\in I}$ linear unabhängig, so ist die Darstellung jedes Vektors $v \in V$ als Linearkombination der v_i eindeutig.
Seien nun $(\alpha_i), (\beta_i) \in K^{(I)}$ endliche Familien und $\sum \alpha_i v_i = v = \sum \beta_i v_i$. Dann ist die Familie $(\alpha_i - \beta_i)_{i\in I}$ auch endlich und es gilt $\sum_{i\in I}(\alpha_i - \beta_i)v_i = 0 \Rightarrow \alpha_i - \beta_i = 0$ für alle i. Hieraus folgt $\alpha_i = \beta_i$ für alle i. □

Beispiel 2.38. Im K^n bilden die Vektoren

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 1)$$

eine Basis. Diese heißt die **kanonische Basis** des K^n. Der Vektor e_i, $(i = 1, \ldots, n)$, heißt der ***i*-te Einheitsvektor**.

Lemma 2.39. *Der K-Vektorraum V habe die endliche Basis $(v_1, \ldots, v_n)$. Dann ist die Abbildung*

$$\begin{array}{rccc} \phi: & K^n & \longrightarrow & V \\ & (\alpha_1, \ldots, \alpha_n) & \longmapsto & \sum_{i=1}^{n} \alpha_i v_i \end{array}$$

ein Vektorraumisomorphismus.

Beweis. Zunächst ist ϕ linear.
$v_1, \ldots, v_n$ linear unabhängig $\Rightarrow \mathrm{Kern}(\phi) = 0 \Rightarrow \phi$ ist injektiv.
$v_1, \ldots, v_n$ sind Erzeugendensystem $\Rightarrow \phi$ ist surjektiv. □

Bemerkungen 2.40.
- Im Moment wissen wir noch nicht, ob für $n \neq m$ eventuell ein Isomorphismus $K^n \cong K^m$ existieren könnte.
- Aus unseren Konventionen folgt, dass der triviale K-Vektorraum $\{0\}$ die leere Basis hat.
- Jeder Vektorraum V hat ein Erzeugendensystem, z.B. das, welches aus allen Vektoren besteht (wähle $I = V$ und $\mathrm{id} : V \to V$).
- Ist $V \neq \{0\}$ und $0 \neq v \in V$, so ist das 1-elementige System (v_1), $v_1 = v$, linear unabhängig ($\alpha_1 v_1 = 0$ und $\alpha_1 \neq 0 \Rightarrow 0 = \alpha_1^{-1}\alpha_1 v_1 = v_1$, Widerspruch).

Definition 2.41. Ein Vektorraum V heißt **endlich erzeugt**, wenn es ein endliches Erzeugendensystem $(v_1, \ldots, v_n)$ von V gibt.

Beispiel 2.42. K^n ist endlich erzeugt.

Bemerkung 2.43. Im Moment wissen wir noch nicht, ob jeder Untervektorraum eines endlich erzeugten Vektorraums wieder endlich erzeugt ist. Später werden wir dies zeigen.

Definition 2.44. Ein Erzeugendensystem $(v_i)_{i \in I}$ eines Vektorraums V heißt **minimal**, wenn für jede echte Teilmenge $J \subsetneqq I$ das System $(v_i)_{i \in J}$ kein Erzeugendensystem ist.

Beispiel 2.45. Das Erzeugendensystem $(e_1, \ldots, e_n)$ des K^n ist minimal. Lässt man den i-ten Einheitsvektor weg, so kann man nur noch Elemente $(\alpha_1, \ldots, \alpha_n) \in K^n$ mit $\alpha_i = 0$ als Linearkombination erhalten. Wegen $1 \neq 0$ in K fehlt also z.B. der Vektor $(0, \ldots, 1, \ldots, 0)$ (die 1 steht an i-ter Stelle).

Satz 2.46. *Ein Erzeugendensystem ist genau dann minimal, wenn es eine Basis ist.*

Beweis. Sei $(v_i)_{i \in I}$ eine Basis und $J \subsetneqq I$ eine echte Teilmenge. Wähle ein $i_0 \in I \setminus J$. Trivialerweise gilt $v_{i_0} = 1 \cdot v_{i_0}$. Wegen der Eindeutigkeit der Darstellung, läßt sich also v_{i_0} nicht als Linearkombination der v_j, $j \in J$, schreiben, und deshalb

ist $(v_i)_{i\in J}$ kein Erzeugendensystem. Folglich ist $(v_i)_{i\in I}$ ein minimales Erzeugendensystem.

Sei nun $(v_i)_{i\in I} \in V^I$ ein minimales Erzeugendensystem. Nach 2.37 müssen wir zeigen, dass $(v_i)_{i\in I}$ linear unabhängig ist. Angenommen es gäbe ein von 0 verschiedenes endliches System $(\alpha_i) \in K^{(I)}$ mit $\sum_{i\in I} \alpha_i v_i = 0$. Sei $i_0 \in I$ mit $\alpha_{i_0} \neq 0$. Dann gilt

$$-\alpha_{i_0} v_{i_0} = \sum_{i\in I\smallsetminus\{i_0\}} \alpha_i v_i,$$

also $v_{i_0} = \sum_{i\in I\smallsetminus\{i_0\}} -\frac{\alpha_i}{\alpha_{i_0}} v_i$.

Behauptung: $(v_i)_{i\in I\smallsetminus\{i_0\}}$ ist auch ein Erzeugendensystem.

Beweis der Behauptung: Sei $v \in V$. Dann existiert eine endliche Familie $\beta_i \in K^{(I)}$ mit $v = \sum_{i\in I} \beta_i v_i$. Nun gilt

$$v = \beta_{i_0} v_{i_0} + \sum_{i\in I\smallsetminus\{i_0\}} \beta_i v_i = \sum_{i\in I\smallsetminus\{i_0\}} \left(-\frac{\beta_{i_0}\cdot\alpha_i}{\alpha_{i_0}} + \beta_i\right) v_i.$$

Dies zeigt die Behauptung und wir erhalten einen Widerspruch zur Minimalität des Systems $(v_i)_{i\in I}$. □

Zu Mengen I, J kann man die *disjunkte Vereinigung* $I \dot\cup J$ bilden. Die Elemente in $I \dot\cup J$ sind die Elemente von I und die Elemente von J. Sind I und J Teilmengen einer Menge M, so kann man ihre Vereinigung bilden und es gibt eine natürliche Surjektion

$$I \dot\cup J \longrightarrow I \cup J,$$

die dann und nur dann bijektiv ist, wenn $I \cap J = \emptyset$ gilt.
Sind nun $(v_i)_{i\in I}$ und $(w_i)_{i\in J}$ zwei Systeme von Vektoren eines Vektorraums V, so bezeichnet man das System

$$(u_i)_{i\in I\dot\cup J} \quad \text{mit } u_i = \begin{cases} v_i & i \in I \\ w_i & i \in J \end{cases}$$

als die **Vereinigung** der Systeme $(v_i)_{i\in I}$ und $(w_i)_{i\in J}$.

Definition 2.47. Ein linear unabhängiges System von Vektoren $(v_i)_{i\in I} \in V^I$ heißt **maximal**, wenn für jeden Vektor $v \in V$ das System $(v_i)_{i\in I\dot\cup\{*\}}$ mit $v_i = v_i$ für $i \in I$ und $v_* = v$ nicht linear unabhängig ist.

Satz 2.48. *Ein linear unabhängiges System ist genau dann maximal, wenn es eine Basis ist.*

Beweis. Sei (v_i) eine Basis und $v \in V$ beliebig. Dann existiert $(\alpha_i)_{i\in I} \in K^{(I)}$ mit $v = \sum \alpha_i v_i$. Dies formuliert man zu

$$\sum \alpha_i v_i + (-1)v = 0$$

um und sieht, dass die Vereinigung von $(v_i)_{i\in I}$ mit dem 1-elementigen System (v) nicht linear unabhängig ist. Also ist (v_i) ein maximales linear unabhängiges System.

Sei (v_i) ein maximales linear unabhängiges System. Nach 2.37 ist zu zeigen, dass (v_i) ein Erzeugendensystem ist. Angenommen nicht. Dann gäbe es ein

$$v \in V \setminus \mathrm{Lin}((v_i)_{i\in I}).$$

Behauptung: Das System $(v_i)_{i\in I \dot\cup \{*\}}$ mit $v_i = v_i$ für $i \in I$, $v_* = v$ ist linear unabhängig.

Beweis der Behauptung: Sei $(\alpha_i)_{i\in I\dot\cup\{*\}}$ eine endliche Familie mit $\sum\limits_{i\in I\dot\cup\{*\}} \alpha_i v_i = 0$. Dann gilt $\alpha_* v = -\sum\limits_{i\in I} \alpha_i v_i$. Wegen $v \notin \mathrm{Lin}((v_i)_{i\in I})$ folgt $\alpha_* = 0$. Da das System $(v_i)_{i\in I}$ linear unabhängig ist, folgt $\alpha_i = 0$ für alle $i \in I$. Dies zeigt die Behauptung.

Wegen der Maximalität von $(v_i)_{i\in I}$ erhalten wir einen Widerspruch, also gilt $\mathrm{Lin}((v_i)_{i\in I}) = V$. □

Satz 2.49. *(Basisergänzungssatz) Sei $(v_i)_{i\in I}$ ein Erzeugendensystem des Vektorraums V und $I' \subset I$ eine Teilmenge, so dass das System $(v_i)_{i\in I'}$ linear unabhängig ist. Dann gibt es eine Teilmenge $J \subset I$, mit $I' \subset J$ so dass $(v_i)_{i\in J}$ eine Basis ist. Insbesondere besitzt jeder Vektorraum eine Basis und jeder endlich erzeugte Vektorraum besitzt eine endliche Basis.*

Beweis. Wir begründen zunächst das „insbesondere“. Sei $(v_i)_{i\in I}$ ein Erzeugendensystem von V (jeder Vektorraum besitzt ein solches). Setzt man $I' = \emptyset$, so erhält man $J \subset I$ so dass $(v_i)_{i\in J}$ eine Basis von V ist. War I endlich, so ist auch J endlich.

Nun beweisen wir die Aussage des Satzes. Die Strategie ist die folgende: Wir erhalten durch Vergrößern der Menge I' ein maximal linear unabhängiges System, welches nach 2.48 eine Basis ist. Der Prozess des Vergrößerns ist im Fall dass I ein unendliches System ist mengentheoretisch aufwendig. Wir beschränken uns daher auf den Fall dass I endlich ist. Einen Beweis im allgemeinen Fall findet man z.B. in W. Greub „Lineare Algebra“ oder in F. Brieskorn „Lineare Algebra und analytische Geometrie“ .

Sei nun $(v_1, \ldots, v_n)$, $n \geq 0$, ein linear unabhängiges System und $(w_1, \ldots, w_m)$ ein System, so dass V durch $(v_1, \ldots, v_n, w_1, \ldots, w_m)$ erzeugt wird. Wir zeigen: es

gibt eine Zahl s, $0 \leq s \leq m$, und Indizes $1 \leq j(1) < \cdots < j(s) \leq m$ so dass $(v_1, \ldots, v_n, w_{j(1)}, , \ldots, w_{j(s)})$ eine Basis ist:

Wir starten mit dem System $(v_1, \ldots, v_n)$.

- nehme w_1 zum System hinzu. Wenn es dadurch linear abhängig wird, entfernen wir w_1 wieder.
- nehme w_2 zum System hinzu. Wenn es dadurch linear abhängig wird, entfernen wir w_2 wieder.

usw.

- nehme w_m zum System hinzu. Wenn es dadurch linear abhängig wird, entfernen wir w_m wieder.

Wir erhalten ein System $(w_{j(1)}, \ldots, w_{j(s)})$ mit folgenden Eigenschaften:

- $(v_1, \ldots, v_n, w_{j(1)}, \ldots, w_{j(s)})$ ist linear unabhängig
- wenn man ein weiteres w hinzunimmt wird das System linear abhängig

Nach Umnumerierung von $w_1, \ldots, w_m$ sei dieses System $(v_1, \ldots, v_n, w_1, \ldots, w_s)$.

Behauptung: Das linear unabhängige System $(v_1, \ldots, v_n, w_1, \ldots, w_s)$ ist ein Erzeugendensystem, also eine Basis.

Beweis der Behauptung: Sei $s < i \leq m$. Nach Konstruktion ist das System $(v_1, \ldots, v_n, w_1, \ldots, w_s, w_i)$ linear abhängig. Daher existieren Skalare $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s, \beta_i \in K$ mit

$$\alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 w_1 + \cdots + \beta_s w_s + \beta_i w_i = 0,$$

wobei nicht alle Koeffizienten gleich 0 sind. Wäre $\beta_i = 0$, so wären alle anderen Koeffizienten auch 0 (lineare Unabhängigkeit von $(v_1, \ldots, v_n, w_1, \ldots, w_s)$). Also ist $\beta_i \neq 0$. Daher gilt $w_i = -\beta_i^{-1}(\alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 w_1 + \cdots + \beta_s w_s)$, d.h. für $s < i \leq m$ kann man w_i als Linearkombination von $v_1, \ldots, v_n, w_1, \ldots, w_s$ schreiben. Ein beliebiges Element $v \in V$ kann nach Voraussetzung als Linearkombination von $v_1, \ldots, v_n, w_1, \ldots, w_m$ und daher (nach Substitution von $w_{s+1}, \ldots, w_m$) auch als Linearkombination von $(v_1, \ldots, v_n, w_1, \ldots, w_s)$, geschrieben werden. Dies zeigt die Behauptung und beendet den Beweis. □

Mit dem Basisergänzungssatz 2.49 und Lemma 2.39 sehen wir, dass jeder endlich erzeugte Vektorraum isomorph zu einem K^n ist. Aber ist das n eindeutig bestimmt? Wichtig ist nun der

Satz 2.50. *Sei $(v_1, \ldots, v_n)$ linear unabhängig und $(w_1, \ldots, w_m)$ eine Basis von V. Dann gilt $n \leq m$.*

Beweis. In linear unabhängigen Systemen kommt kein Vektor doppelt vor, also gilt: $\#\{v_1, \ldots, v_n\} = n$, $\#\{w_1, \ldots, w_m\} = m$. Sei

$$k = \#(\{v_1, \ldots, v_n\} \smallsetminus \{w_1, \ldots, w_m\}).$$

Dann gilt $0 \leq k \leq n$. Wir führen den Beweis per Induktion nach k.
Induktionsanfang: $k = 0 \Rightarrow \{v_1, \ldots, v_n\} \subset \{w_1, \ldots, w_m\}$, also $n \leq m$.
Induktionsvoraussetzung: Die Aussage sei für beliebige Systeme $(v_1, \ldots, v_n)$, $(w_1, \ldots, w_m)$ mit den obigen Eigenschaften und $\#(\{v_1, \ldots, v_n\} \smallsetminus \{w_1, \ldots, w_m\}) < k$ schon bewiesen.
Induktionsschritt: Seien nun $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_m)$ solche Systeme mit $\#(\{v_1, \ldots, v_n\} \smallsetminus \{w_1, \ldots, w_m\}) = k$. Nach Umnummerierung können wir annehmen:

- $\{v_1, \ldots, v_k\} \cap \{w_1, \ldots, w_m\} = \emptyset$
- $\{v_{k+1}, \ldots, v_n\} \subset \{w_1, \ldots, w_m\}$

Wir betrachten nun das linear unabhängige System

$$(v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n).$$

Nach 2.49 gibt es $w_{j(1)}, \ldots, w_{j(s)}$ so dass

$$(v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n, w_{j(1)}, \ldots, w_{j(s)})$$

eine Basis ist. Wegen $v_k \notin \mathrm{Lin}(v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n)$ gilt $s \geq 1$. Wir wenden nun die Induktionsvoraussetzung auf die Systeme

$$(v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n, w_{j(1)}, \ldots, w_{j(s)}), \quad (w_1, \ldots, w_m)$$

an. Dies geht wegen

$$\#(\{v_1, \ldots, v_{k-1}, v_{k+1}, \ldots, v_n, w_{j(1)}, \ldots, w_{j(s)}\} \smallsetminus \{w_1, \ldots, w_m\}) < k$$

(beachte $v_{k+1}, \ldots, v_n \in \{w_1, \ldots, w_m\}$). Nach Induktionsvoraussetzung gilt $n - 1 + s \leq m$ und wegen $s \geq 1$ folgt $n \leq m$. □

Korollar 2.51. *Sei V ein Vektorraum, der eine Basis aus n Vektoren hat. Dann gilt:*

(i) *mehr als n Vektoren sind stets linear abhängig,*

(ii) *jede Basis von V besteht aus genau n Vektoren,*

(iii) *jedes Erzeugendensystem besteht aus mindestens n Vektoren.*

Beweis. (i) folgt aus 2.50.
(ii): ist $(v_1, \ldots, v_n)$ eine Basis und $(w_1, \ldots, w_m)$ eine andere Basis, so folgt aus 2.50 dass $n \leq m$ und $m \leq n$.
(iii) Wäre $(w_1, \ldots, w_m)$, $m < n$, ein Erzeugendensystem, so gäbe es nach 2.49 eine Basis aus weniger als n Vektoren, was (ii) widerspräche. □

Definition 2.52. Ist V ein endlich erzeugter Vektorraum, so nennt man die Kardinalität einer (jeder) Basis die **Dimension** von V. (Bezeichnung: $\dim_K V$ oder einfach $\dim V$). Ist V nicht endlich erzeugt, so setzt man $\dim V = \infty$.

Beispiele 2.53. $V = \{0\} \iff \dim V = 0$.
• $\dim K^n = n$, insbesondere gilt: $K^n \cong K^m \Rightarrow n = m$, da isomorphe Vektorräume die gleiche Dimension haben.
• $\dim_{\mathbb{R}} C^0(\mathbb{R}, \mathbb{R}) = \infty$.

Beweis der letzten Aussage: Sei $n \in \mathbb{N}$ beliebig und seien $a_0, \ldots, a_n \in \mathbb{R}$ reelle Zahlen, nicht alle 0. Dann ist $a_0 + a_1 x + \cdots + a_n x^n$ nicht das Nullpolynom, hat daher nur endlich viele Nullstellen und ist insbesondere nicht konstant 0. Das bedeutet, dass die $n+1$ Funktionen $1, x, x^2, \ldots, x^n$ linear unabhängig sind. Daher gilt $\dim_{\mathbb{R}} C^0(\mathbb{R}, \mathbb{R}) > n$ für alle $n \in \mathbb{N}$, was die Aussage zeigt.

Satz 2.54. *Ist V ein endlich erzeugter Vektorraum und $W \subset V$ ein Untervektorraum, so ist W endlich erzeugt und es gilt $\dim W \leq \dim V$. Die Gleichheit ist äquivalent zu $W = V$.*

Beweis. Sei $n = \dim V$. Wir erhalten eine endliche Basis von W wie folgt.

(1) $W = \{0\}$ fertig.

(2) $W \neq \{0\}$. Wähle $w_1 \in W \smallsetminus \{0\}$.
(w_1) Basis von W fertig. Ansonsten ist (w_1) kein maximales linear unabhängiges System und wir finden $w_2 \in W$ mit (w_1, w_2) linear unabhängig.
(w_1, w_2) Basis fertig, ansonsten suche w_3 usw.

Dieser Prozess bricht ab, weil mehr als n Vektoren in V (und damit in W) stets linear abhängig sind. Wir erhalten eine Basis $(w_1, \ldots, w_m)$ von W mit $m \leq n$. Im Fall $m = n$ ist $(w_1, \ldots, w_m)$ ein maximales linear unabhängiges System von Vektoren in V, also eine Basis, daher $W = \mathrm{Lin}(w_1, \ldots, w_n) = V$. □

Von jetzt an benutzen wir das Wort endlich-dimensionaler Vektorraum für endlich erzeugte Vektorräume.

Lemma 2.55. *Sei $f : V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen Vektorräumen. Dann gilt*

(i) *Ist f injektiv und $(v_1, \ldots, v_n)$ linear unabhängig in V, so ist $(f(v_1), \ldots, f(v_n))$ linear unabhängig in W. Insbesondere gilt $\dim V \leq \dim W$ und Gleichheit gilt dann und nur dann, wenn f ein Isomorphismus ist.*

(ii) *Ist f surjektiv und $(v_1, \ldots, v_n)$ ein Erzeugendensystem von V, so ist $(f(v_1), \ldots, f(v_n))$ ein Erzeugendensystem von W. Es gilt $\dim V \geq \dim W$ und Gleichheit gilt genau dann, wenn f ein Isomorphismus ist.*

Beweis. (i) Sei $(v_1, \ldots, v_n)$ ein linear unabhängiges System in V. Dann gelten die Implikationen

$$\sum_{i=1}^{n} \alpha_i f(v_i) = 0 \Rightarrow f\left(\sum_{i=1}^{n} \alpha_i v_i\right) = 0$$

$$\Rightarrow \sum_{i=1}^{n} \alpha_i v_i = 0 \Rightarrow \alpha_i = 0 \text{ für } i = 1, \ldots, n.$$

Daher ist das System $(f(v_1), \ldots, f(v_n))$ von Vektoren in W linear unabhängig. Ist nun $(v_1, \ldots, v_n)$ eine Basis von V, folgt aus der linearen Unabhängigkeit von $(f(v_1), \ldots, f(v_n)$ und aus 2.54 die Ungleichung $\dim V = n \leq \dim W$.
Da f injektiv ist, induziert f einen Isomorphismus

$$F : V \xrightarrow{\sim} \text{Bild}(f),\ v \mapsto f(v) \in \text{Bild}(f) \subset W.$$

Wir erhalten $\dim \text{Bild}(f) = \dim V$. Nun folgt

$$f \text{ Isomorphismus } \Leftrightarrow \text{Bild}(f) = W \overset{2.54}{\Leftrightarrow}$$

$$\dim \text{Bild}(f) = \dim W \Leftrightarrow \dim V = \dim W.$$

(ii) Sei f surjektiv und $(v_1, \ldots, v_n)$ ein Erzeugendensystem von V. Es sei $w = f(v) \in W$ beliebig. Dann existieren $\alpha_1, \ldots, \alpha_n \in K$ mit $v = \sum_{i=1}^{n} \alpha_i v_i$. Es folgt $w = f(v) = \sum_{i=1}^{n} \alpha_i f(v_i)$. Daher ist $(f(v_1), \ldots, f(v_n))$ ein Erzeugendensystem von W.
Wählen wir nun eine Basis $(v_1, \ldots, v_{\dim(V)})$, so ist $(f(v_1), \ldots, f(v_{\dim(V)})$ ein Erzeugendensystem, also $\dim V \geq \dim W$.

Ist f ein Isomorphismus, so gilt offenbar $\dim V = \dim W$. Umgekehrt gelte $\dim V = \dim W =: n$. Sei $(w_1, \ldots, w_n)$ eine Basis von W und $w_i = f(v_i)$, $i = 1, \ldots, n$. Dann ist $(v_1, \ldots, v_n)$ linear unabhängig (Grund: $\sum \alpha_i v_i = 0 \Rightarrow \sum \alpha_i f(v_i) = 0 \Rightarrow \alpha_i = 0$, $i = 1, \ldots, n$), und wegen $n = \dim V$ maximal linear unabhängig, also eine Basis von V.

Ist nun $\sum_{i=1}^{n} \alpha_i v_i \in \text{Kern}(f)$, so folgt $0 = f(\sum_{i=1}^{n} \alpha_i v_i) = \sum_{i=1}^{n} \alpha_i w_i$, also $\alpha_i = 0$, $i = 1, \ldots, n$. Daher gilt $\text{Kern}(f) = \{0\}$ und f ist ein Isomorphismus. □

Korollar 2.56. *Sei V ein endlich-dimensionaler K-Vektorraum und $f : V \to V$ ein Endomorphismus. Dann sind äquivalent:*

(i) *f ist injektiv,*

(ii) *f ist surjektiv,*

(iii) *f ist ein Isomorphismus.*

Beweis. Ist f injektiv, so ist f Isomorphismus nach 2.55 (i). Ist f surjektiv, so ist f Isomorphismus nach 2.55 (ii). Die verbleibenden Implikationen sind trivial. □

Lemma 2.57. *Sind U, V Vektorräume, so gilt*

$$\dim U \oplus V = \dim U + \dim V.$$

Bemerkung 2.58. Per Konvention gilt $\infty + n = \infty = \infty + n$ für $n \in \mathbb{N}_0$, sowie $\infty + \infty = \infty$.

Beweis von 2.57. Gilt $\dim U = \infty$ oder $\dim V = \infty$, so gilt nach 2.54 auch $\dim U \oplus V = \infty$. Sind $n = \dim U$ und $m = \dim V$ endlich, $(u_1, \ldots, u_n)$ eine Basis von U und $(v_1, \ldots, v_m)$ eine Basis von V, so sieht man unmittelbar, dass

$$((u_1, 0), (u_2, 0), \ldots, (u_n, 0), (0, v_1), \ldots, (0, v_m))$$

eine Basis von $U \oplus V$ ist. Dies zeigt die Dimensionsformel. □

Definition 2.59. Es sei V ein Vektorraum und $U \subset V$ ein Untervektorraum. Ein Untervektorraum U' von V heißt **Komplement** zu U, wenn gilt

$$U \cap U' = \{0\} \quad \text{und} \quad U + U' = V.$$

Bemerkung 2.60. Ist U' ein Komplement zu U, so ist U ein Komplement zu U'.

Satz 2.61. *Sei V ein Vektorraum und $U \subset V$ ein Untervektorraum. Dann existiert ein Komplement U' zu U.*

Beweis. Sei $(u_i)_{i \in I}$ eine Basis von U. Wir ergänzen diese zu einer Basis $(u_i)_{i \in I \dot\cup J}$ von V. Setze $U' = \mathrm{Lin}((u_i)_{i \in J})$. Dann gilt $U \cap U' = \{0\}$, $U + U' = V$. □

Lemma 2.62. *Sei V ein Vektorraum, $U \subset V$ ein Untervektorraum und $U' \subset V$ ein Komplement zu U. Dann ist die natürliche Abbildung*

$$U \oplus U' \longrightarrow V, \quad (u, u') \mapsto u + u',$$

ein Isomorphismus. Insbesondere gilt $\dim V = \dim U + \dim U'$.

Beweis. Der Isomorphismus folgt aus 2.24, die Dimensionsformel aus 2.57. □

Satz 2.63 (Dimension des Faktorraums)**.** *Sei V ein endlich-dimensionaler Vektorraum und $U \subset V$ ein Untervektorraum. Dann ist V/U endlich-dimensional und es gilt*

$$\dim V/U = \dim V - \dim U.$$

Beweis. Sei U' ein Komplement zu U in V. Wir betrachten die zusammengesetzte Abbildung

$$\varphi : U' \xrightarrow{i} V \xrightarrow{p} V/U.$$

Behauptung: φ ist ein Isomorphismus.

Beweis der Behauptung: $\mathrm{Kern}(\varphi) = \mathrm{Kern}(p) \cap U' = U \cap U' = \{0\}$. Also ist φ injektiv. Sei nun $v + U \in V/U$ beliebig. Wegen $U + U' = V$ existiert $u \in U$ und $u' \in U'$ mit $u + u' = v$, also $u' + U = v + U$. Somit ist u' ein Urbild von $v + U$ unter φ, φ also surjektiv und damit ein Isomorphismus.

Insbesondere erhalten wir $\dim U' = \dim V/U$ und die Aussage folgt aus 2.62. □

Satz 2.64. *(Dimensionsformel für lineare Abbildungen). Ist $f : V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen Vektorräumen, so gilt*

$$\dim V = \dim(\mathrm{Kern}(f)) + \dim(\mathrm{Bild}(f)).$$

Beweis. Nach Satz 2.28 gilt $V/\mathrm{Kern}(f) \cong \mathrm{Bild}(f)$. Die Aussage folgt aus 2.63. □

Satz 2.65. *Seien U_1, U_2 Untervektorräume des endlich-dimensionalen Vektorraums U Dann gilt*

$$\dim U_1 + \dim U_2 = \dim(U_1 + U_2) + \dim(U_1 \cap U_2)$$

Beweis. Wir betrachten wie im Beweis von Lemma 2.24 die surjektive lineare Abbildung

$$\varphi : U_1 \oplus U_2 \longrightarrow U_1 + U_2,\ (u_1, u_2) \longmapsto u_1 + u_2.$$

Behauptung: Die Abbildung

$$i : U_1 \cap U_2 \longrightarrow \mathrm{Kern}(\varphi),\ u \longmapsto (u, -u),$$

ist ein Isomorphismus.

Beweis der Behauptung: Injektivität ist klar. Sei $(u_1, u_2) \in \mathrm{Kern}(\varphi)$. Dann gilt $u_1 = -u_2$, also $u_1 \in U_1 \cap U_2$. Setze $u = u_1$, dann gilt $i(u) = (u_1, u_2)$. Dies zeigt die Surjektivität.

