Lineare Algebra WS2017/18 + SS2018

Dozent: Prof. Dr. Arno Fehm

21. November 2018

Inhaltsverzeichnis

Vorwort

Schön, dass du unser Skript für die Vorlesung *Lineare Algebra und analytische Geometrie 1 + 2* bei Prof. Dr. Arno Fehm im WS2017/18 und SS2018 gefunden hast! [1]

Wir verwalten dieses Skript mittels Github [2], d.h. du findest den gesamten LaTeX-Quelltext auf https://github.com/henrydatei/TUD_MATH_BA. Unser Ziel ist, für alle Pflichtveranstaltungen von *Mathematik-Bachelor* ein gut lesbares Skript anzubieten. Für die Programme, die in den Übungen zur Vorlesung *Programmieren für Mathematiker* geschrieben werden sollen, habe ich ein eigenes Repository eingerichtet; es findet sich bei https://github.com/henrydatei/TU_PROG.

Es lohnt sich auf jeden Fall während des Studiums die Skriptsprache LaTeX zu lernen, denn Dokumente, die viele mathematische oder physikalische Formeln enthalten, lassen sich sehr gut mittels LaTeX darstellen, in Word oder anderen Office-Programmen sieht so etwas dann eher dürftig aus.

LaTeX zu lernen ist gar nicht so schwierig, ich habe dafür am Anfang des ersten Semesters wenige Wochen benötigt, dann kannte ich die wichtigsten Befehle und konnte den Vorgänger dieses Skriptes schreiben (`1. Semester/LAAG`, Vorsicht: hässlich, aber der Quelltext ist relativ gut verständlich).

Es sei an dieser Stelle darauf hingewiesen (wie in jedem anderem Skript auch ☺), dass dieses Skript nicht den Besuch der Vorlesungen ersetzen kann. Es könnte sein, dass Prof. Fehm seine Vorlesung immer mal wieder an die Studenten anpasst; wahrscheinlich immer dann, wenn die Prüfungsergebnisse zu schlecht waren. Nichtsdestotrotz veröffentlicht Prof. Fehm sein Skript auf seiner Homepage http://www.math.tu-dresden.de/~afehm/lehre.html. Allerdings ist dieses Skript recht hässlich, besonders was die Übersichtlichkeit angeht.

Wir möchten deswegen ein Skript bereitstellen, dass zum einen übersichtlich ist, zum anderen *alle* Inhalt aus der Vorlesung enthält, das sind insbesondere Diagramme, die sich nicht im offiziellen Skript befinden, aber das Verständnis des Inhalts deutlich erleichtern. Ich denke, dass uns dies erfolgreich gelungen ist.

Trotz intensivem Korrekturlesen können sich immer noch Fehler in diesem Skript befinden. Es wäre deswegen ganz toll von dir, wenn du auf unserer Github-Seite https://github.com/henrydatei/TUD_MATH_BA ein neues Issue erstellst und damit auch anderen hilfst, dass dieses Skript immer besser wird.

Und jetzt viel Spaß bei *Lineare Algebra und analytische Geometrie*!

Henry, Pascal und Daniel

[1] Obwohl man sagen kann, dass es in dieser Vorlesung nur um Lineare Algebra ging, der Teil mit der analytischen Geometrie wurde vernachlässigt. Liegt wahrscheinlich auch daran, dass es demnächst eine Reform der Studienordnung gibt, in der aus der Vorlesung *Lineare Algebra und analytische Geometrie* die Vorlesung *Einführung in die Lineare Algebra* wird.

[2] Github ist eine Seite, mit der man Quelltext online verwalten kann. Dies ist dahingehend ganz nützlich, dass man die Quelltext-Dateien relativ einfach miteinander synchronisieren kann, wenn man mit mehren Leuten an einem Projekt arbeitet.

Kapitel I

Grundbegriffe der Linearen Algebra

1. Logik und Mengen

Wir werden die Grundlagen der Logik und der Mengenlehre kurz ansprechen.
Überblick (Aussagenlogik)
Jede mathematisch sinnvolle Aussage ist entweder wahr oder falsch, aber nie beides!

- "$1+1=2$" $\rightarrow$ wahr
- "$1+1=3$" $\rightarrow$ falsch
- "Es gibt unendlich viele Primzahlen" $\rightarrow$ wahr

Man ordnet jeder mathematischen Aussage A einen Wahrheitswert "wahr" oder "falsch" zu. Aussagen lassen sich mit logischen Verknüpfungen zu neuen Aussagen zusammensetzen.

- $\vee \rightarrow$ oder
- $\wedge \rightarrow$ und
- $\neg \rightarrow$ nicht
- $\Rightarrow \rightarrow$ impliziert
- $\iff \rightarrow$ äquivalent

Sind also A und B zwei Aussagen, so ist auch $A \vee B$, $A \wedge B$, $\neg A$, $A \Rightarrow B$ und $A \iff B$ Aussagen. Der Wahrheitswert einer zusammengesetzten Aussage ist eindeutig bestimmt durch die Wahrheitswerte ihrer Einzelaussagen.

- $\neg(1+1=3) \rightarrow$ wahr
- "2 ist ungerade" $\Rightarrow$ "3 ist gerade" $\rightarrow$ wahr
- "2 ist gerade" $\Rightarrow$ "Es gibt unendlich viele Primzahlen" $\rightarrow$ wahr

A	B	$A \vee B$	$A \wedge B$	$\neg A$	$A \Rightarrow B$	$A \iff B$
w	w	w	w	f	w	w
w	f	w	f	f	f	f
f	w	w	f	w	w	f
f	f	f	f	w	w	w

Überblick (Prädikatenlogik)
Wir werden die Quantoren

- $\forall$ (Allquantor, "für alle") und
- $\exists$ (Existenzquantor, "es gibt") verwenden.

Ist $P(x)$ eine Aussage, deren Wahrheitswert von einem unbestimmten x abhängt, so ist
$\forall x : P(x)$ genau dann wahr, wenn $P(x)$ für alle x wahr ist,
$\exists x : P(x)$ genau dann wahr, wenn $P(x)$ für mindestens ein x wahr ist.

Insbesondere ist $\neg\forall x : P(x)$ genau dann wahr, wenn $\exists x : \neg P(x)$ wahr ist.
Analog ist $\neg\exists x : P(x)$ genau dann wahr, wenn $\forall x : \neg P(x)$ wahr ist.

Überblick (Beweise)
Unter einem Beweis verstehen wir die lückenlose Herleitung einer mathematischen Aussage aus einer Menge von Axiomen, Voraussetzungen und schon früher bewiesenen Aussagen.
Einige Beweismethoden:

- **Widerspruchsbeweis**
  Man nimmt an, dass eine zu beweisende Aussage A falsch sei und leitet daraus ab, dass eine andere Aussage sowohl falsch als auch wahr ist. Formal nutzt man die Gültigkeit der Aussage $\neg A \Rightarrow (B \wedge \neg B) \Rightarrow A$.
- **Kontraposition**
  Ist eine Aussage $A \Rightarrow B$ zu beweisen, kann man stattdessen die Implikation $\neg B \Rightarrow \neg A$ beweisen.
- **vollständige Induktion**
  Will man eine Aussage $P(n)$ für alle natürlichen Zahlen zeigen, so genügt es, zu zeigen, dass $P(1)$ gilt und dass unter der Induktionsbehauptung $P(n)$ stets auch $P(n+1)$ gilt (Induktionschritt). Dann gilt $P(n)$ für alle n.
  Es gilt also das Induktionsschema: $P(1) \wedge \forall n : (P(n) \Rightarrow P(n+1)) \Rightarrow \forall n : P(n)$.

Überblick (Mengenlehre)
Jede Menge ist eine Zusammenfassung bestimmter wohlunterscheidbarer Objekte zu einem Ganzen. Eine Menge enthält also solche Objekte, die Elemente der Menge. Die Menge ist durch ihre Elemente vollständig bestimmt. Diese Objekte können für uns verschiedene mathematische Objekte, wie Zahlen, Funktionen oder andere Mengen sein. Man schreibt $x \in M$ bzw. $x \notin M$, wenn x ein bzw. kein Element der Menge ist.

Ist $P(x)$ ein Prädikat, so bezeichnet man eine Menge mit $X := \{x \mid P(x)\}$. Hierbei muss man vorsichtig sein, denn nicht immer lassen sich alle x für die $P(x)$ gilt, widerspruchsfrei zu einer Menge zusammenfassen.

■ **Beispiel 1.5 (endliche Mengen)**
Eine Menge heißt endlich, wenn sie nur endlich viele Elemente enthält. Endliche Mengen notiert man oft in aufzählender Form: $M = \{1; 2; 3; 4; 5; 6\}$. Hierbei ist die Reihenfolge der Elemente nicht relevant, auch nicht die Häufigkeit eines Elements.
Sind die Elemente paarweise verschieden, dann ist die Anzahl der Elemente die Mächtigkeit (oder Kardinalität) der Menge, die wir mit $|M|$ bezeichnen.

■ **Beispiel 1.6 (unendliche Mengen)**

- Menge der natürlichen Zahlen: $\mathbb{N} := \{1, 2, 3, 4, ...\}$
- Menge der natürlichen Zahlen mit der 0: $\mathbb{N}_0 := \{0, 1, 2, 3, 4, ...\}$
- Menge der ganzen Zahlen: $\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$
- Menge der rationalen Zahlen: $\mathbb{Q} := \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$
- Menge der reellen Zahlen: $\mathbb{R} := \{x \mid x \text{ ist eine reelle Zahl}\}$

Ist M eine Menge, so gilt $|M| = \infty$

■ **Beispiel 1.7 (leere Menge)**
Es gibt genau eine Menge, die keine Elemente hat, die leere Menge $\emptyset := \{\}$.

Definition 1.8 (Teilmenge)
Sind X und Y zwei Mengen, so heißt X eine Teilmenge von Y, wenn jedes Element von X auch Element von Y ist, dass heißt wenn für alle x $(x \in X \Rightarrow x \in Y)$ gilt.

Da eine Menge durch ihre Elemente bestimmt ist, gilt $X = Y \Rightarrow (X \subset Y) \wedge (Y \subset X)$. Will man Mengengleichheit beweisen, so genügt es, die beiden Inklusionen $X \subset Y$ und $Y \subset X$ zu beweisen.

Ist X eine Menge und $P(x)$ ein Prädikat, so bezeichnet man mit $Y := \{x \in X \mid P(x)\}$ die Teilmenge von X, die das Prädikat $P(x)$ erfüllen.

Definition 1.9 (Mengenoperationen)
Seien X und Y Mengen. Man definiert daraus weitere Mengen wie folgt (Mengenoperationen):

- $X \cup Y := \{x \mid x \in X \vee x \in Y\}$
- $X \cap Y := \{x \mid x \in X \wedge x \in Y\}$
- $X \backslash Y := \{x \in X \mid x \notin Y\}$
- $X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}$
- $\mathcal{P}(X) := \{Y \mid Y \subset X\}$

Neben den offensichtlichen Mengengesetzen, wie dem Kommutativgesetz, gibt es auch weniger offensichtliche Gesetze, wie die Gesetze von DE MORGAN: Für $X_1, X_2 \subset X$ gilt:

- $X \backslash (X_1 \cup X_2) = (X \backslash X_1) \cap (X \backslash X_2)$
- $X \backslash (X_1 \cap X_2) = (X \backslash X_1) \cup (X \backslash X_2)$

Sind X und Y endliche Mengen, so gilt:

- $|X \times Y| = |X| \cdot |Y|$
- $|\mathcal{P}(X)| = 2^{|X|}$

2. Abbildungen

Überblick (Abbildungen)
Eine Abbildung f von eine Menge X in einer Menge Y ist eine Vorschrift, die jedem $x \in X$ auf eindeutige Weise genau ein Element $f(x) \in Y$ zuordnet. Man schreibt dies als

$$f : \begin{cases} X \to Y \\ x \mapsto y \end{cases}$$

oder $f : X \to Y, x \mapsto y$ oder noch einfacher $f : X \to Y$. Dabei heißt X die Definitionsmenge und Y die Zielmenge von f. Zwei Abbildungen heißen gleich , wenn ihre Definitionsmengen und Zielmengen gleich sind und sie jedem $x \in X$ das selbe Element $y \in Y$ zuordnen. Die Abbildungen von X nach Y bilden wieder eine Menge, welche wir mit $\mathrm{Abb}(X, Y)$ bezeichnen.

■ **Beispiel 2.2**

- Abbildungen mit Zielmenge $\mathbb{R}$ nennt man Funktion: $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
- Abbildungen mit Zielmenge $\subset$ Definitionsmenge: $f : \mathbb{R} \to \mathbb{R}_{\leq 0}, x \mapsto x^2$
  $\to$ Diese Abbildungen sind verschieden, da sie nicht die selbe Zielmenge haben.
- $f : \{0, 1\} \to \mathbb{R}, x \mapsto x^2$
- $f : \{0, 1\} \to \mathbb{R}, x \mapsto x$
  $\to$ Diese Funktionen sind gleich. Sie haben die gleichen Definitions- und Zielmengen und sie ordnen jedem Element der Definitionsmenge das gleiche Element der Zielmenge zu.

■ **Beispiel 2.3**

- auf jeder Menge X gibt es die identische Abbildung (Identität)
  $\mathrm{id} : X \to X, x \mapsto x$
- allgemein kann man zu jeder Teilmenge $A \subset X$ die Inklusionsabbildung zuordnen $\iota_A : A \to X, x \mapsto x$
- zu je zwei Mengen X und Y und einem festen $y_0 \in Y$ gibt es die konstante Abbildung $c_{y_0} : X \to Y x \mapsto y_0$
- zu jder Menge X und Teilmenge $A \subset X$ definiert man die charakteristische Funktion
  $\chi_A : X \to \mathbb{R}, \begin{cases} x \mapsto 1 & (x \in A) \\ x \mapsto 0 & (x \notin A) \end{cases}$
- zu jeder Menge X gibt es die Abbildung
  $f : X \times X \to \mathbb{R}, (x, y) \mapsto \delta_{x,y} \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$

■ **Beispiel 2.4 (Eigenschaften von Funktionen)**

- injektiv : Zuordnung ist eindeutig: $F(m_1) = F(m_2) \Rightarrow m_1 = m_2$
  Bsp: x^2 ist nicht injektiv, da $F(-2) = F(2) = 4$

- surjektiv : $F(M) = N$ $(\forall n \in N\ \exists m \in M \mid F(m) = n)$
  Bsp: $\sin(x)$ ist nicht surjektiv, da es kein x für $y = 27$ gibt
- bijektiv : injektiv und surjektiv

■ **Beispiel 2.5**

- Die identische Abbildung $\mathrm{id}_X : X \to X$ ist stets bijektiv.
- Für jede Teilmenge $A \subseteq X$ ist die Inklusionsabbildung $\iota_A : A \to X$ injektiv, aber im Allgemeinen nicht surjektiv.
- Die Funktion $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ mit $x \mapsto x^2$ ist surjektiv, aber nicht injektiv.
- Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $x \mapsto x^3$ ist bijektiv.

Definition 2.6 (Einschränkung)
Sei $f : x \mapsto y$ eine Abbildung. Für $A \subset X$ definiert man die Einschränkung /Restrikton von f auf A als die Abbildung

$$f|_A : \begin{cases} A \to Y \\ a \mapsto f(a) \end{cases}$$

Das Bild von A unter f ist $f(A) := \{f(a) : a \in A\}$.
Das Urbild einer Menge $B \subset Y$ unter f ist $f^{-1} := \{x \in X : f(x) \in B\}$.
Man nennt $\mathrm{Im}(f) := f(X)$ das Bild von f.

▶ **Bemerkung 2.7**
Man ordnet der Abbildung $f : X \to Y$ auch die Abbildungen $\mathcal{P}(X) \to \mathcal{P}(Y)$ und $\mathcal{P}(Y) \to \mathcal{P}(X)$ auf den Potenzmengen zu. Man benutzt hier das gleiche Symbol $f(\dots)$ sowohl für die Abbildung $f : X \to Y$ als auch für $f : P(X) \to P(Y)$, was unvorsichtig ist, aber keine Probleme bereiten sollte.
In anderen Vorlesungen wird für $y \in Y$ auch $f^{-1}(y)$ statt $f^{-1}(\{y\})$ geschrieben.

▶ **Bemerkung 2.8**
Genau dann ist $f : X \to Y$ surjektiv, wenn $\mathrm{Im}(f) = Y$

$$\text{Genau dann ist } f : X \to Y \begin{cases} \text{injektiv} \\ \text{surjektiv} \\ \text{bijektiv} \end{cases} \text{, wenn } |f^{-1}(\{y\})| = \begin{cases} \leq 1 \\ \geq 1 \\ = 1 \end{cases} \qquad \forall y \in Y$$

Definition 2.9 (Komposition)
Sind $f : X \to Y$ und $g : Y \to Z$ Abbildungen, so ist die Komposition $g \circ f$ die Abbildung

$$g \circ f := \begin{cases} X \to Z \\ x \mapsto f(g(x)) \end{cases}$$

Man kann die Komposition auffassen als eine Abbildung $\circ : \mathrm{Abb}(Y, Z) \times \mathrm{Abb}(X, Y) \to \mathrm{Abb}(X, Z)$.

Satz 2.10
Die Abbildung von Kompositionen ist assoziativ, d.h. es gilt:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

.

Beweis. Sowohl $h \circ (g \circ f)$ als auch $(h \circ g) \circ f$ haben die Definitionsmenge X und die Zielmenge W und für jedes $x \in X$ ist $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. □

Definition 2.11 (Umkehrabbildung)
Ist $f : X \to Y$ bijektiv, so gibt es zu jedem $y \in Y$ genau ein $x_y \in X$ mit $f(x_y) = y$ (Bemerkung 2.7), durch

$$f^{-1} : \begin{cases} Y \to X \\ y \mapsto x_y \end{cases}$$

wird also eine Abbildung definiert, die Umkehrabbildung zu f.

Satz 2.12
Ist die Abbildung $f : X \to Y$ bijektiv, so gelten

$$f^{-1} \circ f = id_x$$
$$f \circ f^{-1} = id_y$$

Beweis. Es ist $f^{-1} \in \mathrm{Abb}(X, X)$ und $f \circ f^{-1} \in \mathrm{Abb}(Y, Y)$. Für $y \in Y$ ist $(f \circ f^{-1})(x) = f(f^{-1}(y)) = y = \mathrm{id}_Y$. Für $x \in X$ ist deshalb $f((f^{-1} \circ f)(x)) = (f \circ (f^{-1} \circ f))(x) \overset{2.10}{=} ((f \circ f^{-1}) \circ f)(x) = (\mathrm{id}_Y \circ f)(x) = f(x)$. Da f injektiv, folgt $f^{-1} \circ f = \mathrm{id}_X$. □

▶ **Bemerkung 2.13**
Achtung, wir verwenden hier das selbe Symbol f^{-1} für zwei verschiedene Dinge: Die Abbildung $f^{-1} : \mathcal{P}(X) \to \mathcal{P}(Y)$ aus Definition 2.6 existiert für jede Abbildung $f : X \to Y$, aber die Umkehrabbildung $f^{-1} : Y \to X$ aus Satz 2.10 existiert nur für bijektive Abbildungen $f : X \to Y$.

Definition 2.14 (Familie)
Seien I und X Mengen. Eine Abbildung $x : I \to X, i \mapsto x_i$ nennt man Familie von Elementen von X mit einer Indexmenge I (oder I-Tupel von Elementen von X) und schreibt diese auch als $(x_i)_{i \in I}$. Im Fall $I = \{1, 2, ..., n\}$ identifiziert man die I-Tupel auch mit den n-Tupeln aus Definition 1.8. Ist $(x_i)_{i \in I}$ eine Familie von Teilmengen einer Menge X, so ist

- $\bigcup X_i = \{x \in X \mid \exists i \in I(x \in X)\}$
- $\bigcap X_i = \{x \in X \mid \forall i \in I(x \in X)\}$
- $\prod X_i = \{f \in \mathrm{Abb}(I, X) \mid \forall i \in I(f(i) \in X_i)\}$

Die Elemente von $\prod X_i$ schreibt man in der Regel als Familien $(x_i)_{i \in I}$.

■ **Beispiel 2.15**

Eine Folge ist eine Familie $(x_i)_{i\in I}$ mit der Indexmenge $\mathbb{N}_0$.

Definition 2.16 (Graph)

Der Graph einer Abbildung $f : X \to Y$ ist die Menge

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

▶ **Bemerkung 2.17 (Formal korrekte Definition einer Abbildung)**

Eine Abbildung f ist ein Tripel (X, Y, Γ), wobei $\Gamma \subset X \times Y \quad \forall x \in X$ genau ein Paar (x, y) mit $y \in Y$ enthält. Die Abbildungsvorschrift schickt dann $x \in X$ auf das eindeutig bestimmte $y \in Y$ mit $(x, y) \in \Gamma$. Es ist dann $\Gamma = \Gamma_f$.

▶ **Bemerkung 2.18**

In anderen Vorlesungen wird die Zielmenge nicht immer als Teil der Definition einer Abbildung aufgefasst, d.h. man betrachtet zwei Abbildungen $f : X \to Y$ und $g : X \to Z$ mit gleicher Definitionsmenge dann als gleich, wenn $f(x) = g(x)$ für alle $x \in X$. Dies ist gleichbedeutend mit $\Gamma_f = \Gamma_g$. So würde man dann zum Beispiel f_1 und f_2 aus Beispiel 2.2 als gleich auffassen.

3. Gruppen

Definition 3.1 ((Halb-)Gruppe)
Sei G eine Menge. Eine (innere, zweistellige) Verknüpfung auf G ist eine Abbildung $* : G \times G \to G, (x, y) \mapsto x * y$. Das Paar $(G, *)$ ist eine Halbgruppe , wenn das folgende Axiom erfüllt ist:

- (G1) Für $x, y, z \in G$ ist $(x * y) * z = x * (y * z)$.

Eine Halbgruppe $(G, *)$ ist ein Monoid , wenn zusätzlich das folgende Axiom gilt:

- (G2) Es gibt ein Element $e \in G$, welches für alle $x \in G$ die Gleichung $x * e = e * x = x$ erfüllt. Dieses Element heißt dann neutrales Element der Verknüpfung $*$.

■ **Beispiel 3.2**

- Für jede Menge X ist $(\mathrm{Abb}(X, Y), \circ)$ eine Halbgruppe (Satz 2.10) mit dem neutralen Element id_x, also ein Monoid.
- $\mathbb{N}$ bildet mit der Addition eine Halbgruppe $(\mathbb{N}, +)$, aber kein Monoid, da die 0 nicht in Fehm's Definition der natürlichen Zahlen gehörte
- $\mathbb{N}_0$ bildet mit der Addition ein Monoid $(\mathbb{N}_0, +)$
- $\mathbb{N}$ bildet mit der Multiplikation ein Monoid $(\mathbb{N}, \cdot)$
- $\mathbb{Z}$ bildet mit der Multiplikation ein Monoid $(\mathbb{Z}, \cdot)$

Satz 3.3 (Eindeutigkeit des neutralen Elements)
Ein Monoid $(G, *)$ hat genau ein neutrales Element.

Beweis. Nach Definition besitzt $(G, *)$ mindestens ein neutrales Element. Seien $e_1, e_2 \in G$ neutrale Elemente. Dann ist $e_1 = e_1 * e_2 = e_2$. Damit besitzt $(G, *)$ höchstens ein neutrales Element, also genau ein neutrales Element. □

Definition 3.4 ((abelsche) Gruppe)
Eine Gruppe ist ein Monoid $(G, *)$ mit dem neutralen Element e, in dem zusätzlich das folgende Axiom gilt:

- (G3) Für jedes $x \in G$ gibt es ein $x' \in G$ mit $x' * x = x * x' = e$.

Gilt weiterhin

- (G4) Für alle $x, y \in G$ gilt $x * y = y * x$, so heißt diese Gruppe abelsch .

Ein x' heißt inverses Element zu x.

■ **Beispiel 3.5**

- $\mathbb{N}_0$ bildet mit der Addition keine Gruppe $(\mathbb{N}_0, +)$
- $\mathbb{Z}$ bildet mit der Addition eine abelsche Gruppe $(\mathbb{Z}, +)$
- Auch $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen
- $(\mathbb{Q}, \cdot)$ ist keine Gruppe, aber $(\mathbb{Q}\backslash\{0\}, \cdot)$ schon

Satz 3.6 (Eindeutigkeit des Inversen)
Ist $(G, *)$ eine Gruppe, so hat jedes $x \in G$ genau ein inverses Element.

Beweis. Nach Definition hat jedes $x \in G$ mindestens ein Inverses. Seien $x', x'' \in G$ inverse Elemente zu x. Dann ist $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. Es gibt also genau ein Inverses zu x. □

■ **Beispiel 3.7**

- Eine triviale Gruppe besteht nur aus ihrem neutralen Element. Tatsächlich ist $G = \{e\}$ mit $e * e = e$ eine Gruppe.
- Sei X eine Menge. Die Menge $\mathrm{Sym}(X) := \{f \in \mathrm{Abb}(X, X) \mid f \text{ ist bijektiv}\}$ der Permutationen von X bildet mit der Komposition eine Gruppe $(\mathrm{Sym}(X), \circ)$, die symmetrische Gruppe auf X. Für $n \in \mathbb{N}$ schreibt man $S_n := \mathrm{Sym}(\{1, 2, ..., n\})$. Für $n \geq 3$ ist S_n nicht abelsch.

▶ **Bemerkung 3.8**
Häufig benutzte Notationen für die Gruppenverknüpfung $\cdot$:

- In der multiplikativen Notation schreibt man $\cdot$ statt $*$ (oft auch xy statt $x \cdot y$), bezeichnet das neutrale Element mit 1 oder 1_G und das Inverse zu x mit x^{-1}.
- In der additiven Notation schreibt man $+$ für $*$, bezeichnet das neutrale Element mit 0 oder 0_G und das Inverse zu x mit $-x$. Die additive Notation wird nur verwendet, wenn die Gruppe abelsch ist.

In abelschen Gruppen notiert man Ausdrücke auch mit dem Summen- und Produktzeichen.

Satz 3.9
Sei $(G, \cdot)$ eine Gruppe. Für $x, y \in G$ gelten

$$(x^{-1})^{-1} = x$$
$$(xy)^{-1} = x^{-1} \cdot y^{-1}$$

Beweis. Nach Definition erfüllt $z = x$ die Identitäten $x^{-1}z = zx^{-1} = 1$ und somit ist $(x^{-1})^{-1} = z = x$. Ebenso ist $(y^{-1}x^{-1}) \cdot (xy) = y^{-1}(x^{-1}x)y = 1$ und $(xy) \cdot (x^{-1}y^{-1}) = x(yy^{-1})x^{-1} = 1$, also $y^{-1}x^{-1} = (xy)^{-1}$. □

Satz 3.10
Sei $(G, \cdot)$ eine Gruppe. Für $a, b \in G$ haben die Gleichungen $ax = b$ und $ya = b$ eindeutige Lösungen in G, nämlich $x = a^{-1} \cdot b$ und $y = b \cdot a^{-1}$. Insbesondere gelten die folgenden Kürzungsregeln: $ax = ay \Rightarrow x = y$ und $xa = ya \Rightarrow x = y$.

Beweis. Es ist $a \cdot a^{-1} \cdot b = 1b = b$, also ist $x = a^{-1} \cdot b$ eine Lösung. Ist umgekehrt $ax = b$ mit $x \in G$, so ist $a^{-1} \cdot b = a^{-1} \cdot ax = 1x = x$ die Lösung und somit eindeutig. Für die zweite Gleichung argumentiert man analog. Den "Insbesondere"-Fall erhält man durch Einsetzen von $b = ay$ bzw. $b = xa$. □

▶ **Bemerkung 3.11**

Wenn aus dem Kontext klar ist, welche Verknüpfung gemeint ist, schreibt man auch einfach G anstatt $(G, \cdot)$ bzw. $(G, +)$. Eine Gruppe G heißt endlich, wenn die Menge G endlich ist. Die Mächtigkeit $|G|$ von G nennt man dann die Ordnung von G. Eine endliche Gruppe kann durch ihre Verknüpfungstafel vollständig beschrieben werden.

■ **Beispiel 3.12**

- die triviale Gruppe $G = \{e\}$

$\cdot$	e
e	e

- die Gruppe $\mu_2 = \{1, -1\}$ der Ordnung 2

$\cdot$	1	-1
1	1	-1
-1	-1	1

- die Gruppe $S_2 = \mathrm{Sym}(\{1, 2\}) = \{\mathrm{id}_{\{1,2\}}, f\}$, wobei $f(1) = 2$ und $f(2) = 1$

$\circ$	$\mathrm{id}_{\{1,2\}}$	f
$\mathrm{id}_{\{1,2\}}$	$\mathrm{id}_{\{1,2\}}$	f
f	f	$\mathrm{id}_{\{1,2\}}$

Definition 3.13 (Untergruppe)

Eine Untergruppe einer Gruppe $(G, \cdot)$ ist eine nichtleere Teilmenge $H \subset G$, für die gilt:

- (UG1) Für alle $x, y \in H$ ist $x \cdot y \in H$ (Abgeschlossenheit unter Multiplikation).
- (UG2) Für alle $x \in H$ ist $x^{-1} \in H$ (Abgeschlossenheit unter Inversen).

Satz 3.14

Sei $(G, \cdot)$ eine Gruppe und $\emptyset \neq H \subset G$. Genau dann ist H eine Untergruppe von G, wenn sich die Verknüpfung $\cdot : G \times G \to G$ zu einer Abbildung $\cdot_H : H \times H \to H$ einschränken lässt (d.h. $\cdot|_{H \times H} = \iota_H \circ \cdot_H$, wobei $\iota_H \cdot \cdot_H \to G$ die Inklusionsabbildung ist) und $(H, \cdot_H)$ eine Gruppe ist.

Beweis. $\Rightarrow$: Sei H eine Untergruppe von G. Nach (UG1) ist $\mathrm{Im}(\cdot|_{H \times H}) \subset H$ und somit lässt sich $\cdot$ zu einer Abbildung $\cdot_H : H \times H \; toH$ einschränken. Wir betrachten jetzt H mit dieser Verknüpfung. Da G (G1) erfüllt, erfüllt auch H (G1). Da $H \neq \emptyset$ existiert ein $x \in H$. Nach (UG1) und (UG2) ist $x \cdot x^{-1} = e \in H$. Da $e_G \cdot y = y \cdot e_G = y$ für alle $y \in G$, insbesondere auch für alle $y \in H$ (G2). Wegen (UG2) erfüllt H auch das Axiom (G3). H ist somit eine Gruppe.
$\Leftarrow$: Sei nun umgekehrt $(H, \cdot_H)$ eine Gruppe. Für $x, y \in H$ ist dann $xy = x \cdot_H y \in H$, also erfüllt H (UG1). Aus $e_H \cdot e_H = e_H = e_H \cdot e_G$ folgt $e_H = e_G$. Ist also x' das Inverse zu x aus der Gruppe H, so ist $x'x = xx' = e_G = e_H$, also $x^{-1} = x' \in H$ und somit erfüllt H auch (UG2). Wir haben gezeigt, dass H eine Untergruppe von G ist. □

▶ **Bemerkung 3.15**
Wir nennen nicht nur die Menge H eine Untergruppe von G, sondern auch die Gruppe $(H, \cdot_H)$. Wir schreiben $H \subseteq G$.

■ **Beispiel 3.16**

- Jede Gruppe G hat die triviale Untergruppe $H = \{e_G\}$ und $H = G$
- Ist $H \subseteq G$ und $K \subseteq H$, so ist $K \subseteq G$ (Transitivität)
- Unter Addition ist $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ eine Kette von Untergruppen
- Unter Multiplikation ist $\mu_2 \subseteq \mathbb{Q}^+ \subseteq \mathbb{R}^+$ eine Kette von Untergruppen
- Für $n \in \mathbb{N}_0$ ist $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z}$

Lemma 3.17
Ist G eine Gruppe und $(H_i)_{i\in I}$ eine Familie von Untergruppen von G, so ist auch $H := \bigcap H_i$ eine Untergruppe von G.

Beweis. Wir haben 3 Dinge zu zeigen

- $H \neq \emptyset$: Für jedes $i \in I$ ist $e_G \in H$, also auch $e_G \in \bigcap H_i = H$
- (UG1): Seien $x, y \in H$. Für jedes $i \in I$ ist $x, y \in H_i$, somit $xy \in H_i$, da $H_i \subseteq G$. Folglich ist $xy \in \bigcap H_i = H$.
- (UG2): Sei $x \in H$. Für jedes $i \in I$ ist $x \in H_i$, somit $x^{-1} \in H_i$, da $H_i \subseteq G$. Folglich ist $x^{-1} \in \bigcap H_i = H$.

□

Satz 3.18
Ist G eine Gruppe und $X \subset G$. so gibt es eine eindeutig bestimmte kleinste Untergruppe H von G, die X enthält, d.h. H enthält X und ist H' eine weitere Untergruppe von G, die X enthält, so ist $H \subset H'$.

Beweis. Sei $\mathcal{H}$ die Menge aller Untergruppen von G, die X enthalten. Nach Lemma 3.17 ist $H := \bigcap \mathcal{H} := \bigcap H$ eine Untergruppe von G. Da $X \subset H'$ für jedes $H' \in \mathcal{H}$ ist auch $X \subset H$. Nach Definition ist H in jedem $H' \subseteq G$ mit $X \subset H'$ enhalten. □

Definition 3.19 (erzeugte Untergruppe)
Ist G eine Gruppe und $X \subseteq G$, so nennt man diese kleinste Untergruppe von G, die X enthält, die von X erzeugte Untergruppe von G und bezeichnet diese mit $\langle X \rangle$, falls $X = \{x_1, x_2, ..., x_n\}$ enthält auch mit $\langle x_1, x_2, ..., x_n \rangle$. Gibt es eine endliche Menge $X \subset G$ mit $G = \langle X \rangle$, so nennt man G endlich erzeugt.

■ **Beispiel 3.20**

- Die leere Menge $X = \emptyset \subseteq G$ erzeugt stets die triviale Untergruppe $\langle \emptyset \rangle = \{e\} \subseteq G$
- Jede endliche Gruppe G ist endlich erzeugt $G = \langle G \rangle$
- Für $n \in \mathbb{N}_0$ ist $n\mathbb{Z} = \langle n \rangle \subseteq \mathbb{Z}$. Nach Beispiel 3.16 ist $n \in n\mathbb{Z} \subseteq \mathbb{Z}$. Ist $H \subseteq \mathbb{Z}$ mit $n \in H$, so ist auch $kn = nk = n + n + ... + n \in H$ und somit auch $n\mathbb{Z} \subseteq H$.

4. Ringe

Definition 4.1 (Ring)
Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R, einer Verknüpfung $+ : R \times R \to R$ (Addition) und einer anderen Verknüpfung $\cdot : R \times R \to R$ (Multiplikation), sodass diese zusammen die folgenden Axiome erfüllen:

- (R1) $(R, +)$ ist eine abelsche Gruppe.
- (R2) $(R, \cdot)$ ist eine Halbgruppe.
- (R3) Für $a, x, y \in R$ gelten die Distributivgesetze $a(x+y) = ax+ay$ und $(x+y)a = xa+ya$.

Ein Ring heißt kommutativ, wenn $xy = yx$ für alle $x, y \in R$.
Ein neutrales Element der Multiplikation heißt Einselement von R.
Ein Unterring eines Rings $(R, +, \cdot)$ ist eine Teilmenge, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Ring ist.

▶ **Bemerkung 4.2**
Hat ein Ring ein Einselement, so ist dieses eindeutig bestimmt. Notationelle Konfektionen: Das neutrale Element der Addition wird häufig mit 0 bezeichnet; die Multiplikation wird nicht immer notiert; Multiplikation bindet stärker als die Addition.
Wenn die Verknüpfungen aus dem Kontext klar sind, schreibt ma R statt $(R, +, \cdot)$.

■ **Beispiel 4.3**

- Der Nullring ist $R = \{0\}$ mit den einzig möglichen Verknüpfungen $+$ und $\cdot$ auf R. Der Nullring ist sogar kommutativ und hat ein Einselement, nämlich die 0.
- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement 1, ebenso $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$.
- $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, aber ohne Einselement.

▶ **Bemerkung 4.4**
Ist R ein Ring, dann gelten die folgenden Aussagen für $x, y \in R$

- $0 \cdot x = x \cdot 0 = 0$
- $x \cdot (-y) = (-x) \cdot y = -xy$
- $(-x) \cdot (-y) = xy$

▶ **Bemerkung 4.5**
Wir führen eine wichtige Klasse endlicher Ringe ein. Hierfür erinnern wir uns an eine der Grundlagen der Arithmetik in $\mathbb{Z}$.

Theorem 4.6
Sei $b \neq 0 \in \mathbb{Z}$. Für jedes $a \in \mathbb{Z}$ gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ (r ist "Rest"), mit $a = qb + r$ und $0 \leq r < |b|$.

Beweis. Existenz und Eindeutigkeit

- Existenz: oBdA nehmen wir an, dass $b > 0$ (denn ist $a = qb + r$, so ist auch $a = (-q)(-b) + r$). Sei $q \in \mathbb{Z}$ die größte Zahl mit $q \leq \frac{a}{b}$, und sei $r = a - qb \in \mathbb{Z}$. Dann ist $a \leq \frac{a}{b} - q < 1$, woraus $0 \leq r < b$ folgt.
- Eindeutigkeit: Sei $a = qb + r = q'b + r'$ mit $q, q', r, r' \in \mathbb{Z}$ und $0 \leq r, r' < |b|$. Dann ist $(q - q')b = r - r'$ und $|r - r'| < |b|$. Da $q - q' \in \mathbb{Z}$ ist, folgt $r - r' = 0$ und daraus wegen $b \neq 0$, dann $q - q' = 0$. □

■ **Beispiel 4.7 (Restklassenring)**
Wir fixieren $n \in \mathbb{N}$. Für $a \in \mathbb{Z}$ sei $\overline{a} := a + n\mathbb{Z} := \{a + nx \mid x \in \mathbb{Z}\}$ die Restklasse von "a mod n".
Für $a, a' \in \mathbb{Z}$ sind äquivalent:

- $a + n\mathbb{Z} = a' + n\mathbb{Z}$
- $a' \in a + n\mathbb{Z}$
- n teilt $a' - a$ (in Zeichen $n|a' - a$), d.h. $a' = a + nk$ für $k \in \mathbb{Z}$

Beweis.
- 1) ⇒ 2): klar, denn $0 \in \mathbb{Z}$
- 2) ⇒ 3): $a' \in a + n\mathbb{Z} \Rightarrow a' = a + nk$ mit $k \in \mathbb{Z}$
- 3) ⇒ 1): $a' = a + nk$ mit $k \in \mathbb{Z} \Rightarrow a + n\mathbb{Z} = \{a + nk + nx \mid x \in \mathbb{Z}\} = \{a + n(k + x) \mid x \in \mathbb{Z}\} = a + n\mathbb{Z}$

Insbesondere besteht $a + n\mathbb{Z}$ nur aus den ganzen Zahlen, die bei der Division durch n den selben Rest lassen wie a. □

Aus Theorem 4.6 folgt weiter, dass $\mathbb{Z}/n\mathbb{Z} := \{\overline{a} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ eine Menge der Mächtigkeit n ist (sprich: "$\mathbb{Z}$ mod $n\mathbb{Z}$").

Wir definieren Verknüpfungen auf $\mathbb{Z}/n\mathbb{Z}$ durch $\overline{a} + \overline{b} := \overline{a+b}$, $\overline{a} \cdot \overline{b} := \overline{ab}$ $a, b \in \mathbb{Z}$. Hierbei muss man zeigen, dass diese Verknüpfungen wohldefiniert sind, also nicht von den gewählten Vertretern a, b der Restklassen $\overline{a}$ und $\overline{b}$ abhängen. Ist etwa $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, also $a' = a + nk_1$ und $b' = b + nk_2$ mit $k_1, k_2 \in \mathbb{Z}$, so ist
$a' + b' = a + b + n(k_1 + k_2)$, also $\overline{a' + b'} = \overline{a + b}$
$a' \cdot b' = ab + n(bk_1 + ak_2 + nk_1k_2)$, also $\overline{a'b'} = \overline{ab}$
Man prüft nun leicht nach, dass $\mathbb{Z}/n\mathbb{Z}$ mit diesen Verknüpfungen ein kommutativer Ring mit Einselement ist, da dies auch für $(\mathbb{Z}, +, \cdot)$ gilt. Das neutrale Element der Addition ist $\overline{0}$, das Einselement ist $\overline{1}$.

■ **Beispiel 4.8**
Im Fall $n = 2$ ergeben sich die folgenden Verknüpfungstafeln für $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{2} = \overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Definition 4.9 (Charakteristik)
Sei R ein Ring mit Einselement. Man definiert die Charakteristik von R als die kleinste natürliche Zahl n mit $1+1+...+1=0$, falls so ein n existiert, andernfalls ist die Charakteristik 0.

Definition 4.10 (Nullteiler)
Sei R ein Ring mit Einselement. Ein $0 \neq x \in R$ ist ein Nullteiler von R, wenn er ein $0 \neq y \in R$ mit $xy = 0$ oder $yx = 0$ gibt. Ein Ring ohne Nullteiler ist nullteilerfrei.

Definition 4.11 (Einheit)
Sei R ein Ring mit Einselement. Ein $x \in R$ heißt invertierbar (oder Einheit von R), wenn es ein $x' \in R$ mit $xx' = x'x = 1$ gibt. Wir bezeichnen die invertierten Elemente von R mit $R^\times$.

Beispiel 4.12

- reelle Zahlen sind ein nullteilerfreier Ring der Charakteristik 0 mit $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$
- $\mathbb{Z}$ ist ein nullteilerfreier Ring der Charakteristik 0 mit $\mathbb{Z}^\times = \{1, -1\}$
- $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring der Charakteristik n. Ist n keine Primzahl, so ist $\mathbb{Z}$ nicht nullteilerfrei.

Satz 4.13
Sei R ein Ring mit Einselement.

- Ist $x \in R$ invertierbar, so ist x kein Nullteiler in R.
- Die invertierbaren Elemente von R bilden mit der Multiplikation eine Gruppe.

Beweis.

- Ist $xx' = x'x = 1$ und $xy = 0$ mit $x', y \in R$, so ist $0 = x' \cdot 0 = x \cdot xy = 1 \cdot y = y$, aber $y \neq 0$ für Nullteiler
- Sind $x, y \in R^\times$, also $xx' = x'x = yy' = y'y = 1$. Dann ist $(xy)(y'x') = x \cdot 1 \cdot x' = 1$ und $(y'x')(xy) = y' \cdot 1 \cdot y = 1$, somit $R^\times$ abgeschlossen unter der Multiplikation. Da $1 \cdot 1 = 1$ gilt, ist auch $1 \in R^\times$. Nach Definition von $R^\times$ hat jedes $x \in R^\times$ ein Inverses $x' \in R^\times$. □

5. Körper

Definition 5.1 (Körper)
Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$ mit Einselement $1 \neq 0$, in dem jedes Element $x \neq x \in K$ invertierbar ist.

▶ **Bemerkung 5.2**
Nach Satz 4.13 ist ein Körper ist stets nullteilerfrei und $(K\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe. Ein Körper ist also ein Tripel $(K, +, \cdot)$ bestehend aus einer Menge K und 2 Verknüpfungen $+ : K \times K \to K$ und $\cdot : K \times K \to K$, für die gelten:
(K1): $(K, +)$ ist eine abelsche Gruppe
(K2): $(K\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe, deren neutrales Element wir mit 1 bezeichnen
(K3): Es gelten die Distributivgesetze.

▶ **Bemerkung 5.3**
Sei K ein Körper und $a, x, y \in K$. Ist $ax = ay$ und $a \neq 0$, so ist $x = y$.

Definition 5.4 (Teilkörper)
Ein Teilkörper eines Körpers $(K, +, \cdot)$ ist die Teilemenge $L \subset K$, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Körper ist.

■ **Beispiel 5.5**

- Der Nullring ist kein Körper.
- Der Körper $\mathbb{Q}$ der rationalen Zahlen ist ein Teilkörper des Körpers $\mathbb{R}$ der reellen Zahlen.
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper

■ **Beispiel 5.6 (Komplexe Zahlen)**
Wir definieren die Menge $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ und darauf Verknüpfungen wie folgt: Für $(x_1, y_1), (x_2, y_2) \in \mathbb{C}$ ist:

- $(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$
- $(x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$

Wie man nachprüfen kann, ist $(\mathbb{C}, +, \cdot)$ ein Körper, genannt Körper der komplexen Zahlen. Da $(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0)$ und $(x_1, 0) \cdot (x_2, 0) = (x_1x_2, 0)$, können wir $\mathbb{R}$ durch "$x = (x, 0)$" mit dem Teilkörper $\mathbb{R} \times \{0\}$ von $\mathbb{C}$ identifizieren.
Die imaginäre Einheit $i = (0, 1)$ erfüllt $i^2 = -1$ und jedes $z \in \mathbb{C}$ kann eindeutig geschrieben werden als $z = x + iy$ mit $x, y \in \mathbb{R}$

Lemma 5.7
Sei $a \in \mathbb{Z}$ und sei p eine Primzahl, die a nicht teilt. Dann gibt es $b, k \in \mathbb{Z}$ mit $ab + kp = 1$.

Beweis. Sei $n \in \mathbb{N}$ die kleinste natürliche Zahl der Form $n = ab+kp$. Angenommen, $n \geq 2$. Schreibe $a = qp+r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < p$ (Theorem 4.6). Aus der Nichtteilbarkeit von a folgt $r \neq 0$, also $r \in \mathbb{N}$. Wegen $r = a \cdot 1 - qp$ ist $n \leq r$. Da p Primzahl ist und $2 \leq n \leq r < p$, gilt n teilt nicht p. Schreibe $p = c \cdot n + m$ mit $c, m \in \mathbb{Z}$ und $0 \leq m < n$ (Theorem 4.6). Aus n teilt nicht p folgt $m \neq 0$, also $m \in \mathbb{N}$. Da $m = p - cn = -abc + (1 - kc)p$, ist

$m < n$ ein Widerspruch zur Minimalität von n. Die Annahme $n \geq 2$ war somit falsch. Es gilt $n = 1$. □

■ **Beispiel 5.8 (Endliche Primkörper)**
Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Ist $\overline{a} \neq \overline{0}$, so gilt p teilt nicht a und somit gibt es nach Lemma 5.7 $b, k \in \mathbb{Z}$ mit

$$ab + kp = 1$$
$$(ab \bar{+} kp) = \overline{1} = \overline{(ab)} = \overline{a} \cdot \overline{b}$$

und somit ist $\overline{a}$ invertierbar in $\mathbb{Z}/p\mathbb{Z}$. Somit sind für $n \in \mathbb{N}$ äquivalent:

- $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper
- $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei
- n ist Primzahl

Beweis.
- $1 \Rightarrow 2$: Satz 4.13
- $2 \Rightarrow 3$: Beispiel 4.12
- $3 \Rightarrow 1$: gegeben

Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei, d.h. aus $p|ab$ folgt $p|a$ oder $p|b$. □

▶ **Bemerkung 5.9**
Ist K ein Körper und $a, b \in K$, $b \neq 0$, so schreiben wir $\frac{a}{b}$ für $ab^{-1} = b^{-1}a$. Es gelten die bekannten Rechenregeln für Brüche (vgl. Satz 3.10):

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

6. Polynome

In diesem Abschnitt sei R ein kommutativer Ring mit Einselement.

▶ **Bemerkung 6.1**
Unter einem Polynom in der "Unbekannte" x versteht man einen Ausdruck der Form $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n = \sum_{k=0}^{n} a_k x^k$ mit $a_0, ..., a_n \in R$. Fasst man x als ein beliebiges Element von R auf, gelten einige offensichtliche Rechenregeln:
Ist $f(x) = \sum_{k=0}^{n} a_k x^k$ und $g(x) = \sum_{k=0}^{n} b_k x^k$ so ist

- $f(x) + g(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$
- $f(x) \cdot g(x) = \sum_{k=0}^{2n} c_k x^k$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$

Dies motiviert die folgende präzise Definition für den Ring der Polynome über R in einer "Unbestimmten" x.

Definition 6.2 (Polynom)
Sei $R[X]$ die Menge der Folgen in R (siehe Bemerkung 2.13), die fast überall 0 sind, also

$$R[X] := \{(a_k)_{k \in \mathbb{N}_0} \mid \forall k (a_k \in R) \wedge \exists n_0 : \forall k > n_0 (a_k = 0)\}$$

Wir definieren Addition und Multiplikation auf $R[X]$:

- $(a_k)_{k \in \mathbb{N}_0} + (b_k)_{k \in \mathbb{N}_0} = (a_k + b_k)_{k \in \mathbb{N}_0}$
- $(a_k)_{k \in \mathbb{N}_0} \cdot (b_k)_{k \in \mathbb{N}_0} = (c_k)_{k \in \mathbb{N}_0}$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$

Mit diesen Verknüpfungen wird $R[X]$ zu einem kommutativen Ring mit Einselement. Diesen Ring nennt man Polynomring (in einer Variablen X) über R. Ein $(a_k)_{k \in \mathbb{N}_0} \in R[X]$ heißt Polynom mit den Koeffizienten $a_0, ..., a_n$. Wenn wir $a \in R$ mit der Folge $(a, 0, 0, ..., 0) := (a, \delta_{k,0})_{k \in \mathbb{N}_0}$ identifizieren, wird R zu einem Unterring von $R[X]$.

Definiert man X als die Folge $(0, 1, 0, .., 0) := (\delta_{k,1})_{k \in \mathbb{N}_0}$ (die Folge hat an der k-ten Stelle eine 1, sonst nur Nullen). Jedes $f(a_k)_{k \in \mathbb{N}_0}$ mit $a_k = 0$ für $k > n_0$ lässt sich eindeutig schreiben als $f(X) = \sum_{k=0}^{n_0} a_k X^k$. Alternativ schreiben wir auch $f = \sum_{k \geq 0} a_k X^k$ mit dem Verständnis, dass diese unendliche Summe nur endlich von 0 verschiedene Summanden enthält.

Sei $0 \neq f(X) = \sum_{k \geq 0} a_k X^k \in R[X]$. Der Grad von f ist das größte k mit $a_k \neq 0$, geschrieben $\deg(f) := max\{k \in \mathbb{N}_0 \mid a_k \neq 0\}$. Man definiert den Grad des Nullpolynoms als $\deg(0) = -\infty$, wobei $-\infty < k \forall k \in \mathbb{N}_0$ gelten soll. Man nennt a_0 den konstanten Term und $a_{\deg(f)}$ den Leitkoeffizienten von f. Hat f den Grad 0, 1 oder 2, so nennt man f konstant , linear bzw. quadratisch .

■ **Beispiel 6.3**
Das lineare Polynom $f(X) = X - 2 \in R[X]$ hat den Leitkoeffizient 1 und den konstanten Term -2.

Satz 6.4
Seien $f, g \in R[X]$

- Es ist $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.
- Es ist $\deg(f \cdot g) \leq \deg(f) + \deg(g)$.
- Ist R nullteilerfrei, so ist $\deg(f \cdot g) = \deg(f) + \deg(g)$ und auch $R[X]$ ist nullteilerfrei.

Beweis. • offenbar

- Ist $\deg(f) = n$ und $\deg(g) = m$, $f = \sum_{i\geq 0} f_i X^i$, $g = \sum_{j\geq 0} g_j X^j$, so ist auch $h = fg = \sum_{k\geq 0} h_k X^k$ mit $h_k = \sum_{i+j=k} f_i \cdot g_j$ für alle $k \geq 0$. Ist $k > n+m$ und $i+j = k$, so ist $i > n$ oder $j > m$, somit $f_i = 0$ oder $g_j = 0$ und somit $h_k = 0$. Folglich ist $\deg(h) \leq n+m$.
- Ist $f = 0$ oder $g = 0$, so ist die Aussage klar, wir nehmen als $n, m \geq 0$ an. Nach b) ist $\deg(h) \leq n+m$ und $h_{m+n} = \sum_{i+j=n+m} f_i g_j = f_n g_m$. Ist R nullteilerfrei, so folgt aus $f_n \neq 0$ und $g_m \neq 0$ schon $f_n g_m \neq 0$, und somit $\deg(h) = n+m$. □

Theorem 6.5 (Polynomdivision)
Sei K ein Körper und sei $0 \neq g \in K[X]$. Für jedes Polynom $f \in K[X]$ gibt es eindeutig bestimmte $g, h, r \in K[X]$ mit $f = gh + r$ und $\deg(r) < \deg(g)$.

Beweis. Existenz und Eindeutigkeit

- Existenz: Sei $n = \deg(f)$, $m = \deg(g)$, $f = \sum_{k=0}^{n} a_k X^k$, $g = \sum_{k=0}^{m} b_k X^k$
  Induktion nach n bei festem g.
  IA: Ist $n < m$, so wählt man $h = 0$ und $r = f$.
  IB: Wir nehmen an, dass die Aussage für alle Polynome vom Grad kleiner als n gilt.
  IS: Ist $n \geq m$, so betrachtet man $f_1 = f - \frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X)$. Da $\frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X)$ ein Polynom vom Grad $n - m + \deg(g) = n$ mit Leitkoeffizient $\frac{a_n}{b_m} \cdot b_m = a_n$ ist, ist $\deg(f_1) < n$. Nach IB gibt es also $h_1, r_1 \in K[X]$ mit $f_1 = gh_1 + r_1$ und $\deg(r) < \deg(g)$. Somit ist $f(X) = f_1(X) + \frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X) = gh + r$ mit $h(X) = h_1(X) + \frac{a_n}{b_m} \cdot X^{n-m}, r = r_1$.
- Eindeutigkeit: Sei $n = \deg(f), m = \deg(g)$. Ist $f = gh + r = gh' + r'$ und $\deg(r), \deg(r') < m$, so ist $(h-h')g = r' - r$ und $\deg(r'-r) < m$. Da $\deg(h-h') = \deg(h'-h) + m$ muss $\deg(h-h') < 0$, also $h' - h = 0$ sein. Somit $h' = h$ und $r' = r$. □

▶ **Bemerkung 6.6**
Der Existenzbeweis durch Induktion liefert uns ein konstruktives Verfahren, diese sogenannte Polynomdivision durchzuführen.

■ **Beispiel**
in $\mathbb{Q}[X]$: $(x^3 + x^2 + 1) : (x^2 + 1) = x + 1$ Rest $-x$

Definition 6.7 (Nullstelle)
Sei $f(X) = \sum_{k\geq 0} a_k X^k \in \mathbb{R}[X]$. Für $\lambda \in \mathbb{R}$ definiert man die Auswertung von f in λ $f(\lambda) = \sum_{k\geq 0} a_k \lambda^k \in \mathbb{R}$. Das Polynom f liefert auf diese Weise eine Abbildung $\tilde{f} : \mathbb{R} \to \mathbb{R}$ und $\lambda \mapsto f(\lambda)$.
Ein $\lambda \in \mathbb{R}$ $f(\lambda) = 0$ ist eine Nullstelle von f.

Lemma 6.8
Für $f, g \in \mathbb{R}[X]$ und $\lambda \in \mathbb{R}$i ist

$$(f+g)(\lambda) = f(\lambda) + g(\lambda)$$
$$(fg)(\lambda) = f(\lambda) \cdot g(\lambda)$$

Beweis. Ist $f = \sum_{k\geq 0} a_k X^k$ und $g = \sum_{k\geq 0} b_k X^k$, so ist

$$\begin{aligned} f(\lambda) + g(\lambda) &= \sum_{k\geq 0} a_k \lambda^k + \sum_{k\geq 0} b_k \lambda^k \\ &= \sum_{k\geq 0} (a_k + b_k)\lambda^k \\ &= (f+g)(\lambda) \end{aligned}$$

und

$$\begin{aligned} f(\lambda) \cdot g(\lambda) &= \sum_{k\geq 0} a_k \lambda^k \cdot \sum_{k\geq 0} b_k \lambda^k \\ &= \sum_{k\geq 0} \sum_{i+j=k} (a_i + b_j)\lambda^k \\ &= (fg)(\lambda) \end{aligned}$$

□

Satz 6.9
Ist K ein Körper und $\lambda \in K$ eine Nullstelle von $f \in K[X]$ so gibt es ein eindeutig bestimmtes $h \in K[X]$ mit $f(X) = (X - \lambda) \cdot h(x)$.

Beweis. Nach Theorem 6.5 gibt es gibt $h, r \in K[X]$ mit $f(X) = (X-\lambda)\cdot h(x) + r(x)$ und $\deg(r) < \deg(X-\lambda) = 1$, also $r \in K$. Da λ Nullstelle von f ist, gilt $0 = f(\lambda) = (\lambda - \lambda) \cdot h(\lambda) + r(\lambda) = r(\lambda)$ nach Lemma 6.8. Hieraus folgt $r = 0$. Eindeutigkeit folgt aus Eindeutigkeit in Theorem 6.5. □

Folgerung 6.10
Sei K ein Körper. Ein Polynom $0 \neq f \in K[X]$ hat höchstens $\deg(f)$ viele Nullstellen.

Beweis. Induktion nach $\deg(f) = n$
Ist $n = 0$, so ist $f \in K^\times$ und hat somit keine Nullstellen.
Ist $n > 0$ und hat f eine Nullstelle $\lambda \in K$, so ist $f(X) = (X - \lambda) * h(x)$ mit $h(x) \in K[X]$ und $\deg(f) = \deg(X - \lambda) + \deg(h) = n - 1$. Nach IV besitzt h höchstens $\deg(h) = n - 1$ viele Nullstellen. Ist λ' eine Nullstelle von f, so ist $0 = f(\lambda') = (\lambda' - \lambda) * h(\lambda')$, also $\lambda' = \lambda$ oder λ' ist Nullstelle von h. Somit hat f höchstens n viele Nullstellen in K. □

Folgerung 6.11
Ist K ein unendlicher Körper, so ist die Abbildung $K[X] \to \mathrm{Abb}(K, K)$ und $f \mapsto \tilde{f}$ injektiv.

Beweis. Sind $f, g \in K[X]$ mit $\tilde{f} = \tilde{g}$, also $f(\lambda) = g(\lambda)$ für jedes $\lambda \in K$, so ist jedes λ Nullstelle von $h := f - g \in K[X]$. Da $|K| = \infty$ ist, so ist $h = 0$, also $f = g$. □

▶ **Bemerkung 6.12**

Dieses Korollar besagt uns, dass man über einem unendlichen Körper Polynome als polynomiale Abbildungen auffassen kann. Ist K aber endlich, so ist dies im Allgemeinen nicht richtig. Beispiel: $K = \mathbb{Z}\backslash 2\mathbb{Z}$, $f(X) = X$, $g(X) = X^2 \Rightarrow f \neq g$, aber $\tilde{f} = \tilde{g}$.

■ **Beispiel 6.13**

Sei $f(X) = X^2 + 1 \in \mathbb{R}[X] \subset \mathbb{C}[X]$

In $K = \mathbb{R}$ hat f keine Nullstelle: Für $\lambda \in \mathbb{R}$ $f(\lambda) = \lambda^2 + 1 \geq 1 > 0$.

