Skript zur Vorlesung

Lineare Algebra I

Wintersemester 2004/2005

Universität Konstanz

private Mitschrift

Stand: 16. April 2005
www.meidert.net/uni

Achtung:
Dies ist kein offizielles Script, sondern nur eine private Mitschrift. Ich kann daher keine Gewähr für die Richtigkeit und Vollständigkeit übernehmen. Vor allem können die Nummerierungen zum Teil von den in den Vorlesungen verwendeten abweichen. Falls jemand einen Fehler entdeckt, so möge er/sie mir bitte eine eMail schicken - vielen Dank!

Frieder Meidert (uni@meidert.net)

Inhaltsverzeichnis

1. Grundlagen

a. Mengen und Abbildungen

Definition 1.1. (Symbole der Aussagenlogik)
$\wedge$ - „und“
$\vee$ - „und/oder“
$\neg$ - „nicht“
$\forall$ - „für alle“
$\exists$ - „es existiert (mindestens) ein“
$\exists_1$ - „es existiert genau ein“
$\Rightarrow$ - „daraus folgt“
$\Leftrightarrow$ - „äquivalent“

Definition 1.2. (Mengen)
Eine Menge besteht aus Elementen und ist durch ihre Elemente bestimmt. Mengen gibt man an z.B. in aufzählender Form: $\{1, 2, 3\}$ oder $\{1, 2, 3, \ldots\}$; "$\ldots$" darf nur bei klarem Bildungsgesetz verwendet werden.
$\{x|\mathcal{P}(x)\}$ ist die Menge aller x, für die die Aussage $\mathcal{P}(x)$ gilt.

Wichtige Mengen:

$\mathbb{N} := \{1, 2, 3, \ldots\}$	natürliche Zahlen
$\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$	natürliche Zahlen mit Null
$\mathbb{Z} := \{x|x \in \mathbb{N}_0 \textit{ oder } -x \in \mathbb{N}\} = \{0, 1, -1, 2, -2, \ldots\}$	ganze Zahlen

In der Beschreibung von Mengen können Elemente mehrfach genannt werden, sie „zählen“aber nur einfach; es kommt auch nicht auf die Reihenfolge an:
$\{2, 1\} = \{1, 2\} = \{1, 2, 1, 2, 2\}$
Die Anzahl der (verschiedenen Elemente in einer Menge X heißt die **Mächtigkeit** (oder **Kardinalität**) von X; $|X|$.
Also $|\{1, 2\}| = 2 = |\{2, 1, 1\}|$.
Für uns ist:
$|X| \in \mathbb{N} \vee \{\infty\}$, wobei $|X| = \infty \Leftrightarrow \forall n \in \mathbb{N} |X| > n$.
$|X| = 0 \Leftrightarrow X = \{\} = \emptyset$, leere Menge.
Ist x Element der Menge X: $x \in X$
Ist x nicht Element der Menge X: $x \notin X$
Zwei Mengen X und Y heißen gleich, wenn $X = Y \Leftrightarrow$ es gilt $\forall x\ (x \in X \Leftrightarrow y \in Y)$.

Definition und Satz 1.3. *(neue Mengen aus alten)*
Seien $X_1, X_2, \ldots, X_n$, $n \in \mathbb{N}$ Mengen.

(i) *Vereinigung*
$X_1 \cup X_2 \cup X_3 \cup \ldots \cup X_n = \bigcup_{i=1}^{n} X_i = \{x | x \in X_1 \vee x \in X_2 \vee \ldots \vee x \in X_n\}$

(ii) *Durchschnitt*
$X_1 \cap X_2 \cap X_3 \cap \ldots \cap X_n = \bigcap_{i=1}^{n} X_i = \{x | x \in X_1 \wedge x \in X_2 \wedge \ldots \wedge x \in X_n\}$

(iii) *Produktmenge (kartesisches Produkt)*
$X_1 \times X_2 \times \ldots \times X_n = \prod_{i=1}^{n} X_i = \{(x_1, x_2, \ldots, x_n) | x_i \in X_i, i = 1, 2, \ldots, n\}$
Bemerkung: $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \Leftrightarrow x_i = y_i, (i = 1, 2, \ldots, n)$.

(iv) *Teilmenge*
X heißt Teilmenge von Y: $X \subset Y$ *(oder* $Y \supset X$*),*
$\forall x \, (x \in X \Rightarrow x \in Y)$
Hinweis: $X = Y$ *erlaubt.*

(v) *Komplement*
X, Y seien Mengen.
$X \setminus Y := \{x \in X | x \notin Y\}$ *(sprich " X ohne Y")*
Hinweis: $Y \subset X$ *ist nicht verlangt.*
Ist $Y \subset X$*, so ist* $X \setminus Y$ *das* ***Komplement*** *von Y in X.*

(vi) *Potenzmenge*
$\mathcal{P}(X)$ *der Menge X ist die Menge aller Teilmengen von X. Z.B.* $\mathcal{P}(\emptyset) = \{\emptyset\}$
$|\mathcal{P}(\emptyset)| = 1$
ist $|X| = n < \infty, n \in \mathbb{N}_0 \Rightarrow |\mathcal{P}(X)| = 2^n$

(vii) *Regeln:*
$X \cup Y = Y \cup X$
$(X \cup Y) \cup Z = X \cup (Y \cup Z) = X \cup Y \cup Z$
$(X \cap Y) \cap Z = X \cap (Y \cap Z) = X \cap Y \cap Z$
$(X_1 \times X_2) \cap (Y_1 \times Y_2) = (X_1 \cap Y_1) \times (X_2 \cap Y_2)$

Lemma 1.4.
Sind $M_1, M_2, \ldots, M_r$ *und* $N_1, N_2, \ldots, N_s$ *Mengen, dann gelten folgende* ***Distributivgesetze:***

(i) $\left(\bigcap\limits_{i=1}^{r} M_i\right) \cup \left(\bigcap\limits_{j=1}^{s} N_j\right) = \bigcap\limits_{i=1,\ldots,r\, j=1,\ldots,s} \left(M_i \cup N_j\right)$

(ii) $\left(\bigcup\limits_{i=1}^{r} M_i\right) \cap \left(\bigcup\limits_{j=1}^{s} N_j\right) = \bigcup\limits_{i=1,\ldots,r\, j=1,\ldots,s} \left(M_i \cap N_j\right)$

Beweis:
$X = Y \Leftrightarrow X \subset Y \wedge Y \subset X$

(i) (a) Schritt 1: "$\subset$"
Sei $x \in \left(\bigcap\limits_{i=1}^{r} M_i\right) \cup \left(\bigcap\limits_{j=1}^{s} N_j\right)$
Seien $i \in \{1, \ldots r\}$, $j \in \{1, \ldots s\}$ fest.
Zu zeigen: $x \in M_i \cup N_j$
Nach Voraussetzung ist $x \in \bigcap\limits_{k=1}^{r} M_k$ oder $x \in \bigcap_{l=1}^{s} N_l$
Im ersten Fall ist $x \in M_i$
im zweiten Fall $x \in N_j$

(b) Schritt 2: "$\supset$"
Sei $x \in \bigcap\limits_{i=1,\ldots,r\, j=1,\ldots,s} \left(M_i \cup N_j\right)$
1. Fall: $x \in \bigcap\limits_{i=1}^{r} M_i \Rightarrow$ fertig
2. Fall: $x \notin \bigcap\limits_{i=1}^{r} M_i$
d.h. es gibt ein i_0 mit $x \notin M_{i_0}$
Nach Voraussetzung ist $x \in M_{i_0} \cup N_j$ für jedes $j = 1, \ldots, s$
Wegen $x \notin M_{i_0} \Rightarrow x \in \bigcap\limits_{j=1}^{s} N_j \Rightarrow$ fertig

(ii) analog zu (i).

□

Definition 1.5. (Abbildungen)
X, Y seien Mengen. Eine Abbildung $f : X \to Y$ von X nach Y ist eine Vorschrift, die jedem $x \in X$ ein $y \in Y$ mit $f(x) = y$ zuordnet.
X: Definitionsmenge
Y: Zielmenge
Die Menge aller Abbildungen von X nach Y heißt $Abb(X, Y)$ oder Y^X.

Bemerkungen und Beispiele 1.6.

(i) Zwei Abbildungen $f : X \to Y$ und $f' : X' \to Y'$ heißen nur dann gleich, wenn $X = X'$, $Y = Y'$ und $f(x) = f'(x)\,\forall x \in X$ gilt.
$f : \mathbb{R} \to \mathbb{R}, f(x) := x^2$ ist nicht gleich $g : \mathbb{R} \to [0, \infty[:= \{x \in \mathbb{R} | x \geqq 0\}, g(x) := x^2$

(ii) Für jede Menge X hat man die Identität $id = id_X : X \to X$, die durch $id(x) = x\,(x \in X)$ definiert ist.
Allgemein: Hat man für jedes $Y \subset X$ die Inklusionsabbildung $\iota : Y \to X, \iota(y) := y\,(y \in Y)$

(iii) Die Abbildung $f : \{1, \ldots, n\} \to X$ identifiziert man oft mit Elementen von $X^n = X \times X \times \ldots \times X\,(n - mal)$, nämlich f mit $(f(1), \ldots, f(n))$.
Allgemein: Eine Abbildung $f : \mathbb{N} \to X$ identifiziert man oft mit unendlichen Folgen $(x_1, x_2, \ldots)$ in X

Definition 1.7. (Komposition)
Sind $f : X \to Y$ und $g : Y \to Z$ Abbildungen, so ist die Komposition $g \circ f : X \to Z$ definiert durch $g \circ f(x) := g(f(x))$
$f : X_1 \to X_2, g : Y_1 \to Y_2$ nur komponierbar, wenn $X_2 = Y_1$.
Es gilt:
$f : X \to Y; g : Y \to Z; h : Z \to W$, dann:
$(h \circ g) \circ f = h \circ (g \circ f)$, nämlich $x \mapsto h(g(f(x)))$.

Beispiel 1.8.
Sei $f : \mathbb{R} \cup \{\infty\} \to \mathbb{R} \cup \{\infty\}$ mit

$$f(x) := \begin{cases} -1 - \frac{1}{x} & \text{für } x \notin \{0, \infty\} \\ \infty & \text{für } x = 0 \\ -1 & \text{für } x = \infty \end{cases}$$

Dann gilt: $f \circ f \circ f = id$

Definition 1.9. (Bild, Urbild, Restriktion)

(i) Sei $f : X \to Y$ eine Abbildung.
Für $M \subset X$ heißt $f(M) := \{f(x) | x \in M\}$ das **Bild von** M **unter** f - $f(M) \subset Y$.

(ii) Für $N \subset Y$ heißt $f^{-1}(N) := \{x \in X | f(x) \in N\}$ das **Urbild von N unter f** - $f^{-1}(N) \subset X$.

(iii) Ist $M \subset X$, so heißt $f|_M : M \to Y, x \mapsto f(x)\,(x \in M)$ die **Restriktion von f auf M**.

Beispiel 1.10.
$f : \mathbb{R} \to \mathbb{R}, f(x) := x^2; f(\mathbb{R}) = [0, \infty[$.
Für $y \in \mathbb{R}$ ist $f^{-1}(y) = \begin{cases} \emptyset & , y < 0 \\ \sqrt{y}, -\sqrt{y} & , y \geqq 0 \end{cases}$.
$$|f^{-1}(\{y\})| = \begin{cases} 0 & , y < 0 \\ 1 & , y = 0 \\ 2 & , y > 0 \end{cases}.$$

Definition 1.11. (Graph)
Ist $f : X \to Y$, so heißt die Teilmenge $\Gamma_f := \{(x, f(x)) | x \in X\}$ von $X \times Y$ der Graph von f.
Beispiel:
$f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$.
$\Gamma_f = \{(x, x^2) | x \in \mathbb{R}\}$
Aus Γ_f gewinnt man f wieder zurück.

Definition 1.12. (injektiv, surjektiv, bijektiv)
Die Abbildung $f : X \to Y$ heißt

(i) injektiv, falls $|f^{-1}(\{y\})| \leqq 1 \; \forall y \in Y$

(ii) surjektiv, falls $|f^{-1}(\{y\})| \geqq 1 \; \forall y \in Y$

(iii) bijektiv, falls $|f^{-1}(\{y\})| = 1 \; \forall y \in Y$

Synonym: Injektion, Surjektion, Bijektion.

Definition 1.13. (Umkehrabbildung)
Sei $f : X \to Y$ eine bijektive Abbildung, dann heißt $f^{-1} : Y \to X$ mit $f^{-1}(y) := x \in \{x | f(x) = y, x \in X\}$ die **Umkehrabbildung von f**.

Es gilt:
$f^{-1} \circ f = id_X$; $f \circ f^{-1} = id_Y$ und $\left(f^{-1}\right)^{-1} = f$.

Vorsicht:
Notation f^{-1} für Urbild und für Umkehrabbildung; vgl. $f^{-1}(N)$ und $f^{-1}(y)$.