Nach 2.64 gilt nun $\dim(U_1 \oplus U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$ und nach 2.57 gilt $\dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2$. Zusammen zeigt das die Aussage. □

2.5 Basen und lineare Abbildungen

Sei $f : V \to W$ eine lineare Abbildung und $(v_i)_{i \in I}$ eine Basis von V. Wir erhalten das System $(f(v_i))_{i \in I}$ von Vektoren in W. Umgekehrt gilt:

Satz 2.66. *Zu jedem System $(w_i)_{i\in I}$ von Vektoren in W gibt es eine eindeutig bestimmte lineare Abbildung $f : V \to W$ mit $w_i = f(v_i)$ für alle $i \in I$.*

Beweis. Jedes $v \in V$ hat eine eindeutige Darstellung $v = \sum_{i\in I} \alpha_i v_i$, $\alpha_i = 0$ f.f.a. i. Wegen der Eindeutigkeit der Darstellung ist die Abbildung

$$f : V \longrightarrow W,\ f(v) = \sum_{i\in I} \alpha_i w_i,$$

wohldefiniert, linear und hat die gewünschte Eigenschaft. Sind nun f_1, f_2 zwei lineare Abbildungen und $f_1(v_i) = w_i = f_2(v_i)$ für alle $i \in I$, so gilt für $v = \sum \alpha_i v_i$:

$$f_1(v) = \sum_{i\in I} \alpha_i f_1(v_i) = \sum \alpha_i w_i = \sum \alpha_i f_2(v_i) = f_2(\sum \alpha_i v_i) = f_2(v),$$

also $f_1 = f_2$. □

Korollar 2.67. *Für jeden Vektorraum V ist die kanonische Auswertungsabbildung $\varphi : V \to V^{**}$ injektiv.*

Beweis. Zu zeigen: $\mathrm{Kern}(\varphi) = 0$, d.h.: aus $f(u) = 0$ für alle $f \in V^*$ folgt $u = 0$. Sei $u \neq 0$. Nach dem Basisergänzungssatz 2.49 existiert eine Basis $(u_i)_{i\in I}$, die u enthält, d.h. $u_{i_0} = u$ für ein $i_0 \in I$. Wir definieren eine Linearform $f : V \to K$ durch $f(u_{i_0}) = 1$ und $f(u_i) = 0$ für $i \neq i_0$. Dann gilt $f(u) \neq 0$. □

Satz 2.68. *Ist V ein endlich-dimensionaler Vektorraum, so gilt* $\dim V = \dim V^*$.

Beweis. Sei $(v_1, \ldots, v_n)$ eine Basis von V. Seien $v_1^*, \ldots, v_n^* \in V^*$ definiert durch $v_i^*(v_j) = \delta_{ij}$, wobei $\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$ (Kroneckersymbol).

Behauptung: $(v_1^*, \ldots, v_n^*)$ ist eine Basis von V^*.
Beweis: Sei $\alpha_1 v_1^* + \cdots + \alpha_n v_n^*$ der Nullhomomorphismus $V \to K$. Zu zeigen: $\alpha_1 = \cdots = \alpha_n = 0$. Es gilt

$$\begin{aligned} \alpha_1 &= \alpha_1 + 0 + \cdots + 0 \\ &= \alpha_1 v_1^*(v_1) + \alpha_2 v_2^*(v_1) + \cdots + \alpha_n v_n^*(v_1) \\ &= (\alpha_1 v_1^* + \cdots + \alpha_n v_n^*)(v_1) = 0. \end{aligned}$$

Analog zeigt man $\alpha_2 = \cdots = \alpha_n = 0$, weshalb $(v_1^*, \ldots, v_n^*)$ ein linear unabhängiges System in V^* ist. Sei nun $f : V \to K$ beliebig und sei $f(v_i) = \alpha_i$, $i = 1, \ldots, n$. Dann gilt $f = \alpha_1 v_1^* + \cdots + \alpha_n v_n^*$, weil beide Seiten Linearformen auf V sind, die die gleichen Bilder auf den Basisvektoren $v_1, \ldots, v_n$ haben. □

Definition 2.69. Die eben definierte Basis $(v_1^*, \ldots, v_n^*)$ von V^* heißt die zur Basis $(v_1, \ldots, v_n)$ von V **duale Basis**.

Korollar 2.70. *Ist V ein endlich-dimensionaler Vektorraum, so ist die kanonische Auswertungsabbildung $\varphi : V \to V^{**}$ ein Isomorphismus.*

Beweis. Nach 2.67 ist φ injektiv. Nach 2.68 gilt

$$\dim V = \dim V^* = \dim V^{**}$$

Wegen 2.55 (i) ist φ ein Isomorphismus. □

Bemerkung 2.71. Für unendlich-dimensionale Vektorräume ist 2.70 falsch!

2.6 Der Rangsatz

Definition 2.72. Seien V, W endlich-dimensionale Vektorräume und $f : V \to W$ eine lineare Abbildung. Der **Rang von f** ist definiert durch

$$\mathrm{Rg}(f) = \dim(\mathrm{Bild}(f)).$$

Bemerkung 2.73. • $f = 0 \iff \mathrm{Rg}(f) = 0$.
• f surjektiv $\iff \mathrm{Rg}(f) = \dim W$.
I.A. gilt die Ungleichung

$$0 \leq \mathrm{Rg}(f) \leq \min(\dim V, \dim W).$$

Nun definiert f die duale Abbildung $f^* : W^* \to V^*$, $\varphi \mapsto \varphi \circ f$. Es gilt der

Satz 2.74 (Rangsatz)**.** *Sei $f : V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen Vektorräumen. Dann gilt*

$$\mathrm{Rg}(f) = \mathrm{Rg}(f^*)$$

Beweis. Es gilt

$$\mathrm{Rg}(f^*) = \dim(\mathrm{Bild}(f^*)) \overset{2.64}{=} \dim(W^*) - \dim(\mathrm{Kern}(f^*))$$

$$\overset{2.27}{=} \dim(W^*) - \dim((W/\mathrm{Bild}(f))^*) \overset{2.68}{=} \dim(W) - \dim(W/\mathrm{Bild}(f))$$

$$\overset{2.64}{=} \dim(W) - \dim(W) + \dim(\mathrm{Bild}(f)) = \mathrm{Rg}(f).$$ □

Kapitel 3

Matrizen und lineare Gleichungssysteme

Im ganzen Kapitel sei K ein fester Körper. Jeder endlich-dimensionale Vektorraum V über K ist isomorph zum K^n, $n = \dim V$. Der Isomorphismus ist unkanonisch und hängt von der Auswahl einer Basis ab (Lemma 2.39).

3.1 Matrizen

Definition 3.1. Eine $\boldsymbol{m \times n}$**-Matrix mit Einträgen in** $\boldsymbol{K}$ ist ein Schema

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \text{ mit } \quad a_{ij} \in K \text{ für } 1 \leq i \leq m,\ 1 \leq j \leq n.$$

Die Menge der $m \times n$-Matrizen über K wird mit $M_{m,n}(K)$ bezeichnet.

Definition 3.2. $M_{m,n}(K)$ wird zum K-Vektorraum durch

- $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$,
- $\alpha \cdot (a_{ij}) = (\alpha a_{ij})$, $\alpha \in K$.

Die $m \times n$ Matrix mit 0 an allen Stellen wird mit $0 \in M_{m,n}(K)$ bezeichnet. Üblicherweise identifiziert man K^n mit $M_{n,1}(K)$ durch

$$(a_1, \dots, a_n) \longmapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \text{ (Spaltenvektoren).}$$

Definition 3.3. (Matrixprodukt) Sind $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M_{m,n}(K)$ und $B = (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq k}} \in M_{n,k}(K)$ Matrizen, so heißt die Matrix

$$C = (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq k}} \in M_{m,k}(K) \text{ mit } c_{ij} = \sum_{s=1}^{n} a_{is} \cdot b_{sj}.$$

das **Produkt** der Matrizen A und B. Schreibweise: $C = A \cdot B$.

Beispiele 3.4.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \end{pmatrix}$$

$$(1\ 2) \begin{pmatrix} 5 \\ 5 \end{pmatrix} = (15)$$

Warnung: I.A. ist $B \cdot A$ nicht definiert und selbst im Fall $m = n = k$ gilt i.A. $A \cdot B \neq B \cdot A$!

Lemma 3.5. *Das Matrixprodukt ist assoziativ, d.h. für $A \in M_{m,n}(K)$, $B \in M_{n,k}(K)$, $C \in M_{k,l}(K)$ gilt*

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

Beweis. Ausrechnen ergibt, dass beide Seiten der behaupteten Gleichung $m \times l$-Matrizen sind, bei denen an der Stelle (i, j) der Wert

$$\sum_{s=1}^{n} \sum_{t=1}^{k} a_{is} b_{st} c_{tj}$$

steht. □

Identifizieren wir wie oben den K^n mit $M_{n,1}(K)$, so definiert die Multiplikation mit einer festen Matrix $A \in M_{m,n}(K)$ eine Abbildung

$$F_{m,n}(A) : K^n \to K^m.$$

Wir erhalten so eine Zuordnung

$$A \longmapsto F_{m,n}(A),$$

die jeder $m \times n$-Matrix eine Abbildung $K^n \to K^m$ zuordnet.

Satz 3.6. *Die eben definierte Zuordnung definiert einen Vektorraum-Isomorphismus*

$$F_{m,n} : M_{m,n}(K) \xrightarrow{\sim} \mathrm{Hom}_K(K^n, K^m).$$

Für $A \in M_{m,n}(K)$ und $B \in M_{n,k}(K)$, gilt

$$F_{m,k}(A \cdot B) = F_{m,n}(A) \circ F_{n,k}(B)$$

in $\mathrm{Hom}_K(K^k, K^m)$.

Beweis. 1.) $F_{m,n}(A)$ ist eine lineare Abbildung:

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + A\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}x_1 + a_{12}x_2 & +\cdots+ & a_{1n}x_n \\ \vdots & & \vdots \\ a_{m1}x_1 & +\cdots+ & a_{mn}x_n \end{pmatrix} + \begin{pmatrix} a_{11}y_1 + \cdots + a_{1n}y_n \\ \vdots \\ a_{m1}y_1 + \cdots + a_{mn}y_n \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}(x_1+y_1) & +\cdots+ & a_{1n}(x_n+y_n) \\ \vdots & & \vdots \\ a_{m1}(x_1+y_1) & +\cdots+ & a_{mn}(x_n+y_n) \end{pmatrix}$$

$$= A\begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix} = A\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right)$$

$$A\left(\alpha\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = A\begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix} = \begin{pmatrix} a_{11}\alpha x_1 & +\cdots+ & a_{1n}\alpha x_1 \\ & \vdots & \\ a_{m1}\alpha x_1 & +\cdots+ & a_{mn}\alpha x_n \end{pmatrix}$$
$$= \alpha\begin{pmatrix} a_{11}x_1 & +\cdots+ & a_{1n}x_n \\ \vdots & & \vdots \\ a_{m1}x_1 & +\cdots+ & a_{mn}x_n \end{pmatrix} = \alpha\, A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

2.) $F_{m,n} : M_{m,n}(K) \to \mathrm{Hom}_K(K^n, K^m)$ ist linear:

Man muss nachrechnen: $F_{m,n}(A+B) = F_{m,n}(A) + F_{m,n}(B)$ und $F_{m,n}(\alpha \cdot A) = \alpha F_{m,n}(A)$. Beide Gleichheiten von linearen Abbildungen zeigt man durch Einsetzen eines beliebigen Vektors $(x_1, \ldots, x_n) \in K^n$ und Anwendung der Definitionen. Dies sind einfache Rechnungen, ähnlich denen wie unter 1). Wir lassen das als Übung.

3.) Beobachtung: Für $1 \leq i \leq n$ gilt

$$F_{m,n}(A)(e_i) = A\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{-te Stelle} = \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{m,i} \end{pmatrix} = i\text{-te Spalte von A.}$$

Nun ist $(e_1, \ldots, e_n)$ eine Basis des K^n und nach 2.66 ist eine lineare Abbildung $\varphi : K^n \to K^m$ eindeutig durch das System $(\varphi(e_1), \ldots, \varphi(e_n))$ im K^m gegeben und umgekehrt. Daher ist $F_{m,n}$ ein Isomorphismus. Es verbleibt die Formel für die Komposition zu zeigen. Es genügt zu zeigen: für $i = 1, \ldots, k$ gilt

$$F_{m,k}(A \cdot B)(e_i) = F_{m,n}(A)(F_{n,k}(B)(e_i))$$

Linke Seite:
$F_{m,k}(A \cdot B)(e_i) = i$-te Spalte von $A \cdot B$

$$= \begin{pmatrix} a_{11}b_{1i} + a_{12}b_{2i} + \cdots + a_{1n}b_{ni} \\ \vdots \\ a_{m1}b_{1i} + a_{m2}b_{2i} + \cdots + a_{mn}b_{ni} \end{pmatrix}$$

Rechte Seite:
$A \cdot$ (i-te Spalte von B) = dasselbe. □

Korollar 3.7. *Für $m = n = k$ erhalten wir einen Isomorphismus unitärer Ringe*

$$F_{n,n} : M_{n,n}(K) \xrightarrow{\sim} \mathrm{End}_K(K^n).$$

Definition 3.8. Die Matrix $E_n = (\delta_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le n}}$ (also Einsen auf der Hauptdiagonale und sonst Nullen) heißt die **Einheitsmatrix vom Rang n**.

Bemerkungen 3.9.

- Es gilt $F_{n,n}(E_n) = \mathrm{id}_{K^n}$
- Eine $n \times n$ Matrix A heißt **invertierbar**, wenn eine $n \times n$ Matrix B mit $B \cdot A = E_n$ existiert. A ist dann und nur dann invertierbar, wenn $F_{n,n}(A)$ ein Automorphismus ist.
- Die Menge der invertierbaren $n \times n$-Matrizen wird mit $\mathrm{GL}_n(K)$ bezeichnet und bildet eine Gruppe bezüglich Matrixmultiplikation, die durch $F_{n,n}$ isomorph auf $\mathrm{GL}(K^n) = \mathrm{Aut}_K(K^n)$ abgebildet wird. Aus allgemeinen gruppentheoretischen Gründen (siehe 1.4) sehen wir, dass eine invertierbare Matrix A auch ein Rechtsinverses hat, welches mit dem Linksinversen übereinstimmt. Bezeichnung A^{-1}.
- Wir bezeichnen den zum Isomorphismus $F_{m,n}$ inversen Isomorphismus mit

  $$M_{m,n} : \mathrm{Hom}_K(K^n, K^m) \xrightarrow{\sim} M_{m,n}(K).$$

  Für eine lineare Abbildung $f : K^n \to K^m$ heißt $M_{m,n}(f) \in M_{m,n}(K)$ die **Darstellungsmatrix** (oder auch darstellende Matrix) von f.

Definition 3.10. Ein Diagramm von Vektorräumen und linearen Abbildungen heißt **kommutativ**, wenn jede Verbindung zwischen zwei Vektorräumen im Diagramm dieselbe Abbildung repräsentiert.

Beispiele 3.11. 1)

$$\begin{array}{ccc} U & \xrightarrow{f} & V \\ & \searrow^{h} & \downarrow{\scriptstyle g} \\ & & W \end{array}$$

ist kommutativ, falls $h = g \circ f$.

2.)

$$\begin{array}{ccc} U & \xrightarrow{f} & V \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle g} \\ W & \xrightarrow[\varphi]{} & S \end{array}$$

ist kommutativ, falls $g \circ f = \varphi \circ h$.

Seien nun V, W endlich-dimensionale Vektorräume, $n = \dim V$, $m = \dim W$ und $\underline{v} = (v_1, \ldots, v_n)$, $\underline{w} = (w_1, \ldots, w_m)$ Basen von V und W. Nach 2.39 erhalten wir Isomorphismen

$$\phi_{\underline{v}} : K^n \xrightarrow{\sim} V \ , \ (\alpha_1, \ldots, \alpha_n) \longmapsto \sum_{i=1}^{n} \alpha_i v_i,$$

$$\phi_{\underline{w}} : K^m \xrightarrow{\sim} W \ , \ (\beta_1, \ldots, \beta_m) \longmapsto \sum_{j=1}^{m} \beta_j w_j.$$

Für $A \in M_{m,n}(K)$ erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{F_{m,n}(A)} & K^m \\ {\scriptstyle \phi_{\underline{v}}}\downarrow\wr & & \wr\downarrow{\scriptstyle \phi_{\underline{w}}} \\ V & \xrightarrow[\phi_{\underline{w}} \circ F_{m,n}(A) \circ \phi_{\underline{v}}^{-1}]{} & W. \end{array}$$

Korollar 3.12. *Wir erhalten einen Isomorphismus von Vektorräumen*

$$\begin{array}{rcl} F_{\underline{w}}^{\underline{v}} : M_{m,n}(K) & \longrightarrow & \mathrm{Hom}_K(V, W) \\ A & \longmapsto & \phi_{\underline{w}} \circ F_{m,n}(A) \circ \phi_{\underline{v}}^{-1} \end{array}$$

Den inversen Isomorphismus bezeichnen wir mit

$$M_{\underline{w}}^{\underline{v}} : \mathrm{Hom}_K(V, W) \xrightarrow{\sim} M_{m,n}(K).$$

Bezeichnung: $M_{\underline{w}}^{\underline{v}}(f)$ heißt die, die lineare Abbildung f bzgl. der Basen $\underline{v} = (v_1, \ldots, v_n)$ und $\underline{w} = (w_1, \ldots, w_m)$ **darstellende Matrix**. Alternative Bezeichnungen: Darstellungsmatrix, Koordinatenmatrix.

Aus den Definitionen folgt für eine lineare Abbildung $f : V \to W$ das kommutative Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{F_{m,n}(M_{\underline{w}}^{\underline{v}}(f))} & K^m \\ {\scriptstyle \phi_{\underline{v}}}\downarrow\wr & & \wr\downarrow{\scriptstyle \phi_{\underline{w}}} \\ V & \xrightarrow[f]{} & W. \end{array}$$

Wechsel der Basen: Seien nun $\underline{v}' = (v_1', \ldots, v_n')$ und $\underline{w}' = (w_1', \ldots, w_m')$ andere Basen von V bzw. W. Wie ändert sich für eine lineare Abbildung $f : V \to W$ die repräsentierende Matrix?

Definition 3.13. Sind $\underline{v} = (v_1, \ldots, v_n)$ und $\underline{v}' = (v_1', \ldots, v_n')$ zwei Basen desselben Vektorraums V, so heißt die Matrix

$$T = M_{\underline{v}'}^{\underline{v}}(\mathrm{id}_V) \in M_{n,n}(K)$$

die **Transformationsmatrix** von $\underline{v}$ nach $\underline{v}'$.

Lemma 3.14. *T ist invertierbar. T^{-1} ist die Transformationsmatrix von $\underline{v}'$ zu $\underline{v}$.*

Beweis. Das Diagramm

$$\begin{array}{ccccc} K^n & \xrightarrow{F_{n,n}(M_{\underline{v}'}^{\underline{v}}(\mathrm{id}_V))} & K^n & \xrightarrow{F_{n,n}(M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V))} & K^n \\ {\scriptstyle \phi_{\underline{v}}}\downarrow\wr & & \wr\downarrow{\scriptstyle \phi_{\underline{v}'}} & & \wr\downarrow{\scriptstyle \phi_{\underline{v}}} \\ V & \xrightarrow[\mathrm{id}_V]{} & V & \xrightarrow[\mathrm{id}_V]{} & V. \end{array}$$

setzt sich aus zwei kommutativen Diagrammen zusammen und ist daher kommutativ. Daher gilt

$$\mathrm{id}_V \circ \mathrm{id}_V \circ \phi_{\underline{v}} = \phi_{\underline{v}} \circ F_{n,n}(M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V)) \circ F_{n,n}(M_{\underline{v}'}^{\underline{v}}(\mathrm{id}_V)).$$

Eine Anwendung von $\phi_{\underline{v}}^{-1}$ liefert

$$\mathrm{id}_{K^n} = F_{n,n}(M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V)) \circ F_{n,n}(M_{\underline{v}'}^{\underline{v}}(\mathrm{id}_V)).$$

Wegen $\mathrm{id}_{K^n} = F_{n,n}(E_n)$ und weil $F_{n,n}$ nach 3.7 ein Isomorphismus ist, folgt

$$E_n = M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V) \cdot M_{\underline{v}'}^{\underline{v}}(\mathrm{id}_V). \qquad \square$$

Bemerkung 3.15. Im Moment haben wir noch kein Verfahren zur Berechnung der inversen Matrix T^{-1} zur Hand. Diesem Problem widmen wir uns später.

Wir erinnern uns an das kommutative Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{F_{m,n}(M_{\underline{w}}^{\underline{v}}(f))} & K^m \\ {\scriptstyle \phi_{\underline{v}}}\downarrow\wr & & \wr\downarrow{\scriptstyle \phi_{\underline{w}}} \\ V & \xrightarrow[f]{} & W. \end{array}$$

Hieraus erkennen wir:

Lemma 3.16. *Ist $M_{\underline{w}}^{\underline{v}}(f) = (a_{ij}) \in M_{m,n}(K)$, so gilt für $j = 1, \ldots, n$:*

$$f(v_j) = a_{1,j}w_1 + \ldots + a_{m,j}w_m.$$

Beweis. In der j-ten Spalte der Matrix $M_{\underline{w}}^{\underline{v}}(f) = (a_{ij})$ steht das Bild des j-ten Basisvektors also der Vektor

$$F_{m,n}(M_{\underline{w}}^{\underline{v}}(f))(e_j) \in K^m.$$

Nun gilt $\phi_{\underline{v}}(e_j) = v_j$ und die Kommutativität des Diagramms zeigt

$$f(v_j) = \phi_{\underline{w}}(F_{m,n}(M_{\underline{w}}^{\underline{v}}(f))(e_j)) = \phi_{\underline{w}}(\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix})$$

$$= a_{1,j}w_1 + \ldots + a_{m,j}w_m. \qquad \square$$

Lemma 3.17. *Es seien U, V, W endlich-dimensionale Vektorräume $\underline{u} = (u_1, \ldots, u_n)$, $\underline{v} = (v_1, \ldots, v_m)$ und $\underline{w} = (w_1, \ldots, w_k)$ Basen von U, V und W und $f : U \to V$ und $g : V \to W$ lineare Abbildungen. Dann gilt:*

$$M_{\underline{w}}^{\underline{v}}(g) \cdot M_{\underline{v}}^{\underline{u}}(f) = M_{\underline{w}}^{\underline{u}}(g \circ f).$$

Beweis. Es sei $M_{\underline{w}}^{\underline{u}}(g \circ f) = (c_{i,j})$. Dann gilt:

$$g(f(u_j)) = c_{1,j}w_1 + \cdots + c_{k,j}w_k.$$

Setzt man $M_{\underline{v}}^{\underline{u}}(f) = (b_{i,j})$ und $M_{\underline{w}}^{\underline{v}}(g) = (a_{i,j})$, so gilt

$$f(u_j) = b_{1,j}v_1 + \cdots b_{m,j}v_m$$

und

$$g(v_i) = a_{1,i}w_1 + \ldots + a_{k,i}w_k.$$

Zusammen ergibt sich

$$g(f(u_j)) = g(b_{1,j}v_1 + \cdots b_{m,j}v_m) = b_{1,j}g(v_1) + \cdots + b_{m,j}g(v_m) =$$

$$b_{1,j}a_{1,1}w_1 + \cdots + b_{1,j}a_{k,1}w_k + b_{2,j}a_{1,2}w_1 + \cdots .$$

Wir erhalten durch Koeffizientenvergleich von $g(f(u_j))$ vor w_i für $i = 1, \ldots, k$, $j = 1, \ldots, n$

$$c_{i,j} = a_{i,1}b_{1,j} + \cdots + a_{i,m}b_{m,j}. \qquad \square$$

Satz 3.18. *(Basiswechselsatz). Seien V, W endlich-dimensionale Vektorräume und $f : V \to W$ eine lineare Abbildung. Seien $\underline{v} = (v_1, \ldots, v_n)$ und $\underline{v}' = (v_1', \ldots, v_n')$ zwei Basen von V und $T_1 \in M_{n,n}(K)$ die Transformationsmatrix. Seien weiterhin $\underline{w} = (w_1, \ldots, w_m)$ und $\underline{w}' = (w_1', \ldots, w_m')$ zwei Basen von W und T_2 die Transformationsmatrix. Dann gilt*

$$M_{\underline{w}'}^{\underline{v}'}(f) = T_2 \cdot M_{\underline{w}}^{\underline{v}}(f) \cdot T_1^{-1}$$

Beweis. Wir wenden 3.17 auf die Abbildungen

$$V \xrightarrow{\mathrm{id}_V} V \xrightarrow{f} W \xrightarrow{\mathrm{id}_W} W$$

und die Basen $\underline{v}'$, $\underline{v}$, $\underline{w}$, $\underline{w}'$ an und erhalten unter Verwendung von $T_1^{-1} = M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V)$ (siehe 3.14)

$$T_2 \cdot M_{\underline{w}}^{\underline{v}}(f) \cdot T_1^{-1} = M_{\underline{w}'}^{\underline{w}}(\mathrm{id}_W) \cdot M_{\underline{w}}^{\underline{v}}(f) \cdot M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V) =$$

$$M_{\underline{w}'}^{\underline{v}}(f) \cdot M_{\underline{v}}^{\underline{v}'}(\mathrm{id}_V) = M_{\underline{w}'}^{\underline{v}'}(f). \qquad \square$$

3.2 Ränge von Matrizen

Definition 3.19. Sei $A \in M_{m,n}(K)$ eine Matrix. Der **Zeilen-(bzw. Spalten-) rang** von A ist die Dimension des durch die Zeilen (bzw. Spalten) von A im K^n (bzw. im K^m) aufgespannten Untervektorraums.
Bezeichnung: $Z\,\mathrm{Rg}(A)$, $S\,\mathrm{Rg}(A)$.

Es spannen n Vektoren im K^m höchstens einen Vektorraum der Dimension $\min(m, n)$ auf. Daher gilt:

$$0 \leq Z\,\mathrm{Rg}(A), S\,\mathrm{Rg}(A) \leq \min(m, n).$$

Ziel dieses Abschnitts ist der Beweis von

Satz 3.20. *(Rangsatz für Matrizen). Für jede Matrix $A \in M_{m,n}(K)$ gilt*

$$Z\,\mathrm{Rg}(A) = S\,\mathrm{Rg}(A).$$

Danach werden wir die Notation $\mathrm{Rg}(A)$ für diese Zahl benutzen. Um den Rangsatz zu zeigen, beginnen wir mit

Lemma 3.21. *(i) Für $A \in M_{m,n}(K)$ gilt*

$$S\,\mathrm{Rg}(A) = \mathrm{Rg}(F_{m,n}(A)).$$

(ii) Seien V, W endlich-dimensionale Vektorräume, $n = \dim V$, $m = \dim W$, und $\underline{v} = (v_1, \ldots, v_n)$, $\underline{w} = (w_1, \ldots, w_m)$ Basen von V und W. Sei $f : V \to W$ ein Homomorphismus. Dann gilt

$$\mathrm{Rg}(f) = S\,\mathrm{Rg}(M^{\underline{v}}_{\underline{w}}(f)).$$

Beweis. (i) Die Spalten von A sind die Bilder der Basisvektoren $e_1, \ldots, e_n \in K^n$ unter $F_{m,n}(A)$. Diese Bilder spannen $F_{m,n}(A)(K^n)$ auf. Dies zeigt (i).
(ii) Aus dem kommutativen Diagramm

$$\begin{array}{ccc} K^n & \xrightarrow{F_{m,n}(M^{\underline{v}}_{\underline{w}}(f))} & K^m \\ {\scriptstyle \phi_{\underline{v}}}\downarrow\wr & & \wr\downarrow{\scriptstyle \phi_{\underline{w}}} \\ V & \xrightarrow[f]{} & W. \end{array}$$

folgt, dass die Einschränkung von $\phi_{\underline{w}}$ auf den Untervektorraum

$$\mathrm{Bild}(F_{m,n}(M^{\underline{v}}_{\underline{w}}(f))) \subset K^m$$

einen Isomorphismus

$$\mathrm{Bild}(F_{m,n}(M^{\underline{v}}_{\underline{w}}(f))) \xrightarrow{\sim} \mathrm{Bild}(f)$$

induziert. Insbesondere gilt

$$\mathrm{Rg}(f) = \mathrm{Rg}(F_{m,n}(M^{\underline{v}}_{\underline{w}}(f))) \overset{(i)}{=} S\,\mathrm{Rg}(M^{\underline{v}}_{\underline{w}}(f)). \qquad \square$$

Definition 3.22. Zu $A = (a_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \in M_{m,n}(K)$ definiert man die **transponierte Matrix** $A^t \in M_{n,m}(K)$ durch

$$A^t = (a_{ji})_{\substack{j=1,\ldots,n \\ i=1,\ldots,m}}.$$

Beispiel 3.23.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

$$(1,0,0)^t = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Bemerkung 3.24. Oft wird auch die Bezeichnung ${}^tA$ anstelle von A^t verwendet. Offenbar gilt:

$$Z\,\mathrm{Rg}(A) = S\,\mathrm{Rg}(A^t).$$

Für $A \in M_{m,n}(K)$, $B \in M_{n,k}(K)$ gilt

$$(A \cdot B)^t = B^t \cdot A^t \in M_{k,m}(K).$$

Erinnerung: Ist V ein endlich-dimensionaler Vektorraum mit Basis $\underline{v} = (v_1, \ldots, v_n)$, so hat der duale Vektorraum $V^* = \mathrm{Hom}_K(V, K)$ die duale Basis $\underline{v}^* = (v_1^*, \ldots, v_n^*)$, die durch $v_i^*(v_j) = \delta_{ij}$ gegeben ist.