In $K = \mathbb{C}$ hat f die beiden Nullstellen $\lambda_1 = i$ und $\lambda_2 = -i$ und zerfällt dort in Linearfaktoren: $f(X) = (X - i)(X + i)$.

Satz 6.14

Für einen Körper K sind äquivalent:

- Jedes Polynom $f \in K[X]$ mit $\deg(f) > 0$ hat eine Nullstelle in K.
- Jedes Polynom $f \in K[X]$ zerfällt in Linearfaktoren, also $f(X) = a \cdot \prod_{i=1}^{n}(X - \lambda_i)$ mit $n = \deg(f), a, \lambda_i \in K$.

Beweis.

- $1 \Rightarrow 2$: Induktion nach $n = \deg(f)$

  Ist $n \leq 0$, so ist nichts zu zeigen.

  Ist $n > 0$, so hat f eine Nullstelle $\lambda_n \in K$, somit $f(X) = (X - \lambda_n) \cdot g(X)$ mit $g(X) \in K[X]$ und $\deg(g) = n - 1$, Nach IV ist $g(X) = a \cdot \prod_{i=1}^{n}(X - \lambda_i)$. Nach Satz 6.9 ist $f(X) = a \cdot \prod_{i=1}^{n}(X - \lambda_i)$.
- $2 \Rightarrow 1$: Sei $f \in K[X]$ mit $n = \deg(f) > 0$. Damit gilt $f(X) = a \cdot \prod_{i=1}^{n}(X - \lambda_i)$. Da $n > 0$, hat f z.B. die Nullstelle λ_1. □

Definition 6.15 (algebraisch abgeschlossen)

Ein Körper K heißt algebraisch abgeschlossen , wenn er eine der äquivalenten Bedingungen aus Satz 6.14 erfüllt.

Theorem 6.16 (Fundamentalsatz der Algebra)

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

▶ **Bemerkung 6.17**

Wir werden das Theorem zwar benutzen, aber nicht beweisen.

Kapitel II

Vektorräume

1. Definition und Beispiele

In diesem Kapitel sei K ein Körper.

■ **Beispiel 1.1**
Ist $K = \mathbb{R}$, so haben wir für $K^3 = \mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(a, b, c) | a, b, c \in \mathbb{R}\}$ eine geometrische Anschauung, nämlich den euklidischen Raum. Welche algebraische Struktur können wir hierauf sinnvollerweise definieren?

Definition 1.2 (Vektorraum)
Ein K-Vektorraum (auch Vektorraum über K) ist ein Tripel $(V, +, \cdot)$ bestehend aus einer Menge V, einer Verknüpfung $+ : V \times V \to V$, genannt Addition, und einer Abbildung $\cdot : K \times V \to V$, genannt Skalarmultiplikation, für die gelten:

- (V1): $(V, +)$ ist eine abelsche Gruppe
- (V2): Addition und Skalarmultiplikation sind verträglich:
  - $\lambda(x + y) = (\lambda \cdot x) + (\lambda \cdot y)$
  - $(\lambda + \mu) \cdot x = (\lambda \cdot x) + (\mu \cdot x)$
  - $\lambda(\mu \cdot x) = (\lambda \cdot \mu) \cdot x$
  - $1 \cdot x = x$

▶ **Bemerkung 1.3**
Wir haben sowohl im Körper K als auch im Vektorraum V eine Addition definiert, die wir mit dem selben Symbol + notieren. Ebenso benutzen wir das Symbol $\cdot$ sowohl für die Multiplikation im Körper K als auch für die Skalarmultiplikation. Zur Unterscheidung nennt man die Elemente von V Vektoren und die Elemente von K Skalare. Wir werden bald auch den Nullvektor mit 0 bezeichnen, also mit dem selben Symbol wie das neutrale Element im Körper K. Auch für Vektorräume gibt es notationelle Konvektionen: So bindet die Skalarmultiplikation stärker als die Addition und wird manchmal nicht notiert.

■ **Beispiel 1.4**
Für $n \in \mathbb{N}$ ist $V = K^n := \prod_{i=1}^{n} K = \{(x_1, x_2, ..., x_n) \mid x_1, x_2, .., x_n \in K\}$ mit komponentenweiser Addition und Skalarmultiplikation $\lambda(x_1, ..., x_n) = (\lambda \cdot x_1, ..., \lambda \cdot x_n)$ ein K-Vektorraum, genannt der (n-dimensionale) Standardraum über K.
Insbesondere (Spezialfall $n = 1$) ist K ein K-Vektorraum.
Für $n = 0$ definiert man K^0 als Nullraum $V = \{0\}$, der einzig möglichen Addition und Skalarmultiplikation einen K-Vektorraum bildet.

Satz 1.5
ist V ein K-Vektorraum, so gelten für $\lambda \in K$ und $x \in V$:

- $0 \cdot x = 0$
- $\lambda \cdot 0 = 0$
- $(-\lambda) \cdot x = \lambda \cdot (-x) = -\lambda \cdot x$. Insbesondere $(-1)x = -x$
- Ist $\lambda \cdot x = 0$, so ist $\lambda = 0$ oder $x = 0$

Beweis.
- Es ist $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, woraus $0 = 0 \cdot x$
- Es ist $\lambda \cdot 0 = \lambda(0 + 0) = \lambda \cdot 0 + 0 \cdot \lambda$, woraus $0 = \lambda \cdot 0$
- Es ist $\lambda \cdot x + (-\lambda \cdot x) = (\lambda + (-\lambda)) \cdot x = 0 \cdot x = 0$, also $(-\lambda)x = -(\lambda x)$
- Ist $\lambda \cdot x = 0$ und $\lambda \neq 0$, so ist $0 = \lambda^{-1} \cdot \lambda \cdot x = 1 \cdot x = x$ □

■ **Beispiel 1.6**
- Schränkt man die Multiplikation im Polynomring $K[X] \times K[X] \to K[X]$ zu einer Abbildung $K \times K[X] \to K[X]$ ein, so wird $K[X]$ mit dieser Skalarmultiplikation zu einem K-Vektorraum. Die Skalarmultiplikation ist also gegen $\lambda \cdot \sum_{k \geq 0} a_k \cdot X^k = \sum_{k \geq 0} \lambda \cdot a_k \cdot X^k$ ersetzt wurden.
- Schränkt man die komplexe Multiplikation $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ zu einer Abbildung $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$ ein, so wird $\mathbb{C}$ mit dieser Skalarmultiplikation zu einem $\mathbb{R}$-Vektorraum. Die Skalarmultiplikation ist gegeben durch $\lambda(x + iy) = \lambda \cdot x + i \cdot \lambda \cdot y$.
- Verallgemeinerung von 1 und 2: Ist der Körper K ein Unterring eines kommutativen Rings R mit Einselement $1_K \in K$, so wird R durch Einschränkung der Multiplikation $R \times R \to R$ zu einer Abbildung $K \times R \to R$ zu einem K-Vektorraum.
- Ist X eine Menge, so wird die Menge der Abbildungen $\mathrm{Abb}(X, K)$ durch punktweise Addition $(f + g)(x) = f(x) + g(x)$ und die Skalarmultiplikation $(\lambda \cdot f)(x) = \lambda \cdot f(x)$ zu einem K-Vektorraum. Im Spezialfall $X = \{1, 2, ..., n\}$ erhält man den Standardraum K^n.

Definition 1.7 (Untervektorraum)
Sei V ein K-Vektorraum. Ein Untervektorraum (Untervektorraum) von V ist eine nichtleere Teilmenge $W \subseteq V$ mit:

- (UV1): Für $x, y \in W$ ist $x + y \in W$.
- (UV2): Für $x \in W$ und $\lambda \in K$ ist $\lambda \cdot x \in W$.

Satz 1.8
Sei V ein K-Vektorraum und $W \subseteq V$. Genau dann ist W ein Untervektorraum von V, wenn W mit geeigneter Einschränkung der Addition und Skalarmultiplikation wieder ein K-Vektorraum ist.

Beweis.
- $\Rightarrow$: Lassen sich $+ \colon V \times V \to V$ und $\cdot \colon K \times V \to V$ einschränken zur Abbildung $+_w \colon W \times W \to W$, $\cdot_w \colon K \times W \to W$ so gilt für $x, y \in W$ und $\lambda \in K$: $x + y = x +_w y \in W$ und $\lambda \cdot x = \lambda \cdot_w x \in W$. Ist $(W, +_w, \cdot_w)$ ein K-Vektorraum, so ist insbesondere W nicht leer. Somit ist W ein Untervektorraum.
- $\Leftarrow$: Nach (UV1) und (UV2) lassen sich $+$ und $\cdot$ einschränken zu Abbildungen $+_w \colon W \times W \to W$ und

$\cdot_w$: $K \times W \to W$. Nach (UV1) ist abgeschlossen und unter der Addition und für $x \in W$ ist auch $-x = (-1)x \in W$ nach (UV2), W ist somit Untergruppe von $(V, +)$. Insbesondere ist $(W, +)$ eine abelsche Gruppe (Satz 3.14), erfüllt also (V1). Die Verträglichkeit (V2) ist für $\lambda, \mu \in K$ und $x, y \in W$ gegeben, da sie auch für $x, y \in V$ erfüllt ist. Somit ist $(W, +_w, \cdot_w)$ ein K-Vektorraum. □

Beispiel 1.9

- Jeder K-Vektorraum hat triviale Untervektorraum $W = \{0\}$ und $W = V$
- Ist V ein K-Vektorraum und $x \in V$, so ist $W = K \cdot x = \{\lambda \cdot x \mid \lambda \in K\}$ ein Untervektorraum von V. Insbesondere besitzt z.B. der $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ unendlich viele Untervektorraum, nämlich alle Ursprungsgeraden. Hieran sehen wir auch, dass die Vereinigung zweier Untervektorraum im Allgemeinen kein Untervektorraum ist. $\mathbb{R} \cdot (1, 0) \cup \mathbb{R} \cdot (1, 0) \subseteq \mathbb{R}^2$ verletzt (UV1).
- Der K-Vektorraum $K[X]$ hat unter anderem die folgenden Untervektorraum:
  - Den Raum K der konstanten Polynome
  - Den Raum $K[X]_{\leq 1} = \{aX + b \mid a, b \in K\}$ der linearen (oder konstanten) Polynome
  - allgemeiner den Raum $K[X]_{\leq n} = \{f \in K[X] \mid \deg(f) \leq n\}$ der Polynome von höchstens Grad n
- In der Analysis werden Sie verschiedene Untervektorraum des $\mathbb{R}$-Vektorraum $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$ kennenlernen, etwa den Raum $\mathcal{C}(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen und den Raum $\mathcal{C}^{-1}(\mathbb{R}, \mathbb{R})$ der stetig differenzierbaren Funktionen. Die Menge der Polynomfunktionen $\{\tilde{f} \mid \tilde{f} \in \mathbb{R}[X]\}$ (vgl. Definition 6.7) bildet einen Untervektorraum des $\mathbb{R}$-Vektorraum $\mathcal{C}^{-1}(\mathbb{R}, \mathbb{R})$

Lemma 1.10
Ist V ein Vektorraum und $(W_i)_{i \in I}$ eine Familie von Untervektorraum von V, so ist auch $W = \bigcap W_i$ ein Untervektorraum von V.

Beweis. Da $0 \in W_i$ ist auch $0 \in W$, insbesondere $W \neq \emptyset$.

- (UV1): Sind $x, y \in W$, so ist auch $x, y \in W_i$ und deshalb $x + y \in \bigcap W_i = W$.
- (UV2): Ist $x \in W$ und $\lambda \in K$, so ist auch $x \in W_i$ und somit $\lambda x \in \bigcap W_i = W$. □

Satz 1.11
Ist V ein K-Vektorraum und $X \subseteq V$, so gibt es einen eindeutig bestimmten kleinsten Untervektorraum W von V mit $X \subseteq W$.

Beweis. Sei $\mathcal{V}$ die Menge aller Untervektorraum von X, die X enthalten. Sei $W = \bigcap \mathcal{V}$. Damit ist W ein Untervektorraum (Lemma 1.10) von V der X enthält. □

Definition 1.12 (Erzeugendensystem)
Ist V ein K-Vektorraum und $X \subseteq V$, so nennt man den kleinsten Untervektorraum von V, der X enthält den von X erzeugten Untervektorraum von V und bezeichnet diesen mit $\langle X \rangle$. Eine Menge $X \subseteq V$ mit $\langle X \rangle = V$ heißt Erzeugendensystem von V. Der Vektorraum V heißt endlich erzeugt, wenn er ein endliches Erzeugendensystem besitzt.

2. Linearkombinationen

Sei V ein K-Vektorraum.

Definition 2.1 (Linearkombination)

- Sei $n \in \mathbb{N}_0$. Ein $x \in V$ ist eine Linearkombination eines n-Tupels $(x_1, ..., x_n)$ von Elementen von V, wenn es $\lambda_1, ..., \lambda_n \in K$ gibt mit $x = \lambda_1 \cdot x_1, ..., \lambda_n \cdot x_n$. Der Nullvektor ist stets eine Linearkombination von $(x_1, ..., x_n)$ auch wenn $n = 0$.
- Ein $x \in V$ ist eine Linearkombination einer Familie (x_i) von Elementen von V, wenn es $n \in \mathbb{N}_0$ und $i_1, ..., i_n \in I$ gibt, für die x Linearkombination von $(x_{i_1}, ..., x_{i_n})$ ist.
- Die Menge aller $x \in V$, die Linearkombination von $\mathcal{F} = (x_i)$ sind, wird mit $\text{span}_K(\mathcal{F})$ bezeichnet.

▶ **Bemerkung 2.2**

- Offenbar hängt die Menge der Linearkombinationen von $(x_1, ..., x_n)$ nicht von der Reihenfolge der x_i ab. Wegen (V2)(ii) hängt sie sogar nur von der Menge $\{x_1, ..., x_n\}$ ab.
- Deshalb stimmt 2. für endliche Familien $(x_1, ..., x_n)$ mit 1. überein.
- Auch die Menge der Linearkombinationen einer Familie $\mathcal{F} = (x_1, ..., x_n)$ hängt nur von der Menge $X = \{x_i \mid i \in I\}$ ab. Man sagt deshalb auch, x ist Linearkombination von X und schreibt $\text{span}_K(X) = \text{span}_K(\mathcal{F})$, also $\text{span}_K(X) = \{\sum_{i=1}^{n} \lambda_i \cdot n_i \mid n \in \mathbb{N}_0, x_i \in X, \lambda_1, ..., \lambda_n \in K\}$. Nach Definition ist stets $0 \in \text{span}_K(X)$ auch für $X = \emptyset$.
- Wie schon bei Polynomen schreibt man hier gerne formal unendliche Summen $x = \sum_{i \in I} \lambda_i \cdot x_i$, bei denen nur endlich viele λ_i von 0 verschieden sind.

Lemma 2.3
Für jede Teilmenge $X \subseteq V$ ist $\text{span}_K(X)$ ein Untervektorraum von V.

Beweis.

- Sei $W = \text{span}_K(X)$. Nach Definition ist $0 \in W$, insbesondere $W \neq \emptyset$
- (UV1): Sind $x, y \in W$, also $x = \lambda_1 \cdot x + ... + \lambda_n \cdot x_n$ und $y = \mu_1 \cdot x + ... + \mu_n \cdot x_n$, so ist $x + y = (\lambda_1 + \mu_1)x_1 + ... + (\lambda_n + \mu_n)x_n \in W$
- (UV2): Ist $\lambda \in K$ und $x \in W$, so ist $\lambda x = \lambda \cdot \sum_{i=1}^{n} \lambda_i \cdot x_i = \sum_{i=1}^{n} (\lambda \cdot \lambda_i)x_i \in W$ □

Satz 2.4
Für jede Teilmenge $X \subseteq V$ ist $\text{span}_K(X) = \langle X \rangle$.

Beweis.

- $\text{span}_K(X)$ ist Untervektorraum von V, der wegen $x = x \cdot 1$ die Menge X enthält, und $\langle X \rangle$ ist der kleinste solche.
- Ist $W \subseteq V$ ein Untervektorraum von V, der X enthält, so enthält er auch wegen (UV2) alle Elemente der Form $\lambda \cdot x$, und wegen (UV1) dann auch alle Linearkombinationen aus X. Insbesondere gilt dies auch für $W = \langle X \rangle$ □

▶ **Bemerkung 2.5**

Wir erhalten $\text{span}_K(X) = \langle X \rangle$ auf 2 verschiedenen Wegen. Erstens "von oben" als Schnitt über alle Untervektorraum von V, die X enthalten und zweitens "von unten" als Menge der Linearkombinationen. Man nennt $\text{span}_K(X)$ auch den von X aufgespannten Untervektorraum oder die lineare Hülle von X.

■ **Beispiel 2.6**

- Sei $V = K^n$ der Standardraum. Für $i = 1, ..., n$ sei $e_i = (\delta_{i,1}, ..., \delta_{i,n})$, also $e_1 = (1, 0, ...0)$, $e_2 = (0, 1, 0, ..., 0), ..., e_n = (0, ..., 1)$. Für $x = (x_1, ..., x_n) \in V$ ist $x = \sum_{i=1}^{n} x_i \cdot e_1$, folglich $\text{span}_K(e_1, .., e_n) = V$. Insbesondere ist K^n eindeutig erzeugt. Man nennt $(e_1, ..., e_n)$ die Standardbasis des Standardraums K^n.
- Sei $V = K[X]$ Polynomring über K. Da $f = \sum_{i=1}^{n} a_i \cdot X^i$ ist $\text{span}_K((X^i)_{i \in I}) = K[X]$. Genauer ist $\text{span}_K(1, X, X^2, ..., X^n) = K[X]_{\leq n}$. Tatsächlich ist der K-Vektorraum $K[X]$ nicht endlich erzeugt. Sind $f_1, ..., f_r \in K[X]$ und ist $d = \max\{\deg(f_1), ..., \deg(f_r)\}$, so sind $f_1, ..., f_r \in K[X]_{\leq d}$ und somit $\text{span}_K(f_1, ..., f_r) \subseteq K[X]_{\leq d}$, aber es gibt Polynome, deren Grad größer d ist.
- Für $x \in V$ ist $\langle x \rangle = \text{span}_K(x) = K \cdot x$. Im Fall $K = \mathbb{R}$, $V = \mathbb{R}^3$, $x \neq 0$ ist dies eine Ursprungsgerade.
- Im $\mathbb{R}$-Vektorraum $\mathbb{C}$ ist $\text{span}_{\mathbb{R}}(1) = \mathbb{R} \cdot 1 = \mathbb{R}$, aber im $\mathbb{C}$-Vektorraum $\mathbb{C}$ ist $\text{span}_{\mathbb{C}}(1) = \mathbb{C} \cdot 1 = \mathbb{C}$

Definition 2.7 (linear (un)abhängig)

- Sei $n \in \mathbb{N}_0$. Ein n-Tupel $(x_1, ..., x_n)$ von Elementen von V ist linear abhängig , wenn es $\lambda_1, ..., \lambda_n \in K$ gibt, die nicht alle 0 sind und $\lambda_1 \cdot x_1 + ... + \lambda_n \cdot x_n = 0$ (*) erfüllen. Andernfalls heißt das Tupel linear unabhängig .
- Eine Familie (x_i) von Elementen von V ist linear abhängig, wenn es $n \in \mathbb{N}_0$ und paarweise verschiedene $i_1, ..., i_n \in I$ gibt, für die $(x_{i_1}, ..., x_{i_n})$ linear abhängig ist. Andernfalls linear unabhängig.

Mathematica/WolframAlpha-Befehle (Lineare Unabhängigkeit)

In WolframAlpha kann man mittels

```
linear independence (1,2,3), (4,5,6)
```

überprüfen, ob die Vektoren $(1, 2, 3)^T$ und $(4, 5, 6)^T$ linear unabhängig sind.

▶ **Bemerkung 2.8**

- Offenbar hängt die Bedingung (*) nicht von der Reihenfolge der $x_1, ..., x_n$ ab und ist $(x_1, ..., x_k)$ linear abhängig für ein $k \leq n$, so ist auch $(x_1, ..., x_n)$ linear abhängig. Deshalb stimmt die 2. Definition für endliche Familien mit der 1. überein und (x_i) ist genau dann linear abhängig, wenn es eine endliche Teilmenge $J \subseteq I$ gibt, für die (x_j) linear abhängig ist.
- Eine Familie ist genau dann linear unabhängig, wenn für jede endliche Teilmenge $J \subseteq I$ und für jede Wahl an Skalaren $(\lambda_i)_{i \in J}$ aus $\sum \lambda_i \cdot x_i = 0$ schon $\lambda_i = 0$ folgt, also wenn sich der Nullvektor nur trivial linear kombinieren lässt.

Satz 2.9
Genau dann ist (x_i) linear abhängig, wenn es $i_0 \in I$ gibt mit $x_{i_0} \in \text{span}_K((x_i)_{i\in I\setminus\{i_0\}})$. In diesem Fall ist $\text{span}_K((x_i)_{i\in I}) = \text{span}_K((x_i)_{i\in I\setminus\{i_0\}})$.

Beweis. Es reicht, die Aussage für $I = \{1, ..., n\}$ zu beweisen.

- Hinrichtung: Ist $(x_1, ..., x_n)$ linear anhängig, so existieren $\lambda_1, ..., \lambda_n$ mit $\sum_{i=1}^n \lambda_i \cdot x_i = 0$. oBdA. sei $\lambda_n \neq 0$. Dann ist $x_n = \lambda_n^{-1} \cdot \sum_{i=1}^{n-1} \lambda_i \cdot x_i = \sum_{i=1}^{n-1} \lambda_n^{-1} \cdot \lambda_i \cdot x_i \in \text{span}_K(x_1, ..., x_n)$.
- Rückrichtung: oBdA. $i_0 = n$, also $\sum_{i=0}^{n-1} \lambda_i \cdot x_i$. Mit $\lambda_n = -1$ ist $\sum_{i=1}^n \lambda_i \cdot x_i = 0$, was zeigt, dass $(x_1, ..., x_n)$ linear abhängig ist.
  Sei nun $x_n = \sum_{i=1}^{n-1} \lambda_i \cdot x_i \in \text{span}_K(x_1, ..., x_{n-1})$. Wir zeigen, dass $\text{span}_K(x_1, ..., x_{n-1}) = \text{span}_K(x_1, ..., x_n)$
  - klar, da bei mehr Elementen die Anzahl der Linearkombinationen nicht abnimmt
  - Ist $y = \sum_{i=1}^n \mu_i \cdot x_i \in \text{span}_K(x_1, ..., x_n)$, so ist $y = \sum_{i=1}^{n-1} \mu_i + \mu_n \cdot \lambda_i \cdot x_i \in \text{span}_K(x_1, ..., x_n)$ □

Satz 2.10
Genau dann ist (x_i) linear unabhängig, wenn sich jedes $x \in \text{span}_K((x_i))$ in eindeutiger Weise als Linearkombination der (x_i) schreiben lässt, d.h. $x = \sum_{i\in I} \lambda_i \cdot x_i = \sum_{i\in I} \lambda_i' \cdot x_i$, so ist $\lambda_i = \lambda_i'$

Beweis. Es reicht, die Aussage für $I = \{1, ..., n\}$ zu beweisen.

- Hinrichtung: Ist $(x_,..., x_n)$ linear unabhängig und $x = \sum_{i\in I} \lambda_i \cdot x_i = \sum_{i\in I} \lambda_i' \cdot x_i$, so folgt daraus $\sum_{i\in I}(\lambda_i - \lambda_i')x_i = 0$ wegen der linearen Unabhängigkeit der x_i, dass $\lambda_i = \lambda_i' = 0$

- Rückrichtung: Lässt sich jedes $x \in \text{span}_K(x_1, ..., x_n)$ in eindeutiger Weise als Linearkombination der x_i schreiben, so gilt dies insbesondere für $x = 0$. Ist also $\sum_{i=1}^n \lambda_i \cdot x_i = 0$, so folgt schon $\sum_{i=1}^n 0 \cdot x_i = 0$ schon $\lambda_i = 0$ □

■ **Beispiel 2.11**

- Die Standardbasis $(e_1, ..., e_n)$ des K^n ist linear unabhängig. Es ist $\sum_{i=1}^n \lambda_i \cdot e_i = (\lambda_1, ..., \lambda_n)$
- Im K-Vektorraum $K[X]$ sind die Monome (X^i) linear unabhängig.
- Ein einzelner Vektor $x \in V$ ist genau dann linear abhängig, wenn $x = 0$.
- Ein Paar (x_1, x_2) von Elementen von V ist linear abhängig, wenn es ein skalares Vielfaches des anderen ist, also z.B. $x_1 = \lambda \cdot x_2$.
- Im $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ sind die beiden Vektoren $(1, 2)$ und $(2, 1)$ linear unabhängig.
  Im $\mathbb{Z}\backslash 3\mathbb{Z}$-Vektorraum $(\mathbb{Z}\backslash 3\mathbb{Z})^2$ sind diese Vektoren linear unabhängig, da $x_1 + x_2 = (1, 2) + (2, 1) = (3, 3) = (0, 0) = 0$.
- Im $\mathbb{R}$-Vektorraum $\mathbb{C}$ ist $(1, i)$ linear unabhängig, aber im $\mathbb{C}$-Vektorraum $\mathbb{C}$ ist $(1, i)$ linear abhängig, denn $\lambda_1 \cdot 1 + \lambda_2 \cdot i = 0$ für $\lambda_1 = 1$ und $\lambda_2 = i$.

▶ **Bemerkung 2.12**

- Ist $x_{i_0} = 0$, ist (x_i) linear abhängig: $1 \cdot x_{i_0} = 0$
- Gibt es $i, j \in I$ mit $i \neq j$, aber $x_i = x_j$, so ist (x_i) linear abhängig: $x_i - x_j = 0$

- Dennoch sagt man auch "die Teilmenge $X \subseteq V$ ist linear abhängig" und meint damit, dass die Familie $(x_x)_{x \in X}$ linear abhängig ist, d.h. es gibt ein $n \in \mathbb{N}_0$, $x_1, ..., x_n \in X$ paarweise verschieden, mit $\sum_{i=1}^{n} \lambda_i \cdot x_i = 0$.

3. Basis und Dimension

Definition 3.1 (Basis)
Eine Familie (x_i) von Elementen von V ist eine Basis von V, wenn gilt:

- (B1): Die Familie ist linear unabhängig.
- (B2): Die Familie erzeugt V, also $\text{span}_K(x_i) = V$.

▶ **Bemerkung 3.2**
Kurz gesagt ist eine Basis ein linear unabhängiges Erzeugendensystem.

Satz 3.3
Sei (x_i) eine Familie von Elementen von V. Genau dann ist (x_i) eine Basis von V, wenn sich jedes $x \in V$ auf eindeutige Weise als Linearkombination der (x_i) schreiben lässt.

Beweis. Dies folgt sofort aus Satz 2.10 □

■ **Beispiel 3.4**

- Die leere Familie ist eine Basis des Nullraums.
- Die Standardbasis $(e_1, ..., e_n)$ ist eine Basis des Standardraums.
- Die Monome (X^i) bilden eine Basis des K-Vektorraum $K[X]$.
- Die Basis des $\mathbb{R}$-Vektorraum $\mathbb{C}$ ist gegeben durch $(1, i)$, eine Basis des $\mathbb{C}$- Vektorraum $\mathbb{C}$ ist gegeben durch (1)
- Der $\mathbb{C}$-Vektorraum $\mathbb{C}$ hat viele weitere Basen.

Satz 3.5
Für eine Familie (x_i) von Elementen von V sind äquivalent:

- B ist eine Basis von V.
- B ist ein minimales Erzeugendensystem.
- B ist maximal linear unabhängig, d.h. B ist linear unabhängig, aber wenn Elemente zur Basis hinzugefügt werden, ist diese nicht mehr linear unabhängig.

Beweis.

- $1 \Rightarrow 2$: Sei B eine Basis von V und J eine echte Teilmenge von I. Nach Definition ist B ein Erzeugendensystem. Wähle $i_0 \in I \backslash J$. Da (x_i) linear unabhängig ist, ist x_{i_0} keine Element $\text{span}_K((x_i)_{i \in I \backslash \{i_0\}}) \supseteq \text{span}_K((x_i)_{i \in J})$ (Satz 2.9). Insbesondere ist $(x_i)_{i \in J}$ kein Erzeugendensystem von V.
- $2 \Rightarrow 3$: Sei B ein minimales Erzeugendensystem und $(x_i)_{i \in J}$ eine Familie mit J echter Obermenge von I. Wäre (x_i) linear abhängig, so gäbe es ein i_0 mit $\text{span}_K((x_i)_{i \in I \backslash \{i_0\}}) = \text{span}_K((x_i)_{i \in I}) = V$ im Widerspruch zur Minimalität von B. Also ist $B = (x_i)$ linear unabhängig. Wähle $j_0 \in J \backslash I$. Dann ist $x_{j_0} \in V = \text{span}_K(x_i) \leq \text{span}_K((x_i)_{i \in J \backslash \{j_0\}})$ und somit ist $(x_i)_{i \in J}$ linear abhängig nach Satz 2.9.
- $3 \Rightarrow 1$: Sei B nun maximal linear unabhängig. Angenommen B wäre kein Erzeugendensystem. Dann gibt es ein $x \in V \backslash \text{span}_K(x_i)$. Definiere $J = I \cup \{j_0\}$ mit $j_0 \notin I$ und $x_{j_0} := x$. Aufgrund der Maximalität von B ist (x_i) linear abhängig, es gibt als Skalare λ, (λ_i), nicht alle gleich 0, mit $\lambda \cdot x + \sum_{i \in I} \lambda_i \cdot x_i = 0$. Da (x_i) linear abhängig ist, muss $\lambda \neq 0$ sein, woraus der Widerspruch $x = \lambda^{-1} \cdot \sum_{i \in I} \lambda_i \cdot x_i \in \text{span}_K(x_i)$.

Somit ist B ein Erzeugendensystem. □

Theorem 3.6 (Basisauswahlsatz)
Jedes endliche Erzeugendensystem von V besitzt eine Basis als Teilfamilie: Ist (x_i) ein endliches Erzeugendensystem von V, so gibt es eine Teilmenge $J \subseteq I$, für die $(x_i)_{i\in J}$ eine Basis von V ist.

Beweis. Sei (x_i) ein endliches Erzeugendensystem von V. Definiere $\mathcal{J} := \{J \subseteq I \mid (x_i)_{i\in J} \text{ J ist Erzeugendensystem von } V\}$. Da I endlich ist, ist auch $\mathcal{J}$ endlich. Da (x_i) Erzeugendensystem ist, ist $I \in J$, insbesondere $\mathcal{J} \neq \emptyset$. Es gibt deshalb ein bezüglich Inklusion minimales $J_0 \in \mathcal{J}$, d.h. $J_1 \in \mathcal{J}$ so gilt nicht $J_1 \subsetneq J_0$. Deshalb ist $(x_i)_{i\in J_0}$ eine Basis von V (Satz 3.5). □

Folgerung 3.7
Jeder endlich erzeugte K-Vektorraum besitzt eine endliche Basis.

▶ **Bemerkung 3.8**
Der Beweis von Theorem 3.6 liefert ein konstruktives Verfahren: Ist $(x_1, ..., x_n)$ ein endliches Erzeugendensystem von V, so prüfe man, ob es ein i_0 mit $x_{i_0} \in \text{span}_K((x_i)_{i\neq i_0})$ gibt. Falls Nein, ist $(x_1, ..., x_n)$ eine Basis von V. Falls Ja, macht man mit $(x_1, ..., x_{i_{0-1}}, x_{i_{0+1}}, ..., x_n)$ weiter.

▶ **Bemerkung 3.9**
Man kann jedoch zeigen, dass jeder Vektorraum eine Basis besitzt. Die Gültigkeit der Aussage hängt jedoch von bestimmten mengentheoretischen Axiomen ab, auf die wir an dieser Stelle nicht eingehen werden. Siehe dazu LAAG 2. Semester.

Lemma 3.10 (Austauschlemma)
Sei $B = (x_1, ..., x_n)$ eine Basis von V. Sind $\lambda_1, ..., \lambda_n \in K$ und $y = \sum_{i=1}^n \lambda_i \cdot x_i$, so ist für jedes $j \in \{1, 2, ..., n\}$ mit $\lambda_j \neq 0$ auch $B' = (x_1, ..., x_{j-1}, y, x_{j+1}, ..., x_n)$ eine Basis von V.

Beweis. oBdA. sei $j = 1$, also $B' = (y, x_2, ..., x_n)$. Wegen $\lambda_1 \neq 0$ ist $x_1 = \lambda_1^{-1} \cdot y - \sum_{i=2}^n \lambda_i \cdot x_i \in \text{span}_K(y, x_2, ..., x_n)$ und somit ist B' ein Erzeugendensystem. Sind $\mu_1, ..., \mu_n \in K$ mit $\mu_1 \cdot y - \sum_{i=2}^n \mu_i \cdot x_i = 0$, so folgt $0 = \mu_1(\sum_{i=1}^n \lambda_i \cdot x_i + \sum_{i=2}^n \mu_i \cdot x_i) = \mu_1 \cdot \lambda_1 \cdot x_1 + \sum_{i=2}^n (\mu_1 \cdot \lambda_i + \mu_i)x_i$ und aus der linearen Unabhängigkeit von B somit $\mu_1 \cdot \lambda_1 = 0$, $\mu_1 \cdot \lambda_2 + \mu_2 = 0$, ..., $\mu_1 \cdot \lambda_n + \mu_n = 0$. Wegen $\lambda_1 \neq 0$ folgt $\mu_1 = 0$ und daraus $\mu_i = 0$. Folglich ist B' linear unabhängig. □

Theorem 3.11 (Steinitz'scher Austauschsatz)
Sei $B = (x_1, ..., x_n)$ eine Basis von V und $\mathcal{F} = (y_1, ..., y_r)$ eine linear unabhängige Familie in V. Dann ist $r \leq n$ und es gibt $i_1, ..., i_{n-r} \in \{1, ..., n\}$, für die $B' = (y_1, ..., y_r, x_{i_1}, ..., x_{i_{n-r}})$ eine Basis von V ist.

Beweis. Induktion nach r
Für $r = 0$ ist nichts zu zeigen.
Sei nun $r \geq 1$ und gelte die Aussage für $(y_1, ..., y_{r-1})$. Insbesondere ist $r - 1 \leq n$ und es gibt $i_1, .., i_{n-(r-1)} \in \{1, ..., n\}$ für die $B' = (y_1, ..., y_r, x_{i_1}, ..., x_{i_{n-(r-1)}})$ eine Basis von V ist. Da $y_r \in V = \text{span}_K(B')$ ist $y_r = \sum_{i=1}^{r-1} \lambda_i \cdot y_1 + \sum_{j=0}^{n-(r-1)} \mu_j \cdot x_{i_j}$. Da $(y_1, ..., y_r)$ linear unabhängig, ist $y_r \notin \text{span}_K(y_1, ..., y_{r-1})$. Folglich gibt es $j_0 \in \{1, ..., n - (r-1)\}$ mit $\mu_{j_0} \neq 0$. Insbesondere ist $n - (r-1) \geq 1$, also $r \leq n$. oBdA. $j_0 = 1$, dann ergibt sich

mit dem Austauschlemma (Lemma 3.10), dass auch $(y_1, ..., y_{r-1}, y_r, x_{i_2}, ..., x_{i_{n-(r-1)}})$ eine Basis von V ist. □

Folgerung 3.12 (Basisergänzungssatz)
Ist V endlich erzeugt, so lässt sich jede linear unabhängige Familie zu einer Basis ergänzen: Ist $(x_1, ..., x_n)$ linear unabhängig, so gibt es $m \geq n$ und $x_{n+1}, x_{n+2}, ..., x_m$ für die $(x_1, ..., x_n, x_{n+1}, ..., x_m)$ eine Basis von V ist.

Beweis. Nach dem Basisauswahlsatz (Theorem 3.6 und Folgerung 3.7) besitzt V eine endliche Basis, die Behauptung folgt somit aus dem Steinitz'schen Austauschsatz (Theorem 3.11). □

Folgerung 3.13
Sind (x_i) und (x_j) Basen von V und ist I endlich, so ist $|I| = |J|$.

Beweis. Da (y_r) linear unabhängig ist, ist $|J| \leq |I|$ nach dem Steinitz'schen Austauschsatz (Theorem 3.11). Insbesondere ist J endlich, also $|I| \leq |J|$ nach dem Austauschsatz (Theorem 3.11). □

Folgerung 3.14
Ist V endlich erzeugt, so haben alle Basen von V die gleiche Mächtigkeit.

Beweis. V besitzt eine endliche Basis (Folgerung 3.7), deshalb folgt die Behauptung aus Folgerung 3.13. □

Definition 3.15 (Dimension)
Ist V endlich erzeugt, so ist die Dimension des Vektorraum V die Mächtigkeit $\dim_K(V)$ einer Basis von V. Andernfalls sagt man, dass V unendliche Dimensionen hat und schreibt $\dim_K(V) = \infty$.

■ **Beispiel 3.16**

- $\dim_K(K^n) = n$
- $\dim_K(K[X]) = \infty$
- $\dim_K(K[X]_{\leq n}) = n + 1$
- $\dim_{\mathbb{R}}(\mathbb{C}) = 2$
- $\dim_{\mathbb{C}}(\mathbb{C}) = 1$

▶ **Bemerkung 3.17**

- V ist genau dann endlich erzeugt, wenn $\dim_K(V) < \infty$.
- Mit Satz 3.5 $\dim_K(V) = \min\{|B| \mid \text{span}_K(B) = V\} = \max\{|B| \mid B \text{ linear unabhängig}\}$

Satz 3.18
Sei V endlich erzeugt und $W \leq V$ ein Untervektorraum.

- Es ist $\dim_K(W) \leq \dim_K(V)$. Insbesondere ist W endlich erzeugt.
- Ist $\dim_K(W) = \dim_K(V)$, so ist auch $W = V$.

Beweis.

- Ist F eine linear unabhängige Familie in W, so ist auch F linear unabhängig in V und somit $|F| \leq \dim_K(V)$. Insbesondere gibt es eine maximal linear unabhängige Familie B in W und es folgt $\dim_K(W) = |B| \leq \dim_K(V)$.
- Sei B eine Basis von W. Dann ist B auch in V linear unabhängig. Ist $\dim_K(W) = \dim_K(V)$, so muss auch B in V maximal linear unabhängig sein. Insbesondere ist $W = \text{span}_K(B) = V$. □

4. Summen von Vektorräumen

Sei V ein K-Vektorraum und (W_i) eine Familie von Untervektorräumen von V.

Definition 4.1 (Summe von Vektorräumen)
Die Summe der W_i ist der Untervektorraum

$$\sum_{i\in I} W_i := \operatorname{span}_K\left(\bigcup W_i\right)$$

Im Fall $I = \{1, ..., n\}$ schreibt man auch $W_1 + ... + W_n$ für $\sum_{i=1}^{n} W_i$.

Lemma 4.2
Es ist $\sum_{i\in I} W_i = \{\sum_{i\in I} x_i \mid x_i \in W_i$, fast alle gleich $0\}$.

Beweis.
- " $\supseteq$ ": klar, $\sum x_i \in \operatorname{span}_K(\bigcup W_i)$
- " $\subseteq$ ": Die rechte Seite enthält jedes W_i und ist ein Untervektorraum von V:
  Für $x_i, x_i' \in W$, fast alle gleich 0 und $\lambda \in K$ ist $\sum x_i + \sum x_i' = \sum(x_i + x_i')$, $\lambda \cdot \sum x_i = \sum \lambda \cdot x_i \Rightarrow$ Untervektorraum □

Beispiel 4.3
Ist $(x_i)_{i\in I}$ eine Familie von Elementen von V, so ist

$$\operatorname{span}_K((x_i)_{i\in I}) = \sum_{i\in I} Kx_i$$

wobei Kx_i der Untervektorraum aus Beispiel 1.9 und Beispiel 2.6 ist.

Satz 4.4
Es sind äquivalent:

- Jedes $x \in \sum_{i\in I} W_i$ ist eindeutig als $\sum_{i\in I} x_i$ mit $x_i \in W_i$ darstellbar.
- Für jedes $i \in I$ ist $W_i \cap \sum_{j\neq i} W_j = \{0\}$.

Beweis.
- $1 \Rightarrow 2$: Sei $x \in W_i \cap \sum_{i\neq j} W_j$. Dann ist $x = \sum_j x_j$ mit $x_j \in W_j$ und $x_i = 0$. Die Eindeutigkeit der Darstellung impliziert also, dass $x = 0$.
- $2 \Rightarrow 1$: Sei $x = \sum_{j\in I} x_j = \sum_{j\in I} x_j'$ mit $x_j, x_j' \in W_j$ für alle j. Dann ist $0 = \sum_{j\in I}(x_j - x_j')$, also

$$x_i - x_i' = -\sum_{j\neq i}(x_j - x_j') \in W_i \cap \sum_{j\neg i} W_j = \{0\}$$ □

Definition 4.5 (direkte Summe)
Ist jedes $x \in \sum W_i$ eindeutig als Summe von x_i mit $x_i \in W_i$ darstellbar, so sagt man, dass $\sum W_i$ die direkte Summe der Untervektorräume W_i ist und schreibt $\oplus W_i$ für $\sum W_i$. Im Fall $I = \{1, ..., n\}$ schreibt man auch $W_1 \oplus W_2 \oplus ... \oplus W_n$ für $\oplus W_i$.

■ **Beispiel 4.6**
Ist $(x_1, ..., x_n)$ eine Basis von V, so ist $V = Kx_1 \oplus ... \oplus Kx_n$.

▶ **Bemerkung 4.7**
Wir wollen uns näher mit dem wichtigen Spezialfall $I = \{1, 2\}$ beschäftigen und schreiben noch mal auf:

Folgerung 4.8
Seien W_1, W_2 Untervektorräume von V. Es sind äquivalent:

- $V = W_1 \oplus W_2$
- $V = W_1 + W_2$ und $W_1 \cap W_2 = \{0\}$

Satz 4.9
Sind W_1, W_2 Untervektorräume von V mit Basen $(x_i)_{i\in I_1}$ bzw. $(x_i)_{i\in I_2}$, wobei $I_1 \cap I_2 = \emptyset$, so sind äquivalent:

- $V = W_1 \oplus W_2$
- $(x_i)_{i\in I_1\cap I_2}$ ist eine Basis von V

Beweis. Sei $I = I_1 \cup I_2$.

- $1 \Rightarrow 2$: Da $\text{span}_K((x_i)_{i\in I_1}) = W_1$ und $\text{span}_K((x_i)_{i\in I_2}) = W_2$ ist $\text{span}_K((x_i)_{i\in I}) = W_1 + W_2 = V$. Ist $\sum \lambda_i x_i = 0$, so ist $\sum_{i\in I_1} \lambda_i x_i = -\sum_{i\in I_2} \lambda_i x_i \in W_1 \cap W_2 = \{0\}$. Da $(x_i)_{i\in I_1}$ linear unabhängig ist, ist $\lambda_i = 0$, analog für $i \in I_2$.
- $2 \Rightarrow 1$: $W_1 + W_2 = \text{span}_K((x_i)_{i\in I_1}) + \text{span}_K((x_i)_{i\in I_2}) = \text{span}_K((x_i)_{i\in I}) = V$. Ist $x \in W_1 \cap W_2$, so ist $x = \sum_{i\in I_1} \lambda_i x_i = \sum_{i\in I_2} \lambda_i x_i$. Somit $0 = \sum_{i\in I_1} \lambda_i x_i - \sum_{i\in I_2} \lambda_i x_i$, woraus wegen $(x_i)_{i\in I}$ linear unabhängig schon $\lambda_i = 0$ folgt. Somit ist $x = 0$. □

Folgerung 4.10
Ist $\dim_K(V) < \infty$, so ist jeder Untervektorraum ein direkter Summand: Ist W ein Untervektorraum von V, so gibt es einen Untervektorraum W' von V mit $V = W \oplus W'$ (W' heißt das lineare Komplement von W in V). Es ist

$$\dim_K(W') = \dim_K(V) - \dim_K(W)$$

Beweis. Sei $(x_1, ..., x_m)$ eine Basis von W. Nach dem Basisergänzungssatz (Folgerung 3.13) lässt sich diese zu einer Basis $(x_1, ..., x_n)$ von V ergänzen. Mit $W' := \text{span}_K(x_{m+1}, ..., x_n)$ ist dann $V = W \oplus W'$. □

▶ **Bemerkung 4.11**
Ist $\dim_K(V) < \infty$, so folgt aus $W_1 \cap W_2 = \{0\}$ also insbesondere $\dim_K(W_1 + W_2) = \dim_K(W_1) + \dim_K(W_2)$.

Theorem 4.12 (Dimensionsformel)
Sei $\dim_K(V) < \infty$. Für Untervektorräume W_1, W_2 von V gilt:

$$\dim_K(W_1 + W_2) + \dim_K(W_1 \cap W_2) = \dim_K(W_1) + \dim_K(W_2)$$

Beweis. Da $\dim_K(V) < \infty$ haben alle Untervektorräume von V Basen. Sei also $B_0 = (X_1, ..., x_n)$ eine Basis von $W_1 \cap W_2$. Nach dem Basisergänzungssatz (Folgerung 3.13) können wir B_0 zu den Basen $B_1 = (x_1, ..., x_n, y_1, ..., y_p)$ von W_1 und $B_2 = (x_1, ..., x_n, z_1, ..., z_q)$ von W_2 ergänzen. Wir behaupten, dass $B = (x_1, ..., x_n, y_1, ..., y_p, z_1, ..., z_q)$ eine Basis von $W_1 + W_2$ ist. Offenbar ist B ein Erzeugendensystem von $W_1 + W_2$. Seien nun $\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_p, \eta_1, ..., \eta_q \in K$ mit $\sum_{i=1}^n \lambda_i x_i + \sum_{j=1}^p \mu_j y_j + \sum_{k=1}^q \eta_k z_k = 0$. Dann ist $\sum_{i=1}^n \lambda_i x_i + \sum_{j=1}^p \mu_j y_j = -\sum_{k=1}^q \eta_k z_k \in W_1 \cap W_2$. Da $\operatorname{span}_K(B_0) = W_1 \cap W_2$ und B_1 linear unabhängig ist, ist $\mu_j = 0$. Analog zeigt man auch, dass $\eta_k = 0$. Aus B_0 linear unabhängig folgt dann auch, dass $\lambda_i = 0$. Somit ist B linear unabhängig. Wir haben gezeigt, dass B eine Basis von $W_1 + W_2$ ist.
$\Rightarrow \dim_K(W_1) + \dim_K(W_2) = |B_1| + |B_2| = (n+p) + (n-q) = (n+p+q) + n = |B| + |B_0| = \dim_K(W_1 + W_2) + \dim_K(W_1 \cap W_2)$. □

Definition 4.13 (externes Produkt)
Das externe Produkt einer Familie (V_i) von K-Vektorräumen ist der K-Vektorraum $\prod V_i$ bestehend aus dem kartesischen Produkt der V_i mit komponentenweiser Addition und Skalarmultiplikation, $(x_i) + (x_i') := (x_i + x_i')$ und $\lambda(x_i) := (\lambda x_i)$.

Definition 4.14 (externe Summe)
Die externe Summe einer Familie (V_i) von K-Vektorräumen ist der Untervektorraum $\oplus V_i := \{(x_i) \in \prod V_i \mid x_i = 0; \text{ für fast alle } i\}$ des K-Vektorraum $\prod V_i$.

▶ **Bemerkung 4.15**
Man prüft sofort nach, dass $\prod V_i$ ein K-Vektorraum ist und $\oplus V_i$ ein Untervektorraum davon ist. Für endliche Indexmengen ist $\prod V_i = \oplus V_i$, z.B. $K^n = \prod_{i=1}^n K = \oplus K$.

Eine erste Beziehung zwischen externer direkter Summe und direkter Summe im Sinne von Definition 4.5 gibt das folgende Lemma. Im nächsten Kapitel werden wir den Zusammenhang dann vollständig verstehen.

Lemma 4.16
Sei (V_i) eine Familie von K-Vektorräumen und sei $V = \oplus V_i$. Für jedes $j \in I$ ist $\tilde{V}_j := V \times \prod_{i \in I \setminus \{j\}} \{0\}$ ein Untervektorraum von V und $V = \oplus \tilde{V}_j$

Beweis. Ist $x = (x_i) \in V$ mit $x_i \in V_i$, fast alle $x_i = 0$, so ist $x = \sum \tilde{x}_i$ mit $\tilde{x} := (x_i \delta_{ij}) \in \tilde{V}_j$. Somit ist $V = \sum \tilde{V}_i$. Die Gleichung $\tilde{V}_i \cap \sum_{j \neq i} \tilde{V}_j = \{0\}$ folgt aus Definition der $\tilde{V}_i$. □

Kapitel III

Lineare Abbildungen

1. Matrizen

Sei K ein Körper.

Definition 1.1 (Matrix)
Seien $m, n \in \mathbb{N}_0$. Eine $m \times n$-Matrix über K ist ein rechteckiges Schema:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Man schreibt dies auch als $A = (a_{ij})_{i=1,\dots,n\ j=1,\dots,m}$ oder $A = (a_{ij})_{i,j}$, wenn m und n aus dem Kontext hervorgehen. Die a_{ij} heißen die Koeffizienten der Matrix A und wir definieren $A_{i,j} = a_{ij}$. Die Menge der $m \times n$-Matrizen über K wird mit $\mathrm{Mat}_{m\times n}(K)$ oder $K^{m\times n}$ bezeichnet. Man nennt das Paar (m, n) auch den Typ von A. Ist $m = n$, so spricht man von quadratischen Matrizen und schreibt $\mathrm{Mat}_n(K)$. Zu einer Matrix $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$ definiert man die zu A transponierte Matrix $A^t := (a_{ij})_{j,i} \in \mathrm{Mat}_{n\times m}(K)$.

Mathematica/WolframAlpha-Befehle (Matrizen)
Matrizen werden in Mathematica bzw. WolframAlpha folgendermaßen dargestellt:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

$$\Rightarrow \Big\{\{1,2,3\},\{4,5,6\},\{7,8,9\}\Big\}$$

Wenn Mathematica als Ergebnis eine Matrix ausgibt, so lässt sich diese als Zeile schlecht lesen. Mit dem Suffix `//MatrixForm` lässt sich der Output als Matrix formatieren:

```
{{1,2,3},{4,5,6},{7,8,9}}*3 //MatrixForm
```

$$\Rightarrow \begin{pmatrix} 3 & 6 & 9 \\ 12 & 15 & 18 \\ 21 & 24 & 27 \end{pmatrix}$$

■ **Beispiel 1.2**

- Die Nullmatrix ist $0 = (0)_{i,j} \in \mathrm{Mat}_{m\times n}(K)$.
- Für $k, l \in \{1, ..., n\}$ ist die (k, l)-Basismatrix gegeben durch $E_{kl} = (\delta_{jk}\delta_{jl}) \in \mathrm{Mat}_{m\times n}(K)$.
- Die Einheitsmatrix ist $\mathbb{1}_n = (\delta_{ii}) \in \mathrm{Mat}_n(K)$.
- Für $a_i, ..., a_n \in K$ definiert man eine Diagonalmatrix $\mathrm{diag}(a_1, ..., a_n) = (\delta_{ij} \cdot a_i)$.
- Für eine Permutation $\sigma \in S_n$ definiert man die Permutationsmatrix $P_\sigma := (\delta_{\sigma(i),j})$.
- Für $a_1, ..., a_n$ definiert man einen Zeilenvektor $(a_1, ..., a_n) \in \mathrm{Mat}_{1\times n}(K)$ bzw. einen Spaltenvektor $(a_1, ..., a_n)^t$.

Definition 1.3 (Addition und Skalarmultiplikation)
Seien $A = (a_{ij})$ und $B = (b_{ij})$ desselben Typs und $\lambda \in K$. Man definiert auf $\mathrm{Mat}_{m\times n}(K)$ eine koeffizientenweise Addition und Skalarmultiplikation .

Mathematica/WolframAlpha-Befehle (Matrizenoperationen)
Die komponentenweise Addition bzw. Skalarmultiplikation von Matrizen A und B lässt sich in Mathematica bzw. WolframAlpha folgendermaßen realisieren:

```
A+B
A*B
```

Satz 1.4
$(\mathrm{Mat}_{m\times n}, +, \cdot)$ ist ein K-Vektorraum der Dimension $\dim_K(\mathrm{Mat}_{m\times n}) = n \cdot m$ mit Basismatrix als Basis.

Beweis. Dies ist klar, weil wir $\mathrm{Mat}_{m\times n}$ mit dem Standardraum K^{mn} identifizieren können. Wir haben die Elemente nur als $m \times n$-Matrix statt als mn-Tupel geschrieben. □

Definition 1.5 (Matrizenmultiplikation)
Seien $m, n, r \in \mathbb{N}_0$. Sind $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$, $B = (b_{jk}) \in \mathrm{Mat}_{n\times r}(K)$ so definieren wir die Matrizenmultiplikation $C = AB$ als die Matrix $C = (c_{ik}) \in \mathrm{Mat}_{m\times r}(K)$ mit $c_{ik} = \sum_{j=1}^{n} a_{ij} \cdot b_{jk}$. Kurz geschrieben "Zeile · Spalte".

Mathematica/WolframAlpha-Befehle (Matrizenmultiplikation)
Die Matrizenmultiplikation in Mathematica und WolframAlpha für Matrizen A und B geht so:

`A.B` oder `Dot[A,B]`

■ **Beispiel 1.6**

- Für $A \in \mathrm{Mat}_n(K)$ ist $0 \cdot A = 0$ und $1 \cdot A = A$.
- Für $\sigma \in S_n$ und $A \in \mathrm{Mat}_{n\times r}(K)$ geht $P_\sigma \cdot A$ aus A durch Permutation der Zeilen hervor.

Lemma 1.7
Für $m, n, r \in \mathbb{N}_0$ und $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$, $B = (b_{jk}) \in \mathrm{Mat}_{n\times r}(K)$ und $\lambda \in K$ gilt:

$$A(\lambda B) = (\lambda A)B = \lambda(AB)$$

Beweis. Schreibe $A = (a_{ij})$, $B = (b_{jk})$. Dann ist $A(\lambda B) = \sum_{j=1}^{n} a_{ij} \cdot \lambda b_{jk} = \sum_{j=1}^{n} \lambda a_{ij} \cdot b_{jk} = (\lambda A)B = \lambda \cdot \sum_{j=1}^{n} a_{ij} b_{jk} = \lambda(AB)$. □

Lemma 1.8
Matrizenmultiplikation ist assoziativ:

$$A(BC) = (AB)C$$

Beweis. Sei $D = BC \in \mathrm{Mat}_{n\times s}(K)$, $E = AB \in \mathrm{Mat}_{m\times r}(K)$. Schreibe $A = (a_{ij})$ usw. Für i, l ist $(AD) = \sum_{j=1}^{n} a_{ij} d_{jl} = \sum_{j=1}^{n} a_{ij} \cdot \sum_{k=1}^{r} b_{jk} c_{kl} = \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} b_{jk} c_{kl}$.
$(EC) = \sum_{k=1}^{n} e_{ik} c_{kl} = \sum_{k=1}^{r} \sum_{j=1}^{n} a_{ij} b_{jk} c_{kl}$. Also ist $AD = EC$. □

Lemma 1.9
Für $m, n, r \in \mathbb{N}_0$ und $A, A' \in \mathrm{Mat}_{m\times n}(K)$, $B, B' \in \mathrm{Mat}_{n\times r}(K)$ ist

$$(A + A')B = AB + A'B$$
$$A(B' + B) = AB' + AB$$

Beweis. Schreibe $A = (a_{ij})$ etc. Dann ist $(A + A')B = \sum_{j=1}^{n} (a_{ij} + a'ij) b_{jk} = \sum_{j=1}^{n} a_{ij} + b_{jk} + \sum_{j=1}^{n} a'_{ij} + b_{jk} = (AB + A'B)$. Rest analog. □

Satz 1.10
Mit der Matrizenmultiplikation wird $\mathrm{Mat}_n(K)$ zu einem Ring mit Einselement 1.

Beweis. Nach Satz 1.4, Lemma 1.8 und Lemma 1.9 ist $\mathrm{Mat}_n(K)$ ein Ring und dass $\mathbb{1}_n$ ein neutrales Element ist, haben wir schon in Beispiel 1.6 gesehen □

■ **Beispiel 1.11**

- Für $n = 1$ können wir dem Ring $\mathrm{Mat}_n(K)$ mit K identifizieren, der Ring ist also ein Körper, insbesondere ist er kommutativ.
- Für $n \geq 2$ ist $\mathrm{Mat}_n(K)$ nicht kommutativ.

Definition 1.12 (invertierbar)
Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt invertierbar oder regulär , wenn sie im Ring $\mathrm{Mat}_n(K)$ invertierbar ist, sonst singulär . Die Gruppe $\mathrm{GL}_n(K) = \mathrm{Mat}_n(K)^\times$ der invertierbaren $n \times n$ -Matrizen heißt allgemeine Gruppe .

Mathematica/WolframAlpha-Befehle (Matizen invertieren)
Das Inverse einer Matrix A in Mathematica bzw. WolframAlpha lässt sich mit der Funktion

```
Inverse[A]
```

berechnen.

■ **Beispiel 1.13**
Sei $n = 2$. Zu

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(K)$$

definiert man

$$\tilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathrm{Mat}_2(K)$$

Man prüft nach, dass $A \cdot \tilde{A} = \tilde{A} \cdot A = (ad - bc) \cdot \mathbb{1}_2$. Definiert man nun $\det(A) = ad - bc$ so sieht man: Ist $\det(A) \neq 0$, so ist A invertierbar mit $A^{-1} = \det(A)^{-1} \cdot \tilde{A}$. Ist $\det(A) = 0$ so A ist Nullteiler und somit nicht invertierbar (Satz 4.13). Mehr dazu in Kapitel IV.

Lemma 1.14
Für $A, A_1, A_2 \in \mathrm{Mat}_{m\times n}(K)$ und $B = \mathrm{Mat}_{n\times r}(K)$ ist

- $(A^t)^t = A$
- $(A_1 + A_2)^t = A_1^t + A_2^t$
- $(AB)^t = B^t A^t$

Beweis. Übung □

Satz 1.15
Für $A \in \mathrm{GL}_n(K)$ ist $A^t \in \mathrm{GL}_n(K)$ und $(A^{-1})^t = (A^t)^{-1}$

Beweis. Aus $AA^{-1} = 1$ folgt nach Lemma 1.14, dass $(A^{-1})^t A^t = \mathbb{1}_n^t = \mathbb{1}_n$. Somit ist $(A^{-1})^t$ das Inverse zu A^t. □

2. Homomorphismen von Gruppen

Seien G, H zwei multiplikativ geschriebene Gruppen.

Definition 2.1 (Gruppenhomomorphismus)
Eine Abbildung $f : G \to H$ ist ein Gruppenhomomorphismus , wenn gilt:

- (GH): $f(xy) = f(x) \cdot f(y)$

Die Menge der Homomorphismen $f : G \to H$ bezeichnet man mit $\mathrm{Hom}(G, H)$.