Definition 1.14. (Familien)
Vergleiche 1.6
Allgemein: Sei I eine beliebige Menge („Indexmenge"). Sei X eine Menge.
Abbildungen $x : I \to X$ werden auch als (mit I indizierte) **Familien** von Elementen in X bezeichnet.
Man schreibt x dann als ein „I-Tupel"($x = x_i | i \in I) = (x_i)_{i \in I}$ mit $x_i := x(i)$ $(i \in I)$.
I heißt Indexmenge dieser Familie.
$I = \emptyset$ ist erlaubt (man spricht dann von einer "leeren Familie").
Analog: Familien von anderen Objekten; z.B. gegeben für jedes $i \in I$ eine Menge X_i; dann ist $(X_i)_{i \in I}$ **Familie von Mengen**.
Beachte:
Mengen: keine Unterscheidung von Reihenfolgen und Wiederholungen.
Familien: Beachtung von Reihenfolgen und Wiederholungen.
z.B. $\{1,2,3,2,3\} = \{1,2,3,2,1\}$
aber: $(1,2,3,2,3) \neq (1,2,3,2,1)$

Bemerkung 1.15.
Einige mengentheoretische Operationen verallgemeinern sich von endlich auf beliebig viele Mengen:

(i) Ist $(X_i)_{i \in I}$ Familie von Mengen, so gilt:
$\bigcap\limits_{i \in I} = \{x | x \in X_i \, (i \in I)\}$
$\bigcup\limits_{i \in I} = \{x | \exists i \in I \; x \in X_i\}$

(ii) $\prod\limits_{i \in I} X_i := \{(x_i)_{i \in I} | \forall i \in I \; x_i \in X_i\}$

b. Gruppen

Definition 1.16. (Gruppe)
Eine **Gruppe** ist ein Paar $(G, \circ)$ aus einer Menge G und einer Abbildung $\circ : G\times G \to G, (x, y) \mapsto x \circ y$, so dass gilt:
(G1) $\circ$ ist assoziativ: $a, b, c \in G$: $(a \circ b) \circ c = a \circ (b \circ c)$.
(G2) es gibt ein neutrales Element $e \in G$ mit $\forall a \in G\ e \circ a = a$.
(G3) $\forall a \in G\ \exists a' \in G$ mit $a' \circ a = e$.
$a \circ b$ heißt das **Produkt** von a und b; e heißt **neutrales Element** von G; a' heißt ein zu a **inverses Element**.

Definition 1.17. (abelsche Gruppe)
Eine Gruppe $(G, \circ)$ heißt **abelsch** (oder **kommutativ**, falls $\circ$ kommutativ ist.
$\forall a, b \in G\ a \circ b = b \circ a$.

Lemma 1.18.
Gegeben: Gruppe $(G, \circ)$

(i) *Element e ist eindeutig bestimmt und es gilt* $a \circ e = e \circ a = a\ \forall a \in G$

(ii) *für jedes* $a \in G$ *ist das inverse Element* a' *eindeutig bestimmt,* $a' \circ a = a \circ a' = e$ $\forall a \in G$.

Beweis:
* Zeige Teil von (ii):
Sind $g, h \in G$ und $g \circ h = e$, so ist auch $h \circ g = e$ mit e neutrales Element.
Es gibt ein g' mit $g' \circ g = e$ und es folgt:
$h \circ g = e \circ (h \circ g) = (g' \circ g) \circ (h \circ g)$
$= g' \circ (g \circ (h \circ g)) = g' \circ ((g \circ h) \circ g)$ $\qquad (g \circ h = e)$
$= g' \circ (e \circ g) = g' \circ g = e.$ $\qquad (e \circ g = g)$

(i) Sei auch $\widetilde{e} \in G$ mit $\widetilde{e} \circ a = a\ \forall a \in G$.
Insbesondere $(a := e)$: $\widetilde{e} \circ e = e \Rightarrow e \circ \widetilde{e} = e.$ (mit (*))
Andererseits $e \circ \widetilde{e} = \widetilde{e}$ wegen e neutral $\Rightarrow \widetilde{e} = e$.
Sei $a \in G$. Dann $a \circ e = a \circ (a' \circ a) = (a \circ a') \circ a = e \circ a = a.$ (mit (*))

(ii) Sei $a \in G$, sei auch $\widetilde{a} \in G$ ein inverses Element von a, d.h. $\widetilde{a} \circ a = e$. Multipliziere dies mit a' von rechts:

$a' = e \circ a' = (\widetilde{a} \circ a) \circ a' = \widetilde{a} \circ (a \circ a') = \widetilde{a} \circ e = \widetilde{a}$. mit (i) (*)
Die letzte Aussage in (ii) folgt wieder aus (*).

□

Beispiele 1.19.

(i) $(\mathbb{R}, +)$ ist eine Gruppe: Neutrales Element ist $e = 0$, inverses Element zu $x \in \mathbb{R}$ ist $-x : (-x) + x = 0$.
$(\mathbb{R}, +)$ ist abelsch. Ebenso sind $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ abelsche Gruppen.

(ii) $\mathbb{R}^* := \mathbb{R} \setminus \{0\}; (\mathbb{R}^*, \cdot)$ ist eine abelsche Gruppe, mit neutralem Element $e = 1$, und zu $x \in \mathbb{R}^*$ inversem Element $\frac{1}{x}$.
Nebenbemerkung: $(\mathbb{R}, \cdot)$ ist keine Gruppe!
Ebenso: $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Q}^*_+, \cdot)$, $(\mathbb{R}^*_+ \cdot)$ sind abelsche Gruppen, wobei $\mathbb{R}^*_+ := \{x \in \mathbb{R} | x > 0\}$, usw.

(iii) Beispiele von nichtabelschen Gruppen:
Sei M eine Menge, sei $Sym\,(M)$ die Menge aller bijektiven Abbildungen $\sigma : M \to M$.
Behauptung: $(Sym\,(M)\,, \circ)$ ist eine Gruppe, wobei $\circ$ die Komposition von Abbildungen bedeute.
Beweis: Assoziativität gilt.
Neutrales Element: $\sigma = id_M$
Zu σ inverses Element: σ^{-1}, die Umkehrabbildung von σ. (Denn $\sigma^{-1} \circ \sigma = id$)
Die Gruppe $(Sym\,(M)\,, \circ)$ heißt die **symmetrische Gruppe** der Menge M. Ihre Elemente nennt man auch die **Permutationen** von M.
Ist $M = \{1, \ldots, n\}$ (mit $n \in \mathbb{N}$), so schreibt man $S_n := Sym\,(M)$.
Man schreibt $\sigma \in S_n$ symbolisch in der Form $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma\,(1) & \sigma\,(2) & \ldots & \sigma\,(n) \end{pmatrix}$
z.B.: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$

Satz 1.20.
Sei $n \in \mathbb{N}$.

(i) $|S_n| = n!$

(ii) *Ist $n \geqq 3$, so ist die Gruppe S_n nicht abelsch.*

Beweis:

(i) Abzählargument!

(ii) Betrachte folgende Permutationen:
$\sigma := \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$, $\tau := \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$
$\sigma \circ \tau\,(1) = 1$, aber $\tau \circ \sigma\,(1) = 3$: es ist also
$\sigma \circ \tau \neq \tau \circ \sigma$.

Konvention: Allgemeine Gruppen werden stets multiplikativ geschrieben. $(G, \cdot)$.
Den Multiplikationspunkt lässt man meist noch weg: $ab := a \cdot b$.
Neutrales Element: e;
zu $a \in G$ inverses Element: a^{-1} (statt bisher a'): $a \cdot a^{-1} = a^{-1} \cdot a = e$.

□

Lemma 1.21.
Sei G eine Gruppe, seinen $a, b \in G$.

(i) $\left(a^{-1}\right)^{-1} = a$

(ii) $(ab)^{-1} = b^{-1}a^{-1}$

Beweis:

(i) $a^{-1} \cdot a = e \Rightarrow a \cdot a^{-1} = e.$ (nach Lemma 1.18)

(ii) $(ab) \cdot \left(b^{-1}a^{-1}\right) = a\left(b\left(b^{-1}a^{-1}\right)\right) = a\left(e \cdot a^{-1}\right) = a \cdot a^{-1} = e$

□

Lemma 1.22.
Sei G eine Menge, sei $\cdot : G \times G \to G$ eine Abbildung. Genau dann ist $(G, \cdot)$ eine Gruppe, wenn $G \neq \emptyset$, das Assoziativgesetz (G1) gilt und gilt: $\forall a, b \in G$ gibt es genau ein $x \in G$ mit $a \cdot x = b$, und genau ein $y \in G$ mit $y \cdot a = b$.

Beweis:
"$\Rightarrow$": Sei $(G,\cdot)$ eine Gruppe. Dann ist $G \neq \emptyset$ (wegen $e \in G$). Seien $a, b \in G$.
Setze $x := a^{-1}b$, $y := ba^{-1}$, dann $ax = b$, $ya = b$.
Dies sind auch die einzigen Lösungen: ist etwa auch $a\widetilde{x} = b$, so gilt: $a^{-1}(a\widetilde{x}) = a^{-1}b$.
Analog für die zweite Gleichung.
"$\Leftarrow$: Sei $a \in G$, sei $e \in G$ die Lösung von $ae = a$. Sei auch $b \in G$, zeige: $e \cdot b = b$.
Denn $ab = (ae)\,b = a\,(eb)$.
Also folgt $b = eb$ (wegen eindeutiger Lösbarkeit von $ax = ab$)
Inverse Elemente: folgt aus Lösbarkeit von $y \cdot a = b$

□

Korollar 1.23.
Man darf Gleichungen kürzen.
Ist G eine Gruppe, so gilt für $a, x, y \in G$:
$ax = ay \Rightarrow x = y$
$xa = ya \Rightarrow x = y$

□

Vorsicht: *Aus $ax = ya$ folgt im Allgemeinen **nicht** $x = y$!*

Satz 1.24.
Sei G eine Gruppe, seien $x_1, \ldots, x_n \in G\,(n \in \mathbb{N})$. Dann ist das Produkt $x_1 \cdot \ldots \cdot x_n$ von der Klammerung unabhängig.
Beispiel: $(x_1x_2)\,x_3 = x_1\,(x_2x_3)$

Beweis: (vollständige Induktion nach n)
$n \leqq 3$: klar. (G1)
Sei $n > 3$, sei Aussage für weniger als n Faktoren schon bewiesen. Seien g, h zwei Klammerungen des Produkts $x_1 \cdot \ldots \cdot x_n$. Betrachte die Klammern auf der äußersten Ebene: dann gibt es Indizes $1 \leqq i, j \leqq n$ mit $g = (x_1 \cdot \ldots \cdot x_i)\,(x_{i+1} \cdot \ldots \cdot x_n)$ und $h = \left(x_1 \cdot \ldots \cdot x_j\right)\left(x_{j+1} \cdot \ldots \cdot x_n\right)$ (mit jeweils individueller Klammerung der inneren Produkte). Nach Induktionsvoraussetzung sind diese inneren Produkte von deren Klammerung unabhängig.
Fall 1: $i = j \Rightarrow$ fertig.
Fall 2: $i \neq j$, sei ohne Einschränkung der Allgemeinheit $i < j$. Dann
$g = (x_1 \cdot \ldots \cdot x_i)\left(\left(x_{i+1} \cdot \ldots \cdot x_j\right)\left(x_{j+1} \cdot \ldots \cdot x_n\right)\right)$
$h = \left((x_1 \cdot \ldots \cdot x_i)\left(x_{i+1} \cdot \ldots \cdot x_j\right)\right)\left(x_{j+1} \cdot \ldots \cdot x_n\right)$
$\Rightarrow g = h$

□

Definition 1.25.

Sei G eine Gruppe. Für $a \in G$ und $n \in \mathbb{Z}$ schreibe $a^n := \begin{cases} \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n-mal} & n \geqq 1 \\ e & n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{(-n)-mal} & n \leqq 1 \end{cases}$

Satz 1.26.
$a^m \cdot a^n = a^{m+n}$ für alle $m, n \in \mathbb{Z}, \forall a \in G$.

Bemerkung 1.27.
$\cdot, \circ, +, *, \ldots$: mögliche Symbole für Gruppenprodukt.
$+$ verwendet man **nur** bei abelschen Gruppen.
Ist $(G, +)$ eine additiv geschriebene (abelsche) Gruppe, so heißt das neutrale Element 0, das zu $x \in G$ inverse Element heißt $-x$. Auch schreibt man $n \cdot a := a + a + \ldots + a$ (a-mal) (statt a^n).

$(G, \cdot)$	$(G, +)$
allgemeine Gruppe	abelsche Gruppe
ab	$a + b$
a^{-1}	$-a$
$e\,(oder 1)$	0
$\left(a^{-1}\right)^{-1} = a$	$-(-a) = a$
a^n	na

Definition 1.28. (Untergruppe)
Sei G eine Gruppe. Eine Teilmenge H von G heißt eine **Untergruppe** von G, wenn gilt:

(i) $\forall h_1, h_2 \in H$: $h_1 h_2 \in H$

(ii) $(H, \cdot)$ ist eine Gruppe. ($\leftarrow$ H mit der Multiplikation $H \times H \to H, (h_1, h_2 \mapsto h_1 h_2)$

Man schreibt dafür $H \leqq G$.