Eine lineare Abbildung $f : V \to W$ induziert die duale Abbildung $f^* : W^* \to V^*$ die durch $f^*(\varphi) = \varphi \circ f$ gegeben ist. Für $V \xrightarrow{f} W \xrightarrow{g} U$ gilt $(g \circ f)^* = f^* \circ g^* : U^* \to V^*$.

Lemma 3.25. *Seien V, W endlich-dimensionale Vektorräume mit Basen $\underline{v} = (v_1, \ldots, v_n)$, $\underline{w} = (w_1, \ldots, w_m)$. Dann gilt für jede lineare Abbildung $f : V \to W$:*

$$M_{\underline{v}^*}^{\underline{w}^*}(f^*) = (M_{\underline{w}}^{\underline{v}}(f))^t \in M_{n,m}(K). \qquad (*)$$

Beweis. Sei $M_{\underline{w}}^{\underline{v}}(f) = (a_{ij}) \in M_{m,n}(K)$, d.h. für $i = 1, \ldots, n$ gilt

$$f(v_i) = a_{1i}w_1 + \cdots + a_{mi}w_m.$$

Die Spalten der Matrix auf der linken Seite von $(*)$ sind die Koordinaten von $f^*(w_1^*), \ldots, f^*(w_m^*) \in V^*$ bzgl. der Basis $(v_1^*, \ldots, v_n^*)$. Um Gleichheit mit $(a_{ij})^t$ zu zeigen, ist daher für jedes $1 \le j \le m$ die Identität

$$f^*(w_j^*) = a_{j1}v_1^* + \cdots + a_{jn}v_n^* \qquad (**)$$

zu zeigen. Beide Seiten von $(**)$ sind Linearformen auf V, d.h. Elemente in $V^* = \mathrm{Hom}_K(V, K)$. Es genügt daher zu zeigen, dass für alle i, $1 \le i \le n$, gilt

$$f^*(w_j^*)(v_i) = (a_{j1}v_1^* + \cdots + a_{jn}v_n^*)(v_i) = a_{ji}.$$

Nach Definition ist $f^*(w_j^*)$ die Komposition $V \xrightarrow{f} W \xrightarrow{w_j^*} K$. Daher gilt

$$\begin{aligned} f^*(w_j^*)(v_i) = w_j^*(f(v_i)) &= w_j^*(a_{1i}w_1 + \cdots + a_{mi}w_m) \\ &= a_{ji}. \end{aligned}$$

□

Beweis des Rangsatzes für Matrizen 3.20. Wir betrachten die Abbildung

$$f = F_{m,n}(A) : K^n \longrightarrow K^m.$$

Nach 3.25 wird $f^* : (K^m)^* \to (K^n)^*$ bezüglich der zu den kanonischen Basen dualen Basen $(e_1^*, \ldots, e_m^*)$ von $(K^m)^*$ und $(e_1^*, \ldots, e_n^*)$ von $(K^n)^*$ durch die transponierte Matrix A^t dargestellt.
Der Rangsatz für lineare Abbildungen 2.74 und 3.21 zeigen uns daher

$$S\,\mathrm{Rg}(A) = \mathrm{Rg}\, f = \mathrm{Rg}\, f^* = S\,\mathrm{Rg}(A^t) = Z\,\mathrm{Rg}(A). \qquad \square$$

Korollar 3.26. *Für eine Matrix $A \in M_{n,n}(K)$ sind die folgenden Aussagen äquivalent*

(i) A ist invertierbar, d.h. $A \in \mathrm{GL}_n(K)$
(ii) die Zeilen von A bilden eine Basis des K^n
(iii) die Spalten von A bilden eine Basis des K^n
(iv) $\mathrm{Rg}(A) = n$.

Beweis. Die Äquivalenz (ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv) folgt aus dem Rangsatz. Schließlich gilt

A invertierbar $\iff F_{n,n}(A)$ ist bijektiv
$\overset{2.56}{\iff} F_{n,n}(A)$ ist surjektiv $\iff \mathrm{Rg}(A) = n$. □

Korollar 3.27. *Ist $A \in M_{m,n}(K)$ und $T \in \mathrm{GL}_n(K)$, $S \in \mathrm{GL}_m(K)$, so gilt*

$$\mathrm{Rg}(A) = \mathrm{Rg}(SAT).$$

Beweis. Sei $f = F_{m,n}(A) : K^n \to K^m$. Sei $\underline{w} = (w_1, \ldots, w_m)$ die durch die Spalten von S^{-1} gegebene Basis des K^m und $\underline{v} = (v_1, \ldots, v_n)$ die durch die Spalten von T gegebene Basis des K^n. Dann ist S die Transformationsmatrix von $(e_1, \ldots, e_m)$ zu $(w_1, \ldots, w_m)$ im K^m (interpretiere die Gleichung $SS^{-1} = E_m$) und T^{-1} die Transformationsmatrix von $(e_1, \ldots, e_n)$ zu $(v_1, \ldots, v_n)$ im K^n. Nach 3.18 gilt

$$\begin{aligned} M^{\underline{v}}_{\underline{w}}(f) &= SA(T^{-1})^{-1} \\ &= SAT \end{aligned}$$

und deshalb nach 3.21

$$\mathrm{Rg}(A) = \mathrm{Rg}(f) = \mathrm{Rg}(SAT).$$ □

Korollar 3.28. *Sei $A \in M_{m,n}(K)$ und $r = \mathrm{Rg}(A)$. Dann gibt es eine invertierbare $r \times r$ Untermatrix von A, d.h. Indizes $1 \le i_1 < \cdots < i_r \le m$, $1 \le j_1 < \cdots < j_r \le n$, so dass die Matrix*

$$\tilde{A} = (a_{ij})_{\substack{i \in \{i_1, \ldots, i_r\} \\ j \in \{j_1, \ldots, j_r\}}}$$

invertierbar ist. Umgekehrt folgt aus der Existenz einer invertierbaren $s \times s$ Untermatrix, dass $s \le r$ gilt.

Beweis. Wähle r Zeilen aus, dass diese eine Basis des (r-dimensionalen) von den Zeilen von A im K^n aufgespannten Untervektorraums bilden. Dann streiche die anderen Zeilen. Die so erhaltene Matrix hat Rang r. Dann wähle r linear unabhängige Spalten aus und erhalte eine $r \times r$-Matrix mit Rang $= r$. Diese ist invertierbar nach 3.26.
Umgekehrt: Ist A' eine invertierbare $s \times s$ Untermatrix von A, so sind die Spalten von A' linear unabhängig, also auch die s-vielen Spalten von A, die A' treffen. Daher gilt $r \ge s$. □

Satz 3.29. *Sei $f : V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen Vektorräumen, $n = \dim V$, $m = \dim W$, $r = \mathrm{Rg}(f)$.*

Dann gibt es Basen $\underline{v} = (v_1, \ldots, v_n)$, $\underline{w} = (w_1, \ldots, w_m)$ von V und W, so dass

$$M_{\underline{w}}^{\underline{v}}(f) = \left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right) \in M_{m,n}(K).$$

Beweis. $\mathrm{Rg}(f) = \mathrm{Rg}(M^{\text{irgendeine Basis}}_{\text{irgendeine Basis}}(f)) \leq \min(n, m)$.

Es gilt $r = \dim f(V) \overset{2.64}{=} \dim(V) - \dim \mathrm{Kern}(f)$ also $\dim \mathrm{Kern}(f) = n - r$.

Sei $U \subset V$ ein Komplement zu $\mathrm{Kern}(f)$ (siehe 2.61). Nach 2.62 gilt $U \oplus \mathrm{Kern}(f) \cong V$, daher können wir eine Basis $(v_1, \ldots, v_n)$ von V wählen, so dass $\mathrm{Lin}(v_1, \ldots, v_r) = U$ und $\mathrm{Lin}(v_{r+1}, \ldots, v_n) = \mathrm{Kern}(f)$ gilt. Die eingeschränkte Abbildung $f|_U : U \to W$ ist wegen $U \cap \mathrm{Kern}(f) = \{0\}$ injektiv. Setze nun $w_i = f(v_i)$ für $i = 1, \ldots, r$ und wähle $w_{r+1}, \ldots, w_m$ so dass $(w_1, \ldots, w_m)$ eine Basis von W ist. Dann ist die Darstellungsmatrix von f bezüglich der Basen $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_m)$ von der gewünschten Form. □

Korollar 3.30. *Sei $A \in M_{m,n}(K)$ und $r = \mathrm{Rg}(A)$. Dann existieren Matrizen $S \in \mathrm{GL}_m(K)$, $T \in \mathrm{GL}_n(K)$ mit*

$$SAT = \left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right) \in M_{m,n}(K).$$

Beweis. Wende 3.29 auf $F_{m,n}(A) : K^n \to K^m$ und den Basiswechselsatz 3.18 an. □

3.3 Gauß-Elimination

Aufgabe: $v_1, \ldots, v_m \in K^n$ seien gegeben. Berechne eine Basis von $\mathrm{Lin}(v_1, \ldots, v_m)$!

Definition 3.31. Zwei Tupel $(v_1, \ldots, v_m)$ und $(w_1, \ldots, w_k)$ von Vektoren im K^n heißen **linear äquivalent**, wenn $\mathrm{Lin}(v_1, \ldots, v_m) = \mathrm{Lin}(w_1, \ldots, w_k)$ gilt. Man setzt:

$$\mathrm{Rg}(v_1, \ldots, v_m) = \dim \mathrm{Lin}(v_1, \ldots, v_m).$$

Die folgenden Operationen heißen **Zeilen-Umformungen**. Mit ihrer Hilfe erhält man aus einem Tupel von Vektoren ein linear äquivalentes Tupel:

(i) Multiplikation von v_i mit $\lambda \neq 0$ für ein i
(ii) Ersetzen von v_i durch $v_i + \lambda v_j$, $i \neq j$
(iii) Vertauschen der v_i
(iv) Streichen von v_i, wenn $v_i = 0$.

(Nullvektoren sind entbehrlich, die anderen Operationen sind umkehrbar.)

Bemerkung 3.32. Schreibt man $v_1, \ldots, v_m$ in der Form

$$\begin{array}{rcl} v_1 & = & (a_{11}, \ldots, a_{1n}) \\ & \vdots & \\ v_m & = & (a_{m1}, \ldots, a_{mn}) \end{array}$$

so bewirken die Operationen (i), (ii), (iii) auf der $m \times n$-Matrix $A = (a_{ij})$ das folgende:
(i) Multiplikation von links mit der $m \times m$-Matrix $E_i(\lambda)$, die definiert ist durch

$$E_i(\lambda)_{k,\ell} = \begin{cases} 0 & k \neq \ell \\ 1 & k = \ell \neq i \\ \lambda & k = \ell = i \end{cases}, \text{ d.h. } E_i(\lambda) := \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

($\lambda \neq 0$ steht an der Stelle (i,i)).
(ii) Multiplikation von links mit der $m \times m$ Matrix $E_{ij}(\lambda)$, die definiert ist durch

$$E_{i,j}(\lambda)_{k,\ell} = \begin{cases} 1 & k = \ell \\ \lambda & k = i \text{ und } \ell = j \\ 0 & \text{sonst.} \end{cases},$$

$$\text{d.h. } E_{i,j}(\lambda) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ \lambda & & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \end{pmatrix}$$

λ steht an der Stelle (i,j), $(i \neq j)$.
(iii) Multiplikation von links mit der $m \times m$-Matrix P_{ij}, die gegeben ist durch

$$(P_{i,j})_{k,\ell} = \begin{cases} 1 & (k,\ell) = (i,j) \text{ oder } (j,i) \\ 1 & i \neq k = \ell \neq j \\ 0 & \text{sonst.} \end{cases}$$

(vertausche i-te und j-te Zeile in E_m).

$$P_{ij} = \begin{array}{c} \\ \\ j \\ \\ i \\ \\ \\ \\ \end{array} \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \hline & & 0 & & & 1 & \\ \hline & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ \hline & & 1 & & & 0 & \\ \hline & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}$$

$$\begin{array}{cccccc} & & & & & \\ & & j & & & i \end{array}$$

Definition 3.33. Eine $m \times n$-Matrix A hat **Zeilenstufenform**, wenn es ganze Zahlen $0 \leq r \leq m$, $1 \leq j_1 < \cdots < j_r \leq n$ gibt, so dass gilt

(1) $a_{ij} = 0$ falls $i > r$ oder falls $i \leq r$ und $j < j_i$.
(2) $a_{ij_i} = 1$ für alle $1 \leq i \leq r$.

Man sagt dass A **strenge Zeilenstufenform** hat, wenn dazu noch gilt

(3) $a_{ij_k} = 0$ für alle $1 \leq k \leq r$, $k \neq i$.

Bild für strenge Zeilenstufenform:

$$\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} j_1 & & j_2 & & j_r \end{array} \\ \begin{pmatrix} 0 \cdots 0 & 1 * \cdots * & 0 * \cdots * & & 0 * \cdots * \\ & & 1 * \cdots * & & 0 * \cdots * \\ & & & & 0 * \cdots * \\ & & & \cdots & \vdots \quad \vdots \quad \vdots \\ & & & & 0 * \cdots * \\ & & & & 1 * \cdots * \end{pmatrix} \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \left.\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right\} r$$

Satz 3.34 (Gauß-Elimination)**.** *Durch Zeilenumformungen (i), (ii), (iii) kann man jede $(m \times n)$-Matrix in strenge Zeilenstufenform bringen.*

Beweis. Die j-te Spalte sei die erste, die nicht nur aus Nullen besteht. $j_1 = j$
1) Heraufbringen: Ein Zeilentausch (iii) bringt $a_{1j} \neq 0$
2) Normieren: Anwenden von (i) bewirkt $a_{1j} = 1$
3) Ausräumen: Durch Ersetzen von v_i, $i \neq 1$, durch $v_i - a_{ij}v_1$ erhält die Matrix bis zur j-ten Spalte die gewünschte Form
Jetzt betrachte die Matrix ohne die erste Zeile und wähle j_2. Mache Schritt 1, 2, 3 und beachte, dass sich auch in Schritt 3 der wesentliche Teil der ursprünglich ersten Zeile nicht ändert usw. □

Beispiel 3.35. Sei $\mathrm{char}(K) \neq 2$

$$\begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \xrightarrow{(i)} \begin{pmatrix} 1 & 2 & 1 & 3 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \xrightarrow{(ii)} \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 \end{pmatrix}$$

$$\xrightarrow{(iii)} \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{(ii)} \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Satz 3.36. *Der von Vektoren $v_1, \ldots, v_m$ im K^n erzeugte Untervektorraum ist durch die strenge Stufe eindeutig bestimmt und umgekehrt.*

D.h.: gilt $\mathrm{Lin}(v_1, \ldots, v_m) = \mathrm{Lin}(w_1, \ldots, w_k)$ so unterscheiden sich die strengen Zeilenstufenmatrizen nur um 0-Zeilen unterhalb der Stufe.

Beweis. Sei $U = \mathrm{Lin}(v_1, \ldots, v_m)$ und $r := \dim U$. Dann ist $U = \mathrm{Lin}(v'_1, \ldots, v'_r)$ wobei $v'_1, \ldots, v'_r$ die ersten r-Zeilen der assoziierten Matrix in strenger Zeilenstufenform sind.
Seien nun $(v_1, \ldots, v_m)$ und $(w_1, \ldots, w_k)$ mit $\mathrm{Lin}(v_1, \ldots, v_m) = \mathrm{Lin}(w_1, \ldots, w_k)$ gegeben und seien $A \in M_{m,n}(K)$ und $B \in M_{k,n}(K)$ die strengen Zeilenstufenformen der assoziierten Matrizen. Wegen $\mathrm{Rg}(A) = \dim U = \mathrm{Rg}(B)$ sind bei A und B die i-ten Zeilen mit $i > r = \dim U$ alle Null.
Betrachten wir für $1 \leq j \leq n$ die Projektionen $p_j : K^n \to K^j$, $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_j)$, so sind die Stufen bei A wie bei B gerade die Indizes j, mit $\dim p_j(U) > \dim p_{j-1}(U)$. Daher stimmen die Stufenindizes $j_1, \ldots, j_r$ für A und B überein, d.h. die Stufen bei A und B haben dieselbe geometrische Form.

Seien nun $a_1 = (a_{11}, \ldots, a_{1n}), \ldots, a_r = (a_{r1}, \ldots, a_{rn})$ die ersten r-Zeilen von A und $b_1 = (b_{11}, \ldots, b_{1n}), \ldots, b_r = (b_{r1}, \ldots, b_{rn})$ die ersten r-Zeilen von B. Es sind $(a_1, \ldots, a_r)$ und $(b_1, \ldots, b_r)$ beides Basen von U.

Schreiben wir nun $a_j = \sum_{i=1}^{r} \lambda_{ij} b_i$, so ist (weil die j_i-te Spalte von B genau eine 1 bei (i, j_i) hat) $\lambda_{ij} = a_{jj_i}$. Aber A ist in strenger Zeilenstufenform, also $a_{jj_i} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$. Hieraus folgt $\lambda_{ij} = 0$, falls $i \neq j$, und $= 1$, falls $i = j$, und damit $a_j = b_j$ für $j = 1, \ldots, r$. □

Berechnung der inversen Matrix

Ist $A \in \mathrm{GL}_n(K)$, d.h. $A \in M_{n,n}(K)$ und $n = \mathrm{Rg}(A)$, so ist die strenge Zeilenstufenform von A die Einheitsmatrix E_n. Dies gibt die folgende Methode zur Berechnung von A^{-1}:

Führe die gleichen Operationen die A auf strenge Zeilenstufenform (d.h. auf E_n) bringen mit E_n aus. Das Ergebnis ist A^{-1}.
Begründung: Jede der Operationen (i), (ii) und (iii) entspricht der Linksmultiplikation mit einer Matrix. Ist M das (von rechts nach links gebildete) Produkt dieser Matrizen, so gilt $M \cdot A = E_n$, also $M = A^{-1}$. Wegen $M \cdot E_n = M$ entsteht M durch die entsprechenden Manipulationen an E_n.

Beispiel 3.37. Suche $\begin{pmatrix} 2 & 0 & -1 \\ -1 & -1 & 2 \\ 0 & 1 & -1 \end{pmatrix}^{-1}$ wenn $\mathrm{char}(K) \neq 2$, d.h. $\frac{1}{2} \in K$:

$$\left(\begin{array}{ccc|ccc} 2 & 0 & -1 & 1 & 0 & 0 \\ -1 & -1 & 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ -1 & -1 & 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & -1 & \frac{3}{2} & \frac{1}{2} & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -\frac{3}{2} & -\frac{1}{2} & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -\frac{3}{2} & -\frac{1}{2} & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 1 & -\frac{3}{2} & -\frac{1}{2} & -1 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & -\frac{3}{2} & -\frac{1}{2} & -1 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{array}\right)$$
$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{array}\right)$$

Also gilt $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 & -1 \\ -1 & -1 & 2 \\ 0 & 1 & -1 \end{pmatrix} = E_3$.

und das gilt auch in $\mathrm{char}(K) = 2$ (wie man durch Ausmultiplizieren einsieht).

Beispiel 3.38. Suche $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 3 & 1 & 1 \end{pmatrix}^{-1}$ wenn $\mathrm{char}(K) \neq 2$:

$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 3 & 1 & 1 \end{array}\right) \left| \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)\right.$$
$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & -2 & -2 \\ 0 & -2 & -2 \end{array}\right) \left| \left(\begin{array}{ccc} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{array}\right)\right.$$
$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & -2 & -2 \end{array}\right) \left| \left(\begin{array}{ccc} 1 & 0 & 0 \\ 1 & -\frac{1}{2} & 0 \\ -3 & 0 & 1 \end{array}\right)\right.$$
$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{array}\right) \left| \left(\begin{array}{ccc} 0 & \frac{1}{2} & 0 \\ 1 & -\frac{1}{2} & 0 \\ -1 & -1 & 0 \end{array}\right)\right.$$

Der Prozess bricht ab. Matrix nicht invertierbar da der Rang gleich $2 < 3$ ist. Wenn $\mathrm{char} K = 2$:

$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 2 & 0 & 0 \\ 3 & 1 & 1 \end{array}\right) = \left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{array}\right)$$
$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{array}\right) \left| \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)\right.$$
$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right) \left| \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right)\right.$$

bricht ab, der Rang ist 1.

Berechnen der dualen Basis.

Elemente des Dualraums $(K^n)^*$ sind Linearformen auf K^n. Die kanonische Basis des $(K^n)^*$ ist durch die zur kanonischen Basis $(e_1, \ldots, e_n)$ des K^n duale Basis $(e_1^*, \ldots, e_n^*)$ gegeben. Wie vorher schreiben wir Elemente des K^n als Spaltenvektoren (d.h. $(n\times 1)$-Matrizen). Jeder Zeilenvektor (d.h. $(1\times n)$-Matrix) $(a_1, \ldots, a_n)$ definiert mit Hilfe der Matrixmultiplikation $M_{1,n}(K) \times M_{n,1}(K) \to M_{1,1}(K) = K$ durch

$$(x_1, \ldots, x_n)^t \longmapsto (a_1, \ldots, a_n) \cdot (x_1, \ldots, x_n)^t = a_1 x_1 + \cdots + a_n x_n \in K$$

ein Element von $(K^n)^*$. Es gilt

$$(1, 0, \ldots, 0) = e_1^*, \ \ldots \ , (0, \ldots, 0, 1) = e_n^*.$$

Daher lässt sich die Linearform $\varphi = a_1 e_1^* + \cdots + a_n e_n^*$ durch den Zeilenvektor $(a_1, \ldots, a_n)$ darstellen, mit anderen Worten: wir können den $(K^n)^*$ mit dem Vektorraum der Zeilenvektoren der Länge n identifizieren.

Sei nun $(v_1, \ldots, v_n)$ eine Basis des K^n und $(v_1^*, \ldots, v_n^*)$ die duale Basis des $(K^n)^*$. Die Zeilenvektorform der dualen Basis berechnet man wie folgt:

- bilde die Matrix A deren i-te Spalte gleich v_i ist.
- die i-te Zeile von A^{-1} ist v_i^*.

Begründung: v_i^* ist durch $v_i^*(v_j) = \delta_{ij}$ charakterisiert. D.h. für den als Zeile geschriebenen Vektor v_i^* gilt: $v_i^* \cdot v_j = \delta_{ij}$. Bildet man die Matrix B mit den v_i^* als Zeilen, so gilt $B \cdot A = E_n$, also $B = A^{-1}$.

Basisergänzung
Seien $(v_1, \ldots, v_k)$ linear unabhängige Vektoren im K^n und $(w_1, \ldots, w_m)$ ein Erzeugendensystem. Wir suchen Indizes $1 \leq j(1) < \cdots < j(s) \leq m$, $s = n - k$, so dass

$$(v_1, \ldots, v_k, w_{j(1)}, \ldots, w_{j(s)})$$

eine Basis ist (diese Indizes existieren nach 2.49).

Das machen wir wie folgt: Wir bringen die Matrix A mit Zeilenvektoren v_1, …, v_k, w_1, …, w_m auf strenge Zeilenstufenform. Hierbei musste (evtl.) mehrere Male der Schritt 1 (Heraufbringen)des Algorithmus von 3.34 durchgeführt werden. Wir gehen dabei so vor, dass der notwendige Zeilentausch stets mit der Zeile ausgeführt wird, die am weitesten oben steht und einen nicht verschwindenden Eintrag in der untersuchten Spalte hat. Dann gilt: Unter den ersten n Zeilen sind $s = n - k$ Stück, die ursprünglich zu einem Zeilenvektor $w_{j(i)}$ gehörten $(i = 1, \ldots, s)$. Dies liefert die gesuchten $j(i)$.

Lineares Komplement
Gegeben $U = \mathrm{Lin}(v_1, \ldots, v_m) \subset K^n$.
Gesucht: $U' \subset K^n$ mit $U \cap U' = \{0\}$ und $U + U' = K^n$ und eine Basis von U'.
Methode: Forme die Matrix mit Zeilen $v_1, \ldots, v_m$ in strenge Zeilenstufenform um. Die von 0 verschiedenen Zeilen sind eine Basis von U. Die Einheitsvektoren e_j, wobei j kein Stufenindex ist (das sind $n - \dim(U)$ viele Indizes) sind dann Basis eines Teilraums U' mit $U \cap U' = \{0\}$, $U + U' = K^n$.

Von jetzt ab Notationsvereinfachung:

Wir identifizieren eine $m \times n$ Matrix direkt mit der assoziierten linearen Abbildung $K^n \to K^m$ und umgekehrt.

3.4 Lineare Gleichungssysteme

Ein lineares Gleichungssystem ist ein System von Gleichungen

$$\begin{array}{ccccc} a_{11}x_1 + a_{12}x_2 & + \cdots + & a_{1n}x_n = & b_1 & \\ \vdots & & \vdots & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 & + \cdots + & a_{mn}x_n = & b_m & \end{array} \qquad (*)$$

$(*)$ heißt **homogen**, wenn alle $b_i = 0$ sind, ansonsten **inhomogen**. Ist $(*)$ inhomogen, so nenne man das System $(**)$ mit den gleichen a_{ij} und rechts überall Nullen das **zugehörige homogene System**. Wir schreiben $(*)$ in der Form

$$A \cdot x = b$$

mit $A = (a_{ij})$, $x = (x_1, \ldots, x_n)^t$, $b = (b_1, \ldots, b_m)^t$.

Satz 3.39. *Die Menge der Lösungen $x \in K^n$ des homogenen Gleichungssystems*

$$Ax = 0 \qquad (**)$$

ist ein Untervektorraum des K^n. Seine Dimension ist gleich $n - \mathrm{Rg}(A)$.

Beweis. Offensichtlich ist die Lösungsmenge gleich dem Kern von A. Die Aussage über die Dimension folgt aus 2.64 sowie aus $\mathrm{Rg}(A) = \dim(\mathrm{Bild}(A))$. □

Korollar 3.40. *Die folgenden Aussagen sind äquivalent:*

(i) $\mathrm{Rg}(A) = n$.

(ii) *A ist invertierbar.*

(iii) *Das homogene System $(**)$ hat genau die triviale Lösung $x = (0, \ldots, 0) \in K^n$.*

Beweis. (i) $\Leftrightarrow$ (ii) haben wir schon in 3.26 gesehen. (i) $\Leftrightarrow$ (iii) folgt aus 3.39. □

Definition 3.41. Eine Teilmenge A eines Vektorraums V heißt **affiner Teilraum**, wenn es ein $v \in V$ und einen Untervektorraum $U \subset V$ gibt so dass

$$A = v + U = \{v + u \mid u \in U\}$$

gilt.

Bemerkung: Ein affiner Teilraum ist ein Element in V/U, wobei U ein Untervektorraum von V ist.

Beispiel. Die affinen Unterräume des $\mathbb{R}^2$ sind: der ganze $\mathbb{R}^2$, alle Geraden (nicht notwendig durch den Ursprung) und alle Punkte.

Lemma 3.42. *Ist $A \subset V$ ein affiner Teilraum, so gibt es genau einen Untervektorraum U mit der Eigenschaft $A = v + U$ für ein $v \in V$.*

Beweis. Ein solcher Untervektorraum U existiert nach Definition. Sei $A = v_0 + U_0 = v_1 + U_1$. Dann gilt

$$U_0 = \{a - a' \mid a, a' \in A\} = U_1. \qquad \square$$

Definition 3.43. Ist $A \subset V$ ein affiner Teilraum, so setzt man

$$\dim A := \dim U,$$

wobei U der nach 3.42 eindeutig bestimmte Untervektorraum mit $A = v + U$ ist.

Satz 3.44. *Für das inhomogene Gleichungssystem $Ax = b \quad (*)$ gibt es genau die beiden folgenden Möglichkeiten:*

(i) *$b \notin \mathrm{Bild}(A)$ und die Lösungsmenge L von $(*)$ ist leer.*

(ii) *$b \in \mathrm{Bild}(A)$. Dann ist die Lösungsmenge L ein affiner Teilraum des K^n der Dimension $n - \mathrm{Rg}(A)$. Ist $v_0 \in L$ eine Lösung von $(*)$, so gilt*

$$L = v_0 + U,$$

wobei U der Lösungsraum des zugehörigen homogenen Systems

$$Ax = 0 \qquad (**)$$

ist.