▶ **Bemerkung 2.2**
Ein Gruppenhomomorphismus ist also eine Abbildung, welche mit der Verknüpfung, also der Struktur der Gruppe, verträglich ist. Man beachte: für additiv geschrieben Gruppen lautet die Bedingung: $f(x + y) = f(x) + f(y)$.

■ **Beispiel 2.3**

- $\mathrm{id}_G : G \to G$
- $c_1 : G \to H$ mit $x \mapsto 1_H$
- $G_0 \leq G$ Untergruppe, $\iota : G_0 \to G$
- $(A, +)$ abelsche Gruppe, $k \in \mathbb{Z}$, $A \to A$ mit $a \mapsto ka$
- $\mathbb{Z} \to \mathbb{Z}\backslash n\mathbb{Z}$ mit $\overline{a} \mapsto a + n\mathbb{Z}$
- $\mathbb{R} \to \mathbb{R}^\times$ mit $x \mapsto e^x$
- $\mathrm{Mat}_n(K) \to \mathrm{Mat}_n(K)$ mit $A \mapsto A^t$
- $\mathbb{C} \to \mathbb{R}^\times$ mit $z \mapsto |z|$

Satz 2.4
Sei $f \in \mathrm{Hom}(G, H)$. Dann gilt:

- $f(1_G) \to 1_H$
- Für $x \in G$ ist $f(x^{-1}) = (f(x))^{-1}$.
- Für $x_1, ..., x_n \in G$ ist $f(x_1, ..., x_n) = f(x_1) \cdot ... \cdot f(x_n)$.
- Ist $G_0 \leq G$, so ist $f(G_0) \leq H$.
- Ist $H_0 \leq H$, so ist $f^{-1}(H_0) \leq G$.

Beweis.

- $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \Rightarrow$ kürzen, weil H Gruppe $\Rightarrow 1 = f(1)$
- $f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1) = 1$
- Induktion nach n
- $x, y \in G_0 \Rightarrow f(x) \cdot f(y) = f(xy) \in f(G_0)$, $f^{-1}(x) = f(x^{-1}) \in f(G_0)$
- $x, y \in f^{-1}(H_0) \Rightarrow f(x) \cdot f(y) = f(xy) \in H_0 \Rightarrow xy \in f^{-1}(H_0)$, $f(x^{-1}) = (f(x))^{-1} \in H_0 \Rightarrow x^{-1} \in f^{-1}(H_0)$, $f(1) = 1 \in H_0 \Rightarrow 1 \in f^{-1}(H_0)$, insbesondere $f^{-1}(H_0) \neq \emptyset$ □

Satz 2.5
Seien G_1, G_2, G_3 Gruppen. Sind $f_1 : G_1 \to G_2$, $f_2 : G_2 \to G_3$ Homomorphismen, so ist auch $f_2 \circ f_1 : G_1 \to G_3$.

Beweis. Für $x, y \in G_1$ ist $(f_2 \circ f_1)(xy) = f_2(f_1(xy)) = f_2(f_1(x) \cdot f_1(y)) = f_2(f_1(x)) \cdot f_2(f_1(y)) = (f_2 \circ f_1)(x) \cdot (f_2 \circ f_1)(y)$ □

Definition 2.6 (Arten von Homomorphismen)
Ein Homomorphismus ist

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

Die Gruppen G und H heißen isomorph , in Zeichen $G \cong H$, wenn es einen Isomorphismus $G \to H$ gibt.

Lemma 2.7
Ist $f : G \to H$ ein Isomorphismus, so ist auch $f^{-1} : H \to G$ ein Isomorphismus.

Beweis. Da f^{-1} wieder bijektiv ist, müssen wir nur zeigen, dass f^{-1} ein Homomorphismus ist. Seien $x, y \in H$. Dann ist $f(f^{-1}(x) \cdot f^{-1}(y)) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = xy$, somit $f^{-1}(xy) = f^{-1}(x) \cdot f^{-1}(y)$. □

Satz 2.8
Sei $f : G \to H$ ein Homomorphismus. Genau dann ist f ein Isomorphismus, wenn es einen Homomorphismus $f' : H \to G$ mit $f' \circ f = \mathrm{id}_G$ und $f \circ f' = \mathrm{id}_H$ gibt.

Beweis. Ist f ein Isomorphismus, so erfüllt $f' := f^{-1}$ nach Lemma 2.7 das Gewünschte. Ist umgekehrt f' wie angegeben, so muss f bijektiv sein:

- $f' \circ f = \mathrm{id}_G$ injektiv $\Rightarrow f$ injektiv
- $f \circ f' = \mathrm{id}_H$ surjektiv $\Rightarrow f$ surjektiv □

Folgerung 2.9
Isomorphie von Gruppen ist eine Äquivalenzrelation : Sind G, G_1, G_2, G_3 Gruppen, so gilt:

- $G \cong G$ (Reflexivität)
- Ist $G_1 \cong G_2$, so ist auch $G_2 \cong G_1$ (Symmetrie)
- Ist $G_1 \cong G_2$ und $G_2 \cong G_3$, dann ist auch $G_1 \cong G_3$ (Transitivität)

Beweis.
- id_G ist ein Isomorphismus
- Lemma 2.7
- Folgt aus Satz 2.5 und der Tatsache, dass die Komposition bijektiver Abbildungen wieder bijektiv ist. □

▶ **Bemerkung 2.10**
Satz 2.8 erklärt die Bedeutung des Isomorphismus: Eine mit der Struktur verträgliche Abbildung,

die eine mit der Struktur verträgliche Umkehrabbildung besitzt, also eine strukturerhaltende Abbildung. Tatsächlich können wir uns einen Isomorphismus $f : G \to H$ so vorstellen, dass wir nur die Elemente von G umbenennen. Alle Aussagen, die sich nur aus der Struktur selbst ergeben, bleiben damit wahr. Zum Beispiel: Ist $G \cong H$ und ist G abelsch, so auch H und umgekehrt.

■ **Beispiel 2.11**

- Es ist $\mathbb{Z}^\times = \mu_2 \cong \mathbb{Z}\backslash 2\mathbb{Z} \cong (\mathbb{Z}\backslash 3\mathbb{Z})^\times \cong S_2$. Je zwei beliebige Gruppen der Ordnung 2 sind zueinander isomorph.
- $e : \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$ liefert einen Isomorphismus, da $(\mathbb{R}, +) \to (\mathbb{R}, \cdot)$.

Definition 2.12 (Kern)
Der Kern eines Gruppenhomomorphismus $f : G \to H$ ist $\mathrm{Ker}(f) := f^{-1}(\{1\}) = \{x \in G \mid f(x) = 1_H\}$.

Lemma 2.13
Ist $f : G \to H$ ein Homomorphismus, so ist $N := \mathrm{Ker}(f)$ eine Untergruppe von G mit $x \cdot y \cdot x^{-1} \in N$ für alle $x \in G$ und $y \in N$.

Beweis. Nach Satz 2.4 ist N eine Untergruppe. Für $x \in G$ und $y \in N$ ist $f(xyx^{-1}) = f(x) \cdot f(y) \cdot f(x^{-1}) = f(x) \cdot f(x^{-1}) \cdot 1 = f(x) \cdot f(x^{-1}) = 1$, also $xyx^{-1} \in N$. □

Satz 2.14
Sei $f \in \mathrm{Hom}(G, H)$. Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = \{1_G\}$.

Beweis. Schreibe $N = \mathrm{Ker}(f)$.

- Hinrichtung: Ist f injektiv, so ist $N \leq G$ mit $|N| \leq 1$, also $N = \{1_G\}$.
- Rückrichtung: Sei $N = \{1_G\}$. Sind $x, y \in G$ mir $f(x) = f(y)$, so ist $1 = (f(x))^{-1} \cdot f(y) = f(x^{-1} \cdot y)$, also $x^{-1} \cdot y \in N = \{1\}$ und somit $x = y$. Folglich ist f injektiv. □

Definition 2.15 (Normalteiler)
Ist $N \leq G$ mit $x^{-1}yx \in N$ für alle $x \in G$ und $y \in N$, so nennt man N einen Normalteiler von G und schreibt $N \trianglelefteq G$.

3. Homomorphismen von Ringen

Seien R, S und T Ringe.

Definition 3.1 (Ringhomomorphismus)
Eine Abbildung $f : R \to S$ ist ein Ringhomomorphismus , wenn für $x, y \in R$ gilt:

- (RH1:) $f(x + y) = f(x) + f(y)$
- (RH2:) $f(xy) = f(x) \cdot f(y)$

Die Menge der Ringhomomorphismen $f : R \to R$ wird mit $\mathrm{Hom}(R, S)$ bezeichnet. Ein Homomorphismus $f : R \to S$ ist ein Mono-, Epi- oder Isomorphismus, wenn f injektiv, surjektiv oder bijektiv ist. Gibt es einen Isomorphismus $f : R \to S$, so nennt man R und S isomorph und schreibt $R \cong S$. Die Elemente von $\mathrm{End}(R) := \mathrm{Hom}(R, R)$ nennt man Endomorphismen . Der Kern eines Ringhomomorphismus $f : R \to S$ ist $\mathrm{Ker}(f) := f^{-1}(\{0\})$.

▶ **Bemerkung 3.2**
Ein Ringhomomorphismus $f : R \to S$ ist ein Gruppenhomomorphismus der abelschen Gruppen $(R, +)$ und $(S, +)$, der mit der Multiplikation verträglich ist, also eine strukturverträgliche Abbildung zwischen Ringen.

■ **Beispiel 3.3**

- $\mathrm{id}_R : R \to R$ ist ein Ringisomorphismus
- Ist $R_0 \leq R$ ein Unterring von R, so ist $\iota : R_0 \to R$ ein Ringmonomorphismus
- $\mathbb{Z} \to \mathbb{Z}\backslash n\mathbb{Z}$ mit $\overline{a} \mapsto a + n\mathbb{Z}$ it ein Ringepimorphismus
- Sei R kommutativ mit Einselement. Für $\lambda \in R$ ist die Auswertungsabbildung $R[X] \to R$ mit $f \mapsto f(\lambda)$ ein Ringepimorphismus. Dies ist die Aussage von Lemma 6.8
- $\mathbb{C} \to \mathbb{C}$ mit $z \mapsto \overline{z}$ ist ein Ringisomorphismus

Satz 3.4
Sind $f : R \to S$ und $g : S \to T$ Ringhomomorphismen, so auch $g \circ f : R \to T$.

Beweis. Übung, analog zu Satz 2.5 □

Lemma 3.5
Ist $f : R \to S$ ein Ringisomorphismus, so auch $f^{-1} : S \to R$.

Beweis. Nach Lemma 2.7 wissen wir: f^{-1} ist ein Isomorphismus der abelschen Gruppen $(S, +) \to (R, +)$. Die Verträglichkeit mit der Multiplikation zeigt man analog. □

Satz 3.6
Sei $f \in \mathrm{Hom}(R, S)$. Genau dann ist f ein Ringisomorphismus, wenn es $f' \in \mathrm{Hom}(S, R)$ mit $f' \circ f = \mathrm{id}_R$ und $f \circ f' = \mathrm{id}_S$ gibt.

Beweis. Klar, analog zu Satz 2.8 □

Lemma 3.7
Der Kern $I := \mathrm{Ker}(f)$ eines Ringhomomorphismus $f : R \to S$ ist eine Untergruppe von $(R, +)$ mit $x \cdot a, a \cdot x \in I$ für alle $a \in I$ und $x \in R$.

Beweis. Nach Lemma 2.13 ist I eine Untergruppe von $(R, +)$. Für $x \in R$ und $a \in I$ ist $f(xa) = f(x) \cdot f(a) = f(x) \cdot 0 = 0$. Somit ist $xa \in I$. Analog ist $ax \in I$. □

Satz 3.8
Sei $f \in \mathrm{Hom}(R, S)$. Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = \{0\}$.

Beweis. Klar aus Satz 2.14, da $f : (R, +) \to (S, +)$ ein Gruppenhomomorphismus ist. □

Definition 3.9 (Ideal)
Ist I eine Untergruppe von $(R, +)$ und $xa, ax \in I$ mit $x \in R$ und $a \in I$, so nennt man I ein Ideal von R und schreibt $I \trianglelefteq R$.

Beispiel 3.10
Der Kern des Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}\backslash n\mathbb{Z}$ mit $a \mapsto \overline{a}$ ist das Ideal $I = n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

4. Homomorphismen von Vektorräumen

Seien U, V, W drei K-Vektorraum.

Definition 4.1 (linear)
Eine Abbildung $f : V \to W$ heißt K-linear er Homomorphismus von K-Vektorraum, wenn für alle $x, y \in V$ und $\lambda \in K$ gilt:

- (L1): $f(x + y) = f(x) + f(y)$
- (L2): $f(\lambda x) = \lambda \cdot f(x)$

Die Menge der K-linearen Abbildungen $f : V \to W$ wird mit $\mathrm{Hom}_K(V, W)$ bezeichnet. Die Elemente von $\mathrm{End}_K(V) := \mathrm{Hom}_K(V, V)$ nennt man die Endomorphismen von V. Ein $f \in \mathrm{Hom}_K(V, W)$ ist ein Mono-, Epi- bzw. Isomorphismus, falls f injektiv, surjektiv bzw. bijektiv ist. Einen Endomorphismus der auch ein Isomorphismus ist, nennt man Automorphismus von V und bezeichnet die Menge der Automorphismen von V mit $\mathrm{Aut}_K(V)$. Der Kern einer linearen Abbildung $f : V \to W$ ist $\mathrm{Ker}(f) := f^{-1}(\{0\})$.

▶ **Bemerkung 4.2**
Eine K-lineare Abbildung $f : V \to W$ ist also ein Homomorphismus der abelschen Gruppen $(V, +) \to (W, +)$, der mit der Skalarmultiplikation verträglich ist, d.h. eine strukturverträgliche Abbildung zwischen Vektorräumen.

Satz 4.3
Eine Abbildung $f : V \to W$ ist genau dann K-linear, wenn für alle $x, y \in V$ und $\lambda, \mu \in K$ gilt:
(L): $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$.

Beweis.
- Hinrichtung: $f(\lambda x + \mu y) = f(\lambda x) + f(\mu y) = \lambda f(x) + \mu f(y)$
- Rückrichtung: (L1): $f(x + y) = f(1x + 1y) = 1f(x) + 1f(y)$, (L2): $f(\lambda x) = f(\lambda x + 0y) = \lambda f(x)$. □

■ **Beispiel 4.4**
- $\mathrm{id}_V : V \to V$ ist ein Automorphismus von V
- $c_0 : V \to W$ mit $x \mapsto 0$ ist K-linear
- Für einen Untervektorraum $V_0 \leq V$ ist $\iota : V_0 \to V$ ein Monomorphismus
- Im K-Vektorraum $K[X]$ kann man die (formale) Ableitung definieren: $(\sum_{i=0}^{n} a_i X^i)' := \sum_{i=1}^{n} i a_i X^{i-1}$. Diese Abbildung $K[X] \to K[X]$ mit $f \mapsto f'$ ist ein K-Endomorphismus von $K[X]$.

■ **Beispiel 4.5**
Sei $V = K^n$ und $W = K^m$. Wir fassen die Elemente von V und W als Spaltenvektoren auf. Zu einer Matrix $A \in \mathrm{Mat}_{m \times n}(K)$ definieren wir die Abbildung $f_A : V \to W$ mit $x \mapsto Ax$.

Ausgeschrieben: Ist $A = (a_{ij})$ und $x = (x_1, ..., x_n)^t$ so ist

$$f_A(x) = Ax = \begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & & ... \\ a_{m1} & ... & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} \cdot x_1 + ... + a_{1n} \cdot x_n \\ ... \\ a_{m1} \cdot x_1 + ... + a_{mn} \cdot x_n \end{pmatrix}$$

Nach Lemma 1.9 und Lemma 1.7 ist f_A eine lineare Abbildung.

Satz 4.6
Für ein $f \in \mathrm{Hom}_K(V, W)$. Dann gilt:

- $f(0) = 0$
- Für $x, y \in V$ ist $f(x - y) = f(x) - f(y)$.
- Sind (x_1) aus V, (λ_i) aus K, fast alle gleich 0, so ist $f(\sum_{i \in I} \lambda_i \cdot x_i) = \sum_{i \in I} \lambda_i \cdot f(x)$.
- Ist (x_i) linear abhängig in V, so ist $f(x_i)$ linear abhängig in W.
- Ist $V_0 \leq V$ ein Untervektorraum von V, so ist $f(V_0) \leq W$ ein Untervektorraum.
- Ist $W_0 \leq W$ ein Untervektorraum von W, so ist $f^{-1}(W_0) \leq V$ ein Untervektorraum.

Beweis.
- klar
- klar
- Induktion
- $\sum \lambda_i \cdot x_i = 0 \Rightarrow 0 = f(0) = f(\sum \lambda_i \cdot x_i) = \sum \lambda_i \cdot f(x_i)$
- $x, y \in V_0 \Rightarrow f(x) + f(y) = f(x + y) \in f(V_0)$
  $x \in V_0, \lambda \in K \Rightarrow f(x \cdot \lambda = f(\lambda x) \in f(V_0))$
- $f(0) = 0 \in W_0 \Rightarrow 0 \in f^{-1}(W_0)$, insbesondere ist $f^{-1}(W_0) \neq \emptyset$
  $x, y \in f^{-1}(W_0) \Rightarrow f(x + y) = f(x) + f(y) \in W_0$, also $x + y \in f^{-1}(W_0)$
  $x \in f^{-1}(W_0)$ und $\lambda \in K \Rightarrow f(\lambda x) = \lambda f(x) \in W_0$, also $\lambda x \in f^{-1}(W_0)$ □

Satz 4.7
Sind $f : V \to W$ und $g : W \to U$ K-linear, so auch $g \circ f : V \to U$.

Beweis. Für $x, y \in V$ und $\lambda, \mu \in K$ ist $(g \circ f)(\lambda x + \mu y) = g(f(\lambda x + \mu y)) = g(\lambda f(x) + \mu f(y)) = \lambda(g \circ f)(x) + \mu(g \circ f)(y)$. □

Lemma 4.8
Ist $f : V \to W$ ein Isomorphismus, so auch $f^{-1} : W \to V$.

Beweis. Wir müssen nur zeigen, dass f^{-1} linear ist. Für $x, y \in V$ und $\lambda, \mu \in K$ ist $f(\lambda f^{-1}(x) + \mu f^{-1}(y)) = \lambda(f \circ f^{-1})(x) + \mu(f \circ f^{-1})(y) = \lambda x + \mu y$, also $f^{-1}(\lambda x + \mu y) = \lambda f^{-1}(x) + \mu f^{-1}(y)$. □

Satz 4.9
Sei $f : V \to W$ linear. Genau dann ist f ein Isomorphismus, wenn es eine lineare Abbildung $f' : W \to V$ gibt mit $(f' \circ f) = \mathrm{id}_V$ und $(f \circ f') = \mathrm{id}_W$.

Beweis. Ist f ein Isomorphismus, so erfüllt $f' = f^{-1}$ nach Lemma 4.8 die Behauptung. Existiert umgekehrt f' wie angegeben, so muss f bijektiv sein. □

▶ **Bemerkung 4.10**
Wie auch bei Gruppen sehen wir hier bei Vektorräumen, dass Isomorphismen genau die strukturerhaltenden Abbildungen sind. Wieder können wir uns einen Isomorphismus $f : V \to W$ so vorstellen, dass wir nur die Elemente von V umbenennen. Alle Aussagen, die sich nur aus der Struktur selbst ergeben, bleiben damit wahr, wie z.B. $\dim_K(V) = \dim_K(W) \iff V = W$. Insbesondere ist $K^n \cong K^m$ für $n = m$.

Satz 4.11
Ist $f : V \to W$ eine lineare Abbildung, so ist $\mathrm{Ker}(f)$ ein Untervektorraum von V. Genau dann ist f ein Monomorphismus, wenn $\mathrm{Ker}(f) = \{0\}$.

Beweis. Der erste Teil folgt aus Satz 4.6, der zweite folgt aus Satz 2.14, da $f : (V, +) \to (W, +)$ ein Gruppenhomomorphismus ist. □

5. Der Vektorraum der linearen Abbildungen

Seien V und W zwei K-Vektorräume.

Satz 5.1
Sei (x_i) eine Basis von V und (y_i) eine Familie in W. Dann gibt es genau eine lineare Abbildung $f : V \to W$ mit $f(x_i) = y_i$. Diese Abbildung ist durch $f(\sum \lambda_i x_i) = \sum \lambda_i y_i$ (*) ($\lambda_i \in K$, fast alle gleich 0) gegeben und erfüllt

- $\mathrm{Im}(f) = \mathrm{span}_K(y_i)$
- genau dann ist f injektiv, wenn (y_i) linear unabhängig ist

Beweis. Ist $f : V \to W$ linear mit $f(x_i) = y_i$, so folgt aus Satz 4.6 $f(\sum \lambda_i x_i) = \sum \lambda_i y_i$. Da sich jedes $x \in V$ als $x = \sum \lambda_i x_i$ schreiben lässt, ist f dadurch schon eindeutig bestimmt. Andererseits wird durch (*) eine wohldefinierte Abbildung beschrieben, da die Darstellung von x eindeutig ist (denn x_i sind linear unabhängig). Es bleibt zu zeigen, dass die durch (*) definierte Abbildung $f : V \to W$ tatsächlich linear ist. Ist $x = \sum \lambda_i x_i$ und $x' = \sum \lambda_i' x_i$ so ist $f(x + x') = f(\sum(\lambda_i + \lambda_i')x_i) = \sum(\lambda_i + \lambda_i')y_i = \sum \lambda_i y_i + \sum \lambda_i' y_i = f(x) + f(x')$. $f(\lambda x) = f(\sum \lambda\lambda_i x_i) = \sum \lambda\lambda_i y_i = \lambda \sum \lambda_i y_i = \lambda f(x)$.

- $\mathrm{Im}(f)$ ist ein Untervektorraum nach Satz 4.6 von W und $\{y_i\} \subset \mathrm{Im}(f) \subset \mathrm{span}_K(y_i)$, somit $\mathrm{Im}(f) = \mathrm{span}_K(y_i)$
- Satz 4.11: f ist injektiv $\iff$ $\mathrm{Ker}(f) = \{0\}$
  $\iff$ $\lambda_i \in K$ gilt: $f(\sum \lambda_i x_i) = 0 \Rightarrow \sum \lambda_i x_i = 0$
  $\iff$ $\lambda_i \in K$ gilt: $\sum \lambda_i y_i = 0 \Rightarrow \lambda_i = 0$
  $\iff$ (y_i) linear unabhängig. □

Folgerung 5.2
Sei $\dim_K < \infty$. Ist $(x_1, ..., x_n)$ eine linear unabhängige Familie in V und $(y_1, ..., y_n)$ eine Familie in W, so gibt es eine lineare Abbildung $f : V \to W$ mit $f(x_i) = y_i$

Beweis. Nach dem Basisergänzungssatz (Folgerung 3.13) können wir die Familie (x_i) zu einer Basis $x_1, ..., x_m$ ergänzen. Die Behauptung folgt aus Satz 5.1 für beliebige $y_{n+1}, ..., y_m \in W$. □

Folgerung 5.3
Ist (x_i) eine Basis von V und (y_i) eine Basis in W, so gibt es genau einen Isomorphismus $f : V \to W$ mit $f(x_i) = y_i$.

Beweis. Sei f wie in Satz 5.1. (y_i) ist Erzeugendensystem $\Rightarrow \mathrm{Im}(f) = \mathrm{span}_K(y_i) = W$, also f surjektiv. (y_i) linear abhängig $\Rightarrow f$ ist injektiv. □

Folgerung 5.4
Zwei endlichdimensionale K-Vektorräume sind genau dann isomorph, wenn sie dieselbe Dimension haben.

Beweis. Folgerung 5.3 und Bemerkung 4.10 □

Folgerung 5.5
Ist $B = (v_1, ..., v_n)$ eine Basis von V, so gibt es genau einen Isomorphismus $\Phi_B : K^n \to V$ mit $\Phi_B(e_i) = v_i$. Insbesondere ist jeder endlichdimensionale K-Vektorraum zu einem Standardraum isomorph, nämlich zu K^n für $n = \dim_K(V)$.

Definition 5.6 (Koordinatensystem)
Die Abbildung Φ_B heißt Koordinatensystem zu B. Für $v \in V$ ist $(x_1, ..., x_n)^t = \Phi_B^{-1}(v) \in K^n$ der Koordinatenvektor zu v bezüglich B und $(x_1, ..., x_n)$ sind die Koordinaten von v bezüglich B.

Satz 5.7
Die Menge $\mathrm{Hom}_K(V, W)$ ist ein Untervektorraum des K-Vektorraums $\mathrm{Abb}(V, W)$.

Beweis. Seien $f, g \in \mathrm{Hom}_K(V, W)$ und $\eta \in K$.

- $f + g \in \mathrm{Hom}_K(V, W)$: Für $x, y \in V$ und $\lambda, \mu \in K$ ist $(f + g)(\lambda x + \mu y) = f(\lambda x + \mu y) + g(\lambda x + \mu y) = \lambda f(x) + \mu f(y) + \lambda g(x) + \mu g(y) = \lambda(f + g)(x) + \mu(f + g)(y)$
- $\eta f \in \mathrm{Hom}_K(V, W)$: Für $x, y \in V$ und $\lambda, \mu \in K$ ist $(\eta f)(\lambda x + \mu y) = \eta \cdot f(\lambda x + \mu y) = \eta(\lambda f(x) + \mu f(y)) = \lambda(\eta f)(x) + \mu(\eta f)(y)$
- $\mathrm{Hom}_K(V, W) \neq \emptyset$: $c_0 \in \mathrm{Hom}_K(V, W)$ □

Lemma 5.8
Sei U ein weiterer K-Vektorraum. Sind $f, f_1, f_2 \in \mathrm{Hom}_K(V, W)$ und $g, g_1, g_2 \in \mathrm{Hom}_K(U, V)$, so ist $f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$ und $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$.

Beweis. Für $x \in U$ ist

- $(f \circ (g_1 + g_2))(x) = f((g_1 + g_2)(x)) = f(g_1(x) + g_2(x)) = f(g_1(x)) + f(g_2(x)) = (f \circ g_1 + f \circ g_2)(x)$
- $((f_1 + f_2) \circ g)(x) = (f_1 + f_2)(g(x)) = f_1(g(x)) + f_2(g(x)) = (f_1 \circ g + f_2 \circ g)(x)$ □

Folgerung 5.9
Unter der Komposition wird $\mathrm{End}_K(V)$ zu einem Ring mit Einselement id_V und $\mathrm{End}_K(V)^\times = \mathrm{Aut}_K(V)$.

Beweis. $(\mathrm{End}_K(V), +)$ ist eine abelsche Gruppe (Satz 4.9), die Komposition eine Verknüpfung auf $\mathrm{End}_K(V)$ ist assoziativ und die Distributivgesetze gelten (Lemma 5.8). □

▶ **Bemerkung 5.10**
Die Menge der strukturverträglichen Abbildungen zwischen K-Vektorräumen trägt also wieder die Struktur eines K-Vektorraums. Wir können diesen mit unseren Mitteln untersuchen und z.B. nach Dimension und Basis fragen.

Lemma 5.11
Seien $m, n, r \in \mathbb{N}$, $A \in \mathrm{Mat}_{m \times n}(K)$, $B \in \mathrm{Mat}_{n \times r}(K)$. Für die linearen Abbildungen $f_A \in \mathrm{Hom}_K(K^n, K^m)$, $f_B \in \mathrm{Hom}_K(K^r, K^n)$ aus Beispiel 4.5 gilt dann $f_{AB} = f_A \circ f_B$.

Beweis. Sind $A = (a_{ij})$ und $B = (b_{jk})$, so ist $(f_A \circ f_B)(e_k) = f_A(f_B(e_k)) = f_A(Be_k) = f_A(b_{1k}, ..., b_{nk})^t = A \cdot (b_{1k}, ..., b_{nk})^t = (\sum_{j=1}^n a_{ij}b_{jk}, ..., \sum_{j=1}^n a_{mj}b_{jk})^t = AB \cdot e_k = f_{AB}(e_k)$ für $k = 1, ..., r$, also $f_A \circ f_B = f_{AB}$ nach Satz 5.1. □

Satz 5.12
Die Abbildung $A \to f_A$ aus Beispiel 4.5 liefert einen Isomorphismus von K-Vektorräumen $F_{m\times n}$: $\mathrm{Mat}_{m\times n}(K) \to \mathrm{Hom}_K(K^n, K^m)$ sowie einen Ringisomorphismus $F_n : \mathrm{Mat}_n(F) \to \mathrm{End}_K(K^n)$ der $\mathrm{GL}_n(K)$ auf $\mathrm{Aut}_K(K^n)$ abbildet.

Beweis. Wir schreiben F für $F_{m\times n}$

- F ist linear: Sind $A, B \in Mat - n \times m(K)$ und $\lambda, \mu \in K$, so ist $F(\lambda A + \mu B)(x) = f_{\lambda A+\mu B}(x) = (\lambda A + \mu B)x = \lambda Ax + \mu Bx = \lambda f_A(x) + \mu f_B(x) = (\lambda F(A) + \mu F(B))(x)$, also ist F linear.
- F ist injektiv: Es genügt zu zeigen, dass $\mathrm{Ker}(f) = \{0\}$ (Satz 4.11). Ist $A = (a_{ij}) \in \mathrm{Mat}_{n\times m}(K)$ mit $F(A) = 0$, so insbesondere $0 = F(A)(e_j) = f_A(e_j) = Ae_j = (a_{1j}, ..., a_{mj})^t$, also $A = 0$.
- F ist surjektiv: Sei $f \in \mathrm{Hom}_K(V, W)$. Schreibe $f(e_j) = (a_{1j}, ..., a_{mj})^t$ und setze $A = (a_{ij}) \in \mathrm{Mat}_{n\times m}(K)$. Dann ist $f_A \in \mathrm{Hom}_K(K^n, K^m)$ mit $f_A(e_j) = Ae_j = f(e_j)$, also $f = f_A = F(A) \in \mathrm{Im}(f)$ nach Satz 5.1.
- F_n ist eine Ringhomomorphismus (Lemma 5.11):
  (RH1) aus (L1)
  (RH2) aus $f_{AB} = f_A \circ f_B$.
- Somit ist F_n eine Ringisomorphismus $\Rightarrow F_n(\mathrm{Mat}_n(K)^\times) = \mathrm{End}_K(V)^\times$, also $F_n(\mathrm{GL}_n(K)) = \mathrm{Aut}_K(V)$ nach Folgerung 5.9. □

▶ **Bemerkung 5.13**
Wir sehen also, dass die linearen Abbildungen zwischen Standardräumen sehr konkret durch Matrizen beschrieben werden können. Da jeder endlichdimensionale Vektorraum zu einem Standardraum isomorph ist (Folgerung 5.5), kann man diese Aussage auf solche Vektorräume erweitern. Dies wollen wir im nächsten Abschnitt tun.

6. Koordinatendarstellung linearer Abbildungen

Seien V, W endlichdimensionale K-Vektorräume mit den Basen $B = (x_1, ..., x_n)$ und $C = (y_1, ..., y_m)$.

Definition 6.1 (darstellende Matrix)
Sei $f \in \mathrm{Hom}_K(V, W)$. Für $j = 1, ..., n$ schreiben wir $f(x_j) = \sum_{i=1}^{m} a_{ij} y_i$ mit eindeutig bestimmten $a_{ij} \in K$. Die Matrix $M_C^B(f) = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$ heißt die darstellende Matrix von f bezüglich der Basen B und C.

Satz 6.2
Sei $f \in \mathrm{Hom}_K(V, W)$. Die darstellende Matrix $M_C^B(f)$ ist die eindeutig bestimmte Matrix $A \in \mathrm{Mat}_{n\times m}(K)$, für die das folgenden Diagramm kommutiert:

$$\begin{array}{ccc} K^n & \xrightarrow{f_A} & K^m \\ {\scriptstyle \Phi_B}\downarrow & & \downarrow{\scriptstyle \Phi_C} \\ V & \xrightarrow[f]{} & W \end{array}$$

d.h. $f \circ \Phi_B = \Phi_C \circ f_A$.

Beweis. Sei zunächst $A = M_C^B(f)$. Für $j = 1, ..., n$ ist $\Phi_C(f_A(e_j)) = \Phi_C((a_{1j}, ..., a_{mj})^t) = \sum_{i=1}^{m} a_{ij} \cdot y_i = f(x_j) = f(\Phi_B(e_j))$, also $\Phi_C \circ f_A = f \circ \Phi_B$.
Sei umgekehrt $A \in \mathrm{Mat}_{m\times n}(K)$ mit $\Phi_C \circ f_A = f \circ \Phi_B$. Da Φ_B und Φ_C Isomorphismen sind, ist f_A eindeutig bestimmt: $f_A = \Phi_C^{-1} \circ f \circ \Phi_B$ und deshalb auch A (Satz 5.12). □

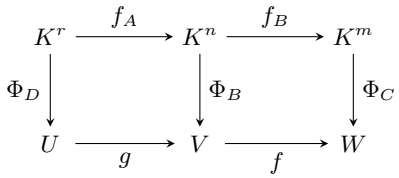
Folgerung 6.3
Die Abbildung M_C^B: $\mathrm{Hom}_K(V, W) \to \mathrm{Mat}_{m\times n}(K)$ ist ein Isomorphismus von K-Vektorräumen.

Beweis. Definiere A: $\mathrm{Hom}_K(V, W) \to \mathrm{Mat}_{m\times n}(K)$ mit $f \mapsto \Phi_C^{-1} \circ f \circ \Phi_B$. $A(f) = F_{m\times n}(M_C^B(f))$, also $A = F_{m\times n} \circ M_C^B$. Die Abbildung ist bijektiv, da Φ_B und Φ_C bijektiv sind, und linear, da Φ_B und Φ_C linear sind (Lemma 5.8). Also ist A ein Isomorphismus. Da auch $F_{m\times n}^{-1}$ ein Isomorphismus ist (Satz 5.12), ist folglich auch $M_C^B = F_{m\times n}^{-1} \circ A$. □

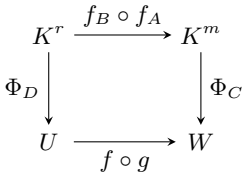
Lemma 6.4
Sei U ein weiterer K-Vektorraum mit endlicher Basis D. Für $f \in \mathrm{Hom}_K(V, W)$ und $g \in \mathrm{Hom}_K(U, V)$ ist

$$M_C^B(f) \cdot M_B^D(g) = M_C^D(f \circ g)$$

Beweis. Sei $r = \dim_K(U)$ und $A = M_B^D(g)$ und $B = M_C^B(f)$. Nach Satz 6.2 kommutieren die beiden kleinen Quadrate in:



Deshalb kommutiert auch:



Die Eindeutigkeit in Satz 6.2 impliziert deshalb, dass $F_{m\times n}(M_C^B(f)) \circ F_{r\times m}(M_B^D(g)) = F_{r\times n}(M_C^D(f \circ g))$. Da $F_{r\times n}$ injektiv ist, folgt mit Lemma 5.11 und Satz 5.12 $M_C^B(f) \cdot M_B^D(g) = M_C^D(f \circ g)$. □

Folgerung 6.5
Sei $f \in \mathrm{Hom}_K(V, W)$. Genau dann ist f ein Isomorphismus, wenn $m = n$ und $M_C^B(f) = \mathrm{GL}_n(K)$. In diesem Fall ist $M_B^C(f^{-1}) = M_C^B(f)^{-1}$.

Beweis. Sei $A = M_C^B(f)$. Nach Satz 6.2 ist f genau dann ein Isomorphismus, wenn f_A einer ist, und in diesem Fall ist $m = n$. Zudem ist f_A genau dann ein Isomorphismus, wenn $A \in \mathrm{GL}_n(K)$ (Satz 5.12). Ist f ein Isomorphismus, so ist $M_B^C(f^{-1}) \cdot M_C^B(f) = M_C^C(f^{-1} \circ f) = \mathbb{1}_n$, also $M_B^C(f^{-1}) = M_C^B(f)^{-1}$ (Lemma 6.4). □

Folgerung 6.6
Die Abbildung $M_B := M_B^B \colon \mathrm{End}_K(V) \to \mathrm{Mat}_n(K)$ ist ein Ringisomorphismus, der $\mathrm{Aut}_K(V)$ auf $\mathrm{GL}_n(K)$ abbildet.

Beweis. Folgerung 6.3, Lemma 6.4, Folgerung 6.5 □

Definition 6.7 (Transformationsmatrix)
Sind B und B' Basen von V, so nennt man $T_{B'}^B := M_{B'}^B(\mathrm{id}_V) \in \mathrm{GL}_n(K)$ die Transformationsmatrix des Basiswechsels von B nach B'.

▶ **Bemerkung 6.8**
Nach Satz 6.2 ist $T_{B'}^B$, also die Matrix A, die $f_A = \Phi_B^{-1} \circ \Phi_B$ erfüllt. Ist $x = \Phi_B^{-1}(v) \in K^n$ der Koordinatenvektor von v bezüglich B, so ist $T_{B'}^B \cdot x = f_{T_{B'}^B}(x) = (\Phi_{B'} \circ \Phi_B)(\Phi_B^{-1}(v)) = \Phi_{B'}^{-1}(v)$ der Koordinatenvektor von v bezüglich B'.

Satz 6.9 (Transformationsformel)
Seien B, B' Basen von V und C, C' Basen von W. Für $f \in \mathrm{Hom}_K(V, W)$ ist

$$M_{C'}^B(f) = T_{C'}^C \cdot M_C^B(f) \cdot (T_{B'}^B)^{-1}$$

Beweis. $f = \mathrm{id}_W \circ f \circ \mathrm{id}_V$ mit den Basen B', B, C, C' und erhält (Lemma 6.4) $M_{C'}^{B'}(f) = M_{C'}^C(\mathrm{id}_W) \cdot M_C^B(f) \cdot M_B^{B'}(\mathrm{id}_V) = T_{C'}^C \cdot M_C^B(f) \cdot T_B^{B'}$ und $T_B^{B'} = M_B^{B'}(\mathrm{id}_V) = M_B^{B'}(\mathrm{id}_V^{-1}) = M_{B'}^B(\mathrm{id}_V)^{-1} = (T_{B'}^B)^{-1}$ nach Folgerung 6.5. □

Folgerung 6.10
Sind B und B' Basen von V und $f \in \mathrm{End}_K(V)$, so gilt $M_{B'}(f) = T_{B'}^B \cdot M_B(f) \cdot (T_{B'}^B)^{-1}$.

7. Quotientenräume

Seien V, W K-Vektorräume und $U \subseteq V$ ein Untervektorraum.

Definition 7.1 (affiner Unterraum)
Ein affiner Unterraum von V ist eine Teilmenge der Form

$$x + U := \{x + u \mid u \in U\} \subseteq V$$

wobei $U \subseteq V$ ein beliebiger Untervektorraum von V ist und $x \in V$.

Lemma 7.2
Für $x, x' \in V$ sind äquivalent:

- $x + U = x' + U$
- $x' \in x + U$
- $x' - x \in U$

Beweis.
- $1 \Rightarrow 2$: $x' = x' + 0 \in x' + U = x + U$
- $2 \Rightarrow 3$: $x' \in x + U \Rightarrow x' = x + u$ mit $u \in U \Rightarrow x' - x = u \in U$
- $3 \Rightarrow 1$: Sei $u_0 := x' - x \in U$. Für $u \in U$ ist $x + u = x' - u_0 + u \in x' + U$, also $x' + U \subseteq x + U$, $x' + u = x + u_0 + u \in x + U$, also $x + U \subseteq x' + U$. □

Lemma 7.3
Sei $f \in \mathrm{Hom}_K(V, W)$ und $U = \mathrm{Ker}(f)$. Für $y \in f(V)$ ist die Faser $f^{-1}(y) = f^{-1}(\{y\})$ von f der affine Unterraum $x_0 + U$ für ein beliebiges $x_0 \in f^{-1}(y)$.

Beweis. $f^{-1}(y) = \{x \in V \mid f(x) = f(x_0)\} = \{x \in V \mid f(x - x_0) = 0\} = \{x \in V \mid x - x_0 \in U\} = x_0 + U$ □

■ **Beispiel 7.4**
Sind $K = \mathbb{R}$, $V = \mathbb{R}^2$, $W = \mathbb{R}$ und $f(x, y) = x - 2y$ so sind die Fasern von f die Geraden $L \subseteq \mathbb{R}^2$ der Steigung $\frac{1}{2}$.

Lemma 7.5
Seien $x_1, x_1', x_2, x_2' \in V$ und $\lambda \in K$. Ist $x_1 + U = x_1' + U$ und $x_2 + U = x_2' + U$, so ist $(x_1 + x_2) + U = (x_1' + x_2') + U$, und $\lambda x_1 + U = \lambda x_1' + U$.

Beweis.
- $x_1 + U = x_1' + U$, $x_2 + U = x_2' + U \Rightarrow x_1' - x_1, x_2' - x_2 \in U$ Lemma 7.2 $\Rightarrow (x_1' + x_2') - (x_1 + x_2) = (x_1' - x_1) - (x_2' - x_2) \in U \Rightarrow (x_1 + x_2) + U = (x_1' + x_2') + U$
- $x_1 + U = x_1' + U \Rightarrow x_1' - x_1 \in U \Rightarrow \lambda x_1' - \lambda x_1 \in U \Rightarrow \lambda x_1' + U = \lambda x_1 + U$ □

Definition 7.6 (Quotientenraum)
Der Quotientenraum von V modulo U ist die Menge der affinen Unterräume

$$V/U := \{x + U \mid x \in V\}$$

mit der Addition $(x_1 + U) + (x_2 + U) = (x_1 + x_2) + U$ und der Multiplikation $\lambda(x + U) = \lambda x + U$. Dies ist wohldefiniert nach Lemma 7.5.

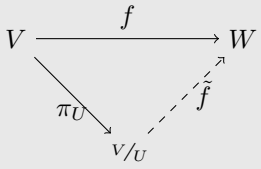
Wir definieren die Abbildung $\pi_U : V \to V/U$ durch $\pi_U(x) = x + U$.

Satz 7.7
Der Quotientenraum V/U ist ein K-Vektorraum und π_U ein Epimorphismus mit Kern U.

Beweis.
- $(V/U, +)$ ist eine abelsche Gruppe:
  - Assoziativität un Kommutativität: überträgt sich von $(V, +)$
  - neutrales Element: $0 + U = U$
  - inverses Element: $-(x + U) = (-x) + U$
- $(V/U, +)$ ist K-Vektorraum: (V2) überträgt sich von $(V, +, \cdot)$
- π_U surjektiv: nach Definition von V/U
- π_U linear: nach Definition von $+$ und $\cdot$ auf V/U
- $\mathrm{Ker}(\pi_U) = \{x \in V \mid x + U = U\} = \{x \in V \mid x \in 0 + U\} = U$ □

▶ **Bemerkung 7.8**
Die Untervektorraum sind also genau die Kerne linearer Abbildungen! Ist $f : V \to W$ linear, so ist $\mathrm{Ker}(f) \subseteq V$ ein Untervektorraum. Ist $U \subseteq V$ ein Untervektorraum, so ist $\pi_U : V \to V/U$ linear mit Kern U.

Theorem 7.9 (Homomorphiesatz)
Sei $f \in \mathrm{Hom}_K(V, W)$ mit $U \subseteq \mathrm{Ker}(f)$. Dann gibt es genau eine lineare Abbildung $\tilde{f} : V/U \to W$ mit $f = \tilde{f} \circ \pi_U$, d.h. es kommutiert:



Diese erfüllt $\mathrm{Ker}(\tilde{f}) = \mathrm{Ker}(f)/U = \{x + U \mid x \in \mathrm{Ker}(f)\} \subseteq V/U$.

Beweis. Ist $f = \tilde{f} \circ \pi_U$, so gilt $\tilde{f}(x + U) = \tilde{f}(\pi_U) = f(x)$ $(*)$, somit ist $\tilde{f}$ dann eindeutig bestimmt. Umgekehrt wird durch $(*)$ eine wohldefinierte Abbildung $\tilde{f}$ erklärt: Sind $x, x' \in V$ mit $x + U = x' + U$, so ist $x - x' \in U \subseteq \mathrm{Ker}(f)$ und deshalb $f(x) = f(x')$.

- Linearität: Für $x, y \in V$ und $\lambda \in K$ ist $\tilde{f}(\lambda(x + U) + \mu(y + U)) = \tilde{f}(\lambda\pi_U(x) + \mu\pi_U(y)) = \lambda\tilde{f}(x + U) + \mu\tilde{f}(y + U)$.

- Kern: $\tilde{f}(x+U)=0 \iff f(x)=0 \iff x\in \mathrm{Ker}(f)$. □

Folgerung 7.10
Für $f\in \mathrm{Hom}_K(V,W)$ ist $\mathrm{Im}(f)\cong {}^{V}\!/_{\mathrm{Ker}(f)}$. Insbesondere gilt: Ist f ein Epimorphismus, so ist $W\cong {}^{V}\!/_{\mathrm{Ker}(f)}$.

Beweis. Betrachte $\tilde{f}: {}^{V}\!/_{\mathrm{Ker}(f)}\to W$. Nach Theorem 7.9 ist $\mathrm{Ker}(\tilde{f})={}^{\mathrm{Ker}(f)}\!/_{\mathrm{Ker}(f)}=\{\mathrm{Ker}(f)\}$, also $\tilde{f}$ injektiv. Nach Definition ist $\tilde{f}({}^{V}\!/_{\mathrm{Ker}(f)})=f(V)=\mathrm{Im}(f)$. Somit ist $\tilde{f}: {}^{V}\!/_{\mathrm{Ker}(f)}\to \mathrm{Im}(f)$ ein Isomorphismus. □

Satz 7.11
Seien U,U' Untervektorraum von V. Genau dann ist $V=U\oplus U'$, wenn $\pi_U|_{U'}: U'\to {}^{V}\!/_{U}$ ein Isomorphismus ist.

Beweis.
- $\pi_U|_{U'}$ injektiv $\iff \mathrm{Ker}(\pi_U|_{U'})=\{0\} \iff \mathrm{Ker}(\pi_U)\cap U'=\{0\} \iff U\cap U'=\{0\}$
- $\pi_U|_{U'}$ surjektiv $\iff \forall x\in V\exists u'\in U: \pi_U(u')=\pi_U(x) \iff u'-x\in \mathrm{Ker}(\pi_U)=U \iff x=u+u' \iff V=U+U'$ □

Folgerung 7.12
Ist $\dim_K(V)<\infty$, so ist $\dim_K({}^{V}\!/_{U})=\dim_K(V)-\dim_K(U)$.

Beweis. Nach Folgerung 4.10 existiert ein lineares Komplement U' zu U in V (d.h. $V=U\oplus U'$) und $\dim_K(U')=\dim_K(V)-\dim_K(U)$. Es gilt ${}^{V}\!/_{U}={}^{U'}$. □

Folgerung 7.13
Ist $\dim_K(V)<\infty$ und $f\in \mathrm{Hom}_K(V,W)$, so ist $\dim_K(V)=\dim_K(\mathrm{Ker}(f))+\dim_K(\mathrm{Im}(f))$.

Beweis. Satz 7.11 und Folgerung 7.12 □

Folgerung 7.14
Ist $\dim_K(V)<\infty$ und $f\in \mathrm{End}_K(V)$, so sind äquivalent:

- $f\in \mathrm{Aut}_K(V)$
- f ist injektiv
- f ist surjektiv

Beweis.
- $2 \iff \dim_K(\mathrm{Ker}(f))=0$
- $3 \iff \dim_K(\mathrm{Im}(f))=\dim_K(V)$ □

▶ **Bemerkung 7.15**
Analog zu dem Quotientenräumen kann man definieren:

- Quotientengruppen ${}^{G}\!/_{N}$, wobei N Normalteiler von G ist
- Quotientenringe ${}^{R}\!/_{I}$, wobei I ein Ideal von R ist (z.B. ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$)

Diese werden in der Vorlesung *Algebra und Zahlentheorie* behandelt.

8. Rang

Seien V, W zwei endlichdimensionale K-Vektorräume und $f \in \mathrm{Hom}_K(V, W)$.

Definition 8.1 (Rang)
Der Rang von f ist $\mathrm{rk}(f) = \dim_K(\mathrm{Im}(f))$.

▶ **Bemerkung 8.2**
Nach Folgerung 7.13 ist $\mathrm{rk}(f) = \dim_K(V) - \dim_K(\mathrm{Ker}(f))$. Also ist f genau dann injektiv, wenn $\mathrm{rk}(f) = \dim_K(V)$. Auch sehen wir, dass $\mathrm{rk}(f) \leq \min\{\dim_K(V), \dim_K(W)\}$.

Lemma 8.3
Sei U ein weiterer endlichdimensionaler K-Vektorraum und $g \in \mathrm{Hom}_K(U, V)$.

- Ist g surjektiv, dann ist $\mathrm{rk}(f \circ g) = \mathrm{rk}(f)$.
- Ist f injektiv, dann ist $\mathrm{rk}(f \circ g) = \mathrm{rk}(g)$.

Beweis. Dies folgt sofort aus $\mathrm{Im}(f \circ g) = f(\mathrm{Im}(g))$. □

Satz 8.4
Sei $r \in \mathbb{N}_0$. Genau dann ist $\mathrm{rk}(f) = r$, wenn es B von V und C von W gibt, für die

$$M_C^B(f) = E_r = \sum_{i=1}^{r} E_{ii}$$

$$E_r = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & 0 \end{pmatrix}$$

Beweis.
- Rückrichtung: Ist $M_C^B(f) = E_r$ und $C = (y_1, ..., y_n)$, so ist $\mathrm{Im}(f) = \mathrm{span}_K(y_1, ..., y_r)$, also $\mathrm{rk}(f) = r$.
- Hinrichtung: Sei $r = \mathrm{rk}(f)$. Setze $U = \mathrm{Ker}(f)$ und $W = \mathrm{Im}(f)$. Wähle Basis $(y_1, ..., y_r)$ und ergänze diese zu einer Basis C von W. Wähle für $i = 1, ..., r$ ein $x_i \in f^{-1}(y_i)$. Dann ist $(x_1, ..., x_r)$ linear unabhängig und mit $U' = \mathrm{span}_K(x_1, ..., x_r)$ ist $f|_{U'} : U' \to W_0$ ein Isomorphismus nach Satz 5.1. Insbesondere ist $U \cap U' = \{0\}$ und mit Satz 7.11 folgt $V = U \oplus U'$. Ist also $(x_{r+1}, ..., x_n)$ eine Basis von U, so ist $B = (x_1, ..., x_n)$ eine Basis von V (Satz 4.9). Diese Basis erfüllt $M_C^B(f) = E_r$. □

Definition 8.5 (Rang einer Matrix)
Der Rang einer Matrix $A \in \mathrm{Mat}_{m \times n}(K)$ ist $\mathrm{rk}(A) = \mathrm{rk}(f_A)$, wobei $f_A : K^n \to K^m$ die durch A beschriebene lineare Abbildung ist.

Mathematica/WolframAlpha-Befehle (Rang einer Matrix)
Auch für den Rang einer Matrix A hat Mathematica bzw. WolframAlpha eine Funktion

```
MatrixRank[A]
```

▶ **Bemerkung 8.6**
Sei $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$. Man fasst die Spalten $a_j = (a_{1j}, ..., a_{mj})^t$ als Elemente des K^m auf und definiert den Spaltenraum $\mathrm{SR}(A) = \mathrm{span}_K(a_1, ..., a_n) \subseteq K^m$. Entsprechend definiert man den Zeilenraum $\mathrm{ZR}(A) = \mathrm{span}_K(\tilde{a}_1^t, .., \tilde{a}_m^t) \subseteq K^n$. Es ist $\mathrm{Im}(f_A) = \mathrm{SR}(A)$ und folglich $\mathrm{rk}(A) = \dim_K(\mathrm{SR}(A))$. Außerdem ist $\mathrm{SR}(A^t) = \mathrm{ZR}(A)$ und deshalb $\mathrm{rk}(A^t) = \dim_K(\mathrm{ZR}(A))$. Man nennt $\mathrm{rk}(A)$ deshalb auch den Spaltenrang von A und $\mathrm{rk}(A^t)$ den Zeilenrang von A.

Lemma 8.7
Ist $A \in \mathrm{Mat}_{m\times n}(K)$, $S \in \mathrm{GL}_m(K)$, $T \in \mathrm{GL}_n(K)$, so ist $\mathrm{rk}(SAT) = \mathrm{rk}(A)$.

Beweis. $\mathrm{rk}(SAT) = \mathrm{rk}(f_{SAT}) = \mathrm{rk}(f_S \circ f_A \circ f_T) = \mathrm{rk}(f_A) = \mathrm{rk}(A)$, da f_S und f_T bijektiv sind (Lemma 8.3).□

Satz 8.8
Für jedes $A \in \mathrm{Mat}_{m\times n}(K)$ gibt es $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ mit $SAT = E_r$, wobei $r = \mathrm{rk}(A)$.

Beweis. Es gibt Basen B von K^n und C von K^m mit $M_C^B(f_A) = E_r$ (Satz 8.4). Mit den Standardbasen E_n bzw. E_m gilt: $M_C^B(f_A) = T_C^{E_m} \cdot M_{E_m}^{E_n}(f_A) \cdot (T_B^{E_n})^{-1} = SAT$ mit $S = T_C^{E_m} \in \mathrm{GL}_m(K)$ und $T = (T_B^{E_n})^{-1} \in \mathrm{GL}_n(K)$.□

Folgerung 8.9
Seien $A, B \in \mathrm{Mat}_{m\times n}(K)$. Genau dann gibt es $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ mit $B = SAT$, wenn $\mathrm{rk}(A) = \mathrm{rk}(B)$.

Beweis.
- Hinrichtung: Lemma 8.7
- Rückrichtung: $r = \mathrm{rk}(A) = \mathrm{rk}(B) \Rightarrow$ Nach Satz 8.8 gibt $S_1, S_2 \in \mathrm{GL}_m(K)$ und $T_1, T_2 \in \mathrm{GL}_n(K)$ mit $S_1AT_1 = E_r = S_2BT_2 \Rightarrow B = S_2^{-1} \cdot SAT_1 \cdot T_2^{-1}$. □

Satz 8.10
Für $A \in \mathrm{Mat}_{m\times n}(K)$ ist $\mathrm{rk}(A) = \mathrm{rk}(A^t)$, anders gesagt: $\dim_K(\mathrm{SR}(A)) = \dim_K(\mathrm{ZR}(A))$.

Beweis. Mit Satz 8.8 ergibt sich: $SAT = E_r$ mit $r = \mathrm{rk}(A)$, $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$. Aus $E_r^t = (SAT)^t = T^tA^tS^t$, folgt, dass $\mathrm{rk}(A^t) = \mathrm{rk}(E_r^t) = \mathrm{rk}(A)$. □

Folgerung 8.11
Für $A \in \mathrm{Mat}_n(K)$ sind äquivalent:
- $A \in \mathrm{GL}_n(K)$, d.h. es gibt $S \in \mathrm{GL}_n(K)$ mit $SA = AS = \mathbb{1}_n$
- $\mathrm{rk}(A) = n$
- Die Spalten von A sind linear unabhängig.

- Die Zeilen von A sind linear unabhängig.
- Es gibt $S \in \mathrm{GL}_n(K)$ mit $SA = \mathbb{1}_n$.
- Es gibt $T \in \mathrm{GL}_n(K)$ mit $AT = \mathbb{1}_n$.

Beweis.

- (1) $\iff$ (2): Lemma 5.11 und Folgerung 7.14
- (2) $\iff$ (3): Bemerkung 8.6
- (2) $\iff$ (4): Bemerkung 8.6 und Satz 8.10
- (1) $\iff$ (5) $\wedge$ (6): trivial
- (5) $\wedge$ (6) $\iff$ (2): Folgerung 8.9

□

9. Lineare Gleichungssysteme

Sei $A \in \mathrm{Mat}_{m\times n}(K)$ und $b \in K^m$.

Definition 9.1 (Lineares Gleichungssystem)
Unter einem Linearen Gleichungssystem verstehen wir eine Gleichung der Form $Ax = b$. Diese heißt homogen , wenn $b = 0$, sonst inhomogen und $L(A, b) = \{x \in K^n \mid Ax = b\}$ ist sein Lösungsraum .

Mathematica/WolframAlpha-Befehle (Lineare Gleichungssysteme)
Für das Lösen von Linearen Gleichungssystemen gibt es in WolframAlpha bzw. Mathematica verschiedene Verfahren:

- `Solve[]`:

```
Solve[a == 2 b && b == 5 && c + a == b, {a, b, c}]
```

- `LinearSolve[]`: Braucht 2 Argumente: Zum einen die Koeffizientenmatrix A und den Ergebnisvektor b. Rückgabe ist dann der Variablenvektor x.

```
LinearSolve[{{1, 1}, {0, 1}}, {6, 10}]
```

▶ **Bemerkung 9.2**
Ist $A = (a_{ij})$, $b = (b_1, ..., b_m)^t$, so schreibt man das Lineare Gleichungssystem $Ax = b$ auch

$$\left|\begin{array}{rcl} a_{11}x_1 + \cdots + a_{1n}x_n & = & b_1 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n & = & b_m \end{array}\right|$$

▶ **Bemerkung 9.3**
Das homogene System $Ax = 0$ hat als Lösungsraum den Untervektorraum $L(A, 0) = \mathrm{Ker}(f_A)$ der Dimension $\dim_K(L(A, 0)) = n - \mathrm{rk}(A)$. Das inhomogene System hat entweder $L(A, b) = \emptyset$ oder der Lösungsraum ist der affine Unterraum $L(A, b) = f^{-1}(b) = x_0 + L(A, 0)$, wobei $x_0 \in L(A, b)$ beliebig. Man erhält so alle Lösungen des inhomogenen Systems, wenn man eine Lösung und die Lösungen des homogenen Systems kennt.

Definition 9.4 (Zeilenstufenform)
Die Matrix $A = (a_{ij})$ hat Zeilenstufenform , wenn es ganze Zahlen $0 \leq r \leq m$ und $1 \leq k_1 < ... < k_r \leq n$ gibt mit:

- für $1 \leq i \leq r$ und $1 \leq j < k_i$ ist $a_{ij} = 0$
- für $1 \leq i \leq r$ ist $a_{ik_i} \neq 0$ (sogenannte Pivotelemente)
- für $r < i \leq m$ und $1 \leq j \leq n$ ist $a_{ij} = 0$

$$\begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & * & \dots & \dots & * \\ 0 & \dots & \dots & 0 & a_{2k_2} & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & a_{rk_r} \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$$

Lemma 9.5
Sei A in Zeilenstufenform. Dann ist $\mathrm{rk}(A) = r$.

Beweis. Wegen $\mathrm{rk}(A) = \mathrm{rk}(A^t) = \dim_K(\mathrm{ZR})$ genügt es zu zeigen, dass die ersten r Zeilen $a_1, ..., a_r$ linear unabhängig sind. Ist $\sum_{i=1}^{r} \lambda a_i = 0$, so ist insbesondere $0 = \sum_{i=1}^{r} \lambda_i a_{ik_i} = \lambda_1 a_{1k_1}$, also $\lambda_1 = 0$, und dann immer so weiter. □

Satz 9.6
Sei A in Zeilenstufenform.