Satz 1.29.
G sei eine Gruppe, $H \subset G$ eine Teilmenge. Dann:
$H \leqq G \Leftrightarrow$ es gelten

(i) $H \neq \emptyset$

(ii) $\forall a, b \in H : ab^{-1} \in H$

Beweis:
Sei e das neutrale Element von G. Sei $H \leqq G$: Sei $\widetilde{e}$ das neutrale Element von H. Gilt $\widetilde{e}\widetilde{e} = \widetilde{e}$ und $e\widetilde{e} = \widetilde{e} \Rightarrow$ (Kürzen, 2.8) $\widetilde{e} = e$. Sei $h \in H$, sei h^{-1} das inverse Element von h in G und h' das inverse Element von h in H. Habe $h^{-1}h = e = \widetilde{e} = h'h \Rightarrow h^{-1} = h'$.
Beweis von (ii) nun klar, also "$\Rightarrow$" gezeigt.
Umgekehrt sei $H \subset G$, $H \neq \emptyset$, mit (ii). Starte auf einem $h \in H$. Nach (ii) ist $hh' = e \in H$. Also $(H, \cdot)$ ein neutrales Element, nämlich e. Sei $b \in H$ beliebig. Anwenden von (ii) mit $a := e$ zeigt, dass auch $b^{-1} \in H$. Es ist $H \cdot H \subset H$: für $h_1, h_2 \in H$ ist $h_1 h_2 = h_1 \left(h_2^{-1}\right)^{-1} \in H$. Also $H \leqq G$.

□

Korollar 1.30.
Sei G eine Gruppe, $(H_i)_{i\in I}$ eine Familie von Untergruppen in G. Dann ist auch $\bigcap\limits_{i\in I} H_i$ eine Untergruppe von G.

Beweis:
Verwende 2.14: Wir wissen $e = e_G \in H_i \; \forall i$ (siehe letzter Beweis). Also $e \in \bigcap\limits_{i\in I} H_i$, somit $\bigcap\limits_{i\in I} H_i \neq \emptyset$, somit klar: $\forall a, b \in \bigcap\limits_{i\in I} H_i$ ist $ab^{-1} \in \bigcap\limits_{i\in I} H_i$.

□

Definition 1.31.
Sei G eine Gruppe, sei X eine Teilmenge von G. Dann heißt
$\langle X \rangle := \bigcap \{H : H \subset G \text{ ist Untergruppe von } G \text{ mit } X \subset H\}$
die von X **erzeugte Untergruppe** von G.
NB: $\langle X \rangle$ ist **die** kleinste Untergruppe, welche X enthält.

Bemerkungen und Beispiele 1.32.

(i) $\{e\}$ ist Untergruppe von G, die sogenannte **triviale Untergruppe**.

(ii) Untergruppenrelation ist transitiv:
$H \leqq G \wedge K \leqq H \Rightarrow K \leqq G$.

(iii) $\mathbb{Z} \leqq \mathbb{Q} \leqq \mathbb{R} \leqq \mathbb{C}$: Kette von Untergruppen bezüglich der Addition.

(iv) $\mathbb{Q}^*_+ \leqq \mathbb{Q}^* \leqq \mathbb{R}^*$ sind Untergruppen bezüglich der Multiplikation. ($\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$)

(v) Für $g \in G$ ist $\langle g \rangle := \langle \{g\} \rangle = \{g^n | n \in \mathbb{Z}\}$. (nach 2.11). Solche Untergruppen heißen **zyklische Untergruppen**.

(vi) Beispiel: $G = (\mathbb{Z}, +)$. Für $n \in \mathbb{Z}$ ist $\langle n \rangle = \mathbb{Z} \cdot n = \{kn | k \in \mathbb{Z}\}$.
Dabei gilt für $m, n \in \mathbb{Z}$:
$\mathbb{Z}m \subset \mathbb{Z}n \Leftrightarrow n|m$ („n teilt m“).

c. Ringe und Körper

Definition 1.33. (Ringe)
Ein **Ring** ist ein Tripel $(A, +, \cdot)$ aus einer Menge A und zwei Abbildungen $+, \cdot : A \times A \to A$ mit folgenden Eigenschaften:
(R1) $(A, +)$ ist eine abelsche Gruppe
(R2) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \forall a, b, c \in A$
(R3a) $a \cdot (b + c) = a \cdot b + b \cdot c \ \forall a, b, c \in A$
(R3b) $(a + b) \cdot c = a \cdot c + b \cdot c \ \forall a, b, c \in A$
Der Ring heißt kommutativ, wenn
(R4) $a \cdot b = b \cdot a \ \forall a, b \in A$

Bemerkung 1.34.

(i) $\cdot$ bindet stärker als $+$, den Malpunkt lässt man oft weg.

(ii) Das neutrale Element bezüglich der Addition schreibt man als 0, das bezüglich der Addition zu $\in A$ Inverse mit $-a$.

(iii) Meist verlangt man auch:
(R5) $\exists\, 1 \in A\ (\forall a \in A\ 1 \cdot a = a \cdot 1 = a)$
Mann spricht dann von einem **Ring mit Eins**.
Für $n \in \mathbb{Z}$ schreibt man dann einfach $n := n \cdot 1$ in A.

Beispiel 1.35.

(i) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit 1.

(ii) $A = \{0\}$ (mit $+, \cdot$ in der einzig möglichen Weise) ist ein Ring mit Eins ($1 = 0$), der **Nullring**.

(iii) Für $n \in \mathbb{N}$ ist $(\mathbb{Z}n, +, \cdot)$ ein „kommutativer Ring“ ohne Eins, falls $n > 1$.

Satz 1.36. *(Division mit Rest)*
Sei $a, b \in \mathbb{Z}$. Dann gibt es $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leqq r < |b|$.
Dadurch sind q und r sind eindeutig bestimmt.

Beweis:
Sei $b > 0$ (ohne Einschränkung der Allgemeinheit).
$q := \lfloor \frac{a}{b} \rfloor := max\{k \in \mathbb{Z} | k \leqq \frac{a}{b}\}$
$0 \leqq \frac{a}{b} - q < 1$
$0 \leqq a - bq < b$
Eindeutigkeit: ist $a = qb + r = q'b + r'$ mit $0 \leqq r, r' < |b|, q, q' \in \mathbb{Z}$
$(q - q')b = r' - r$ (Element $\{0, 1, \ldots, |b| - 1\}$

□

Beispiel 1.37.
Sei $n \in \mathbb{N}$ fest. Definiere den Ring $\mathbb{Z}/\mathbb{Z}n$:
Für $a \in \mathbb{Z}$ sei $\overline{a} := a + \mathbb{Z}n = \{a + kn | k \in \mathbb{Z}\}$ (eine Teilmenge von $\mathbb{Z}$). Für $a, b \in \mathbb{Z} : \overline{a} = \overline{b} \Leftrightarrow n | a - b$ (also etwa $\overline{0} = \overline{n} = \overline{2n} = \ldots$). Definiere $\mathbb{Z}/\mathbb{Z}n := \{\overline{a} | a \in \mathbb{Z}\}$ (als Menge).
Es ist also $|\mathbb{Z}/\mathbb{Z}n| = n$. Definition von $+ : (\mathbb{Z}/\mathbb{Z}n) \times (\mathbb{Z}/\mathbb{Z}n) \to \mathbb{Z}/\mathbb{Z}n$.
Seien $a, b \in \mathbb{Z}$. Um $\overline{a}$ und $\overline{b}$ zu addieren, definieren wir: $\overline{a} + \overline{b} := \overline{a + b}$. Wohldefiniertheit zu zeigen!
Ist $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$, so $a_2 = a_1 + k_1 n, b_2 = b_1 + k_2 n$ mit $k_1, k_2 \in \mathbb{Z} \Rightarrow a_2 + b_2 = a_1 + b_1 + (k_1 + k_2)n$.
Analog: $\overline{a} \cdot \overline{b} := \overline{ab}$; Wohldefiniertheit analog.

Wir sehen: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1.

Bemerkungen 1.38.

(i) Ist A ein Ring mit Eins, so ist die Eins eindeutig bestimmt.

(ii) $a \cdot 0 = 0 \cdot a = 0$ $(a \in A)$
$-(ab) = (-a)b = a(-b) = -ab$ $(a \in A)$

(iii) In einem Ring ist jedes $x_1 \cdot x_2 \cdot \ldots \cdot x_n$ von der Klammerung unabhängig. (Beweis siehe Gruppen)

Definition 1.39. (Körper)

(i) Ein Ring mit Eins $(K, +, \cdot)$ heißt ein **Schiefkörper**, wenn $1 \neq 0$, und gilt:
(SK) $\forall a \in K \setminus \{0\} \exists b \in K \; ba = 1$.

(ii) Ein **Körper** ist ein kommutativer Schiefkörper (d.h. mit (R4)).
Die Bedingung $1 \neq 0$ schließt nur den Nullring aus, denn in jedem anderen Ring mit Eins ist $1 \neq 0$.

Satz 1.40.
Ein Ring mit Eins ist genau dann ein Schiefkörper, wenn
(*) $K^* := K \setminus \{0\}$ *ist eine Gruppe bezüglich der Multiplikation.*

Beweis:
Sei K ein Schiefkörper, dann ist K nullteilerfrei:
$0 = xy$, sei $x \neq 0 \Rightarrow \exists z \in K \; (zx)y = 1 \cdot y = y$ (SK)
Also $\cdot : K^* \times K^* \to K^*$. $\Rightarrow (K^*, \cdot)$ ist eine Gruppe.
Umgekehrt: Ist $(K^*, \cdot)$ eine Gruppe, so folgt (*) aus der Existenz von inversen Elementen in dieser Gruppe.

□

Bemerkung 1.41.
(*) aus 1.40 impliziert:
$\forall x, y \in K \; (xy = 0 \Rightarrow x = 0 \vee y = 0)$.
Ein Ring mit dieser Eigenschaft heißt **nullteilerfrei**.
(Beispiel: $A = \mathbb{Z}/6\mathbb{Z} : \overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$)

Beispiele 1.42. (Körper)

(i) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper.

(ii) Ist K ein Körper (kommutativ!), so schreibe auch $\frac{1}{a} := a^{-1}$ $(a \in K*)$, und $\frac{a}{b} := a^{-1}b = ba^{-1}$.

(iii) Aus Analysis: $(\mathbb{C}, +, \cdot)$, Körper der komplexen Zahlen.
Man kann $\mathbb{C}$ definieren als $\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$ mit
$(a_1, b_1) + (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$,
$(a_1, b_a \cdot (a_2, b_2) := a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$.
$(0, 1) =: i$; $i^2 = -1$.

(iv) Sei $d \in N$, sei $\mathbb{Q}[\sqrt{d}] := \{a + b \cdot \sqrt{d} : a, b \in \mathbb{Q}\}(\sqrt{d} \in \mathbb{R})$
$(\mathbb{Q}[\sqrt{d}], +, \cdot)$ ist ein kommutativer Ring mit 1.
$(\mathbb{Q}[\sqrt{d}], +, \cdot)$ ist sogar ein Körper: Sei $x = a + b\sqrt{d} \neq 0$, sei $\sqrt{d} \notin \mathbb{Q}$
$\frac{1}{x} = \frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{a-b\sqrt{d}}{a^2-b^2d} \in \mathbb{Q}[\sqrt{d}]$.
Dabei ist Erweiterung erlaubt, da $a - b\sqrt{d} \neq 0$.

Lemma 1.43.
Für $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{Z}$ ist $\sqrt{d} \notin \mathbb{Q}$.

Beweis:
Benutze Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen:
Annahme: $\sqrt{d} = \frac{x}{y}; x, y \in \mathbb{N}$
$\Rightarrow dy^2 = x^2$: jeder Primfaktor kommt gerade oft vor in d.
$\Rightarrow \sqrt{d} \in \mathbb{N}$, Widerspruch.

□

Satz 1.44.
Für jede Primzahl p ist $\mathbb{F}_p := \mathbb{Z}/\mathbb{Z}_p$ ein Körper.
Erinnerung: $\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$.

Beweis:
$\mathbb{F}_p$ ist nullteilerfrei: Seien $m, n \in \mathbb{Z}$ mit $\overline{m}, \overline{n} \neq 0$ in $\mathbb{F}_p \Rightarrow \overline{m} \cdot \overline{n} = \overline{mn} \neq 0$, denn $\overline{m}, \overline{n} \neq 0$ sagt: m, n nicht durch p teilbar; also auch ihr Produkt nicht durch p teilbar. □

Lemma 1.45.
Jeder endliche nullteilerfreie Ring K ist ein Schiefkörper.

Beweis:
Sei $a \in K, a \neq 0$. Die Abbildung $m_a : K \setminus \{0\} \to K \setminus \{0\}, m_a(x) := xa$ ist wohldefiniert wegen K nullteilerfrei.
Sie ist injektiv: $m_a(x) = m_a(y) \Rightarrow xa = ya$
$\Rightarrow (x - y)a = 0 \Rightarrow x - y = 0$ (da nullteilerfrei)
Abbildung ist surjektiv, da $K \setminus \{0\}$ und injektiv.
Insbesondere: $\exists x \in K \setminus \{0\}$ mit $xa = 1$.

□

Beispiel 1.46.
Sei etwa $p = 7$,

Inverse?

a	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\frac{1}{a}$	$\overline{1}$	$\overline{4}$	$\overline{5}$	$\overline{2}$	$\overline{3}$	$\overline{6}$

Definition 1.47. (Charakteristik)
K sei ein Körper. Die **Charakteristik** von K ist

$$char(K) := \begin{cases} 0 & \text{, falls } n \neq 0 \text{ in } K \\ min\{n \in \mathbb{N} : n = 0 \text{in } K\} & \text{, ansonsten} \end{cases}$$

Bemerkung 1.48.

(i) $\mathbb{Q}, \mathbb{R}, \mathbb{Q}[\sqrt{d}], \mathbb{C}$ alle Charakteristik 0.

(ii) Ist $(K, \leqq)$ ein angeordneter Körper (s. Analysis I), so ist $char(K) = 0$.
Denn $1 \geqq 0$. Wäre $n = n \cdot 1 = 0$ mit $n \in \mathbb{N}$, so $n - 1 = -1$ in $K \rightarrow$ Widerspruch.