Beweis. Es gilt nach Definition $b \notin \mathrm{Bild}(A) \Longleftrightarrow L = \emptyset$. Ist $b \in \mathrm{Bild}(A)$ so gibt es eine Lösung $v_0 \in K^n$ mit $Av_0 = b$. Sei $U = \mathrm{Kern}(A)$ die Lösungsmenge von $(**)$. Für $u \in U$ gilt $A(v_0 + u) = Av_0 + Au = b + 0 = b$, also $v_0 + U \subset L$. Andererseits sei $v \in L$, d.h. $Av = b$. Dann gilt für $u = v - v_0$: $Au = Av - Av_0 = b - b = 0$, also $u \in U$ und $v = v_0 + u$. Daher gilt auch $L \subset v_0 + U$. Schließlich gilt

$$\dim L = \dim U = n - \mathrm{Rg}(A). \qquad \square$$

Korollar 3.45. *Das inhomogene System $(*)$ hat genau dann eine Lösung wenn*

$$\mathrm{Rg}(A) = \mathrm{Rg}(A|b)$$

gilt. Hier ist $(A|b)$ die $m \times (n+1)$ Matrix, die durch Anfügen von b an A als $(n+1)$-te Spalte entsteht.

Beweis. $\mathrm{Rg}(A) = \mathrm{Rg}(A|b) \Longleftrightarrow b \in \mathrm{Lin}(\text{Spalten von } A) \Longleftrightarrow b \in \mathrm{Bild}(A)$. $\square$

3.5 Explizite Lösung linearer Gleichungssysteme

Wir betrachten das homogene System

$$Ax = 0. \qquad (*)$$

Das Ausführen von Zeilenumformungen (i)–(iii) ändert den Lösungsraum $\mathrm{Kern}(A)$ nicht (z.B. weil diese Umformungen der Multiplikation von links und invertierbaren Matrizen entspricht).
Daher erhalten wir folgendes Verfahren:

1. Schritt: Bringe A auf strenge Zeilenstufenform.
2. Schritt: Sei nun S die strenge Zeilenstufenform von A:

$$S = \begin{array}{c} \begin{array}{ccccccc} & & j_1 & & j_2 & & j_r \end{array} \\ \left(\begin{array}{ccccccc} 0 \cdots 0 & \vline & 1 * \cdots * & & 0 * \cdots * & & 0 * \cdots * \\ & & \multicolumn{1}{|}{\underline{}} & & 1 * \cdots * & & 0 * \cdots * \\ & & & & \multicolumn{1}{|}{\underline{}} & & 0 * \cdots * \\ & & & \cdots & & & \vdots \quad \vdots \quad \vdots \\ & & & & & & 0 * \cdots * \\ & & & & & & 1 * \cdots * \end{array} \right) \end{array} \left. \begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array} \right\} r$$

Die von $j_1, \ldots, j_r$ verschiedenen Indizes in $\{1, \ldots, n\}$ seien $k_1 < \cdots < k_{n-r}$, d.h.

$$\{1, \ldots, n\} = \{j_1, \ldots, j_r, k_1, \ldots, k_{n-r}\}.$$

Dann gilt $Sx = 0 \iff$

$$\begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_r} \end{pmatrix} = -B \cdot \begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix},$$

wobei B aus den ersten r Zeilen von S entsteht, indem man die Spalten zu den Indizes j_i, $i = 1, \ldots, r$, weglässt (also $B \in M_{r,n-r}(K)$).

Folglich kann man $x_{k_1}, \ldots, x_{k_{n-r}}$ beliebig wählen und $x_{j_1}, \ldots, x_{j_r}$ ergeben sich dann eindeutig. Setzt man nun den i-ten Standardbasisvektor im K^{n-r} ein, erhält man links die i-te Spalte von $-B$ und einen i-ten Basisvektor $(x_1, \ldots, x_n)$ der Lösungsmenge durch $(x_{k_1}, \ldots, x_{k_{n-r}}) = e_i$, $(x_{j_1}, \ldots, x_{j_r}) = i$-te Spalte von $-B$.

Beispiel 3.46. Sei $\mathrm{char}\, K \neq 2$ und betrachte

$$\begin{array}{rcrcrcrcl} 2x_1 & + & 4x_2 & + & 2x_3 & + & 6x_4 & = & 0 \\ 3x_1 & + & 6x_2 & + & 3x_3 & + & 9x_4 & = & 0 \\ 4x_1 & + & 8x_2 & + & 5x_3 & + & 9x_4 & = & 0. \end{array}$$

$$A = \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \overset{\text{Bsp. } 3.35}{\rightsquigarrow} S = \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$j_1 = 1,\ j_2 = 3, \quad k_1 = 2,\ k_2 = 4.$

$$B = \begin{pmatrix} 2 & 6 \\ 0 & -3 \end{pmatrix} \quad -B = \begin{pmatrix} -2 & -6 \\ 0 & 3 \end{pmatrix}$$

Basis des 2-dimensionalen Lösungsraums: $((-2,1,0,0),(-6,0,3,1))$.

Nun betrachten wir das inhomogene System

$$Ax = b. \tag{$*$}$$

Die Zeilenumformungen (i), (ii), (iii) auf der Matrix $(A|b)$ verändern nicht den Lösungsraum. Wir kommen auf $(S|s)$ in strenger Zeilenstufenform.

Sei $r = \mathrm{Rg}(A) = \mathrm{Rg}(S)$. Wegen $\mathrm{Rg}(A|b) = \mathrm{Rg}(S|s)$ ist die Existenz von Lösungen nach 3.45 äquivalent zu $s_{r+1} = \cdots = s_m = 0$. Ist dies erfüllt, setze $x_j = 0$ für $j \notin \{j_1, \ldots, j_r\}$ und $(x_{j_1}, \ldots, x_{j_r}) = (s_1, \ldots, s_r)$ um eine spezielle Lösung zu erhalten. Alle anderen Lösungen erhält man durch Addition von Lösungen des zugeordneten homogenen Systems.

Beispiel 3.47. Es sei char $K \neq 2$. Wir betrachten das inhomogene lineare Gleichungssystem

$$\begin{aligned} 2x_1 + 4x_2 + 2x_3 + 6x_4 &= 4 \\ 3x_1 + 6x_2 + 3x_3 + 9x_4 &= 6 \\ 4x_1 + 8x_2 + 5x_3 + 9x_4 &= 9. \end{aligned}$$

$$(A|b) = \begin{pmatrix} 2 & 4 & 2 & 6 & 4 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 & 6 & 1 \\ 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$\mathrm{Rg} = 2$, also existiert Lösung. Außerdem haben wir die Stufenindizes $j_1 = 1$, $j_2 = 3$: Spezielle Lösung $(1,0,1,0)$.
Die allgemeine Lösung ist $(1,0,1,0) + \mathrm{Lin}((-2,1,0,0),(-6,0,3,1))$, d.h.

$$L = \{(1 - 2x_2 - 6x_4, x_2, 1 + 3x_4, x_4) \in K^4 \mid x_2, x_4 \in K\}.$$

Kapitel 4

Determinanten und Eigenwerte

4.1 Polynome

Definition 4.1. Ein **Polynom** mit Koeffizienten in einem Körper K ist ein Ausdruck

$$f = f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,\ a_j \in K.$$

Das Zeichen x heißt die **Unbestimmte** oder **Variable** des Polynoms. Die Menge der Polynome mit Koeffizienten in K wird mit $K[x]$ bezeichnet.

Bemerkung 4.2. 1) Ein Polynom ist ein formaler Ausdruck, d.h. nichts weiter als die Familie seiner Koeffizienten $a_0, a_1, \ldots$, d.h. eine Abbildung $f : \mathbb{N}_0 \to K$ mit $f(i) = 0$ f.f.a. i.
2) Jedes Polynom $f(x) = a_0 + \cdots + a_n x^n \in K[x]$ induziert eine Abbildung

$$K \longrightarrow K, \quad \alpha \mapsto f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

I.A. ist f durch diese Abbildung nicht eindeutig bestimmt. Z.B. induzieren die Polynome x^2 und $x \in \mathbb{Z}/2\mathbb{Z}[x]$ die gleiche Abbildung $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ (nämlich die Identität).

$K[x]$ wird folgendermaßen zu einem unitären kommutativen Ring:

Sei $f = \sum_{i=0}^{\infty} a_i x^i$, $g = \sum_{i=0}^{\infty} b_i x^i$. Dann setzt man

$$f + g = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$f \cdot g = \sum_{s=0}^{\infty} \left(\sum_{i=0}^{s} a_i \cdot b_{s-i} \right) x^s.$$

Wir haben eine natürliche Inklusion $K \hookrightarrow K[x]$, die einem $\alpha \in K$ das „konstante“ Polynom α (d.h. $a_0 = \alpha$, $a_i = 0$ für alle $i > 0$) zuordnet.

Definition 4.3. Ist $f = a_0 + a_1 x + \cdots + a_n x^n$ und $a_n \neq 0$, so heißt n der **Grad von f** (Notation: $\deg(f)$) und a_n der **Leitkoeffizient** (Notation: $a_n = e(f)$). Gilt $a_n = 1$ so nennt man f **normiert**.

Konvention: $\deg(0) = -\infty$, $e(0) = 0$.

Lemma 4.4. (i) $\deg(f \cdot g) = \deg(f) + \deg(g)$.

(ii) *Es gilt* $\deg(f+g) \leq \max(\deg(f), \deg(g))$ *und wenn* $\deg(f) \neq \deg(g)$, *so gilt* $\deg(f+g) = \max(\deg(f), \deg(g))$.

(iii) *Es gilt* $e(f \cdot g) = e(f) \cdot e(g)$.

Beweis. Das liest man direkt aus den Definitionen ab, wobei man verwendet, dass K nullteilerfrei ist, d.h. es gilt $ab = 0 \Rightarrow (a = 0 \text{ oder } b = 0)$. □

Korollar 4.5. *Der Ring $K[x]$ ist nullteilerfrei, d.h. aus $f \cdot g = 0$ folgt $f = 0$ oder $g = 0$.*

Beweis. Es gilt $f = 0 \Leftrightarrow e(f) = 0$. Daher folgt die Aussage aus $e(f \cdot g) = e(f) \cdot e(g)$ und der Nullteilerfreiheit von K (1.15). □

Satz 4.6 (Division mit Rest)**.** *Seien $f, g \in K[x]$, $g \neq 0$. Dann existieren eindeutig bestimmte Polynome $q, r \in K[x]$ mit*

$$f = q \cdot g + r \ , \ \deg(r) < \deg(g).$$

Das Polynom r heißt der **Rest der Division von f durch g**.

Beweis. Eindeutigkeit: Sei $f = q_1 \cdot g + r_1 = q_2 \cdot g + r_2$. Dann gilt

$$(q_1 - q_2) \cdot g = r_2 - r_1.$$

Wegen $\deg(r_2 - r_1) < \deg(g)$ folgt $q_1 - q_2 = 0$ also auch $r_2 - r_1 = 0$.

Existenz: Per Induktion nach $\deg(f)$. Ist $\deg(f) < \deg(g)$, setze $q = 0$, $f = r$. Sonst sei

$f = ax^{n+k} +$ niedrigere Potenzen
$g = bx^n +$ niedrigere Potenzen, $n, k \geq 0$, $a, b \in K^\times$.

Dann gilt

$$\deg\left(f - \frac{a}{b} x^k g\right) < \deg f.$$

Nach Induktionsannahme gibt es q_1, r_1 mit

$$f - \frac{a}{b} x^k g = q_1 \cdot g + r_1, \quad \deg(r_1) < \deg(g).$$

Wir erhalten die Darstellung

$$f = \left(q_1 + \frac{a}{b} x^k\right) \cdot g + r_1$$

□

Beispiel 4.7. $f = x^5 + 3x^4 - 4x^3 + 2$, $g = x^2 + 1$. Man findet g und r wie beim schriftlichen Dividieren ganzer Zahlen:

$$\begin{array}{l}
x^5 + 3x^4 - 4x^3 + 0x^2 + 0x + 2 : (x^2 + 1) = x^3 + 3x^2 - 5x - 3 \\
\underline{x^5 + \qquad x^3} \\
\quad 3x^4 - 5x^3 + 0x^2 + 0x + 2 \\
\quad \underline{3x^4 \qquad + 3x^2} \\
\qquad -5x^3 - 3x^2 + 0x + 2 \\
\qquad \underline{-5x^3 \qquad - 5x} \\
\qquad\qquad -3x^2 + 5x + 2 \\
\qquad\qquad \underline{-3x^2 \qquad - 3} \\
\qquad\qquad\qquad 5x + 5 \quad \text{Rest.}
\end{array}$$

Definition 4.8. Ein $\alpha \in K$ heißt **Nullstelle** von $f \in K[x]$, wenn $f(\alpha) = 0$ gilt.

Korollar 4.9. *Ist $\alpha \in K$ eine Nullstelle von $f \in K[x]$, so gibt es ein $g \in K[x]$ mit $f = g \cdot (x - \alpha)$.*

Beweis. Ist $f = 0$ setze $g = 0$. Ansonsten ist f nicht konstant, also $\deg f \geq 1$, und wir können schreiben:

$$f = g(x - \alpha) + r \quad \text{mit} \quad \deg(r) < \deg(x - \alpha) = 1.$$

Folglich gilt $\deg(r) \leq 0$, d.h. r ist konstant. Setzt man α ein, erhält man

$$0 = f(\alpha) = g(\alpha)(\alpha - \alpha) + r(\alpha) = r(\alpha)$$

also $r = 0$. □

Korollar 4.10. *Ein Polynom $0 \neq f \in K[x]$ vom Grad n hat höchstens n Nullstellen in K.*

Beweis. Gibt es keine Nullstellen, ist die Aussage wahr. Ansonsten sei α eine Nullstelle. Wir schreiben $f = (x - \alpha)g$, $\deg(g) \leq n - 1$. Ist nun $\beta \neq \alpha$ eine weitere Nullstelle, so gilt $0 = f(\beta) = (\beta - \alpha) \cdot g(\beta)$, woraus $g(\beta) = 0$ folgt. Die Behauptung folgt mit vollständiger Induktion nach dem Grad von f. □

Definition 4.11. Wir sagen ***f* teilt *g*** (Notation: $(f \mid g)$) wenn $g = f \cdot h$ für ein Polynom h gilt.

Euklidischer Algorithmus

Seien $f_1, f_2 \in K[x]$ beide nicht 0. Der **euklidische Algorithmus** ist die Folge von Divisionen mit Rest

$$\begin{array}{rcll}
f_1 & = & q_1 f_2 + f_3 & \deg f_3 < \deg f_2 \\
f_2 & = & q_2 f_3 + f_4 & \deg f_4 < \deg f_3 \\
 & \vdots & & \\
f_{n-2} & = & q_{n-2} f_{n-1} + f_n & \deg f_n < \deg f_{n-1} \\
f_{n-1} & = & q_{n-1} f_n + 0. &
\end{array}$$

Der Algorithmus stoppt, weil die Grade abnehmen.

Satz 4.12. *Seien $f_1, f_2 \in K[x]$ beide $\neq 0$ und $d = f_n$ wie im euklidischen Algorithmus. Dann gilt:*

(i) $d|f_1$, $d|f_2$.
(ii) Aus $g|f_1$ und $g|f_2$ folgt $g|d$.
(iii) Es gibt Polynome $p, q \in K[x]$ mit

$$pf_1 + qf_2 = d.$$

Beweis. (i) Steige den Algorithmus aufwärts:
$d|f_n \Rightarrow d|f_{n-1} \quad f_{n-2} = qf_{n-1} + f_n \Rightarrow d|f_{n-2}$ usw. $\Rightarrow d|f_2$, $d|f_1$
(ii) Steige ab: $g|f_1$, $g|f_2 \Rightarrow g|f_3 \Rightarrow \cdots \Rightarrow g|f_n = d$.
(iii) Den Algorithmus absteigend sieht man, dass jedes f_k eine Darstellung der Form $f_k = p_k f_1 + q_k f_2$ hat. □

Definition 4.13. Ein Polynom d mit den Eigenschaften (i) und (ii) aus 4.12 heißt **ein größter gemeinsamer Teiler** von f_1 und f_2.

Satz 4.14. *Sind $f_1, f_2 \in K[x]$ beide nicht 0, so existiert ein größter gemeinsamer Teiler. Dieser ist bis auf einen konstanten Faktor $\neq 0$ eindeutig bestimmt.*

Beweis. Die Existenz folgt aus 4.12. Sind d_1, d_2 beide g.g.T., so gilt $d_1|d_2$ und $d_2|d_1$, also $\deg(d_1) \leq \deg(d_2) \leq \deg(d_1) \Rightarrow \deg d_1 = \deg d_2$ und aus $d_1|d_2$ folgt $d_2 = \alpha \cdot d_1$, $\alpha \in K$, $\alpha \neq 0$. □

Bemerkung 4.15. Unter allen größten gemeinsamen Teilern gibt es genau ein normiertes Polynom. Dies nennt man *den* größten gemeinsamen Teiler. Bezeichnung: $\mathrm{ggT}(f_1, f_2)$. Dieser kann in der Form

$$\mathrm{ggT}(f_1, f_2) = pf_1 + qf_2$$

dargestellt werden.

Korollar 4.16. *Haben die nicht verschwindenden Polynome f und g nur konstante gemeinsame Teiler, so existieren Polynome p, q mit*

$$pf + qg = 1.$$

Beweis. $\mathrm{ggT}(f, g) = 1$. □

Definition 4.17. Ein Polynom f, $\deg(f) \geq 1$, heißt **irreduzibel**, wenn aus $f = g \cdot h$ folgt, dass g oder h konstant ist. Ansonsten heißt f reduzibel.

Beispiel 4.18. • Jedes Polynom $ax + b$, $a \neq 0$, vom Grad 1 ist irreduzibel
• $x^2 + 2x + 1 = (x + 1)^2$ ist reduzibel.
• x^2+1 ist irreduzibel als Polynom über $\mathbb{Q}$ und $\mathbb{R}$ (keine Nullstelle), aber reduzibel als Polynom über $\mathbb{C}$ wegen $x^2 + 1 = (x + i)(x - i)$.

Lemma 4.19. *Ist f irreduzibel und $f \mid (g \cdot h)$, so gilt $f|g$ oder $f|h$.*

Beweis. Da f irreduzibel ist, sind die Polynome der Form a und af, $a \in K$, $a \neq 0$, die einzigen Teiler von f. Gilt nun $f \nmid g$, so folgt $\mathrm{ggT}(f,g) = 1$. Also existieren $p, q \in K[x]$ mit $p \cdot f + q \cdot g = 1 \Rightarrow p \cdot f \cdot h + q \cdot g \cdot h = h \Rightarrow f|h$. □

Satz 4.20. *Jedes Polynom $f \neq 0$ besitzt eine, bis auf die Reihenfolge der Faktoren eindeutige „Primfaktorzerlegung“:*

$$f = a \cdot p_1 \cdots p_k \ , \ a = e(f), \ e(p_i) = 1, \ i = 1, \ldots, k,$$

mit irreduziblen, normierten Faktoren p_i.

Beweis. Existenz: Induktion nach $\deg f$. Sei $\deg f = 0$. Setze $k = 0$, $a = f$.

Sei $\deg(f) = n \geq 1$. Ist f irreduzibel, so schreibt man $f = e(f)e(f)^{-1}f$ und $e(f)^{-1}f$ ist normiert und irreduzibel. Ansonsten gilt $f = g \cdot h$ mit $\deg(g), \deg(h) < n$. Die Induktionsvoraussetzung für g und h liefert Darstellungen für g und h und im Produkt auch eine Darstellung für f.

Eindeutigkeit: $a = e(f)$ ist eindeutig. Angenommen es gilt $p_1 \cdots p_k = q_1 \cdots q_\ell$ mit irreduziblen, normierten Polynomen $p_1, \ldots, p_k, q_1, \ldots, q_\ell$. Zu zeigen:

$k = \ell$ und $p_1, \ldots, p_k$ und $q_1, \ldots, q_\ell$ unterscheiden sich nur in der Reihenfolge.

Aus 4.19 erhalten wir $p_k \mid q_i$ für ein i, $1 \leq i \leq \ell$. O.B.d.A. (Umnumerierung) sei $i = \ell$. Da q_ℓ irreduzibel ist, folgt $p_k = q_\ell$. Also

$$p_k(p_1 \ldots p_{k-1} - q_1 \ldots q_{\ell-1}) = 0.$$

Aus 4.5 folgt: $p_1 \ldots p_{k-1} = q_1 \ldots q_{\ell-1}$. Dann weiter ... □

Bemerkung. Die Aussage, dass jedes $a \in \mathbb{Z}$, $a \neq 0$, eine eindeutige Primzerlegung $a = (\pm 1) \cdot p_1 \cdots p_k$ hat, zeigt man genauso.

4.2 Determinanten

Definition 4.21. Sei V ein K-Vektorraum. Eine **Multilinearform** (n-Form) auf V ist eine Abbildung

$$\alpha : \underbrace{V \times \cdots \times V}_{n-\text{mal}} \longrightarrow K,$$

die in jeder Variable (d.h. bei Festhalten der $(n-1)$ anderen) linear ist. α heißt **alternierend**, wenn $\alpha(v_1, \ldots, v_n) = 0$ für jedes n-Tupel $(v_1, \ldots, v_n)$ mit $v_i = v_j$ für irgendwelche $i \neq j$ gilt.

Alternierende n-Formen können addiert und mit Skalaren multipliziert werden und bilden in natürlicher Weise einen K-Untervektorraum von $\mathrm{Abb}(V^n, K)$, der mit $\mathrm{Alt}^n V$ bezeichnet wird.

Spezialfall $n = 1$: $\mathrm{Alt}^1 V = V^*$ (Dualraum).

Bemerkung 4.22. Ist α eine alternierende k-Form, so wechselt α beim Vertauschen zweier Einträge das Vorzeichen, wegen

$0 = \alpha(v_1, \ldots, v_i + v_j, \ldots, v_i + v_j, \ldots, v_n) =$
$\alpha(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_n) + \alpha(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n)$
$+\alpha(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n) + \alpha(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_n)$, also

$$\alpha(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n) = -\alpha(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n).$$

Satz 4.23. *Eine alternierende n-Form $\alpha : V^n \to K$ ist*
(i) ***homogen**, d.h.*

$$\alpha(v_1, \ldots, v_{j-1}, \lambda v_j, v_{j+1}, \ldots, v_n) = \lambda\alpha(v_1, \ldots, v_n)$$

für alle $\lambda \in K$, $v_1, \ldots, v_n \in V$, $j = 1, \ldots, n$.

(ii) ***scherungsinvariant**, d.h.*

$$\alpha(v_1, \ldots, v_{j-1}, v_j + \lambda v_i, v_{j+1}, \ldots, v_n) = \alpha(v_1, \ldots, v_n)$$

für alle $\lambda \in K$, $v_1, \ldots, v_n \in V$, $i, j \in \{1, \ldots, n\}$, $i \neq j$.

Beweis. (i) folgt aus der Multilinearität.
(ii) Es gilt

$$\alpha(v_1, \ldots, v_j + \lambda v_i, \ldots, v_n) = \alpha(v_1, \ldots, v_j, \ldots, v_n) + \alpha(v_1, \ldots, \lambda v_i, \ldots, v_n)$$

und

$$\alpha(v_1, \ldots, \lambda v_i, \ldots, v_i, \ldots, \ldots, v_n) = \lambda\alpha(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_n) = 0. \qquad \square$$

Lemma 4.24. *Ist $\alpha : V^n \to K$ eine homogene und scherungsinvariante Abbildung und sind $(v_1, \ldots, v_n)$ linear abhängig, so gilt $\alpha(v_1, \ldots, v_n) = 0$.*

Beweis. Sei z.B. $v_1 = \lambda_2 v_2 + \cdots + \lambda_n v_n$. Dann folgt aus der Scherungsinvarianz

$$\begin{aligned} \alpha(v_1, \ldots, v_n) &= \alpha(v_1 - \lambda_2 v_2 - \cdots - \lambda_n v_n, v_2, \ldots, v_n) \\ &= \alpha(0, v_2, \ldots, v_n) \\ &= 0 \cdot \alpha(0, v_2, \ldots, v_n) = 0. \end{aligned}$$

$\square$

Satz 4.25. *Sei V ein n-dimensionaler K-Vektorraum. Dann ist jede homogene und scherungsinvariante Abbildung $V^n \to K$ eine alternierende n-Form auf V.*

Beweis. Sei $\alpha : V^n \to K$ homogen und scherungsinvariant. Dann gilt $\alpha(v_1, \ldots, v_n) = 0$ falls $(v_1, \ldots, v_n)$ linear abhängig (siehe 4.24.)
Bleibt z.z.: α ist n-Form. Wegen der Homogenität genügt es zu zeigen:

$$\alpha(v_1, \ldots, v_i + v_i', v_n) = \alpha(v_1, \ldots, v_i, v_n) + \alpha(v_1, \ldots, v_i', \ldots, v_n)$$

1. Fall: $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ sind linear abhängig $\Rightarrow$ beide Seiten $= 0$.
2. Fall: sonst ergänze zu einer Basis $(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n)$. Dann ist $v_i = x + \lambda w$, $v_i' = x' + \lambda' w$ mit $\lambda, \lambda' \in K$ und $x, x' \in \mathrm{Lin}(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$.
Wegen der Scherungsinvarianz gilt

$$\begin{aligned} \alpha(v_1, \ldots, v_i, \ldots, v_n) &= \alpha(v_1, \ldots, \lambda w, \ldots, v_n) = \lambda \alpha(v_1, \ldots, w, \ldots, v_n) \\ \alpha(v_1, \ldots, v_i', \ldots, v_n) &= \alpha(v_1, \ldots, \lambda' w, \ldots, v_n) = \lambda' \alpha(v_1, \ldots, w, \ldots, v_n) \end{aligned}$$

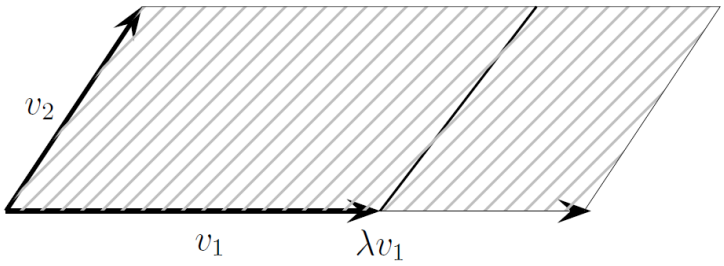
analog

$$\alpha(v_1, \ldots, v_i + v_i', \ldots, v_n) = (\lambda + \lambda')\alpha(v_1, \ldots, w, \ldots, v_n)$$ □

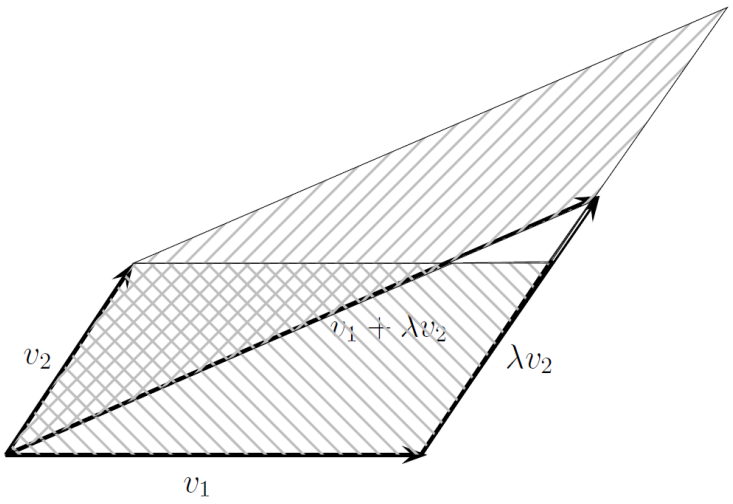
Von jetzt an sei $n = \dim_K V$. Die Bedingungen Homogenität und Scherungsinvarianz, also (i) und (ii) aus 4.23, sind geometrische Forderungen an ein „Volumen“

In dim 2:

(i) Streckt man in eine Richtung um den Faktor λ, so multipliziert sich das Volumen mit λ.



(ii) Die beiden schraffierten Parallelogramme haben gleiches Volumen (Prinzip des Cavalieri, wird im 3. Semester Analysis streng bewiesen „Satz von Fubini“).



Wegen dieses geometrischen Hintergrunds nennt man eine scherungsinvariante und homogene Abbildung $\alpha : V^n \to K$, $n = \dim_K V$, $\alpha \neq 0$, eine **Volumenform** auf V. Wir werden zeigen, dass eine Volumenform bis auf einen (nicht-verschwindenden) Faktor eindeutig bestimmt ist. In der „realen“ Welt (d.h. $K = \mathbb{R}$) normiert man das Volumen durch eine Maßeinheit (z.B. Kubikmeter, wenn $n = 3$).