- Ist $b_i \neq 0$ für ein $r < i \leq m$, so ist $L(A, b) = \emptyset$.
- Ist $b_i = 0$ für alle $r < i \leq m$, so erhält man alle $x \in L(A, b)$, indem man erst $x_j \in K$ für $j \in \{1, .., n\} \backslash \{k_1, ..., k_r\}$ beliebig wählt und dann für $i = r, r-1, ..., 1$ rekursiv $x_{k_i} = a_{1k_i}^{-1} \cdot (b_i - \sum_{j=k_i+1}^{n} a_{ij} \cdot x_j) \quad (*)$ setzt.

Beweis.
- Klar.
- Sicher erhält man auf diese Weise Lösungen $x \in L(A, b)$. Umgekehrt muss jede solche Lösung $(*)$ erfüllen, man erhält auf diese Weise also alle. □

Definition 9.7 (Elementarmatrizen)
Für $i, j \in \{1, ..., m\}$, $\lambda \in K^\times$ und $\mu \in K$ definieren wir $m \times m$-Matrizen, die sogenannten Elementarmatrizen :

- $S_i(\lambda) := \mathbb{1}_m + (\lambda - 1)E_{ii}$
- $Q_{ij}(\mu) := \mathbb{1}_m + \mu E_{ij}$
- $P_{ij} := \mathbb{1}_m + E_{ij} + E_{ji} - E_{ii} - E_{jj}$

▶ **Bemerkung 9.8**

Multiplikation einer dieser Matrizen von links an die Matrix A hat folgende Wirkung:

- $S_i(\lambda) \cdot A$: Multiplikation der i-ten Zeile mit λ
- $Q_{ij}(\mu) \cdot A$: Addition des μ-fachen der j-ten Zeile zur i-ten Zeile
- P_{ij}: Vertauschung von i-ter und j-ter Zeile

Man spricht dann von sogenannten elementaren Zeilenumformungen der Matrix A von Typ I, II oder III.

Lemma 9.9

Es sind $S_i(\lambda), Q_{ij}(\mu), P_{ij} \in \mathrm{GL}_m(K)$. Dann ist $S_i(\lambda)^{-1} = S_i(\lambda^{-1}), Q_{ij}(\mu)^{-1} = Q_{ij}(-\mu), P_{ij}^{-1} = P_{ij}$. Insbesondere gilt: Ist E eine der Elementarmatrizen, so ist $\mathrm{ZR}(EA) = \mathrm{ZR}(A)$ und $L(EA, 0) = L(A, 0)$. Weiterhin ist $\mathrm{rk}(EA) = \mathrm{rk}(A)$.

Beweis. Inverse nachprüfen. Da $E \in \mathrm{GL}_m(K)$ sind $f_E, f_{E^t} \in Aut_K(K^m)$, also $\mathrm{ZR}(EA) = \mathrm{SR}((EA)^t) = \mathrm{Im}(f_{A^tE^t}) = \mathrm{Im}(f_{A^t} \circ f_{E^t}) = \mathrm{Im}(f_{A^t}) = \mathrm{ZR}(A)$ und $L(EA, 0) = \mathrm{Ker}(f_{EA}) = \mathrm{Ker}(f_E \circ f_A) = \mathrm{Ker}(f_A) = L(A, 0)$. □

▶ **Bemerkung 9.10**

Anders gesagt: Elementare Zeilenumformungen verändern den Lösungsraum eines homogenen linearen Gleichungssystems nicht.

Theorem 9.11 (Eliminierungsverfahren nach Gauß)

Zu jeder Matrix $A \in \mathrm{Mat}_{m\times n}(K)$ gibt es $l \in \mathbb{N}_0$ und Elementarmatrizen $E_1, ..., E_l$ vom Typ II und III für die $E_l \cdot ... \cdot E_1 \cdot A$ in Zeilenstufenform ist.

Beweis. Seien $a_1, ..., a_n$ die Spalten von A.
Ist $A = 0$ so ist nichts zu tun.
Sei nun $A \neq 0$ und sei k_1 minimal mit $a_{k_1} \neq 0$. Es gibt also ein i mit $a_{ik_1} \neq 0$. Durch Vertauschen der ersten und der i-ten Zeile erreichen wir, dass $a_{1k_1} = 0$, d.h. wir multiplizieren A mit $E_1 = P_{1i}$. Nun addieren wir für $i = 2, .., m$ ein geeignetes Vielfaches der ersten Zeile zur i-ten Zeile, um $a_{ik_1} = 0$, d.h. wir multiplizieren A mit $E_i = Q_{i1}(\mu_i)$ für $\mu_i = \frac{a_{ik_1}}{a_{1k_1}}$. Nach diesen Umformungen haben wir eine Matrix der Form:

$$\begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & * & \dots & * \\ 0 & \dots & \dots & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & * & \dots & * \end{pmatrix}$$

und können nun mit dem Rest der Matrix $A =: A'$ von vorne beginnen. Die nun folgenden Zeilenumformungen werden die erste Zeile und die ersten k_1 Spalten nicht mehr ändern, und weil A' weniger Zeilen und Spalten als A hat, bricht das Verfahren nach endlich vielen Schritten ab. □

Mathematica/WolframAlpha-Befehle (Gauss-Verfahren)
Auch für das Gauss-Verfahren hat Mathematica bzw. WolframAlpha eine Funktion. Sie gibt die Matrix nach Ausführung des Gauss-Algorithmus zurück.

```
RowReduce[{{1, 4}, {2, 5}}]
```

Folgerung 9.12
Zu jeder Matrix A gibt es eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ für die SA in Zeilenstufenform ist.

Beweis. folgt direkt aus Theorem 9.11 mit $S = E_l \cdot ... \cdot E_1$ □

▶ **Bemerkung 9.13**
Der Beweis für das Eliminierungsverfahren (Theorem 9.11) liefert ein Verfahren, die Elementarmatrizen $E_1, ..., E_l$ zu finden. Damit erhält man ein Verfahren ein lineares Gleichungssystem zu lösen. Setzt man $S = E_l \cdot ... \cdot E_1$, $A' = SA$ und $b' = Sb$, so ist $L(A, b) = L(A', b')$: $Ax = b \Rightarrow SAx = Sb$ bzw. $A'x = b' \Rightarrow S^{-1}A'x = S^{-1}b'$.
Das Gleichungssystem kann dann mit Satz 9.6 gelöst werden. Praktisch führt man die elementaren Zeilenumformungen an A parallel dazu auch an b durch.

▶ **Bemerkung 9.14**
Es gibt von diesem Verfahren verschiedene Varianten und weitere Anwendungen: So kann man z.B. die Invertierbarkeit einer Matrix $A \in \mathrm{Mat}_n(K)$ prüfen und ggf. das Inverse bestimmen: Ist $E_l \cdot ... \cdot E_1 \cdot A$ in Zeilenstufenform, so ist A genau dann invertierbar, wenn alle Zeilen von Null verschieden sind. Ist dies der Fall, so ist $r = n$ und $k_i = i$ für alle i, und man findet weitere Elementarmatrizen $E_{l+1}, ..., E_s$ vom Typ I und II, für die $E_s \cdot ... \cdot E_1 \cdot A = \mathbb{1}_n$. Dann ist $S' = E_s \cdot ... \cdot E_1 \cdot A = A^{-1}$ (vgl. Folgerung 8.11). Praktisch erhält man A^{-1}, indem man die Zeilenumformungen an A parallel dazu auch an $\mathbb{1}_n$ ausführt.

Folgerung 9.15
Jedes $A \in \mathrm{GL}_m(K)$ ist ein Produkt von Elementarmatrizen.

Beweis. $A^{-1} = S' = E_s \cdot ... \cdot E_1 \Rightarrow A = (E_s \cdot ... \cdot E_1)^{-1} = E_1^{-1} \cdot ... \cdot E_s^{-1}$ □

Kapitel IV

Determinanten

1. Das Vorzeichen einer Permutation

In diesem Kapitel sei K ein Körper und R ein kommutativer Ring mit Einselement.

▶ **Bemerkung 1.1**
Wir erinnern uns an die symmetrische Gruppe S_n aus Beispiel 3.7, die aus den Permutationen der Menge $X = \{1, .., n\}$ (also den bijektiven Abbildungen $X \to X$) mit der Komposition als Verknüpfung. Es ist $|S_n| = n!$ und $S_2 \cong \mathbb{Z}\backslash 2\mathbb{Z}$, doch für $n \geq 3$ ist S_n nicht abelsch. Wir schreiben $\sigma_1\sigma_2$ für $\sigma_1 \circ \sigma_2$ und notieren $\sigma \in S_n$ auch als

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

■ **Beispiel 1.2**
Für $i, j \in \{1, ..., n\}$ mit $i \neq j$ bezeichne $\tau_{ij} \in S_n$ die Transposition

$$\tau_{ij}(k) = \begin{cases} j & \text{falls k=i} \\ i & \text{falls k=j} \\ k & \text{sonst} \end{cases}$$

Offenbar gilt $\tau_{ij}^2 = \mathrm{id}$, also $\tau_{ij}^{-1} = \tau_{ij} = \tau_{ji}$.

Satz 1.3
Für jedes $\sigma \in S_n$ gibt es ein $r \in \mathbb{N}_0$ und die Transpositionen $\tau_1, ..., \tau_r \in S_n$ mit

$$\sigma = \tau_1 \circ ... \circ \tau_r$$

Beweis. Sei $1 \leq k \leq n$ maximal mit $\sigma(i) = i$ für $i \leq k$. Induktion nach $n - k$.
Ist $n - k = 0$, so ist $\sigma = \mathrm{id}$ und wir sind fertig.
Andernfalls ist $l = k + 1 \leq n$ und $\sigma(l) > l$. Für $\sigma' = \tau_{l,\sigma(l)} \circ \sigma$ ist $\sigma(l) = l$ und somit $\sigma'(i) = i$ für $1 \leq i \leq k + 1$.
Nach Induktionshypothese gibt es Transpositionen $\tau_1, ..., \tau_r$ mit $\sigma' = \tau_1 \circ ... \circ \tau_r$. Es folgt $\sigma = \tau_{l,\sigma(l)}^{-1} \circ \sigma^{-1} = \tau_{l,\sigma(l)} \circ \tau_1 \circ ... \circ \tau_r$. □

Definition 1.4 (Fehlstand, Vorzeichen)
Sei $\sigma \in S_n$.

- Ein Fehlstand von σ ist ein Paar (i,j) mit $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$.
- Das Vorzeichen (oder Signum) von σ ist $\operatorname{sgn}(\sigma) = (-1)^{f(\sigma)} \in \{-1, 1\}$, wobei $f(\sigma)$ die Anzahl der Fehlstände von σ ist.
- Man nennt σ gerade , wenn $\operatorname{sgn}(\sigma) = 1$, sonst ungerade .

■ **Beispiel 1.5**

- Genau dann hat σ keine Fehlstände, wenn $\sigma = \mathrm{id}$. Insbesondere $\operatorname{sgn}(\mathrm{id}) = 1$.
- Die Permutation

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

  hat die Fehlstände $(1,3)$ und $(2,3)$, somit $\operatorname{sgn}(\sigma) = 1$.
- Die Transposition

$$\tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

  hat die Fehlstände $(1,2)$, $(2,3)$ und $(3,1)$, somit $\operatorname{sgn}(\tau_{13}) = -1$.
- Eine Transposition $\tau_{ij} \in S_n$ ist ungerade: Ist $i < j$, so sind die Fehlstände $(i, i+1), ..., (i,j)$ und $(j+1, j)...(j-1, j)$, also $j - (i+1) + 1 + (j-1) - (i-1) + 1 = 2(j-1) - 1$ viele.

Lemma 1.6
Für $\sigma \in S_n$ ist

$$\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{Q}$$

Beweis. Durchläuft (i,j) alle Paare $1 \leq i < j \leq n$, so durchläuft $\{\sigma(i), \sigma(j)\}$ alle zweielementigen Teilmengen von $\{1, ..., n\}$. Das Produkt $\prod_{i<j} \sigma(j) - \sigma(i)$ hat also bis auf das Vorzeichen die selben Faktoren wie das Produkt

$$\prod_{i<j} j - i = \prod_{i<j} |j - i|$$

und

$$\begin{aligned} \prod_{i<j} \sigma(j) - \sigma(i) &= \prod_{i<j, \sigma(i)<\sigma(j)} \sigma(j) - \sigma(i) \cdot \prod_{i<j, \sigma(i)>\sigma(j)} \sigma(j) - \sigma(i) \\ &= (-1)^{f(\sigma)} \cdot \prod_{i<j} |\sigma(j) - \sigma(i)| \\ &= \operatorname{sgn}(\sigma) \cdot \prod_{i<j} j - i \end{aligned}$$

□

Satz 1.7
Die Abbildung $\operatorname{sgn} : S_n \to \mathbb{Z}^\times = \mu_2$ ist ein Gruppenhomomorphismus.

Beweis. Seien $\sigma, \tau \in S_n$. Dann ist

$$\begin{aligned}\operatorname{sgn}(\sigma\tau) &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j-i} \\ &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{i<j} \frac{\tau(j) - \tau(i)}{j-i}\end{aligned}$$

Da mit $\{i, j\}$ auch $\{\tau(i), \tau(j)\}$ alle zweielementigen Teilmengen von $\{1, ..., n\}$ und

$$\frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)}$$

ist

$$\begin{aligned}\prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} &= \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j-i} \\ &= \operatorname{sgn}(\sigma)\end{aligned}$$

und

$$\prod_{i<j} \frac{\tau(j) - \tau(i)}{j-i} = \operatorname{sgn}(\tau)$$

Somit ist $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$. □

Folgerung 1.8
Für $\sigma \in S_n$ ist

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$$

Beweis. $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^{-1} = \operatorname{sgn}(\sigma)$ □

Folgerung 1.9
Sei $\sigma \in S_n$. Sind $\tau_1, ..., \tau_r$ Transpositionen mit $\sigma = \tau_1 \circ ... \circ \tau_r$, so ist

$$\operatorname{sgn}(\sigma) = (-1)^r$$

Beweis. Beispiel 1.5 und Satz 1.7 □

Folgerung 1.10
Die geraden Permutationen $A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ bilden einen Normalteiler von S_n, genannt die alternierende Gruppe . Ist $\tau \in S_n$ mit $\operatorname{sgn}(\tau) = -1$, so gilt für $A_n\tau = \{\sigma\tau \mid \sigma \in A_n\}$: $A_n \cup A_n\tau = S_n$ und $A_n \cap A_n\tau = \emptyset$.

Beweis. Es ist $A_n = Ker(\operatorname{sgn})$ und nach Lemma 2.13 ist dieser auch ein Normalteiler. Ist $\sigma \in S_n \backslash A_n$, so ist

$$\operatorname{sgn}(\sigma\tau^{-1}) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)^{-1} = (-1)(-1)^{-1} = 1$$

also $\sigma = \sigma\tau^{-1} \in A_n\tau$, somit $A_n \cup A_n\tau = S_n$. Ist $\sigma \in A_n$, so ist $\operatorname{sgn}(\sigma\tau) = -1$, also $A_n \cap A_n\tau = \emptyset$. □

2. Determinante einer Matrix

▶ **Bemerkung 2.1**

Wir werden nun auch Matrizen mit Koeffizienten in Ring R anstatt K betrachten. Mit der gewohnten Addition und Multiplikation bilden die $n \times n$-Matrizen einen Ring $\mathrm{Mat}_n(R)$, und wir definieren wieder $\mathrm{GL}_n(R) = \mathrm{Mat}_n(R)^\times$.

▶ **Bemerkung 2.2**

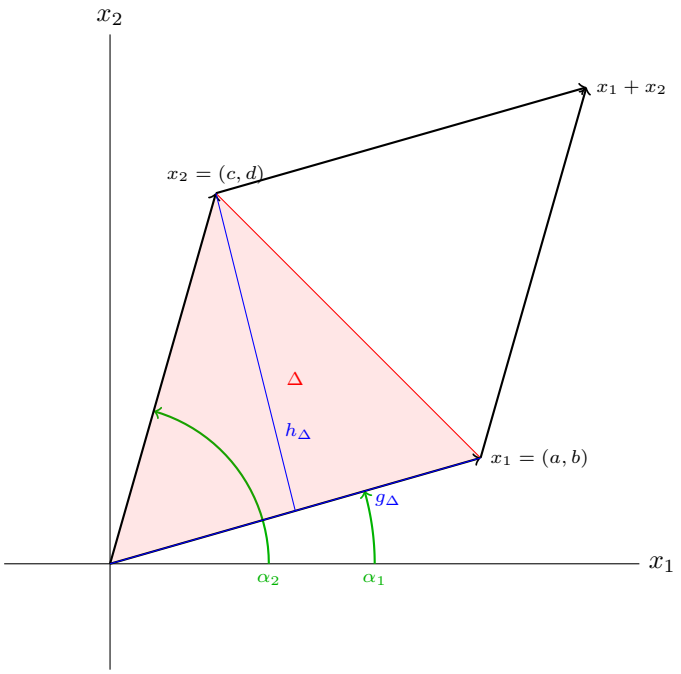
Seien $a_1, ..., a_n \in R^m$ Spaltenvektoren, so bezeichnen wir mit $A = (a_1, ..., a_n) \in \mathrm{Mat}_{m\times n}(R)$ die Matrix mit den Spalten $a_1, ..., a_n$. sind $\widetilde{a_1}, ..., \widetilde{a_m} \in R^n$ Zeilenvektoren, so bezeichnen wir mit $\tilde{A} = (\widetilde{a_1}, ..., \widetilde{a_m}) \in \mathrm{Mat}_{m\times n}(R)$ die Matrix mit den Zeilen $\widetilde{a_1}, ..., \widetilde{a_m}$.

▶ **Bemerkung 2.3**

Wir hatten bereits definiert: $\det(A) = ad - bc$ (Beispiel 1.13) mit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(K)$$

und hatten festgestellt: $\det(A) \neq 0 \iff A \in \mathrm{GL}_2(K)$. Interpretation im $K = \mathbb{R}$:



Parallelogramm hat die Fläche $|\det A|$. Polarkoordinaten: $x_i = \lambda_i(\cos a_i, \sin a_i)$. Ohne Einschränkung:

$0 \leq a_1 \leq a_2 \leq \pi$

$$F_P = 2 \cdot F_\Delta = 2 \cdot \frac{1}{2} \cdot g_\Delta \cdot h_\Delta$$
$$g_\Delta = \lambda_1$$
$$h_\Delta = \lambda_2 \cdot \sin(a_2 - a_1)$$
$$F_P = \lambda_1\lambda_2(\cos a_1 \sin a_2 - \sin a_1 \cos a_2) = \det(\begin{pmatrix} \lambda_1 \cos a_1 & \lambda_1 \sin a_1 \\ \lambda_2 \cos a_2 & \lambda_2 \sin a_2 \end{pmatrix})$$
$$= \det A$$

Insbesondere erfüllt det die folgenden Eigenschaften:

- Für $\lambda \in R$ ist $\det(\lambda x_1, x_2) = \det(x_1, \lambda x_2) = \lambda \cdot \det(x_1, x_2)$
- Für $x_i = x_i' + x_i''$ ist $\det(x_1, x_2) = \det(x_1', x_2) + \det(x_1'', x_2)$
- Ist $x_1 = x_2$, so ist $\det A = 0$
- $\det(\mathbb{1}_2) = 1$

Definition 2.4 (Determinantenabbildung)
Eine Abbildung $\delta : \mathrm{Mat}_n(R) \to R$ heißt Determinantenabbildung , wenn gilt:

- (D1): δ ist linear in jeder Zeile: sind $a_1, ..., a_n$ die Zeilen von A und ist $i \in \{1, ..., n\}$ und $a_i = \lambda' a_i' + \lambda'' a_i''$ mit $\lambda', \lambda'' \in R$ und den Zeilenvektoren a_i', a_i'', so ist $\delta(A) = \lambda' \cdot \delta(a_1, ..., a_i', ..., a_n) + \lambda'' \cdot \det(a_1, ..., a_i'', ..., a_n)$.
- (D2): δ ist alternierend: sind $a_1, ..., a_n$ die Zeilen von A und $i, j \in \{1, ..., n\}$, $i \neq j$ mit $a_i = a_j$, so ist $\delta(A) = 0$.
- (D3): δ ist normiert: $\delta(\mathbb{1}_n) = 1$.

Mathematica/WolframAlpha-Befehle (Determinante)
Die Determinante einer Matrix lässt sich in Mathematica bzw. WolframAlpha wie folgt berechnen:

```
Det[{{1, 4}, {2, 5}}]
```

■ **Beispiel 2.5**
Sei $\delta : \mathrm{Mat}_n(K) \to K$ eine Determinantenabbildung. Ist $A \in \mathrm{Mat}_n(K)$ nicht invertierbar, so sind die Zeilen $a_1, ..., a_n$ von A linear abhängig, es gibt also ein i mit $a_i = \sum_{j \neq i} \lambda_j \cdot a_j$. Es folgt $\delta(A) = \delta(a_1, ..., a_n) = \sum_{j \neq i} \lambda_j \cdot \delta(a_1, ..., a_j, ..., a_n)$ mit $a_i = a_j$ mit D2: $\sum_{j \neq i} \lambda_j \cdot 0 = 0 = \delta(A)$.

Lemma 2.6
Erfüllt $\delta : \mathrm{Mat}_n(R) \to R$ die Axiome D1 und D2, so gilt für jedes $\sigma \in S_n$ und die Zeilenvektoren $a_1, ..., a_n$:

$$\delta(a_{\sigma(1)}, ..., a_{\sigma(n)}) = \mathrm{sgn}(\sigma) \cdot \delta(a_1, ..., a_n)$$

Beweis. σ ist ein Produkt von Transpositionen. Es genügt also die Behauptung für $\sigma = \tau_{ij}$ mit $1 \leq i < j \leq n$ zu zeigen (Satz 1.7).

$$\begin{aligned}
0 &= \delta(a_1, ..., a_i + a_j, ..., a_j + a_i, ..., a_n) \\
&= \delta(a_1, ..., a_i, ..., a_j, ..., a_n) + \delta(a_1, ..., a_i, ..., a_i, ..., a_n) + \delta(a_1, ..., a_j, ..., a_j, ..., a_n) + \delta a_1, ..., a_j, ..., a_i, ..., a_n \\
&= \delta(a_1, ..., a_n) + \delta(a_{\sigma(1)}, ..., a_{\sigma(n)}) \\
&= 0
\end{aligned}$$

Mit $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_{ij}) = -1$ folgt die Behauptung. □

Lemma 2.7
Erfüllt $\delta : \mathrm{Mat}_n(R) \to R$ die Axiome D1 und D2, so gilt für $A = (a_{ij}) \in \mathrm{Mat}_n(R)$:

$$\delta(A) = \delta(\mathbb{1}_n) \cdot \sum_{\sigma \in S_n} \left(\prod_{i=1}^{n} a_{i,\sigma(i)} \right)$$

Beweis. Schreibe $a_i = (a_{j_1}, ..., a_{in}) = \sum_{j=1}^{n} a_{ij} \cdot e_j$. Wiederholtes Anwenden von D1 gibt

$$\begin{aligned}
\delta(A) &= \delta(a_1, ..., a_n) \\
&= \sum_{j_1=1}^{n} a_{1j_1} \cdot \delta(e_{j_1}, a_2, ..., a_n) \\
&= \sum_{j_1=1}^{n} ... \sum_{j_n=1}^{n} \delta(e_{j_1}, ..., e_{j_n}) \cdot \prod_{i=1}^{n} a_{ij_i}
\end{aligned}$$

Wegen D2 ist $\delta(e_{j_1}, ..., e_{j_n}) = 0$ falls $j_i = j_{i'}$ für ein $i \neq i'$. Andernfalls ist $\sigma(i) = j_i$ einer Permutation von $\{1, ..., n\}$ und

$$\begin{aligned}
\delta(e_{j_1}, ..., e_{j_n}) &= \delta(e_{\sigma(1)}, ..., e_{\sigma(n)}) \\
&= \operatorname{sgn}(\sigma) \cdot \delta(e_1, ..., e_n) \\
&= \operatorname{sgn}(\sigma) \cdot \delta(\mathbb{1}_n)
\end{aligned}$$

nach Lemma 2.6. □

Theorem 2.8
Es gibt genau eine Determinantenabbildung $\delta : \mathrm{Mat}_n(R) \to R$ und diese ist gegeben durch die Leibnitzformel

$$\det(a_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{\sigma \in A_n} \prod_{i=1}^{n} a_{i,\sigma(i)} - \sum_{\sigma \in S_n \setminus A_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Beweis. Eindeutigkeit der Abbildung folgt wegen D3 aus Lemma 2.7. Bleibt nur noch zu zeigen, dass det auch die Axiome D1 bis D3 erfüllt.
D1: klar
D3: klar

D2: Seien $\mu \neq v$ mit $a_\mu = a_v$. Mit $\tau = \tau_{\mu v}$ ist $S_n \backslash A_n = A_n \tau$, somit

$$\begin{aligned}\det(a_{ij}) &= \sum_{\sigma \in A_n} \prod_{i=1}^{n} a_{i,\sigma(i)} - \sum_{\sigma \in A_n \tau} \prod_{i=1}^{n} a_{i,\sigma\tau(i)} \\ &= \sum_{\sigma \in A_n} \left(\prod_{i=1}^{n} a_{i,\sigma(i)} - \prod_{i=1}^{n} a_{i,\sigma\tau(i)} \right)\end{aligned}$$

nach Folgerung 1.10. Da $a_{ij} = a_{\tau(i),j}$ für alle i, j ist

$$\begin{aligned}\prod_{i=1}^{n} a_{i,\sigma(i)} &= \prod_{i=1}^{n} a_{\tau(i),\sigma\tau(i)} \\ &= \prod_{i=1}^{n} a_{i,\sigma\tau(i)}\end{aligned}$$

für jedes $\sigma \in S_n$, woraus $\det(a_{ij}) = 0$ folgt. □

■ **Beispiel 2.9**

- $n = 2$, $S_2 = \{\mathrm{id}, \tau_{12}\}$,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

  $\det(A) = \sum_{\sigma \in S_2} a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$

- $n = 3$, $S_3 = \{id, \tau_{12}, \tau_{23}, \tau_{13}, 2 \text{ zyklische Vertauschungen}\}$, $A_3 = \{\mathrm{id}, 2 \text{ zyklische Vertauschungen}\}$, $S_3 \backslash A_3 = \{\tau_{12}, \tau_{23}, \tau_{13}\}$ und

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

  ergibt sich: $\det(A) = \sum_{\sigma \in A_3} a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot a_{3,\sigma(3)} - \sum_{\sigma \in S_3 \backslash A_3} a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot a_{3,\sigma(3)} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$

- Ist $A = (a_{ij})$ eine obere Dreiecksmatrix, so ist $\det(A) = \prod_{i=1}^{n} a_{ii}$
- Für $i \neq j$, $\lambda \in K^\times$, $\mu \in K$ ist $\det(S_i(\lambda)) = \lambda$, $\det(Q_{ij}(\mu)) = 1$, $\det(P_{ij}) = -1$
- Ist A eine Blockmatrix der Gestalt

$$\begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix}$$

  mit quadratischen Matrizen A_1, A_2, C, so ist $\det(A) = \det(A_1) \cdot \det(A_2)$

Folgerung 2.10
Für $A \in \mathrm{Mat}_n(R)$ ist $\det(A) = \det(A^t)$. Insbesondere erfüllt det die Axiome D1 und D2 auch für Spalten anstatt Zeilen.

Beweis. Mit $\rho = \sigma^{-1}$ gilt $\mathrm{sgn}(\rho) = \mathrm{sgn}(\sigma)$ nach Folgerung 1.8 und somit

$$\begin{aligned}\det(A) &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \\ &= \sum_{\rho \in S_n} \mathrm{sgn}(\rho) \cdot \prod_{i=1}^{n} a_{\rho(i),i} \\ &= \det(A^t)\end{aligned}$$

nach Theorem 2.8. □

Theorem 2.11 (Determinantenmultiplikationssatz)
Für $A, B \in \mathrm{Mat}_n(R)$ ist

$$\det(AB) = \det(A) \cdot \det(B)$$

Beweis. Fixiere A und betrachte die Abbildung $\delta : \mathrm{Mat}_n(R) \to R$ mit $B \mapsto \det(AB^{-1})$. Diese Abbildung erfüllt die Axiome D1 und D2. sind $b_1, ..., b_n$ die Zeilen von B, so hat AB^{-1} die Spalten $Ab_1^t, ..., Ab_n^t$, es werden die Eigenschaften von det auf δ übertragen.
$\Rightarrow \det(AB) = \delta(B^t) = \delta(\mathbb{1}_n) \cdot \det(B^t) = \det(A) \cdot \det(B)$. □

Folgerung 2.12
Die Abbildung $\det : \mathrm{Mat}_n(R) \to R$ schränkt sich zu einem Gruppenhomomorphismus $\mathrm{GL}_n(R) \to R^\times$ ein. Ist $R = K$ ein Körper, so ist $A \in \mathrm{Mat}_n(K)$ also genau dann invertierbar, wenn $\det(A) \neq 0$ und in diesem Fall ist $\det(A^{-1}) = \det(A)^{-1}$.

Beweis. Aus $AA^{-1} = \mathbb{1}_n$ folgt $\det(A^{-1}) * \det(A) = \det(\mathbb{1}_n) = 1$, insbesondere $\det(A) \in R^\times$. Der zweite Teil folgt wegen $K^\times = K \backslash \{0\}$ (Beispiel 2.5). □

Folgerung 2.13
Die Matrizen mit Determinante 1 bilden einen Normalteiler $\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n \mid \det(A) = 1\}$ der allgemeinen linearen Gruppe, die sogenannte spezielle lineare Gruppe .

Folgerung 2.14
Elementare Zeilenumformungen vom Typ II ändern die Determinante nicht, elementare Zeilenumformungen vom Typ III ändern nur das Vorzeichen der Determinante.

Beweis. $\det(Q_{ij}(\mu)A) = \det(Q_{ij}(\mu)) \cdot \det(A) = 1 \cdot \det(A) = \det(A)$ (Beispiel 2.9), Rest analog. □

▶ **Bemerkung 2.15**
Aus Folgerung 2.14 und Beispiel 2.9 erhält man eine praktische Methode zur Berechnung der Determinante. Man bringt die Matrix mit dem Gauss-Algorithmus Theorem 9.11 auf Zeilenstufenform, bildet das Produkt über die Diagonale und multipliziert mit -1, falls am eine ungerade Anzahl von Zeilenvertauschungen vorgenommen hat.

3. Minoren

Seien $m, n \in \mathbb{N}$.

Definition 3.1 (adjungierte Matrix)
Sei $A = (a_{ij}) \in \mathrm{Mat}_n(R)$. Für $i, j \in \{1, ..., n\}$ definieren wir die $n \times n$-Matrix:

$$A_{ij} = \begin{pmatrix} a_{11} & ... & a_{1,j-1} & 0 & a_{1,j+1} & ... & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & ... & a_{i-1,j.1} & 0 & a_{i-1,j+1} & ... & a_{i-1,n} \\ 0 & ... & 0 & 1 & 0 & ... & 0 \\ a_{i+1,1} & ... & a_{i+1,j.1} & 0 & a_{i+1,j+1} & ... & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & ... & a_{n,j-1} & 0 & a_{n,j+1} & ... & a_{nn} \end{pmatrix}$$

die durch Ersetzen der i-ten Zeile und der j-ten Spalte durch e_j aus A hervorgeht, sowie die $(n-1) \times (n-1)$- Matrix:

$$A'_{ij} = \begin{pmatrix} a_{11} & ... & a_{1,j-1} & a_{1,j+1} & ... & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & ... & a_{i-1,j.1} & a_{i-1,j+1} & ... & a_{i-1,n} \\ a_{i+1,1} & ... & a_{i+1,j.1} & a_{i+1,j+1} & ... & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & ... & a_{n,j-1} & a_{n,j+1} & ... & a_{nn} \end{pmatrix}$$

die durch Streichen der i-ten Zeile und der j-ten Spalten entsteht. Weiterhin definieren wir die zu A adjungierte Matrix als $A^{\#} = (a_{ij}^{\#}) \in \mathrm{Mat}_n(R)$, wobei $a_{ij}^{\#} = \det(A_{ji})$.

Lemma 3.2
Sei $A \in \mathrm{Mat}_n(R)$ mit Spalten $a_1, ..., a_n$. Für $i, j \in \{1, .., n\}$ gilt:

- $\det(A_{ij}) = (-1)^{i+j} \cdot \det(A'_{ij})$
- $\det(A_{ij}) = \det(a_1, ..., a_{j-1}, e_i, a_{j+1}, ..., a_n)$

Beweis.

- Durch geeignete Permutation der ersten i Zeilen und der ersten j Zeilen erhält man

$$\det(A_{ij}) = (-1)^{(i-1)+(j-1)} \cdot \det\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A'_{ij} & \\ 0 & & & \end{pmatrix}$$
$$\overset{2.9}{=} (-1)^{i+j} \cdot \det(\mathbb{1}_n) \cdot \det(A'_{ij})$$

- Man erhält A_{ij} aus $(a_1, ..., e_i, ..., a_n)$ durch elementare Spaltenumformungen vom Typ II. □

Satz 3.3
Für $A \in \mathrm{Mat}_n(R)$ ist

$$A^{\#} \cdot A = A \cdot A^{\#} = \det(A) \cdot \mathbb{1}_n$$

Beweis.

$$\begin{aligned}
(A^{\#}A)_{ij} &= \sum_{k=1}^{n} a^{\#}_{ik} \cdot a_{kj} \\
&= \sum_{k=1}^{n} a_{kj} \cdot \det(A_{kj}) \\
&\overset{3.2}{=} \sum_{k=1}^{n} a_{kj} \cdot \det(a_1, ..., a_{i-1}, a_j, a_{i+1}, ..., a_n) \\
&= \det(a_1, ..., a_{i-1}, \sum_{k=1}^{n} a_{kj} e_k, a_{i+1}, ..., a_n) \\
&= \det(a_1, ..., a_{i-1}, a_j, a_{i+1}, ..., a_n) \\
&= \delta_{ij} \cdot \det(A) \\
&= (\det(A) \cdot \mathbb{1}_n)_{ij}
\end{aligned}$$

Analog bestimmt man die Koeffizienten von $AA^{\#}$, wobei man $\det(A_{jk}) = \det(A^t_{jk}) = \det((A^t)_{kj})$ benutzt. □

Folgerung 3.4
Es ist $\mathrm{GL}_n(R) = \{A \in \mathrm{Mat}_n(R) \mid \det(A) \in R^\times\}$ und für $A \in \mathrm{GL}_n(R)$ ist $A^{-1} = \frac{1}{\det(A)} \cdot A^{\#}$.

Beweis. Satz 3.3 und Folgerung 2.12 □

Satz 3.5 (Laplace'scher Entwicklungssatz)
Sei $A = (a_{ij}) \in \mathrm{Mat}_n(R)$. Für jedes $i, j \in \{1, .., n\}$ gilt die Formel für die Entwicklung nach der i-ten Zeile:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A'_{ij})$$

Gleiches gilt auch für Spalten.

Beweis. Nach Satz 3.3 ist

$$\begin{aligned}\det(A) = (AA^{\#})_{ij} &= \sum_{j=1}^{n} a_{ij} \cdot a_{ij}^{\#} \\ &= \sum_{j=1}^{n} a_{ij} \cdot \det(A_{ij}) \\ &= \sum_{j=1}^{n} a_{ij} \cdot (-1)^{i+j} \cdot \det(A'_{ij})\end{aligned}$$

Analog auch für Spalten. □

Satz 3.6 (Cramer'sche Regel)
Sei $A \in \mathrm{GL}_n(R)$ mit Spalten $a_1, ..., a_n$ und sei $b \in R^n$. Weiter sei $x = (x_1, ..., x_n)^t \in R^n$ die eindeutige Lösung des Linearen Gleichungssystems $Ax = b$. Dann ist für $i = 1, ..., n$

$$x_i = \frac{\det(a_1, ..., a_{i-1}, b, a_{i+1}, ..., a_n)}{\det(A)}$$

Beweis.

$$\begin{aligned}x_i &= (A^{-1}b)_i \\ &= \sum_{j=1}^{n} (A^{-1})_{ij} \cdot b_j \\ &\overset{3.4}{=} \frac{1}{\det(A)} \cdot \sum_{j=1}^{n} a_{ij}^{\#} \cdot b_j \\ &\overset{3.2}{=} \frac{1}{\det(A)} \cdot \sum_{j=1}^{n} b_j \cdot \det(a_1, ..., a_{i-1}, e_i, a_{i+1}, ..., a_n) \\ &= \frac{1}{\det(A)} \cdot \det(a_1, ..., a_{i-1}, b_j, a_{i+1}, ..., a_n)\end{aligned}$$ □

Definition 3.7 (Minor)
Sei $A = (a_{ij}) \in \mathrm{Mat}_{m \times n}(R)$ und $1 \leq r \leq m$, $1 \leq s \leq n$. Eine $r \times s$- Teilmatrix von A ist eine Matrix der Form $(a_{i\mu, jv})_{\mu,v} \in \mathrm{Mat}_{r \times s}(R)$ mit $1 \leq i_1 < ... < i_r \leq m$ und $1 \leq j_1 < ... < j_s \leq n$. Ist A' eine $r \times r$-Teilmatrix von A, so bezeichnet man $\det(A')$ als einen r-Minor von A.

■ **Beispiel 3.8**
Ist $A \in \mathrm{Mat}_n(R)$ und $i, j \in \{1, ..., n\}$, so ist A'_{ij} eine Teilmatrix und $\det(A'_{ij}) = (-1)^{i+j} \cdot a_{ji}^{\#}$ ein $(n-1)$-Minor von A.

Satz 3.9
Sei $A \in \mathrm{Mat}_n(R)$ und $r \in \mathbb{N}$. Genau dann ist $\mathrm{rk}(A) \geq r$, wenn es eine $r \times r$- Teilmatrix A' von A mit $\det(A') \neq 0$ gibt.

Beweis.
- Hinrichtung: Ist $\mathrm{rk}(A) \geq r$, so hat A r linear unabhängige Spalten $a_1, ..., a_r$. Die Matrix $\tilde{A} = (a_1, ..., a_r)$ hat den Rang r und deshalb r linear unabhängige Zeilen $\widetilde{a_1}, ..., \widetilde{a_r}$. Die $r \times r$-Matrix A hat dann Rang r, ist also invertierbar, und $\det(A) \neq 0$.

- Rückrichtung: Ist A' eine $r \times r$-Teilmatrix von A mit $\det(A') \neq 0$, so ist $\mathrm{rk}(A) \geq \mathrm{rk}(A') = r$. □

Folgerung 3.10
Sei $A \in \mathrm{Mat}_{m\times n}(K)$. Der Rang von A ist das größte $r \in \mathbb{N}$, für das A einen von Null verschiedenen r-Minor hat.

4. Determinante und Spur von Endomorphismen

Sei $n \in \mathbb{N}$ und V ein K-Vektorraum mit $\dim_K(V) = m$.

Satz 4.1
Sei $f \in \mathrm{Hom}_K(V,W)$, A' eine Basis von V und $A = M_{A'}(f)$. Sei weiter $B \in \mathrm{Mat}_n(K)$. Genau dann gibt es eine Basis B' von V mit $B = M_{B'}(f)$, wenn es $S \in \mathrm{GL}_n(K)$ mit $B = SAS^{-1}$ gibt.

Beweis. Ist B' eine Basis von V mit $B = M_{B'}(f)$, so ist $B = SAS^{-1}$ mit $S = T_{B'}^{A'}$. Sei umgekehrt $B = SAS^{-1}$ mit $S \in \mathrm{GL}_n(K)$. Es gibt eine Basis B' von V mit $T_{B'}^{A'} = S$, also $M_{B'}(f) = T_{B'}^{A'} \cdot M_{A'}(f) \cdot (T_{B'}^{A'})^{-1} = SAS^{-1} = B$: Mit $B' = (\Phi_{A'}(f_s^{-1}(e_1)), ..., \Phi_{A'}(f_s^{-1}(e_n)))$ ist $\Phi_{A'} \circ f_s^{-1} = \mathrm{id}_V \circ \Phi_{B'}$, also $T_{B'}^{A'} = M_{A'}^{A'}(\mathrm{id}_V) = S^{-1}$. Folglich ist $T_{B'}^{A'} = (T_{A'}^{B'})^{-1} = (S^{-1})^{-1} = S$ nach Satz 6.2. □

Definition 4.2 (Ähnlichkeit)
Zwei Matrizen $A, B \in \mathrm{Mat}_n(R)$ heißen ähnlich , wenn (in Zeichen $A \sim B$) es $S \in \mathrm{GL}_n(R)$ mit $B = SAS^{-1}$ gibt.

Satz 4.3
Ähnlichkeit von Matrizen ist eine Äquivalenzrelation auf $\mathrm{Mat}_n(R)$.

Beweis.
- Reflexivität: $A = \mathbb{1}_n \cdot A \cdot (\mathbb{1}_n)^{-1}$
- Symmetrie: $B = SAS^{-1} \Rightarrow A = S^{-1}BS = S^{-1}B(S^{-1})^{-1}$
- Transitivität: $B = SAS^{-1}$, $C = TBT^{-1} \Rightarrow C = TSAS^{-1}T^{-1} = (TS)A(ST)^{-1}$ □

Satz 4.4
Seien $A, B \in \mathrm{Mat}_n(R)$. Ist $A \sim B$, so ist

$$\det(A) = \det(B)$$

Beweis. $B = SAS^{-1}$, $S \in \mathrm{GL}_n(R)$, $\det(B) = \det(S) \cdot \det(A) \cdot \det(S)^{-1} = \det(A)$ nach Theorem 2.11 und Folgerung 2.12 □

Definition 4.5 (Determinante eines Endomorphismus)
Die Determinante eines Endomorphismus $f \in \mathrm{End}_K(V)$ ist

$$\det(f) = \det(M_B(f))$$

wobei B eine Basis von V ist. (Diese ist wohldefiniert nach Satz 4.1 und Satz 4.4)

Satz 4.6
Für $f, g \in \mathrm{End}_K(V)$ gilt:
- $\det(\mathrm{id}_V) = 1$
- $\det(f \circ g) = \det(f) \cdot \det(g)$
- Genau dann ist $\det(f) \neq 0$, wenn $f \in \mathrm{Aut}_K(V)$. In diesem Fall ist $\det(f^{-1}) = \det(f)^{-1}$

Beweis.
- klar
- folgt aus Folgerung 6.6 und Theorem 2.11
- folgt aus Folgerung 6.5 und Folgerung 2.12 □

Definition 4.7 (Spur einer Matrix)
Die Spur einer Matrix $A = (a_{ij}) \in \mathrm{Mat}_n(R)$ ist

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$$

Mathematica/WolframAlpha-Befehle (Spur einer Matrix)
Auch für die Spur einer Matrix hat Mathematica bzw. WolframAlpha eine Funktion:

```
Tr[{{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}]
```

Lemma 4.8
Seien $A, B \in \mathrm{Mat}_n(R)$
- $\mathrm{tr} : \mathrm{Mat}_n(R) \to R$ ist R-linear
- $\mathrm{tr}(A^t) = \mathrm{tr}(A)$
- $\mathrm{tr}(AB) = \mathrm{tr}(BA)$

Beweis. in den Übungen bereits behandelt □

Satz 4.9
Seien $A, B \in \mathrm{Mat}_n(R)$. Ist $A \sim B$, so ist $\mathrm{tr}(A) = \mathrm{tr}(B)$.

Beweis. $B = SAS^{-1}$, $S \in \mathrm{GL}_n(R) \Rightarrow \mathrm{tr}(B) = \mathrm{tr}(SAS^{-1}) \overset{4.8}{=} \mathrm{tr}(AS^{-1}S) = \mathrm{tr}(A)$ □

Definition 4.10 (Spur eines Endomorphismus)
Die Spur eines Endomorphismus $f \in \mathrm{End}_K(V)$ ist

$$\mathrm{tr}(f) = \mathrm{tr}(M_B(f))$$

wobei B eine Basis von V ist (Diese ist wohldefiniert nach Satz 4.1 und Satz 4.9)

▶ **Bemerkung 4.11**
Im Fall $K = \mathbb{R}$ kann man wie in Bemerkung 2.3 den Absolutbetrag der Determinante eines $f \in \mathrm{End}_K(K^n)$ geometrisch interpretieren, nämlich als das Volumen von $f(Q)$, wobei $Q = [0,1]^n$ der Einheitsquader ist, und somit als Volumenänderung durch f. Auch das Vorzeichen von $\det(f)$ hat eine Bedeutung: Es gibt an, ob f orientierungserhaltend ist. Für erste Interpretationen der Spur siehe A100.

Kapitel V

Endomorphismen

In diesem Kapitel seien K ein Körper, $n \in \mathbb{N}$ eine natürliche Zahl, V ein n-dimensionaler K-VR und $f \in \mathrm{End}_K(V)$ ein Endomorphismus.

Das Ziel dieses Kapitels ist, die Geometrie von f besser zu verstehen und Basen zu finden, für die $M_B(f)$ eine besonders einfache oder kanonische Form hat.

1. Eigenwerte

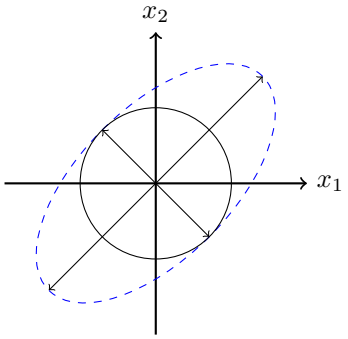
▶ **Bemerkung 1.1**
Wir erinnern uns daran, dass $\mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)$ sowohl einen K-VR als auch einen Ring bildet. Bei der Wahl einer Basis B von V wird $f \in \mathrm{End}_K(V)$ durch die Matrix $M_B(f) = M_B^B(f)$ beschrieben.

■ **Beispiel 1.2**
$K = \mathbb{R}, A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R}), f = f_A \in \mathrm{End}_K(K^2)$

$$A \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix}, \; A \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$\Rightarrow$ mit $B = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$ ist $M_B(f) = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}$.

Der Endomorphismus $f = f_A$ streckt also entlang der Achse $\mathbb{R} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ um den Faktor 3 und spiegelt entlang der Achse $\mathbb{R} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}$



Definition 1.3 (Eigenwert, Eigenvektor, Eigenraum)
Sind $0 \neq x \in V$ und $\lambda \in K$ mit $f(x) = \lambda x$ so nennt man λ einen Eigenwert von f und x einen Eigenvektor von f zum Eigenwert λ. Der Eigenraum zu $\lambda \in K$ ist $\mathrm{Eig}(f, \lambda) = \{x \in V \mid f(x) = \lambda x\}$.

▶ **Bemerkung 1.4**
Für jedes $\lambda \in K$ ist $\mathrm{Eig}(f, \lambda)$ ein UVR von V, da

$$\begin{aligned}\mathrm{Eig}(f, \lambda) &= \{x \in V \mid f(x) = \lambda x\} \\ &= \{x \in V \mid f(x) - \lambda \cdot \mathrm{id}_V(x) = 0\} \\ &= \{x \in V \mid (f - \lambda \cdot \mathrm{id}_V)(x) = 0\} \\ &= \mathrm{Ker}(f - \lambda \cdot \mathrm{id}_V)\end{aligned}$$

und $f - \lambda \cdot \mathrm{id}_V \in \mathrm{End}_K(V)$.

▶ **Bemerkung 1.5**
Achtung! Der Nullvektor ist nach Definition kein Eigenvektor, aber $\lambda = 0$ kann ein Eigenwert sein, nämlich genau dann, wenn $f \notin \mathrm{Aut}_K(V)$, siehe Übung. Die Menge der Eigenvektoren zu λ ist also $\mathrm{Eig}(f, \lambda) \backslash \{0\}$ und λ ist genau dann ein Eigenwert von f, wenn $\mathrm{Eig}(f, \lambda) \neq \{0\}$.

■ **Beispiel 1.6**
Ist $A = \mathrm{diag}(\lambda_1, ..., \lambda_n)$ und $f = f_A \in \mathrm{End}_K(K^n)$, so sind $\lambda_1, ..., \lambda_n$ EW von f und jedes e_i ist ein EV zum EW λ_i.

Satz 1.7
Sei B eine Basis von V. Genau dann ist $M_B(f)$ eine Diagonalmatrix, wenn B aus EV von f besteht.

Beweis. Ist $B = (x_1, ...x_n)$ eine Basis aus EV zu EW $\lambda_1, ..., \lambda_n$, so ist $M_B(f) = \mathrm{diag}(\lambda_1, ..., \lambda_n)$ und umgekehrt. □

■ **Beispiel 1.8**
Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$ und $f_\alpha \in \mathrm{End}_K(\mathbb{R}^2)$ die Drehung um den Winkel $\alpha \in [0, 2\pi)$

$$\Rightarrow M_{\mathcal{E}}(f_\alpha) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

Für $\alpha = 0$ hat $f_\alpha = \mathrm{id}_{\mathbb{R}^2}$ nur den EW 1.
Für $\alpha = \pi$ hat $f_\alpha = -\mathrm{id}_{\mathbb{R}^2}$ nur den EW -1.
Für $\alpha \neq 0, \pi$ hat f_α keine EW.

Lemma 1.9
Sind $\lambda_1, ..., \lambda_n$ paarweise verschiedene EW von f und ist x_i ein EV zu λ_i für $i = 1, ..., m$, so ist $(x_1, ..., x_m)$ linear unabhängig.

Beweis. Induktion nach m
$m = 1$: klar, denn $x_1 \neq 0$

$\underline{m-1 \to m}$: Sei $\sum_{i=1}^{m} \mu_i x_i = 0$ mit $\mu_1, ..., \mu_m \in K$.

$$\begin{aligned} 0 &= (f - \lambda \cdot \mathrm{id}_V) \left(\sum_{i=1}^{m} \mu_i x_i \right) \\ &= \sum_{i=1}^{m} \mu_i (f(x_i) - \lambda_m \cdot x_i) \\ &= \sum_{i=1}^{m-1} \mu_i (\lambda_i - \lambda_m) \cdot x_i \end{aligned}$$

Nach IB ist $\mu_i(\lambda_i - \lambda_m) = 0$ für $i = 1, ..., m-1$, da $\lambda_i \neq \lambda_m$ für $i \neq m$ also $\mu_i = 0$ für $i = 1, ..., m-1$. Damit ist auch $\mu_m = 0$. Folglich ist $(x_1, ..., x_m)$ linear unabhängig. □

Satz 1.10
Sind $\lambda_1, ..., \lambda_m \in K$ paarweise verschieden, so ist

$$\sum_{i=1}^{m} \mathrm{Eig}(f, \lambda_i) = \bigoplus_{i=0}^{m} \mathrm{Eig}(f, \lambda_i).$$

Beweis. Seien $x_i, y_i \in \mathrm{Eig}(f, \lambda_i)$ für $i = 1, ..., m$. Ist $\sum_{i=1}^{m} x_i = \sum_{i=1}^{m} y_i$, so ist $\sum_{i=1}^{m} \underbrace{x_i - y_i}_{z_i} = 0$.

o. E. seien $z_i \neq 0$ für $i = 1, ..., r$ und $z_i = 0$ für $i = r+1, ..., m$. Wäre $r > 0$, so wären $(z_1, ..., z_r)$ linear abhängig, aber $z_i = x_i - y_i \in \mathrm{Eig}(f, \lambda_i) \backslash \{0\}$, im Widerspruch zu Lemma 1.9. Somit ist $x_i = y_i$ für alle i und folglich ist die Summe $\sum \mathrm{Eig}(f, \lambda_i)$ direkt. □

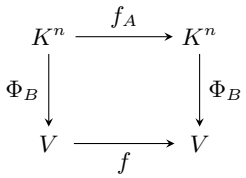
Definition 1.11 (EW und EV für Matrizen)
Sei $A \in \mathrm{Mat}_n(K)$. Man definiert Eigenwerte, Eigenvektoren, etc von A als Eigenwerte, Eigenvektoren von $f_A \in \mathrm{End}_K(K^n)$.

Mathematica/WolframAlpha-Befehle (Eigenwerte und Eigenvektoren)
Um die Eigenwerte und Eigenvektoren einer Matrix A zu berechnen, gibt es in Mathematica bzw. WolframAlpha verschiedene Möglichkeiten:

- `Eigenvalues[A]`: liefert eine Liste der Eigenwerte
- `Eigenvectors[A]`: liefert eine Liste der Eigenvektoren
- `Eigensystem[A]`: liefert zu jeden Eigenwert den Eigenvektor

Satz 1.12
Sei B eine Basis von V und $\lambda \in K$. Genau dann ist λ ein EW von f, wenn λ ein EW von $A = M_B(f)$ ist. Insbesondere haben ähnliche Matrizen die selben EW.

Beweis. Dies folgt aus dem kommutativen Diagramm



denn $f_A(x) = \lambda x \iff (\Phi_B \circ f_A)(x) = \Phi_B(\lambda x) \iff f(\Phi_B(x)) = \lambda \Phi_B(x)$.
Ähnliche Matrizen beschreiben den selben Endomorphismus bezüglich verschiedener Basen, vgl. Satz 4.1 □

2. Das charakteristische Polynom

Satz 2.1
Sei $\lambda \in K$. Genau dann ist λ ein EW von f, wenn $\det(\lambda \cdot \mathrm{id}_V - f) = 0$.

Beweis. Da $\mathrm{Eig}(f, \lambda) = \mathrm{Ker}(\lambda \cdot \mathrm{id}_V - f)$ ist λ genau dann ein EW von f, wenn $\dim_K(\mathrm{Ker}(\lambda \cdot \mathrm{id}_V - f)) > 0$, also wenn $\lambda \cdot \mathrm{id}_V - f \notin \mathrm{Aut}_K(V)$. Nach Satz 4.6 bedeutet dies, dass $\det(\lambda \cdot \mathrm{id}_V - f) = 0$ □

Definition 2.2 (charakteristisches Polynom)
Das charakteristische Polynom einer Matrix $A \in \mathrm{Mat}_n(K)$ ist die Determinante der Matrix $t \cdot \mathbb{1}_n - A \in \mathrm{Mat}_n(K[t])$.

$$\chi_A(t) = \det(t \cdot \mathbb{1}_n - A) \in K[t]$$

Das charakteristische Polynom eines Endomorphismus $f \in \mathrm{End}_K(V)$ ist $\chi_f(t) = \chi_{M_B(f)}(t)$, wobei B eine Basis von V ist.

Mathematica/WolframAlpha-Befehle (charakteristisches Polynom)
Die folgende Funktion liefert das charakteristische Polynom einer Matrix A mit der Variable x

```
CharacteristicPolynomial[A,x]
```

Satz 2.3
Sind $A, B \in \mathrm{Mat}_n(K)$ mit $A \sim B$, so ist $\chi_A = \chi_B$. Insbesondere ist χ_f wohldefiniert.

Beweis. Ist $B = SAS^{-1}$ mit $S \in \mathrm{GL}_n(K)$, so ist $t \cdot \mathbb{1}_n - B = S(t \cdot \mathbb{1}_n - A)S^{-1}$, also $t \cdot \mathbb{1}_n - B \sim t \cdot \mathbb{1}_n - A$ und ähnliche Matrizen haben die selben Determinante Satz 4.4.
Sind B, B' Basen von V, so sind $M_B(f) \sim M_{B'}(f)$, also $\chi_{M_B(f)} = \chi_{M_{B'}(f)}$ □

Lemma 2.4
Für $\lambda \in K$ ist $\chi_f(\lambda) = \det(\lambda \cdot \mathrm{id}_V - f)$.

Beweis. Sei B eine Basis von V und $A = M_B(f) = (a_{ij})_{i,j}$. Dann ist $M_B(\lambda \cdot \mathrm{id}_V - f) = \lambda \cdot \mathbb{1}_n - A$. Aus IV.2.8 und I.6.8 folgt $\det(t \cdot \mathbb{1}_n - A)(\lambda) = \det(\lambda \cdot \mathbb{1}_n - A)$. Folglich ist

$$\begin{aligned}
\chi_f(\lambda) &= \chi_A(\lambda) \\
&= \det(t \cdot \mathbb{1}_n - A)(\lambda) \\
&= \det(\lambda \cdot \mathbb{1}_n - A) \\
&= \det(\lambda \cdot \mathrm{id}_V - f)
\end{aligned}$$

□

Satz 2.5
Sei $\dim_K(V) = n$ und $f \in \mathrm{End}_K(V)$. Dann ist $\chi_f(t) = \sum_{i=0}^{n} \alpha_i t^i$ ein Polynom vom Grad n mit

$$\begin{aligned} \alpha_n &= 1 \\ \alpha_{n-1} &= -\operatorname{tr}(f) \\ \alpha_0 &= (-1)^n \cdot \det(f) \end{aligned}$$

Die Nullstellen von χ_f sind genau die EW von f.

Beweis. Sei B eine Basis von V und $A = M_B(f) = (a_{ij})_{i,j}$. Wir erinnern uns daran, dass $\operatorname{tr}(f) = \operatorname{tr}(A = \sum_{i=1}^{n} a_{ii}$. Es ist $\chi_f(t) = \det(t - \cdot 1_n - A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (t\delta_{i,\sigma(i)} - a_{i,\sigma(i)})$.
Der Summand für $\underline{\sigma = \mathrm{id}}$ ist $\prod_{i=1}^{n}(t - a_{ii}) = t^n + \sum_{i=1}^{n}(-a_{ii})t^{n-1} + \ldots + \prod_{i=1}^{n}(-a_{ii})$
Für $\underline{\sigma \neq \mathrm{id}}$ ist $\sigma(i) \neq i$ für mindestens zwei i, der entsprechende Summand hat also Grad höchstens $n-2$. Somit haben α_n und α_{n-1} die oben behauptete Form, und $\alpha_0 = \chi_A(0) = \det(-A) = (-1)^n \cdot \det(f)$.
Die Aussage über die Nullstellen von χ_f folgt aus Satz 2.1 und Lemma 2.4. □

Folgerung 2.6
Ist $\dim_K(V) = n$, so hat f höchstens n Eigenwerte.

Beweis. Satz 2.5 und Folgerung 6.10 □

Definition 2.7 (normiertes Polynom)
Ein Polynom $0 \neq P \in K[t]$ mit Leitkoeffizient 1 heißt $\underline{\text{normiert}}$.