(iii) $char(\mathbb{F}_p) = p$, p Primzahl.

Satz 1.49.
K ein Körper. Ist $char(K) \neq 0$, so ist $char(K)$ eine Primzahl.

Beweis:
Sei $char(K) = m \cdot n$ mit $m, n > 1$
$\Rightarrow m \cdot n = 0$ in $K \Rightarrow m = 0 \wedge n = 0$ in $K \rightarrow$ Widerspruch zu Definition (da Körper nullteilerfrei).

□

Definition 1.50. (Teilring, Teilkörper)
Sei A ein Ring mit Eins. Eine Teilmenge B von A heißt ein **Teilring** von A, falls B unter $+$ und $\cdot$ in A abgeschlossen ist und falls $(B, +, \cdot)$ ein Ring ist und $1 \in B$ ist.
Ist $(B, +, \cdot)$ ein Körper, so heißt B auch ein **Teilkörper** von A.

Beispiele 1.51.

(i) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}[\sqrt{d}] \subset \mathbb{R} \subset \mathbb{C}$ Kette von Unterringen.

(ii) $\mathbb{Z}/\mathbb{Z}n$ ist **kein** Unterring von $\mathbb{Z}$!

2. Vektorräume

a. Erste Definitionen

Im folgenden stets: K ist ein Körper.
(z.B. $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p, \ldots$)

Definition 2.1. (Vektorraum)
Ein K-**Vektorraum** (K-VR) ist eine Menge V mit Abbildungen $+ : V \times V \to V$, $\cdot : K \times V \to V$, so dass gelten:
(VR1) $(V, +)$ ist abelsche Gruppe,
(VR2) $\forall a, b \in K, \forall v, w \in V$: $(a + b)v = av + bv$, $a(v + w) = av + aw$.
(VR3) $\forall a, b \in K, \forall v \in V$: $a(bv) = (ab)v$
(VR4) $\forall v \in V$: $1 \cdot v = v$

Bemerkungen 2.2.
Den Malpunkt lässt man meist weg.
Die Null in $(V, +)$ wird (vorerst) mit $\underline{0}$ bezeichnet (Nullvektor).
Die Elemente von V nennt man „Vektoren";
die Elemente von K nennt man „Skalare".

Lemma 2.3.
Sei V ein K-VR.
Seien $a \in K, v \in V$.

(i) $av = \underline{0} \Leftrightarrow a = 0 \vee v = \underline{0}$.

(ii) $(-a)v = -(av) = a(-v)$.

Beweis:

(i) $av = \underline{0}, a \neq 0 \Rightarrow$
$v = 1v = (a^{-1}a)v = a^{-1}(av) = \underline{0}$.
$\Leftarrow$: $a \cdot 0 = a(\underline{0} + \underline{0}) = a \cdot \underline{0} + a \cdot \underline{0} \Rightarrow a \cdot \underline{0} = 0$.
Analog $0 \cdot v = \underline{0}$.

(ii) analog

□

Beispiele 2.4.

(i) $V = \{\underline{0}\}$, der Nullverktorraum.

(ii) $V = K^n = \{(x_1, \dots, x_n) | x_1, \dots, x_n \in K\}$ mit komponentenweise definierter Addition und Multiplikation.
$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$
$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n)$
$\underline{0} = (0, \dots, 0)$
Für $K = \mathbb{R}$: $n = 1$: Gerade; $n = 2$: Ebene; $n = 3$: Raum; usw.

(iii) Sei X Menge, $V := Abb(X, K)$ ist K-VR bezüglich „punktweiser" Definition von Addition und Multiplikation:
$f, g \in V, x \in K$:
$(f + g)(x) := f(x) + g(x)$, $(a \cdot f)(x) := a \cdot f(x)$ mit $c \in X$
(Spezialfall $X = \{1, \dots, n\}$ ist das vorige Beispiel!)

(iv) $\mathbb{R}$ ist ein $\mathbb{Q}$-VR (mit der normalen Definition von $\cdot$).
Allgemeiner: Ist L ein Teilkörper des Körpers K, und ist V ein K-VR, so können wir V auch als L-VR auffassen (Skalarmultiplikation $L \times V \to V$ definiert als Restriktion von $K \times V \to V$).

(v) Sei $(V_i)_{i \in I}$ eine Familie von K-Vektorräumen, dann ist $\prod\limits_{i \in I} V_i = \{(v_i)_{i \in I} : \forall i \in I, v_i \in V\}$ ein K-VR, wenn $+$ und $\cdot$ komponentenweise definiert werden.
Er heißt das **direkte Produkt** der $V_i (i \in I)$.
Ist $I = \{1, \dots, n\}$, so schreibe auch:
$V_1 \times \dots \times V_n$ für $\prod\limits_{i=1}^{n} V_i$.
(Beispiel: $K^n = K \times \dots \times K$)
Beispiel: $K^{\mathbb{N}} = \prod\limits_{i \in \mathbb{N}} K = \{(x_1, x_2, x_3, \dots) | x_i \in K (i \in \mathbb{N})\}$ der VR aller unendlichen Folgen in K

Definition 2.5. (Untervektorraum)
Sei V ein K-VR. Ein (K-)**Untervektorraum** von V (kurz: UR von V) ist eine Teilmenge U von V mit:
(UR1) $(U, +)$ ist Untergruppe von $(V, +)$
(UR2) $\forall a \in K, \forall u \in U$ ist $au \in U$.

Gilt (UR1) und (UR2), ist $(U, +, \cdot)$ selbst ein K-VR.

Lemma 2.6.
Sei V ein K-VR, sei $U \subset V$ eine Teilmenge.
Genau dann ist U ein UR von V, wenn gelten:
(UR1) $\neq \emptyset$
(UR2) $\forall x, y \in U \; x + y \in U$
(UR3) $\forall x \in U \; \forall a \in K \; ax \in U$.

Beweis:
U UR $\Rightarrow$ es gelten (UR1, UR2, UR3)
Umgekehrt gelte (UR1, UR2, UR3):
Für $x, y \in U$ ist $x - y = x + (-1) \cdot y$ (nach 1.3)
$\Leftrightarrow x - y \in U$, wegen (UR2) und (UR3).
Nach Kriterium für Untergruppen: U ist Untergruppe von $(U, +)$.

□

Satz 2.7.
Ist $(U_i)_{i \in I}$ Familie von Unterräumen von V, so ist auch $\bigcap_{i \in I} U_i$ ein UR von V.

Beispiele 2.8.

(i) Für jeden UR U von V ist $\underline{0} \in U$. $U = \{\underline{0}\}$ ist ein UR von V, der kleinste UR.

(ii) VRe und URe kommen überall in der Analysis vor:
z.B. sei $C^n(\mathbb{R}, \mathbb{R}) := \{f \in Abb(\mathbb{R}, \mathbb{R}) | f \text{n-mal stetig differenzierbar}\}$ $(n = 0, 1, 2, \ldots)$, dann ist
$\ldots \subset C^2(\mathbb{R}, \mathbb{R}) \subset C^1(\mathbb{R}, \mathbb{R}) \subset C^0(\mathbb{R}, \mathbb{R}) \subset Abb(\mathbb{R}, \mathbb{R})$.
In $V = \mathbb{R}^{\mathbb{N}}$ hat man z.B. den UR aller konvergenten Folgen, oder den UR der summierbaren Folgen, oder ...

(iii) Sei $V = K^n$, dann ist $U = \{x \in K^n | a_1 x_1 + \ldots + a_n x_n = 0\}$ für jede Wahl von $a_1, \ldots, a_n \in K$ ein UR von V.
Werden bald sehen: jeder UR von K^n ist Durchschnitt von höchstens n solchen UR.

(iv) Sei $V = K^{\mathbb{N}}$ = VR aller unendlichen Folgen $(x_1, x_2, \ldots)$ in K.
Dann ist $U := \{x = (x_1, x_2, \ldots) | \exists n_0 \in \mathbb{N} \forall n \geqq n_0 \; x_n = 0\}$ ein UR von V

b. Lineare Abhängigkeit, Basis, Dimension

Definition 2.9.
Sei V ein VR, sei $\mathcal{F} = (v_i)_{i\in I}$ eine Familie mit $v_i \in V$ $(i \in I)$.

(i) Ein Vektor $v \in V$ heißt eine **Linearkombination** von $\mathcal{F}$, wenn es endlich viele Indizes $i_1, \dots, i_n \in I$ und $a_1, \dots, a_n \in K$ mit $v = a_1 v_{i_1} + \dots + a_n v_{i_n}$ gibt.

(ii) Die Menge aller Linearkobinationen von $\mathcal{F}$ wird mit $span_K(\mathcal{F}) = span(\mathcal{F})$ bezeichnet.

(iii) Ist $M \subset V$ eine Teilmenge von V, so heißt $v \in V$ **Linearkombination** von M, falls v Linearkombination von $(x)_{x\in M}$ ist, d.h. falls $v = a_1 x_1 + \dots + a_n x_n$ mit $a_1, \dots a_n \in K$, $x_1, \dots, x_n \in M$ $(n \in M)$. Definiere $span_K(M) = span(M)$ analog.

Bemerkungen 2.10.

(i) $v = \underline{0}$ ist stets LK von $\mathcal{F}$, auch für $I = \emptyset$ (leere Familie).

(ii) $V = K^n$, dann ist jedes $x \in K^n$ LK von $e_1, \dots, e_n$, wobei
$e_i := (0, \dots, 0, 1, 0, \dots, 0) \in K^n$ $(i = 1, \dots n)$. (1 an der i-ten Stelle)
$x = \sum\limits_{i=1}^{n} x_i e_i$. also $span(e_1, \dots, e_n) = K^n$.

(iii) Sei I Menge, sei $\mathcal{P}$ eine Eigenschaft, die für jedes $i \in I$ entweder wahr oder falsch ist. Man sagt, dass $\mathcal{P}$ **für fast alle** $i \in I$ gilt, falls $\{i \in I | \text{ nicht } \mathcal{P}(i)\}$ endlich ist. (Abkürzung: f.f.a. $i \in I$)
Ist $(x_i)_{i\in I}$ eine Familie von Vektoren in V und ist $x_i = \underline{0}$ f.f.a. $i \in I$, so ist $\sum\limits_{i\in I} x_i \in V$ wohldefiniert (auch wenn $|I| = \infty$ ist).
Daher schreibt man LKen formal als unendliche Summen:
$span(v_i | i \in I) = \{\sum\limits_{i\in I} a_i v_i | a_i \in K, a_i = 0 \text{ f.f.a. } i \in I\}$.

Definition und Satz 2.11.
Für jede Teilmenge M von V ist $span_k(M)$ ein K-UR von V. Er heißt der von M ***aufgespannte*** *(oder* ***erzeugte****) UR.*

Beweis:
$\sum\limits_{x \in M} a_x x + \sum\limits_{x \in M} b_x x = \sum x \in M(a_x + b_x)x$
analog mit Skalarmultiplikation.
Dies zeigt (UR2), (UR3).

□

Beispiele 2.12.

(i) Sei $M \subset V$ eine Teilmenge. Dann ist $span_K(M)$ der kleinste K-VR von V, der M enthält:
$span_K(M) = \bigcap\{U | U \text{ist UR von} V \text{mit} M \subset U\}$

(ii) $span(\emptyset) = \{\underline{0}\}$, $span(v) = Kv := \{av | a \in K\}$.

(iii) $M_1 \subset M_2 \Rightarrow span(M_1) \subset span(M_2)$.

(iv) Sei $V = K^3$, $v_1 = (2, 1, -3)$, $v_2 = (0, -2, 2)$, $v_3 = (1, -1, 0)$.
Dann ist $span(v_1, v_2, v_3) = \{x = (x_1, x_2, x_3) \in K^3 | x_1 + x_2 + x_3 = 0\}$.
$\subset$: OK
$\supset$: Sei $x \in K^3$ mit $x_1 + x_2 + x_3 = 0$, dann ist $x = -x_3 v_1 - x_3 v_2 + (x_3 - x_2)v_3$.

Lemma 2.13.
Sind $M_1, M_2 \subset V$ mit $M_2 \subset span(M_1)$, so ist $span(M_1 \cup M_2) = span(M_1)$.

Beweis:
Klar. (siehe 2.9 und 2.11) □

Definition 2.14.
Ein K-VR V heißt **endlich erzeugt**, falls es eine endliche Menge $M \subset V$ gibt mit $V = span_K(M)$.

Definition 2.15. (lineare Abhängigkeit)

(i) Eine endliche Familie $(v_1, \dots, v_n)$ in V heißt **linear abhängig** (über K), wenn es $a_1, \dots, a_n \in K$ mit $a_i \neq 0$ für mindestens ein i mit $\sum\limits_{i=1}^{n} a_i v_i = \underline{0}$ gibt.

(ii) Eine beliebige Familie $(v_i)_{i\in I}$ in V heißt **linear abhängig**, falls $\exists$ endliche Teilmenge $J \subset I$ existiert, so dass $(v_j)_{j\in J}$ linear abhängig ist.

(iii) Eine Familie heißt **linear unabhängig**, wenn sie nicht linear abhängig ist.

Bemerkungen 2.16.

(i) Eine Familie ist linear abhängig, wenn der Nullvektor nichttrivial darstellbar ist.

(ii) Die leere Familie ist linear unabhängig.