Satz 4.26. *Sei $n = \dim V$ und $(v_1, \ldots, v_n)$ eine Basis von V. Dann ist die lineare Abbildung*

$$\mathrm{Alt}^n V \longrightarrow K, \quad \alpha \longmapsto \alpha(v_1, \ldots, v_n),$$

ein K-Vektorraum-Isomorphismus. Insbesondere gibt es zu jedem $\lambda \in K$ genau eine alternierende n-Form auf V mit $\alpha(v_1, \ldots, v_n) = \lambda$ und es gilt

$$\dim \mathrm{Alt}^n V = 1.$$

Beweis. Dies folgt vermittels des Isomorphismus: $K^n \to V$, $(\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1 v_1 + \ldots, \lambda_n v_n$, aus dem nächsten Satz. □

Satz 4.27. *Es gibt genau eine alternierende n-Form auf dem K^n*

$$\det : (K^n)^n \to K$$

mit $\det(e_1, \ldots, e_n) = 1$. Sie wird **Determinante** *genannt.*

Beweis. Wir fassen Vektoren $v_1, \ldots, v_n \in K^n$ als Zeilen einer Matrix auf. Damit ist Existenz und Eindeutigkeit einer Funktion

$$\det : M_{n,n}(K) \longrightarrow K$$

zu zeigen mit

(i) det ist multilinear in den Zeilen,

(ii) Sind in A zwei Zeilen gleich, so gilt $\det(A) = 0$,

(iii) $\det(E_n) = 1$.

Nach 4.23 und 4.25 sind (i) und (ii) (zusammen) äquivalent zu

(i)' det bleibt invariant unter der Zeilenumformung $v_i \mapsto v_i + \lambda v_j$, $i \neq j$, $\lambda \in K$,

(ii)' bei der Zeilenumformung $v_i \mapsto \lambda v_i$, $\lambda \in K^\times$, multipliziert sich det mit λ.

Eindeutigkeit: Sei det eine solche Funktion. Ist $(v_1, \ldots, v_n)$ linear abhängig, so gilt $\det(v_1, \ldots, v_n) = 0$ nach 4.24. Ansonsten kann man die Matrix mit den Zeilen $v_1, \ldots, v_n$ durch Zeilenumformung vom Typ (i)' und vom Typ (ii)' mit $\lambda \neq 0$ auf E_n transformieren. Wegen (iii) gilt $\det(E_n) = 1$ und rückwärts ist $\det(v_1, \ldots, v_n)$ bestimmt.

Existenz: Für $n = 1$ setze $\det(a) = a$. Sei $n \geq 2$ und $\det : M_{n-1,n-1}(K) \to K$ bereits konstruiert. Sei $A \in M_{n,n}(K)$. Für $1 \leq i, j \leq n$ sei $A_{ij} \in M_{n-1,n-1}(K)$ die Matrix die durch Streichen der i-ten Zeile und j-ten Spalte aus A entsteht. Sei nun j, $1 \leq j \leq n$, beliebig aber fest. Wir definieren

$$\det : M_{n,n}(K) \to K$$

induktiv durch „Entwicklung nach der j-ten Spalte“:

$$\det(A) \stackrel{df}{=} \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}).$$

Zu zeigen: die so definierte Funktion $\det : M_{n,n}(K) \to K$ erfüllt die Eigenschaften (i)–(iii).

Nach Induktionvoraussetzung ist $\det : M_{n-1,n-1}(K) \to K$ eine alternierende $(n-1)$-Form mit $\det(E_{n-1}) = 1$. Wir erhalten:

$$\begin{aligned} \det(E_n) &= \sum_{i=1}^{n} (-1)^{i+j} \delta_{ij} \det((E_n)_{ij}) \\ &= \delta_{jj} \det(E_{n-1}) = 1 \end{aligned}$$

Als Funktion in den Zeilen $v_1, \ldots, v_n$ ist det multilinear, was man direkt aus der definierenden Formel abliest, also gilt (i). Es verbleibt, (ii) zu zeigen. Sei $v_s = v_k$ für $s \neq k$. Falls $k = s + 1$, so stimmen die Matrizen A_{sj} und A_{kj} überein. Ansonsten gehen sie nach $|k - s - 1|$ vielen Zeilenvertauschungen in einander über. Da det das Vorzeichen wechselt, wenn man zwei Zeilen vertauscht, erhalten wir

$$\det(A_{sj}) = (-1)^{s+k+1} \det(A_{kj}),$$

woraus wegen $a_{sj} = a_{kj}$ die Gleichung

$$0 = (-1)^{s+j} a_{sj} \det(A_{sj}) + (-1)^{k+j} a_{kj} \det(A_{kj})$$

folgt. Für $i \neq s$, $i \neq k$ hat A_{ij} zwei gleiche Zeilen, d.h. $\det(A_{ij}) = 0$ für $i \notin \{s, k\}$. Zusammen ergibt sich

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) =$$

$$(-1)^{s+j} a_{sj} \det(A_{sj}) + (-1)^{k+j} a_{kj} \det(A_{kj}) = 0.$$

Dies zeigt (ii) und beendet den Beweis. □

Man schreibt die Determinante auch in der Form

$$\det A = |A| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Der Existenzbeweis liefert auch gleich eine Berechnungsmöglichkeit. In kleinen Dimensionen erhält man

$n = 1$: $\det(a) = a$.

$n = 2$: $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$.

$n = 3$:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}$$

$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$
$-a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13}$.

4.3 Eigenschaften der Determinante

Lemma 4.28. *(Spaltenentwicklung) Es sei $j \in \{1, \dots, n\}$. Dann gilt*

$$|A| = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}).$$

Beweis. Dies haben wir innerhalb des Existenzbeweises der Determinante in 4.27 gesehen. □

Satz 4.29. *Eine Funktion $\alpha : M_{n,n}(K) \to K$, die als Funktion auf den Zeilen homogen und scherungsinvariant ist, ist von der Form $\alpha = c \cdot \det$ für ein $c \in K$.*

Beweis. Nach 4.25 ist α eine alternierende n-Form. Nach 4.26 gilt $\dim \mathrm{Alt}^n(K^n) = 1$ und $0 \neq \det \in \mathrm{Alt}^n(K^n)$. □

Erinnern wir uns an die Matrizen

$$E_j(\lambda) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \quad \lambda \text{ an der Stelle } (j,j),$$

$$E_{ij}(\lambda) = \begin{pmatrix} 1 & & \\ & \ddots & \\ \lambda & & 1 \end{pmatrix} \quad \lambda \text{ an der Stelle } (i,j),\ i \neq j.$$

Die $n \times n$ Einheitsmatrix bezeichnen wir einfach nur mit E. Es gilt

$\alpha : M_{n,n}(K) \to K$ ist

homogen $\iff \alpha(E_j(\lambda) \cdot A) = \lambda \cdot \alpha(A) \quad \forall\, A, j, \lambda,$
scherungsinvariant $\iff \alpha(E_{ij}(\lambda) \cdot A) = \alpha(A) \quad \forall\, A, \lambda, i \neq j.$

Korollar 4.30. *Es gilt* $\det(E_j(\lambda)) = \lambda$, $\det(E_{ij}(\lambda)) = 1$.

Beweis. $\det(E_j(\lambda)) = \det(E_j(\lambda) \cdot E) = \lambda \cdot \det(E) = \lambda$
$\det(E_{ij}(\lambda)) = \det(E_{ij}(\lambda)E) = \det(E) = 1.$ □

Satz 4.31. *Sind* $A, B \in M_{n,n}(K)$, *so gilt* $|A \cdot B| = |A| \cdot |B|$.

Beweis. Für festes B betrachten wir die Abbildung

$$\alpha : M_{n,n}(K) \longrightarrow K,\ A \longmapsto |A \cdot B|$$

Es gilt

$$\begin{aligned} \alpha(E_j(\lambda) \cdot A) &= |E_j(\lambda) \cdot A \cdot B| \\ &= \lambda |A \cdot B| = \lambda \alpha(A), \end{aligned}$$

also ist α homogen. Desweiteren gilt

$$\alpha(E_{ij}(\lambda) \cdot A) = |E_{ij}(\lambda) \cdot A \cdot B| = |A \cdot B| = \alpha(A),$$

weshalb α auch scherungsinvariant ist. Nach 4.29 gilt $\alpha(A) = c \cdot |A|$ für alle A und ein festes $c \in K$. Setzt man $A = E$, erhält man $c = |B|$. □

Satz 4.32. *Es gilt* $|A| = |A^t|$.

Beweis. Betrachte

$$\alpha : M_{n,n}(K) \longrightarrow K,\ A \longmapsto \det(A^t).$$

Dann gilt

$$\begin{aligned}
\alpha(E_j(\lambda)\cdot A) &= |E_j(\lambda)\cdot A)^t| \\
&= |A^t\cdot E_j(\lambda)^t| \\
&= |A^t|\cdot|E_j(\lambda)| \\
&= \lambda\cdot\alpha(A) \\
\alpha(E_{ij}(\lambda)\cdot A) &= |(E_{ij}(\lambda)\cdot A)^t| \\
&= |A^t\cdot E_{ij}(\lambda)^t| \\
&= |A^t|\cdot|E_{ji}(\lambda)| \\
&= |A^t| = \alpha(A).
\end{aligned}$$

$\alpha(E) = |E^t| = |E| = 1$. Also gilt $\alpha = \det$. □

Korollar 4.33. *(Zeilenentwicklung) Es sei $i \in \{1,\dots,n\}$. Dann gilt*

$$|A| = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}|A_{ij}|\,.$$

Beweis. Man entwickle $|A^t|$ nach der i-ten Spalte und verwende 4.32. □

Definition 4.34. Die Matrix $\tilde{A} = (\tilde{a}_{ij})$ mit $\tilde{a}_{ij} = (-1)^{i+j}|A_{ji}|$ heißt die **Adjunkte** zu A.

Beispiel 4.35. $A = \begin{pmatrix} 3 & 5 \\ 1 & 3 \end{pmatrix} \Rightarrow \tilde{A} = \begin{pmatrix} 3 & -5 \\ -1 & 3 \end{pmatrix}$.

Es gilt $\tilde{A}\cdot A = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = A\cdot\tilde{A} = \begin{pmatrix} |A| & 0 \\ 0 & |A| \end{pmatrix}$.

Das ist kein Zufall:

Satz 4.36 (Erste Cramersche Regel).

$$\tilde{A}\cdot A = A\cdot\tilde{A} = |A|\cdot E.$$

Beweis. Sei $(B)_{ij}$ der Koeffizient der Matrix B an der Stelle (i,j). Dann gilt

$$\begin{aligned}
(A\cdot\tilde{A})_{ii} = \sum_j a_{ij}\tilde{a}_{ji} &= \sum_j a_{ij}(-1)^{i+j}|A_{ij}| \\
&= |A|
\end{aligned}$$

Für $i \neq j$ ist

$$(A\cdot\tilde{A})_{ij} = \sum_k (-1)^{j+k}a_{ik}|A_{jk}|$$

Rechts steht die Entwicklung nach der j-ten Zeile der Matrix, die man erhält, wenn man in A die j-te durch die i-te Zeile ersetzt, also die Determinante einer Matrix mit zwei gleichen Zeilen, d.h. 0.
Der Beweis von $\tilde{A}\cdot A = |A|\cdot E$ geht analog mit Spaltenentwicklung. □

Korollar 4.37. *$A \in M_{n,n}(K)$ ist genau dann invertierbar wenn $|A| \neq 0$.*

Beweis. Ist A invertierbar, so gilt $1 = |E| = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|$, also $|A| \neq 0$. Ist $|A| \neq 0$, so gilt $|A|^{-1} \cdot \tilde{A} \cdot A = E$, also ist A invertierbar. □

Korollar 4.38. *Die Determinante induziert einen surjektiven Gruppenhomomorphismus*

$$\det : \mathrm{GL}_n(K) \longrightarrow K^\times.$$

Beweis. $A \in \mathrm{GL}_n(K) \Rightarrow |A| \in K^\times$ nach 4.37. Die Homomorphismuseigenschaft folgt aus 4.31. Surjektivität folgt aus $|E_j(\lambda)| = \lambda$. □

Definition 4.39. Die Gruppe

$$\mathrm{SL}_n(K) := \mathrm{Kern}(\det : \mathrm{GL}_n(K) \longrightarrow K^\times),$$

also die multiplikative Gruppe der (invertierbaren) Matrizen mit Determinante 1, heißt die **spezielle lineare Gruppe**.

Satz 4.40. *Es sei $R \subset K$ ein unitärer Unterring und A eine $n \times n$-Matrix mit Koeffizienten in R. Es existiert genau dann eine inverse Matrix von A mit Koeffizienten in R, wenn $|A| \in R^\times$ gilt.*

Beweis. Die Entwicklung über Spalten zeigt induktiv, dass $|A| \in R$ gilt. Existiert $A^{-1} \in M_{n,n}(K)$ und hat Koeffizienten in $R \subset K$, so gilt $|A^{-1}| \cdot |A| = 1$ und daher $|A| \in R^\times$. Die Koeffizienten der Adjunkten $\tilde{A}$ sind Wechselsummen von Determinanten von Untermatrizen und daher in R. Gilt $|A| \in R^\times$, so hat auch $A^{-1} = |A|^{-1} \cdot \tilde{A}$ Koeffizienten in R. □

Korollar 4.41. *Sei A eine $n \times n$-Matrix mit Koeffizienten in $\mathbb{Z}$. Es existiert genau dann A^{-1} mit Koeffizienten in $\mathbb{Z}$ wenn $|A| = \pm 1$ gilt.*

Beweis. Es gilt $\mathbb{Z}^\times = \{\pm 1\}$. □

Satz 4.42 (Zweite Cramersche Regel). *Das lineare Gleichungssystem*

$$A \cdot x = b\ ,\ A \in \mathrm{GL}_n(K),\ b \in K^n,$$

hat die Lösung

$$x = |A|^{-1} \tilde{A} \cdot b.$$

Für die i-te Komponente x_i von x gilt daher

$$x_i = |A|^{-1} \sum_j (-1)^{i+j} |A_{ji}| \cdot b_j = \frac{|(A, i, b)|}{|A|}.$$

Hier ist (A, i, b) die Matrix, die aus A entsteht, wenn man die i-te Spalte durch b ersetzt.

Beweis. $A^{-1} = |A|^{-1}\tilde{A}$. □

Bemerkung 4.43. Diese Formel ist zur praktischen Berechnung ungeeignet, aber manchmal zu theoretischen Zwecken nützlich.

Praktische Berechnungsregeln für det

• Für $A \in M_{s,s}(K)$ und $k \in \mathbb{N}$ gilt: $\left|\begin{array}{c|c} E_k & 0 \\ \hline B & A \end{array}\right| = |A|$

(Entwicklung nach der ersten Zeile und Induktion nach k).

• Analog

$$\left|\begin{array}{c|c} A & 0 \\ \hline B & E_k \end{array}\right| = |A| = \left|\begin{array}{c|c} E_k & B \\ \hline 0 & A \end{array}\right|$$

$$\left|\begin{array}{c|c} 0 & A \\ \hline E_k & B \end{array}\right| = (-1)^s|A| = \left|\begin{array}{c|c} B & A \\ \hline E_k & 0 \end{array}\right|$$

• Sind A und C quadratisch erhalten wir

$$\left|\begin{array}{c|c} A & 0 \\ \hline B & C \end{array}\right| = \left|\begin{array}{c|c} A & 0 \\ \hline B & E \end{array}\right| \cdot \left|\begin{array}{c|c} E & 0 \\ \hline 0 & C \end{array}\right| = |A| \cdot |C|$$

und durch Transponieren

$$\left|\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right| = |A| \cdot |C|.$$

• Induktiv erhält man so

$$\begin{vmatrix} \lambda_1 & & 0 \\ & \ddots & \\ * & & \lambda_n \end{vmatrix} = \lambda_1 \cdots \lambda_n = \begin{vmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{vmatrix}$$

Also muss man zur praktischen Berechnung von det die Matrix in Dreiecksgestalt bringen.

Beispiele 4.44.

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{vmatrix} = 0$$

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 8 & 6 \\ 1 & 3 & 3 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 0 & -6 \\ 0 & 1 & 0 \end{vmatrix} = - \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & -6 \end{vmatrix} = 6$$

Definition 4.45. Die Elemente der Gruppe

$$\mathrm{GL}_n^+(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}),\ |A| > 0\}$$

heißen **orientierungserhaltend**.

Lemma 4.46. *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und $\mathcal{B}$ die Menge der Basen von V. Die Relation*

$$(v_1,\dots,v_n)\sim(w_1,\dots,w_n)\Longleftrightarrow M_{w_1,\dots,w_n}^{v_1,\dots,v_n}(\mathrm{id}_V)\in \mathrm{GL}_n^+(\mathbb{R})$$

ist eine Äquivalenzrelation auf $\mathcal{B}$. Es gibt genau zwei Äquivalenzklassen.

Beweis. Da sich Transformationsmatrizen (und damit deren Determinanten) multiplizieren, ist $\sim$ eine Äquivalenzrelation. Sei $(v_1,\dots,v_n)$ eine fixierte Basis. Dann gilt

$$\begin{gathered}(w_1,\dots,w_n)\not\sim(v_1,\dots,v_n)\text{ und }(w_1',\dots,w_n')\not\sim(v_1,\dots,v_n)\\ \Longrightarrow (w_1,\dots,w_n)\sim(w_1',\dots,w_n').\end{gathered}$$

Also gibt es höchstens zwei Äquivalenzklassen. Da det surjektiv ist, kommen negative Determinanten vor, also gilt $\mathrm{GL}_n^+(\mathbb{R})\subsetneq \mathrm{GL}_n(\mathbb{R})$ und daher existierten genau zwei Klassen. □

Definition 4.47. Die Auswahl einer Äquivalenzklasse bzgl. $\sim$ heißt **Orientierung des n-dimensionalen reellen Vektorraums V**. Jedes Element in dieser Äquivalenzklasse heißt dann **orientierte Basis**.

Bemerkung 4.48. Der $\mathbb{R}^n$ wird durch die Äquivalenzklasse der Standardbasis $(e_1,\dots,e_n)$ orientiert (**kanonische Orientierung des $\mathbb{R}^n$**). Eine Basis $(v_1,\dots,v_n)$ des $\mathbb{R}^n$ ist somit genau dann orientiert, wenn $\det(v_1,\dots,v_n)>0$ gilt.

Beispiel 4.49. Seien (x,y) linear unabhängig im $\mathbb{R}^3$. Dann ist $z:=x\times y\neq 0$ und es gilt

$$\det(x,y,z)\overset{\S 2.1}{=}\langle x\times y,z\rangle=\langle z,z\rangle=|z|^2>0.$$

Also ist $(x,y,x\times y)$ eine orientierte Basis des $\mathbb{R}^3$.

4.4 Die Leibniz-Formel

Erinnern wir uns an die Gruppe

$$\mathfrak{S}_n=\mathrm{Aut}(\{1,\dots,n\})$$

deren Elemente (Permutationen) wir in der Form

$$\pi=\begin{pmatrix}1 & 2 & \cdots & n\\ \pi(1) & \pi(2) & \cdots & \pi(n)\end{pmatrix}$$

schreiben.

Definition 4.50. Ein Element $\sigma\in\mathfrak{S}_n$ heißt **Transposition**, wenn es zwei Zahlen zwischen 1 und n vertauscht und alle anderen festhält. Schreibweise: $\sigma=(ij)$ vertauscht i und j $(i\neq j)$ und hält alle anderen fest.

Lemma 4.51. *Die Transpositionen erzeugen $\mathfrak{S}_n$, d.h. jedes Element in $\mathfrak{S}_n$ kann (auf nicht notwendig eindeutige Weise) als Produkt von Transpositionen geschrieben werden.*

Beweis. $n = 1$: die Aussage ist formal.
$n = 2$: die Aussage ist trivial.
Sei $n > 2$. Induktion über n. Wir erinnern uns an die Einbettung $\mathfrak{S}_{n-1} \hookrightarrow \mathfrak{S}_n$ durch $\pi \mapsto \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \pi(1) & \pi(2) & \dots & \pi(n-1) & n \end{pmatrix}$, bezüglich derer wir $\mathfrak{S}_{n-1}$ als Untergruppe in $\mathfrak{S}_n$ auffassen.
Sei nun $\sigma \in \mathfrak{S}_n$ beliebig. Gilt $\sigma(n) = n$, so ist $\sigma \in \mathfrak{S}_{n-1}$ und nach Induktionsvoraussetzung ist σ Produkt von Transpositionen.
Ist $\sigma(n) = m$, $1 \leq m \leq n-1$, so ist $(mn) \cdot \sigma \in \mathfrak{S}_{n-1}$, also Produkt von Transpositionen $(mn)\sigma = t_1 \cdots t_r$, also $\sigma = (mn) \cdot t_1 \cdots t_r$. □

Wie eindeutig ist die Darstellung als Produkt von Transpositionen? Wir werden sehen, dass die Anzahl der Transpositionen modulo 2 wohlbestimmt ist.

Lemma 4.52. *Die Abbildung*

$$\operatorname{sgn} : \mathfrak{S}_n \longrightarrow \{\pm 1\}, \quad \sigma \longmapsto \prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i) - \sigma(j)},$$

ist ein Gruppenhomomorphismus.

Beweis. Zunächst bemerken wir, dass in $\prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i)-\sigma(j)}$ im Zähler wie Nenner die gleichen Faktoren vorkommen, aber eventuell mit verschiedenem Vorzeichen. Daher gilt $\operatorname{sgn}(\sigma) \in \{\pm 1\}$. Für $\sigma, \tau \in \mathfrak{S}_n$ und $1 \leq i < j \leq n$ mit $\tau(i) > \tau(j)$ gilt

$$\frac{\tau(i) - \tau(j)}{\sigma\tau(i) - \sigma\tau(j)} = \frac{\tau(j) - \tau(i)}{\sigma\tau(j) - \sigma\tau(i)}. \tag{$*$}$$

Wir erhalten

$$\prod_{1 \leq i < j \leq n} \frac{\tau(i) - \tau(j)}{\sigma\tau(i) - \sigma\tau(j)} = \prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i) - \sigma(j)},$$

weil nach Anwendung von $(*)$ links und rechts die gleichen Terme stehen. Daher

gilt

$$\begin{aligned}\operatorname{sgn}(\sigma\tau) &= \prod_{1\le i<j\le n}\frac{i-j}{\sigma\tau(i)-\sigma\tau(j)}\\ &= \prod_{1\le i<j\le n}\frac{\tau(i)-\tau(j)}{\sigma\tau(i)-\sigma\tau(j)}\cdot\prod_{1\le i<j\le n}\frac{i-j}{\tau(i)-\tau(j)}\\ &= \prod_{1\le i<j\le n}\frac{i-j}{\sigma(i)-\sigma(j)}\cdot\prod_{1\le i<j\le n}\frac{i-j}{\tau(i)-\tau(j)}\\ &= \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau).\end{aligned}$$

□

Definition 4.53. Die Zahl $\operatorname{sgn}(\sigma)\in\{\pm 1\}$ heißt das **Signum** der Permutation σ.

Lemma 4.54. *Für eine Transposition $t=(ij)\in\mathfrak{S}_n$ gilt* $\operatorname{sgn}(t)=-1$.

Beweis. Sei $t=(ij)\in\mathfrak{S}_n$ und ohne Einschränkung $i<j$. Wir betrachten für $1\le\alpha<\beta\le n$ das Vorzeichen von

$$\frac{\alpha-\beta}{t(\alpha)-t(\beta)}.$$

Der Zähler ist stets negativ und wir erhalten die folgende Fallunterscheidung

$\{\alpha,\beta\}\cap\{i,j\}=\emptyset$	$+$	
$\alpha=i<\beta\le j$	$-$	$(j-i)$ mal.
$\alpha=i<j<\beta$	$+$	
$\alpha<i<j=\beta$	$+$	
$i<\alpha<j=\beta$	$-$	$(j-i-1)$ mal
$i<j=\alpha<\beta$	$+$	
$\alpha<\beta=i<j$	$+$	

Also folgt

$$\operatorname{sgn}(t)=(-1)^{2j-2i-1}=-1.$$ □

Satz 4.55. *Ist*

$$\sigma=t_1\cdots t_r$$

eine Darstellung von σ als Produkt von Transpositionen, so gilt $\operatorname{sgn}(\sigma)=(-1)^r$. *Insbesondere ist die Restklasse von r modulo 2 von der Wahl der Darstellung unabhängig.*

Beweis. Es ist sgn ein Homomorphismus, also

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(t_1) \cdots \operatorname{sgn}(t_r) = (-1)^r. \qquad \square$$

Anwendung: Schiebespiel „Ohne-Fleiß-kein-Preis-Spiel“, „15er Puzzle“ (Gegen Ende Januar 1880 setzte der Zahnarzt Charles Pevey ein Preisgeld für die Lösung des 15er-Puzzles aus. Das Spiel wurde in den USA im Februar, in Kanada im März und in Europa im April 1880 sehr populär.)

Ausgangsstellung:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Frage: Kommt man auf

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

?

Antwort: nein.
Begründung: Wir bezeichnen das leere Feld mit 16. Jeder Zustand des Spiels entspricht einem Element in S_{16}.
Man startet mit dem neutralen Element $e \in \mathfrak{S}_{16}$. Ein Zug entspricht der Multiplikation mit einer Transposition. Das Schema

+	-	+	-
-	+	-	+
+	-	+	-
-	+	-	+

zeigt, dass ein Zustand σ mit Loch rechts unten nur nach einer geraden Anzahl von Transpositionen erreicht wird, d.h. $\operatorname{sgn}(\sigma) = +1$ für solche σ. Daher kann der Zustand (12), dessen Signum -1 ist, nicht erreicht werden!

Definition 4.56. Die Untergruppe

$$\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}(\sigma) = 1\}$$

heißt die **alternierende Gruppe** (über n Elemente).

Bemerkung 4.57. Es gilt $\mathfrak{A}_n = \operatorname{Kern}(\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\})$ und für $n \geq 2$ ist sgn surjektiv. Also folgt für $n \geq 2$

$$\#\mathfrak{A}_n = \frac{\#\mathfrak{S}_n}{2} = \frac{n!}{2}.$$

Nun sei K ein Körper. Wir betrachten die Abbildung

$$\varphi : \mathfrak{S}_n \longrightarrow \mathrm{GL}_n(K),\ \varphi(\sigma)(e_i) = e_{\sigma(i)},$$

d.h. $\varphi(\sigma)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}$.

Seien $\sigma, \tau \in \mathfrak{S}_n$ und $x \in K^n$. Setzt man $y = \varphi(\tau)(x)$, so gilt

$$y_i = x_{\tau^{-1}(i)},\ i = 1, \ldots, n,$$

und damit

$$\begin{aligned}\big(\varphi(\sigma) \circ \varphi(\tau)(x)\big)_i = (\varphi(\sigma)(y))_i = y_{\sigma^{-1}(i)} \\ = x_{\tau^{-1}\sigma^{-1}(i)} = x_{(\sigma\tau)^{-1}(i)} = \varphi(\sigma\tau)(x)_i.\end{aligned}$$

Dies zeigt $\varphi(\sigma) \circ \varphi(\tau)(x) = \varphi(\sigma\tau)(x)$ für alle $x \in K^n$, also $\varphi(\sigma) \circ \varphi(\tau) = \varphi(\sigma\tau)$. Daher ist $\varphi : \mathfrak{S}_n \to \mathrm{GL}_n(K)$ ein (injektiver) Gruppenhomomorphismus.

Definition 4.58. Matrizen der Form $\varphi(\sigma)$, $\sigma \in \mathfrak{S}_n$, heißen **Permutationsmatrizen**.

Ist $t = (ij)$ eine Transposition, so gilt $\varphi(t) = P_{ij}$ (die Matrix, die aus der Einheitsmatrix durch Vertauschen der i-ten und j-ten Zeile entsteht) und daher

$$\det(\varphi(t)) = \det P_{ij} = -1_K.$$

Nach 4.55 gilt daher:

Korollar 4.59. *Ist $\sigma \in \mathfrak{S}_n$ Produkt von r Transpositionen, so gilt*

$$\det(\varphi(\sigma)) = (-1_K)^r = \mathrm{sgn}(\sigma).$$

Hier fassen wir $\mathrm{sgn}(\sigma) \in \{\pm 1\}$ als Element von K auf.

Satz 4.60 (Leibniz-Formel). *Für $A = (a_{ij}) \in M_{n,n}(K)$ gilt*

$$|A| = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}$$

Beweis.

$$|A| = \det(\sum_j a_{1j} e_j, \ldots, \sum_j a_{nj} e_j),$$

wobei e_j den j-ten Einheitsvektor in K^n bezeichnet. Dies rechnen wir multilinear aus und erhalten

$$|A| = \sum_{J=(j_1,\ldots,j_n)} a_{1j_1} a_{2j_2} \ldots a_{nj_n} \cdot \det(e_{j_1}, \ldots, e_{j_n})$$

Ist $\begin{pmatrix} 1,\ldots,n \\ j_1,\ldots,j_n \end{pmatrix}$ keine Permutation, so ist $\det(e_{j_1},\ldots,e_{j_n}) = 0$ (ein Vektor kommt doppelt vor).
Ist $\sigma = \begin{pmatrix} 1,\ldots,n \\ j_1,\ldots,j_n \end{pmatrix}$ eine Permutation, so gilt $\det(e_{j_1},\ldots,e_{j_n}) = \operatorname{sgn}(\sigma)$ nach 4.59. □

Bemerkung 4.61. Die Leibniz-Formel ist für die praktische Berechnung ungeeignet (zu viele Summanden).