■ **Beispiel 2.8**

1. Ist $A = (a_{ij})_{i,j}$ eine obere Dreiecksmatrix, so ist $\chi_A(t) = \prod_{i=1}^{n}(t - a_{ii})$, vgl. Beispiel 2.9
   Insbesondere ist $\chi_{1_n}(t) = (t-1)^n$, $\chi_0(t) = t^n$
2. Für eine Blockmatrix $A = \begin{pmatrix} A_1 & B \\ 0 & A_2 \end{pmatrix}$ mit quadratischen Matrizen A_1, A_2 ist $\chi_A = \chi_{A_1} \cdot \chi_{A_2}$
   vgl. Beispiel 2.9
3. Für

$$\begin{pmatrix} 0 & \ldots & \ldots & \ldots & 0 & -c_0 \\ 1 & \ddots & & & \vdots & \vdots \\ 0 & \ddots & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & -c_{n-1} \end{pmatrix} \quad c_0, \ldots, c_{n-1} \in K$$

   ist $\chi_A(t) = t^n + \sum_{i=0}^{n-1} c_i t^i$
   Man nennt diese Matrix die Begleitmatrix zum normierten Polynom $P = t^n + \sum_{i=0}^{n-1} c_i t^i$ und schreibt $M_P := A$

3. Diagonalisierbarkeit

Definition 3.1 (diagonalisierbar)
Man nennt f diagonalisierbar , wenn V eine Basis B besitzt, für die $M_B(f)$ eine Diagonalmatrix ist.

Lemma 3.2
Genau dann ist f diagonalisierbar, wenn

$$V = \sum_{\lambda \in K} \mathrm{Eig}(f, \lambda)$$

.

Beweis. ($\Rightarrow$): Ist B eine Basis aus EV von f (vgl. Satz 1.7), so ist $B \leq \bigcup_{\lambda \in K} \mathrm{Eig}(f, \lambda)$, also $V = \mathrm{span}_K(\bigcup_{\lambda \in K} \mathrm{Eig}(f, \lambda)) = \sum_{\lambda \in K} \mathrm{Eig}(f, \lambda)$.
($\Leftarrow$): Ist $V = \sum_{\lambda \in K} \mathrm{Eig}(f, \lambda)$, so gibt es $\lambda_1, ..., \lambda_n \in K$ mit $V = \sum_{i=1}^{r} \mathrm{Eig}(f, \lambda_i)$. Wir wählen Basen B_i von $\mathrm{Eig}(f, \lambda_i)$. Dann ist $\bigcup_{i=1}^{r} B_i$ ein endliches Erzeugendensystem von V, enthält also eine Basis von V (Theorem 3.6). Diese besteht aus EV von f. □

Satz 3.3
Ist $\dim_K(V) = n$, so hat f höchstens n Eigenwerte. Hat f genau n Eigenwerte, so ist f diagonalisierbar.

Beweis. Ist λ ein EW von f, so ist $\dim_K(\mathrm{Eig}(f, \lambda)) \geq 1$. Sind also $\lambda_1, ..., \lambda_n$ paarweise verschiedene EW von f, so ist

$$\begin{aligned} n = \dim_K(V) &\geq \dim_K \left(\sum_{i=1}^{m} \mathrm{Eig}(f, \lambda_i) \right) \\ &\overset{1.10}{=} \dim_K \left(\bigoplus_{i=0}^{m} \mathrm{Eig}(f, \lambda_i) \right) \\ &= \sum_{i=1}^{m} \dim_K(\mathrm{Eig}(f, \lambda_i)) \\ &\geq m \end{aligned}$$

Ist zudem $m = n$, so muss

$$\dim_K(V) = \dim_K(\sum_{i=1}^{m} \mathrm{Eig}(f, \lambda_i)) \text{ sein, also}$$
$$V = \sum_{i=1}^{m} \mathrm{Eig}(f, \lambda_i)$$

Nach Lemma 3.2 ist f genau dann diagonalisierbar. □

Definition 3.4 (a teilt b)
Sei R ein kommutativer Ring mit seien $a, b \in R$. Man sagt, a teilt b (in Zeichen $a \mid b$), wenn es $x \in R$ mit $b = ax$ gibt.

Definition 3.5 (Vielfachheit)
Für $0 \neq P \in K[t]$ und $\lambda \in K$ nennt man $\mu(P,\lambda) = \max\{r \in \mathbb{N}_{>0} \mid (t-r)^r \mid P\}$ die Vielfachheit der Nullstelle λ von P.

Lemma 3.6
Genau dann ist $\mu(P,\lambda) \geq 1$, wenn λ eine Nullstelle von P ist.

Beweis. ($\Rightarrow$): $(t-\lambda) \mid P \Rightarrow P(t) = (t-\lambda)\cdot Q(t)$ mit $Q(t) \in K[t] \Rightarrow P(\lambda) = 0 \cdot Q(\lambda) = 0$.
($\Leftarrow$): $P(\lambda) = 0 \overset{6.9}{=} (t-\lambda) \mid P(t) \Rightarrow \mu(P,\lambda) \geq 1$. □

Lemma 3.7
Ist $P(t) = (t-\lambda)^r \cdot Q(t)$ mit $Q(t) \in K[t]$ und $Q(\lambda) \neq 0$, so ist $\mu(P,\lambda) = r$

Beweis. Offensichtlich ist $\mu(P,\lambda) \geq r$. Wäre $\mu(P,\lambda) \geq r+l$, so $(t-\lambda)^{r+l} \mid P(t)$ also $(t-\lambda)^r \cdot Q(t) = (t-\lambda)^{r+l} \cdot R(t)$ mit $R(t) \in K[t]$, folglich $(t-\lambda) \mid Q(t)$, insbesondere $Q(\lambda) = 0$.
(Denn wir dürfen kürzen: R ist nullteilerfrei, genau so wie $K[t]$).
$(t-\lambda)^r(Q(t) - (t-\lambda)R(t)) = 0 \Rightarrow Q(t) = (t-\lambda)R(t)$. □

Lemma 3.8
Sind $P, Q, R \in K[t]$ mit $PQ = PR$, und ist $P \neq 0$, so ist $Q = R$.

Beweis. $PQ = PR \Rightarrow P(Q-R) = 0 \overset{K[t] \text{ nullteilerfrei}}{\Rightarrow} Q - R = 0$, d.h. $Q = R$. □

Lemma 3.9
Es ist $\sum_{\lambda \in K} \mu(P,\lambda) \leq \deg(P)$, mit Gleichheit genau dann, wenn P in Linearfaktoren zerfällt.

Beweis. Schreibe $P(t) = \prod_{\lambda \in K}(t-\lambda)^{r_\lambda} \cdot Q(t)$, wobei $Q(t) \in K[t]$ keine Nullstellen mehr besitzt. Nach Lemma 3.7 ist $\mu(P,\lambda) = r_\lambda$ für alle λ und somit $\deg(P) = \sum_{\lambda \in K} r_\lambda + \deg(Q) \geq \sum_{\lambda \in K} \mu(P,\lambda)$ mit Gleichheit genau dann,wenn $\deg(Q) = 0$, also $Q = c \in K$, d.h. genau dann, wenn $P(t) = c \cdot \prod_{\lambda \in K}(t-\lambda)^{r_\lambda}$. □

Lemma 3.10
Für $\lambda \in K$ ist

$$\dim_K(\mathrm{Eig}(f,\lambda)) \geq \mu(x_f,\lambda)$$

Beweis. Ergänze eine Basis B von $\mathrm{Eig}(f,\lambda)$ zu einer Basis B von V. Dann ist

$$A = M_B(f) = \begin{pmatrix} \lambda \mathbb{1}_s & * \\ 0 & A' \end{pmatrix}$$

mit einer Matrix $A' \in \mathrm{Mat}_{n-s}(K)$, also $\chi_f(t) = \chi_A(t) \overset{2.8}{=} \chi_{\lambda\mathbb{1}} \cdot \chi_{A'}(t) = (t-\lambda)^s \cdot \chi_{A'}(t)$ und somit $\dim_K(\mathrm{Eig}(f,\lambda)) = s \leq \mu(x_f,\lambda)$. □

Satz 3.11 (Diagonalisierungssatz)
Genau dann ist f diagonalisierbar, wenn χ_f in Linearfaktoren zerfällt und $\dim_K(\mathrm{Eig}(f,\lambda)) = \mu(\chi_f,\lambda)$ für alle $\lambda \in K$.

Beweis. Es gilt

$$\begin{aligned}
\dim_K(\sum_{\lambda\in K}\mathrm{Eig}(f,\lambda)) &\overset{1.10}{=} \dim_K(\bigoplus_{\lambda\in K}\mathrm{Eig}(f,\lambda)) \\
&\overset{\text{Theorem } 4.12}{=} \sum_{\lambda\in K}\dim_K(\mathrm{Eig}(f,\lambda)) \\
&\overset{3.10}{\leq} \sum_{\lambda\in K}\mu(\chi_f,\lambda) \qquad (1)\\
&\leq \deg(\chi_f) \qquad (2)\\
&= n
\end{aligned}$$

Nach Lemma 3.2 ist f genau dann diagonalisierbar, wenn $\dim_K(\sum_{\lambda\in K}\mathrm{Eig}(f,\lambda)) = n$, also wenn bei (1) und (2) Gleichheit herrscht. Gleichheit bei (1) bedeutet $\dim_K(\mathrm{Eig}(f,\lambda)) = \mu(\chi_f,\lambda)$ für alle $\lambda \in K$, und Gleichheit bei (2) bedeutet nach Lemma 3.9, dass χ_f in Linearfaktoren zerfällt. □

Definition 3.12 (algebraische und geometrische Vielfachheit)
Man nennt $\mu_a(f,\lambda) = \mu(\chi_f,\lambda)$ die algebraische Vielfachheit und $\mu_g(f,\lambda) = \dim_K(\mathrm{Eig}(f,\lambda))$ die geometrische Vielfachheit des Eigenwertes λ von f.

▶ **Bemerkung 3.13**
Wieder nennt man $A \in \mathrm{Mat}_n(K)$ diagonalisierbar, wenn $f_A \in \mathrm{End}_K(K^n)$ diagonalisierbar ist, also wenn $A \sim D$ für eine Diagonalmatrix D.

4. Trigonalisierbarkeit

Definition 4.1
Man nennt f trigonalisierbar , wenn V eine Basis B besitzt, für die $M_B(f)$ eine obere Dreiecksmatrix ist.

■ **Beispiel 4.2**
Ist f diagonalisierbar, so ist f auch trigonalisierbar.

Lemma 4.3
Ist f trigonalisierbar, so zerfällt χ_f in Linearfaktoren.

Beweis. Klar aus Beispiel 2.8 und Satz 2.3. □

Definition 4.4 (invariant)
Ein Untervektorraum $W \leq V$ ist f-invariant , wenn $f(W) \leq W$.

▶ **Bemerkung 4.5**
Ist W ein f-invarianter UVR von V, so ist $f|_W \in \mathrm{End}_K(W)$.

■ **Beispiel 4.6**

1. V hat stets die f-invarianten UVR $W = \{0\}$ und $W = V$.
2. Jeder UVR $W \leq \mathrm{Eig}(f, \lambda)$ ist f-invariant.
3. Ist $B = (x_1, ..., x_n)$ eine Basis von V, für die $M_B(f)$ eine obere Dreiecksmatrix ist, so sind alle UVR $W_i = \mathrm{span}_K(x_1, ..., x_i)$ f-invariant.
4. Sei $V = W \oplus U$, $B_1 = (x_1, ..., x_r)$ Basis von W, $B_2(x_{r+1}, ..., x_n)$ Basis von U und $B = (x_1, ..., x_n)$. Ist W f-invariant, so ist

$$M_B(f) = \begin{pmatrix} M_{B_1}(f|_W) & * \\ 0 & * \end{pmatrix}$$

Sind W und U f-invariant, so ist

$$M_B(f) = \begin{pmatrix} M_{B_1}(f|_W) & 0 \\ 0 & M_{B_2}(f|_U) \end{pmatrix}$$

Lemma 4.7
Ist $W \subset V$ ein f-invarianter UVR, so gilt $\chi_{f|_W} \mid \chi_f$. Hat W ein lineares Komplement U, dass auch f-invariant ist, so $\chi_f = \chi_{f|_W} \cdot \chi_{f|_U}$.

Beweis. Ergänze eine Basis $B_0 = (x_1, ..., x_r)$ von W zu einer Basis $B = (x_1, ..., x_n)$ von V. Sei $A = M_B(f)$,

$A_0 = M_{B_0}(f|_W)$. Dann ist

$$A = \begin{pmatrix} A_0 & * \\ 0 & C \end{pmatrix} \quad C \in \mathrm{Mat}_{n-r}(K)$$

folglich $\chi_f = \chi_A = \chi_{A_0} \cdot \chi_C$, insbesondere $\chi_{f|_W} \mid \chi_f$.
Ist auch $U = \mathrm{span}_K(x_{r+1}, ..., x_n)$ f-invariant, so ist

$$A = \begin{pmatrix} A_0 & 0 \\ 0 & C \end{pmatrix}$$

und folglich $\chi_f = \chi_A = \chi_{A_0} \cdot \chi_C = \chi_{f|_W} \cdot \chi_{f|_U}$. □

Theorem 4.8 (Trigonalisierungssatz)
Genau dann ist f trigonalisierbar, wenn χ_f in Linearfaktoren zerfällt.

Beweis. ($\Rightarrow$): Lemma 4.3
($\Leftarrow$): Induktion nach $n = \dim_K(V)$.
$\underline{n = 1}$: trivial
$\underline{n - 1 \to n}$: Nach Annahme ist $\chi_f(t) = \prod_{i=1}^{n}(t - \lambda_i)$ mit $\lambda_1, ..., \lambda_n \in K$. Sei x_1 ein EV zum EW λ_1. Dann ist $V_1 = K \cdot x_1$ ein f-invarianter UVR. Ergänze $B_1 = (x_1)$ zu einer Basis $B = (x_1, ..., x_n)$ von V und setze $B_2 = (x_2, ..., x_n)$, $V_2 = \mathrm{span}_K(B_2)$.

$$\Rightarrow M_B(f) = \begin{pmatrix} \lambda_1 & * \\ 0 & A_2 \end{pmatrix} \quad A_2 \in \mathrm{Mat}_{n-1}(K)$$

$$\chi_f(t) = \chi_{\lambda_1 \mathbb{1}_1} \cdot \chi_{A_2} = (t - \lambda_1) \cdot \chi_{A_2}(t)$$

$$\overset{3.7}{\Rightarrow} \chi_{A_2}(t) = \prod_{i=2}^{n}(t - \lambda_i)$$

Seien $\pi_1, \pi_2 \in \mathrm{End}_K(V)$ gegeben durch $M_B(\pi_1) = \mathrm{diag}(1, 0, ..., 0)$ und $M_B(\pi_2) = \mathrm{diag}(0, 1, ..., 1)$. Dann ist $\pi_1 + \pi_2 = \mathrm{id}_V$ und $f_i = \pi_1 \circ f$ ist $f = \mathrm{id}_V \circ f = f_1 + f_2$ und $f_2|_{V_2} \in \mathrm{End}_K(V_2)$. Nach Induktionshypothese ist $f_2|_{V_2}$ trigonalisierbar, da $M_B(f_2|_{V_2}) = A_2$, also $\chi_{f_2|_{V_2}} = \chi_{A_2}$. Dies bedeutet, es gibt also eine Basis $B_2' = (x_2', ..., x_n')$ von V_2, für die $M_{B_2'}(f_2|_{V_2})$ eine obere Dreiecksmatrix ist. Somit ist für $B' = (x_1, x_2', ..., x_n')$ auch

$$M_{B'}(f) = M_{B'}(f_1) + M_{B'}(f_2)$$
$$= \begin{pmatrix} \lambda_1 & * \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & M_{B_2'}(f_2|_{V_2}) \end{pmatrix}$$

eine obere Dreiecksmatrix. □

Folgerung 4.9
Ist K algebraisch abgeschlossen, so ist jedes $f \in \mathrm{End}_K(V)$ trigonalisierbar.

Beweis. Ist K algebraisch abgeschlossen, so zerfällt nach Satz 6.14 jedes Polynom über K in Linearfaktoren, insbesondere also χ_f. □

Folgerung 4.10
Ist V ein endlichdimensionaler $\mathbb{C}$-VR, so ist jedes $f \in \mathrm{End}_{\mathbb{C}}(V)$ trigonalisierbar.

Beweis. Nach dem Fundamentalsatz der Algebra Theorem 6.16 ist $\mathbb{C}$ algebraisch abgeschlossen. □

5. Das Minimalpolynom

Definition 5.1
Für ein Polynom $P(t) = \sum_{i=0}^{n} c_i t^i \in K[t]$ definieren wir $P(f) = \sum_{i=0}^{m} c_i f^i \in \mathrm{End}_K(V)$, wobei $f^0 = \mathrm{id}_V$, $f^1 = f$, $f^2 = f \circ f$, ...

Analog definiert man $P(A)$ für $A \in \mathrm{Mat}_n(K)$.

▶ **Bemerkung 5.2**
Die Abbildung $\begin{cases} K[t] \to \mathrm{End}_K(V) \\ P \mapsto P(f) \end{cases}$ ist ein Homomorphismus von K-VR und Ringen. Sein Kern ist das Ideal

$$\mathcal{I}_f := \{P \in K[t] \mid P(f) = 0\}$$

und sein Bild ist der kommutative Unterring

$$\begin{aligned} K[f] :&= \{P(f) \mid P \in K[t]\} \\ &= \mathrm{span}_K(f^0, f^1, f^2, ...) \end{aligned}$$

des (im Allgemeinen nicht kommutativen) Rings $\mathrm{End}_K(V)$.

Analog definiert man $\mathcal{I}_A$ und $K[A] \leq \mathrm{Mat}_n(K)$.

Lemma 5.3
$\mathcal{I}_f \neq \{0\}$

Beweis. Wäre $\mathcal{I}_f = \{0\}$, so wäre $K[t] \to \mathrm{End}_K(V)$ injektiv, aber $\dim_K(K[t]) = \infty > n^2 = \dim_K(\mathrm{End}_K(V))$, ein Widerspruch. □

Satz 5.4
Es gibt ein eindeutig bestimmtes normiertes Polynom $0 \neq P \in K[t]$ kleinsten Grades mit $P(f) = 0$. Dieses teilt jedes $Q \in K[t]$ mit $Q(f) = 0$.

Beweis. Nach Lemma 5.3 gibt es $0 \neq P \in K[t]$ mit $P(f) = 0$ von minimalem Grad d. Indem wir durch den Leitkoeffizienten von P teilen, können wir annehmen, dass P normiert ist.
Sei $Q \in \mathcal{I}_f$. Polynomdivision liefert $R, H \in K[t]$ mit $Q = P \cdot H + R$ und $\deg(R) < \deg(P) = d$. Es folgt $R(f) = \underbrace{Q(f)}_{=0} - \underbrace{P(f)}_{=0} \cdot H(f) = 0$. Aus der Minimalität von d folgt $R = 0$ und somit $P \mid Q$.
Ist Q zudem normiert vom Grad d, so ist $H = 1$, also $Q = P$, was die Eindeutigkeit zeigt. □

Definition 5.5 (Minimalpolynom)
Das eindeutig bestimmte normierte Polynom $0 \neq P \in K[t]$ kleinsten Grades mit $P(f) = 0$ nennt man das Minimalpolynom P_f von f.

Analog definiert man das Minimalpolynom $P_A \in K[t]$ einer Matrix $A \in \mathrm{Mat}_n(K)$.

Mathematica/WolframAlpha-Befehle (Minimalpolynom)
Die Funktion für das Minimalpolynom p mit der Variable t von einer Matrix A in Mathematica bzw. WolframAlpha lautet:

```
MinimalPolynomial[A,x]
```

■ **Beispiel 5.6**

1. $A = \mathbb{1}_n$, $\chi_A(t) = (t-1)^n$, $P_A(t) = t-1$
2. $A = 0$, $\chi_A(t) = t^n$, $P_A(t) = t$
3. Ist $A = \operatorname{diag}(a_1, ..., a_n)$ mit paarweise verschiedenen Eigenwerten $\lambda_1, ..., \lambda_r$, so ist $\chi_A(t) = \prod_{i=1}^{n}(t-a_i) = \prod_{i=1}^{n}(t-\lambda_i)^{\mu_a(f_A,\lambda_i)}$, $P_A(t) = \prod_{i=1}^{r}(t-\lambda_i)$ und es folgt $\deg(P_A) \geq |\{a_1, ..., a_n\}| = r$.

Definition 5.7 (f-zyklisch)
Ein f-invarianter UVR $W \leq V$ heißt f-zyklisch , wenn es ein $x \in W$ mit $W = \operatorname{span}_K(x, f(x), f^2(x), ...)$ gibt.

Lemma 5.8
Sei $x \in V$ und $x_i = f^i(x)$. Es gibt ein kleinstes k mit $x_k \in \operatorname{span}_K(x_0, x_1, ..., x_{k-1})$, und $W = \operatorname{span}_K(x_0, ..., x_{k-1})$ ein f-zyklischer UVR von V mit Basis $B = (x_0, ..., x_{k-1})$ und $M_B(f|_W) = M_{\chi_{f|_W}}$.

Beweis. Da $\dim_K(V) = n$ ist $(x_0, ..., x_n)$ linear abhängig, es gibt also ein kleinstes k mit $(x_0, ..., x_{k-1})$ linear unabhängig, aber $(x_0, ..., x_k)$ linear abhängig, folglich $x_k \in \operatorname{span}_K(x_0, ..., x_{k-1})$. Mit $x_k = f(x_{k-1}) = \sum_{i=0}^{k-1} -c_i x_i$ ist dann Da $\dim_K(V) = n$ ist $(x_0, ..., x_n)$ linear abhängig, es gibt also ein kleinstes k mit $(x_0, ..., x_{k-1})$ linear unabhängig, aber $(x_0, ..., x_k)$ linear abhängig, folglich $x_k \in \operatorname{span}_K(x_0, ..., x_{k-1})$. Mit $x_k = f(x_{k-1}) = \sum_{i=0}^{k-1} -c_i x_i$ ist dann

$$M_B(f|_W) = \begin{pmatrix} 0 & ... & ... & ... & 0 & -c_0 \\ 1 & \ddots & & & \vdots & \vdots \\ 0 & \ddots & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & ... & 0 & 1 & 0 & -c_{k-1} \end{pmatrix}$$

somit $\chi_{f|_W} = t^k + \sum_{i=0}^{k-1} c_i t^i$, also $M_B(f|_W) = M_{\chi_{f|_W}}$. □

Theorem 5.9 (Satz von Cayley-Hamilton)
Für $f \in \operatorname{End}_K(V)$ ist $\chi_f(f) = 0$.

Beweis. Sei $x \in V$. Definiere $x_i = f^i(x)$ und $W = \operatorname{span}_K(x_0, ..., x_{k-1})$ wie in Lemma 5.8. Sei $\chi_{f|_W} = t^k +$

$\sum_{i=0}^{k-1} c_i t^i$, also $f(x_{k-1}) = \sum_{i=0}^{k-1} -c_i x_i$. Wenden wir $\chi_{f|_W}(f) \in \mathrm{End}_K(V)$ auf x an, so erhalten wir

$$\begin{aligned}\chi_{f|_W}(f)(x) &= \left(f^k + \sum_{i=1}^{k-1} c_i f^i\right)(x) \\ &= \sum_{i=1}^{k-1} -c_i x_i + \sum_{i=1}^{k-1} c_i x_i \\ &= 0\end{aligned}$$

Aus $\chi_{f|_W} \mid \chi_f$ (Beispiel 4.6) folgt somit $\chi_f(f)(x) = 0$, denn ist $\chi_f = Q \cdot \chi_{f|_W}$ mit $Q \in K[t]$, so ist $\chi_f(f) = Q(f) \circ \chi_{f|_W}(f)$, also $\chi_f(f)(x) = Q(f)(\underbrace{\chi_{f|_W}(f)(x)}_{=0}) = 0$. Da $x \in V$ beliebig war, folgt $\chi_f(f) = 0 \in \mathrm{End}_K(V)$. □

Folgerung 5.10
Es gilt $P_f \mid \chi_f$. Insbesondere ist $\deg(P_f) \leq n$.

Beweis. Theorem 5.9 + Satz 5.4 □

▶ **Bemerkung 5.11**
Ist B eine Basis von V und $A = M_B(f)$, so ist $P_A = P_f$. Insbesondere ist $P_A = P_B$ für $A \sim B$. Als Spezialfall von Theorem 5.9 erhält man $\chi_A(A) = 0$ und $P_A \mid \chi_A$.

▶ **Bemerkung 5.12**
Der naheliegende "Beweis" $\underbrace{\chi_A}_{\in \mathrm{Mat}_n(K)} = \det(t\mathbb{1}_n - A)(A) = \det(A\mathbb{1}_n - A) = \det(0) = \underbrace{0}_{\in K}$ ist falsch!

6. Nilpotente Endomorphismen

▶ **Bemerkung 6.1**
Für $f \in \mathrm{End}_K(V)$ sind

- $f\{0\} = \mathrm{Ker}(f^0) \subseteq \mathrm{Ker}(f^1) \subseteq \mathrm{Ker}(f^2) \subseteq ...$
- $V = \mathrm{Im}(f^0) \supseteq \mathrm{Im}(f^1) \supseteq \mathrm{Im}(f^2) \supseteq ...$

Folgen von UVR von V. Nach der Kern-Bild-Formel Folgerung 7.13III.7.13 ist

$$\dim_K(\mathrm{Ker}(f^i)) + \dim_K(\mathrm{Im}(f^i)) = \dim_K(V) \quad \forall i$$

Da $\dim_K(V) = n < \infty$ gibt es ein d mit $\mathrm{Ker}(f^d) = \mathrm{Ker}(f^{d+i})$ und $\mathrm{Im}(f^d) = \mathrm{Im}(f^{d+i})$ für jedes $i \geq 0$.

■ **Beispiel 6.2**
$f = f_A$, $A \in \mathrm{Mat}_2(K)$.

- $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$: $\{0\} = \mathrm{Ker}(f^0) = \mathrm{Ker}(f^1) = ...$
- $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$: $\{0\} = \mathrm{Ker}(f^0) \subset \mathrm{Ker}(f^1) \subsetneq \mathrm{Ker}(f^2) = ... = \mathrm{span}_K(e_2)$
- $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$: $\{0\} = \mathrm{Ker}(f^0) \subset \underbrace{\mathrm{Ker}(f^1)}_{=\mathrm{span}_K(e_1)} \subset \mathrm{Ker}(f^2) = ... = K^2$
- $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$: $\{0\} = \mathrm{Ker}(f^0) \subset \mathrm{Ker}(f^1) = \mathrm{Ker}(f^2) = ... = K^2$

Lemma 6.3
Seien $f, g \in \mathrm{End}_K(V)$. Wenn f und g kommutieren, d.h. $f \circ g = g \circ f$, so sind die UVR $\mathrm{Ker}(g)$ und $\mathrm{Im}(g)$ f invariant.

Beweis. Ist $x \in \mathrm{Ker}(f)$, so ist $g(f(x)) = f(g(x)) = f(0) = 0$, also $f(x) \in \mathrm{Ker}(g)$. Für $g(x) \in \mathrm{Im}(g)$ ist $f(g(x)) = g(f(x)) \in \mathrm{Im}(g)$. □

Satz 6.4 (Lemma von Fitting)
Seien $V_i = \mathrm{Ker}(f^i)$, $W_i = \mathrm{Im}(f^i)$, $d = \min\{i \mid V_i = V_{i+1}\}$. Dann sind

$$\{0\} = V_0 \subsetneq V_1 \subsetneq ... \subsetneq V_d = V_{d+1} = ...$$
$$V = W_0 \supsetneq W_1 \supsetneq ... \supsetneq W_d = W_{d+1} = ...$$

Folgen f-invarianter UVR und $V = V_d \oplus W_d$.

Beweis. Da f^i und f^j für beliebige i, j kommutieren, sind V_i und V_j nach Lemma 6.3 f-invariant für jedes i. Aus $\dim_K(V_i) + \dim_K(W_i) = n$ folgt $d = \min\{i \mid W_i = W_{i+1}\}$, insbesondere ist $\mathrm{Im}(f^d) = \mathrm{Im}(f^{d+1}) = f(\mathrm{Im}(f^d))$, somit $W_{d+i} = \mathrm{Im}(f^{d+i}) = W_d$ für $i \geq 0$, also auch $V_d = V_{d+i}$ für alle $i \geq 0$.
Insbesondere ist $f^d|_{W_d} : W_d \to W_{2d} = W_d$ surjektiv, also auch injektiv, also $V_d \cap W_d = \{0\}$. Aus der Dimensionsformel II.4.12 folgt dann $\dim_K(V_d + W_d) = \dim_K(V_d) + \dim_K(W_d) = \dim_K(V)$. Folglich ist $V_d + W_d = V$ und $V_d \cap W_d = \{0\}$, also $V = V_d \oplus W_d$. □

Definition 6.5 (nilpotent)
Ein $f \in \mathrm{End}_K(V)$ heißt nilpotent , wenn $f^k = 0$ für ein $k \in \mathbb{N}$. Analog heißt $A \in \mathrm{Mat}_n(K)$ nilpotent, wenn $A^k = 0$ für $k \in \mathbb{N}$. Das kleinste k mit $f^k = 0$ bzw. A^k heißt die Nilpotenzklasse von f bzw. A.

Lemma 6.6
Ist f nilpotent, so gibt es eine Basis B von V, für die $M_B(f)$ eine strikte obere Dreiecksmatrix ist.

Beweis. Induktion nach $n = \dim_K(V)$.
$n = 1$: $f^k = 0 \Rightarrow f = 0$
$n > 1$: Sei k die Nilpotenzklasse von f und $U = \mathrm{Ker}(f^{k-1})$. Dann ist $U \subset V$. Da $f^k = f^{k-1} \circ f$ ist $f(V) \subset U$, insbesondere $f|_U \in \mathrm{End}_K(U)$. Da $f|_U$ nilpotent ist, gibt es nach I.H. eine Basis B_0 von U, für die $M_B(f|_U)$ eine strikte obere Dreiecksmatrix ist. Ergänze B_0 zu einer Basis B von V. Da $f(V) \subset U$ ist dann auch

$$M_B(f) = \begin{pmatrix} M_{B_0}(f|_U) & * \\ 0 & 0 \end{pmatrix}$$

eine strikte obere Dreiecksmatrix. □

Satz 6.7
Für $f \in \mathrm{End}_K(V)$ sind äquivalent:

1) f ist nilpotent
2) $f^n = 0$ für $n \in \mathbb{N}$
3) $P_f(t) = t^r$ für ein $r \leq n$
4) $\chi_f(t) = t^n$
5) Es gibt eine Basis B von V, mit

$$M_B(f) = \begin{pmatrix} 0 & * & \dots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 0 \end{pmatrix}$$

eine strikte obere Dreiecksmatrix ist.

Beweis.

- 1) $\Rightarrow$ 5): Lemma 6.6
- 5) $\Rightarrow$ 4): Beispiel 2.8
- 4) $\Rightarrow$ 3): Nach Folgerung 5.10 ist $P_f \mid \chi_f = t^n$, also $t^n = P_f(t)Q(t)$ mit $Q \in K[t]$. Schreibe $P_f(t) = t^a \cdot P_1(t), Q(t) = t^b \cdot Q_1(t)$ mit $a, b \in \mathbb{N}$, $P_1, Q_1 \in K[t]$, $P_1(0) \neq 0$, $Q_1(0) \neq 0$
  $\overset{3.8}{\Rightarrow} t^{n-(a+b)} = P_1(t)Q_1(t)$ und $(P_1Q_1)(0) \neq 0$
  $\Rightarrow n - (a+b) = 0 \Rightarrow P_1 = 1$, somit $P_f(t) = t^a$
- 3) $\Rightarrow$ 2): $t^r = 0$, $r \leq n \Rightarrow f^n = 0$
- 2) $\Rightarrow$ 1): nach Definition □

Folgerung 6.8
Die Nilpotenzklasse eines nilpotenten Endomorphismus $f \in \mathrm{End}_K(V)$ ist höchstens $\dim_K(V)$.

Folgerung 6.9
Ist $d := \min\{i \mid \mathrm{Ker}(f^i) = \mathrm{Ker}(f^{i+1})\}$, so ist $d \leq \dim_K(\mathrm{Ker}(f)) = \mu_a(f, 0)$.

Beweis. Sei $V_d = \mathrm{Ker}(f^d)$, $W_d = \mathrm{Im}(f^d)$, $k = \dim_K(V_d)$. Da $V = V_d \oplus W_d$ ist $\chi_f = \chi_{f|_{V_d}} \cdot \chi_{f|_{W_d}}$. Da $f|_{V_d}$ nilpotent ist, ist $\chi_{f|_{V_d}} = t$ nach Satz 6.7. Da $f|_{W_d}$ injektiv ist, ist $\chi_{f|_{W_d}}(0) \neq 0$. Somit ist $\mu_a(f, 0) = \mu(\chi_f, 0) \overset{3.6}{=} k$. Da $\dim_K(\mathrm{Ker}(f^d)) > ... > \dim_K(\mathrm{Ker}(f)) > 0$ ist $k = \dim_K(\mathrm{Ker}(f^d)) \geq d$, falls $d > 0$, sonst klar. □

▶ **Bemerkung 6.10**
Die Bedeutung nilpotenter Endomorphismen beim Finden geeigneter Basen ergibt sich aus der folgenden Beobachtung:
Ist A eine obere Dreiecksmatrix, so ist $A = D + N$, wobei D eine Diagonalmatrix ist und N eine strikte obere Dreiecksmatrix ist. Anders gesagt: Jeder trigonalisierbare Endomorphismus ist Summe aus einem diagonalisierbaren und einem nilpotenten Endomorphismus.

Definition 6.11 (Jordan-Matrix)
Für $k \in \mathbb{N}$ definieren wir die JORDAN-Matrix

$$J_k = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & ... & ... & ... & 0 \end{pmatrix} \in \mathrm{Mat}_k(K)$$

weiter setzen wir für $\lambda \in K$ $J_k(\lambda) := \lambda \mathbb{1} + J_k$.

Lemma 6.12
Die JORDAN-Matrix J_k ist nilpotent von Nilpotenzklasse k.

Beweis. Es ist $(J_k)^r = (\delta_{i+r,j})_{i,j}$ für $r \geq 1$. □

Satz 6.13
Ist f nilpotent von Nilpotenzklasse k, so gibt es eindeutig bestimmte $r_1, .., r_k \in \mathbb{N}_{>0}$ mit $\sum_{d=1}^{k} dr_d = n$ und eine Basis B von V mit

$$M_B(f) = \text{diag}(\underbrace{J_k, ..., J_k}_{r_k \text{ viele}}, ..., \underbrace{J_1, ..., J_1}_{r_1 \text{ viele}})$$

Beweis. Sei $U_i = \text{Ker}(f^i)$. Nach Satz 6.4 haben wir eine Folge $\{0\} = U_0 \subset U_1 \subset ... \subset U_k = V$ mit $f(U_i) \subseteq U_{i-1}$ für alle $i > 0$.
Wir konstruieren eine Zerlegung $V = \bigoplus_{d=1}^{k} W_d$ mit $U_i = U_{i-1} \oplus W_i$, $f(W_i) \subseteq W_{i-1}$, $f|_{W_d}$ injektiv für $i > 1$.

$$\begin{aligned} V &= U_k \\ V &= U_{k-1} \oplus W_k \\ V &= U_{k-2} \oplus W_{k-1} \oplus W_k \\ &\vdots \\ V &= U_0 \oplus W_1 \oplus ... \oplus W_k \end{aligned}$$

Wähle W_k mit $V = U_k = U_{k-1} \oplus W_k$. Ist $k > 1$, so ist $W_k \cap \text{Ker}(f) \subseteq W_k \cap U_{k-1} = \{0\}$, also $f|_{W_k}$ ist injektiv. Des weiteren ist $f(W_k) \subseteq U_{k-1}$ und aus $W_k \cap U_{k-1} = \{0\}$ folgt $f(W_k) \cap U_{k-2} = \{0\}$. Wir können deshalb W_{k-1} mit $U_{k-1} = U_{k-2} \oplus W_{k-1}$ und $f(W_k) \subseteq W_{k-1}$ wählen. Somit ist $V = U_{k-1} \oplus W_k = U_{k-2} \oplus W_{k-1} \oplus W_k$. Wir setzen dies fort und erhalten $V = U_0 \oplus W_1 \oplus ... \oplus W_k$ mit $f(W_i) \subseteq W_{i-1}$ und $f|_{W_i}$ injektiv für $i > 1$, wobei $U_0 = \{0\}$ und $W_1 = \text{Ker}(f)$.
Sie $r_d = \dim_K(W_d) - \dim_K(W_{d+1})$, wobei wir $W_{k+1} = \{0\}$. Wähle nun eine Basis $(x_{k,1}, ..., x_{k,r_k})$ von W_k. Ist $k > 1$, so ist $f|_{W_k}$ injektiv und wir können $(f(x_{k,1}), ..., f(x_{k,r_k}))$ durch Elemente $x_{k-1,1}, ..., x_{k-1,r_{k-1}}$ zu einer Basis von W_{k-1} ergänzen, und so weiter.
Da $V = \bigoplus_{d=1}^{k} W_d$ ist

$$B = \{f^i(x_{d,j}) \mid d = 1, ..., k, j = 1, ..., r_d, i = 0, ..., d-1\}$$

eine Basis von V, die bei geeigneter Anordnung das Gewünschte leistet.
Es bleibt zu zeigen, dass $r_1, ..., r_k$ eindeutig bestimmt sind. Ist B_0 eine Basis, für die $M_{B_0}(f)$ in der gewünschten Form ist, so ist

$$\begin{aligned} \dim_K(U_1) &= \sum_{d=1}^{k} r_d \\ \dim_K(U_2) &= \sum_{d=2}^{k} r_d + \sum_{d=1}^{k} r_d \\ &\vdots \\ \dim_K(U_k) &= \sum_{d=k}^{k} r_d + ... + \sum_{d=1}^{k} r_d \end{aligned}$$

woraus man sieht, dass $r_1, ..., r_k$ durch $U_1, ..., U_k$, also durch f eindeutig bestimmt. □

■ **Beispiel 6.14**
Sei $f = f_A$ mit $A = \begin{pmatrix} 0 & 1 & 3 \\ & 0 & 2 \\ & & 0 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{R})$

$$A^2 = \begin{pmatrix} 0 & 0 & 2 \\ & 0 & 0 \\ & & 0 \end{pmatrix}, A^3 = 0$$

$\Rightarrow k = 3, U_0 = \{0\}, U_1 = \mathbb{R}e_1, U_2 = \mathbb{R}e_1 + \mathbb{R}e_2, U_3 = V$.
Wähle W_3 mit $V = U_3 = U_2 \oplus W_3$, z.B. $W_3 = \mathbb{R}e_3$.
Wähle W_2 mit $U_2 = U_1 \oplus W_2$ und $f(W_3) \subseteq W_2$, also

$$W_2 = \mathbb{R} \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}$$

Setze $W_1 = U_1 = \mathrm{Ker}(f) = \mathbb{R}e_1 \Rightarrow$ Basis $B = (f^2(e_3), f(e_3), e_3)$

$$M_B(f) = \begin{pmatrix} 0 & 1 & 0 \\ & 0 & 1 \\ & & 0 \end{pmatrix}$$

7. Die Jordan-Normalform

Definition 7.1 (Hauptraum)
Der Hauptraum von f zum EW λ der Vielfachheit $r = \mu_a(f, \lambda)$ ist

$$\mathrm{Hau}(f, \lambda) = \mathrm{Ker}\left((f - \lambda \,\mathrm{id}_V)^r\right)$$

Lemma 7.2
$\mathrm{Hau}(f, \lambda)$ ist ein f-invarianter UVR der Dimension $\dim_K(\mathrm{Hau}(f, \lambda)) = \mu_a(f, \lambda)$, auf dem $f - \lambda \,\mathrm{id}_V$ nilpotent ist und $\chi_{f|_{\mathrm{Hau}(f,\lambda)}} = (t - \lambda)^{\mu_a(f,\lambda)}$

Beweis. f kommutiert sowohl mit f als auch mit id_V, somit auch mit $(f - \lambda \,\mathrm{id}_V)^r$. Die f-Invarianz von $U = \mathrm{Hau}(f, \lambda)$ folgt aus Lemma 6.3. Nach Folgerung 6.9 ist $\dim_K(U) = \mu_a(f - \lambda \,\mathrm{id}_V, 0)$ und da $\chi_f(t) = \chi_{f-\lambda \,\mathrm{id}_V}(t - \lambda)$ ist $\mu_a(f, \lambda) = \mu(\chi_f, \lambda) = \mu_a(f - \lambda \,\mathrm{id}_V, 0)$. Da $f - \lambda \,\mathrm{id}_V \,|_U$ nilpotent ist $\chi_{f-\lambda \,\mathrm{id}_V \,|_U}(t) = t^r$, somit $\chi_{f|_U}(t) = (t - \lambda)^r$. □

Satz 7.3 (Hauptraumzerlegung)
Ist $\chi_f(t) = \prod_{i=1}^m (t - \lambda_i)^{r_i}$ mit $\lambda_1, ..., \lambda_m \in K$ paarweise verschieden und $r_1, ..., r_m \in \mathbb{N}$, so ist $V = \bigoplus_{i=1}^m V_i$ mit $V_i = \mathrm{Hau}(f, \lambda_i)$ eine Zerlegung in f-invariante UVR und für jedes i ist $\chi_{f|_{V_i}}(t) = (t - \lambda_i)^{r_i}$.

Beweis. Induktion nach m.
$\underline{m = 1}$: $r_1 = n \overset{7.2}{\Rightarrow} V = V_1$.
$\underline{m - 1 \to m}$: Nach Satz 6.4 ist $V = V_1 \oplus W_1$ mit $W_1 = \mathrm{Im}((f - \lambda_i \,\mathrm{id}_V)^r)$ eine Zerlegung in f-invariante UVR mit $\dim_K(V_1) = r_1$, $\dim_K(W_1) = n - r_1$. Somit ist $\chi_f = \chi_{f|_{V_1}} \cdot \chi_{f|_{W_1}}$ und $\chi_{f|_{V_1}} \overset{7.2}{=} (t - \lambda_1)^{r_1}$ also $\chi_{f|_{W_1}} = \prod_{i=2}^m (t - \lambda_i)^{r_i}$. Nach I.H. ist also $W_1 = \bigoplus_{i=2}^m \mathrm{Hau}(f|_{W_1}, \lambda_i)$. Es ist für $i \geq 2$ $\mathrm{Hau}(f|_{W_1}, \lambda_i) \subseteq \mathrm{Hau}(f, \lambda_i) = V_i$ und da $\dim_K(\mathrm{Hau}(f|_{W_1}, \lambda_i)) = r_i = \dim_K(\mathrm{Hau}(f, \lambda_i))$ gilt Gleichheit. Damit ist

$$\begin{aligned} V &= V_1 \oplus W_1 \\ &= V_1 \oplus \bigoplus_{i=2}^m \mathrm{Hau}(f|_{W_1}, \lambda_i) \\ &= V_1 \oplus \bigoplus_{i=2}^m V_i \\ &= \bigoplus_{i=1}^m V_i \end{aligned}$$

□

■ **Beispiel 7.4**
$f = f_A$

$$A = \begin{pmatrix} 1 & 3 & \\ & 1 & 4 \\ & & 2 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{R})$$

$\chi_A(t) = (t-1)^2(t-2) \Rightarrow \mathbb{R}^3 = \underbrace{\mathrm{Hau}(f,1)}_{\dim=2} \oplus \underbrace{\mathrm{Hau}(f,2)}_{\dim=1}$
$\mathrm{Hau}(f,1) = \mathrm{Ker}((f-\mathrm{id})^2) = L((A-\mathbb{1})^2, 0)$
$\mathrm{Hau}(f,2) = \mathrm{Ker}(f - 2\,\mathrm{id}) = \mathrm{Eig}(f,2) = L(A - 2\mathbb{1}, 0)$

$$A - \mathbb{1} = \begin{pmatrix} 0 & 3 & \\ & -1 & 4 \\ & & 0 \end{pmatrix}, (A-\mathbb{1})^2 = \begin{pmatrix} 0 & & 12 \\ & 0 & 4 \\ & & 1 \end{pmatrix} \qquad \Rightarrow \mathrm{Hau}(f,1) = \mathbb{R}e_1 + \mathbb{R}e_2$$

$$A - 2\mathbb{1} = \begin{pmatrix} -1 & 3 & \\ & -1 & 4 \\ & & 0 \end{pmatrix} \qquad \Rightarrow \mathrm{Hau}(f,2) = \mathbb{R}\begin{pmatrix} 12 \\ 4 \\ 1 \end{pmatrix}$$

Mit $B = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 12 \\ 4 \\ 1 \end{pmatrix} \right)$ ist

$$M_B(f) = \begin{pmatrix} \begin{pmatrix} 1 & 3 \\ & 1 \end{pmatrix} & \\ & 2 \end{pmatrix}$$

Theorem 7.5 (Jordan-Normalform)
Sei $f \in \mathrm{End}_K(V)$ ein Endomorphismus, dessen charakteristisches Polynom χ_f in Linearfaktoren zerfällt. Dann gibt es $r \in \mathbb{N}$, $\mu_1, ..., \mu_r \in K$ und $k_1, ..., k_r \in \mathbb{N}$ mit $\sum_{i=1}^r k_i = \dim_K(V)$ und eine Basis B von V mit

$$M_B(f) = \mathrm{diag}(J_{k_1}(\mu_1), ..., J_{k_r}(\mu_r))$$

Die Paare $(\mu_1, k_1), ..., (\mu_r, k_r)$ heißen die JORDAN-Invarianten von f und sind bis auf Reihenfolge eindeutig bestimmt.

Beweis. Schreibe $\chi_f(t) = \prod_{i=1}^m (t-\lambda_i)^{r_i}$ mit $\lambda_1, ..., \lambda_m \in K$ paarweise verschieden, $r_i \in \mathbb{N}$. Sei $V_i = \mathrm{Hau}(f, \lambda_i)$. Nach Satz 7.3 ist $V = \bigoplus_{i=1}^m V_i$ eine Zerlegung in f-invariante UVR. Für jedes i wenden wir Satz 6.13 auf $(f - \lambda_i\,\mathrm{id}_V)|_{V_i}$ an und erhalten eine Basis B_i von V_i und $k_{i,1} \geq ... \geq k_{i,s_i}$ mit

$$M_B((f-\lambda_i\,\mathrm{id})|_{V_i}) = \mathrm{diag}(J_{k_{i,1}}, ..., J_{k_{i,s_i}})$$

Es folgt $M_{B_i}(f|_{V_i}) = M_{B_i}(\lambda_i\,\mathrm{id}_{V_i}) + M_{B_i}((f-\lambda_i\,\mathrm{id}_V)|_{V_i})$. Ist nun B die Vereinigung der B_i, so hat $M_B(f)$ die gewünschte Form. Die Eindeutigkeit der JORDAN-Invarianten folgt aus der Eindeutigkeit der $k_{i,j}$ in Lemma 6.3.□

▶ **Bemerkung 7.6**

Ist K algebraisch abgeschlossen, so haben wir nun eine (bis auf Permutationen) eindeutige Normalform für Endomorphismen $f \in \mathrm{End}_K(V)$ gefunden. Aus ihr lassen sich viele Eigenschaften des Endomorphismus leicht ablesen.

Folgerung 7.7

Sei $f \in \mathrm{End}_K(V)$ trigonalisierbar mit $\chi_f(t) = \prod_{i=1}^m (t-\lambda_i)^{\mu_a(f,\lambda_i)}$, $P_f(t) = \prod_{i=1}^m (t-\lambda_i)^{d_i}$ und JORDAN-Invarianten $(\mu_1, k_1), ..., (\mu_r, k_r)$. Mit $J_i = \{j \mid \mu_j = \lambda_i\}$ ist dann

$$\begin{aligned} \mu_g(f, \lambda_i) &= |J_i| \\ \mu_a(f, \lambda_i) &= \sum_{j \in J_i} k_j \\ d_i &= \max\{k_j \mid j \in J_i\} \end{aligned}$$

Beweis.

- μ_a: klar, da $\chi_f(t) = \prod_{j=1}^r (t-\mu_j)^{k_j} = \prod_{i=1}^m (t-\lambda_i)^{\mu_a(f,\lambda_i)}$
- μ_g: lese Basis von $\mathrm{Eig}(f, \lambda_i)$ aus JORDAN-NF: Jeder Block $J_{k_j}(\lambda_i)$ liefert ein Element der Basis.
- d_i: folgt, da J_{k_j} nilpotent von Nilpotenzklasse k_j ist (Lemma 6.12). □

Folgerung 7.8

Genau dann ist f diagonalisierbar, wenn

$$\begin{aligned} \chi_f(t) &= \prod_{i=1}^m (t-\lambda_i)^{r_i} \quad \lambda_1, ..., \lambda_m \in K \text{ paarweise verscheiden und} \\ P_f(t) &= \prod_{i=1}^m (t-\lambda_i) \end{aligned}$$

Beweis. Genau dann ist f diagonalisierbar, wenn f trigonalisierbar ist und die JORDAN-NF die Diagonalmatrix ist (Eindeutigkeit der JNF), also $k_j = 1$ für alle j. Nach Folgerung 7.7 ist dies äquivalent dazu, dass $d_i = 1$ für alle i, also $P_f = \prod_{i=1}^m (t-\lambda_i)$. □

▶ **Bemerkung 7.9**

Wieder definiert man die JORDAN-Invarianten, etc. von einer Matrix $A \in \mathrm{Mat}_n(K)$ als die JORDAN-Invarianten von $f_A \in \mathrm{End}_K(K^n)$.

Folgerung 7.10

Seien $A, B \in \mathrm{Mat}_n(K)$ trigonalisierbar. Genau dann ist $A \sim B$, wenn A und B die gleichen JORDAN-Invarianten haben.

Beweis. Existenz und Eindeutigkeit der JORDAN-Normalform. □

Kapitel VI

Skalarprodukte

In diesem ganzen Kapitel seien

- $K = \mathbb{R}$ oder $K = \mathbb{C}$
- $n \in \mathbb{N}$
- V ein n-dimensionaler K-VR

1. Das Standardskalarprodukt

Sei zunächst $K = \mathbb{R}$.

Definition 1.1 (Standardskalarprodukt in $\mathbb{R}$)
Auf den Standardraum $V = \mathbb{R}^n$ definiert man das Standardskalarprodukt in $\mathbb{R}$ $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ durch

$$\langle x, y \rangle = x^t y = \sum_{i=1}^{n} x_i y_i$$

Satz 1.2
Das Standardskalarprodukt erfüllt die folgenden Eigenschaften:

- Für $x, x', y, y' \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ ist:

$$\begin{aligned} \langle x + x', y \rangle &= \langle x, y \rangle + \langle x', y \rangle \\ \langle \lambda x, y \rangle &= \lambda \langle x, y \rangle \\ \langle x, y + y' \rangle &= \langle x, y \rangle + \langle x, y' \rangle \\ \langle x, \lambda y \rangle &= \lambda \langle x, y \rangle \end{aligned}$$

- Für $x, y \in \mathbb{R}^n$ ist $\langle x, y \rangle = \langle y, x \rangle$
- Für $x \in \mathbb{R}^n$ ist $\langle x, x \rangle \geq 0$ und $\langle x, x \rangle = 0 \iff x = 0$

Beweis.
- klar
- klar
- $\langle x, x \rangle = \sum_{i=1}^{n} x_i^2 \geq x_j^2$ für jedes $j \Rightarrow \langle x, x \rangle \geq 0$ und $\langle x, x \rangle > 0$ falls $x_j \neq 0$ für ein j. □

Definition 1.3 (euklidische Norm in $\mathbb{R}$)
Auf $V = \mathbb{R}^n$ definiert man euklidische Norm in $\mathbb{R}$ $\| \cdot \| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ durch

$$\|x\| = \sqrt{\langle x, x \rangle}$$

Satz 1.4 (Ungleichung von Cauchy-Schwarz)
Für $x, y \in \mathbb{R}^n$ gilt

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

Gleichheit genau dann, wenn x und y linear abhängig sind.

Beweis. siehe Analysis, siehe VI.§3 □

Anmerkung
Der Beweis dieser Ungleichung wird im Skript später noch behandelt, war aber für mich nicht verständlich, deswegen hier noch mal ein einfach zu verstehender Beweis: Wir betrachten dazu das Skalarprodukt

$$0 \leq \langle x - \lambda y, x - \lambda y\rangle$$

Mit dem Anwenden der Rechenregeln ergibt sich:

$$\begin{aligned}
\langle x - \lambda y, x - \lambda y\rangle &= \langle x - \lambda y, x\rangle - \langle x - \lambda y, \lambda y\rangle \\
&= \langle x - \lambda y, x\rangle - \overline{\lambda}\,\langle x - \lambda y, y\rangle \\
&= \langle x, x\rangle - \langle \lambda y, x\rangle - \overline{\lambda}\,\langle x, y\rangle + \overline{\lambda}\,\langle \lambda y, y\rangle \\
&= \langle x, x\rangle - \lambda\,\langle y, x\rangle - \overline{\lambda}\,\langle x, y\rangle + \lambda\overline{\lambda}\,\langle y, y\rangle
\end{aligned}$$

Jetzt setzen wir

$$\lambda = \frac{\langle x, y\rangle}{\langle y, y\rangle} = \frac{\langle x, y\rangle}{\|y\|^2}$$

Also ergibt sich

$$\begin{aligned}
\langle x - \lambda y, x - \lambda y\rangle &= \langle x, x\rangle - \frac{\langle x, y\rangle}{\langle y, y\rangle}\,\langle y, x\rangle - \overline{\lambda}\,\langle x, y\rangle + \overline{\lambda}\frac{\langle x, y\rangle}{\langle y, y\rangle}\,\langle y, y\rangle \\
&= \|x\|^2 - \frac{\langle x, y\rangle}{\|y\|^2}\,\langle y, y\rangle \\
&\leq \|x\|^2 - \frac{\langle x, y\rangle}{\|y\|^2} \\
\frac{\langle x, y\rangle}{\|y\|^2} &\leq \|x\|^2 \\
\langle x, y\rangle &\leq \|x\|^2 \cdot \|y\|^2 \\
\Rightarrow |\,\langle x, y\rangle\,| &\leq \|x\| \cdot \|y\|
\end{aligned}$$

Satz 1.5
Die euklidische Norm erfüllt die folgenden Eigenschaften:

- Für $x \in \mathbb{R}^n$ ist $\|x\| = 0 \iff x = 0$
- Für $x \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ ist $\|\lambda x\| = |\lambda| \cdot \|x\|$
- Für $x, y \in \mathbb{R}^n$ ist $\|x + y\| \leq \|x\| + \|y\|$

Beweis.
- Satz 1.2
- Satz 1.2
- $\|x+y\|^2 = \langle x+y, x+y\rangle = \langle x,x\rangle + 2\langle x,y\rangle + \langle y,y\rangle \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2 \overset{1.4}{\Rightarrow} \|x+y\| \leq \|x\| + \|y\|$ □

Sei nun $K = \mathbb{C}$.

Definition 1.6 (komplexe Konjugation, Absolutbetrag)
Für $x, y \in \mathbb{R}$ und $z = x + iy \in \mathbb{C}$ definiert man $\overline{z} = x - iy$ heißt komplexe Konjugation . Man definiert den Absolutbetrag von z als

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2} \in \mathbb{R}_{\geq 0}$$

Für $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{m\times n}(\mathbb{C})$ sehen wir

$$\bar{A} = (\overline{a_{ij}})_{i,j} \in \mathrm{Mat}_{m\times n}(\mathbb{C})$$

Satz 1.7
Komplexe Konjugation ist ein Ringautomorphismus von $\mathbb{C}$ mit Fixkörper

$$\{z \in \mathbb{C} \mid z = \overline{z}\} = \mathbb{R}$$

Beweis. siehe LAAG1 H47 □

Folgerung 1.8
Für $A, B \in \mathrm{Mat}_n(\mathbb{C})$ und $S \in \mathrm{GL}_n(\mathbb{C})$ ist $\overline{A+B} = \overline{A} + \overline{B}, \overline{AB} = \overline{A} \cdot \overline{B}, \overline{A^t} = \overline{A}^t, \overline{S^{-1}} = \overline{S}^{-1}$

Beweis. Satz 1.7, einfache Übung □

Definition 1.9 (Standardskalarprodukt in $\mathbb{C}$)
Auf $V = \mathbb{C}^n$ definiert man das Standardskalarprodukt in $\mathbb{C}$ $\langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ durch

$$\langle x, y\rangle = x^t \overline{y} = \sum_{i=1}^{n} x_i \overline{y}_i$$

Satz 1.10
Das komplexe Standardskalarprodukt erfüllt die folgenden Eigenschaften:

- Für $x, x', y, y' \in \mathbb{C}^n$ und $\lambda \in \mathbb{C}$ ist:

$$\begin{aligned}\langle x + x', y\rangle &= \langle x, y\rangle + \langle x', y\rangle\\ \langle \lambda x, y\rangle &= = \lambda\langle x, y\rangle\\ \langle x, y + y'\rangle &= \langle x, y\rangle + \langle x, y'\rangle\\ \langle x, \lambda y\rangle &= \overline{\lambda}\langle x, y\rangle\end{aligned}$$

- Für $x, y \in \mathbb{C}^n$ ist $\langle x, y\rangle = \overline{\langle y, x\rangle}$
- Für $x \in \mathbb{C}^n$ ist $\langle x, x\rangle \in \mathbb{R}_{\geq 0}$ und $\langle x, x\rangle = 0 \iff x = 0$

Beweis.
- klar
- klar
- $\langle x, x\rangle = \sum_{i=1}^n x_i\overline{x_i} = \sum_{i=1}^n |x_i|^2$ □

Definition 1.11 (euklidische Norm in $\mathbb{C}$)
Auf $V = \mathbb{C}^n$ definiert man die euklidische Norm in $\mathbb{C}$ $\|\cdot\| : \mathbb{C}^n \to \mathbb{R}_{\geq 0}$ durch

$$\|x\| = \sqrt{\langle x, x\rangle}$$

▶ **Bemerkung 1.12**
Schränkt man das komplexe Skalarprodukt auf den $\mathbb{R}^n$ ein, so erhält man das Standardskalarprodukt auf dem $\mathbb{R}^n$. Wir werden ab jetzt die beiden Fälle $K = \mathbb{R}$ und $K = \mathbb{C}$ parallel behandeln. Wenn nicht anders angegeben, werden wir die Begriffe für den komplexen Fall benutzen, aber auch den reellen Fall einschließen.

2. Bilinearformen und Sesquilinearformen

Sei $K = \mathbb{R}$ oder $K = \mathbb{C}$.

Definition 2.1 (Bilinearform, Sesquilinearform)
Eine Bilinearform ($K = \mathbb{R}$) bzw. Sesquilinearform ($K = \mathbb{C}$) ist eine Abbildung $s : V \times V \to K$ für die gilt:

- Für $x, x', y \in V$ ist $s(x + x', y) = s(x, y) + s(x', y)$
- Für $x, y, y' \in V$ ist $s(x, y + y') = s(x, y) + s(x, y')$
- Für $x, y \in V$, $\lambda \in K$ ist $s(\lambda x, y) = \lambda s(x, y)$
- Für $x, y \in V$, $\lambda \in K$ ist $s(x, \lambda y) = \overline{\lambda} s(x, y)$

▶ **Bemerkung 2.2**
Im Fall $K = \mathbb{R}$ ist $\lambda = \overline{\lambda}$. Wir werden der Einfachheit halber auch in diesem Fall von Sesquilinearformen sprechen, vgl. Bemerkung 1.12

■ **Beispiel 2.3**
Für $A = (a_{ij})_{i,j} \in \mathrm{Mat}_n(K)$ ist $s_A : K^n \times K^n \to K^n$ gegeben durch

$$s_A(x, y) = x^t A\overline{y} = x^t \left(\sum_{j=1}^{n} a_{ij} \overline{y}_j \right)_i = \sum_{i,j=1}^{n} a_{ij} x_i \overline{y}_j$$

eine Sesquilinearform auf $V = K^n$.