(iii) Eine Familie (v) der Länge 1 ist genau dann linear abhängig, wenn $v = \underline{0}$.

(iv) Eine Familie (v, w) der Länge 2 ist genau dann linear abhängig, wenn $v \in Kw$ oder $w \in Kv$.

(v) $V = \mathbb{R}^3$, $K = \mathbb{R}$: Zwei Vektoren $x, y \in \mathbb{R}^3$ sind genau dann linear abhängig, wenn $\underline{0}, x, y$ auf einer Geraden liegen; drei Vektoren $x, y, z \in \mathbb{R}^3$ sind genau dann linear abhängig, wenn $\underline{0}, x, y, z$ in einer Ebene liegen.

(vi) (v_1, v_2, v_3) aus Bsp. 2.12 sind linear abhängig.

Satz 2.17.
Sei $(v_i)_{i\in I}$ in V. Äquivalent:

(i) *$(v_i)_{i\in I}$ ist linear abhängig.*

(ii) *aus $\sum\limits_{i\in I} a_i v_i = \sum\limits_{i\in I} b_i v_i$ ($a_i, b_i \in K, a_i = b_i = 0$ f.f.a $i \in I$) folgt $a_i = b_i\ \forall i \in I$.*

Satz 2.18.
Eine Familie $(v_i)_{i\in I}$ ist genau dann linear abhängig, wenn einer ihrer Vektoren durch die anderen ausgedrückt werden kann.
$(v_i)_{i\in I}$ ist linear abhängig $\Leftrightarrow \exists j \in I\ v_j \in span(v_i | i \in I \setminus \{j\})$

Beweis:
$\Rightarrow$: Ist $(v_i)_{i\in I}$ linear abhängig: $\sum\limits_{i\in I} a_i v_i = \underline{0}$ mit $a_i \in K$, $a_i = 0$ f.f.a. $i \in I$, $a_j \neq 0$ für ein $j \in I \Rightarrow v_j = -\sum\limits_{i\in I\setminus\{j\}} \frac{a_i}{a_j} v_i$
$\Leftarrow$: $v_j = \sum\limits_{i\in I} a_i v_i \Rightarrow \underline{0} = 1v_j - \sum\limits_{i\in I\setminus\{j\}} a_i v_i$.

□

Definition 2.19. (Basis)
Eine Familie $\mathcal{B} = (v_i)_{i\in I}$ in V heißt eine **Basis** des K-VRs V, wenn $span(\mathcal{B}) = V$ und $\mathcal{B}$ linear unabhängig über K ist.

Satz 2.20.
$\mathcal{B}$ ist Basis von $V \Leftrightarrow$ jedes $v \in V$ ist in eindeutiger Weise LK von $\mathcal{B}$.

Beispiele 2.21.

(i) $V = \{\underline{0}\}$ hat eine Basis, nämlich die leere Familie.

(ii) $V = K^n$ hat z.B. die Basis $(e_1, \ldots, e_n)$, mit $e_i = \underbrace{(0, \ldots, 1, \ldots, 0)}_{\text{1 an der i-ten Stelle}}$.

Es gibt auch viele andere Basen. z.B. $(v_1, \ldots, v_n)$ mit $v_i = e_1 + \ldots + e_i$ ($i = \{1, 2, \ldots, i\}$)

(iii) Ist $(v_1, v_2, \ldots v_n)$ eine Basis von V, so ist auch jede Permutation $(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$ mit $\sigma \in S_n$.

(iv) Fassen wir $\mathbb{C}$ als $\mathbb{R}$-VR auf, so ist $(1, i)$ ($i = \sqrt{-1}$) eine $\mathbb{R}$-Basis von $\mathbb{C}$. Über $\mathbb{C}$ ist dies keine Basis, denn $\mathbb{C}$ ist linear abhängig: $i \cdot 1 - 1 \cdot i = 0$.
Konzept der Basis hängt also vom Grundkörper ab!

Definition 2.22. (Notation - disjunkte Vereinigung)

(i) Seien I, J Mengen. Mit $I \sqcup J := (I \times \{1\}) \cup (J \times \{2\})$ wird die **disjunkte Vereinigung** von I und J bezeichnet. Man identifiziert dabei meist wieder $i \in I$ mit $(i, 1) \in I \sqcup J$ und $j \in J$ mit $(j, 2) \in I \sqcup J$.

(ii) Seien $\mathcal{F} = (v_i)_{i\in I}$, $\mathcal{G} = (w_j)_{j\in J}$ Familien (von Vektoren).

Dann heißt die Familie $\mathcal{F} \sqcup \mathcal{G} := (z_k)_{k\in I\sqcup J}$ mit $z_k := \begin{cases} v_i & \text{, falls } k = (i,1) \\ w_j & \text{, falls } k = (j,2) \end{cases}$ die **Aneinanderhängung** von $\mathcal{F}$ und $\mathcal{G}$.

Beispiel 2.23.
Ist $\mathcal{F} = (v_1, \dots v_m)$, $\mathcal{G} = (w_1, \dots, w_n)$, so $\mathcal{F} \sqcup \mathcal{G} = (v_1, \dots, v_m, w_1, \dots w_n)$.

Satz 2.24. *(Basis)*
V ein VR, $\mathcal{F} = (v_i)_{i\in I}$ eine Familie mit $(v_i) \in V$. Äquivalente Aussagen:

(i) *$\mathcal{F}$ ist Basis von V,*

(ii) *$\mathcal{F}$ ist ein **minimales Erzeugendensystem** von V, d.h. $span(\mathcal{F}) = V$, aber $span(v_i|i \in I \setminus \{j\}) \neq V$ für jedes $j \in I$.*

(iii) *$\mathcal{F}$ ist eine **maximale linear unabhängige** Familie in V, d.h. $\mathcal{F}$ ist linear unabhängig, aber für jedes $v \in V$ ist $\mathcal{F} \sqcup (v)$ linear abhängig.*

Beweis:
(i) $\Rightarrow$ (ii):
Sei $\mathcal{F}$ Basis, sei $j \in I$.
Behauptung: $v_j \notin span(v_i|i \in I \setminus \{j\})$. Dann wäre $v_j = \sum\limits_{i\in I, i\neq j} a_i v_i$ (mit $a_i \in K$, $a_i = 0$ f.f.a. i),
so $\underline{0} = -1 \cdot v_j + \sum\limits_{i\in I, i\neq j} a_i v_i$. $\rightarrow$ Widerspruch zu $\mathcal{F}$ ist linear unabhängig.
(ii) $\Rightarrow$ (iii):
Wäre $\mathcal{F}$ linear abhängig, so $v_j \in span(v_i|i \in I, i \neq j)$ für ein $j \in I$. (2.10) Es folgt $span(v_i|i \neq j) = span(v_i|i \in I) = V \rightarrow$ Widerspruch zu $\mathcal{F}$ minimales Erzeugendensystem. Für $v \in V$ ist $v \in span(\mathcal{F})$, also $\mathcal{F} \sqcup (v)$ linear abhängig nach 2.10.
(iii) $\Rightarrow$ (i):
Zu zeigen: $span(\mathcal{F}) = V$.
Angenommen: es gebe $v \in V$ mit $v \notin span(\mathcal{F})$.
Behauptung: Dann ist auch die Familie $\mathcal{F} \sqcup (v)$ linear unabhängig. (dann Widerspruch zu (iii))
Sei also $\underline{0} = \sum\limits_{i\in I} a_i v_i + av$ $(a_i, a \in K, f.f.a. a_i = 0)$.
Wäre $a \neq 0$, so $v = -\sum\limits_{i\in I} \frac{a_i}{a} v_i \in span(\mathcal{F})$, $\Rightarrow$ Widerspruch.
Also $a = 0$, $\Rightarrow$ alle $a_i = 0$ wegen $\mathcal{F}$ linear unabhängig.

□

Bemerkung 2.25.
Ist $\mathcal{F}$ eine linear unabhängige Familie in V, so gilt für alle $v \in V$: $\mathcal{F} \sqcup (v)$ ist linear abhängig genau dann, wenn $v \in span(\mathcal{F})$ (Beweis siehe (iii) $\Rightarrow$ (i) in 2.24)

Satz 2.26. *(Basisergänzungssatz)*
Jede linear unabhängige Familie $\mathcal{F}$ in V lässt sich zu einer Basis von V ergänzen, d.h. es gibt eine Familie $\mathcal{G}$ in V, so dass $\mathcal{F} \sqcup \mathcal{G}$ Basis von V ist.

Beweis: (von 2.26)
Sei zunächst V endlich erzeugt, etwa $V = span(v_1, \dots, v_n)$.
Ist $v_i \in span(\mathcal{F})$ für alle $i = 1, \dots, n$, so $span(\mathcal{F}) = V$, also $\mathcal{F}$ ist Basis, $\rightarrow$ fertig.
Sonst gibt es $i \in \{1, \dots, n\}$ mit $v_i \notin span(\mathcal{F})$. Dann ist auch $\mathcal{F}_1 = \mathcal{F} \sqcup (v_i$ linear unabhängig (2.16). Nun wiederhole das Argument mit $\mathcal{F}_1$ usw. Spätestens nach n Schritten ist die erhaltene Familie eine Basis von V.

□

Ist V nicht endlich erzeugt, so muss man dieses Argument „transfinit„ oft wiederholen. Dazu braucht man stärkere Axiome der Mengenlehre:
Auswahlaxiom bzw. **Zorn'sches Lemma**. Wir werden diesen Beweis nicht geben.

Auswahlaxiom:
X_i seien Mengen mit $i \in I$.
$X_i \neq \emptyset$
$\Rightarrow \prod\limits_{i \in I} X_i \neq \emptyset$.

$\mathcal{F} = (v_i)_{i \in I}$ eine Familie $\Rightarrow$ Länge von $\mathcal{F}$ ist definiert als $|\mathcal{F}| := |I|$.

Korollar 2.27.
Jeder VR hat eine Basis!

Beweis:
(Nimm $\mathcal{F}$:= leere Familie in 2.26)

□

Lemma 2.28.
Sei V (endlich erzeugter) VR, sei $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V. Sei $w = \sum\limits_{i=1}^{n} a_i v_i \in V$, mit $a_i \in K$.
Ist $j \in \{1, \dots, n\}$ mit $a_j \neq 0$, so ist auch $(v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_n)$ eine Basis von V.

Beweis:
$v_j = w - \sum_{i=1, i \neq j}^{n} \frac{a_i}{a_j} v_i \in span(\mathcal{B}') \Rightarrow span(\mathcal{B}') \supset span(\mathcal{B}) = V.$
Lineare Unabhängigkeit von $\mathcal{B}'$:
Sei $bw + \sum_{i=1, i \neq j}^{n} c_i v_i = \underline{0}$ mit $b, c_i \in K (i \neq j)$.
Setze Definition von w ein $\rightsquigarrow$
$b \sum_{i=1}^{n} a_i v_i + \sum_{i=1, i \neq j}^{n} c_i v_i = \underline{0}$
Wegen $\mathcal{B}$ linear unabhängig, verschwindet insbesondere der Koeffizient von v_j; dieser ist $ba_j = 0 \Rightarrow b = 0 \Rightarrow$ alle $b_i = 0$ OK. □

Satz 2.29. *(Austauschsatz von Steinitz, 1871-1928)*
Sei $\mathcal{B} = (v_1, \ldots v_n)$ eine (endliche) Basis von V, sei $(w_1, \ldots, w_r)$ eine linear unabhängige Familie. Dann ist $r \leqq n$. Weiter gibt es r paarweise verschiedene Indizes $i_1, \ldots, i_r \in \{1, \ldots, n\}$, so dass die aus $\mathcal{B}$ durch Austausch von v_{i_k} gegen $w_k (k = 1, \ldots, r)$ entstehende Familie wieder eine Basis von V ist.

Beweis: (Induktion nach r)
$r = 0$: nichts zu tun!
$r = 1$: $w_1 \neq 0$, da linear unabhängig: benutze Lemma 2.20.
Schritt von $r - 1$ nach r:
Wende die Induktionsannahme auf die Familie $(w_1, \ldots, w_{r-1})$ an. Es folgt $r - 1 \leqq n$ und nach Umnummerierung (der v_i):
$(w_1, \ldots, w_{r-1}, v_r, \ldots v_n)$ ist Basis von V.
Habe $w_r = \sum_{i=1}^{r-1} a_i w_i + \sum_{j=r}^{n} b_j v_j$ $(a_i, b_j \in K)$. Wegen $(w_1, \ldots, w_r)$ linear unabhängig, ist $b_j \neq 0$ für ein $j \in \{r, \ldots, n\}$. $(\Rightarrow r \leqq n)$.
Lemma 2.28 $\Rightarrow$ man kann v_j durch w_r ersetzen und erhält wieder eine Basis.
□

Satz 2.30. *(Basisauswahlsatz)*
V ein VR, sei $(v_i | i \in I)$ ein Erzeugendensystem. Dann existiert eine Teilmenge $J \subset I$, so dass $(v_i | i \in J)$ eine Basis von V ist.

Beweis:
Ist I endlich:
Fall 1: ist bereits Basis, dann OK
Fall 2: ein v_i weglassen - dann OK oder Schritt 2 wiederholen; fertig nach endlich vielen Schritten.
$|I| = \infty$: hierzu benötigt man wieder das Zorn'sche Lemma.
□

Korollar 2.31.
Je zwei Basen von V haben dieselbe Länge ($\in \mathbb{N}_0 \cup \{\infty\}$).