Anwendungen sind:

Korollar 4.62. *Für $K = \mathbb{R}$ ist die Abbildung* $\det : \mathbb{R}^{n^2} = M_{n,n}(\mathbb{R}) \to \mathbb{R}$ *beliebig oft stetig differenzierbar.*

Definition 4.63. Ist R ein kommutativer unitärer Ring und $A \in M_{n,n}(R)$ eine $n \times n$-Matrix mit Einträgen in R, so definiert man $\det(A) \in R$ über die Leibnizformel.

Man kann dann zeigen

1.) det kann über Zeilen- oder Spaltenentwicklung berechnet werden
2.) $\det(A \cdot B) = \det(A) \cdot \det(B)$, $A \cdot \tilde{A} = \tilde{A} \cdot A = \det(A) \cdot E$, wobei $\tilde{A}$ die Adjunkte ist.
3.) A ist dann und nur dann invertierbar, wenn $\det(A) \in R^\times$ ist und dann gilt $A^{-1} = \det(A)^{-1} \cdot \tilde{A}$.
4.) Ist $f : R \to S$ ein Ringhomomorphismus, so gilt für $f(A) \in M_{n,n}(S)$ die Formel $\det(f(A)) = f(\det(A))$.

4.5 Das charakteristische Polynom

Sei $A \in M_{n,n}(K)$.

Definition 4.64. Die **Spur** von $A = (a_{ij})$ ist durch $\operatorname{Sp}(A) := \sum_{i=1}^{n} a_{ii}$ definiert.

Lemma 4.65. $\operatorname{Sp}(A \cdot B) = \operatorname{Sp}(B \cdot A)$.

Beweis. Es gilt

$$\begin{aligned} (A \cdot B)_{ii} &= \sum_j a_{ij} b_{ji} \quad \text{und} \\ (B \cdot A)_{jj} &= \sum_i b_{ji} a_{ij}. \quad \text{Also} \\ \operatorname{Sp}(A \cdot B) &= \sum_{i,j} a_{ij} b_{ji} = \operatorname{Sp}(B \cdot A) \end{aligned}$$

□

Korollar 4.66. *Für $T \in \mathrm{GL}_n(K)$ gilt*

$$\begin{aligned} \det(TAT^{-1}) &= \det(A), \\ \mathrm{Sp}(TAT^{-1}) &= \mathrm{Sp}(A). \end{aligned}$$

Beweis. Es gilt $\det(AB) = \det(BA)$ nach 4.31, sowie $\mathrm{Sp}(AB) = \mathrm{Sp}(BA)$ nach 4.65. Wir erhalten

$$\det(TAT^{-1}) = \det(T^{-1}TA) = \det(EA) = \det(A).$$

Das Argument für die Spur ist dasselbe. □

Wir arbeiten nun im Polynomring $K[t]$ über K.

Definition 4.67. Sei $A \in M_{n,n}(K)$. Das Polynom

$$\chi_A(t) := \det(tE - A) \in K[t]$$

heißt das **charakteristische Polynom** der Matrix A.

Lemma 4.68. *χ_A ist ein normiertes Polynom vom Grad n*

$$\chi_A(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$$

und es gilt $c_0 = \chi_A(0) = (-1)^n|A|$ und $c_{n-1} = -\mathrm{Sp}(A)$.

Beweis. Die Leibnizformel zeigt, dass χ_A die Form

$$\chi_A(t) = (t - a_{11}) \cdots (t - a_{nn}) + (\text{Polynom vom Grad } \leq n - 2)$$

hat. Daher ist χ_A normiert vom Grad n und $c_{n-1} = -a_{11} - a_{22} \cdots - a_{nn}$. Schließlich gilt

$$c_0 = \chi_A(0) = |0 \cdot E - A| = |-A| = (-1)^n|A|.$$ □

Lemma 4.69. *Ist $T \in \mathrm{GL}_n(K)$, so gilt*

$$\chi_{TAT^{-1}} = \chi_A.$$

Beweis.

$$\begin{aligned} \chi_{TAT^{-1}} &= |tE - TAT^{-1}| \\ &= |T(tE - A)T^{-1}| \\ &= |T| \cdot |tE - A| \cdot |T^{-1}| \\ &= \chi_A. \end{aligned}$$

□

Unsere Regeln zur Determinantenberechnung wenden sich nun hier an und wir erhalten:

- $A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \Rightarrow \quad tE - A = \begin{pmatrix} t-\lambda_1 & & * \\ & \ddots & \\ 0 & & t-\lambda_n \end{pmatrix}$

$\Longrightarrow \chi_A(t) = (t-\lambda_1)\cdots(t-\lambda_n)$.

- $A = \begin{pmatrix} B & * \\ 0 & C \end{pmatrix}$ oder $A = \begin{pmatrix} B & 0 \\ * & C \end{pmatrix}$

$\Longrightarrow \chi_A(t) = \chi_B(t) \cdot \chi_C(t)$.

Sei nun $f = c_0 + c_1 t + \cdots + c_r t^r \in K[t]$ ein Polynom. Durch die Regel

$$f(A) = c_0 E + c_1 A + c_2 A^2 + \cdots + c_r A^r \in M_{n,n}(K)$$

definiert f eine Abbildung $M_{n,n}(K) \to M_{n,n}(K)$, $A \mapsto f(A)$.

Bemerkung 4.70. Für $f, g \in K[t]$ und $A \in M_{m,m}(K)$ gilt

$$f(A) \cdot g(A) = (f \cdot g)(A) = (g \cdot f)(A) = g(A) \cdot f(A),$$

d.h. die Matrizen $f(A)$ und $g(A)$ *kommutieren*.

Satz 4.71 (Cayley-Hamilton). *Es gilt* $\chi_A(A) = 0$.

Beweis. Sei D die Adjunkte zu $(tE - A)$ also

$$D \cdot (tE - A) = \det(tE - A) \cdot E = \chi_A(t) \cdot E. \qquad (*)$$

In der Definition der Adjunkten treten Determinanten von $(n-1)\times(n-1)$-Untermatrizen auf, also sind die Einträge von D Polynome in $K[t]$ vom Grad $\leq n-1$. Wir schreiben

$$D = \sum_{i=0}^{n-1} D_i t^i, \quad D_i \in M_{n,n}(K).$$

Desweiteren sei $\chi_A(t) = \sum_{i=0}^{n} a_i t^i$, mit $a_i \in K$. Ein Koeffizientenvergleich in $(*)$ liefert

$$a_i E = D_{i-1} - D_i A$$

wobei wir $D_{-1} = 0$ und $D_n = 0$ ergänzen. Es folgt:

$$\chi_A(A) = \sum_{i=0}^{n} a_i A^i = \sum_{i=0}^{n} (D_{i-1} - D_i A) A^i$$
$$= -D_0 A + D_0 A - D_1 A^2 + \cdots + D_{n-1} A^n - D_n A^{n+1} = 0.$$

□

4.6 Endomorphismen

Sei $f : V \to W$ eine lineare Abbildung. Wir haben gelernt, siehe 3.29, dass sich f bei Wahl geeigneter Basen $(v_1, \dots, v_n)$, $(w_1, \dots, w_m)$ von V und W durch die Matrix

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

darstellen lässt. Ist nun $V = W$, will man $(v_1, \dots, v_n) = (w_1, \dots, w_n)$ und die Sache wird komplizierter.

Sei V ein n-dimensionaler K-Vektorraum und $\alpha : V \to V$ ein Endomorphismus. Sei A die Darstellungsmatrix von α bzgl. einer Basis $(v_1, \dots, v_n)$. Bzgl. einer anderen Basis $(v'_1, \dots, v'_n)$ wird α durch TAT^{-1} dargestellt, wobei $T \in \mathrm{GL}_n(K)$ die Transformationsmatrix ist. Nach 4.69 hängt das charakteristische Polynom nicht von der Wahl der Basis ab und wir erhalten, dass die folgenden Objekte wohldefiniert sind:

Definition 4.72. $\mathrm{Sp}(\alpha) \stackrel{\mathrm{df}}{=} \mathrm{Sp}(A)$, $\det(\alpha) \stackrel{\mathrm{df}}{=} \det(A)$, $\chi_\alpha(t) \stackrel{\mathrm{df}}{=} \chi_A(t)$, wobei A die α bzgl. irgendeiner Basis darstellende Matrix ist.

Definition 4.73. Sei $\alpha \in \mathrm{End}(V)$. Ein $\lambda \in K$ heißt **Eigenwert von** α, wenn es einen Vektor $v \in V$, $v \neq 0$, mit $\alpha(v) = \lambda \cdot v$ gibt. Ist λ ein Eigenwert von α, so heißt der Untervektorraum

$$V_\lambda = \mathrm{Kern}(\lambda \cdot \mathrm{id}_V - \alpha)$$

der **Eigenraum** zu λ. Seine Elemente $\neq 0$, d.h. solche $v \neq 0$ mit $\alpha(v) = \lambda \cdot v$ heißen **Eigenvektoren** zum Eigenwert λ.

Bemerkung 4.74. Ideal wäre es, wenn man V in die direkte Summe von Eigenräumen zerlegen könnte. Dann hätte α bezüglich einer Basis von V Diagonalgestalt. Leider geht das nicht immer.

Beispiel 4.75. $\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ entspricht der Drehung um $\pi/2$ in der rellen Ebene und hat keinen Eigenwert.

Satz 4.76. *Die Eigenwerte von α sind genau die Nullstellen von $\chi_\alpha(t)$.*

Beweis. Es sei α bezüglich irgendeiner Basis durch die Matrix A dargestellt:
λ EW von $\alpha \Leftrightarrow \exists\, v \neq 0$: $\alpha(v) = \lambda(v) \Leftrightarrow \exists\, v \neq 0\ (\lambda \mathrm{id}_V - \alpha)v = 0 \Leftrightarrow$
$\mathrm{Kern}(\lambda \mathrm{id}_V - \alpha) \neq 0 \Leftrightarrow \det(\lambda \mathrm{id}_V - \alpha) = 0 \Leftrightarrow \det(\lambda E - A) = 0 \Leftrightarrow \chi_A(\lambda) = 0$. □

Bemerkung 4.77. Damit sehen wir auch algebraisch, dass die reelle Matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ keinen Eigenwert hat, weil $\chi_A(t) = t^2+1$ keine reellen Nullstellen hat. Aber $\pm i$ sind komplexe Nullstellen, d.h. als komplexe 2×2-Matrix aufgefasst, besitzt A zwei Eigenwerte.

Sei nun $f = c_0 + c_1 t + \cdots + c_r t^r \in K[t]$, V ein n-dimensionaler K-Vektorraum und $\alpha \in \mathrm{End}(V)$. Nach 2.31 ist $\mathrm{End}(V)$ mit der Komposition als Multiplikation ein unitärer Ring, der K als Unterring enthält. Daher kann man Endomorphismen in f einsetzen und erhält Endomorphismen. Explizit bedeutet dies

$$f(\alpha) = c_0 \cdot \mathrm{id}_V + c_1\alpha + c_2\alpha \circ \alpha + \cdots + c_r \underbrace{\alpha \circ \alpha \cdots \circ \alpha}_{r-\text{mal}} \in \mathrm{End}(V).$$

Bemerkung 4.78. Für $f, g \in K[t]$ und $\alpha \in \mathrm{End}(V)$ gilt

$$f(\alpha) \circ g(\alpha) = (f \cdot g)(\alpha) = (g \cdot f)(\alpha) = g(\alpha) \circ f(\alpha),$$

d.h. die Endomorphismen $f(\alpha)$ und $g(\alpha)$ kommutieren.

Satz 4.79 (Cayley-Hamilton für Endomorphismen).

$$\chi_\alpha(\alpha) = 0.$$

Beweis. Sei α bzgl. einer Basis durch die Matrix A dargestellt. Dann wird für $f \in K[t]$, $f(\alpha)$ durch $f(A)$ dargestellt. Insbesondere wird $\chi_\alpha(\alpha)$ durch $\chi_A(A) = 0$ (Cayley-Hamilton) dargestellt. □

4.7 Zerlegung in Eigenräume

Sei V ein n-dimensionaler K-Vektorraum und $\alpha \in \mathrm{End}(V)$.

Definition 4.80. Man sagt, eine Matrix $A = (a_{ij})$ habe **Diagonalgestalt**, wenn $a_{ij} = 0$ für $i \neq j$ gilt. Man schreibt dann

$$A = \mathrm{diag}(a_{11}, \ldots, a_{nn}).$$

Der Endomorphismus α von V heißt **diagonalisierbar**, wenn die Darstellungsmatrix von α bezüglich einer Basis $(v_1, \ldots, v_n)$ von Diagonalgestalt ist.

Lemma 4.81. *Der Endomorphismus α ist genau dann diagonalisierbar, wenn es eine Basis $(v_1, \ldots, v_n)$ von V, bestehend aus Eigenvektoren zu α gibt.*

Beweis. Es ist $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$ genau dann die Darstellungsmatrix von α bezüglich der Basis $(v_1, \dots, v_n)$, wenn $\alpha(v_i) = \lambda_i v_i$ gilt. □

Bemerkung 4.82. Ist α diagonalisierbar, also die Darstellungsmatrix von α bezüglich einer Basis $(v_1, \dots, v_n)$ von Diagonalgestalt $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$, so gilt

$$\chi_\alpha(t) = \det\left(\begin{pmatrix} t-\lambda_1 & & 0 \\ & \ddots & \\ 0 & & t-\lambda_n \end{pmatrix}\right) = (t-\lambda_1)\cdots(t-\lambda_n),$$

d.h. χ_α zerfällt in das Produkt von Linearfaktoren.

Satz 4.83. *Es seien $\lambda_1, \dots, \lambda_m$ paarweise verschiedene Eigenwerte von α und $v_1, \dots, v_m \in V$ Eigenvektoren zu $\lambda_1, \dots, \lambda_m$. Dann ist das System*

$$(v_1, \dots, v_m)$$

linear unabhängig.

Beweis. Nach Voraussetzung gilt $(\alpha - \lambda_i \operatorname{id}_V)(v_j) = (\lambda_j - \lambda_i)v_j$. Setzt man

$$\beta_i = (\alpha - \lambda_1 \operatorname{id}_V) \circ \cdots \circ (\alpha - \lambda_{i-1} \operatorname{id}_V) \circ (\alpha - \lambda_{i+1} \operatorname{id}_V) \circ \cdots \circ (\alpha - \lambda_m \operatorname{id}_V),$$

so folgt

$$\beta_i(v_j) = \Big(\prod_{k \neq i}(\lambda_j - \lambda_k)\Big) \cdot v_j = \begin{cases} 0 & i \neq j \\ (\text{Skalar} \neq 0) \cdot v_j & i = j. \end{cases}$$

Gilt nun

$$a_1 v_1 + \cdots + a_m v_m = 0, \quad a_1, \dots, a_m \in K,$$

so erhält man für jedes $i = 1, \dots, m$ durch Anwendung von β_i die Gleichung $a_i = 0$. Daher ist das System $(v_1, \dots, v_m)$ linear unabhängig. □

Satz 4.84. *Sei V ein n-dimensionaler K-Vektorraum und $\alpha \in \operatorname{End}(V)$. Zerfällt das charakteristische Polynom von α in paarweise verschiedene Linearfaktoren, d.h.*

$$\chi_\alpha(t) = (t-\lambda_1)\cdots(t-\lambda_n)$$

mit $\lambda_i \neq \lambda_j$ für $i \neq j$, so gibt es eine Basis von V aus Eigenvektoren von α. Insbesondere wird α bezüglich einer Basis von V durch eine Diagonalmatrix dargestellt.

Beweis. In diesem Fall sind $\lambda_1, \dots, \lambda_n$ paarweise verschiedene Eigenwerte. Sind $v_1, \dots, v_n$ zugehörige Eigenvektoren, so ist $(v_1, \dots, v_n)$ nach 4.83 ein linear unabhängiges System und wegen $n = \dim V$ eine Basis. □

Wie macht man das explizit?
Betrachte den Endomorphismus α des $\mathbb{R}^2$ der bzgl. der kanonischen Basis durch die Matrix $A = \begin{pmatrix} 1 & -2 \\ 1 & 4 \end{pmatrix}$ gegeben ist.

$$\begin{aligned} \chi_\alpha(t) = \det \begin{pmatrix} t-1, 2 \\ -1, t-4 \end{pmatrix} &= (t-1)(t-4)+2 \\ &= t^2 - 5t + 6 \\ &= (t-2)(t-3) \end{aligned}$$

Daher ist $\{2, 3\}$ die Menge der Eigenwerte.

Nun suchen wir Eigenvektoren. Wir betrachten das homogene lineare Gleichungssystem

$$\begin{array}{c} (2E - A)x = 0 \\ \| \\ \begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0 \end{array}$$

Nichttriviale Lösung: $(2, -1)^t$ ist Eigenvektor zum Eigenwert $\lambda = 2$.

$$\begin{array}{l} (3E - A)x = 0 \\ \quad \| \\ \begin{pmatrix} 2 & 2 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \end{array}$$

Lösung: $(-1, 1)^t$

Also hat α bzgl. der Basis $((2, -1)^t, (-1, 1)^t)$ die Darstellungsmatrix $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

4.8 Trigonalisierbarkeit

Definition 4.85. Sei V ein n-dimensionaler K-Vektorraum und $\alpha \in \mathrm{End}(V)$. Der Endomorphismus α heißt **trigonalisierbar**, wenn es eine Basis gibt bzgl. derer α durch eine obere Dreiecksmatrix, d.h. durch eine Matrix der Form

$$\begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix}$$

dargestellt wird.

Satz 4.86. *α ist genau dann trigonalisierbar, wenn $\chi_\alpha(t)$ vollständig in Linearfaktoren zerfällt.*

Beweis. Ist α bzgl. einer Basis durch $\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ gegeben, so gilt

$$\chi_\alpha(t) = \begin{vmatrix} t-\lambda_1 & & * \\ & \ddots & \\ 0 & & t-\lambda_n \end{vmatrix} = (t-\lambda_1)\cdots(t-\lambda_n).$$

Die andere Richtung beweisen wir per Induktion nach n. Der Fall $n = 1$ ist klar, Sei $n > 1$ und $\chi_\alpha = (t-\lambda_1)\cdots(t-\lambda_n)$ und v_1 ein Eigenvektor zu λ_1. Wir ergänzen v_1 zu einer Basis $(v_1, \ldots, v_n)$ von V. Bzgl. dieser Basis hat α die Gestalt $A = \left(\begin{array}{c|c} \lambda_1 & * \\ \hline 0 & A' \end{array}\right)$ mit einer $(n-1)\times(n-1)$ Matrix A'. Sei $V' = \mathrm{Lin}(v_2, \ldots, v_n)$. Dann gilt

$$V = K \cdot v_1 \oplus V'.$$

Außerdem gilt $(t-\lambda_1)\cdots(t-\lambda_n) = \chi_A(t) = (t-\lambda_1)\cdot\chi_{A'}(t)$. Wegen der Nullteilerfreiheit von $K[t]$ folgt

$$\chi_{A'}(t) = (t-\lambda_2)\cdots(t-\lambda_n),$$

also zerfällt auch $\chi_{A'}(t)$ in Linearfaktoren. Sei α' der auf V' bzgl. der Basis $(v_2, \ldots, v_n)$ durch A' dargestellte Endomorphismus. Nach Induktionsvoraussetzung gibt es eine Basis $(v_2', \ldots, v_n')$ von V' bzgl. derer α' durch eine obere Dreiecksmatrix B' dargestellt wird. Dann wird α bzgl. der Basis $(v_1, v_2', \ldots, v_n')$ von V durch die Matrix $\left(\begin{array}{c|c} \lambda_1 & * \\ \hline 0 & B' \end{array}\right)$ dargestellt, ist also trigonalisierbar. □

Korollar 4.87. *Über $K = \mathbb{C}$ ist jeder Endomorphismus eines endlich-dimensionalen Vektorraums trigonalisierbar.*

Beweis. Über $\mathbb{C}$ zerfällt jedes Polynom in Linearfaktoren („Hauptsatz der Algebra"). □

Sei nun K wieder allgemein und λ ein Eigenwert von $\alpha \in \mathrm{End}(V)$.

Definition 4.88. (i) Die **algebraische Vielfachheit** $\mu_{\mathrm{alg}}(\lambda)$ ist die Vielfachheit von λ als NS von $\chi_\alpha(t)$, d.h. die Potenz von $(t-\lambda)$ in der Primzerlegung von $\chi_\alpha(t)$.
(ii) Die **geometrische Vielfachheit** $\mu_{\mathrm{geo}}(\lambda)$ ist gleich $\dim V_\lambda$.

Satz 4.89. *Es gilt*

$$\mu_{\mathrm{geo}}(\lambda) \leq \mu_{\mathrm{alg}}(\lambda).$$

Beweis. Sei $r = \mu_{\text{geo}}(\lambda)$ und $v_1, \ldots, v_r$ eine Basis von V_λ. Ergänzen wir zu einer Basis $(v_1, \ldots, v_r, v_{r+1}, \ldots, v_n)$, so wird α durch eine Matrix der Form $A = \left(\begin{array}{c|c} \lambda E_r & * \\ \hline 0 & A' \end{array}\right)$ dargestellt. Also gilt $\chi_\alpha(t) = \chi_A(t) = (t-\lambda)^r \cdot \chi_{A'}(t)$. Dies impliziert $\mu_{\text{alg}}(\lambda) \geq r$. □

Satz 4.90. *Für einen Endomorphismus α auf dem n-dimensionalen K-Vektorraum V gilt*

$$\alpha \text{ diagonalisierbar} \iff \sum_{\lambda \text{ EW von } \alpha} \mu_{\text{geo}}(\lambda) = n$$

$$\alpha \text{ trigonalisierbar} \iff \sum_{\lambda \text{ EW von } \alpha} \mu_{\text{alg}}(\lambda) = n.$$

Beweis. Es seien $\lambda_1, \ldots, \lambda_r$ die (verschiedenen) Eigenwerte von α. Gilt

$$\sum_{i=1}^{r} \mu_{\text{alg}}(\lambda) = n = \deg \chi_\alpha(t),$$

so folgt

$$\chi_\alpha(t) = (t - \lambda_1)^{\mu_{\text{alg}}(\lambda_1)} \cdots (t - \lambda_r)^{\mu_{\text{alg}}(\lambda_r)},$$

und nach 4.86 ist α trigonalisierbar. Ist umgekehrt α trigonalisierbar, so zerfällt χ_α nach 4.86 in Linearfaktoren und es folgt $\sum_{\lambda \, EW} \mu_{\text{alg}}(\lambda) = n$.

Ist α diagonalisierbar, so zerfällt V in die direkte Summe der Eigenräume, daher gilt

$$n = \dim V = \sum_{\lambda \, EW} \dim V_\lambda = \sum_{\lambda \, EW} \mu_{\text{geo}}(\lambda).$$

Gelte umgekehrt diese Formel. Wir betrachten den natürlichen Homomorphismus

$$\varphi : \bigoplus_{i=1}^{r} V_{\lambda_i} \longrightarrow V, \ (v_1, \ldots, v_r) \longmapsto v_1 + \ldots + v_r$$

und zeigen, dass φ ein Isomorphismus ist. Nach Voraussetzung haben Quelle und Ziel die gleiche Dimension, also gzz., dass φ injektiv ist. Dies folgt aus 4.83. Mit Hilfe des Isomorphismus ϕ erhalten wir eine Basis von V aus Eigenvektoren von α, also ist α diagonalisierbar. □

Kapitel 5

Bilinearformen

Wir betrachten Bilinearformen (2-Formen) auf einem Vektorraum V

$$\gamma : V \times V \longrightarrow K,$$

d.h. γ ist in jedem Argument linear:

$$\gamma(av_1 + bv_2, w) = a\gamma(v_1, w) + b\gamma(v_2, w)$$

$$\gamma(v, aw_1 + bw_2) = a\gamma(v, w_1) + b(v, w_2).$$

5.1 Bilinearformen

Definition 5.1. Sei V ein endlich-dimensionaler Vektorraum mit Basis $(v_1, \ldots, v_n)$ und

$$\gamma : V \times V \longrightarrow K$$

eine Bilinearform. Die Matrix

$$G = (g_{ij}) = (\gamma(v_i, v_j))$$

heißt die **Fundamentalmatrix** von γ bzgl. dieser Basis.

Da γ bilinear ist, gilt für Vektoren $v = \sum a_i v_i$ und $w = \sum b_j v_j$

$$(*) \qquad \gamma(v, w) = \gamma(\sum a_i v_i, \sum b_j v_j) = (a_1, \ldots, a_n) G \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a^t G b \in K,$$

weshalb die Bilinearform γ durch ihre Fundamentalmatrix G schon eindeutig bestimmt ist. Umgekehrt definiert jede Matrix $G \in M_{n,n}(K)$ mit Hilfe der Gleichung $(*)$ eine Bilinearform $\gamma : V \times V \to K$ mit Fundamentalmatrix G.

Die Menge $\mathrm{Bil}(V)$ aller Bilinearformen auf V wird zum Vektorraum durch

$$(a\gamma_1 + b\gamma_2)(v,w) := a\gamma_1(v,w) + b\gamma_2(v,w), \quad a,b \in K.$$

Sind G_1 und G_2 die Fundamentalmatrizen zu γ_1 und γ_2, so ist $aG_1 + bG_2$ die Fundamentalmatrix zu $a\gamma_1 + b\gamma_2$. Wir erhalten daher

Lemma 5.2. *Sei V ein n-dimensionaler K-Vektorraum und sei $\underline{v} = (v_1, \ldots, v_n)$ eine Basis von V. Dann gibt es einen Isomorphismus von Vektorräumen*

$$\begin{array}{rccc} \varphi_{\underline{v}} : \mathrm{Bil}(V) & \longrightarrow & M_{n,n}(K) \\ \gamma & \longmapsto & G. \end{array}$$

Wie ändert sich die Fundamentalmatrix G bei Basiswechsel?
Sei $\underline{w} = (w_1, \ldots, w_n)$ eine weitere Basis und $S = M_{\underline{v}}^{\underline{w}}(\mathrm{id}_V)$ die Transformationsmatrix. Dann ist die Fundamentalmatrix von γ bzgl. $\underline{w}$ gegeben durch

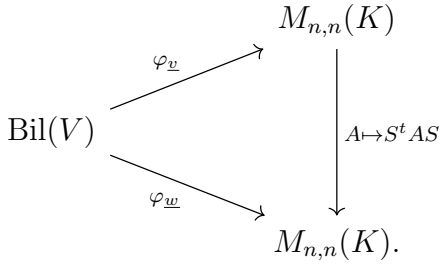
$$\begin{aligned} G' = (g'_{ij}) &= (\gamma(w_i, w_j))_{ij} \\ &= \left(\gamma\left(\sum_{k=1}^{n} s_{ki} v_k, \sum_{\ell=1}^{n} s_{\ell j} v_\ell\right)\right)_{ij} \\ &= \left(\sum_{k=1}^{n}\sum_{\ell=1}^{n} s_{ki} g_{k\ell} s_{\ell j}\right)_{ij} \\ &= S^t G S. \end{aligned}$$

Daher wird das Basiswechselverhalten wie folgt beschrieben:

Lemma 5.3. *Sei V ein n-dimensionaler K-Vektorraum und seien $\underline{v} = (v_1, \ldots, v_n)$ und $\underline{w} = (w_1, \ldots, w_n)$ Basen von V. Ist $S = M_{\underline{v}}^{\underline{w}}(\mathrm{id}_V)$, so gilt*

$$\varphi_{\underline{w}}(\gamma) = S^t \varphi_{\underline{v}}(\gamma) S,$$

d.h. es kommutiert das Diagramm



Bemerkung 5.4. Beim Basiswechsel $G \to S^t G S$ gilt

$$\det(S^t G S) = \det(S)^2 \cdot \det(G).$$

D.h. die Determinante der Fundamentalmatrix ist *nicht* basisunabhängig. Immerhin kann man ablesen, ob $\det(G) \neq 0$ gilt.

Sei $\gamma : V \times V \to K$ eine Bilinearform. Die assoziierte Abbildung

$$\Gamma : V \longrightarrow V^*, \quad \Gamma(v)(w) := \gamma(v, w),$$

ist linear (elementare Rechnung). Umgekehrt definiert jede lineare Abbildung $\Gamma : V \to V^*$ eine Bilinearform $\gamma : V \times V \to K$ durch $\gamma(v, w) = \Gamma(v)(w)$.

Definition 5.5. Eine Bilinearform $\gamma : V \times V \to K$ heißt **nicht ausgeartet**, wenn die zugehörige Abbildung $\Gamma : V \to V^*$ ein Isomorphismus ist (und anderenfalls ausgeartet).