Definition 2.4
Sei s eine Sesquilinearform auf V und $B = (v_1, ..., v_n)$ eine Basis von V. Die darstellende Matrix von s bzgl. B ist

$$M_B(s) = (s(v_i, v_j))_{i,j} \in \mathrm{Mat}_n(K)$$

■ **Beispiel 2.5**
Die darstellende Matrix des Standardskalarprodukts $s = s_{\mathbb{1}_n}$ auf den Standardraum $V = K^n$ bzgl. der Standardbasis $\mathcal{E}$ ist

$$M_{\mathcal{E}}(s) = \mathbb{1}_n$$

Lemma 2.6
Seien $v, w \in V$. Mit $x = \Phi_B^{-1}(v)$, $y = \Phi_B^{-1}(w)$ und $A = M_B(s)$ ist $s(v, w) = x^t A\overline{y} = s_A(x, y)$.

Beweis. Achtung: v_i beschreibt das i-te Element der Basis B!
$s(v, w) = s(\sum_{i=1}^n x_i v_i, \sum_{j=1}^n y_j v_j) = \sum_{i,j=1}^n x_i \overline{y} s(v, v_j) = x^t A\overline{y}$ □

Satz 2.7
Sei B eine Basis von V. Die Abbildung $s \mapsto M_B(s)$ ist eine Bijektion zwischen den Sesquilinearformen auf V und $\mathrm{Mat}_n(K)$.

Beweis.
- injektiv: Lemma 2.6
- surjektiv: Für $A \in \mathrm{Mat}_n(K)$ wird durch $s(v,w) = \Phi_B^{-1}(v)^t \cdot A \cdot \overline{\Phi_B^{-1}(w)}$ eine Sesquilinearform auf V mit $M_B(s) = (s(v_i, w_j))_{i,j} = (e_i^t A \overline{e_j})_{i,j} = (e_i A e_j)_{i,j} = A$ definiert. □

Satz 2.8 (Transformationsformel)
Seien B und B' Basen von V und s eine Sesquilinearform auf V. Dann gilt:

$$M_{B'}(s) = (T_B^{B'})^t \cdot M_B(s) \cdot \overline{T_B^{B'}}$$

Beweis. Seien $v, w \in V$. Definiere $A = M_B(s)$, $A' = M_{B'}(s)$, $T = T_B^{B'}$ und $x, y, x', y' \in K^n$ mit $v = \Phi_B(x) = \Phi_B(x')$, $w = \Phi_B(y) = \Phi_B(y')$. Dann ist $x = Tx'$, $y = Ty'$ und somit

$$\begin{aligned}(x')^t A' \overline{y'} &\overset{2.6}{=} s(v,w) \\ &\overset{2.6}{=} x^t A \overline{y} \\ &= (Tx')^t A \overline{Ty'} \\ &= (x')^t T^t A \overline{T} \overline{y'}\end{aligned}$$

Da $v, w \in V$ und somit $x', y' \in K$ beliebig waren, folgt $A = T^t A \overline{T}$. □

■ **Beispiel 2.9**
Sei s das Standardskalarprodukt auf dem K^n und $B = (b_1, ..., b_n)$ eine Basis des K^n. Dann ist

$$M_B(s) = (T_{\mathcal{E}}^B)^t \cdot M_{\mathcal{E}}(s) \cdot \overline{T_{\mathcal{E}}^B} = B^t \cdot \mathbb{1}_n \cdot \overline{B} = B^t B$$

wobei $B = (b_1, ..., b_n) \in \mathrm{Mat}_n(K)$.

Satz 2.10
Sei s eine Sesquilinearform auf V. Dann sind äquivalent:
- Es gibt $0 \neq v \in V$ mit $s(v,w) = 0$ für alle $w \in V$.
- Es gibt $0 \neq w \in V$ mit $s(v,w) = 0$ für alle $v \in V$.
- Es gibt eine Basis B von V mit $\det(M_B(s)) = 0$.
- Für jede Basis B von V gilt $\det(M_B(s)) = 0$.

Beweis. Sei B eine Basis von V, $v = \Phi_B(x)$ und $A = M_B(s)$. Genau dann ist die (semilineare) Abbildung $w \mapsto s(v,w)$ die Nullabbildung, wenn $x^t A \overline{y} = 0$ für alle $y \in K^n$, also wenn $0 = x^t A$, d.h. $A^t x = 0$. Somit ist (1) genau dann erfüllt, wenn A^t nicht invertierbar ist, also wenn $0 = \det(A^t) = \det(A)$. Damit (1) ⇒ (4) ⇒ (3) ⇒ (1) gezeigt und (2) ⟺ (4) zeigt man analog. □

Definition 2.11 (ausgeartet)
Eine Sesquilinearform s auf V heißt ausgeartet , wenn eine der äquivalenten Bedingungen aus Satz 2.10 erfüllt ist, sonst nicht-ausgeartet.

Definition 2.12 (symmetrisch, hermitesch)
Eine Sesquilinearform s auf V heißt symmetrisch , wenn bzw. hermitesch , wenn

$$s(x,y) = \overline{s(y,x)} \quad \text{für alle } x,y \in V$$

Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt symmetrisch bzw. hermitesch, wenn $A = A^* = \overline{A}^t = \overline{A^t}$.

Mathematica/WolframAlpha-Befehle (symmetrische bzw. hermitesche Matrizen)
Wie für vieles Andere auch, hat Mathematica bzw. WolframAlpha auch dafür eine Funktion:

```
SymmetricMatrixQ[A]
HermitianMatrixQ[A]
```

Satz 2.13
Sei s eine Sesquilinearform auf V und B eine Basis von V. Genau dann ist s hermitesch, wenn $M_B(s)$ dies ist.

Beweis. ($\Rightarrow$): klar aus Definition von $M_B(s)$.
($\Leftarrow$): $x = \Phi_B^{-1}$, $y = \Phi_B^{-1}(w)$, $\overline{s(v,w)} = \overline{s(v,w)^t} = \overline{(x^t A \overline{y})^t} = y^t \overline{A^t} \overline{x} = s(w,v)$ □

Satz 2.14
Für $A, B \in \mathrm{Mat}_n(K)$ und $S \in \mathrm{GL}_n(K)$ ist $(A+B)^* = A^* + B^*$, $(AB)^* = B^* A^*$, $(A^*)^* = A$ und $(S^{-1})^* = (S^*)^{-1}$.

Beweis. Folgerung 1.8, Lemma 1.14, Satz 1.15 □

3. Euklidische und unitäre Vektorräume

Lemma 3.1
Sei s eine hermitesche Sesquilinearform auf V. Dann ist $s(x,x) \in \mathbb{R}$ für alle $x \in V$.

Beweis. Da s hermitesch ist, ist $s(x,x) = \overline{s(x,x)}$, also $s(x,x) \in \mathbb{R}$. □

Definition 3.2 (quadratische Form)
Sei s eine hermitesche Sesquilinearform auf V. Die quadratische Form zu s ist die Abbildung

$$q_s : \begin{cases} V \to \mathbb{R} \\ x \mapsto s(x,x) \end{cases}$$

▶ **Bemerkung 3.3**
Die quadratische Form q_s erfüllt das $q_s(\lambda x) = |\lambda|^2 \cdot q_s(x)$ für alle $x \in V$, $\lambda \in K$. Im Fall $K = \mathbb{R}$, $V = \mathbb{R}^n$, $x = (x_1, ..., x_n)^t$, $s = s_A$, $A \in \mathrm{Mat}_n(\mathbb{R})$ ist $q_s(x) = s_A(x,x) = x^t A x = \sum_{i,j=1}^n a_{ij} x_i x_j$ ein "quadratisches Polynom in den Variablen $x_1, ..., x_n$".

Satz 3.4 (Polarisierung)
Sei s ein hermitesche Sesquilinearform auf V. Dann gilt für $x, y \in V$:

$$s(x,y) = \frac{1}{2}(q_s(x+y) - q_s(x) - q_s(y)) \quad K = \mathbb{R}$$
$$s(x,y) = \frac{1}{4}(q_s(x+y) - q_s(x-y) + iq_s(x+iy) - iq_s(x-iy)) \quad K = \mathbb{C}$$

Beweis. Im Fall $K = \mathbb{R}$ ist

$$\begin{aligned} q_s(x+y) - q_s(x) - q_s(y) &= s(x+y, x+y) - s(x,x) - s(y,y) \\ &= s(x,x) + s(x,y) + s(y,x) + s(y,y) - s(x,x) - s(y,y) \\ &= s(x,y) + s(y,x) - 2s(x,y) \end{aligned}$$

Im Fall $K = \mathbb{C}$: ÜA □

Definition 3.5 ((semi)definit, euklidischer Vektorraum, unitärer Vektorraum)
Sei s eine hermitesche Sesquilinearform auf V. Ist $s(x,x) \geq 0$ für alle $x \in V$, so heißt s positiv semidefinit . Ist $s(x,x) > 0$ für alle $0 \neq x \in V$, so heißt s positiv definit (oder ein Skalarprodukt).

Eine hermitesche Matrix $A \in \mathrm{Mat}_n(K)$ heißt positiv (semi)definit, wenn s_A dies ist.

Einen endlichdimensionalen K-Vektorraum zusammen mit positiv definiten hermiteschen Sesquilinearformen nennt man einen euklidischen bzw. unitären Vektorraum (oder auch Prähilbertraum). Wenn nicht anderes angegeben, notieren wir die Sesquilinearform mit $\langle \cdot, \cdot \rangle$.

■ **Beispiel 3.6**
Der Standardraum $V = K^n$ zusammen mit dem Standardskalarprodukt ist ein euklidischer bzw. unitärer Vektorraum.

■ **Beispiel 3.7**
Ist $A = \text{diag}(\lambda_1, ..., \lambda_n)$ mit $\lambda_i \in \mathbb{R}$, so ist s_A genau dann positiv definit, wenn $\lambda_i > 0$ für alle i, und positiv semidefinit, wenn $\lambda_i \geq 0$ für alle i.

Satz 3.8
Ist V ein unitärer Vektorraum und $U \subseteq V$ ein Untervektorraum, so ist U mit der Einschränkung des Skalarprodukts wieder ein unitärer Vektorraum.

Beweis. klar, die Einschränkung ist wieder positiv definit. □

Definition 3.9
Ist V ein unitärer Vektorraum, so definiert man die Norm von $x \in V$ als

$$\|x\| = \sqrt{\langle x, x \rangle} \in \mathbb{R}_{\geq 0}$$

Satz 3.10
Die Norm eines unitären Vektorraums erfüllt die folgenden Eigenschaften:

- Für $x \in V$ ist $\|x\| = 0 \iff x = 0$
- Für $x \in V$ und $\lambda \in K$ ist $\|\lambda x\| = |\lambda| \cdot \|x\|$
- Für $x, y \in V$ ist $\|x + y\| \leq \|x\| + \|y\|$

Beweis.
- Das Skalarprodukt ist positiv definit.
- klar
- Wie im Fall im $\mathbb{R}^n$ □

Satz 3.11
Ist V ein unitärer Vektorraum, so gilt für $x, y \in V$:

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

Dabei gilt Gleichheit genau dann, wenn x und y linear abhängig sind.

Beweis. Für $y = 0$ ist die Aussage klar.
Sei also $y \neq 0$. Für $\lambda, \mu \in K$ ist

$$\begin{aligned} 0 &\leq \langle \lambda x + \mu y, \lambda x + \mu y \rangle \\ &= \lambda\overline{\lambda} \cdot \langle x, x \rangle + \mu\overline{\mu} \cdot \langle y, y \rangle + \lambda\overline{\mu} \cdot \langle x, y \rangle + \mu\overline{\lambda} \cdot \langle y, x \rangle \end{aligned}$$

Setzt man $\lambda = \overline{\lambda} = \langle y, y \rangle > 0$ und $\mu = -\langle x, y \rangle$ ein, so erhält man

$$\begin{aligned} 0 &\leq \lambda \cdot \|x\|^2 \|y\|^2 + \mu\overline{\mu}\lambda - \lambda\mu\overline{\mu} - \langle x, y \rangle \overline{\lambda} \langle y, x \rangle \\ &= \lambda(\|x\|^2 \|y\|^2 - |\langle x, y \rangle|^2) \end{aligned}$$

Teilen durch λ und Wurzelziehen liefert die Ungleichung. Gilt dort Gleichheit, so ist $\|\lambda x + \mu y\| = 0$ folglich (da $\lambda \neq 0$) sind dann x, y linear unabhängig. Ist $x = \alpha y$ mit $\alpha \in K$, so ist $|\langle x, y \rangle| = |\alpha| \cdot \|y\|^2 = \|x\| \cdot \|y\|$ □

4. Orthogonalität

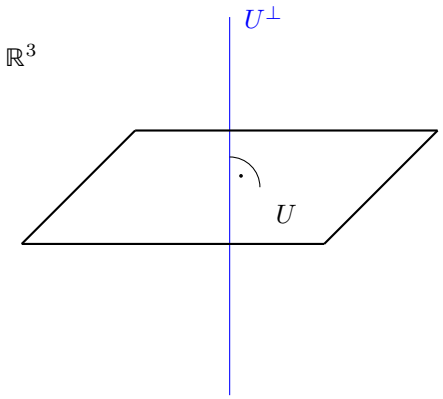
Sei V ein euklidischer bzw. unitärer Vektorraum.

Definition 4.1 (orthogonal, orthogonales Komplement)
Zwei Vektoren $x, y \in V$ heißen orthogonal , in Zeichen $x \perp y$, wenn $\langle x, y\rangle = 0$. Zwei Mengen $X, Y \subseteq V$ sind orthogonal, in Zeichen $X \perp Y$, wenn $x \perp y$ für alle $x \in X$ und $y \in Y$.

Für $U \subseteq V$ bezeichnet

$$U^\perp = \{x \in V \mid x \perp u \text{ für alle } u \in U\}$$

das orthogonale Komplement zu U.



Lemma 4.2
Für $x, y \in V$ ist

- $x \perp y \iff y \perp x$
- $x \perp 0$
- $x \perp x \iff x = 0$

Beweis. klar □

Satz 4.3
Für $U \subseteq V$ ist $U^\perp$ ein Untervektorraum von V mit $U \perp U^\perp$ und $U \cap U^\perp \subseteq \{0\}$.

Beweis. Linearität des Skalarprodukts im ersten Argument liefert, dass $U^\perp$ ein Untervektorraum ist. Die Aussage $U^\perp \perp U$ ist trivial, $U \perp U^\perp$ folgt dann aus Lemma 4.2. Ist $u \in U \cap U^\perp$, so ist insbesondere $u \perp u$, also $u = 0$ nach Lemma 4.2. □

Definition 4.4 (orthonormal)
Eine Familie $(x_i)_{i\in I}$ von Elementen von V ist orthogonal, wenn $x_i \perp x_j$ für alle $i \neq j$, und orthonormal , wenn zusätzlich $\|x_i\| = 1$ für alle i. Eine orthogonale Basis nennt man eine Orthogonalbasis, eine orthonormale Basis nennt man eine Orthonormalbasis.

▶ **Bemerkung 4.5**
Eine Basis B ist genau dann eine Orthonormalbasis, wenn die darstellende Matrix des Skalarprodukts bezüglich B die Einheitsmatrix ist. (Beispiel: Standardbasis des Standardraum bezüglich des Standardskalarprodukts)

Lemma 4.6
Ist die Familie $(x_i)_{i\in I}$ orthogonal und $x_i \neq 0$ für alle $i \in I$, so ist $(x_i)_{i\in I}$ linear unabhängig.

Beweis. Ist $\sum_{i\in I} \lambda_i x_i = 0$, $\lambda_i \in K$, fast alle gleich 0, so ist $0 = \left\langle \sum_{i\in I} \lambda_i x_i, x_j \right\rangle = \sum_{i\in I} \lambda_i \langle x_i, x_j\rangle = \lambda_j \langle x_j, x_j\rangle$
Aus $x_j \neq 0$ folgt $\langle x_j, x_j\rangle > 0$ und somit $\lambda_j = 0$ für jedes $j \in I$. □

Lemma 4.7
Ist $(x_i)_{i\in I}$ orthogonal und $x_i \neq 0$ für alle i, so ist $(y_i)_{i\in I}$ mit

$$y_i = \frac{1}{\|x_i\|} x_i$$

orthonormal.

Beweis. Für alle i ist $\langle y_i, y_i\rangle = \frac{1}{\|x_i\|^2} \langle x_i, x_i\rangle = 1$.
Für alle $i \neq j$ ist $\langle y_i, y_j\rangle = \frac{1}{\|x_i\|\cdot\|x_j\|} \langle x_i, x_j\rangle = 0$. □

Satz 4.8
Sei $U \subseteq V$ ein Untervektorraum und $B = (x_1, ..., x_k)$ eine Orthonormalbasis von U. Es gibt genau einen Epimorphismus $\mathrm{pr}_U : V \to U$ mit $\mathrm{pr}_U|_U = \mathrm{id}_U$ und $\mathrm{Ker}(\mathrm{pr}_U) \perp U$, insbesondere also $x - \mathrm{pr}_U \perp U$ für alle $x \in V$, genannt die orthogonale Projektion auf U, und dieser ist geben durch

$$x \mapsto \sum_{i=1}^{k} \langle x, x_i\rangle x_i \tag{1}$$

Beweis. Sei zunächst pr_U durch Gleichung (1) gegeben. Die Linearität von pr_U folgt aus (S1) und (S3). Für $u = \sum_{i=1}^{k} \lambda_i x_i \in U$ ist $\langle u, x_j\rangle = \left\langle \sum_{i=1}^{k} \lambda_i x_i, x_j \right\rangle = \sum_{i=1}^{k} \lambda_i \langle x_i, x_j\rangle = \lambda_j$, woraus $\mathrm{pr}_U(u) = u$. Somit ist $\mathrm{pr}_U|_U = \mathrm{id}_U$, und insbesondere ist pr_U surjektiv. Ist $\mathrm{pr}_U(x) = 0$, so ist $\langle x, x_i\rangle = 0$ für alle i., woraus mit (S2) und (S4) sofort $x \perp U$ folgt. Somit ist $\mathrm{Ker}(\mathrm{pr}_U) \perp U$.
Für $x \in V$ ist $\mathrm{pr}_U(x - \mathrm{pr}_U(x)) = \mathrm{pr}_U(x) - \mathrm{pr}_U(\mathrm{pr}_U(x)) = \mathrm{pr}_U(x) - \mathrm{pr}_U(x) = 0$, also $x - \mathrm{pr}_U(x) \in \mathrm{Ker}(\mathrm{pr}_U) \subseteq U^\perp$.
Ist $f : V \to U$ ein weiterer Epimorphismus mit $f|_U = \mathrm{id}_U$ und $\mathrm{Ker}(f) \perp U$, so ist

$$\underbrace{\mathrm{pr}_U(x)}_{\in U} - \underbrace{f(x)}_{\in U} = \underbrace{\mathrm{pr}_U(x) - x}_{\in U^\perp} - \underbrace{f(x) - x}_{\in U^\perp} \in U \cap U^\perp = \{0\}$$

für jedes $x \in V$, somit $f = \mathrm{pr}_U$. □

Theorem 4.9 (Gram-Schmidt-Verfahren)
Ist $(x_1, ..., x_n)$ eine Basis von V und $k \leq n$ mit $(x_1, ..., x_k)$ orthonormal, so gibt es eine Orthonormalbasis $(y_1, ..., y_n)$ von V mit $y_i = x_i$ für $i = 1, ..., k$ und $\text{span}_K(y_1, ..., y_l) = \text{span}_K(x_1, ..., x_l)$ für $l = 1, ..., n$.

Beweis. Induktion nach $d = n - k$.
$\underline{d = 0}$: nichts zu zeigen
$\underline{d - 1 \to d}$: Für $i \neq k+1$ definiere $y_I = x_i$. Sei $U = \text{span}_K(x_1, ..., x_k)$, $\tilde{x_{k+1}} = x_{k+1} - \text{pr}_U(x_{k-1})$. Dann ist $\tilde{x_{k+1}} \in \text{Ker}(\text{pr}_U) \subseteq U^\perp$ (vgl. Satz 4.8) und $\text{span}_K(x_1, ..., x_k, \tilde{x_{k+1}}) = \text{span}_K(x_1, ..., x_{k+1})$. Setze $y_{k+1} = \frac{1}{\|\tilde{x_{k+1}}\|}\tilde{x_{k+1}}$. Dann ist $(y_1, ..., y_n)$ eine Basis von V mit $(y_1, ..., y_{k+1})$ orthonormal (vgl. Lemma 4.7). Nach Induktionshypothese gibt es eine Orthonormalbasis von V, die das Gewünschte leistet. □

Folgerung 4.10
Jeder endlichdimensionale euklidische bzw. unitäre Vektorraum V besitzt eine Orthonormalbasis.

Beweis. Wähle irgendeine Basis von V und wende Theorem 4.9 mit $k = 0$ an. □

Folgerung 4.11
Ist U ein Untervektorraum von V, so ist $V = U \oplus U^\perp$ und $(U^\perp)^\perp = U$.

Beweis. Wähle eine Orthonormalbasis von U (vgl. Folgerung 4.10), $B = (x_1, ..., x_k)$ und ergänze diese zu einer Orthonormalbasis $(x_1, ..., x_n)$ von V (vgl. Theorem 4.9). Dann sind $x_{k+1}, ..., x_n \in U \perp$, da $U \cap U^\perp = \{0\}$ ist somit $V = U \oplus U^\perp$. Insbesondere ist $\dim_K(U^\perp) = n - \dim_K(U)$, woraus $\dim_K((U^\perp)^\perp) = \dim_K(U)$ folgt. Zusammen mit der trivialen Inklusion $U \subseteq (U^\perp)^\perp$ folgt $U = (U^\perp)^\perp$. □

Folgerung 4.12
Ist s eine positiv definite hermitesche Sesquilinearform auf V und B eine Basis von V, so ist

$$\det(M_B(s)) \in \mathbb{R}_{>0}$$

Beweis. Wähle eine Orthonormalbasis B' von V bezüglich s. Dann ist $M_{B'}(s) = \mathbb{1}_n$, folglich

$$\begin{aligned}
\det(M_B(s)) &= \det\left((T^B_{B'})^t \cdot \mathbb{1}_n \cdot \overline{T^B_{B'}}\right) \\
&= \det\left((T^B_{B'})^t\right) \cdot \det\left(\overline{T^B_{B'}}\right) \\
&= \det\left(T^B_{B'}\right) \cdot \overline{\det\left(T^B_{B'}\right)} \\
&= |\det\left(T^B_{B'}\right)|^2 \\
&> 0
\end{aligned}$$

□

5. Orthogonale und unitäre Endomorphismen

Sei V ein euklidischer bzw. unitärer Vektorraum und $f \in \mathrm{End}_K(V)$.

Definition 5.1 (orthogonale, unitäre Endomorphismen)
f ist orthogonal bzw. unitär , wenn

$$\langle f(x), f(y)\rangle = \langle x, y\rangle \quad \forall x, y \in V$$

Satz 5.2
Ist f unitär, so gelten

- Für $x \in V$ ist $\|f(x)\| = \|x\|$.
- Sind $x, y \in V$ mit $x \perp y$, so ist $f(x) \perp f(y)$.
- Es ist $f \in \mathrm{Aut}_K(V)$ und auch f^{-1} ist unitär.
- Das Bild einer Orthonormalbasis unter f ist eine Orthonormalbasis.
- Ist λ ein Eigenwert von f, so ist $|\lambda| = 1$.

Beweis.

- klar
- klar
- $f(x) = 0 \iff \|f(x)\| = 0 \iff \|x\| = 0 \iff x = 0$, also ist f injektiv, somit $f \in \mathrm{Aut}_K(V)$ und

$$\left\langle f^{-1}(x), f^{-1}(y)\right\rangle \overset{f \text{ unitär}}{=} \left\langle f(f^{-1}(x)), f(f^{-1}(y))\right\rangle = \langle x, y\rangle$$

- Folgt aus 1, 2 und 3
- Ist $f(x) = \lambda x$, $x \neq 0$, so ist

$$\|x\| = \|f(x)\| = \|\lambda x\| = |\lambda| \cdot \|x\| \Rightarrow |\lambda| = 1$$

□

Satz 5.3
Ist $\|f(x)\| = \|x\|$ für alle $x \in V$, so ist f unitär.

Beweis. Aus $\|f(x)\| = \|x\|$ folgt $\langle f(x), f(x)\rangle = \langle x, x\rangle$. Die Polarisierung (Satz 3.4) für $\langle f(x), f(y)\rangle$ und die Linearität von f liefern $\langle f(x), f(y)\rangle = \langle x, y\rangle$. Zum Beispiel im Fall $K = \mathbb{R}$:

$$\begin{aligned}
\langle f(x), f(y)\rangle &= \frac{1}{2}\left(\left\langle \underbrace{f(x)+f(y)}_{f(x+y)}, \underbrace{f(x)+f(y)}_{f(x+y)}\right\rangle - \langle f(x), f(x)\rangle - \langle f(y), f(y)\rangle\right) \\
&= \frac{1}{2}\left(\langle x+y, x+y\rangle - \langle x, x\rangle - \langle y, y\rangle\right) \\
&= \langle x, y\rangle
\end{aligned}$$

□

Definition 5.4 (orthogonale, unitäre Matrizen)
Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt orthogonal bzw. unitär , wenn

$$A^*A = \mathbb{1}_n$$

Mathematica/WolframAlpha-Befehle (orthogonale bzw. unitäre Matrizen)
Auch für orthogonale bzw. unitäre Matrizen A gibt es eine Mathematica bzw. WolframAlpha-Funktion

```
OrthogonalMatrixQ[A]
UnitaryMatrixQ[A]
```

▶ **Bemerkung 5.5**
Offenbar ist A genau dann unitär, wenn A^* das Inverse zu A ist. Die folgenden Bedingungen sind daher äquivalent dazu, dass A unitär ist:

$$AA^* = \mathbb{1}_n, \overline{A}A^t = \mathbb{1}_n, A^t\overline{A} = \mathbb{1}_n, A^t = \overline{A^{-1}}$$

Satz 5.6
Sei B eine Orthogonalbasis von V. Genau dann ist f unitär, wenn $M_B(f)$ unitär ist.

Beweis. Sei $A = M_B(f)$, $v = \Phi_B(x)$, $\Phi_B(y)$. Dann ist $\langle v, w\rangle = x^t \underbrace{M_B(\langle\cdot,\cdot\rangle)}_{=\mathbb{1}} \cdot \overline{y} = x^t \cdot \overline{y}$. Somit ist f genau dann unitär, wenn $(Ax)^t\overline{Ay} = x^t\overline{y}$ für alle $x, y \in K^n$, also wenn $A^t\overline{A} = \mathbb{1}$, d.h. A unitär. □

Satz 5.7
Die folgenden Mengen bilden Untergruppen der $\mathrm{GL}_n(K)$.

- $\mathrm{O}_n = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A \text{ ist orthogonal}\}$ die orthogonale Gruppe
- $\mathrm{SO}_n = \{A \in \mathrm{O}_n \mid \det(A) = 1\}$ die spezielle orthogonale Gruppe
- $\mathrm{U}_n = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A \text{ ist unitär}\}$ die unitäre Gruppe
- $\mathrm{SU}_n = \{A \in \mathrm{U}_n \mid \det(A) = 1\}$ die spezielle unitäre Gruppe

Beweis. z.B. für U_n: Sind $A^{-1} = A^*$, $B^{-1} = B^*$, so ist $(AB)^{-1} = B^{-1}A^{-1} = B^*A^* = (AB)^*$, $(A^{-1})^{-1} = A = (A^*)^{-1} = (A^{-1})^*$ □

Satz 5.8
Genau dann ist $A \in \mathrm{Mat}_n(K)$ unitär, wenn die Spalten (oder die Zeilen) von A eine Orthonormalbasis des K^n bilden.

Beweis. Sei s das Standardskalarprodukt und $B = (a_1, ..., a_n)$. Nach Bemerkung 4.5 ist B genau dann eine Orthonormalbasis, wenn $M_B(s) = \mathbb{1}_n$, und $M_B(s) = A^t \cdot \mathbb{1}_n \cdot \overline{A}$, vgl. Beispiel 2.9 □

Theorem 5.9
Sei $K = \mathbb{C}$ und $f \in \mathrm{End}_K(V)$. Ist f unitär, so besitzt V eine Orthonormalbasis aus Eigenvektoren von f.

Beweis. Induktion über $n = \dim_K(V)$.
$\underline{n = 0}$: klar
$\underline{n - 1 \to n}$: Da K algebraisch abgeschlossen ist, hat χ_f eine Nullstelle λ, es gibt also einen Eigenvektor x_1 von f zum Eigenwert λ. Ohne Einschränkung nehmen wir $\|x\| = 1$ an. Sei $W = K \cdot x_1$. Nach Folgerung 4.11 ist dann $V = W \oplus W^\perp$. Für $v \in W^\perp, w \in W$ ist

$$0 = \langle v, w\rangle = \langle f(v), f(w)\rangle = \overline{\lambda}\,\langle f(v), w\rangle$$

da $\lambda \neq 0$ (f unitär) also $f(W^\perp) \perp W$. Somit ist $f(W^\perp) \subseteq W^\perp$, d.h. $W^\perp$ ist f-invariant. Da auch $f|_{W^\perp}$ unitär ist, gibt es nach Induktionshypothese eine Orthonormalbasis $(x_1, ..., x_n)$ aus Eigenvektoren von $f|_{W^\perp}$. Da $V = W \oplus W^\perp$ und $W \perp W^\perp$ ist $(x_1, ..., x_n)$ eine Orthonormalbasis von V aus Eigenvektoren von f. □

Folgerung 5.10
Jeder unitäre Endomorphismus eines unitären Vektorraums ist diagonalisierbar.

Folgerung 5.11
Zu jeder $A \in \mathrm{U}_n$ gibt es $S \in \mathrm{U}_n$ so, dass

$$S^*AS = S^{-1}AS = \mathrm{diag}(\lambda_1, ..., \lambda_n)$$

mit $|\lambda_i| = 1$ für $i = 1, ..., n$.

Beweis. Da A unitär ist, ist $f_A \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^n)$ unitär, nach Theorem 5.9 existiert also eine Orthonormalbasis B des $\mathbb{C}^n$ aus Eigenvektoren von A. Die Transformationsmatrix $S = T_{\mathcal{E}}^{B}$ hat als Spalten die Elemente von B und somit ist S nach Satz 5.8 unitär. Nach Satz 5.2 ist $|\lambda| = 1$ für alle Eigenwerte von f_A. □

▶ **Bemerkung 5.12**
Dies (Theorem 5.9) gilt nicht im Fall $K = \mathbb{R}$. Man kann aber auch orthogonale Endomorphismen immer "fast diagonalisieren".

6. Selbstadjungierte Endomorphismen

Sei V ein euklidischer bzw. unitärer Vektorraum und $f \in \mathrm{End}_K(V)$.

Definition 6.1 (selbstadjungiert)
f ist selbstadjungiert , wenn

$$\langle f(x), y\rangle = \langle x, f(y)\rangle \quad \forall x, y \in V$$

Satz 6.2
Sei B eine Orthonormalbasis von V. Genau dann ist f selbstadjungiert, wenn $M_B(f)$ hermitesch ist.

Beweis. Seien $A = M_B(f), v = \Phi_B(x), w = \Phi_B(y)$. Es ist

$$\langle f(v), w\rangle = (Ax)^t\overline{y} = x^tA^t\overline{y}$$
$$\langle v, f(w)\rangle = x^t\overline{Ay} = x^t\overline{A}\overline{y}$$

Somit ist $\langle f(v), w\rangle = \langle v, f(w)\rangle$ genau dann, wenn $A^t = \overline{A}$, d.h. $A = A^*$, also A hermitesch. □

Lemma 6.3
Ist f selbstadjungiert und λ ein Eigenwert von f, so ist $\lambda \in \mathbb{R}$.

Beweis. Ist $0 \neq x \in V$ mit $f(x) = \lambda x$, so ist

$$\lambda\langle x, x\rangle = \langle f(x), x\rangle = \langle x, f(x)\rangle = \overline{\lambda}\langle x, x\rangle$$

und mit $\langle x, x\rangle \neq 0$ folgt $\lambda = \overline{\lambda}$, also $\lambda \in \mathbb{R}$. □

Satz 6.4
Ist f selbstadjungiert, so ist $\chi_f \in \mathbb{R}[t]$ und χ_f zerfällt über $\mathbb{R}$ in Linearfaktoren.

Beweis. Sei B eine Orthonormalbasis von V. Nach Satz 6.2 ist $A = M_B(f) \in \mathrm{Mat}_n(K) \subseteq \mathrm{Mat}_n(\mathbb{C})$ hermitesch. Da $\mathbb{C}$ algebraisch abgeschlossen ist, ist $\chi_f(t)\prod_{i=1}^n(t-\lambda_i)$ mit $\lambda_1, ..., \lambda_n \in \mathbb{C}$. Nach Lemma 6.3 ist aber schon $\lambda_1, ..., \lambda_n \in \mathbb{R}$. Somit zerfällt $\chi_f\chi_A \in \mathbb{R}[t]$ über $\mathbb{R}$ in Linearfaktoren. □

Theorem 6.5
Ist f selbstadjungiert, so besitzt V eine Orthonormalbasis aus Eigenvektoren von f.

Beweis. Induktion über $n = \dim_K(V)$.
$n = 0$: klar
$n - 1 \to n$: Nach Satz 6.4 hat f einen reellen Eigenwert $\lambda \in \mathbb{R}$. Wähle $x_1 \in V$ mit $f(x_1) = \lambda x_1$ und $\|x_1\| = 1$. Sei $W = K \cdot x_1$. Für $y \in W^\perp$ ist

$$\langle x_1, f(y)\rangle = \langle f(x_1), y\rangle = \lambda\langle x_1, y\rangle = 0$$

und folglich ist $W^\perp$ f-invariant. Nach Folgerung 4.11 ist $V = W \oplus W^\perp$ und $f|_{W^\perp}$ ist wieder selbstadjungiert. Nach Induktionshypothese hat $W^\perp$ eine Orthonormalbasis $(x_1, ..., x_n)$ aus Eigenvektoren von $f|_{W^\perp}$. Da $V = W \oplus W^\perp$ und $W \perp W^\perp$ ist $(x_1, ..., x_n)$ eine Orthonormalbasis von V aus Eigenvektoren von f. □

Folgerung 6.6
Jeder selbstadjungierte Endomorphismus eines euklidischen oder unitären Vektorraums ist diagonalisierbar.

Folgerung 6.7
Ist

- f selbstadjungiert ($K = \mathbb{C}$ oder $\mathbb{R}$)
- f unitär ($K = \mathbb{C}$)

so ist

$$V = \bigoplus_{\lambda \in K} \mathrm{Eig}(f, \lambda)$$

eine Zerlegung von V in paarweise orthogonale Untervektorräume.

Beweis. Nach Theorem 5.9 bzw. Theorem 6.5 existiert eine Orthonormalbasis B aus Eigenvektoren. Insbesondere ist f diagonalisierbar, also

$$V = \bigoplus_{\lambda \in K} \mathrm{Eig}(f, \lambda)$$

Zu jedem λ gibt es eine Teilfamilie von B die eine Basis von $\mathrm{Eig}(f, \lambda)$ bildet. Da B eine Orthonormalbasis ist, folgt, dass die Eigenräume paarweise orthogonal sind. □

▶ **Bemerkung 6.8**
Um eine Orthonormalbasis aus Eigenvektoren wie in Theorem 5.9 oder Theorem 6.5 zu bestimmen, kann man entweder wie im Induktionsbeweis vorgehen, oder man bestimmt zunächst Basen B von $\mathrm{Eig}(f, \lambda_i)$, $i = 1, ..., n$ und orthonormalisiert diese mit Theorem 4.9 zu Basen B'. Nach Folgerung 6.7 ist $\bigcup B'$ dann eine Orthonormalbasis von V aus Eigenvektoren von f.

7. Hauptachsentransformation

Sei V ein euklidischer bzw. unitärer Vektorraum und s eine hermitesche Sesquilinearform auf V.

Satz 7.1
Zu $A \in \mathrm{Mat}_n(K)$ hermitesch gibt es $S \in \mathrm{U}_n(K)$ so, dass

$$S^* AS = S^{-1} AS = \mathrm{diag}(\lambda_1, ..., \lambda_n)$$

mit $\lambda_1, ..., \lambda_n \in \mathbb{R}$.

Beweis. Da A hermitesch ist, ist $f_A \in \mathrm{End}_K(K^n)$ selbstadjungiert, es gibt also nach Theorem 6.5 also eine Orthonormalbasis $B = (x_1, ..., x_n)$ aus Eigenvektoren von f_A. Die Transformationsmatrix $S = T_{\mathcal{E}}^B$ hat $x_1, ..., x_n$ als Spalten und ist somit nach Satz 5.8 unitär. Nach Lemma 6.3 sind die Eigenvektoren $\lambda_1, ..., \lambda_n$ reell. □

Folgerung 7.2
Sei $A \in \mathrm{Mat}_n(K)$ hermitesch. Genau dann ist A positiv definit, wenn alle Eigenwerte positiv sind.

Beweis. Nach Satz 7.1 existiert $S \in \mathrm{U}_n(K)$ mit

$$S^* AS = S^{-1} AS = D = \mathrm{diag}(\lambda_1, ..., \lambda_n) \quad \lambda_1, ..., \lambda_n \in \mathbb{R}$$

Die Eigenwerte von A sind die Eigenwerte von $S^{-1}AS$, also $\lambda_1, ..., \lambda_n$. Sei $T = \overline{S}$. Genau dann ist A positiv definit, wenn $T^t A\overline{T} = S^* AS = D$ positiv definit ist (Satz 2.8), also wenn $\lambda_i > 0$. □

Theorem 7.3 (Hauptachsentransformation)
Zu jeder hermiteschen Sesquilinearform s auf V gibt es eine Orthonormalbasis B von V, für die

$$M_B(s) = \mathrm{diag}(\lambda_1, ..., \lambda_n) \quad \lambda_1, ..., \lambda_n \in \mathbb{R}$$

Beweis. Sei $B_0 = (x_1, ..., x_n)$ eine Orthonormalbasis von V und $A = M_{B_0}(s)$. Da s hermitesch ist, ist auch A hermitesch (Satz 2.13). Nach Satz 7.1 gibt es deshalb $S \in \mathrm{U}_n(K)$ mit $S^* AS = D$ eine reelle Diagonalmatrix. Ist nun $f \in \mathrm{End}_K(V)$ mit $M_{B_0}(f) = \overline{S}$, so ist auch $B = (f(x_1), ..., f(x_n))$ eine Basis von V mit $T_{B_0}^B = \overline{S}$ unitär. Da $M_{B_0}(f)$ unitär ist, ist auch f unitär. Nach Satz 5.2 ist $f(B_0) = B$ somit auch eine Orthonormalbasis. Nach Satz 2.8 ist

$$M_B(s) = (T_{B_0}^B)^t \cdot M_{B_0}(s) \cdot \overline{T_{B_0}^B} = S^* AS = D$$ □

■ **Beispiel 7.4**
$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $s = s_A$, $K = \mathbb{R}$, $V = \mathbb{R}^2$
$\Rightarrow q_s(x) = 2x_1^2 + 2x_1x_2 + 2x_2^2$
Wie verhält sich $q_s : \mathbb{R}^2 \to \mathbb{R}$? Wie sehen die "Höhenlinien"

$$H_c = \{x \in \mathbb{R}^2 \mid q_s(x) = c\} \quad c \in \mathbb{R}$$

aus?

$$\chi_A = (t-2)^2 - 1 = (t-1)(t-3) \Rightarrow \lambda_1 = 3, \lambda_2 = 1$$
$$\Rightarrow B = \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right)$$
$$\Rightarrow M_B(s) = \operatorname{diag}(3, 1)$$

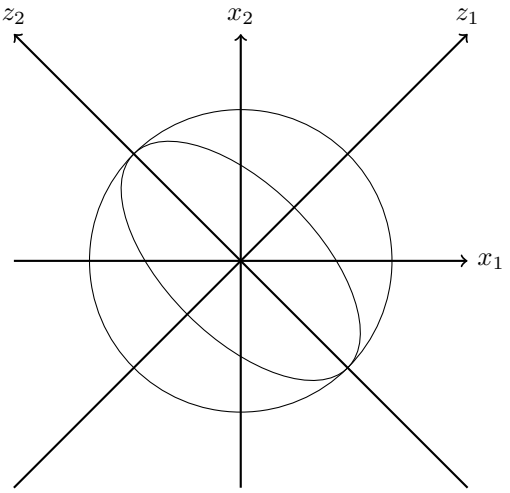
Im neuen Koordinatensystem $z = \Phi_B^{-1}(x)$ ist dann

$$q_s(z) = 3z_1^2 + z_2^2$$

Mit $a_1 = \frac{1}{\sqrt{3}}$, $a_2 = 1$ erhält man "Höhenlinien" der Form

$$\left(\frac{z_1}{a_1}\right)^2 + \left(\frac{z_2}{a_2}\right)^2 = c$$

was für $c > 0$ eine Ellipse beschreibt.



Folgerung 7.5
Zu jeder hermiteschen Sesquilinearform s auf V gibt es eine Basis B von V, für die

$$M_B(s) = \begin{pmatrix} \mathbb{1}_{\mathbb{r}_+(\mathbb{s})} & & \\ & -\mathbb{1}_{\mathbb{r}_-(\mathbb{s})} & \\ & & 0 \end{pmatrix}$$

mit $r_+(s) + r_-(s) \leq n$.

Beweis. Sei $B_0 = (x_1, ..., x_n)$ eine Orthonormalbasis von V mit $A = M_{B_0}(s) = \operatorname{diag}(\lambda_1, ..., \lambda_n)$. Setze

$$\mu_i = \begin{cases} \frac{1}{\sqrt{|\lambda_i|}} & \lambda_i \neq 0 \\ 1 & \lambda_i = 0 \end{cases}$$

Sei $x_i' = \mu_i \cdot x_i$ und $B' = (x_1', ..., x_n')$. Dann ist $M_B(s) = S^t A \overline{S}$ mit $S = T_{B_0}^{B'} = \text{diag}(\mu_1, ..., \mu_n)$ also $M_{B'}(s) = \text{diag}(\lambda_1', ..., \lambda_n')$ mit $\lambda_i' = \mu_i \cdot \lambda_i \cdot \overline{\mu_i} = \mu_i^2 \lambda_i \in \{0, 1, -1\}$. Durch Permutation der Elemente von B' erhält man die gewünschte Basis B. □

Definition 7.6 (Ausartungsraum)
Der Ausartungsraum von s ist

$$V_0 = \{x \in V \mid s(x, y) = 0 \quad \forall y \in V\}$$

Lemma 7.7
V_0 ist ein Untervektorraum von V.

Beweis. Klar aus Linearität im ersten Argument. □

Lemma 7.8
Seien V_+ und V_- Untervektorräume von V mit $V = V_+ \oplus V_- \oplus V_0$ und s positiv definit auf V_+, $-s$ positiv definit auf V_-. Dann ist

$$\dim_K(V_+) = \max\{\dim_K(W) \mid \text{Untervektorraum von } V, s \text{ positiv definit auf } V\}$$
$$\dim_K(V_-) = \max\{\dim_K(W) \mid \text{Untervektorraum von } V, -s \text{ positiv definit auf } V\}$$

Beweis. Beweis nur für V_+, analog für V_-.
$\leq$: klar
$\geq$: Ist $W \leq V$ Untervektorraum mit $s(x, x) > 0 \quad \forall x \in W \backslash \{0\}$, so ist $W \cap (V_- \oplus V_+) = \{0\}$. Ist $x = y + z$ mit $y \in V_-$, $z \in V_0$, so ist $s(x, x) = s(y + z, y + z) = \underbrace{s(y, y)}_{\leq 0} + \underbrace{s(y, z) + s(z, y) + s(z, z)}_{=0} \leq 0 \Rightarrow \dim_K(W) \leq \dim_K(V) - \dim_K(V_-) - \dim_K(V_0) = \dim_K(V_+)$. □

Theorem 7.9 (Trägheitssatz von Sylvester)
Für eine hermitesche Sesquilinearform s auf V sind die Zahlen $r_+(s)$, $r_-(s)$ aus Folgerung 7.5 eindeutig bestimmt.

Beweis. Sei B eine Basis von V wie in Folgerung 7.5, $B = (x_1, ..., x_n)$. Definiere

$$V_+ = \text{span}_K(x_1, ..., x_{r_+(s)})$$
$$V_- = \text{span}_K(x_{r_+(s)+1}, ..., x_{r_+(s)+r_-(s)})$$
$$V_0' = \text{span}_K(x_{r_+(s)+r_-(s)+1}, ..., x_n)$$

Dann ist s positiv definit auf V_+, $-s$ positiv definit auf V_- und $V = V_+ \oplus V_- \oplus V_0'$. Es gilt $V_0' = V_0$
$\subseteq$: klar
$\supseteq$: Ist $x = \sum_{i=1}^n \lambda_i x_i \in V_0$, so ist $0 = s(x, x_i) = \lambda_i \cdot s(x_i, x_i)$ für $i = 1, ..., n$ also $\lambda_i = 0$ für $i = 1, ..., r_+(s) + r_-(s)$, d.h. $x \in V_0'$. Nach Lemma 7.8 ist $r_+(s) = \dim_K(V_+)$ nur von s abhängig, analog für $r_-(s)$. □

Definition 7.10 (Signatur)
Die Signatur von s ist das Tripel

$$(r_+(s), r_-(s), r_0(s))$$

wobei $r_0(s) = \dim_K(V_0)$.

Folgerung 7.11
Ist s eine hermitesche Form auf V und B eine Basis von V, so ist die Zahl der positiven bzw. negativen Eigenwerte von $M_B(s)$ gleich $r_+(s)$ bzw. $r_-(s)$, insbesondere also unabhängig von B.

Beweis. Sei $A = M_B(s)$. Nach Satz 7.1 gibt es $S \in \mathrm{U}_n(K)$ mit S^*AS eine reelle Diagonalmatrix. Da $S^* = S^{-1}$ haben A und S^*AS die selben Eigenwerte. Bringt man S^*AS nun in die Form in Folgerung 7.5, so ändern sich die Vorzeichen der Diagonale nicht mehr. □

8. Quadriken

Sei $n \in \mathbb{N}$.

Definition 8.1 (Quadrik)
Eine Quadrik ist eine Teilmenge von $\mathbb{R}^n$ mit

$$Q = \{x \in \mathbb{R}^n \mid x^t A x + 2b^t x + c = 0\}$$

mit $A \in \mathrm{Mat}_n(\mathbb{R})$ symmetrisch, $b^t \in \mathbb{R}^n$ und $c \in \mathbb{R}$.

▶ **Bemerkung 8.2**

- $Q = \{x \in \mathbb{R}^n \mid \sum_{i,j=1}^n a_{ij} x_i y_j + 2\sum_{i=1}^n b_i x_i + c = 0\}$ also Q ist die Nullstellenmenge eines quadratischen Polynoms in $x_1, ..., x_n$
- Q bestimmt A, b, c nicht eindeutig, da $Q(A, b, c) = Q(\lambda A, \lambda b, \lambda c)$
- Man kann A, b, c so normieren, dass $c = 0$ oder $c = 1$

▶ **Bemerkung 8.3**
Seien A, b, c wie in Definition 8.1, so schreiben wir

$$\tilde{A} = \begin{pmatrix} A & b \\ b^t & c \end{pmatrix}$$
$$\tilde{x} = \begin{pmatrix} x \\ 1 \end{pmatrix}$$

Dann ist $Q = \{x \in \mathbb{R}^n \mid \tilde{x}^t \tilde{A} \tilde{x} = 0\}$. Wir schreiben (A, b) für

$$\begin{pmatrix} A & b \end{pmatrix} \in \mathrm{Mat}_{n,n+1}(\mathbb{R})$$

Es gilt $\mathrm{rk}(A) \leq \mathrm{rk}(A, b) \leq \mathrm{rk}(\tilde{A})$.

▶ **Bemerkung 8.4 (Wiederholung)**
Seien V, W K-Vektorräume. $f : V \to W$ heißt affin, wenn $\exists g \in \mathrm{Hom}_K(V, W)$ mit $f(v) = g(v) + w_0$ $\forall v \in V$. Ist f affin und bijektiv, so ist f^{-1} affin, d.h. $\mathrm{Aff}_K(V) = \{f : V \to V \mid f \text{ affin und bijektiv}\}$.
Im Fall von $V = \mathbb{R}^n$, $K = \mathbb{R}$ ist

$$\mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n) = \{f = \tau_z \circ f_T \mid T \in \mathrm{GL}_n(\mathbb{R}), z \in \mathbb{R}^n\}$$

mit $f_T(x) = Tx$ und $\tau_z(x) = x + z$.

Lemma 8.5
Ist $Q \subseteq \mathbb{R}^n$ eine Quadrik, so ist $f(Q)$ eine Quadrik, für $f \in \mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n)$.

Beweis. $f = \tau_z \circ f_T$ mit $T \in \mathrm{GL}_n(\mathbb{R})$ und $z \in \mathbb{R}^n$. Schreibe $S = T^{-1} \in \mathrm{GL}_n(\mathbb{R})$, $\tilde{S} = \begin{pmatrix} S & 0 \\ 0 & 1 \end{pmatrix}$. Es gilt $\tilde{S}\tilde{x} = \widetilde{Sx}$.

$$\begin{aligned} f_T(Q) &= \{Tx \in \mathbb{R}^n \mid \tilde{x}^t \tilde{A} \tilde{x} = 0\} \\ &= \{y \in \mathbb{R}^n \mid (\tilde{S}\tilde{y})^t \tilde{A} \tilde{S} \tilde{y} = 0\} \\ &= \{y \in \mathbb{R}^n \mid \tilde{y}^t \underbrace{\tilde{S}^t \tilde{A} \tilde{S}}_{\begin{pmatrix} S^tAS & S^tb \\ b^tS & c \end{pmatrix}} \tilde{y} = 0\} \end{aligned}$$

Jetzt für τ_z. Sei $U_z = \begin{pmatrix} \mathbb{1} & z \\ 0 & 1 \end{pmatrix}$. $U_z \tilde{x} = \tilde{\tau}_z(x)$. Man folgert analog, dass

$$\tau_z(Q) = \{y \in \mathbb{R}^n \mid \tilde{y}^t \underbrace{U_z^t \tilde{A} U_z}_{\begin{pmatrix} A & Az+b \\ z^tA+b & z^tAz + b^tz + z^tb + c \end{pmatrix}} \tilde{y} = 0\}$$

□

Definition 8.6 (Typen von Quadriken)
Sei Q gegeben durch (A, b, c) wie in Definition 8.1. Q heißt

- vom kegeligen Typ , wenn $\mathrm{rk}(A) = \mathrm{rk}(A, b) = \mathrm{rk}(\tilde{A})$
- eine Mittelpunktsquadrik , wenn $\mathrm{rk}(A) = \mathrm{rk}(A, b) < \mathrm{rk}(\tilde{A})$
- vom parabolischen Typ , wenn $\mathrm{rk}(A) < \mathrm{rk}(A, b)$
- ausgeartet , wenn $\det(\tilde{A}) = 0$

Lemma 8.7
Ist $Q \subseteq \mathbb{R}^n$ eine Quadrik, $f \in \mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n)$. Von dem Typ, von dem Q ist, ist auch $f(Q)$.

Beweis. $f = f_{S^{-1}}$, $S \in \mathrm{GL}_n(\mathbb{R})$. Da $\tilde{S}$ invertierbar ist, ist $\mathrm{rk}(\tilde{A}) = \mathrm{rk}(\tilde{S}^t \tilde{A} \tilde{S})$, analog auch $\mathrm{rk}(S^tAS) = \mathrm{rk}(A)$. $(S^tAS, S^tb) = S^t(A, b) \begin{pmatrix} S & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \mathrm{rk}(S^tAS, S^tb) = \mathrm{rk}(A, b)$. Für $f = \tau_z$ analog. □

Definition 8.8 (Isometrie)
Eine Isometrie des $\mathbb{R}^n$ ist $f \in \mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n)$ mit

$$f(x) = Ax + b$$

mit $b \in \mathbb{R}^n$ und $A \in \mathrm{GL}_n(\mathbb{R})$ ist orthogonal.

▶ **Bemerkung 8.9**
$f : \mathbb{R}^n \to \mathbb{R}^n$ ist eine Isometrie genau dann, wenn $\|f(x) - f(y)\| = \|x - y\|$ für alle $x, y \in \mathbb{R}^n$.

Theorem 8.10 (Klassifikation der Quadriken bis auf Isometrien)
Sei Q eine Quadrik. Es gibt eine Isometrie $f \in \mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n)$ mit $f(Q)$, die eine der folgenden Formen annimmt:

- $f(Q) = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{k} \left(\frac{x_i}{a_i}\right)^2 - \sum_{i=k+1}^{n} \left(\frac{x_i}{a_i}\right)^2 = 0 \right\} \quad k \geq r-k$
- $f(Q) = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{k} \left(\frac{x_i}{a_i}\right)^2 - \sum_{i=k+1}^{n} \left(\frac{x_i}{a_i}\right)^2 = 1 \right\}$
- $f(Q) = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{k} \left(\frac{x_i}{a_i}\right)^2 - \sum_{i=k+1}^{n} \left(\frac{x_i}{a_i}\right)^2 - 2x_{r+1} = 0 \right\} \quad k \geq r-k, r < n$

mit $a_1, ..., a_r \in \mathbb{R}_{>0}$ und $0 \leq k \leq r \leq n$

Beweis. Sei Q gegeben durch (A, b, c). Nach Satz 7.1 gibt es eine orthogonale Matrix $S \in \mathrm{O}_n$ mit $S^t SAS = \mathrm{diag}(\lambda_1, ..., \lambda_n)$. Indem wir Q durch $f_{S^{-1}}(Q)$ ersetzen, können wir also ohne Einschränkung annehmen, dass $A = \mathrm{diag}(\lambda_1, ..., \lambda_n)$. Ohne Einschränkung ist weiter $\lambda_1, ..., \lambda_k > 0$ und $\lambda_{k+1}, ..., \lambda_r < 0$ und $\lambda_{r+1}, ..., \lambda_n = 0$. Dann ist $(e_{r+1}, ..., e_n)$ eine Orthonormalbasis des Ausartungsraums V_0 von s_A.
Wenn wir Q durch $\tau_z(Q)$ ersetzen, wird b durch $Az+b$ ersetzt, wir können deshalb ohne Einschränkung annehmen, dass $b \in V_0$. Ist $n > r$, also $V_0 \neq \{0\}$, so können wir eine Orthonormalbasis $(v_{r+1}, ..., v_n)$ von V_0 mit $b \in \mathrm{span}_{\mathbb{R}}(v_{r+1})$ wählen.
Indem wir Q durch $f_{S^{-1}}(Q)$ mit $S = (e_1, ..., e_r, v_{r+1}, ..., v_n)$ ersetzen, können wir ohne Einschränkung annehmen, dass $b = \mu \cdot e_{r+1}$ mit $\mu \in \mathbb{R}$.
Ist nun $\mathrm{rk}(A) = \mathrm{rk}(A, b)$, so gibt es z mit $Az = -b$, und indem wir Q durch $\tau_z(Q)$ ersetzen, können wir annehmen, dass $b = 0$.

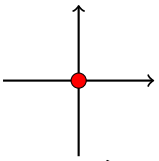
- Im Fall $c = 0$ setzt man $a_i = \frac{1}{\sqrt{|\lambda_i|}}$ und ersetzt gegebenenfalls (A, b, c) mit $(-A, -b, -c)$, um Form 1 zu erhalten.
- Im Fall $c \neq 0$ ersetzt man (A, b, c) durch $(-\frac{1}{c}A, -\frac{1}{c}b, -1)$ und setzt dann $a_i = \frac{1}{\sqrt{|\lambda_i|}}$, um Form 2 zu erhalten.
- Ist $\mathrm{rk}(A) < \mathrm{rk}(A, b)$, so ist insbesondere $r < n$ und $\mu \neq 0$. Nun ersetzten wir Q durch $\tau_z(Q)$ mit $z = -\frac{c}{2\mu} \cdot e_{r+1}$ und können somit auch wieder $c = 0$ annehmen. Ersetzt man $(A, b, 0)$ durch $(-\frac{1}{\mu}A, -1, 0)$ und setzt wieder $a_i = \frac{1}{\sqrt{|\lambda_i|}}$, so erhält man Form 3. (Ist $k < r-k$, so ersetzt man weiter Q durch $f_{-\mathbb{1}_n}(Q)$ und $(A, b, 0)$ durch $(-A, -b, 0)$.) □

Folgerung 8.11
Sei $Q \subseteq \mathbb{R}^n$ eine Quadrik. Es gibt eine invertierbare affine Abbildung $f \in \mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n)$ für die $f(Q)$ eine der folgenden 3 Formen annimmt:

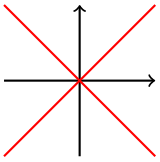
- $f(Q) = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{k} x_i^2 - \sum_{i=k+1}^{r} x_i^2 = 0 \right\} \quad k \geq r-k$
- $f(Q) = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{k} x_i^2 - \sum_{i=k+1}^{r} x_i^2 = 1 \right\}$
- $f(Q) = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{k} x_i^2 - \sum_{i=k+1}^{r} x_i^2 - 2x_{r+1} = 0 \right\} \quad k \geq r-k, r < n$

■ **Beispiel 8.12**
$Q \subseteq \mathbb{R}^2$

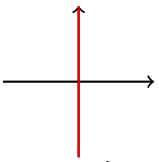
- _ $k = 2, r = 2 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 + \left(\frac{x_2}{a_2}\right)^2 = 0 \right\}$



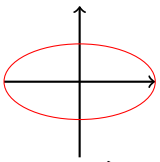
_ $k = 1, r = 2 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 - \left(\frac{x_2}{a_2}\right)^2 = 0 \right\}$



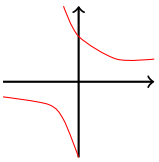
_ $k = 1, r = 1 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 = 0 \right\}$



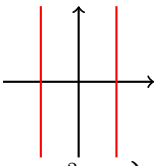
- _ $k = 2, r = 2 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 + \left(\frac{x_2}{a_2}\right)^2 = 1 \right\}$



_ $k = 1, r = 2 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 - \left(\frac{x_2}{a_2}\right)^2 = 1 \right\}$



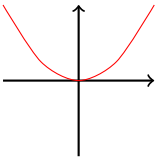
_ $k = 1, r = 1 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 = 1 \right\}$



_ $k = 0, r = 2 : \left\{ x \in \mathbb{R}^2 \mid -\left(\frac{x_1}{a_1}\right)^2 - \left(\frac{x_2}{a_2}\right)^2 = 1 \right\} = \emptyset$

_ $k = 0, r = 1 : \left\{ x \in \mathbb{R}^2 \mid -\left(\frac{x_1}{a_1}\right)^2 - \left(\frac{x_2}{a_2}\right)^2 = 1 \right\} = \emptyset$

- _ $k = 1, r = 1 : \left\{ x \in \mathbb{R}^2 \mid \left(\frac{x_1}{a_1}\right)^2 - 2x_2 = 0 \right\}$



▶ **Bemerkung 8.13**

- Ist $Q \subseteq \mathbb{R}^2$ eine Quadrik, $U \subseteq V$ affiner Untervektorraum, so ist $Q \cap U$ eine Quadrik in dem Sinne, dass $\exists f$ Isometrie : $f(U) = \mathbb{R}^k$ und $f(Q \cap U)$ ist eine Quadrik.
- Ebene Quadriken sind im wesentlichen Kegelschnitte, $Q' = \{x \in \mathbb{R}^3 \mid x_1^2 + x_2^2 = x_3^2\}$, außer 2c und 2d in Beispiel 8.12

▶ **Bemerkung 8.14**

Die Situation wird deutlich übersichtlicher, wenn man den affinen Raum $\mathbb{R}^n$ durch Hinzunahme von Punkten im Unendlichen zum projektiven Raum $\mathbb{P}^n(\mathbb{R})$ vervollständigt und den Abschluss der Quadriken darin betrachtet. Es stellt sich dann heraus, dass vom projektiven Standpunkt aus die meisten ebenen Quadriken ähnlich aussehen. (Siehe Vorlesung *Elementare Algebraische Geometrie*)

Kapitel VII

Dualität

1. Das Lemma von Zorn

Sei K ein Körper und U, V, W seien K-Vektorräume. Zudem sei X eine Menge.