Beweis:
Sei V endlich erzeugt, dann hat V eine endliche Basis $\mathcal{B}$ wegen 2.22.
Ist $\mathcal{B}'$ eine weitere Basis, so ist $|\mathcal{B}'| \leqq |\mathcal{B}|$ nach 2.21. Ebenso gilt dann (durch Vertauschen der Rollen von $\mathcal{B}$ und $\mathcal{B}'$): $|\mathcal{B}| \leqq |\mathcal{B}'|$.
Sei V unendlich erzeugt dann kann es keine endliche Basis geben ...

□

Definition 2.32. (Dimension)
Sei V ein (K-)VR. Die (K-)**Dimension** von V ist

$$\dim(V) := \dim_K(V) := \begin{cases} |\mathcal{B}| & \text{, für Basis von } V \text{ ist endlich erzeugt} \\ \infty & \text{, für Basis von } V \text{ ist nicht endlich erzeugt} \end{cases}$$

Bemerkungen 2.33.

(a) $\dim(V) = 0 \Leftrightarrow V = \{\underline{0}\}$

(b) $\dim(K^n) = n$ ($n \in \mathbb{N}$)

(c) $\dim_K(V) < \infty \Leftrightarrow V$ ist endlich erzeugt
Sage daher in Zukunft **endlich dimensional** statt endlich erzeugt.

(d) $\dim_K(V) = max\{|\mathcal{F}| : \mathcal{F}$ ist K-linear unabhängige Familie in $V\}$

Grund: 2.24

ebenso: $\dim_K(V) = min\{|\mathcal{F}| : \mathcal{F}$ ist Familie in V mit $span_K(\mathcal{F}) = V\}$
(wieder nach 2.24)

(e) Sei $V = K^{\mathbb{N}} = \prod_{n\in\mathbb{N}} K = \{(x_1, x_2, x_3, \dots) : x_i \in K (i \in \mathbb{N})\}$
In V ist die Familie $(e_i)_{i\in\mathbb{N}}$, mit $e_i = \underbrace{(0, \dots, 0, 1, 0, \dots)}_{\text{1 an der Stelle } i}$, linear unabhängig.

$\sum_{i\in\mathbb{N}} a_i e_i = (a_1, a_2, \dots)$ ($a_i = 0$ f.f.a. $i \in \mathbb{N}$) $\Rightarrow \dim(V) = \infty$.
Aber $(e_i)_{i\in\mathbb{N}}$ ist keine Basis, denn

$span(e_i : i \in \mathbb{N}) = \{(x_1, x_2, \ldots) : x_i = 0 f.f.a. i \in \mathbb{N}\}$
z.B. $(1, 1, 1, \ldots) \notin span(e_i : i \in \mathbb{N})$.

(f) Die Dimension von V hängt vom Grundkörper ab!
z.B. ist $\dim_{\mathbb{R}}(\mathbb{C}) = 2$, aber $\dim_{\mathbb{C}}(\mathbb{C}) = 1$

Korollar 2.34.
Sei $\dim(V) = n < \infty$, *sei* $\mathcal{F} = (v_1, v_2, \ldots, v_n)$ *eine Familie der Länge* n *in* V. *Dann ist äquivalent:*

$\mathcal{F}$ *ist eine Basis* $\Leftrightarrow$ $\mathcal{F}$ *ist linear unabhängig* $\Leftrightarrow$ $span(\mathcal{F}) = V$.

Beweis:
Sei $\mathcal{F}$ linear unabhängig. Wäre $\mathcal{F}$ keine Basis, so gäbe es ein $w \in V$ mit $\mathcal{F}_1 = \mathcal{F} \sqcup (w)$ linear unabhängig; $|\mathcal{F}| = n + 1 < \dim(V) \rightarrow$ Widerspruch zu 2.25 (d)
Analog: sei $span(\mathcal{F}) = V$. Wäre $\mathcal{F}$ keine Basis, so könnte man das Erzeugendensystem $\mathcal{F}$ verkürzen; $\rightarrow$ Widerspruch 2.33 (d)

□

Korollar 2.34 wird falsch, wenn man $\dim(V) = \infty$ zulässt: Beispiel 2.33 (e)

Korollar 2.35.
Sei V *ein VR,* U *ein UR von* V.

(i) $\dim(U) \leqq \dim(V)$.

(ii) ist $\dim(U) = \dim(V) < \infty$, *so gilt* $U = V$.

Beweis:

(i) Klar, z.B. mit 2.17

(ii) aus 2.26: Sei $\mathcal{F} = (u_1, \ldots, u_n)$ Basis von U.
$\Rightarrow \mathcal{F}$ ist linear unabhängig in $V \Rightarrow \mathcal{F}$ Basis von V, da $|\mathcal{F}| = \dim(U) = \dim(V)$.
$\Rightarrow U = V$.

□

Wieder ist (b) (im Allgemeinen) falsch, falls $\dim(V) = \dim(U) = \infty$: z.B. 2.33 (e).

Beispiele 2.36.
Die $\mathbb{R}$-URe von $\mathbb{R}^2$ sind $U = \{0\}$, $U = \mathbb{R}^2$ und alle Geraden durch $(0,0)$: $U = \mathbb{R}(u_1, u_2)$ für $(u_1, u_2) \neq (0,0)$.
Die URe von $\mathbb{R}^3$ sind $\{0\}$, $\mathbb{R}^3$, die Geraden durch den Ursprung und die Ebenen durch den Ursprung.

Wir unterscheiden ab jetzt den Nullvektor nicht mehr in der Notation und schreiben einfach 0 *dafür.*

c. Summen von Unterräumen

(Stets: K ein Körper, alle VRe sind K-VRe)

Definition 2.37.
Sei V ein VR, seien $U_1, \ldots, U_n$ URe von V.
Man nennt $\sum\limits_{i=1}^{n} U_i = U_1 + \ldots + U_n := span\left(\bigcup\limits_{i=1}^{n} U_i\right)$ die Summe der URe $U_1, \ldots, U_n$; dies ist selbst ein UR von V.

Lemma 2.38.
$\sum\limits_{i=1}^{n} U_i = \{\sum\limits_{i=1}^{n} u_i | u_i \in U_i \text{ für } i = 1, \ldots, n\}$.

Beweis:
Nach Definition besteht $\sum\limits_{i=1}^{n} U_i$ aus allen Linearkombinationen $\sum\limits_{j=1}^{n} a_j x_j$ mit $a_j \in K$ und $x_1, \ldots, x_m \in \bigcup\limits_{i=1}^{n} U_i$.
Jeder solche Ausdruck hat die Form $\sum\limits_{i=1}^{n} u_i$ mit $u_i \in U_i$ (Zusammenfassen von Elementen im selben U_i)

□

Bemerkung 2.39.
Definition 2.37 und Lemma 2.38 übertragen sich auf beliebige Familien $(U_i)_{i\in I}$ von URe: man definiert $\sum\limits_{i\in I} U_i := span\left(\bigcup\limits_{i\in I} U_i\right)$ und hat $\sum\limits_{i\in I} U_i = \{\sum\limits_{i\in I} u_i | u_i \in U_i, u_i = 0 \text{ f.f.a. } i \in I\}$.

Beispiel 2.40.

(i) Für jede Familie $(v_i)_{i\in I}$ in V ist $span(v_i | i \in I) = \sum\limits_{i\in I} Kv_i$. Insbesondere $span(v_1, \ldots, v_n) = Kv_1 + \ldots + Kv_n$.

(ii) $V = \mathbb{R}^3$: sind U_1, U_2 Geraden durch $(0,0)$, dann ist $U_1 + U_2 =$ die von beiden aufgespannte Ebene (falls $U_1 \neq U_2$).
Ist U_1 eine Gerade, U_2 eine Ebene, und $U_1 \not\subset U_2$, so gilt $U_1 + U_2 = \mathbb{R}^3$.

Satz 2.41.
Sei $(U_i)_{i\in I}$ eine Familie von URen von V. Dann ist äquivalent:

(i) jedes $v \in \sum\limits_{i\in I} U_i$ hat eindeutige Summendarstellung $v = \sum\limits_{i\in I} u_i$ mit $u_i \in U_i$, $u_i = 0$ f.f.a. $i \in I$.

(ii) $\forall j \in I\ U_j \cap \sum\limits_{i\in I, i\neq j} U_i = \{0\}$.

Beweis:
(i) $\Rightarrow$ (ii):
Sei $j \in I$, sei $v \in U_j \cap \sum\limits_{i\neq j} U_i$, etwa $v = \sum\limits_{i\neq j} u_i$ mit $u_i \in U_i$. Also $0 = \underbrace{-v}_{\in U_j} + \sum\limits_{i\neq j} u_i \Rightarrow \underbrace{v = 0}_{(i)}$

(ii) $\Rightarrow$ (i):
Ist $\sum u_i = \sum' u_i'$ (mit $u_i, u_i' \in U_i\ \forall i \in I$), so $0 = \sum\limits_i (u_i - u_i')$. Also genügt es, die Eindeutigkeit in (i) für den Nullvektor zu zeigen. Sei also $0 = \sum\limits_{i\in I} u_i$ mit $u_i \in U_i$, $u_i = 0$ f.f.a. $i \in I$; für festes $i \in I$:
$u_i = -\sum\limits_{j\neq i} u_j \in \left(\sum\limits_{j\neq i} U_j\right) \cap U_i = \{0\} \Rightarrow u_i = 0.$

$\square$

Definition 2.42. (interne direkte Summe)
Sind die Bedingungen aus 2.41 erfüllt, so heißt die Summe $\sum\limits_{i\in I} U_i$ **direkt**, in Zeichen $\bigoplus\limits_{i\in I} U_i$. Mann nennt $\bigoplus\limits_{i\in I} U_i$ auch die (**interne**) **direkte Summe** der U_i.

Korollar 2.43.
Seien U_1, U_2 URe von V. Genau dann ist die Summe $U_1 + U_2$ direkt, wenn $U_1 \cap U_2 = \{0\}$ ist. (2.41)

Satz 2.44. *(komplementärer UR)*
*Zu jedem UR von V gibt es einen UR W von V mit $V = U \oplus W$. Jedes solche W heißt **ein zu** U **komlementärer UR von** V.*

Beweis:
Sei $(u_i)_{i\in I}$ eine Basis von U. Ergänze sie zu einer Basis $(u_i)_{i\in I} \sqcup (w_j)_{j\in J}$ von V (2.26).
Sei $W := span(w_j | j \in J)$ Behauptung: $V = U \oplus W$.

Denn $U + W = V$ klar, und $U \cap W = \{0\}$: $\sum\limits_{i\in I} a_i u_i = \sum\limits_{j\in J} b_j w_j \Rightarrow$ alle $a_i = 0$, alle $b_j = 0$ wegen $\mathcal{B}$ linear unabhängig.

□

Korollar 2.45.
Ist $V = U_1 \oplus \ldots \oplus U_n$, *so ist* $\dim(V) = \sum\limits_{i=1}^{n} \dim(U_i)$.

Beweis: Sei $\mathcal{B}_i$ eine Basis von $U_i (i = 1, \ldots, n) \Rightarrow \mathcal{B}_1 \sqcup \ldots \mathcal{B}_n$ ist Basis von V, mit demselben Argument wie im letzten Beweis ($U_i \cap \sum\limits_{j\neq i} U_i = \{0\}\ \forall i = 1, \ldots, n$).

□

Bemerkungen 2.46.

(a) Im Allgemeinen gibt es zu einem UR U von V **viele** komplementäre URe W (mit $V = U \oplus W$).

(b) Sind $U_1, \ldots U_n$ URe von V mit $U_i \cap U_j = \{0\}$ für $i \neq j, i, j \in \{1, 2, \ldots, n\}$, so folgt für $n \geqq 3$ **nicht**, dass die Summe $U_1 + \ldots + U_n$ direkt ist!

Definition 2.47. (externe direkte Summe)
Sei $(V_i)_{i\in I}$ eine Familie von VRen.
Die (**externe**) **direkte Summe** der V_i ist der VR
$\bigoplus\limits_{i\in I} V_i := \{(x_i)_{i\in I} \in \prod\limits_{i\in I} V_i | x_i = 0 \text{ f.f.a. } i \in I\}$

Dies ist ein VR von $\prod\limits_{i\in I} V_i$.

Bemerkung 2.48.

(a) Für $|I| < \infty$ ist $\bigoplus\limits_{i\in I} V_i = \prod\limits_{i\in I} V_i$.
Für $|I| = \infty$: im Allgemeinen $\neq$!

(b) $V := \bigoplus\limits_{i\in I} V_i$ (externe $\oplus$).
Jedes V_i ist in kanonischer Weise mit einem UR V_i von V identifiziert: es ist $V = \bigoplus\limits_{i\in I} \widetilde{V}_i$ die interne $\oplus$.
Also: interne und externe Summe sind im Wesentlichen dasselbe.

Seien $V_1, \ldots, V_n$ VRe, sei $V := V_1 \oplus \ldots \oplus V_n = \{(v_1, \ldots, v_n) : v_i \in V_i (i = 1, \ldots, n)\}$
Sei $\widetilde{V_i} := \{(0, \ldots, 0 \underbrace{, v_i,}_{i\text{-te Stelle}} 0, \ldots, 0) : v_i \in V_i\} (i = 1, \ldots, n)$ ein mit V_i indentifizierbarer UR von V. Dann ist V die interne direkte Summe von $\widetilde{V_1}, \ldots, \widetilde{V_n}$.