Wegen $\dim V^* = \dim V$ (2.68) ist der Homomorphismus $\Gamma : V \to V^*$ genau dann ein Isomorphismus, wenn er injektiv ist (2.56). Daher ist $\gamma : V \times V \to K$ genau dann nicht ausgeartet, wenn die folgende Implikation gilt:

$$\gamma(v, w) = 0 \text{ für alle } w \in V \Longrightarrow v = 0.$$

Lemma 5.6. *Sei γ eine Bilinearform $\gamma : V \times V \to K$ auf dem n-dimensionalen K-Vektorraum V. Es sei $\underline{v} = (v_1, \ldots, v_n)$ eine Basis von V und $G = \varphi_{\underline{v}}(\gamma) \in M_{n,n}(K)$ die Fundamentalmatrix von γ bzgl. $\underline{v}$. Dann sind die folgenden Aussagen äquivalent.*

(i) *γ ist nicht-ausgeartet.*

(ii) *G ist invertierbar.*

Beweis. Sei $\underline{v}^* = (v_1^*, \ldots, v_n^*)$ die zu $\underline{v}$ duale Basis von V^*, d.h. $v_i^*(v_j) = \delta_{ij}$. Wir betrachten die zu γ assoziierte Abbildung $\Gamma : V \to V^*$.
Behauptung: Es gilt

$$\Gamma(v_i) = \gamma(v_i, v_1)v_1^* + \cdots + \gamma(v_i, v_n)v_n^*.$$

Grund: Per definitionem gilt $\Gamma(v_i)(v_j) = \gamma(v_i, v_j)$. Außerdem gilt

$$\big(\gamma(v_i, v_1)v_1^* + \cdots + \gamma(v_i, v_n)v_n^*\big)(v_j) = \gamma(v_i, v_j).$$

Daher stimmen die beiden Linearformen auf einer Basis überein und sind daher gleich, was die Behauptung zeigt.

Also gilt $M_{\underline{v}^*}^{\underline{v}}(\Gamma) = (\gamma(v_j, v_i))_{ij} = G^t$. Dies impliziert:

γ nicht ausgeartet $\overset{df}{\Leftrightarrow}$ Γ ist Isomorphismus $\Leftrightarrow$ G^t ist invertierbar $\Leftrightarrow$ G ist invertierbar. □

Korollar 5.7. *Ist $\gamma : V \times V \to K$ eine nicht ausgeartete Bilinearform, so gilt die Implikation*

$$(\gamma(v, w) = 0 \text{ für alle } v \in V) \Longrightarrow w = 0.$$

Beweis. Sei G die Fundamentalmatrix von γ zu einer fixierten Basis $(v_1, \ldots, v_n)$ von V. Wir betrachten die Bilinearform $\gamma' : V \times V \to K$, die gegeben ist durch $\gamma'(v, w) := \gamma(w, v)$. Dann hat γ' die Fundamentalmatrix G^t. Nach Voraussetzung ist γ nicht ausgeartet. Daher ist G invertierbar, also auch G^t, d.h. γ' ist nicht ausgeartet. Dies impliziert

$$\gamma(v, w) = 0 \text{ für alle } v \in V \Rightarrow \gamma'(w, v) = 0 \text{ für alle } v \in V \Rightarrow w = 0. \qquad \square$$

Definition 5.8. Eine Bilinearform $\gamma : V \times V \longrightarrow K$ heißt

$$\textbf{symmetrisch} \iff \gamma(v_2, v_1) = \gamma(v_1, v_2) \quad \forall\, v_1, v_2 \in V,$$

$$\textbf{antisymmetrisch} \iff \gamma(v_2, v_1) = -\gamma(v_1, v_2) \quad \forall\, v_1, v_2 \in V.$$

Bemerkung 5.9. Aus 4.22 erhalten wir:

γ alternierend $\Longrightarrow$ γ antisymmetrisch.

Im Fall $\mathrm{char}(K) \neq 2$ gilt auch die Umkehrung, wegen

$$\gamma(v, v) = -\gamma(v, v) \Longrightarrow 2\gamma(v, v) = 0 \overset{1/2 \in K}{\Longrightarrow} \gamma(v, v) = 0 \; \forall\, v \in V.$$

Lemma 5.10. *Sei $\gamma : V \times V \to K$ eine Bilinearform und $\underline{v} = (v_1, \ldots, v_n)$ eine Basis von V. Sei $G = (g_{ij}) = \varphi_{\underline{v}}(\gamma)$ die Fundamentalmatrix. Dann gilt*

(i) *γ symmetrisch $\iff$ G ist symmetrische Matrix (d.h. $G^t = G$).*

(ii) *γ antisymmetrisch $\iff$ G ist antisymmetrische Matrix (d.h. $G^t = -G$).*

Beweis. (i) ($\Longrightarrow$): $g_{ij} = \gamma(v_i, v_j) = \gamma(v_j, v_i) = g_{ji}$.
($\Longleftarrow$): Sei $v = \lambda_1 v_1 + \cdots + \lambda_n v_n,\ w = \mu_1 v_1 + \cdots + \mu_n v_n$ und sei G symmetrisch. Dann gilt

$$\gamma(v, w) = (\lambda_1, \ldots, \lambda_n) G \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} = (\mu_1, \ldots, \mu_n) G^t \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \gamma(w, v)$$

(ii) analog. $\square$

5.2 Quadratische Räume

Sei K ein Körper, $\operatorname{char} K \neq 2$.

Definition 5.11. Ein n-dimensionaler K-Vektorraum V zusammen mit einer symmetrischen Bilinearform $\gamma : V \times V \to K$ heißt **quadratischer Raum** der Dimension n über K. Eine Basis $(v_1, \ldots, v_n)$ von V heißt **Orthogonalbasis**, wenn $\gamma(v_i, v_j) = 0$ für $i \neq j$ gilt.

Bemerkung 5.12. $(v_1, \ldots, v_n)$ ist genau dann eine Orthogonalbasis, wenn die Fundamentalmatrix $G = (\gamma(v_i, v_j))$ eine Diagonalmatrix ist.

Der Kürze halber schreiben wir von jetzt an auch $\gamma(v, w) = \langle v, w \rangle$.

Theorem 5.13. *Sei (V, γ) ein quadratischer Raum. Dann gibt es eine Orthogonalbasis $(v_1, \ldots, v_n)$.*

Beweis. Induktion über die Dimension. Der Fall $n = 1$ ist trivial.
Sei $n \geq 2$. Gilt $\langle v, v \rangle = 0$ für alle $v \in V$, so gilt auch $\langle v + w, v + w \rangle = 2\langle v, w \rangle = 0$ für alle $v, w \in V$ und wegen $\operatorname{char} K \neq 2$ ist γ identisch 0. In diesem Fall ist jede Basis orthogonal. Ansonsten existiert ein $v_1 \in V$ mit $\langle v_1, v_1 \rangle =: a_1 \neq 0$. Sei

$$H = \{w \in V \mid \langle v_1, w \rangle = 0\}.$$

Dann gilt $H = \operatorname{Kern}(\Gamma(v_1) : V \to K)$, also $\dim H \in \{n, n-1\}$ nach der Dimensionsformel. Wegen $v_1 \notin H$ gilt $\dim H = n - 1$ und $V \cong Kv_1 \oplus H$.
Nun ist $(H, \gamma|_{H \times H})$ ein quadratischer Raum der Dimension $n - 1$. Nach Induktionsvoraussetzung existiert eine Orthogonalbasis $v_2, \ldots, v_n$ von H. Dann ist $(v_1, \ldots, v_n)$ eine Basis von V, und die Fundamentalmatrix ist diagonal wegen $\langle v_i, v_j \rangle = 0$ für $i \neq j$. □

Korollar 5.14. *Sei K ein Körper der Charakteristik $\neq 2$ und $A \in M_{n,n}(K)$ eine symmetrische Matrix. Dann gibt es eine Matrix $S \in \mathrm{GL}_n(K)$, so dass $S^t AS$ Diagonalgestalt hat.*

Beweis. Bezüglich der Standardbasis definiert die Matrix A eine symmetrische Bilinearform γ auf dem K^n. Bzgl. einer Orthogonalbasis des K^n hat die Fundamentalmatrix von γ Diagonalgestalt. Der Basiswechsel von der Standardbasis zu dieser Orthogonalbasis überführt A in $S^t AS$ für ein $S \in \mathrm{GL}_n(K)$ und $S^t AS$ hat Diagonalgestalt. □

Definition 5.15. Es seien (V_1, γ_1) und (V_2, γ_2) zwei quadratische Räume. Ein **Homomorphismus quadratischer Räume**

$$f : (V_1, \gamma_1) \longrightarrow (V_2, \gamma_2)$$

ist ein Vektorraumhomomorphismus $f : V_1 \to V_2$, so dass gilt:

$$\gamma_2(f(v_1), f(v_1')) = \gamma_1(v_1, v_1')$$

für alle $v_1, v_1' \in V_1$.

Definition 5.16. Sind (V_1, γ_1) und (V_2, γ_2) zwei quadratische Räume, so heißt (V, γ) mit $V = V_1 \oplus V_2$ und

$$\gamma\big((v_1, v_2), (v_1', v_2')\big) = \gamma_1(v_1, v_1') + \gamma_2(v_2, v_2'),\ v_1, v_1' \in V_1,\ v_2, v_2' \in V_2,$$

die **orthogonale direkte Summe** von (V_1, γ_1) und (V_2, γ_2).
Bezeichnung: $(V, \gamma) = (V_1, \gamma_1) \hat{\oplus} (V_2, \gamma_2)$, oder einfach $V = V_1 \hat{\oplus} V_2$.

Definition/Lemma 5.17. *Seien U_1, U_2 zwei Untervektorräume eines quadratischen Raumes (V, γ). Dann ist der induzierte Homomorphismus*

$$f : (U_1, \gamma|_{U_1}) \hat{\oplus} (U_2, \gamma|_{U_2}) \longrightarrow (V, \gamma),\ f(u_1, u_2) = u_1 + u_2,$$

genau dann ein Homomorphismus quadratischer Räume, wenn $\gamma(u_1, u_2) = 0$ für alle $u_1 \in U_1$, $u_2 \in U_2$ gilt. Ist dies der Fall und ist überdies f ein Isomorphismus (dies ist äquivalent zu $U_1 \cap U_2 = \{0\}$ und $U_1 + U_2 = V$, vgl. 2.24), so sagt man, dass V die **orthogonale direkte Summe** *seiner Unterräume U_1 und U_2 ist, und schreibt $V = U_1 \hat{\oplus} U_2$.*

Beweis. Sei h die Bilinearform auf $(U_1, \gamma|_{U_1}) \hat{\oplus} (U_2, \gamma|_{U_2})$, siehe Definition 5.16. Für $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$ gilt

$$h((u_1, u_2), (u_1', u_2')) = \gamma(u_1, u_1') + \gamma(u_2, u_2').$$

Es ist f genau dann ein Homomorphismus, wenn für beliebige $u_1, u_1' \in U_1, u_2, u_2' \in U_2$ gilt

$$h((u_1, u_2), (u_1', u_2')) = \gamma(f(u_1, u_2), f(u_1', u_2')) = \gamma(u_1 + u_2, u_1' + u_2'),$$

also

$$\gamma(u_1, u_1') + \gamma(u_2, u_2') = \gamma(u_1, u_1') + \gamma(u_1, u_2') + \gamma(u_2, u_1') + \gamma(u_2, u_2'),$$

d.h.

$$0 = \gamma(u_1, u_2') + \gamma(u_1', u_2)\ \forall\ u_1, u_1' \in U_1,\ u_2, u_2' \in U_2.$$

Dies ist äquivalent dazu (setze z.B. $u_2' = 0$), dass $\gamma(u_1, u_2) = 0$ für alle $u_1 \in U_1$, $u_2 \in U_2$ gilt. □

Über $\mathbb{C}$ ist alles etwas einfacher:

Satz 5.18. *Sei (V, γ) ein quadratischer Raum über $\mathbb{C}$. Dann existiert eine Orthogonalbasis $(v_1, \ldots, v_n)$ von V, so dass $\lambda_i = \gamma(v_i, v_i) \in \{0, 1\}$ für alle i. Die Zahlen $r_0 =$ Anzahl der λ_i's $= 0$ und $r =$ Anzahl der λ_i's $= 1$ sind unabhängig von der Wahl der Basis.*

Beweis. Sei $(\tilde{v}_1, \dots, \tilde{v}_n)$ eine Orthogonalbasis. Setze

$$v_i = \begin{cases} \tilde{v}_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) = 0 \\ \frac{1}{\sqrt{\tilde{\lambda}_i}} \tilde{v}_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) \neq 0 \end{cases}$$

Hier ist $\sqrt{\tilde{\lambda}_i}$ eine beliebig gewählte komplexe Zahl α mit $\alpha^2 = \tilde{\lambda}_i$.
Dann ist $(v_1, \dots v_n)$ eine OB mit $\lambda_i = \langle v_i, v_i \rangle \in \{0, 1\}$. Für die Fundamentalmatrix $G = \mathrm{diag}(\lambda_i)$ gilt nun $r = \mathrm{Rg}(G)$, $r_0 = n - r$. Bzgl. einer anderen OB hat γ die Fundamentalmatrix $S^t G S$ für ein $S \in \mathrm{GL}_n(\mathbb{C})$, und nach 3.27 gilt $\mathrm{Rg}(S^t G S) = \mathrm{Rg}(G)$. Daher sind r und r_0 unabhängig von der Auswahl der OB. □

Wir können die OB aus 5.18 noch so umsortieren, dass zuerst die Einsen und dann die Nullen auftreten. In Matrizen liest sich das Ergebnis dann folgendermaßen:

Korollar 5.19. *Sei G eine symmetrische komplexe $n \times n$-Matrix. Dann existiert ein $S \in \mathrm{GL}_n(\mathbb{C})$, so dass*

$$S^t G S = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Die Zahl $r = \mathrm{Rg}(G)$ ist unabhängig von der Wahl von S.

Über $\mathbb{R}$.

Satz 5.20. *Sei (V, γ) ein quadratischer Raum über $\mathbb{R}$. Dann existiert eine OB $(v_1, \dots, v_n)$ von V, so dass $\lambda_i = \gamma(v_i, v_i) \in \{0, \pm 1\}$ für alle i. Die Zahlen*

$$r_0 = \quad \textit{Anz. der} \quad \lambda_i = 0$$

$$r_+ = \quad \textit{Anz. der} \quad \lambda_i = 1$$

$$r_- = \quad \textit{Anz. der} \quad \lambda_i = -1$$

sind unabhängig von der Wahl der Basis.

Beweis. Sei $(\tilde{v}_1, \dots, \tilde{v}_n)$ eine OB. Setze

$$v_i = \begin{cases} \tilde{v}_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) = 0 \\ \frac{1}{\sqrt{|\tilde{\lambda}_i|}} v_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) \neq 0. \end{cases}$$

Wir erhalten die gewünschte OB mit $G = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ und $\lambda_i \in \{0 \pm 1\}$. Wie im Komplexen erhalten wir, dass $r_+ + r_- = \mathrm{Rg}(G)$ und $r_0 = n - \mathrm{Rg}(G)$ von der Basis unabhängig sind. Daher genügt es zu zeigen, dass r_+ unabhängig von der Auswahl der OB ist. Sei V_+ der Untervektorraum, der von den v_i mit $\lambda_i = 1$ erzeugt ist. Analog V_-, V_0. Dann gilt $V = V_+ \oplus V_- \oplus V_0$. Setze

$$a = \max(\dim(W) \mid W \subset V \text{ mit } \gamma(w,w) > 0 \text{ für alle } 0 \neq w \in W).$$

Zunächst hat V_+ diese Eigenschaft, also $a \geq r_+$. Wäre $a > r_+$, so existierte ein Untervektorraum $W \subset V$ mit der obigen Eigenschaft und $\dim W > r_+$. Hieraus folgt $\dim W + \dim V_- + \dim V_0 > n$. Die Dimensionsformel liefert $W \cap (V_- \oplus V_0) > 0$, es gibt also ein $w \in W$ mit $\gamma(w,w) > 0$ und $\gamma(w,w) \leq 0$. Dieser Widerspruch zeigt $r_+ = a$ und a ist unabhängig von der Auswahl der OB, also auch r_+. □

Nach geeignetem Umsortieren der Basis liest sich das Ergebnis in Matrizen wie folgt:

Korollar 5.21. *(**Sylvesterscher Trägheitssatz**). Sei $G \in M_{n,n}(\mathbb{R})$ eine symmetrische reelle $n \times n$ Matrix. Dann existiert ein $S \in \mathrm{GL}_n(\mathbb{R})$, so dass*

$$S^t G S = \left(\begin{array}{c|c|c} E_{r_+} & & \\ \hline & -E_{r_-} & \\ \hline & & 0_{r_0} \end{array}\right)$$

Die Zahlen r_+, r_- und r_0 sind unabhängig von der Auswahl von S.

5.3 Euklidische Räume

Definition 5.22. Eine symmetrische Bilinearform $\gamma : V \times V \to \mathbb{R}$ auf einem endlich-dimensionalen $\mathbb{R}$-Vektorraum V heißt **positiv definit** (bzw. **positiv semidefinit**), wenn $\gamma(v,v) > 0$ (bzw. $\gamma(v,v) \geq 0$) für alle $v \in V \setminus \{0\}$ gilt. Analog definiert sich **negativ (semi-)definit**.

Beispiel 5.23. $\mathbb{R}^n$ mit dem Standardskalarprodukt

$$\langle x, y \rangle = x^t y = \sum_i x_i y_i$$

ist positiv definit, wegen

$$\langle x, x \rangle = x_1^2 + \cdots + x_n^2.$$

Definition 5.24. Ein **euklidischer Raum** ist ein endlich-dimensionaler reeller Vektorraum mit einer positiv definiten symmetrischen Bilinearform. Für ein $v \in V$ nennt man $\|v\| = \sqrt{\langle v, v\rangle}$ die **Norm** von v. Zwei euklidische Vektorräume V und W heißen **isometrisch**, wenn es eine **Isometrie** gibt, d.h. einen Vektorraumisomorphismus $\varphi : V \xrightarrow{\sim} W$ mit

$$\langle \varphi(v_1), \varphi(v_2)\rangle_W = \langle v_1, v_2\rangle_V$$

für alle $v_1, v_2 \in V$. Eine Basis $e_1, \ldots, e_n$ eines euklidischen Vektorraums heißt **Orthonormalbasis**, wenn $\langle e_i, e_j\rangle = \delta_{ij}$ gilt.

Theorem 5.25. *Jeder euklidische Vektorraum (V, γ) besitzt eine Orthonormalbasis.*

Beweis. Sei $(v_1, \ldots, v_n)$ eine Orthogonalbasis von V und G die Fundamentalmatrix von γ bzgl. $(v_1, \ldots, v_n)$. Auf der Diagonale stehen die Werte $\langle v_i, v_i\rangle > 0$. Setze nun $e_i = \frac{1}{\|v_i\|} v_i$. Dann gilt $\langle e_i, e_j\rangle = \delta_{ij}$. □

Korollar 5.26. *Eine positiv definite symmetrische Bilinearform ist nicht ausgeartet. Es gibt eine Basis bzgl. derer sie durch die Einheitsmatrix dargestellt wird.*

Korollar 5.27. *Ein euklidischer Raum (V, γ) mit $\dim_{\mathbb{R}} V = n$ ist isometrisch zum $\mathbb{R}^n$ mit dem Standardskalarprodukt.*

Beweis. Sei $(v_1, \ldots, v_n)$ eine ONB von V. Dann ist $\varphi : (\mathbb{R}^n, \langle\ ,\ \rangle_{\text{Standard}}) \to (V, \gamma)$, $e_i \mapsto v_i$, eine Isometrie. □

Korollar 5.28. *Sei (V, γ) ein euklidischer Raum. Dann gelten*

(i) *Dreiecksungleichung:* $\|x + y\| \leq \|x\| + \|y\|$.
(ii) *Schwarzsche Ungleichung:* $|\langle x, y\rangle| \leq \|x\| \cdot \|y\|$.

Beweis. Dies wurde in 2.9 und 2.8 für den $\mathbb{R}^n$ mit dem Standardskalarprodukt bewiesen. Nach 5.27 gelten die Ungleichungen für jeden euklidischen Vektorraum. □

Ganz analog haben wir jetzt alle Begriffe und Sätze, die wir für den $\mathbb{R}^n$ haben für beliebige euklidische Vektorräume. Z.B.

Korollar 5.29 (Satz des Pythagoras)**.** *Sind x und y orthogonal, d.h. $\langle x, y\rangle = 0$, so gilt $\|x + y\|^2 = \|x\|^2 + \|y\|^2$.*

Die Orthogonalprojektion auf einen Vektor können wir jetzt auf Untervektorräume verallgemeinern.

Definition 5.30. Sei V ein euklidischer Raum und $U \subset V$ ein Untervektorraum. Der Untervektorraum

$$U^\perp = \{v \in V \mid \langle v, u\rangle = 0 \text{ für alle } u \in U\}$$

heißt das **orthogonale Komplement** zu U.

Satz 5.31. *Es gilt* $V = U \hat{\oplus} U^\perp$.

Beweis. Ist $u \in U \cap U^\perp$ so gilt $\langle u, u\rangle = 0$, also $u = 0 \Rightarrow U \cap U^\perp = 0$. Es bleibt zu zeigen: $U + U^\perp = V$. Sei $(u_1, \ldots, u_m)$ eine ONB von U. Für $v \in V$ sei $v' = v - \sum_{i=1}^{m} \langle v, u_i\rangle u_i$.
Dann gilt $\langle v', u_i\rangle = \langle v, u_i\rangle - \langle v, u_i\rangle = 0$ für $i = 1, \ldots, m$, also $v' \in U^\perp$ und natürlich $\sum_{i=1}^{m} \langle v, u_i\rangle u_i \in U$. Daher gilt $V = U \oplus U^\perp$. Schließlich gilt $\langle u, v\rangle = \langle v, u\rangle = 0$ für alle $u \in U, v \in U^\perp$, weshalb die Summe orthogonal ist, siehe 5.17. □

Definition 5.32. Die Projektion $V \xrightarrow{\sim} U \oplus U^\perp \xrightarrow{p_1} U$ heißt die **Orthogonalprojektion** von V auf U.

5.4 Gram-Schmidt-Orthonormalisierung

Explizites Verfahren zur Bestimmung einer ONB (Gram-Schmidt-Verfahren).
Sei (V, γ) ein euklidischer Raum und $(v_1, \ldots, v_n)$ eine Basis. Wir verändern die Basis $(v_1, \ldots, v_n)$ in n Schritten zu einer ONB $(w_1, \ldots, w_n)$.

Im 1. Schritt $w_1 := \frac{1}{\|v_1\|} \cdot v_1$,
Sei $k \geq 2$ und sei eine ONB $w_1, \ldots, w_{k-1}$ von $\mathrm{Lin}(v_1, \ldots, v_{k-1})$ bereits konstruiert.
Im k-ten Schritt setze zunächst:

$$w_k' = v_k - \sum_{i=1}^{k-1} \gamma(v_k, w_i) w_i)$$

Dann gilt für $i = 1, \ldots, k-1$

$$\begin{aligned} \gamma(w_k', w_i) &= \gamma\big(v_k - \sum_{j=1}^{k-1} \gamma(v_k, w_j) w_j, w_i\big) \\ &= \gamma(v_k, w_i) - \gamma(v_k, w_i) \cdot \gamma(w_i, w_i) \\ &= 0. \end{aligned}$$

Außerdem gilt $v_k \notin \mathrm{Lin}(v_1, \ldots, v_{k-1}) = \mathrm{Lin}(w_1, \ldots, w_{k-1})$, also folgt auch $w_k' \notin \mathrm{Lin}(w_1, \ldots, w_{k-1})$. Hieraus folgt, dass $(w_1, \ldots, w_{k-1}, w_k')$ eine Orthogonalbasis von $\mathrm{Lin}(v_1, \ldots, v_k)$ ist. Schließlich setzen wir

$$w_k = \frac{w_k'}{\|w_k'\|}.$$

Wir lassen diesen Prozess durchlaufen und erhalten die ONB $(w_1, \ldots, w_n)$ von (V, γ) .

Beispiel 5.33. Im $\mathbb{R}^2$ mit dem Standardskalarprodukt sei die folgende Basis gegeben: $v_1 = (3,1)^t$, $v_2 = (2,2)^t$.
Wir berechnen: $\|v_1\| = \sqrt{3^2+1^2} = \sqrt{10}$. Also $w_1 = (3/\sqrt{10}, 1/\sqrt{10})^t$.
Zweiter Schritt:
$v_2 - \langle v_2, w_1\rangle w_1 = (2,2)^t - \langle (2,2)^t, (3/\sqrt{10}, 1/\sqrt{10})^t\rangle (3/\sqrt{10}, 1/\sqrt{10})^t$
$= (2,2)^t - 8/\sqrt{10}\cdot(3/\sqrt{10}, 1/\sqrt{10})^t = (2,2)^t - (24/10, 8/10)^t = (-4/10, 12/10)^t = (-2/5, 6/5)^t =: w_2'$.

Wir erhalten $\|w_2'\| = \sqrt{40/25} = 2\sqrt{10}/5$ und somit

$$w_2 = 5/(2\sqrt{10}) \cdot (-2/5, 6/5)^t = 1/\sqrt{10}(-1,3)^t.$$

Daher ist $(3/\sqrt{10}, 1/\sqrt{10})^t, (-1/\sqrt{10}, 3/\sqrt{10})^t)$ eine ONB. Die Standardbasis ist natürlich auch eine ONB, aber wir erhalten sie hier nicht aus dem Gram-Schmidt-Verfahren.

Bemerkung 5.34. Im k-ten Schritt des Gram-Schmidt-Verfahrens entsteht w_k als Linearkombination von $v_1, \ldots, v_k$. Daher ist die Transformationmatrix von $(v_1, \ldots, v_n)$ zu $(w_1, \ldots, w_n)$ eine obere Dreiecksmatrix.

Definition 5.35. Eine symmetrische reelle Matrix G heißt **positiv definit** (Bezeichnung: $G > 0$), wenn die zugehörige Bilinearform

$$(x, y) \longmapsto x^t G y$$

positiv definit ist.

Satz 5.36. *Für eine reelle symmetrische Matrix G sind die folgenden Aussagen äquivalent:*

(i) *G ist positiv definit.*

(ii) *es existiert eine invertierbare obere Dreiecksmatrix T mit $G = T^t T$.*

(iii) *es existiert eine invertierbare Matrix T mit $G = T^t T$.*

Beweis. (i)⇒(ii): Wir betrachten den euklidischen Raum $(\mathbb{R}^n, \gamma)$ mit $\gamma(x,y) = x^tGy$. Ist T die Transformationsmatrix von der Standardbasis des $\mathbb{R}^n$ zu einer ONB bzgl. γ, so gilt

$$E = (T^{-1})^t G (T^{-1})$$

also $T^tT = G$. Konstruieren wir die ONB mit Hilfe des Gram-Schmidt-Verfahrens, so ist T eine (invertierbare) obere Dreiecksmatrix.
(ii)⇒ (iii) ist trivial
(iii)⇒(i) Sei $G = T^tT$. Dann gilt für $x \in \mathbb{R}^n \setminus \{0\}$ beliebig

$$\gamma(x,x) = x^tGx = x^tT^tTx = \langle Tx, Tx\rangle_{\text{Standard}} > 0.$$

Daher ist G positiv definit. □

Definition 5.37. Es sei $A = (a_{ij})_{\substack{i=1,\dots,n\\ j=1,\dots,n}}$ eine $n \times n$-Matrix. Für $k = 1, \dots, n$ sei A_k die $k \times k$ Matrix

$$A_k = (a_{ij})_{\substack{i=1,\dots,k\\ j=1,\dots,k}}.$$

Die Determinante $\det(A_k)$ heißt der ***k*-te Hauptminor** von A.

Satz 5.38 (Hauptminorenkriterium)**.** *Eine symmetrische reelle $n\times n$-Matrix G ist genau dann positiv definit, wenn die k-ten Hauptminoren $k = 1, \dots, n$ sämtlich größer als Null sind.*

Beweis. Ist G positiv definit, so gilt $G = T^tT$ für eine invertierbare Matrix T und also $\det(G) = \det(T^t)\det(T) = \det(T)^2 > 0$. Schränkt man die positiv definite Bilinearform $\gamma(x,y) = x^tGy$ auf dem $\mathbb{R}^n$ auf den von $e_1, \dots, e_k$ aufgespannten Unterraum ein, erhält man eine positiv definite Bilinearform auf dem $\mathbb{R}^k$, die durch die Matrix G_k gegeben ist. Daher ist G_k positiv definit. Nach dem ersten Teil des Beweises erhalten wir $\det(G_k) > 0$ für $k = 1, \dots, n$.