Definition 1.1 (Relation)
Eine Relation ist eine Teilmenge $R \subseteq X \times X$. Man schreibt $(x, x') \in R$ als xRx'. R heißt

- reflexiv , wenn $\forall x \in X$: xRx
- transitiv , wenn $\forall x, y, z \in X$: xRy und $yRz \Rightarrow xRz$
- symmetrisch , wenn $\forall x, y \in X$: $xRy \Rightarrow yRx$
- antisymmetrisch , wenn $\forall x, y \in X$: xRy und $yRx \Rightarrow y = x$
- total , wenn $\forall x, y \in X$: $(x, y) \notin R \Rightarrow (y, x) \in R$

■ **Beispiel 1.2 (Äquivalenzrelation)**
Eine Äquivalenzrelation ist eine reflexive, transitive und symmetrische Relation. Wir haben schon verschiedene Äquivalenzrelationen kennengelernt: Isomorphie von K-Vektorräumen und Ähnlichkeit von Matrizen.

Definition 1.3 (Halbordnung)
Eine Halbordnung (oder partielle Ordnung) ist eine reflexive, transitive und antisymmetrische Relation $\leq$. Eine totale Halbordnung heißt Totalordnung oder lineare Ordnung . Man schreibt $x < y$ für $x \leq y \wedge x \neq y$.

■ **Beispiel 1.4**

1. Die natürliche Ordnung $\leq$ auf $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ und $\mathbb{N}$ ist eine Z Totalordnung.
2. Teilbarkeit $|$ ist eine Halbordnung auf $\mathbb{N}$, aber Teilbarkeit ist keine Halbordnung auf $\mathbb{Z}$, da $1|-1$ und $-1|1$, aber $1 \neq -1$!
3. $\mathcal{P}(X)$ ist die Potenzmenge. "$\subseteq$" ist eine Halbordnung auf $\mathcal{P}$, aber für $|X| > 1$ ist "$\subseteq$" keine Totalordnung.
4. Sei $(X, \leq)$ eine Halbordnung, sei $Y \subseteq X$, so ist $(Y, \leq|_Y)$ eine Halbordnung.

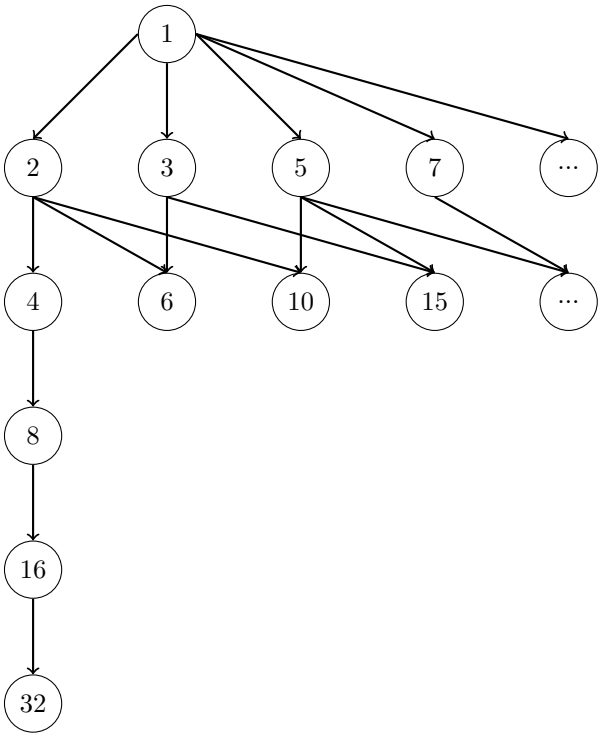
Definition 1.5 (Kette)
Sei $(X, \leq)$ eine Halbordnung, $Y \subseteq X$. Y heißt Kette , wenn $(Y, \leq |_Y)$ total ist.

$x \in Y$ heißt ein minimales Element von Y, wenn $\forall x' \in Y$: $x < x'$.

$x \in Y$ heißt untere Schranke von Y, wenn $\forall y \in Y$: $y \geq x$.

$x \in Y$ heißt kleinstes Element von Y, wenn x untere Schranke von Y ist.

Analog: maximales Element , obere Schranke , größtes Element .



$Y = \{2^n \mid n \in \mathbb{N}\}$ ist eine Kette

▶ **Bemerkung 1.6**

- Hat Y ein kleinstes Element, so ist dies eindeutig bestimmt. Ein kleinstes Element ist minimal.
- Jede endliche Halbordnung hat minimale Elemente. Jede endliche Totalordnung hat ein kleinstes Element. Analog für maximale Elemente und größtes Element.

■ **Beispiel 1.7**
$(\mathbb{N}, \leq)$ hat als kleinstes Element die 1, aber kein größtes Element oder maximale Elemente.

■ **Beispiel 1.8**
$V = \mathbb{R}^3$, $\mathfrak{X}$ die Menge der Untervektorräume des $\mathbb{R}^3$. $(\mathfrak{X}, \leq)$ ist eine Halbordnung auf $Y \subseteq X$ mit $Y = \{U \in \mathfrak{X} \mid \dim_{\mathbb{R}}(U) \leq 2\}$.

- Y hat ein kleinstes Element: $\{0\}$.
- Es gibt unendlich viele maximale Elemente in Y, nämlich die Untervektorräume von V, die die Dimension 2 haben. Es gibt also kein größtes Element.
- V ist die obere Schranke von Y.

Theorem 1.9 (Das Lemma von Zorn)
Sei $(X, \leq)$ eine Halbordnung, die nicht leer ist. Wenn jede Kette eine obere Schranke hat, dann hat X ein maximales Element.

Beweis. Das Lemma von Zorn hat axiomatischen Charakter - es ist äquivalent zum Auswahlaxiom, seine Gültigkeit ist somit abhängig von unseren grundlegenden mengentheoretischen Annahmen. Für einen Beweis des Lemmas von Zorn aus dem Auswahlaxiom siehe die Vorlesung *Mengenlehre*. Wir zeigen hier zumindest die andere Richtung, nämlich dass das Auswahlaxiom aus dem Lemma von Zorn folgt. □

Folgerung 1.10 (Auswahlaxiom)
Zu jeder Familie (x_i), nicht leer, gibt es eine Auswahlfunktion , das heißt eine Abbildung:

$$f : I \to \bigcup_{i \in I} X_i \text{ mit } f(i) \in X_i \quad \forall i$$

Beweis. Sei $\mathcal{F}$ die Menge der Paare (J, f) bestehend aus einer Teilmenge $J \subseteq I$ und einer Abbildung $f : I \to \bigcup_{i \in I} X_i$ mit $f(i) \in X_i \quad \forall i \in J$. Definieren wir $(J, f) \leq (J', f') \iff J \subseteq J'$ und $f'|_J = f$, so ist $\leq$ eine Halbordnung auf $\mathcal{F}$. Da $(\emptyset, \emptyset) \in \mathcal{F}$ ist $\mathcal{F}$ nichtleer. Ist $\mathcal{G} \subseteq \mathcal{F}$ eine nichtleere Kette, so wird auf $J' := \bigcup_{(J,f) \in \mathcal{G}} J$ durch $f'(j) = f(j)$ falls $(J, f) \in \mathcal{G}$ und $j \in J$ eine wohldefinierte Abbildung $f' : J \to \bigcup_{i \in J} X_i$ mit $f'(i) \in X_i \quad \forall i \in J'$ gegeben. Das Paar (J', f') ist eine obere Schranke der Kette $\mathcal{G}$. Nach dem Lemma von Zorn besitzt $\mathcal{F}$ ein maximales Element (J, f). Wir behaupten, dass $J = I$. Andernfalls nehmen wir ein $i' \in I \backslash J$ und ein $x' \in X_{i'}$ und definieren $J' := U \cup \{i'\}$ und $f' : J' \to \bigcup_{i \in J'} X_i$, $j \mapsto \begin{cases} f(j) & j \in J \\ x' & j = i' \end{cases}$. Dann ist $(J', f') \in \mathcal{F}$ und $(J, f) < (J', f')$ im Widerspruch zur Maximalität von (J, f). □

Folgerung 1.11 (Basisergänzungssatz)
Sei V ein K-Vektorraum. Jede linear unabhängige Teilmenge $X_0 \subseteq V$ ist in einer Basis von V enthalten.

Beweis. Sei $\mathfrak{X} = \{X \subseteq V \mid X \text{ ist linear unabhängig, } X_0 \subseteq X\}$ geordnet durch Inklusion. Dann ist $X_0 \in \mathfrak{X}$, also $\mathfrak{X} \neq \emptyset$. Ist $\mathcal{Y}$ eine nichtleere Kette in $\mathfrak{X}$, so ist auch $Y = \bigcup \mathcal{Y} \subseteq V$ linear unabhängig. Sind $y_1, ..., y_n \in Y$ paarweise verschieden, so gibt es $Y_1, ..., Y_n \in \mathcal{Y}$ mit $y_i \in Y_i$ für $i = 1, ..., n$. Da $\mathcal{Y}$ total geordnet ist, besitzt $\{Y_1, ..., Y_n\}$ ein größtes Element, o.E. Y_1. Also sind $y_1, ..., y_n \in Y_1$ und somit linear unabhängig. Folglich ist $Y_1 \in \mathfrak{X}$ eine obere Schranke von $\mathcal{Y}$. Nach dem Lemma von Zorn besitzt $\mathfrak{X}$ ein maximales Element X. Das heißt, X ist eine maximal linear unabhängige Teilmenge von V, nach Satz 3.5 also eine Basis von V. □

2. Der Dualraum

Sei V ein K-Vektorraum.

Definition 2.1 (Dualraum)
Der Dualraum zu V ist der K-Vektorraum

$$V^* = \mathrm{Hom}_K(V, K) = \{\varphi : V \to K \text{ linear}\}$$

Die Elemente von V^* heißen Linearformen auf V.

■ **Beispiel 2.2**
Ist $V = K^n = \mathrm{Mat}_{n\times 1}(K)$, so wird $V^* = \mathrm{Hom}_K(V, K)$ durch $\mathrm{Mat}_{1\times n}(K) \cong K^n$. Wir können also die Elemente von V als Spaltenvektoren und die Linearformen auf V als Zeilenvektoren auffassen.

Lemma 2.3
Ist $B(x_1)_{i\in I}$ eine Basis von V, so gibt es zu jedem $i \in I$ genau $x_i^* \in V^*$ mit

$$x_i^*(x_j) = \delta_{ij} \quad \forall j \in I$$

Beweis. Siehe Satz 5.1, angewandt auf die Familie $(y_j)_{j\in I}$, $y_j\delta_{i.j}$ in $W = K$. □

Satz 2.4
Ist $B = (x_1)_{i\in I}$ eine Basis von V, so ist $B^* = (x_i^*)_{i\in I}$ linear unabhängig. Ist I endlich, so ist B^* eine Basis von V^*.

Beweis. Ist $\varphi = \sum_{i\in I} \lambda_i x_i^*$, $\lambda_i \in K$, fast alle gleich 0, so ist $\varphi(x_j) = \sum_{i\in I} \lambda_j x_i^*(x_j) = \lambda_j$ für jedes $j \in I$. Ist also $\varphi = 0$, so ist $\lambda_j = \varphi(x_j) = 0 \quad \forall j \in I$, B^* ist somit linear unabhängig.
Ist zudem I endlich und $\psi \in V^*$, so ist $\psi = \psi' = \sum_{i\in I} \psi(x_i)x_i^*$, denn $\psi'(x_j) = \sum_{i\in I} \psi(x_i)x_i^*(x_j) = \psi(x_i) \quad \forall j \in I$, und somit ist B^* ein Erzeugendensystem von V^*. □

Definition 2.5 (duale Basis)
Ist $B = (x_i)_{i\in I}$ eine endliche Basis von V, so nennt man $B^* = (x_i^*)_{i\in I}$ die zu B duale Basis .

Folgerung 2.6
Zu jeder Basis B von V gibt es einen eindeutig bestimmtem Monomorphismus

$$f_V \to V^* \text{ mit } f(B) = B^*$$

Ist $\dim_K(V) < \infty$, so ist dieser ein Isomorphismus.

Folgerung 2.7
Zu jedem $= 0 \neq x \in V$ gibt es eine Linearform $\varphi \in V$ mit $\varphi(x) = 1$.

Beweis. Ergänze $x_1 = x$ zu einer Basis $(x_i)_{i\in I}$ von V (Folgerung 1.11) und $\varphi = x_1^*$. □

■ **Beispiel 2.8**
Ist $V = K^n$ mit Standardbasis $\mathcal{E} = (e_1, ..., e_n)$, so können wir V^* mit dem Vektorraum der Zeilen-

vektoren identifizieren, und dann ist

$$e_i^* = e_i^t$$

Definition 2.9 (Bidualraum)
Der Bidualraum zu V ist der K-Vektorraum

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

Satz 2.10
Die kanonische Abbildung

$$\iota : \begin{cases} V \to V^{**} \\ x \to \iota_x \end{cases} \quad \text{wobei } \iota_x(\varphi) = \varphi(x)$$

ist ein Monomorphismus. Ist $\dim_K(V) < \infty$, so ist ι ein Isomorphismus.

Beweis.
- $\iota_x \in V^{**}$:
  - $\iota_x(\varphi + \psi) = (\varphi + \psi)(x) = \varphi(x) + \psi(x) = \iota_x(\varphi) + \iota_x(\psi)$
  - $\iota_x(\lambda\varphi) = (\lambda\varphi)(x) = \lambda\varphi(x) = \lambda\iota_x(\varphi)$
- ι linear:
  - $\iota_{x+y}(\varphi) = \varphi(x+y) = \varphi(x) + \varphi(y) = \iota_x(\varphi) + \iota_y(\varphi) = (\iota_x + \iota_y)(\varphi)$
  - $\iota_{\lambda x}(\varphi) = \varphi(\lambda x) = \lambda\iota_x(\iota) = (\lambda\iota_x)(\varphi)$
- ι injektiv: Sei $0 \neq x \in V$. Nach Folgerung 2.7 existiert $\varphi \in V^*$ mit $\iota_x(\varphi) = \varphi(x) = 1 \neq 0$. Somit ist $\iota_x \neq 0$.
- Ist $\dim_K(V) < \infty$, so ist $V \overset{2.6}{\cong} V^* \overset{2.6}{\cong} V^{**}$, insbesondere $\dim_K(V) = \dim_K(V^{**})$. Der Monomorphismus ι ist somit ein Isomorphismus. □

▶ **Bemerkung 2.11**
Sei $\dim_K(V) < \infty$. Im Gegensatz zu den Isomorphismen $V \to V^*$, die von der Wahl der Basis B abhängen, ist der Isomorphismus $\iota : V \to V^{**}$ kanonisch (von der Wahl der Basis B unabhängig).

Die Voraussetzung, dass $\dim_K(V) < \infty$ ist hier essentiell: Für $\dim_K(V) = \infty$ ist ι nicht surjektiv.

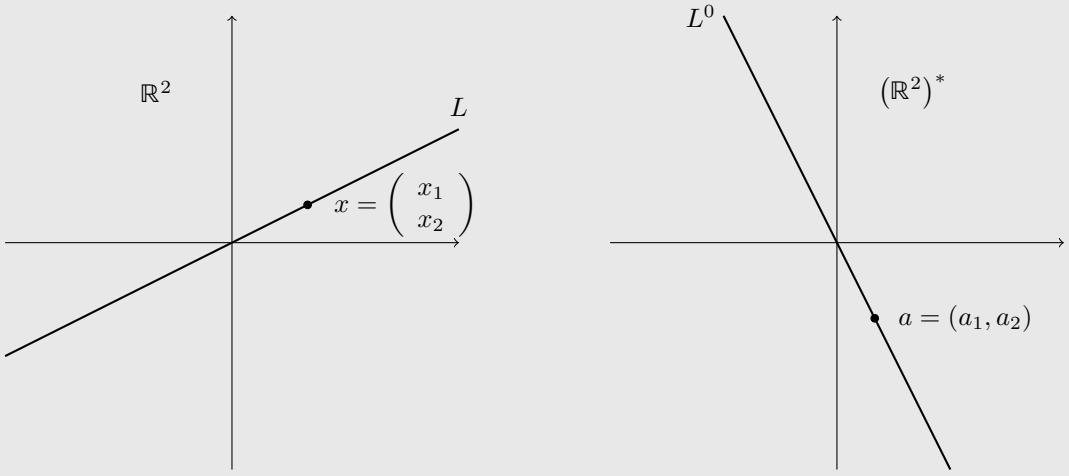
Definition 2.12 (Annulator)
Für eine Teilmenge $U \subseteq V$ bezeichne

$$U^0 = \{\varphi \in V^* \mid \varphi(x) = 0 \quad \forall x \in U\}$$

den Annulator von U.

Anmerkung
Für eine Gerade $L = x \cdot \mathbb{R} \subset \mathbb{R}^2$ sind $a = (a_1, a_2) \in (\mathbb{R}^2)^*$ gesucht mit

$$a_1 x_1 + a_2 x_2 = 0$$



Diese $a \in (\mathbb{R}^2)^*$ liegen auf einer Geraden L^0 in $(\mathbb{R}^2)^*$, die senkrecht auf L steht, wenn man $\mathbb{R}^2$ und $(\mathbb{R}^2)^*$ nicht unterscheidet.

Lemma 2.13
U^0 ist ein Untervektorraum von V^*.

Beweis. Klar. □

Satz 2.14
Ist $\dim_K(V) < \infty$ und $U \subseteq V$ ein Untervektorraum, so ist

$$\dim_K(V) = \dim_K(U) + \dim_K(U^0)$$

Beweis. Ergänze eine Basis $(x_1, ..., x_r)$ von U zu einer Basis $B = (x_1, ..., x_n)$ von V. Dann ist $B^*(x_1^*, ..., x_n^*)$ eine Basis von V^*. Sei $C = (x_{r+1}^*, ..., x_n^*)$. Dann ist C eine Basis von U^0:

- B^* ist Basis $\Rightarrow C$ ist linear unabhängig.
- $C \subseteq U^0$: Für $1 \leq j \leq r < i \leq n$ ist $x_i^*(x_j) = \delta_{ij} = 0$.
- $U^0 \subseteq \text{span}_K(C)$: Ist $\varphi = \sum_{i=1}^n \lambda_i x_i^* \in U^0$, so $0 = \varphi(x_j) = \lambda_j$ für alle $j \leq r$, also $\varphi \in \text{span}_K(x_{r+1}^*, ..., x_n^*)$. □

Folgerung 2.15
Ist $\dim_K(V) < \infty$ und $U \subset V$ ein Untervektorraum, so ist

$$\iota(U) = U^{00}$$

Beweis. Es ist klar, dass $\iota(U) \leq U^{00}$.

Für $\varphi \in U^0$ und $x \in U$ ist $\iota_x(\varphi) = \varphi(x) = 0$. Mit Satz 2.14 ist

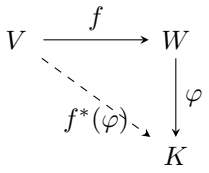
$$\begin{aligned}\dim_K(U^{00}) &= \dim_K(V^*) - \dim_K(U^0) \\ &= \dim_K(V^*) - (\dim_K(V) - \dim_K(U)) \\ &\overset{2.6}{=} \dim_K(U)\end{aligned}$$

und da ι injektiv ist, folgt $\iota(U) = U^{00}$. □

3. Die duale Abbildung

Sei $f \in \mathrm{Hom}_K(V, W)$.

▶ **Bemerkung 3.1**
Ist $\varphi \in W^* = \mathrm{Hom}_K(W, K)$ eine Linearform auf W, so ist $\varphi \circ f \in \mathrm{Hom}_K(V, K) = V^*$ eine Linearform auf V.



Definition 3.2 (duale Abbildung)
Die zu f duale Abbildung ist

$$f^* : \begin{cases} W^* \to V^* \\ \varphi \mapsto \varphi \circ f \end{cases}$$

Lemma 3.3
Es ist $f^* \in \mathrm{Hom}_K(W^*, V^*)$.

Beweis. Sind $\varphi, \psi \in W^*$ und $\lambda \in K$ ist

$$\begin{aligned} f^*(\varphi + \psi) &= (\varphi + \psi) \circ f \\ &= \varphi \circ f + \psi \circ f \\ &= f^*(\varphi) + f^*(\psi) \\ f^*(\lambda\varphi) &= (\lambda\varphi) \circ f \\ &= \lambda \cdot (\varphi \circ f) \\ &= \lambda \cdot f^*(\varphi) \end{aligned}$$

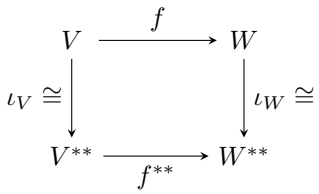
□

Satz 3.4
Sind $B = (x_1, ..., x_n)$ und $C = (y_1, ..., y_m)$ Basen von V bzw. W, so ist

$$M_{B^*}^{C^*}(f^*) = \left(M_C^B(f)\right)^t$$

Beweis. Sei $A = M_C^B(f) = (a_{ij})_{i,j}$ und $B = M_{B^*}^{C^*}(f^*) = (b_{ji})_{j,i}$. Dann ist $f(x_j) = \sum_{i=1}^m a_{ij} y_i$, also $a_{ji} = y_i^*(f(x_j)) = f^*(y_i^*)(x_j)$ und $f^*(y_i^*) = \sum_{j=1}^n b_{ji} x_j^*$, also $b_{ji} = f^*(y_i^*)(x_j) = a_{ij}$. □

Folgerung 3.5
Sind V und W endlichdimensional, und identifizieren wir $V = V^{**}$ und $W = W^{**}$, so ist $f = f^{**}$, das heißt $\iota \circ f = f^{**} \circ \iota$.



Beweis. Seien B und C Basen von V bzw. W. Unter der Identifizierung ist $B^{**} = B$ und $C = C^{**}$, das heißt $\iota(x_i) = x_i^{**}$ bzw. $\iota(y_j) = y_j^{**}$, denn $\iota(x_i)(x_j^*) = x_j^*(x_i) = \delta_{ij} = x_i^{**}(x_j^*) \quad \forall i, j$ und somit

$$M_C^B(f^{**}) \overset{3.4}{=} \left(M_{B^*}^{C^*}(f^*)\right)^t \overset{3.4}{=} \left(M_C^B(f)\right)^{tt} = M_C^B(f)$$

Also $f^{**} = f$. □

Folgerung 3.6
Sind V, W endlichdimensional, so liefert die Abbildung $f \mapsto f^*$ einen Isomorphismus von K-Vektorräumen.

$$\mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(W^*, V^*)$$

Beweis. Sind $f, g \in \mathrm{Hom}_K(V, W)$ und $\lambda \in K$, $\varphi \in W^*$, so ist

$$\begin{aligned}(f+g)^*(\varphi) &= \varphi \circ (f+g) = \varphi \circ f + \varphi \circ g = f^*(\varphi) + g^*(\varphi) = (f^* + g^*)(\varphi)\\ (\lambda f)^*(\varphi) &= \varphi \circ (\lambda f) = \lambda \cdot (\varphi \circ f) = \lambda \circ f^*(\varphi) = (\lambda f^*)(\varphi)\end{aligned}$$

Die Abbildung ist somit linear. Nach Folgerung 3.5 ist sie injektiv. Da

$$\begin{aligned}\dim_K(V, W) &= \dim_K(V) \cdot \dim_K(W)\\ &= \dim_K(V^*) \cdot \dim_K(W^*)\\ &= \dim_K(\mathrm{Hom}_K(W^*, V^*))\end{aligned}$$

ist sie auch ein Isomorphismus. □

Satz 3.7
Sind V, W endlichdimensional so ist

$$\begin{aligned}\mathrm{Im}(f^*) &= \mathrm{Ker}(f)^0\\ \mathrm{Ker}(f^*) &= \mathrm{Im}(f)^0\end{aligned}$$

Beweis.

- $\mathrm{Im}(f^*) \subseteq \mathrm{Ker}(f)^0$: Ist $\varphi \in W^*$, $x \in \mathrm{Ker}(f)$, so ist

$$f^*(\varphi)(x) = (\varphi \circ f)(x) = \varphi(0) = 0$$

- $\mathrm{Ker}(f)^0 \subseteq \mathrm{Im}(f^*)$: Sei $\varphi \in \mathrm{Ker}(f)^0$. Setze eine Basis $(x_1, ..., x_r)$ von $\mathrm{Ker}(f)$ zu einer Basis $(x_1, ..., x_n)$ von V fort. Dann sind $f(x_{r+1}), ..., f(x_n)$ linear unabhängig nach der Kern-Bild-Formel (Folgerung 7.13), es gibt also $\psi \in W^*$ mit

$$\psi(f(x_i)) = \varphi(x_i) \quad \forall i$$

Es folgt

$$f^*(\psi)(x_i) = \psi(f(x_i)) = \varphi(x_i) \quad \forall i$$

also $\varphi = f^*(\psi)$.

- Mit der Identifizierung $V = V^{**}$ ist

$$\mathrm{Im}(f)^0 \overset{3.5}{=} \mathrm{Im}(f^{**})^0 = \mathrm{Ker}(f^*)^{00} \overset{2.15}{=} \mathrm{Ker}(f^*)$$ □

Folgerung 3.8
Sind V, W endlichdimensional, so ist

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

Beweis.

$$\begin{aligned}\mathrm{rk}(f) &= \dim_K(\mathrm{Im}(f)) \\ &\overset{2.14}{=} \dim_K(W) - \dim_K(\mathrm{Im}(f)^0) \\ &\overset{7.13}{=} \dim_K(W^*) - \dim_K(\mathrm{Ker}(f^*)) \\ &= \mathrm{rk}(f^*)\end{aligned}$$ □

Folgerung 3.9
Ist $\dim_K(V) < \infty$ und $U \subseteq V$ ein Untervektorraum, so lässt sich jede Linearform auf U zu einer Linearform auf V fortsetzen.

Beweis. Ist $f : U \to V$ die Inklusionsabbildung, so ist $f^* : V^* \to U^*$, $\varphi \mapsto \varphi|_U$ und

$$\mathrm{rk}(f^*) = \mathrm{rk}(f) = \dim_K(U) = \dim_K(U^*)$$

f^* ist somit surjektiv. □

▶ **Bemerkung 3.10**
Folgerung 3.9 gilt auch ohne die Voraussetzung $\dim_K(V) < \infty$, siehe Übung.

▶ **Bemerkung 3.11**
Ein homogenes lineares Gleichungssystem $Ax = 0$ hat als Lösungsraum $L(A, 0) \subseteq K^n$ ein Untervektorraum des K^n. Unter der Identifizierung $K^n = (K^n)^{**}$ ist $L(A, 0)$ der Annulator der Linearformen beschrieben durch die Zeilen $a_1, ..., a_m \in (K^n)^*$ von A. Wir wollen umgekehrt zu einem Untervektorraum $W \subseteq K^n$ ein $A = (a_1, ..., a_m) \in \mathrm{Mat}_{n\times m}(K)$ mit $W = L(A, 0)$ finden. Ist $W = \mathrm{span}_K(b_1, ..., b_r)$, so ist $W = \mathrm{Im}(f_B)$ mit $B = (b_1, ..., b_r) \in \mathrm{Mat}_{n\times r}(K)$.
$\Rightarrow W \overset{3.7}{=} \mathrm{Ker}(f_B^*)^0$ und $M_{\mathcal{E}^t}(f_B^*) = B^t$. Wenn man also eine Basis $(a_1, ..., a_s)$ von $L(B^t, 0)$ bestimmt und daraus eine Matrix $A = (a_1^t, ..., a_s^t) \in \mathrm{Mat}_{s\times n}(K)$ bildet, so ist $W = L(A, 0)$.

4. Die adjungierte Abbildung

Sei $K = \mathbb{R}$ oder $K = \mathbb{C}$ und V ein endlichdimensionaler unitärer K-Vektorraum.

Definition 4.1 (weitere Skalarmultiplikation)
Wir definieren auf V eine Skalarmultiplikation

$$\lambda * x = \overline{\lambda} \cdot x$$

und schreiben $\overline{V} = (V, +, *)$.

Lemma 4.2
$\overline{V}$ ist ein K-Vektorraum und $\mathrm{End}_K(V) = \mathrm{End}_K(\overline{V})$.

Beweis. Mit LAAG1 VI.1.7 nachprüfen, zum Beispiel:

- $\lambda * (x + y) = \overline{\lambda} \cdot (x + y) = \overline{\lambda}x + \overline{\lambda}y = \lambda * x + \lambda * y$
- $\lambda * (\mu * x) = \overline{\lambda}(\overline{\mu} \cdot x) = \overline{\lambda\mu}x = (\lambda\mu) * x$ □

Weiterhin sei: $f \in \mathrm{End}_K(V)$, $x \in V$, $\lambda \in K$
$\Rightarrow f(\lambda * x) = f(\overline{\lambda}x) = \lambda * f(x)$
$\Rightarrow f \in \mathrm{End}_K(\overline{V})$.
Umgekehrt sei $g \in \mathrm{End}_K(\overline{V})$, $x \in V$, $\lambda \in K$
$\Rightarrow g(\lambda \cdot x) = g(\overline{\lambda} * x) = \lambda \cdot g(x)$
$\Rightarrow g \in \mathrm{End}_K(V)$.

Lemma 4.3
Für $y \in V$ ist

$$\Phi_y : \begin{cases} V \to K \\ x \mapsto \langle x, y \rangle \end{cases}$$

eine Linearform auf V.

Die Abbildung $y \mapsto \Phi_y$ liefert einen Isomorphismus $\Phi : \overline{V} \to V^*$.

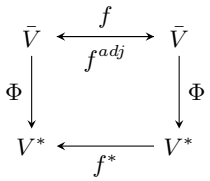
Beweis.
- $\Phi_y \in V^*$: Linearität in ersten Argument.
- $\Phi \in \mathrm{Hom}_K(\overline{V}, V^*)$: Für $y, y' \in V$, $\lambda \in K$, $x \in V$ ist
  - $\Phi_{y+y'}(x) = \langle x, y + y' \rangle = \langle x, y \rangle + \langle x, y' \rangle = \Phi_y(x) + \Phi_{y'}(x)$
  - $\Phi_{\lambda * y}(x) = \langle x, \lambda * x \rangle = \left\langle x, \overline{\lambda}y \right\rangle = \lambda \langle x, y \rangle = \lambda\Phi_y(x)$
- Φ injektiv: Skalarprodukt ist nicht ausgeartet.
- Da $\dim_K(\overline{V}) = \dim_K(V) = \dim_K(V^*)$ ist Φ somit ein Isomorphismus. □

Satz 4.4
Zu $f \in \mathrm{End}_K(V)$ gibt es ein eindeutig bestimmtes $f^{adj} \in \mathrm{End}_K(V)$ mit

$$\langle f(x), y\rangle = \langle x, f^{adj}(y)\rangle \quad \forall x, y \in V$$

Beweis. Existenz und Eindeutigkeit sind zu zeigen.

- Existenz:



  Für $f^{adj} = \Phi{-}1 \circ f^* \circ \Phi \in \mathrm{End}_K(\overline{V}) = \mathrm{End}_K(V)$ ist

$$\Phi_y \circ = (f^* \circ \Phi)(y) = (\Phi \circ f^{adj\cdot})(y) = \Phi_{f^{adj}(y)}$$

  also

$$\langle f(x), y\rangle = (\Phi_y \circ f)(x) = \Phi_{f^{adj}(y)}(x) = \langle x, f^{adj}(y)\rangle \quad \forall x, y \in V$$

- Eindeutigkeit: Erfüllen f_1, f_2 für Gleichung

$$\langle f(x), y\rangle = \langle x, f^{adj}(y)\rangle \quad \forall x, y \in V$$

  so ist

$$0 = \langle x, f_1(y)\rangle - \langle x, f_2(y)\rangle = \langle x, f_1(y) - f_2(y)\rangle \quad \forall x, y \in V$$

  da $\langle \cdot, \cdot \rangle$ nicht ausgeartet ist, folgt daraus, dass $f_1 = f_2$. □

Definition 4.5 (adjungierter Endomorphismus)
Die Abbildung f^{adj} heißt der zu f adjungierte Endomorphismus .

Beispiel 4.6

- Ist f selbstadjungiert, so ist $f^{adj} = f$.
- Ist f unitär, so ist $f \in \mathrm{Aut}_K(V)$ und

$$\langle f(x), y\rangle = \langle x, f^{-1}(y)\rangle \quad \forall x, y \in V$$

  also $f^{adj} = f^{-1}$.

Lemma 4.7
Ist B eine Orthonormalbasis vin V, so ist

$$M_B(f^{adj}) = M_B(f^*)$$

Beweis. Ist $A = M_B(f)$ und $B = M_B(f^{adj})$, $v = \Phi_B(x)$, $w = \Phi_B(y)$, so ist

$$\begin{aligned}(Ax)^t\overline{y} = \langle f(v), w\rangle &= \left\langle v, f^{adj}(w)\right\rangle \\ x^t A^t\overline{y} &= x^t\overline{B}\overline{y} \\ \Rightarrow B = \overline{A^t} &= A^*\end{aligned}$$

□

Lemma 4.8
Für $f, g \in \mathrm{End}_K(V)$ und $\lambda, \mu \in K$ ist

$$\begin{aligned}(\lambda f + \mu g)^{adj} &= \overline{\lambda} f^{adj} + \overline{\mu} g^{adj} \\ (f^{adj})^{adj} &= f\end{aligned}$$

Beweis. Für $x, y \in V$ ist

$$\begin{aligned}\langle(\lambda f + \mu g)(x), y\rangle &= \lambda\langle f(x), y\rangle + \mu\langle g(x), y\rangle \\ &= \lambda\left\langle x, f^{adj}(y)\right\rangle + \mu\left\langle x, g^{adj}\right\rangle \\ &= \left\langle x, (\overline{\lambda} f^{adj} + \overline{\mu} g^{adj})(y)\right\rangle\end{aligned}$$

und

$$\left\langle f^{adj}(x), y\right\rangle = \overline{\left\langle y, f^{adj}(y)\right\rangle} = \overline{\langle f(y), x\rangle} = \langle x, f(y)\rangle$$

□

5. Der Spektralsatz

Sei V ein endlichdimensionaler unitärer K-Vektorraum und $f \in \mathrm{End}_K(V)$.

Definition 5.1 (normaler Endomorphismus, normale Matrix)
Der Endomorphismus f heißt normal , wenn

$$f \circ f^{adj} = f^{adj} \circ f$$

Entsprechend heißt $A \in \mathrm{Mat}_n(K)$ normal , wenn

$$AA^* = A^*A$$

Mathematica/WolframAlpha-Befehle (normale Matrix)
Ob eine Matrix A normal ist, beantwortet folgende Funktion für Mathematica bzw. WolframAlpha:

```
NormalMatrixQ[A]
```

■ **Beispiel 5.2**

- Ist f selbstadjungiert, so ist $f^{adj} = f$, insbesondere ist f normal.
- Ist f unitär, so ist $f^{adj} = f^{-1}$, insbesondere ist f normal.

Lemma 5.3
Genau dann ist $f \in \mathrm{End}_K(V)$ normal, wenn

$$\langle f(x), f(y)\rangle = \left\langle f^{adj}(x), f^{adj}(y)\right\rangle \quad \forall x, y \in V$$

Beweis.

- Hinrichtung: Ist f normal, so ist

$$\begin{aligned}\langle f(x), f(y)\rangle &= \left\langle x, (f^{adj} \circ f)(y)\right\rangle \\ &= \left\langle x, (f \circ f^{adj})(y)\right\rangle \\ &= \left\langle f^{adj}(x), f^{adj}(y)\right\rangle \quad \forall x, y \in V\end{aligned}$$

- Rückrichtung: Ist umgekehrt $\left\langle f^{adj}(x), f^{adj}(y)\right\rangle$, so ist

$$\begin{aligned}\left\langle x, (f^{adj} \circ f)(y)\right\rangle &= \left\langle x, (f \circ f^{adj})(y)\right\rangle \\ 0 &= \left\langle x, (f^{adj} \circ f - f \circ f^{adj})(y)\right\rangle \\ f^{adj} \circ f &= f \circ f^{adj}\end{aligned}$$

□

Lemma 5.4
Ist f normal, ist ist

$$\mathrm{Ker}(f) = \mathrm{Ker}(f^{adj})$$

Beweis. Nach Lemma 5.3 ist

$$\|f(x)\| = \|f^{adj}(x)\| \quad \forall x \in V$$

Insbesondere gilt

$$f(x) = 0 \iff f^{adj}(x) = 0$$ □

Lemma 5.5
Ist f normal, so ist

$$\mathrm{Eig}(f, \lambda) = \mathrm{Eig}(f^{adj}, \overline{\lambda}) \quad \forall \lambda \in K$$

Beweis. Da $(\lambda \cdot \mathrm{id} - f)^{adj} \overset{4.8}{=} \overline{\lambda} \cdot \mathrm{id} - f^{adj}$ ist auch $\lambda \cdot \mathrm{id} - f$ normal. Somit ist

$$\begin{aligned}\mathrm{Eig}(f, \lambda) &= \mathrm{Ker}(\lambda\,\mathrm{id} - f) \\ &\overset{5.4}{=} \mathrm{Ker}((\lambda\,\mathrm{id} - f)^{adj}) \\ &= \mathrm{Ker}(\overline{\lambda}\,\mathrm{id} - f^{adj}) \\ &= \mathrm{Eig}(f^{adj}, \overline{\lambda})\end{aligned}$$ □

Theorem 5.6 (Spektralsatz)
Sei $f \in \mathrm{End}_K(V)$ ein Endomorphismus, für den χ_f in Linearfaktoren zerfällt. Genau dann besitzt V eine Orthonormalbasis aus Eigenvektoren von f, wenn f normal ist.

Beweis.

- Hinrichtung: Ist B eine Orthonormalbasis aus Eigenvektoren von f, so ist $A = M_B(f)$ eine Diagonalmatrix. Dann ist auch $M_B(f^{adj}) \overset{4.7}{=} A^*$ eine Diagonalmatrix und $AA^* = A^*A$. Somit ist f normal.
- Rückrichtung: Sei f normal und $\chi_f(t) = \prod_{i=1}^{n}(t - \lambda_i)$. Beweis nach Induktion nach $n = \dim_K(V)$.
  $\underline{n = 0}$: klar
  $\underline{n - 1 \to n}$: Wähle Eigenvektor zum Eigenwert λ_1, o.E. $\|x_1\| = 1$. Sei $U = K \cdot x_1$. Nach Lemma 5.5 ist $f^{adj}(x_1) = \overline{\lambda_1} x_1$, insbesondere ist U f-invariant und f^{adj}-invariant. Für $x \in U^\perp$ ist

  $$\langle f(x), x_1 \rangle = \left\langle x, f^{adj}(x_1) \right\rangle = \left\langle x, \overline{\lambda_1} x_1 \right\rangle = \lambda_1 \langle x, x_1 \rangle = 0$$

  also $f(x) \in U^\perp$ und

  $$\left\langle f^{adj}(x), x_1 \right\rangle = \langle x, f(x_1) \rangle = \langle x, \lambda_1 x_1 \rangle = \overline{\lambda_1} \langle x, x_1 \rangle = 0$$

  also $f^{adj}(x) \in U^\perp$. Somit ist $V = U \oplus U^\perp$ eine Zerlegung in Untervektorräume, die sowohl f-invariant als auch f^{adj}-invariant sind. Insbesondere st $f^{adj}|_{U^\perp} = (f|_{U^\perp})^{adj}$, woraus folgt, dass auch $f|_{U^\perp}$ normal ist:

  $$f|_{U^\perp} \circ (f|_{U^\perp})^{adj} = f \circ f^{adj}|_{U^\perp} = f^{adj} \circ f|_{U^\perp} = f^{adj}|_{U^\perp} \circ f|_{U^\perp} = (f|_{U^\perp})^{adj} \circ f|_{U^\perp}$$

  Außerdem zerfällt auch $\chi_{f|_{U^\perp}} = \prod_{i=2}^{n}(t - \lambda_i)$ in Linearfaktoren. Nach Induktionshypothese existiert eine Orthonormalbasis $(x_2, ..., x_n)$ von $U^\perp$ bestehend aus Eigenvektoren von $f|_{U^\perp}$ und $(x_1, ..., x_n)$ ist dann eine Orthonormalbasis von V aus Eigenvektoren von f. □

Folgerung 5.7
Sei $A \in \mathrm{Mat}_n(\mathbb{C})$. Genau dann gibt es $S \in \mathrm{U}_n$ mit $S^*AS = D$ eine Diagonalmatrix, wenn A normal ist.

▶ **Bemerkung 5.8**
Theorem 5.6 ist eine gemeinsame Verallgemeinerung von Theorem 5.9 und Theorem 6.5

6. Tensorprodukte

Definition 6.1 (billineare Abbildung)
Eine Abbildung $\xi : V \times W \to U$ ist bilinear , wenn für jedes $v \in V$ die Abbildung

$$\begin{cases} W \to U \\ w \mapsto \xi(v, w) \end{cases}$$

und für jedes $w \in W$ die Abbildung

$$\begin{cases} V \to U \\ v \mapsto \xi(v, w) \end{cases}$$

linear sind.

Wir definieren

$$\mathrm{Bil}_K(V, W, U) = \{\xi \in \mathrm{Abb}(V \times W, U) \mid \xi \text{ bilinear}\}$$

■ **Beispiel 6.2**
Seien $V = W = K[t]_{\leq d}$, $U = K[t]_{\leq 2d}$. Die Abbildung

$$\xi : \begin{cases} V \times W \to U \\ (f.g) \mapsto fg \end{cases} \qquad \text{ist bilinear}$$

Wir sehen, dass $\mathrm{Im}(\xi)$ im Allgemeinen kein Untervektorraum von U ist. Ist zum Beispiel $K = \mathbb{Q}$, $d = 1$, so liegen $t^2 = \xi(t, t)$ und $-2 = \xi(-2, 1)$ im $\mathrm{Im}(\xi)$ nicht jedoch $t^2 - 2$, denn wäre $t^2 - 2 = fg$ mit $f, g \in \mathbb{Q}[t]$ linear, so hätte $t^2 - 2$ eine Nullstelle in $\mathbb{Q}$, aber $\sqrt{2} \notin \mathbb{Q}$.

Lemma 6.3
$\mathrm{Bil}_K(V, W, U)$ bildet einen Untervektorraum des K-Vektorraum $\mathrm{Abb}(V \times W, U)$.

Beweis. klar, zum Beispiel

$$(\xi + \xi')(\lambda v, w) = \xi(\lambda v, w) + \xi'(\lambda v, w) = \lambda\xi(v, w) + \lambda\xi(v, w) = \lambda(\xi + \xi')(v, w)$$ □

Lemma 6.4
Ist $\xi \in \mathrm{Bil}_K(V, W, U)$ und $f \in \mathrm{Hom}_K(U, U')$ für einen K-Vektorraum, so ist

$$f \circ \xi \in \mathrm{Bil}_K(V, W, U')$$

Beweis. klar, zum Beispiel

$$(f \circ \xi)(\lambda v, w) = f(\xi(\lambda v, w)) = f(\lambda\xi(v, w)) = \lambda \cdot (f \circ \xi)(v, w)$$ □

Lemma 6.5
Sei $(v_i)_{i\in I}$ eine Basis von V und $(w_j)_{j\in J}$ eine Basis von W. Zu jeder Familie $(u_{ij})_{(i,j)\in I\times J}$ in U gibt es genau ein $\xi \in \mathrm{Bil}_K(V,W,U)$ mit

$$\xi(v_i, w_i) = u_{ij} \quad \forall i \in I, j \in J$$

Beweis.

- Eindeutigkeit: Ist ξ bilinear, $v = \sum_{i\in I} \lambda_i v_i$, $w = \sum_{j\in J} \mu_j w_j$ so ist

$$\begin{aligned}\xi(v,w) &= \xi\left(\sum_{i\in I}\lambda_i v_i, \sum_{j\in J}\mu_j w_j\right)\\ &= \sum_{i\in I}\lambda_i \xi\left(v_i, \sum_{j\in J}\mu_j w_j\right)\\ &= \sum_{i,j}\lambda_i\mu_j u_{ij} \qquad (1)\end{aligned}$$

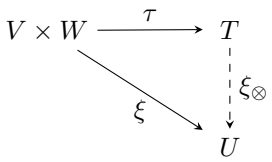
  durch die Familie $(u_{ij})_{i,j}$ bestimmt.

- Existenz: Wird ξ durch (1) definiert, so ist ξ bilinear: Für festes $w = \sum_{j\in J}\mu_j w_j$ ist

$$\begin{cases} V & \to U \\ v = \sum_{i\in I}\lambda_i v_i & \mapsto \xi(v,w) = \sum_{i\in I}\lambda_i\left(\sum_{j\in J}\mu_j u_{ij}\right)\end{cases}$$

  linear (Satz 5.1), analog für festes v. □

Definition 6.6 (Tensorprodukt)
Ein Tensorprodukt von V und W ist ein Paar (T,τ) bestehend aus einem K-Vektorraum T und einer bilinearen Abbildung $\tau \in \mathrm{Bil}_K(V,W,T)$ welche die folgende universelle Eigenschaft erfüllt:
Ist U ein weiterer K-Vektorraum und $\xi \in \mathrm{Bil}_K(V,W,U)$ so gibt es genau ein $\xi_\otimes \in \mathrm{Hom}_K(T,U)$ mit $\xi = \xi_\otimes \circ \tau$.



Anmerkung
Sind V und W zwei Vektorräume und K ein gemeinsamer Körper, so kann man das Tensorprodukt $V \otimes W$, was auch ein Vektorraum ist, wie folgt konstruieren: Wenn $B = (b_1, ..., b_n)$ eine Basis von V und $C = (c_1, ..., c_m)$ eine Basis von W ist, dass ist $V \otimes W$ ein Vektorraum, genannt *Tensorproduktraum*, in dem es eine Basis gibt, die auf eindeutige Weise mit den geordneten Paaren des kartesischen Produkts

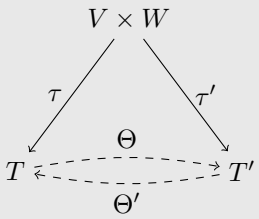
$$B \times C = \{(b_i, c_j)\}$$

der Basen der Ausgangsräume identifiziert werden kann. Die Dimension von $V \otimes W$ ist dann das Produkt der Dimensionen von V und W. Ein Element der Basis von $V \otimes W$, das dem Paar (b_i, c_j) entspricht, wird als $b_i \otimes c_j$ notiert, das $\otimes$ hat also keine tiefere Bedeutung. Ein Element des Tensorproduktes $V \otimes W$ hat dann die Gestalt:

$$\sum_{i,j} \lambda_{ij} \cdot (b_i \otimes c_j)$$

mit $\lambda_{ij} \in K$.

Lemma 6.7
Sind (T, τ) und (T', τ') Tensorprodukte von V und W, so gibt es einen eindeutig bestimmten Isomorphismus $\Theta : T \to T'$ mit $\tau' = \Theta \circ \tau$.



Beweis. Da (T, τ) die universelle Eigenschaft erfüllt, gibt es ein eindeutig bestimmtes $\Theta = (\tau')_{\otimes} \in \mathrm{Hom}_K(T, T')$ mit $\tau' = \Theta \circ \tau$. Analog gibt es $\Theta' \in \mathrm{Hom}_K(T', T)$ mit $\tau = \Theta' \circ \tau'$. Es folgt, dass $\tau = \Theta' \circ \tau' = \Theta' \circ \Theta \circ \tau$. Da auch $\tau = \mathrm{id}_T \circ \tau$ liefert die Eindeutigkeitsaussage in der universellen Eigenschaft von (T, τ), für $U = T$, $\xi = \tau$, dass $\Theta \circ \Theta' = \mathrm{id}_T$. Analog sieht man, dass $\Theta \circ \Theta' = \mathrm{id}_{T'}$. Somit ist Θ ein Isomorphismus. □

Definition 6.8 (Vektorraum mit Basis X)
Sei X eine Menge. Der K-Vektorraum mit Basis X ist der Untervektorraum $V = \mathrm{span}_K((\delta_x)_{x \in X})$ des K-Vektorraum $\mathrm{Abb}(X, K)$ mit $\delta_x(y) = \delta_{x,y} = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$

Lemma 6.9
Sei X eine Menge und V der K-Vektorraum mit Basis X. Dann ist V ein K-Vektorraum und $(\delta_x)_{x \in X}$ ist eine Basis von V.

Beweis. Zu zeigen ist nur, dass $(\delta_x)_{x \in X}$ linear unabhängig ist. Ist $f = \sum_{x \in X} \lambda_x \delta_x$, $\lambda_x \in K$, fast alle gleich 0, und $f = 0$, so ist $\lambda_x = f(x) = 0$ für jedes $x \in X$. □

Lemma 6.10
Sei $(v_i)_{i\in I}$ eine Basis von V und $(w_j)_{j\in J}$ eine Basis von W. Sei T der K-Vektorraum mit der Basis $I \times J$ (im Sinne von Definition 6.8) und $\tau : V \times W \to T$ die bilineare Abbildung gegeben durch $(v_i, w_j) \mapsto \delta_{i,j}$, vergleiche Lemma 6.5. Dann ist (T, τ) ein Tensorprodukt von V und W.

Beweis. Wir schreiben $v_i \otimes w_j$ für $\delta_{i,j}$. Sei U ein weiterer K-Vektorraum und $\xi \in \mathrm{Bil}_K(V, W, U)$. Da $(v_i \otimes w_j)_{(ij)\in I\times J}$ eine Basis von T ist, gibt es genau ein $\xi_\otimes \in \mathrm{Hom}_K(T, U)$ mit $\xi_\otimes(v_i \otimes w_j) = \xi(v_i, w_j)$ für alle i, j, also mit $\xi_\otimes \circ \tau = \xi$ nach Lemma 6.5. Die universelle Eigenschaft ist somit erfüllt. □

Satz 6.11
Es gibt ein bis auf Isomorphie (im Sinne von Lemma 6.7) eindeutig bestimmtes Tensorprodukt

$$(V \otimes_K W, \otimes)$$

von V und W. Sind V und W endlichdimensional, so ist

$$\dim_K(V \otimes_K W) = \dim_K(V) \cdot \dim_K(W)$$

Beweis. Lemma 6.10 und Lemma 6.7 □

■ **Beispiel 6.12**
Durch die Wahl der Standardbasis erhält man einen kanonischen Isomorphismus $K^m \otimes_K K^n \cong \mathrm{Mat}_{m\times n}(K)$.

■ **Beispiel 6.13**
Ist V ein $\mathbb{R}$-Vektorraum mit Basis $(x_1, ..., x_n)$, so ist $\mathbb{C} \otimes_\mathbb{R} V$ ein $\mathbb{R}$-Vektorraum der Dimension $2n$ mit Basis $(1 \otimes x_1 ..., 1 \otimes x_n, i \otimes x_1, ..., i \otimes x_n)$. Durch $\lambda \cdot z \otimes x = (\lambda z) \otimes x$ für $\lambda, z \in \mathbb{C}$, $x \in V$ wird $\mathbb{C} \otimes_\mathbb{R} V$ zu einem $\mathbb{C}$-Vektorraum der Dimension $1 \otimes x_1, ..., 1 \otimes x_n$, $V_\mathbb{C}$, genannt die Komplexifizierung von V.

Satz 6.14
Sei $V \otimes_K W$ ein Tensorprodukt von V und W. Für jeden weiteren K-Vektorraum U liefert die Abbildung $\xi \to \xi_\otimes$ ein Isomorphismus

$$\mathrm{Bil}_K(V, W, U) \xrightarrow{\cong} \mathrm{Hom}_K(V \otimes_K W, U)$$

Beweis. Diese Abbildung heiße Λ.

- Λ ist linear: klar aus Eindeutigkeitsaussage, z.B.

$$(\xi_\otimes + \xi'_\otimes) \circ \otimes = \xi_\otimes \circ \otimes + \xi'_\otimes \circ \otimes = \xi + \xi' = (\xi + \xi')_\otimes \circ \otimes$$

  und somit $\xi_\otimes + \xi'_\otimes = (\xi + \xi')_\otimes$.
- Λ ist injektiv: Ist $\xi \neq 0$, so wegen $\xi = \xi_\otimes \circ \otimes$ auch $\xi_\otimes \neq 0$.
- Λ ist surjektiv: Ist $f \in \mathrm{Hom}_K(V \otimes_K W, U)$, so ist $\xi = f \circ \otimes$ bilinear, die universelle Eigenschaft liefert somit $f = \xi_\otimes \in \mathrm{Im}(\Lambda)$. □

Folgerung 6.15
Sind V und W endlichdimensional, so ist

$$V \otimes_K W \cong \mathrm{Bil}_K(V, W, K)^*$$

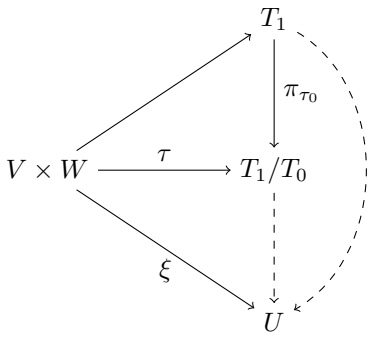
Beweis. Es ist $\dim_K(V \otimes_K W) < \infty$ und deshalb

$$V \otimes_K W \cong (V \otimes_K W)^{**} \overset{6.14}{\cong} \mathrm{Bil}_K(V, W, K) \qquad \square$$

▶ **Bemerkung 6.16**
Während obige Konstruktion des Tensorprodukts von der Wahl (und Existenz) von Basen abhängt, ist die folgende Konstruktion "basisfrei":
Sei T_1 der K-Vektorraum mit Basis $V \times W$ und T_0 der Untervektorraum von T_1 erzeugt von Elementen der Form:

$$\begin{aligned} \delta_{v+v',w} - \delta_{v,w} - \delta_{v',w} \\ \delta_{v,w+w'} - \delta_{v,w} - \delta_{v,w'} \\ \delta_{\lambda v,w} - \lambda \cdot \delta_{v,w} \\ \delta_{v,\lambda w} - \lambda \cdot \delta_{v,w} \end{aligned}$$

mit $v, v' \in V$, $w, w' \in W$ und $\lambda \in K$. Sei weiter $T = T_1/T_0$ und $\tau : V \times W \to T$ gegeben durch $(v, w) \mapsto \delta_{v,w} + T_0$. Dann ist (T, τ) ein Tensorprodukt von V und W.



▶ **Bemerkung 6.17**
Analog kann man für $k \geq 2$ und die K-Vektorräume $V_1, ..., V_k$ k-lineare Abbildungen $V_1 \times ... \times V_k \to U$ definieren und erhält dann Tensorprodukte $V_1 \otimes_K ... \otimes_K V_k$.

Kapitel VIII

Moduln

In diesem ganzen Kapitel sei R ein kommutativer Ring mit Einselement.

1. Moduln

Definition 1.1
Ein R-Modul ist ein Tripel $(M, +, \cdot)$ bestehend aus einer Menge M, einer Verknüpfung $+ : M \times M \to M$ und der Abbildung $\cdot : R \times M \to M$ (Skalarmultiplikation) für die gelten:

- (M1): $(M, +)$ ist eine abelsche Gruppe
- (M2): Addition und Skalarmultiplikation sind verträglich. Für alle $x, y \in M$ und $a, b \in R$ gelten
  1. $a(x + y) = ax + ay$
  2. $(a + b)x = ax + bx$
  3. $a \cdot bx = ab \cdot x$
  4. $1 \cdot x = x$

■ **Beispiel 1.2**

1. Ist $R = K$ ein Körper, so sind die R-Moduln genau die K-Vektorräume.
2. Ist $R = \mathbb{Z}$, so sind die R-Moduln genau die abelschen Gruppen mit der einzig möglichen Skalarmultiplikation

$$\mathbb{Z} \times A \to A, (k, a) \mapsto ka = \underbrace{1 + ... + 1}_{k\text{-mal}} a = \underbrace{a + ... + a}_{k\text{-mal}}$$

   vergleiche Beispiel 2.3
3. Jedes Ideal $M \subseteq R$ ist ein R-Modul mit Einschränkung der Multiplikation als Skalarmultiplikation.
4. Ist K ein Körper, V ein K-Vektorraum und $f \in \mathrm{End}_K(V)$, so wird V durch $P(t) \cdot x := P(f)(x)$ zu einem Modul über dem Ring $R = K[t]$, siehe auch Bemerkung 5.2

▶ **Bemerkung 1.3**
Sei M ein R-Modul. Wie für Vektorräume überzeugt man sich leicht, dass $0x = 0$, $a0 = 0$, $(-a)x = a(-x) = -ax$ für alle $a \in R$, $x \in M$.

Im Gegensatz zu Vektorräumen folgt aber aus $ax = 0$ nicht, dass $a = 0$ oder $x = 0$, siehe zum

Beispiel das $\mathbb{Z}$-Modul $M = \mathbb{Z}/n\mathbb{Z}$. Es ist

$$n \cdot \overline{1} = \overline{n} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$$

aber $0 \neq n \in \mathbb{Z}$.