3. Matrizen, lineare Abbildungen und lineare Gleichungssysteme

a. Matrizen

Sei R zunächst ein beliebiger Ring mit Eins.

Definition 3.1.

Sei $m, n \in \mathbb{N}$. Eine $m \times n$-**Matrix** über R ist ein rechteckiges Schema $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$ mit $a_{ij} \in R$. (m Zeilen, n Spalten). Die a_{ij} heißen **Koeffizienten** von A.
Man schreibt A oft auch als $A = (a_{ij})_{1 \leqq i \leqq m, 1 \leqq j \leqq n} = (a_{ij})$.
Die Menge aller $m \times n$-Matrizen über R ist $M_{m \times n}(R)$.
Für $m = n$ schreibt man auch $M_n(R) := M_{n \times n}(R)$. (quadratische Matrizen).

Bemerkung 3.2.

(a) Eine $1 \times n$-Matrix ist ein **Zeilenvektor** $(a_1, \dots, a_n) = (a_1 \dots a_n)$. Eine $m \times 1$-Matrix ist ein **Spaltenvektor** $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$.

(b) Eine (quadratische) $n \times n$-Matrix $A = (a_{ij})$ heißt eine **obere** (bzw. **untere**) **Dreiecksmatrix**, wenn $A = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$ (bzw. $A = \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix}$) ist (wobei * für beliebige Elemente steht).
d.h., wenn $a_{ij} = 0 \ \forall i > j$ (bzw. $a_{ij} = 0 \ \forall i < j$) gilt.
Ist $A = (x_{ij})$ sowohl obere wie untere Dreiecksmatrix, so heißt A auch eine **Diagonalmatrix**. Für $a_1, \dots, a_n \in \mathbb{R}$ schreibt man $diag(a_1, \dots, a_n) := \begin{pmatrix} a_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_n \end{pmatrix} = (a_{ij})_{1 \leqq i,j \leqq n}$ mit $a_{ij} = \begin{cases} a_i & \text{, falls } i = j \\ 0 & \text{, falls } i \neq j \end{cases}$.

Definition 3.3. (Addition von Matrizen)
Seien $A = (a_{ij}), B = (b_{ij}) \in M_{m \times n}(R)$.

(a) Die **Summe** von A und B ist $A + B := (a_{ij} + b_{ij}) \in M_{m\times n}(R)$.

(b) Für $c \in R$ definiert man $cA := (ca_{ij}) \in M_{m\times n}(R)$.

Lemma 3.4.

(a) $(M_{m\times n}(R), +)$ *ist abelsche Gruppe.*

(b) *Ist $R = K$ ein Körper, so ist $M_{m\times n}(K)$ mit den in 3.3 definierten Operationen ein K-VR.*

Definition 3.5. (Multiplikation von Matrizen)
Seien $A = (a_{ij}) \in M_{m\times n}(R)$, $B = (b_{jk}) \in M_{n\times r}(R)$. Dann ist das Produkt $AB = (c_{ik})_{1\leqq i\leqq m, 1\leqq k\leqq r}$ definiert durch $c_{ik} := \sum\limits_{j=1}^{n} a_{ij}b_{jk} (1 \leqq i \leqq m, 1 \leqq k \leqq r)$. AB ist also eine $m \times r$-Matrix.

Bemerkung 3.6.

(a) AB ist nur definiert, falls A genauso viele Spalten wie B Zeilen hat. Bsp:
$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} -1 & -2 & -3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 28 & 32 & 36 \\ 58 & 65 & 72 \end{pmatrix}$$

(b) $$(x_1, \ldots, x_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (x_1y_1 + \ldots + x_ny_n) \in M_{1\times 1}(R)$$
$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} (x_1, \ldots, x_n) = \begin{pmatrix} y_1x_1 & \ldots & y_1x_n \\ \vdots & \ddots & \vdots \\ y_nx_1 & \ldots & y_nx_n \end{pmatrix} \in M_{n\times n}(R).$$

Definition 3.7. (Notation)
Für die Einheitsmatrix definiert als $I_n := diag(1, \ldots 1) = \begin{pmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{pmatrix} = (\delta_{ij})_{1\leqq i,j\leqq n} \in M_n(R)$
wobei $\delta_{ij} := \begin{cases} 1 & \text{, falls } i = j \\ 0 & \text{, falls } i \neq j \end{cases}$ das **Kronecker-Delta** ist.

Lemma 3.8.

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

(b) $A(B + B') = AB + AB'$; $(A + A')B = AB + A'B$.

(c) $I_m \cdot A = A = A \cdot I_n$

(d) $(aA) \cdot B = a \cdot (AB) = A \cdot (aB)$

für $A, A' \in M_{m\times n}(R)$, $B, B' \in M_{n\times r}(R)$, $C \in M_{r\times s}(R)$ *und* $a \in R$.

Beweis:

(a) (AB)C = A(BC):
Sei $\leqq i \leqq m$, $1 \leqq l \leqq s$ fixiert. Das Element der linken Matrix an der Stelle (i, l) ist
$\sum_{k=1}^{r} (AB)_{i,k} \cdot c_{kl} = \sum_{k=1}^{r} \left(\sum_{j=1}^{n} a_{ij} \cdot b_{jk} \right) c_{kl}$;
für die rechte Matrix steht an dieser Stelle
$\sum_{j=1}^{n} a_{ij} (BC)_{jl} = \sum_{j=1}^{n} \left(a_{ij} \sum_{k=1}^{r} b_{jk} c_{kl} \right)$. $\Rightarrow$ Gleichheit! .

(b) $A(B + B') = AB + AB'$:
selbst machen ...

(c) klar - selbst machen ...

(d) klar - selbst machen ...

□

Definition 3.9. (Notation)
($m, n \in \mathbb{N}$ fest). Für $1 \leqq k \leqq m$, $1 \leqq l \leqq n$ definiere $E_{kl} \in M_{m\times n}(R)$ durch $E_{kl} := (\delta_{ik} \cdot \delta_{jl})_{1\leqq i\leqq m, 1\leqq j\leqq m}$, also $a_{ij} = 0$, wenn nicht $i = k$ und $j = l$; für diesen Fall: $a_{ij} = 1$.

Bemerkungen 3.10.

(a) Für $A = (a_{ij}) \in M_{m\times n}(R)$ ist $A = \sum\limits_{i,j} a_{ij}E_{ij}$
Ist also $R = K$ ein Körper, so ist $(E_{kl})_{1\leqq k\leqq m, 1\leqq l\leqq n}$ eine Basis des K-VR $M_{m\times n}(K)$.

(b) Mit den E_{kl} lässt sich bequem rechnen, wenn man folgende Regel benutzt:
$E_{kl} \cdot E_{rs} = \delta_{lr}E_{ks} = \begin{cases} E_{ks} & \text{, falls } l = r \\ 0 & \text{, sonst} \end{cases}$. (Nachrechnen!!)

Satz 3.11.
Für jedes $n \in \mathbb{N}$ ist $M_n(R)$ ein Ring mit Eins (bezüglich der Matrixaddition und -multiplikation). Für $n \geqq 2$ ist dieser Ring nicht kommutativ.

Beweis:
Ring mit Eins gezeigt (3.4, 3.8)
$M_n(R)$ nicht kommutativ:
$E_{11} \cdot E_{12} = E_{12}$, aber:
$E_{12} \cdot E_{11} = 0$.

□

Ab jetzt sei** $R = K$ **ein Körper.

Definition 3.12. (reguläre, singuläre Matrizen)
Eine quadratische Matrix $A \in M_n(K)$ heißt **regulär** (oder **invertierbar**), falls es eine Matrix $A' \in M_n(K)$ gibt mit $AA' = I_n = A'A$.
Andernfalls heißt A **singulär**.

Definition und Satz 3.13. *(invertierbare Matrix)*
*Sei $A \in M_n(K)$ regulär. Dann ist $A' \in M_n(K)$ mit $AA' = A'A = I_n$ eindeutig bestimmt und heißt die zu A **inverse Matrix** ($A^{-1} = A'$)*

*Die Menge $GL_n(K) := \{A \in M_n(K) | A \text{ ist regulär}\}$ bildet unter der Multiplikation eine Gruppe, die **allgemeine lineare Gruppe**. Für $n \geqq 2$ ist sie nicht abelsch.*

Beweis:
Seien $A', A' \in M_n(K)$ mit $AA' = A'A = I_n = AA'' = A''A$.
$\Rightarrow A' = A' \cdot I_n = A'(AA'') = (A'A)A'' = I_n \cdot A'' = A''$.

Für die zweite Aussage ist zunächst zu zeigen: $A, B \in M_n(K)$ regulär $\Rightarrow AB$ regulär.
Klar: $(AB) \cdot (A^{-1}B^{-1}) = A \cdot I_n \cdot A^{-1} = I_n$.
Damit fertig (denn A regulär $\Rightarrow A^{-1}$ regulär).
Nicht abelsch: Übung!

□

Beispiele 3.14. (Determinante)

1. $GL_n(K) = \{A \in M_n(K) : A \text{ regulär}\}$
   Ist $A \in GL_n(K)$ und $c \in K^*$, so auch $cA \in GL_n(K)$. Denn $A \cdot A^{-1} = A^{-1} \cdot A = I_n$.
   $\Rightarrow (cA)(c^{-1}A^{-1}) = (cc^{-1}) \cdot (AA^{-1}) = I_n$
   analog: $(c^{-1}A^{-1})(cA) = I_n$.

2. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (ad - bc) \cdot I_2$
   Man definiert die **Determinante** von $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ als $det(A) := ad - bc$.

Lemma 3.15.
Für $A, B \in M_2(K)$ ist $det(AB) = \det(A) \cdot \det(B)$.

Beweis:
$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$.

$det(AB) = (a_{11}b_{11} + a_{12}b_{21})(a_{21}b_2a_{22}b_{22}) - (a_{11}b_{12} + a_{12}b_{22})(a_{21}b_1 + a_{22}b_{21}) = \ldots = (a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21}) = \det(A) \cdot \det(B)$.

□

Korollar 3.16.
Für $A \in M_2(K)$ gilt: A regulär $\Leftrightarrow det(A) \neq 0$.

Beweis:
$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
Ist $det(A) \neq 0$, so $A \cdot \frac{1}{det(A)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = I_2 = \frac{1}{det(A)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot A$.
Ist $det(A) = 0$, so auch $0 = \det(AB) = \det(BA)$ für jedes $B \in M_2(K)$. Insbesondere $AB \neq I_2 \; \forall B \in M_2(K)$.

□

Zusatz:
Ist $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $det(A) \neq 0$, so ist $A^{-1} = \frac{1}{det(A)} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Definition 3.17. (transponierte Matrix)
Sei $A = (a_{ij})_{1 \leqq i \leqq m, 1 \leqq j \leqq n} \in M_{m \times n}(K)$.
Die zu A **transponierte Matrix** $A^t \in M_{n \times m}(K)$ ist definiert durch $A^t = (a_{ji})_{1 \leqq j \leqq n, 1 \leqq i \leqq m} \in M_{n \times m}(K)$.

Satz 3.18.
Seien $A, A_1, A_2 \in M_{m \times n}(K), B \in M_{n \times r}(K)$.

1. $(a_1 A_1 + a_2 A_2)^t = a_1 A_1^t + a_2 A_2^t$.

2. $(A^t)^t = A$.

3. $(AB)^t = B^t A^t$.

4. *$(m = n)$ A regulär $\Leftrightarrow A^t$ regulär, und dann ist $(A^t)^{-1} = (A^{-1})^t$.*

Beweis:

1. klar
2. klar
3. Nachrechnen: Ist $A = (a_{ij})_{1 \leqq i \leqq m, 1 \leqq j \leqq n}$, $B = (b_{jk})_{1 \leqq j \leqq n, 1 \leqq k \leqq r}$, so der Koeffizient von $(AB)^t$ an der Stelle (i, j) gleich $\sum\limits_k a_{jk} b_{ki} = \sum\limits_k b_{ki} a_{jk}$, und das ist auch der Koeffizient von $B^t A^t$ an der Stelle (i, j).
4. (d) folgt aus (c):
   A regulär $\Rightarrow A^t \cdot (A^{-1})^t = (A^{-1} A)^t = I_n$-
   $\Rightarrow A^t$ regulär, $(A^t)^{-1} = (A^{-1})^t$.
   Umkehrung darin enthalten.

$\square$

b. Homomorphismen von Gruppen und Ringen

Definition 3.19. (Homomorphismen von Gruppen)
Seien G, H Gruppen (multiplikativ geschrieben).

1. Ein (**Gruppen-**)**Homomorphismus** von G nach H ist eine Abbildung $\varphi : G \to H$ mit $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)\ \forall g_1, g_2 \in G$.

2. φ heißt auch ein **Monomorphismus** (bzw. **Epimorphismus**, bzw. **Isomorphismus**), falls φ zudem injektiv (bzw. surjektiv, bzw. bijektiv) ist.

3. G und H heißen **isomorph**, in Zeichen $G \cong H$, falls es einen Isomorphismus $\varphi : G \to H$ gibt.

Beispiele 3.20.

1. Die konstante Abbildung $\varphi : G \to H$, $\varphi(g) = e\ \forall g \in G$, ist ein Homomorphismus.

2. Ist $H \leqq G$ (d.h. H ist Untergruppe von G), so ist die Inklusion $\varphi : H \to G$, $\varphi(h) = h (h \in H)$, homomorph (und monomorph).