Sei umgekehrt $\det G_k > 0$ für $k = 1, \dots, n$. Wir schauen uns das Gram-Schmidt-Verfahren an, ohne zu wissen, dass die Form $\gamma(x,y) = x^tGy$ positiv definit ist. Wenn das Verfahren durchläuft, erhalten wir eine Orthonormalbasis, und G ist positiv definit. Wir starten mit der kanonischen Basis $(e_1, \dots, e_n)$. Hinreichend für das Durchlaufen des Algorithmus: für jedes k gilt $\gamma(w'_k, w'_k) > 0$ für den Vektor

$$w'_k := e_k - \sum_{i=1}^{k-1} \gamma(e_k, w_i) w_i.$$

Das sieht man so: Die Form $\gamma|_{\mathbb{R}^k}$ auf dem $\mathbb{R}^k$ wird bzgl. der kanonischen Basis durch die Matrix G_k dargestellt. Es ist $(w_1, \dots, w_{k-1}, w'_k)$ eine Orthogonalbasis von $(\mathbb{R}^k, \gamma|_{\mathbb{R}^k})$. Die darstellende $k \times k$ Matrix A hat die Form $\operatorname{diag}(1, \dots, 1, \gamma(w'_k, w'_k))$, hat also insbesondere die Determinante $\gamma(w'_k, w'_k)$. Andererseits gilt $A = T^tG_kT$ für eine invertierbare Matrix T, also gilt

$$\gamma(w'_k, w'_k) = \det(T^tG_kT) = \det(T)^2 \det(G_k) > 0.$$

Daher läuft der Algorithmus durch und wir erhalten eine ONB. Insbesondere ist G positiv definit. □

Wie findet man zu einer positiv definiten symmetrischen Matrix G ein T mit $T^tT = G$?

Antwort: Das Gram-Schmidt-Verfahren liefert eine ONB des $\mathbb{R}^n$ bzgl. der Bilinearform $\gamma(x,y) = x^tGy$? Die Matrix T ist dann die Transformationsmatrix von der Standardbasis zu dieser ONB.

Wir können das Gram-Schmidt-Verfahren auch direkt an der Matrix durchführen. Dann stellt es sich für $G = (g_{ij}) > 0$ wie folgt dar:

1. Schritt: Setze $a = 1/\sqrt{g_{11}}$ und $D_1 = \mathrm{diag}(a, 1, \ldots, 1)$. Dann bilde $D_1GD_1 = (a_{ij})$. Es gilt $a_{11} = 1$.

2. Schritt: Setze

$$S_1 = \begin{pmatrix} 1 & -a_{12} & -a_{13} & \ldots & -a_{1n} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ddots & & \\ 0 & 0 & & \ldots & 1 \end{pmatrix}.$$

Dann hat $S_1^tD_1GD_1S_1$ die Blockform

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & B \end{array}\right).$$

Dann gehe dann mit B weiter vor, u.s.w. Das Verfahren endet mit D_n (und der Einheitsmatrix) und wir erhalten $G = T^tT$ mit

$$T = (D_1S_1 \cdots D_{n-1}S_{n-1}D_n)^{-1} = D_n^{-1}S_{n-1}^{-1}D_{n-1}^{-1} \cdots S_1^{-1}D_1^{-1}.$$

Die Inversen von Matrizen der Form D_i und S_i sieht man leicht. Es ist

$$\mathrm{diag}(a_1, \ldots, a_n)^{-1} = \mathrm{diag}(a_1^{-1}, \ldots, a_n^{-1})$$

und z.B.

$$\begin{pmatrix} 1 & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ddots & & \\ 0 & 0 & & \ldots & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a_2 & -a_3 & \ldots & -a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ddots & & \\ 0 & 0 & & \ldots & 1 \end{pmatrix}.$$

So erhält man T. Eine ONB erhält man aus den Spalten von T^{-1}.

5.5 Orthogonale Matrizen

Wie sehen Koordinatenwechselmatrizen von einer ONB zur anderen aus?

Definition 5.39. Eine Matrix $A \in M_{n,n}(\mathbb{R})$ heißt **orthogonal**, wenn $A^tA = E$ gilt.

Lemma 5.40. *Es sei A eine orthogonale Matrix. Dann gilt*
(i) *A ist invertierbar und $A^{-1} = A^t$.*
(ii) $|A| = \pm 1$.
(iii) $A \cdot A^t = E$.

Beweis. (i) folgt aus $A^tA = E$.
(ii) aus $|A| = |A^t|$ und $|A^t| \cdot |A| = |E| = 1$.
(iii) folgt aus $A^t = A^{-1}$. □

Satz 5.41. *Eine Matrix A ist genau dann orthogonal, wenn die assoziierte lineare Abbildung*

$$A : (\mathbb{R}^n, \langle\ ,\ \rangle) \longrightarrow (\mathbb{R}^n, \langle\ ,\ \rangle)$$

eine Isometrie ist.

Beweis. Für $x, y \in \mathbb{R}^n$ gilt $\langle Ax, Ay\rangle = x^tA^tAy$. Daher ist A genau dann eine Isometrie, wenn die durch A^tA gegebene Bilinearform das Standardskalarprodukt ist, d.h. wenn $A^tA = E$ gilt. □

Definition 5.42. Die Menge der orthogonalen $n\times n$-Matrizen wird mit $O(n)$ bezeichnet. $O(n)$ heißt die **orthogonale Gruppe** vom Rang n.

Verifikation der Gruppeneigenschaften: $E_n \in O(n)$ o.k.
$A, B \in O(n) \Rightarrow (A \cdot B)^t \cdot (A \cdot B) = B^tA^tAB = B^tB = E_n$, also $A \cdot B \in O(n)$.
$A \in O(n) \Rightarrow A^tA = E_n \Rightarrow AA^t = E_n \Rightarrow A^{-1} = A^t \in O(n)$.

Definition 5.43. Die Untergruppe

$$SO(n) = \mathrm{Kern}(\det : O(n) \longrightarrow \mathbb{R}^\times)$$

heißt die **spezielle orthogonale Gruppe** vom Rang n.

Bemerkung 5.44. Für $A \in O(n)$ gilt
$A \in SO(n) \Longleftrightarrow A$ erhält die kanonische Orientierung des $\mathbb{R}^n$.

Wir haben in 2.5 definiert, wann zwei Vektoren des $\mathbb{R}^n$ orthogonal sind. Wir verfeinern dies durch die folgende

Definition 5.45 (Winkel zwischen Vektoren)**.** Für $x, y \in \mathbb{R}^n \smallsetminus \{0\}$ heißt

$$\sphericalangle(x,y) = \cos^{-1}\left(\frac{\langle x,y\rangle}{\|x\|\cdot\|y\|}\right) \in [0,\pi]$$

der Winkel zwischen x und y.

Offenbar entspricht Orthogonalität dem Winkel $\pi/2$. Zudem erinnern wir uns an die Abstandsdefinition 2.4

$$d(x,y) = \|x-y\| = \langle x-y, x-y\rangle^{1/2}.$$

Aus 5.41 folgt direkt:

Korollar 5.46. *Orthogonale Matrizen induzieren abstands- und winkeltreue lineare Abbildungen $\mathbb{R}^n \to \mathbb{R}^n$.*

Umgekehrt gilt:

Satz 5.47. *Sei $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ eine (nicht notwendig lineare) Abbildung. Ist φ abstandstreu (d.h. $\|\varphi(x)-\varphi(y)\| = \|x-y\|$ für alle x, y), so gibt es ein $A \in O(n)$ und ein $b \in \mathbb{R}^n$ so dass*

$$\varphi(x) = Ax + b$$

für alle $x \in \mathbb{R}^n$ gilt (d.h. φ ist eine „affine Isometrie“).

Den Beweis lassen wir aus Zeitgründen weg.

5.6 Hauptachsentransformation

Sei (V,γ) ein euklidischer Raum und $f \in \mathrm{End}(V)$.

Definition/Lemma 5.48. *Es existiert genau eine lineare Abbildung $f^* \in \mathrm{End}(V)$ mit*

$$\gamma(v, f(w)) = \gamma(f^*(v), w) \quad \text{für alle } v, w \in V.$$

Diese heißt die **Adjungierte** *zu f. Der Endomorphismus f heißt* **selbstadjungiert**, *wenn $f = f^*$ gilt. Wird f bzgl. einer ONB $(v_1, \dots, v_n)$ durch die Matrix G dargestellt, so wird f^* bzgl. dieser Basis durch G^t dargestellt. Es ist f genau dann selbstadjungiert, wenn G symmetrisch ist.*

Beweis. Sind $g_1, g_2 \in \mathrm{End}(V)$ Abbildungen mit der obigen Eigenschaft, so gilt für alle $v \in V$

$$\gamma\big(g_1(v)-g_2(v), g_1(v)-g_2(v)\big) =$$
$$\gamma\big(g_1(v), g_1(v)-g_2(v)\big) - \gamma\big(g_2(v), g_1(v)-g_2(v)\big)$$
$$= \gamma\big(v, f(g_1(v)-g_2(v))\big) - \gamma\big(v, f(g_1(v)-g_2(v))\big) = 0,$$

also $g_1(v) - g_2(v)$ und folglich $g_1 = g_2$. Dies zeigt die Eindeutigkeit.

Sei nun $(v_1, \ldots, v_n)$ eine ONB, G die Darstellungsmatrix von f und f^* der durch G^t dargestellte Endomorphismus. Dann gilt für $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$, $w = \mu_1 v_1 + \cdots + \mu_n w_n$ folgendes:

$$\gamma(v, f(w)) = (\lambda_1, \ldots, \lambda_n) G \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} =$$

$$(\mu_1, \ldots, \mu_n) G^t \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \gamma(w, f^*(v)) = \gamma(f^*(v), w).$$

Dies zeigt die Existenz und alle anderen Aussagen. □

Lemma 5.49. *Sei (V, γ) ein euklidischer Raum und $f \in \mathrm{End}(V)$ selbstadjungiert. Dann ist die Form*

$$\gamma' : V \times V \to \mathbb{R},\ \gamma'(x, y) = \gamma(f(x), y),$$

eine symmetrische Bilinearform. Umgekehrt entsteht jede symmetrische Bilinearform $\gamma' : V \times V \to \mathbb{R}$ in der oben beschriebenen Weise aus einem selbstadjungierten Endomorphismus $f : V \to V$. Bzgl. einer (jeder) ONB von V ist die Darstellungsmatrix von f gleich der Fundamentalmatrix von γ'.

Beweis. f s.a. $\Rightarrow \gamma'(x, y) = \gamma(f(x), y) = \gamma(x, f(y)) = \gamma(f(y), x) = \gamma'(x, y)$, also ist γ' symmetrisch.

Nun sei umgekehrt eine symmetrische Bilinearform $\gamma' : V \times V \to \mathbb{R}$ gegeben und $x \in V$ fest. Dann ist

$$\psi_x : V \longrightarrow \mathbb{R},\ y \mapsto \gamma'(x, y)$$

ein Element von V^*. Sei $\Gamma : V \xrightarrow{\sim} V^*$ der zu γ assoziierte Isomorphismus (also $\Gamma(x)(y) = \gamma(x, y)$). Dann es gibt ein eindeutig bestimmtes Element $f(x) \in V$ mit $\Gamma(f(x)) = \psi_x$, d.h. es gilt

$$\gamma'(x, y) = \gamma(f(x), y)$$

für alle $x \in V$. Wir erhalten eine Abbildung $f : V \to V$ mit der Eigenschaft

$$\gamma'(x, y) = \gamma(f(x), y) \quad \text{für alle } x, y \in V.$$

Wir zeigen, dass f linear ist, d.h. $f(ax_1+bx_2)=af(x_1)+bf(x_2)$. Dies folgt aus
$\Gamma\big(f(ax_1+bx_2)-af(x_1)-bf(x_2)\big)(y)$
$=\gamma\big(f(ax_1+bx_2)-af(x_1)-bf(x_2),y\big)$
$=\gamma\big(f(ax_1+bx_2,y)\big)-a\gamma\big(f(x_1),y\big)-b\gamma\big(f(x_2),y\big)$
$=\gamma'\big(ax_1+bx_2,y\big)-a\gamma'(x_1,y)-b\gamma'(x_2,y)=0$
für alle $y\in V$, und weil Γ ein Isomorphismus ist.

Schließlich zeigen wir, dass f selbstadjungiert ist. Z.z: $\gamma(f(x),y)=\gamma(x,f(y))$ für alle $x,y\in V$. Dies folgt aus der Symmetrie von γ und γ':

$$\gamma(f(x),y)=\gamma'(x,y)=\gamma'(y,x)=\gamma(f(y),x)=\gamma(x,f(y)).$$

Die Zuordnungen $f\mapsto\gamma'$ und $\gamma'\mapsto f$ sind offenbar invers zueinander.

Es verbleibt, die Aussage über die Matrizen zu zeigen. Ist G die Darstellungsmatrix von f bzgl. einer ONB (für γ) $(v_1,\dots,v_n)$ so gilt für $w=\lambda_1v_1+\dots+\lambda_nv_n,\ w'=\lambda_1'v_1+\dots+\lambda_n'v_n$:

$$\gamma'(w,w')=\gamma(f(w),w')=(\lambda_1,\dots,\lambda_n)G^t\begin{pmatrix}\lambda_1'\\ \vdots\\ \lambda_n'\end{pmatrix}.$$

Daher ist G^t die Fundamentalmatrix von γ'. Schließlich gilt $G=G^t$ weil f selbstadjungiert ist. □

Theorem 5.50 (Spektralsatz für selbstadjungierte Operatoren)**.** *Sei (V,γ) ein euklidischer Raum und $f\in\mathrm{End}(V)$ ein selbstadjungierter Endomorphismus. Dann gibt es eine ONB von V aus Eigenvektoren von f.*

Wir starten mit zwei Lemmata:

Lemma 5.51. *Ist f selbstadjungiert, so zerfällt χ_f über $\mathbb{R}$ in Linearfaktoren.*

Beweis. O.B.d.A. sei $V=\mathbb{R}^n$ und $\gamma=\langle\ ,\ \rangle_{\text{Standard}}$. Dann wird $f:\mathbb{R}^n\to\mathbb{R}^n$ durch eine Matrix $A\in M_{n,n}(\mathbb{R})$ gegeben. Wir können auch die durch A gegebene $\mathbb{C}$-lineare Abbildung $A:\mathbb{C}^n\to\mathbb{C}^n$, $z\mapsto Az$, betrachten, ohne $\chi_A=\chi_f$ zu verändern. Über $\mathbb{C}$ zerfällt χ_A in Linearfaktoren, d.h.

$$\chi_A(t)=(x-\lambda_1)\cdots(x-\lambda_n),\ \lambda_i\in\mathbb{C}.$$

Sei λ eines der λ_i. Z.z. $\lambda\in\mathbb{R}$. Zunächst bemerken wir dass für $z\in\mathbb{C}^n\smallsetminus\{0\}$

$$z^t\overline{z}=\sum_{i=1}^n z_i\overline{z_i}=\sum_{i=1}^n|z_i|^2$$

reell und größer 0 ist. Hier ist $\overline{z}$ die Komplexkonjugierte zu z.

Ist nun $z \in \mathbb{C}^n \setminus \{0\}$ ein Eigenvektor von λ so gilt

$$\lambda \cdot z^t\overline{z} = (\lambda z)^t\overline{z} = (Az)^t\overline{z} = z^tA^t\overline{z} \overset{(A \text{ symm.})}{=} z^tA \cdot \overline{z}$$

$$\overset{(\text{A reell})}{=} z^t\bar{A}\overline{z} = z^t \cdot \overline{Az} = z^t \cdot \overline{\lambda z} = \overline{\lambda} \cdot z^t\overline{z}.$$

Wegen $z^t\overline{z} \neq 0$ folgt $\lambda = \overline{\lambda}$, also $\lambda \in \mathbb{R}$. □

Lemma 5.52. *Sei f selbstadjungiert. Ist U ein Untervektorraum mit $f(U) \subset U$, so gilt $f(U^\perp) \subset U^\perp$.*

Beweis. Sei $v \in U^\perp$. Dann gilt für alle $u \in U$: $\langle u, f(v)\rangle = \langle f(u), v\rangle = 0$. Also $f(v) \in U^\perp$. □

Beweis von Theorem 5.50. Per Induktion über $\dim V$:
Anfang: $\dim V = 1$ trivial.
Schritt: Sei $n = \dim V \geq 2$. Sei $\lambda \in \mathbb{R}$ ein Eigenwert von f (Existenz siehe 5.51) und $v_1 \neq 0$ ein Eigenvektor, d.h. $f(v_1) = \lambda v_1$. Ersetzt man v_1 durch $\frac{v_1}{\|v_1\|}$, so hat man $\|v_1\| = 1$. Sei $U = \mathbb{R}v_1$. Dann gilt $f(U) \subset U$ und $f(U^\perp) \subset U^\perp$ (5.52). Nun gilt $V = U \oplus U^\perp$ (5.31) und $\dim U^\perp = n - 1$. Ist $(v_2, \ldots, v_n)$ eine ONB von $U^\perp$ aus Eigenvektoren zu f, so ist $v_1, \ldots, v_n$ die gesuchte ONB. □

Korollar 5.53. *Sei (V, γ) ein euklidischer Raum und $\gamma' : V \times V \to \mathbb{R}$ eine symmetrische Bilinearform. Dann gibt es eine ONB von (V, γ) die OB für (V, γ') ist, d.h. bezüglich derer die Fundamentalmatrix von γ' Diagonalgestalt hat.*

Beweis. Sei $f : V \to V$ der nach 5.49 eindeutig bestimmte selbstadjungierte Endomorphismus mit $\gamma'(x, y) = \gamma(f(x), y)$. Und sei $(v_1, \ldots, v_n)$ eine ONB von V aus Eigenwerten von f. Gilt $f(v_i) = \lambda_i v_i$, so gilt $\gamma'(v_i, v_j) = \gamma(\lambda_i v_i, v_j) = \lambda_i\gamma(v_i, v_j) = \lambda_i\delta_{ij}$. Daher hat die Fundamentalmatrix von γ' Diagonalgestalt. □

In Matrizen lesen sich diese Ergebnisse so.

Satz 5.54 (Hauptachsentransformation)**.** *Ist G eine symmetrische reelle $n\times n$-Matrix, so existiert ein $T \in SO(n)$, so dass TGT^{-1} eine Diagonalmatrix ist.*

Beweis. Wir betrachten den $\mathbb{R}^n$ mit dem Standardskalarprodukt. Die symmetrische Matrix G definiert einen selbstadjungierten Endomorphismus $f : \mathbb{R}^n \to \mathbb{R}^n$. Ist $(v_1, \ldots, v_n)$ eine ONB des $\mathbb{R}^n$ aus Eigenvektoren von f wie in 5.50 und T die Transformationsmatrix von $(e_1, \ldots, e_n)$ nach $(v_1, \ldots, v_n)$, so gilt $T \in O(n)$. Ersetzt man, falls nötig, v_1 durch $-v_1$, gilt sogar $T \in SO(n)$. Bzgl. $(v_1, \ldots, v_n)$ hat f Diagonalgestalt, d.h. TGT^{-1} hat Diagonalgestalt. □

Korollar 5.55 (Simultane Diagonalisierung)**.** *Sei P eine symmetrische, positivdefinite und G eine beliebige symmetrische reelle $n\times n$-Matrix. Dann existiert ein $T \in \mathrm{GL}_n(\mathbb{R})$ so dass gilt:*

- $T^tPT = E$,
- T^tGT *ist eine Diagonalmatrix.*

Beweis. Dies folgt aus 5.53 indem man den $\mathbb{R}^n$ mit der durch P definierten Bilinearform als euklidischen Raum auffasst. □

5.7 Volumenform

Sei (V, γ) ein euklidischer Raum.
Für den Fall $(\mathbb{R}^3, \langle\ ,\ \rangle)$ hatten wir das Volumen des von drei Vektoren (x, y, z) aufgespannten Spat definiert durch

$$\mathrm{vol}(x, y, z) = \det(x, y, z).$$

Eine Volumenform auf einem n-dimensionalen K-Vektorraum V ist eine nichtverschwindende alternierende n-Form $\alpha : V^n \to K$ (vgl. Abschnitt 4.2).

Satz 5.56. *Sei (V, γ) ein orientierter euklidischer Raum und sei $\underline{v} = (v_1, \ldots, v_n)$ eine orientierte ONB von V. Dann gibt es genau eine Volumenform ω auf V mit $\omega(v_1, \ldots, v_n) = 1$. Ist $\underline{w} = (w_1, \ldots, w_n)$ eine beliebige Basis von V und $G = (\gamma(w_i, w_j))$ die Fundamentalmatrix, so gilt $g := \det G \geq 0$ und*

$$\omega(w_1, \ldots, w_n) = \begin{cases} \sqrt{g} & \text{wenn } \underline{w} \text{ orientiert} \\ -\sqrt{g} & \text{wenn } \underline{w} \text{ nicht orientiert} \end{cases}$$

Insbesondere gilt

$$\omega(w_1, \ldots, w_n) = 1$$

für jede orientierte Orthonormalbasis $(w_1, \ldots, w_n)$.

Beweis. Existenz und Eindeutigkeit von ω folgen aus 4.26. Im Fall $V = \mathbb{R}^n$, $\underline{v} =$ Standardbasis gilt $\omega = \det$. Sei

$$\varphi : (\mathbb{R}^n, \langle\ ,\ \rangle_{\text{Standard}}) \to (V, \gamma)$$

die Isometrie, die durch $\varphi(e_i) = v_i$ gegeben ist. Dann gilt für beliebige $w_1, \ldots, w_n \in V$:

$$\omega(w_1, \ldots, w_n) = \det(\varphi^{-1}(w_1), \ldots, \varphi^{-1}(w_n)).$$

Ist $\underline{w} = (w_1, \ldots, w_n)$ eine Basis von V und $T = M^{\underline{v}}_{\underline{w}}(\mathrm{id}_V)$ die Transformationsmatrix, so gilt

$$\omega(w_1, \ldots, w_n) = \det T.$$

Für die Fundamentalmatrix G von γ bzgl. $\underline{w}$ gilt $G = T^tT$, also

$$g := \det(G) = \det(T^tT) = \det(T)^2 > 0.$$

Wir erhalten $\omega(w_1, \ldots, w_n) = \pm\sqrt{g}$. Das Ergebnis folgt nun aus

$$\det(T) \quad \begin{cases} > 0 & \text{wenn } \underline{w} \text{ orientiert,} \\ < 0 & \text{wenn } \underline{w} \text{ nicht orientiert.} \end{cases}$$

Ist schließlich $\underline{w}$ eine orientierte ONB, so gilt $T \in SO(n)$ und $\det(T) = 1$. □

Definition 5.57. Es heißt g die **Gramsche Determinante** von $(w_1, \ldots, w_n)$.

— Ab hier nicht klausurrelevant —

5.8 Affine Isometrien

Wir beweisen nun noch 5.47, welcher lautete

Satz 5.47 *Sei $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ eine (nicht notwendig lineare) Abbildung. Ist φ abstandstreu (d.h. $\|\varphi(x) - \varphi(y)\| = \|x - y\|$ für alle x, y), so gibt es ein $A \in O(n)$ und ein $b \in \mathbb{R}^n$ so dass*

$$\varphi(x) = Ax + b$$

für alle $x \in \mathbb{R}^n$ gilt.

Wir beginnen mit einem Lemma.

Lemma 5.58. *Sei (V, γ) ein euklidischer Raum und $v_1, \ldots, v_k$ paarweise orthogonal (d.h. $\gamma(v_i, v_j) = 0$ für $i \neq j$) und alle von 0 verschieden. Dann ist $(v_1, \ldots, v_k)$ linear unabhängig.*

Beweis. Ist $\lambda_1 v_1 + \cdots + \lambda_k v_k = 0$, so folgt für $i = 1, \ldots, k$

$$0 = \gamma(\lambda_1 v_1 + \cdots + \lambda_k v_k, v_i) = \lambda_i \gamma(v_i, v_i)$$

also $\lambda_i = 0$ für $i = 1, \ldots, k$. □

Beweis von 5.47. Setze $b = \varphi(0)$ und $\psi = \varphi - b$, also $\psi(0) = 0$. Es ist zu zeigen, dass ψ eine orthogonale lineare Abbildung ist, d.h. $\psi(x) = Ax$ für ein $A \in O(n)$.

1. Schritt. $\langle \psi(x), \psi(y) \rangle = \langle x, y \rangle$ für alle $x, y \in \mathbb{R}^n$.
Grund:

$$\begin{aligned} -2\langle\psi(x),\psi(y)\rangle &= \|\psi(x)-\psi(y)\|^2 - \|\psi(x)\|^2 - \|\psi(y)\|^2 \\ &= d(\psi(x),\psi(y))^2 - d(\psi(x),0)^2 - d(\psi(y),0)^2 \\ &= d(x,y)^2 - d(x,0)^2 - d(y,0)^2 \\ &= \|x-y\|^2 - \|x\|^2 - \|y\|^2 \\ &= -2\langle x,y\rangle. \end{aligned}$$

2. Schritt. $(\psi(e_1),\dots,\psi(e_n))$ ist eine ONB des $\mathbb{R}^n$.

Grund: Nach 1. gilt $\langle\psi(e_i),\psi(e_j)\rangle = \langle e_i,e_j\rangle = \delta_{ij}$. Es bleibt zu zeigen, dass das System $(\psi(e_1),\dots,\psi(e_n))$ linear unabhängig ist. Das folgt aus 5.58.

3. Schritt. ψ ist linear. Z.z:

$$\psi(ax+by) = a\psi(x) + b\psi(y)$$

für alle $a,b\in\mathbb{R}$, $x,y\in\mathbb{R}^n$. Es genügt zu zeigen:

$$\langle\psi(ax+by) - a\psi(x) - b\psi(y), z\rangle = 0$$

für alle $z\in\mathbb{R}^n$. Wegen Schritt 2 genügt es, dies für $z=\psi(e_1),\dots,\psi(e_n)$ nachzuweisen. Nun gilt

$\langle\psi(ax+by) - a\psi(x) - b\psi(y), \psi(e_i)\rangle$

$= \langle\psi(ax+by),\psi(e_i)\rangle - a\langle\psi(x),\psi(e_i)\rangle - b\langle\psi(y),\psi(e_i)\rangle$

$\overset{\text{Schritt 1}}{=} \langle ax+by,e_i\rangle - a\langle x,e_i\rangle - b\langle y,e_i\rangle = 0.$

4. Schritt. Nach Schritt 3 gilt $\psi(x)=Ax$ für eine Matrix A und nach Schritt 2 gilt $A\in O(n)$. □

Beispiele für kleines n: $n=1$. $O(1)=\{\pm1\}$, $SO(1)=\{1\}$

$n=2$. Sei $A\in O(2)$ und $Ae_1=\binom{a}{b}$. Wegen

$$\|Ae_1\| = \sqrt{\langle Ae_1,Ae_1\rangle} = \sqrt{\langle e_1,e_1\rangle} = 1$$

gilt $a^2+b^2=1$. Nun gilt $Ae_2\perp Ae_1$, also $Ae_2=\lambda\binom{-b}{a}$ mit $\lambda\in\mathbb{R}$; wegen $\|Ae_2\|=1$ folgt $\lambda=\pm1$. Also gilt $A=\left(\begin{smallmatrix} a & -\lambda b\\ b & \lambda a\end{smallmatrix}\right)$, und $|A|=\lambda\in\{\pm1\}$.

Gilt $A\in SO(2)$, d.h. $\lambda=1$, so hat A die Form $A=\left(\begin{smallmatrix} a & -b\\ b & a\end{smallmatrix}\right)$ mit $a^2+b^2=1$. Dann gibt es ein wohlbestimmtes $\varphi\in[0,2\pi)$ mit $a=\cos\varphi$, $b=\sin\varphi$, d.h. A entspricht der Drehung (um 0) um den Winkel φ.

Ist nun $A \in O(2) - SO(2)$, d.h. $\lambda = -1$, so ist A von der Form $A = \left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$.

Es gilt

$$\chi_A(t) = (t-a)(t+a) - b^2 = t^2 - 1 = (t+1)(t-1).$$

Also hat A die zwei verschiedenen reellen Eigenwerte ± 1 und es existieren Vektoren $v_1, v_2 \in \mathbb{R}^2$ mit $Av_1 = v_1$, $Av_2 = -v_2$. Außerdem gilt $\langle v_1, v_2\rangle = \langle Av_1, Av_2\rangle = \langle v_1, -v_2\rangle = -\langle v_1, v_2\rangle$, und daher $\langle v_1, v_2\rangle = 0$, d.h. $v_1 \perp v_2$.

Geometrisch: A ist die Spiegelung an der Geraden $\mathbb{R}v_1$.

Korollar 5.59. *Die Hintereinanderausführung zweier Spiegelungen (an Geraden durch 0) im $\mathbb{R}^2$ ist eine Drehung (um 0).*

Beweis. Eine Spiegelung wird bzgl. einer geeigneten ONB des $\mathbb{R}^2$ durch die Matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ gegeben. Die Transformationsmatrix zur Einheitsmatrix liegt in $O(2)$, d.h. die Spiegelung wird bzgl. (e_1, e_2) durch eine Matrix der Form $A = T^t \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) T$ mit $T \in O(2)$ gegeben. Es gilt $|A| = |T^t| \cdot (-1) \cdot |T| = -1$. Daher gilt $A \in O(2)$, $|A| = -1$. Definiert die Matrix B eine weitere Spiegelung, so gilt $B \in O(2)$, $|B| = -1$, und daher ist $A \cdot B \in SO(2)$ eine Drehung. □

Analog erhält man:

Korollar 5.60. *Die Hintereinanderausführung einer Drehung und einer Spiegelung ist eine Spiegelung.*