Definition 1.4 (Homomorphismus von R-Moduln)
Seien M, M' R-Moduln. Eine Abbildung $f : M \to M'$ ein Homomorphismus von R-Moduln (oder R-Homomorphismus oder R-linear), wenn

$$f(x + y) = f(x) + f(y)$$
$$f(ax) = a \cdot f(x)$$

Wir bezeichnen die Menge der R-Homomorphismen $f : M \to M'$ mit $\mathrm{Hom}_R(M, M')$. Wie üblich definiert man den Kern eines R-Homomorphismus, sowie die Begriffe Monomorphismus , Epimorphismus , Isomorphismus , Endomorphismus und Automorphismus von R-Moduln.

■ **Beispiel 1.5**

- Ist $R = K$, so sind die R-Homomorphismen genau die lineare Abbildungen.
- Ist $R = \mathbb{Z}$, so sind die R-Homomorphismen genau die Gruppenhomomorphismen.

■ **Beispiel 1.6**
Für jedes $a \in R$ ist die Abbildung

$$\begin{cases} M \to M \\ x \mapsto ax \end{cases}$$

einen Endomorphismus von M.

Definition 1.7 (Untermodul, Erzeugendensystem)
Ein Untermodul ist eine nichtleere Teilmenge $N \subseteq M$, für die gilt:

- Sind $x, y \in N$, so ist auch $x + y \in N$.
- Ist $a \in R$ und $x \in N$, so ist auch $ax \in N$.

Für eine Familie $(x_i)_{i \in I}$ ist

$$\sum_{i \in I} Rx_i = \{\sum_{i \in I} ax_i \mid a \in R, \text{ fast alle gleich } 0\}$$

der von $(x_i)_{i \in I}$ erzeugte Untermodul von M. Ist $\sum_{i \in I} Rx_i = M$, so ist $(x_i)_{i \in I}$ ein Erzeugendensystem von M. Der R-Modul M ist endlich erzeugt , wenn er ein endliches Erzeugendensystem besitzt.

▶ **Bemerkung 1.8**
Wieder ist der Kern eines R-Homomorphismus $f : M \to M'$ ein Untermodul von M. Leicht sieht man auch hier, dass $\sum_{i \in I} Rx_i$ ein Untermodul von M ist, und zwar der kleinste, der alle x_i enthält.

■ **Beispiel 1.9**

- Ist $R = K$ ein Körper, so sind die Untermoduln von M genau die Untervektorräume.
- Ist $R = \mathbb{Z}$, so sind die Untermoduln von M genau die Untergruppen und der von einer Familie erzeugte Untermodul ist genau gleich der davon erzeugten Untergruppe.
  Ist zum Beispiel $M = \mathbb{Z}$, so sind alle $n\mathbb{Z}$ Untermoduln von M.

Definition 1.10 (freie Familie, Basis)
Eine Familie $(x_i)_{i\in I}$ in M ist frei oder (R-linear unabhängig), wenn es keine Familie $(\lambda_i)_{i\in I}$ von Elementen von R, fast alle gleich 0, aber nicht alle gleich 0, mit $\sum_{i\in I} \lambda_i x_i = 0$ gibt.

Ein freies Erzeugendensystem heißt Basis . Besitzt M eine Basis, so nennt man M frei .

Satz 1.11
Seien M, M' R-Moduln, $(x_i)_{i\in I}$ eine Basis von M und $(y_i)_{i\in I}$ eine Familie in M'. Dann gibt es genau eine R-lineare Abbildung $f : M \to M'$ mit $f(x_i) = y_i$ für alle i.

Beweis. klar, siehe Satz 5.1 □

■ **Beispiel 1.12**

- Für $n \in \mathbb{N}$ ist $M = R^n$ mit komponentenweiser Addition und Skalarmultiplikation ein endlich erzeugter freier R-Modul mit der üblichen Standardbasis.
- Allerdings ist zum Beispiel der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ zwar endlich erzeugt aber nicht frei. Für $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ist $n\overline{a} = \overline{0}$, also $\overline{a}$ linear abhängig.

Definition 1.13 (Summen von Moduln)
Die Summe einer Familie $(N_i)_{i\in I}$ von Untermoduln von M ist

$$\sum_{i\in I} N_i = \left\{ \sum_{i\in I} x_i \mid x_i \in N_i, \text{ fast alle gleich } 0 \right\}$$

Lässt sich jedes $x \in \sum_{i\in I} N_i$ eindeutig als $\sum_{i\in I} x_i$ mit $x_i \in N_i$ schreiben, so nennt man die Summe direkt und schreibt dafür auch $\bigoplus_{i\in I} N_i$.

Ist $(M_i)_{i\in I}$ eine Familie von R-Moduln, so definiert man deren (externe) direkte Summe als das R-Modul

$$\bigoplus_{i\in I} M_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} M_i \mid x_i = 0 \text{ für fast alle } i \in I \right\}$$

mit komponentenweiser Addition und Skalarmultiplikation.

▶ **Bemerkung 1.14**
Wie auch für Vektorräume ist eine externe direkte Summe eine direkte Summe der entsprechenden Untermoduln und ist $M = \bigoplus_{i\in I} N_i$, so ist M isomorph zur externen direkten Summe der N_i.

Definition 1.15 (Torsionsmodul)
Für $a \in R$ definiert man den a-Torsionsmodul von M als

$$M[a] := \{x \in M \mid ax = 0\}$$

Die Elemente des Torsionsmoduls

$$M_{tor} := \bigcup_{0 \neq a \in R} M[a] = \{x \in M \mid ax = 0 \text{ für ein } a \in R \backslash \{0\}\}$$

nennt man die Torsionselemente von M.

Satz 1.16
Für $a \in R$ ist $M[a]$ ein Untermodul von M. Ist R nullteilerfrei, so ist auch M_{tor} ein Untermodul von M.

Beweis. $M[a]$ ist der Kern des Endomorphismus $x \mapsto ax$ (Beispiel 1.6), somit ein Untermodul (Bemerkung 1.8). Seien $a, b \in R\backslash\{0\}$ und $x \in M[a]$, $y \in M[b]$. Ist R nullteilerfrei so ist $ab \neq 0$ und

$$(ab) \cdot (x + y) = b \cdot \underbrace{ax}_{=0} + a \cdot \underbrace{by}_{=0} = 0$$

also $x + y \in M[ab] \subseteq M_{tor}$. Somit ist M_{tor} in diesem Fall einer Untermodul von M. □

■ **Beispiel 1.17**
Sei $R = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$, dann ist $M_{tor} = M = M[n]$.

2. Teilbarkeit

Definition 2.1 (Teilbarkeit)
Seien $a, b \in R$.

1. a teilt b (in Zeichen $a \mid b$): Es existiert $x \in R$ mit $b = ax$.
2. a und b sind assoziiert (in Zeichen $a \sim b$): Es existiert $x \in R^\times$ mit $b = ax$.

Mathematica/WolframAlpha-Befehle (Teiler)
Möchte man mit Mathematica bzw. WolframAlpha überprüfen, ob n von m geteilt wird, also $m \mid n$ (!), kann man folge Funktion aufrufen:

```
Divisible[n,m]
```

Eine Liste der Teiler einer Zahl x erhält man mit

```
Divisors[x]
```

Lemma 2.2
Für $a, b, c, d \in R$ gelten

1. $a \mid a$
2. $a \mid b$ und $b \mid c \Rightarrow a \mid c$
3. $a \mid b$ und $a \mid c \Rightarrow a \mid (b + c)$
4. $a \mid b$ und $c \mid d \Rightarrow (ac) \mid (bd)$

Beweis. klar □

Lemma 2.3
Für $a, b, c, d \in R$ gelten

1. $a \sim a$
2. $a \sim b$ und $b \sim c \Rightarrow a \sim c$
3. $a \sim b \Rightarrow b \sim a$
4. $a \sim b$ und $c \sim d \Rightarrow (ac) \sim (bd)$

Beweis. klar, da $(R^\times, \cdot)$ eine Gruppe ist. □

▶ **Bemerkung 2.4**
Teilbarkeit auf R ist insbesondere eine Präordnung , das heißt reflexiv und transitiv, und Assoziiertheit ist eine Äquivalenzrelation.

Lemma 2.5
Sei R nullteilerfrei und seien $a, b \in R$. Genau dann ist $a \sim b$, wenn $a \mid b$ und $b \mid a$.

Beweis.
- Hinrichtung: $b = ax$ mit $x \in R^\times \Rightarrow a = bx^{-1}$.
- Rückrichtung: $b = ax$, $a = by$ mit $x, y \in R^\times$

$$a = by = axy$$
$$a(1 - xy) = 0$$

Also $a = 0$ und damit $b = 0$ oder $xy = 1$, also $x, y \in R^\times$. In beiden Fällen folgt $a \sim b$. □

■ **Beispiel**
Offenbar $2 \mid -2$ und $-2 \mid 2$. Es gilt $2 \sim -2$ und $-2 \sim 2$.

Satz 2.6
Sie R nullteilerfrei. Mit $[a] := \{a' \in R \mid a \sim a'\}$ wird durch $[a][b] \iff a \mid b$ eine wohldefinierte Halbordnung auf $R/\sim := \{[a] \mid a \in R\}$ gegeben.

Beweis.
- wohldefiniert: $a \mid b$, $a \sim a'$, $b \sim b' \Rightarrow a' \mid b'$: $ax = b$, $au = a'$, $bv = b$ mit $x \in R$ und $u, v \in R^\times$

$$b' = bv = axv = a' \underbrace{u^{-1}vx}_{\in R}$$

also $a' \mid b'$.
- reflexiv: klar
- transitiv: aus Transitivität von $\mid$
- antisymmetrisch: Lemma 2.5 □

Definition 2.7 (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)
Seien $a, b \in R$. Ein $c \in R$ ist ein größter gemeinsamer Teiler von a und b in Zeichen $c = \mathrm{ggT}(a, b)$, wenn gilt: $c \mid a$ und $c \mid b$ und ist $d \in R$ mit $d \mid a$ und $d \mid b$, so auch $d \mid c$.

Ein $c \in R$ ist ein kleinstes gemeinsames Vielfaches von a und b, in Zeichen $c = \mathrm{kgV}(a, b)$, wenn gilt: $a \mid c$ und $b \mid c$ und ist $d \in R$ mit $a \mid d$ und $b \mid d$, so ist $c \mid d$.

Mathematica/WolframAlpha-Befehle (ggT und kgV)
Die Funktionen für den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache in Mathematica bzw. WolframAlpha sind

```
GCD[6,12,4,32]
LCM[6,12,4,32]
```

▶ **Bemerkung 2.8**
Wenn ggT und kgV in einem nullteilerfreien Ring R existieren, sind sie eindeutig bestimmt, aber nur bis auf Assoziiertheit (Lemma 2.5).

Definition 2.9 (Primzahl, irreduzibel)
Sei $x \in R$.

- x ist prim $\iff$ $x \notin R^\times \cup \{0\}$ und $\forall a, b \in R$ gilt $x \mid (ab) \Rightarrow x \mid a \vee x \mid b$.
- x ist irreduzibel $\iff$ $x \notin R^\times \cup \{0\}$ und $\forall a, b \in R$ gilt $x = ab \Rightarrow a \in R^\times \vee b \in R^\times$.

▶ **Bemerkung 2.10**
Leicht sieht man: Ist $p \in R$ prim und $a_1, ..., a_n \in R$ mit $p \mid (a_1 \dots a_n)$, so gilt $p \mid a_i$ für ein i.

■ **Beispiel 2.11**

- In $R = \mathbb{Z}$ gilt: p prim $\iff$ p irreduzibel
- Sei $f \in R = \mathbb{Q}[t]$.
  - $\deg(f) = 1 \Rightarrow f \sim (t - a)$ ist irreduzibel und prim (denn $(t - a) \mid g \iff g(a) = 0$)
  - $\deg(f) = 2$: $f = t^2 - 1$ ist nicht irreduzibel, $t^2 - 2$ ist irreduzibel

Satz 2.12
Sei R nullteilerfrei und $0 \neq p \in R \backslash R^\times$. Ist p prim, so ist es auch irreduzibel.

Beweis. Sei $p = ab$ mit $a, b \in R$. Da insbesondere $p \mid ab$ und p prim ist, folgt $p \mid a$ oder $p \mid b$. Sei ohne Einschränkung $p \mid a$, das heißt $a = pa'$ mit $a' \in R$.

$$\begin{aligned} &\Rightarrow p = ab = pa'b \\ &\Rightarrow p(1 - ab) = 0 \\ &\Rightarrow a'b = 1, \text{ insbesondere } b \in R^\times \end{aligned}$$

Somit ist p irreduzibel. □

▶ **Bemerkung 2.13**
Erinnerung: Ein Ideal von R ist eine Untergruppe $I \subseteq (R, +)$ mit

$$a \in I, r \in R \Rightarrow ra \in I$$

also genau ein Untermodul des R-Moduls R.

Definition 2.14 (erzeugtes Ideal, Hauptideal)
Sei $A \subseteq R$. Das von A erzeugte Ideal mit

$$\langle A \rangle := \left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, ..., a_n \in A, r_1, ..., r_n \in R \right\}$$

Ist $A = \{a_1, ..., a_n\}$, so schreibt man auch $(a_1, ..., a_n)$ für $\langle A \rangle$. Ein Ideal der Form $I = (a)$ ist ein Hauptideal .

▶ **Bemerkung 2.15**
Das von A erzeugte Ideal $\langle A \rangle$ ist gleich dem von A erzeugten Untermodul des R-Moduls R, und ist das kleinste Ideal von R, das A enthält.

▶ **Bemerkung 2.16**

Für $a \in R$ ist $(a) = Ra$ und für $a, b \in R$ sind äquivalent:

1. $a \mid b$
2. $b \in (a)$
3. $(b) \subseteq (a)$

Für R nullteilerfrei sind zudem äquivalent:

1. $a \sim b$
2. $(a) = (b)$

■ **Beispiel 2.17**

Jeder Ring hat die Ideale $(0) = \{0\}$ und $(1) = R$. Für jedes $a \in R^\times$ ist $(a) = (1)$, ist R also ein Körper, so hat R keine weiteren Ideale.

■ **Beispiel 2.18**

In $R = \mathbb{Z}$: Für $n \in \mathbb{Z}$ ist $(n) = \mathbb{Z} \cdot n = n\mathbb{Z}$.

3. Hauptidealringe

Sei R nullteilerfrei.

Definition 3.1 (Hauptidealring)
Ein Ring R ist ein Hauptidealring , wenn R nullteilerfrei ist und jedes Ideal von R ein Hauptideal ist.

■ **Beispiel 3.2**
Ist $R = K$ ein Körper, so hat R nur die Ideale (0) und (1), und somit ist R ein Hauptidealring.

Definition 3.3 (euklidische Gradfunktion)
Eine euklidische Gradfunktion auf R ist eine Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}_0$ für die gilt:
Für jedes $a \in R$ und $0 \neq b \in R$ gibt es $q, r \in R$ mit $a = bq + r$, wobei $r = 0$ oder $\delta(r) < \delta(b)$.

Ein nullteilerfreier Ring R ist euklidisch , wenn es eine euklidische Gradfunktion auf R gibt.

■ **Beispiel 3.4**

1. Auf $R = \mathbb{Z}$ ist der Absolutbetrag
$$\delta(x) = |x|$$
eine euklidische Gradfunktion. (Theorem 4.6)
2. Auf $R = K[t]$, K ein Körper, ist der Grad
$$\delta(f) = \deg(f)$$
eine euklidische Gradfunktion. (Theorem 6.5)
3. $R = K$ ein Körper ist
$$\delta(x) = 0$$
eine euklidische Gradfunktion, da man in einem Körper jedes Element durch jedes Element (Ausnahme: 0) teilen kann.

Lemma 3.5
Sei $\delta : R\backslash\{0\} \to \mathbb{N}_0$ eine euklidische Gradfunktion und $(0) \neq \trianglelefteq R$ ein Ideal. Ist $0 \neq a \in I$ mit $\delta(a) = \min\{\delta(b) \mid 0 \neq b \in I\}$, so ist $I = (a)$.

Beweis.
- "$\supseteq$": $a \in I \Rightarrow (a) \subset I$
- "$\subseteq$": Sei $0 \neq b \in I$. Schreibe $b = qa + r$ mit $q, r \in R$ und $r = 0$ oder $\delta(r) < \delta(a)$. Da $r = \underbrace{b}_{\in I} - q\underbrace{a}_{\in I} \in I$ folgt wegen der Minimalität von $\delta(a)$, dass $r = 0$, also $b \in (a)$. □

Satz 3.6
Ist R euklidisch, so ist R ein Hauptidealring.

Beweis. Sei $I \trianglelefteq R$ ein Ideal. Ist $I = (0)$, so ist I ein Hauptideal. Andernfalls existiert ein $0 \neq a \in I$ mit $\delta(a)$ minimal. Nach Lemma 3.5 ist $I = (a)$ ein Hauptideal. □

Folgerung 3.7
Die Ringe $\mathbb{Z}$ und $K[t]$, K ein Körper, sind Hauptidealringe.

Lemma 3.8 (Lemma von Bézout)
Sei R ein Hauptidealring und $a, b \in R$. Es existiert ein $c \in R$ mit $c = \mathrm{ggT}(a, b)$ und $(c) = (a, b)$. Insbesondere gibt es $x, y \in R$ mit $c = ax + by$ und $\mathrm{ggT}(x, y) = 1$.

Beweis. R Hauptidealring $\Rightarrow \exists c \in R$ mit $(c) = (a, b)$, insbesondere $c = ax + by$ mit $x, y \in R$.

- $c = \mathrm{ggT}(a, b)$: $a, b \in (c) \Rightarrow c \mid a$ und $c \mid b$. Ist $d \in R$ mit $d \mid a$ und $d \mid b$, so ist $d \mid (ax + by) = c$
- $\mathrm{ggT}(x, y) = 1$: Ist $d \in R$ mit $d \mid x$ und $d \mid y$, so gelten $(cd) \mid (ax)$ und $(cd) \mid (by) \Rightarrow (cd) \mid (ax + by) = c \Rightarrow d \in R^\times$, also $d \sim 1$. □

Satz 3.9
Sei R ein Hauptidealring, $p \in R$. Ist p irreduzibel, so auch prim.

Beweis. Seien $a, b \in R$ mit $p \mid (ab)$. Angenommen $p \nmid a$. DA p irreduzibel ist, ist $\mathrm{ggT}(p, a) = 1$, also $1 = px + ay$ mit $x, y \in R$ nach Lemma 3.8. Also $p \mid (pbx + aby) = b$. □

4. Faktorielle Ringe

Sei R nullteilerfrei.

Definition 4.1 (faktorielle Ringe)
R ist faktoriell $\iff$ jedes $0 \neq x \in R \backslash R^\times$ ist ein Produkt von Primelementen.

Lemma 4.2
Sei R faktoriell und $x \in R$. Ist x irreduzibel, so auch prim.

Beweis. Sei x irreduzibel, insbesondere $0 \neq x \in R \backslash R^\times$. Da R faktoriell, ist $x = p_1, ..., p_n$ mit $p_1, ..., p_n \in R$ prim. Da x irreduzibel ist und $p_i \notin R^\times$ ist $n = 1$ und somit $x = p_1$ prim. □

Lemma 4.3
Sei R ein Hauptidealring und

$$I_1 \subseteq I_2 \subseteq ...$$

eine Kette von Idealen in R. Dann existiert ein $n \in \mathbb{N}$ mit $I_n = I_m$ für alle $m \geq n$.

Beweis. Behauptung: $I = \bigcup_{n=1}^{\infty} I_n$ ist wieder ein Ideal von R.
Beweis: schon in den Übungen zum Teil behandelt, aber hier noch mal kurz bewiesen

- $i \in I$, $r \in R \Rightarrow x \in I_n$ für ein $n \overset{I_n \trianglelefteq}{\Rightarrow} rx \in I_n \subseteq I$
- $x, y \in I \Rightarrow x \in I_n, y \in I_m$ mit $n, m \in \mathbb{N} \overset{\text{Kette}}{\Rightarrow} x + y \in I_k \subseteq$ mit $k = \max\{n, m\}$

Da R Hauptidealring ist, ist somit $I = (x)$ für ein $x \in R$. Mit $I = \bigcup_{n \in \mathbb{N}} I_n$ folgt $x \in I_n$ für ein n, und somit $(x) \subseteq I_n \subseteq I_m \subseteq I = (x)$, für $m \geq n$, also $I_n = I_m$. □

Satz 4.4
Ist R ein Hauptidealring, so ist R faktoriell.

Beweis. Sei $X := \{a \in R \mid a \text{ ist Produkt von Primelementen}\} \cup \{0\} \cup R^\times$. Zu zeigen ist $X = R$. Angenommen, es gebe $a \in R \backslash X$. Da nicht prim ist, insbesondere nicht irreduzibel (Satz 3.9), ist $a = a_1 \cdot a_1'$ mit $a_1, a_1' \in R \backslash R^\times$. Wären a_1 und a_1' in X, so auch a, also ohne Einschränkung $a_1 \notin X$. Fährt man nun mit a_1 so fort, erhält man eine Folge $a_1, a_2, ...$ von Elementen von $R \backslash X$ mit $a_{i+1} \mid a_i$ und $a_{i+1} \nsim a_i$ für alle i. Die entsprechenden Hauptideale bilden eine Kette

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ...$$

im Widerspruch zu Lemma 4.3. Somit ist $X = R$, also R faktoriell. □

Anmerkung
Es gilt also euklidisch ⇒ Hauptidealring ⇒ faktoriell.

Lemma 4.5
Sind $p_1, ..., p_r \in R$ prim, $q_1, ..., q_s \in R$ irreduzibel mit

$$\prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$$

ist $r = s$ und nach Umnummerierung ist

$$p_i \sim q_i \quad \forall i$$

Beweis. Wir zeigen die Behauptung unter der schwächeren Annahme

$$\prod_{i=1}^{r} p_i \sim \prod_{j=1}^{s} q_j$$

durch Induktion nach r.
$\underline{r = 0:}$ $1 \sim \prod_{j=1}^{s} q_j \Rightarrow q_j \in R^\times \ \forall j \overset{q_j \text{ irred.}}{\Rightarrow} s = 0$
$\underline{r - 1 \to r:}$ $p_1 \mid \prod_{i=1}^{r} p_i \sim \prod_{j=1}^{s} q_j \overset{p_1 \text{ prim}}{\Rightarrow} p_1 \mid q_j$ für ein j. Nach Umnummerierung ist $j = 1$. Da q_1 irreduzibel und $p_1 \notin R^\times$ ist $p_1 \sim q_1$, also $q_1 = p_1 \cdot u$ mit $u \in R^\times$. Es folgt

$$p_1 \cdot \left(\prod_{i=2}^{r} p_i - u \cdot \prod_{j=2}^{s} q_j \right) = 0$$

$$\prod_{i=2}^{r} p_i = u \cdot \prod_{j=2}^{s} q_j \sim \prod_{j=2}^{s} q_j$$

Nach Induktionshypothese ist $r - 1 = s - 1$, und nach Umnummerierung ist $p_i \sim q_i$ für $i = 2, ..., r$. □

Satz 4.6
Ist R faktoriell, so lässt sich jedes $0 \neq x \in R \backslash R^\times$ auf eindeutige Weise (bis auf Reihenfolge und Assoziiertheit) als Produkt von Primelementen schreiben.

Beweis. Sei $x = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$ mit p_i, q_j prim. Da die q_j nach Satz 2.12 irreduzibel sind, folgt $r = s$ und $p_i \sim q_i$ für alle i aus Lemma 4.5. □

Folgerung 4.7
Sei R faktoriell und enthalte $\mathcal{P} \subseteq R$ für jede Äquivalenzklasse assoziierter Primelemente genau einen Vertreter. Dann lässt sich jedes $0 \neq a \in R$ als

$$a = \varepsilon \cdot \prod_{p \in \mathcal{P}} p^{\mu(p)}$$

mit eindeutig bestimmten $\varepsilon \in R^\times$ und $\mu(p) \in \mathbb{N}_0$, fast alle gleich 0, schreiben.

■ **Beispiel 4.8**

1. Jedes $n \in \mathbb{N}$ lässt sich eindeutig als

$$n = \prod_{p \in \mathbb{P}} p^{n_p}$$

schreiben, wobei $\mathbb{P}$ die Menge der Primzahlen ist (Hauptsatz der Arithmetik).

2. Bezeichnet $\mathcal{M}$ die Menge der normierten irreduziblen Polynome in $K[t]$ (K Körper), so lässt sich jedes $0 \neq f \in K[t]$ eindeutig als

$$f = c \cdot \prod_{P \in \mathcal{M}} P^{n_p}$$

mit $c \in K^\times$ und $n_p \in \mathbb{N}_0$, fast alle gleich 0, schreiben.

5. Quotienten von Ringen und Moduln

Seien M und M' zwei R-Moduln und $N \subseteq M$ ein Untermodul.

Definition 5.1 (Quotientenmodul)
Für $x \in M$ schreiben wir

$$x + N := \{x + y \mid y \in N\}$$

Der Quotientenmodul (oder Faktormodul) von M modulo N ist

$$M/N := \{x + N \mid x \in M\}$$

zusammen mit der Addition

$$(x + N) + (y + N) := (x + y) + N \quad (x, y \in M)$$

und der Skalarmultiplikation

$$r \cdot (x + N) := rx + N \quad (x \in M, r \in R)$$

Sei $\pi_N : M \to M/N$ die Abbildung gegeben durch $x \mapsto x + N$.

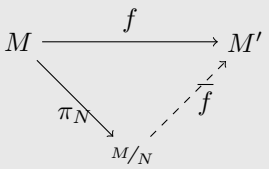
Lemma 5.2
Addition und Skalarmultiplikation sind wohldefiniert und machen M/N zu einem R-Modul. Die Abbildung $\pi_N : M \to M/N$ ist ein R-Epimorphismus mit Kern

$$\mathrm{Ker}(\pi_N) = N$$

Beweis.
- wohldefiniert: wie in Lemma 7.5
- M/N ist R-Modul: wie in Satz 7.7 □

▶ **Bemerkung 5.3**
Durch $x \sim_N x' \iff x - x' \in N$ wird eine Äquivalenzrelation $\sim_N$ auf M definiert, und $x + N$ ist eine $\sim_N$-Äquivalenzklasse $[x]_{\sim_N} = \{y \in M \mid x \sim_N y\}$.

Satz 5.4 (Homomorphiesatz für Moduln)
Sei $f \in \mathrm{Hom}_K(M, M')$ und $N \subseteq M$ ein Untermodul mit $N \subseteq \mathrm{Ker}(f)$. Dann gibt es genau ein $\overline{f} \in \mathrm{Hom}_K(M/N, M')$ mit $f = \overline{f} \circ \pi_N$.



Beweis. Analog zu Theorem 7.9. Man zeigt, dass jedes $\overline{f} \in \mathrm{Hom}_K({}^M\!/_N, M')$

$$\bar{f}(x+N) = f(x) \quad (x \in M)$$

erfüllen muss, und dass dies wiederum eine wohldefinierte Abbildung liefert. □

Lemma 5.5
Durch $U \mapsto \pi_N(U)$ wird eine Bijektion gegeben zwischen

- den Untermoduln von M, die N enthalten
- den Untermoduln von ${}^M\!/_N$.

Beweis. Sei $\mathcal{U}$ die Menge der Untermoduln von M, die N enthalten, $\overline{\mathcal{U}}$ die Menge der Untermoduln von ${}^M\!/_N$.

- $U \in \mathcal{U} \Rightarrow \pi_N(U) \in \overline{\mathcal{U}}$: klar, da π_N ein Homomorphismus ist
- $\overline{U} \in \overline{\mathcal{U}} \Rightarrow \pi_N^{-1} \in \mathcal{U}$: klar, da π_N ein Homomorphismus ist und $N = \mathrm{Ker}(\pi_N) = \pi_N^{-1}(\{0\}) \subseteq \pi_N^{-1}(\overline{U})$
- $\overline{U} \in \overline{\mathcal{U}} \Rightarrow \pi_N(\pi_N^{-1}(\overline{U})) = \overline{U}$: klar, da π_N surjektiv
- $U \in \mathcal{U} \Rightarrow \pi_N^{-1}(\pi_N(U)) = U$:

$$\begin{aligned}
\pi_N^{-1}(\pi_N(U)) &= \bigcup_{x \in U} \pi_N^{-1}(\pi_N(x)) \\
&= \bigcup_{x \in U} \pi_N^{-1}(x+N) \\
&= \bigcup_{x \in U} (x+N) \\
&= U + N = U
\end{aligned}$$

□

▶ **Bemerkung 5.6**
Das Ideal $I \trianglelefteq R$ ist ein Untermodul des R-Moduls R, somit haben wir ein R-Modul ${}^R\!/_I$ definiert. Man kann ${}^R\!/_I$ mit einer Ringstruktur ausstatten.

Definition 5.7 (Quotientenring)
Sei $I \trianglelefteq R$ ein Ideal. Für $x \in R$ schreiben wir

$$x + I = \{x + a \mid a \in I\}$$

Dann ist

$${}^R\!/_I = \{x + I \mid x \in R\}$$

der Quotientenring von R modulo I mit Addition und Skalarmultiplikation

$$\begin{aligned}
(x+I) + (x'+I) &= (x+x') + I \quad \forall x, x' \in R \\
(x+I) \cdot (x'+I) &= (x \cdot x') + I \quad \forall x, x' \in R
\end{aligned}$$

Und wieder $\pi_I : R \to {}^R\!/_I$ mit $x \mapsto x + I$.

Satz 5.8
Addition und Multiplikation sind wohldefiniert und machen R/I zu einem kommutativen Ring mit Einselement. π_I ist ein Ringhomomorphismus mit Kern

$$\mathrm{Ker}(\pi_I) = I$$

Beweis.

- Addition wohldefiniert: Lemma 5.2
- Multiplikation wohldefiniert: Sind $x, x', y, y' \in R$ mit

$$x + I = x' + I$$
$$y + I = y' + I$$

Dann ist

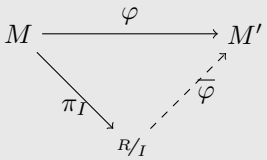
$$x - x' = a \in R \quad \Rightarrow x = x' + a$$
$$y - y' = b \in R \quad \Rightarrow y = y' + a$$

Also

$$xy = (x' + a)(y' + b) = x'y' + \underbrace{ay' + x'b + ab}_{\in I}$$
$$\Rightarrow xy + I = x'y' + I$$

- R/I ist Ring: R1 bis R3 folgen aus den entsprechenden Eigenschaften von R.
- R/I ist kommutativ: folgt auch aus den Eigenschaften von R.
- Einselement: $1 + I$
- π_I ist ein Ringhomomorphismus: folgt nach Definition
- $\mathrm{Ker}(\pi_I)$: klar □

Satz 5.9 (Homomorphiesatz für Ringe)
Sei $\varphi : R \to R'$ ein Ringhomomorphismus, $I \trianglelefteq R$ ein Ideal mit $I \subseteq \mathrm{Ker}(\varphi)$. Dann gibt es genau einen Ringhomomorphismus mit $\overline{\varphi} : R/I \to R'$, sodass $\overline{\varphi} \circ \pi_I = \varphi$.



Beweis. Man sieht, dass

$$\bar{\varphi}(x + I) = \varphi(x) \quad \forall x \in R$$

gelten muss, und das dies auch ein wohldefinierter Ringhomomorphismus ist. □

■ **Beispiel 5.10**

- $R = \mathbb{Z}$, $\forall n \in \mathbb{N}$ ist $n\mathbb{Z}$ ein Ideal.

$$\mathbb{Z}/(n) = \mathbb{Z}\backslash n\mathbb{Z}$$

- Sei K ein Körper und sei $a \in K$. Dann ist $K[t] \to K$, $P \mapsto P(a)$ ist ein Ringepimorphismus. Der Kern $\mathrm{Ker}(\varphi) = (t-a)$, also alle Polynome, die in a eine Nullstelle haben. Es folgt

$$K[t]/(t-a) \cong K$$

☺ $\mathbb{Z}$ ist der Herr der Ringe ☺

■ **Beispiel 5.11**

Sei $0 \neq p \in K[t]$. $K[t]/(p)$ ist ein Ring, aber auch ein $K[t]$-Modul und damit ein K-Vektorraum.

$$\dim_K \left(K[t]/(p)\right) = n = \deg(p)$$

Ist $B = (1, \bar{t}, ..., \overline{t^{n-1}})$ eine Basis wobei $\overline{x} = \pi_{(p)}(x)$ $\forall x \in K[t]$.

6. Der Elementarteilersatz

Sei R Hauptidealring.

Definition 6.1

Seien $a, b, x, y \in R$. Für $i, j \in \{1, ..., n\}$ ist

$$E_{ij} = (\delta_{\sigma,i}, ..., \delta_{\mu,j})_{\sigma,\mu} \in \mathrm{Mat}_n(\mathbb{R})$$

Sei

$$E_{ij}(a, b, x, y) = \mathbb{1}_n - E_{ii} - E_{jj} + aE_{ii} + bE_{ij} + xE_{jj} + yE_{ji}$$

Lemma 6.2

Ist $ax - by \in R^\times$, so ist

$$E_{ij}(a, b, x, y) \in \mathrm{GL}_n(\mathbb{R})$$

Beweis. Folgt aus Folgerung 3.4, da

$$\det(E_{ij}(a, b, x, y)) = ax - by \in R^\times$$

Oder direkt: Das Inverse ist $E_{ij}(xc^{-1}, bc^{-1}, ac^{-1}, -yc^{-1})$, zum Beispiel

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix} \begin{pmatrix} xc^{-1} & -bc^{-1} \\ -yc^{-1} & ac^{-1} \end{pmatrix} = \begin{pmatrix} (ax - by)c^{-1} & 0 \\ 0 & (ax - by)c^{-1} \end{pmatrix}$$

□

▶ **Bemerkung 6.3**

Multiplikation von $E_{ij}(a, b, x, y)$ von links an A führt eine Zeilenumformung durch: Sind $a_1, ..., a_n$ die Zeilen von A, so wird a_i durch $aa_i + ba_j$ ersetzt, und gleichzeitig a_j durch $ya_i + xa_j$ ersetzt. Ist $ax - by = 1$, so sind diese Zeilenumformungen invertierbar.

Spezialfälle: elementare Zeilenumformungen von Typ II und III aus Kapitel III (LAAG 1). Warnung: Im Gegensatz dazu sind über einem Ring R die elementaren Zeilenumformungen vom Typ I (Multiplikation mit einem Skalar) nicht immer invertierbar!

Multiplikation mit $E_{ij}(a, b, x, y)$ von rechts führt entsprechende Spaltenumformungen durch.

Theorem 6.4 (Elementarteilersatz für Matrizen, Smith-Normalform)
Sei $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$. Es gibt $0 \leq r \leq \min\{n,m\}$, $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$ mit

$$SAT = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & \mathbb{0} \end{pmatrix}$$

$$\mathbb{0} \in \mathrm{Mat}_{m-r\times n-r}$$

wobei $d_i \in R\backslash\{0\}$ mit $d_i \mid d_{i+1}$ für $i = 1, ..., n-1$

Beweis. Induktion nach $\min\{m,n\}$. Für $a \in R$ sei $\delta(a) \in \mathbb{N}_0 \cup \{\infty\}$ die Anzahl der Primelemente in der Primfaktorzerlegung von a, mit $\delta(0) := \infty$, und $\delta(A) := \min_{ij}\{\delta(a_{ij})\}$. Wir können annehmen, dass $\delta(A) \leq \delta(SAT)$ für alle $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$. Durch Zeilen- und Spaltenvertauschungen erreichen wir, dass $\delta(a_{11}) = \delta(A)$.

- 1. Behauptung: $a_{11} \mid a_{i1}$ für alle i. Gäbe es ein $i \geq 1$ für dass $a_{11} \nmid a_{i1}$, so sei $c = \mathrm{ggT}(a_{11}, a_{i1}) = xa_{11} + ya_{i1}$ mit $\mathrm{ggT}(x,y) = 1$, also $ax - by = 1$ mit $a, b \in R$. Multiplikation mit $E_{1i}(x,y,a,b)$ von links erzeugt an der Position $(1,1)$ das Element c, und $\delta(c) < \delta(a_{11}) = \delta(A)$, im Widerspruch zur Minimalität von $\delta(A)$. Analog zeigt man, dass $a_{11} \mid a_{1j}$ für alle j. Durch Zeilen- und Spaltenumformungen können wir deshalb nun $a_{i1} = 0$ für alle $i > 1$ und a_{1j} für alle $j > 1$ erreichen.
- 2. Behauptung: $a_{11} \mid a_{ij}$ für alle i, j. Gäbe es $i > 1$ und $j > 1$ mit $a_{11} \nmid a_{ij} := b$, so können wir die j-te Spalte zur ersten Spalte addieren, was a_{11} nicht ändert und $a_{1i} = b$ bewirkt. Wider können wir Behauptung 1 anwenden und erhalten den Widerspruch, dass $a_{11} \mid b$. Damit ist nach diesem Umformungen

$$A = \begin{pmatrix} a_{11} & \\ & a_{11} \cdot A' \end{pmatrix}$$

mit $A' \in \mathrm{Mat}_{(m-1)\times(n-1)}(R)$. Wir wenden nun die Induktionshypothese auf A' an und sind fertig. □

Mathematica/WolframAlpha-Befehle (Smith-Normalform)
Elementarteiler einer Matrix A lassen sich mit Mathematica mit der Funktion

```
SmithDecomposition[A]
```

die als einziges Argument eine Matrix braucht. Allerdings ist der Output unformatiert, mit folgenden Befehl sieht das deutlich besser aus:

```
MatrixForm/@ ({u,r,v} = SmithDecomposition[A])
```

Der Output sind 3 Matrizen, wobei `u` für S, `v` für T und `r` für das Ergebnis von SAT steht.

▶ **Bemerkung 6.5**

Man kann zeigen, dass die $d_1, ..., d_r$ bis auf Assoziiertheit eindeutig bestimmt sind. Man nennt sie deshalb Elementarteiler der Matrix A.

■ **Beispiel 6.6**

Sei $R = \mathbb{Z}$. Die Elementarteiler von

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

sind

$$\begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix} \to \begin{pmatrix} 4 & 0 \\ 4 & 6 \end{pmatrix} \to \begin{pmatrix} 4 & 0 \\ -2 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & -6 \\ 4 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 4 & 12 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$$

2, 2 und 12.

Anmerkung (Teil 1)

Um die Elementarteiler der Matrix A_0 zu ermitteln, muss man geschickt mit Matrizen S und T multiplizieren. Dazu starten wir links oben bei Element $a_{11} \neq 0$ und versuchen nun, auf der ersten Spalte und auf der ersten Zeile nur Nullen zu produzieren, aber $a_{11} \neq 0$ zu erhalten.

Dazu fangen wir mit der ersten Spalte an. Ziel ist es, das letzte Element dieser Spalte durch geschickte Addition der vorletzten Spalte zu 0 werden zu lassen. Wir schauen uns die letzten 2 Elemente, nennen wir sie x und y, dieser ersten Spalte an und bestimmen $\mathrm{ggT}(x, y)$. Weiterhin suchen wir u und v, sodass folgende Gleichung erfüllt ist:

$$\mathrm{ggT}(x, y) = u \cdot x + v \cdot y$$

Da wir eine Zeilenoperation durchführen wollen, brauchen wir eine Matrix S_0, die wir von links an A ranmultiplizieren. Dabei müssen wir auf die richtige Dimension von S_0 aufpassen. Dazu setzen wir S_0 auf $\mathbb{1}_m$ und fügen an der richtigen Stelle die Matrix S_0' ein:

$$S_0' = \begin{pmatrix} u & v \\ -\frac{y}{\mathrm{ggT}(x,y)} & \frac{x}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

Jetzt bestimmen wir $A_1 := A_0 \cdot S_0$. Jetzt haben wir das letzte Element der ersten Spalte zu 0 verwandelt. Wir arbeiten uns jetzt in der ersten Spalte nach oben, versuchen also das vorletzte Element zu 0 zu verwandeln, aber mithilfe der vorvorletzten Zeile. Auch dazu bestimmen wir wieder Matrizen $S_1, S_2, ...$ bis die erste Spalte 0 ist, mit Ausnahme von a_{11}.

Anmerkung (Teil 2)
Jetzt wenden wir uns der ersten Zeile zu: Auch hier versuchen wir das letzte Element zu 0 zu verwandeln, aber eben mit Benutzung der vorletzten Spalte. Die Vorgehensweise ist nahezu identisch, wir bestimmen auch wieder $\mathrm{ggT}(x, y)$ und lösen

$$\mathrm{ggT}(x, y) = u \cdot x + v \cdot y$$

Damit bauen wir uns wieder T_0', die wir an der passenden Stelle in $T_0 = \mathbb{1}_n$ einsetzen

$$T_0' = \begin{pmatrix} u & -\frac{y}{\mathrm{ggT}(x,y)} \\ v & \frac{x}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

Die Matrix T_0 multiplizieren wir aber diesmal von rechts an A_n. So arbeiten wir uns wieder von hinten nach vorne. Es kann passieren, dass wir uns damit leider wieder in der ersten Spalte ein paar Nullen kaputt machen, aber dann bauen wir wieder eine S_n-Matrix mit der wieder Nullen erscheinen. Falls das wieder die Spalten kaputt macht, dann multiplizieren wir wieder mit einer T_n-Matrix. Das Theorem 6.4 garantiert uns, dass wir irgendwann fertig werden.

Anmerkung (Teil 3)
Haben wir nun die erste Zeile und die erste Spalte zu 0 verwandelt, außer a_{11} natürlich, kümmern wir uns um die Untermatrix in Richtung rechts unten. Hier geht der Algorithmus von vorne los; das Schöne ist, dass er uns die erste Zeile/Spalte nicht mehr kaputt machen kann. Irgendwann sind wir rechts unten angekommen und haben nur noch Elemente auf der Hauptdiagonalen stehen. Diese sollten, wie in Theorem 6.4 behauptet eine solche Teilerkette bilden. Tun sie das nicht, kann man wieder mit Matrizen S_n und T_n nachhelfen.

$$S_n' = \begin{pmatrix} u & v \\ -\frac{y}{\mathrm{ggT}(x,y)} & \frac{x}{\mathrm{ggT}(x,y)} \end{pmatrix} \quad T_n' = \begin{pmatrix} 1 & -\frac{vy}{\mathrm{ggT}(x,y)} \\ 1 & \frac{ux}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

$$\text{unter Vorbehalt! } S_n' = \begin{pmatrix} 1 & 1 \\ -\frac{vy}{\mathrm{ggT}(x,y)} & \frac{ux}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

Und dann sind wir endlich fertig! Die Transformationsmatrizen S und T sind dann einfach

$$S = S_1 \cdot S_2 \cdot \ldots$$
$$T = T_1 \cdot T_2 \cdot \ldots$$

Weitere Informationen und Beispiele findet man auf http://www.igt.uni-stuttgart.de/eiserm/lehre/2010/Algebra/Matrizenringe.pdf, ab Abschnitt §7D

Lemma 6.7
Ist M ein endlich erzeugter freier R-Modul und $N \subseteq M$ ein Untermodul, so ist auch N endlich erzeugt.

Beweis. Sei $(x_1, ..., x_m)$ eine Basis von M. Induktion nach m.
$\underline{m = 1:}$ Durch $1 \mapsto x_1$ wird nach Satz 1.11 eine R-lineare Abbildung $f : R \to M$ gegeben, die ein Isomorphismus ist. Der Untermodul $N \subseteq M$ entspricht einem Ideal $I := f^{-1}(N)$ von R. Da R ein Hauptidealring ist, ist $I = (a)$ für ein $a \in R$, somit $N = f(I) = R \cdot f(a)$. Insbesondere ist N endlich erzeugt, sogar von einem Element.
$\underline{m - 1 \to m:}$ Definiere $M' = \sum_{i=1}^{m-1} Rx_i$, $M'' = Rx_m$, $N' = N \cap M'$. Sei unter $\pi : M \to M''$ die R-lineare Abbildung gegeben nach Satz 1.11 durch $\pi(x_i) = \delta_{i,m} x_m$. Nach Induktionshypothese ist N' endlich erzeugt, etwa $N' = \sum_{j=1}^{n} Ry_j$. Aus dem Fall $m = 1$ sehen wir zudem, dass $N'' = \pi(N) = R\pi(y)$ für ein $y \in N$. Sei $\tilde{N} = Ry + \sum_{j=1}^{n} Ry_j \subseteq N$. Da $\mathrm{Ker}(\pi|_N) = M'' \cap N = N' \subseteq \tilde{N}$ und $\pi|_N(\tilde{N}) \supseteq R\pi(y) = N'' = \pi|_N(N)$ ist $\tilde{N} = N$ nach Lemma 5.5 und Satz 5.4. Somit ist N endlich erzeugt. □

Satz 6.8 (Elementarteilersatz für Moduln)
Sei R ein Hauptidealring, $M \cong R^m$ ein endlich erzeugter freier R-Modul, $N \subseteq M$ ein Untermodul. Dann existiert $r \in \mathbb{N}$, eine Basis $B' = (x'_1, ..., x'_m)$ von M und $d_1, ..., d_r \in R \backslash \{0\}$ mit $d_i \mid d_{i+1}$ für $i = 1, ..., r - 1$ für die $(d_1 x'_1, ..., d_r x'_r)$ eine Basis von N ist.

Beweis. Sei $B = (x_1, ..., x_m)$ eine Basis von M. Nach Lemma 6.7 ist N endlich erzeugt, also

$$N = \sum_{j=1}^{n} Ry_j \quad \text{mit} \quad y_j = \sum_{i=1}^{m} a_{ij} x_i \quad a_{ij} \in R$$

Wir betrachten die lineare Abbildung $f : R^n \to M$ gegeben durch $f(e_j) = y_j$. Dann ist $\mathrm{Im}(f) = N$ und

$$M_B^{\mathcal{E}}(f) = A = (a_{ij}) \in \mathrm{Mat}_{m \times n}(R)$$

Nach Theorem 6.4 existieren $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$ mit

$$SAT = D = \mathrm{diag}(d_1, ..., d_r, \mathbb{0})$$

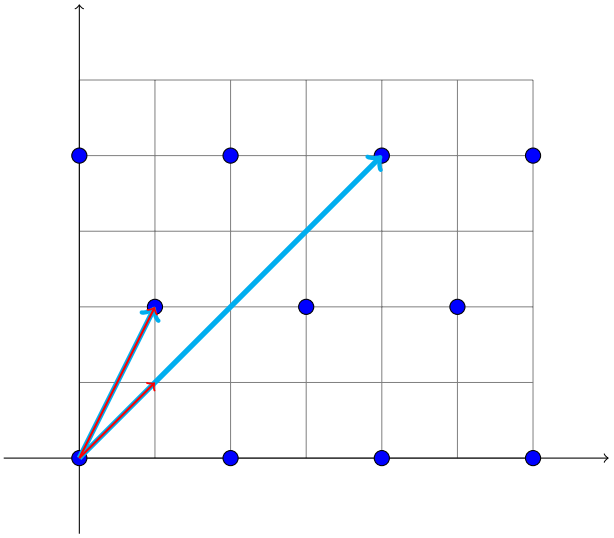
Es gibt somit Basen $\mathcal{E}' = (e'_1, ..., e'_n)$ von R^n, $B' = (x'_1, ..., x'_m)$ von M mit $M_{B'}^{\mathcal{E}'}(f) = D$. Somit ist $N = \mathrm{Im}(f) = \sum_{i=1}^{n} R \cdot f(e'_i) = \sum_{j=1}^{r} Rd_j x'_j$. Da $(x'_1, ..., x'_r)$ frei und R nullteilerfrei ist, ist auch $(d_1 x'_1, ..., d_r x'_r)$ frei, also eine Basis von N. □

■ **Beispiel**
Sei $R = \mathbb{Z}$, $M = \mathbb{Z}^2$, $N = \mathbb{Z}\begin{pmatrix}2\\0\end{pmatrix} + \mathbb{Z}\begin{pmatrix}1\\2\end{pmatrix}$

$$\begin{pmatrix}2 & 1\\0 & 2\end{pmatrix} \to \begin{pmatrix}1 & 2\\2 & 0\end{pmatrix} \to \begin{pmatrix}1 & 0\\2 & -4\end{pmatrix} \to \begin{pmatrix}1 & 0\\0 & 4\end{pmatrix}$$

$$\Rightarrow B = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\4\end{pmatrix}\right) \Rightarrow B' = \left(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right)$$

$$\Rightarrow C = \left(1 \cdot \begin{pmatrix}1\\2\end{pmatrix}, 4 \cdot \begin{pmatrix}1\\1\end{pmatrix}\right) \text{ ist Basis von } N$$



▶ **Bemerkung 6.9**
Wieder kann man zeigen, dass $d_1, ..., d_r$ bis auf Einheiten eindeutig bestimmt sind.

Folgerung 6.10
Ist R ein Hauptidealring, so ist ein Untermodul eines endlich erzeugten freien R-Moduls wieder frei.

▶ **Bemerkung 6.11**
Folgerung 6.10 wird falsch ohne "R Hauptidealring". So ist zum Beispiel $N = (x, y) \trianglelefteq \mathbb{Q}[x, y] = (\mathbb{Q}[x])[y] = R = M$ kein Hauptideal und somit ein nicht freier Untermodul des freien R-Moduls R: Je zwei Elemente von R sind linear abhängig, für $a, b \in R$ ist

$$b \cdot a + (-a) \cdot b = 0$$

Deshalb kann N keine Basis mit mehr als einem Element besitzen.

Die Voraussetzung "endlich erzeugt" ist hingegen nicht notwendig, aber der Beweis wird dadurch einfacher.

Folgerung 6.12
Ist R ein Hauptidealring, so ist ein Untermodul eines endlich erzeugten R-Moduls M wieder endlich erzeugt.

Beweis. Ist $M = \sum_{j=1}^{m} Ry_j$, so betrachte die R-lineare Abbildung $f : R^m \to M$ gegeben durch $f(e_j) = y_j$ für $j = 1, ..., m$. Nach Lemma 6.7 ist $f^{-1}(N) \subseteq R^m$ endlich erzeugt, etwa $f^{-1}(N) = \sum_{i=1}^{n} Rx_i$. Somit ist $N = f(f^{-1}(N)) = \sum_{i=1}^{n} R \cdot f(x_i)$ endlich erzeugt. □

Theorem 6.13 (Hauptsatz über endlich erzeugte Moduln über Hauptidealringen)
Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann ist

$$M = F \oplus M_{tor}$$

wobei $F \cong R^r$ ein endlich erzeugter freier R-Modul ist und

$$M_{tor} \cong \bigoplus_{i=1}^{n} {}^{R}/_{Rd_i}$$

mit Nichteinheiten $d_1, ..., d_n \in R\backslash\{0\}$, die $d_i \mid d_{i+1}$ für $i = 1, ..., n-1$ erfüllen.

Beweis. Sei $M = \sum_{j=1}^{m} Ry_j$. Betrachte die lineare Abbildung $f : R^m \to M$ gegeben durch $f(e_j) = y_j$ und dem Untermodul $N = \mathrm{Ker}(f) \subseteq R^m$. Nach Satz 6.8 existiert eine Basis $(x_1, ..., x_s)$ von R^m, $n \leq s$ und $d_1, ..., d_n \in R\backslash\{0\}$ mit $d_i \mid d_{i+1}$ für die $(d_1x_1, ..., d_nx_n)$ eine Basis von N ist. Nach dem Homomorphiesatz ist

$$\begin{aligned} M = \mathrm{Im}(f) &\cong {}^{R^m}/_{N} = \bigoplus_{i=1}^{s} Rx_i \Big/ \bigoplus_{i=1}^{n} Rd_ix_i \\ &\cong {}^{R^s}/\bigoplus_{i=1}^{n} Rd_ie_i \\ &\cong \bigoplus_{i=1}^{n} {}^{R}/_{Rd_i} \oplus \underbrace{R^{s-n}}_{F} \end{aligned}$$

Ist $d_i \in R^\times$, so ist ${}^{R}/_{Rd_i} = 0$, wir können diese i daher weglassen. Dabei ist $\bigoplus_{i=1}^{n} {}^{R}/_{Rd_i}$ genau der Torsionsmodul M_{tor}:

- "$\subseteq$": Mit $d := d_1 \cdot ... \cdot d_n \in R\backslash\{0\}$ ist $d \cdot (x_i)_{1,...,n} = (dx_i)_{1,...,n} = (0, ..., 0)$ (Vielfache von Rd_i machen das Element zu 0)
- "$\supseteq$": Ist $d \in R\backslash\{0\}$, $x \in \bigoplus_{i=1}^{n} {}^{R}/_{Rd_i}$, $y \in R^{s-n}$ mit $d \cdot (x, y) = 0$, so ist $d \cdot y = 0$ und deshalb $y = 0$. □

▶ **Bemerkung 6.14**
Auch hier sind $d_1, ..., d_n$ (bis auf Einheiten) sowie r eindeutig bestimmt. Man nennt r den (freien) Rang von M.

■ **Beispiel 6.15**

Eine endlich erzeugte abelsche Gruppe A ist von der Form

$$A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$$

mit (eindeutig bestimmten) $d_1, ..., d_k \in \mathbb{N}$, $d_1 \mid d_2 \mid ... \mid d_k$.

7. Zyklische Vektorräume

Sei K ein Körper, V ein n-dimensionaler K-Vektorraum, $f \in \mathrm{End}_K(V)$.

▶ **Bemerkung 7.1**
Wir betrachten V als $K[t]$-Modul mit $P(t) \cdot x = P(f)(x)$, vergleiche .
Erinnerung: V heißt f-zyklisch $\iff \exists x \in V$ mit $V = \mathrm{span}_K(x, f(x), f^2(x), ...)$. Ist k minimal mit $f^k(x) \in \mathrm{span}_K(x, f(x), f^2(x), ..., f^{k-1}(x))$, so ist $\underbrace{(x, ..., f^{k-1}(x))}_{B}$ eine Basis von V und $M_B(f) = M_{\chi_f}$.

Satz 7.2
Es gibt einen $K[t]$-Modul-Isomorphismus

$$V \cong \bigoplus_{i=1}^{m} {}^{K[t]}/_{(P_i)}$$

mit normierten Polynomen $P_1, ..., P_m \in K[t]$, die $P_i \mid P_{i+1}$ $\forall i$ erfüllen.

Beweis. Nach Theorem 6.13 ($K[t]$ Hauptidealring) ist

$$V \cong K[t]^r \oplus \bigoplus_{i=1}^{m} {}^{K[t]}/_{K[t] \cdot P_i}$$

mit $P_i \in K[t] \backslash K$, $P_i \mid P_{i+1}$ $\forall i$. Da $\dim_K(K[t]) = \infty > \dim_K(V)$ ist, ist $r = 0$, und wir können ohne Einschränkung P_i normiert annehmen. □

Lemma 7.3
Für $P \in K[t]$ sei $W := {}^{K[t]}/_{(P)}$. Durch $f_t(x) = \bar{t}x$ wird $f_t \in \mathrm{End}_K(W)$ definiert, wobei $\bar{t} = t + (P) = \pi_{(P)}(t) \in {}^{K[t]}/_{(P)}$. Genau dann ist $\varphi \in \mathrm{Hom}_K(V, W)$ ein $K[t]$-Modul-Homomorphismus, wenn $\varphi(f(x)) = f_t(\varphi(x))$ $\forall x \in V$.

Beweis.
- $f_t \in \mathrm{End}_K(W)$: klar
- Es gilt

$$\begin{aligned} \varphi \text{ ist } K[t]\text{-Modul-Homomorphismus} &\iff \varphi(ax) = a\varphi(x) \quad \forall a \in K[t], \forall x \in V \\ &\iff \varphi(tx) = t\varphi(x) \quad \forall x \in V \\ &\iff \varphi(f(x)) = f_t(\varphi(x)) \quad \forall x \in V \end{aligned}$$

□

Satz 7.4
Genau dann ist ${}^{K[t]}/_{(P)}$ (als $K[t]$-Modul), wenn V f-zyklisch ist. In diesem Fall ist

$$\chi_f = P_f = P$$

Beweis.
- Hinrichtung: Der K-Vektorraum $W = {}^{K[t]}/_{(P)}$ ist erzeugt von $1, \bar{t} = f_t(1), \bar{t}^2 = f_t^2(1), ...$, wobei

$\bar{t} = t + (P)$ und somit ist W f_t-zyklisch mit Basis $C = (1, \bar{t}, \bar{t}^2, ..., \bar{t}^{n-1})$, wobei $n = \deg(P)$. Auch ist $M_C(f_t) = M_P$. Ist $V \cong {}^{K[t]}/_{(P)}$ so ist dann V f-zyklisch.

- Rückrichtung: Ist umgekehrt V ein K-Vektorraum mit Basis $B = (x, f(x), ..., f^{n-1}(x))$, so ist $M_B(f) = M_P$ für $P = \chi_f$. Der K-Vektorraum-Homomorphismus $\varphi : V \to W = {}^{K[t]}/_{(P)}$ gegeben durch $\varphi(f^i(x)) = t^i$ ist dann ein $K[t]$-Modul-Isomorphismus.
- Ist $V \cong W$ als $K[t]$-Modul, so ist $\chi_f = \chi_{f_t}$, $P_f = P_{f_t}$. Aus $M_C(f_t) = M_P$ folgt somit

$$\chi_f = \chi_{f_t} = P$$

Ist $0 \neq Q \in K[t]$ mit $\deg(Q) < \deg(P)$, so ist

$$Q(f_t)(1) = Q(\bar{t}) \neq 0$$

da $Q \neq 0$ und C Basis, insbesondere $Q(f_t) \neq 0 \in \mathrm{End}_K({}^{K[t]}/_{(P)})$. Da $P_{f_t} \mid \chi_{f_t}$ gilt, folgt

$$P_f = P_{f_t} = \chi_{f_t} = P$$ □

Folgerung 7.5
V ist direkte Summe f-zyklischer Untervektorräume.

Folgerung 7.6
Es gilt

$$\chi_f \mid (P_f)^n$$

Insbesondere haben χ_f und P_f die selben irreduziblen Faktoren.

Beweis. In der Situation von Satz 7.2 ist

$$\chi_f = \prod_{i=1}^{m} P_i$$
$$P_f = \mathrm{kgV}(P_1, ..., P_m) = P_m$$

Da $P_i \mid P_m$ für alle i folgt $\chi_f \mid (P_m)^m$, insbesondere $\chi_f \mid (P_m)^n$, denn $m \leq n$. □

Folgerung 7.7 (Frobenius-Normalform)
Es gibt eine Basis B von V, für die

$$M_B(f) = \mathrm{diag}(M_{P_1}, ..., M_{P_m})$$

mit $P_1, ..., P_m \in K[t]$ normiert, die $P_i \mid P_{i+1}$ erfüllen.

► **Bemerkung 7.8**
Im Gegensatz zur Jordan-Normalform existiert die Frobenius-Normalform für beliebige Körper K und beliebige Endomorphismen f. Man kann zeigen, dass die Frobenius-Normalform eines Endomorphismus f eindeutig bestimmt ist.

Anhang

Anhang A: Listen

A.1. Liste der Theoreme

A.2. Liste der benannten Sätze, Lemmata und Folgerungen

A.3. Liste der Mathematica/WolframAlpha-Befehle

☺ für faule Mathematiker ☺