3. Ist R ein Ring und $a \in R$, so sind die Abbildungen $x \mapsto ax$ und $x \mapsto xa$ Homomorphismen von $(R, +)$ in sich.
   Denn $a(x_1 + x_2) = ax_1 + ax_2$ usw.: die Homomorphie dieser Abbildungen ist also nichts anderes als die Distributivgesetze (R3).

4. $det : GL_2(K) \to K^*$ ist ein Gruppenhomomorphismus:
   $det(AB) = \det(A) det(B)$. Es ist sogar ein Epimorphismus.
   Kein Isomorphismus: $det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 = \det\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

5. $\mathbb{C}^* \to \mathbb{R}^*, z \mapsto |z| = \sqrt{z\bar{z}}$ ist ein Homomorphismus der multiplikativen Gruppen, denn $|z_1 z_2| = |z_1| \cdot |z_2|$.

6. $exp : \mathbb{R} \to \mathbb{R}_+^*, x \mapsto e^x$ ist ein Homomorphismus von $(\mathbb{R}, +)$ in $(\mathbb{R}_+^*, \cdot)$: $e^{x+y} = ex \cdot ey$. Tatsächlich ist $\exp : \mathbb{R} \to \mathbb{R}_+^*$ ein Isomorphismus, mit Umkehrabbildung $\log : x \mapsto \log(x)$.
log ist ebenfalls isomorph: $\log : \mathbb{R}_+^* \to \mathbb{R}$.

Lemma 3.21.
Sei $\varphi : G \to H$ ein Homomorphismus von Gruppen.

(a) $\varphi(e) = e$.

(b) $\varphi(g^{-1}) = \varphi(g)^{-1}\ \forall g \in G$.

(c) $\varphi(g_1 \cdot \ldots \cdot g_n) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_n)$.

Beweis:

(a) $\varphi(e_G)^2 = \varphi(e_G^2) = \varphi(e_G) = \varphi(e_G) \cdot e_H \Rightarrow$ Kürzen OK.

(b) $\varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$.

(c) Induktion nach n.

$\square$

Lemma 3.22.
Seien $\varphi : G \to H$, $\psi : H \to M$ Homomorphismen von Gruppen.

(a) $\psi \circ \varphi : G \to M$ *ist Homomorphismus.*

(b) Ist φ Isomorphismus, so auch die Umkehrabbildung $\varphi^{-1} : H \to G$.

Beweis:

(a) $(\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = (\psi \circ \varphi)(g_1) \cdot (\psi \circ \varphi)(g_2)$.

(b) klar

□

Insbesondere gilt für Gruppen G_1, G_2, G_3:

(a) $G_1 \cong G_1$ (Reflexivität)

(b) $G_1 \cong G_2 \Rightarrow G_2 \cong G_1$ (Symmetrie)

(c) $G_1 \cong G_2 \wedge G_2 \cong G_3 \Rightarrow G_1 \cong G_3$ (Transitivität)

Definition 3.23. (Kern)
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann heißt $\ker(\varphi) := \{g \in G | \varphi(g) = e\}$ der **Kern** von φ.

Satz 3.24.
Sei $\varphi : G \to H$ Gruppenhomomorphismus.

(a) $\ker(\varphi)$ *ist Untergruppe von G und für alle $g \in G, x \in \ker(\varphi)$ gilt: $gxg^{-1} \in \ker(\varphi)$.*

(b) *φ ist injektiv $\Leftrightarrow \ker(\varphi) = \{e\}$*

Beweis:
Schreibe $N := \ker(\varphi)$.

(a) $e \in N$ (3.21 (a)), und für $g_1, g_2 \in N$ ist $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e \Rightarrow g_1 g_2^{-1} \in N$.
$g \in G, x \in N \Rightarrow \varphi(gxg^{-1}) = \varphi(g) \cdot \underbrace{\varphi(x)}_{e} \cdot \varphi(g)^{-1} = e \Rightarrow gxg^{-1} \in N$.

(b) $\Rightarrow$: klar.
$\Leftarrow$: seien $g_1, g_2 \in G$ mit $\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1) \cdot \varphi(g_2)^{-1} = e \Rightarrow \varphi(g_1 g_2^{-1}) = e \Rightarrow g_1 g_2^{-1} \in N = \{e\} \Rightarrow g_1 = g_2$.

□

Definition 3.25. (Normalteiler)
Sei G eine Gruppe. Eine Untergruppe N von G heißt **Normalteiler** von G, in Zeichen $N \trianglelefteq G$, falls für alle $g \in G$, alle $x \in N$ gilt: $gxg^{-1} \in N$.

Nach 3.24 (a) ist $\ker(\varphi) \trianglelefteq G$ für jeden Homomorphismus $\varphi : G \to H$.

Beispiele 3.26.

1. ist G abelsche Gruppe, so ist jede Untergruppe von G Normalteiler: $gxg^{-1} = gg^{-1}x = x$.

2. $\ker(det : GL_2(K) \to K^*) = \{A \in GL_2(K) : \det(A) = 1\}$ ist ein Normalteiler in $GL_2(K)$. Man schreibt:
$SL_2(K) := \{A \in GL_2(K) : \det(A) = 1\}$, und nennt $SL_2(K)$ die **spezielle lineare Gruppe**.

3. Der Kern von $|\cdot| : \mathbb{C}^* \to \mathbb{R}^*, z \mapsto |z|$ ist $\{z \in \mathbb{C} : |z| = 1\}$, die Einheitskreislinie in $\mathbb{C}$.

Definition 3.27. (Ringhomomorphismus)
Seien A, B Ringe mit Eins. Eine Abbildung $\varphi : A \to B$ heißt ein **Ringhomomorphismus**, falls

(a) $\forall a_1, a_2 \in A \ \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$.

(b) $\forall a_1, a_2 \in A \ \varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$.

(c) $\varphi(1) = 1$. d.h. $\varphi(1_A) = 1_B$.

Analog zu Gruppenhomomorphismus:

- Epimorphismus, falls φ surjektiv;
- Monomorphismus, falls φ injektiv;
- Isomorphismus, falls φ bijektiv.
- $A \cong B$, A ist isomorph zu B, falls ein Isomorphismus $A \to B$ existiert.

Bemerkungen und Beispiele 3.28.

(1) Sei $n \in \mathbb{Z}$. $\varphi : \mathbb{Z} \to \mathbb{Z}/\mathbb{Z}n$ mit $a \mapsto a + \mathbb{Z}n$ ist Ringepimorphismus.

(2) Es gelten zu Lemma 3.22 analoge Aussagen.

(3) Ist $\varphi : A \to B$ Ringhomomorphismus, so ist $\varphi : (A, +) \to (B, +)$ ein Gruppenhomomorphismus, insbesondere $\varphi(0) = 0$.

(4) Ist $\varphi : A \to B$ ein Ringhomomorphismus, so heißt
$\ker(\varphi) = \{a \in A | \varphi(a) = 0\}$
der Kern von φ.
$I := \ker(\varphi)$ hat die Eigenschaft $\forall a \in A\ \forall x \in I$: $xa \in I$, $ax \in I$.

Definition 3.29. (2-seitiges Ideal)
Sei A ein Ring. Eine Untergruppe I von $(A, +)$ heißt ein **2-seitiges Ideal** von A, wenn
$\forall a \in A\ \forall x \in I$ gilt $ax, xa \in I$.
Ist A kommutativ, so sagt man **Ideal**.

c. Lineare Abbildungen

Sei K ein Körper.

Definition 3.30. (lineare Abbildung, Endomorphismus)
Seien V, W K-VRe.
Eine Abbildung $f : V \to W$ heißt (K-)**linear** (Homomorphismus von (K-)VR), falls für $v, v' \in V$ und $a \in K$ gilt:

(i) $f(v + v') = f(v) + f(v')$ (**Additivität**)

(ii) $f(av) = af(v)$ (**Homogenität**)

- **Epimorphismus**, falls φ surjektiv;
- **Monomorphismus**, falls φ injektiv;
- **Isomorphismus**, falls φ bijektiv.
- $V \cong W$, V ist **isomorph** zu W, falls ein Isomorphismus $V \to W$ existiert.
- $Hom_K(V, W) = Hom(V, W)$ ist die Menge der K-linearen Abbildungen von V nach W.
- Ist $V = W$, so nennt man die linearen Abbildungen $V \to W$ **Endomorphismus**.
  Man schreibt $End_K(V) = End(V) := Hom_K(V, V)$.

Bemerkungen und Beispiele 3.31.

1. Ist $f : V \to W$ K-linear, so ist $f : (V, +) \to (W, +)$ ein Gruppenhomomorphismus, insbesondere $f(0) = 0$.

2. Die Komposition von zwei linearen Abbildungen ist wieder linear. Die Umkehrabbildung einer bijektiven linearen Abbildung ist wieder linear.

3. Die Nullabbildung $f : V \to W$, $f(v) = 0$ (für $v \in V$) ist linear.

4. Sei V ein VR und $v_1, v_2, \ldots, v_n \in V$ fest. Dann
   $f : K^n \to V$, $f(x_1, \ldots, x_n) := \sum\limits_{i=1}^{n} x_i v_i$ $(x_i \in K)$ ist linear.
   Denn: $\overrightarrow{x} = (x_1, \ldots, x_n), \overrightarrow{y} = (y_1, \ldots, y_n) \in K$
   $f(\overrightarrow{x} + \overrightarrow{y}) = \sum\limits_{i=1}^{n} (x_i + y_i) \cdot v_i = \sum\limits_{i=1}^{n} x_i v_i + \sum\limits_{i=1}^{n} y_i v_i.$
   $f(a\overrightarrow{x}) = \sum\limits_{i=1}^{n} a x_i v_i = a \sum\limits_{i=1}^{n} x_i v_i = a f(x_1, \ldots, x_n).$

5. Die Menge V aller (in $\mathbb{R}$) konvergenten Folgen von reellen Zahlen bildet einen $\mathbb{R}$-UR des $\mathbb{R}$-VR $\mathbb{R}^{\mathbb{N}}$.
   Die Abbildung $\lim : V \to \mathbb{R}$, $(a_n)_{n \in \mathbb{N}} \mapsto \lim\limits_{n \to \infty} a_n$ ist $\mathbb{R}$-lineare Abbildung.

6. Jede $m \times n$-Matrix $A = (a_{ij})_{i,j} \in M_{m \times n}(K)$ definiert eine lineare Abbildung:
   $F_A : K^n \to K^m$,
   $$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \mapsto Ay = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} y_1 + \ldots + a_{1n} y_n \\ \vdots \\ a_{m1} y_1 + \ldots + a_{mn} y_n \end{pmatrix}$$

Satz 3.32.
Seien V, W $K-$VRe.
Sei $(v_i)_{i \in I}$ Basis von V. Zu jeder Familie $(w_i)_{i \in I}$ von Vektoren aus W gibt es eine eindeutig bestimmte lineare Abbildung:
$f : V \to W$ mit $f(v_i) = w_i$; (für $i \in I$).

Bemerkung:
Es genügt also, Werte für die Basis anzugeben, um f zu beschreiben. Und diese darf man beliebig wählen.

Beweis:
$v \in V$ hat eine eindeutige Darstellung $v = \sum\limits_{i \in I} a_i v_i$ mit $a_i \in K$.
$f(v) := \sum\limits_{i \in I} a_i w_i$ (für $v \in V$ mit $v = \sum\limits_{i \in I} a_i v_i$).
f ist linear. Denn:

$x = \sum\limits_{i \in I} b_i v_i$
$x + v = \sum\limits_{i \in I} (b_i + a_i) v_i$
$\Rightarrow f(x + v) = \sum\limits_{i \in I} (b_i + a_i) w_i = \sum\limits_{i \in I} b_i w_i + \sum\limits_{i \in I} a_i w_i.$
$f(ax) = \sum\limits_{i \in I} (ab_i) w_i = a \sum\limits_{i \in I} b_i w_i$ für $a \in K$.

Eindeutigkeit:
Sei $\widetilde{f} : V \to W$ linear mit $\widetilde{f}(v_i) = w_i$.
$f(v_i) = \sum\limits_{i \in I} a_i w_i = \sum\limits_{i \in I} a_i \cdots f(v_i) = \sum\limits_{i \in I} a_i \cdot \widetilde{f}(v_i) = \widetilde{f}(v)$.

□

Korollar 3.33.
Die K-linearen Abbildungen $K^n \to K^m$ sind genau die Abbildungen $F_A : K^n \to K^m$ für $A \in M_{m \times n}(K)$.
Damit ist $y \mapsto Ay$ die Abbildung $M_{m \times n}(K) \to Hom_K(K^n, K^m)$.

Beweis:
Es ist für $a \in M_{m \times n}(K)$ die Abbildung $F_A : K^n \to K^m$ linear.
Die Bilder der kanonischen Basisvektoren $e_1, \ldots, e_n$ sind Spalten der Matrix A.

$$F_A(e_j) = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & mn \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

Sei $f : K^n \to K^m$ linear.
f ist eindeutig bestimmt durch $f(e_1), \ldots, f(e_n)$. Sei $B := (f(e_1), \ldots, f(e_n)) \in M_{m \times n}(K)$ und $F_B = f$, da $F_B(e_j) = f(e_j)$.

Die Abbildung $M_{m \times n}(K) \to Hom(K^n, K^m)$ ist somit surjektiv. Sie ist injektiv, da für $A \neq B$ existiert ein $j \in \{1, \ldots, n\}$ mit: die j-te Spalte von A und B ist verschieden. Damit $F_A \neq F_B$, denn $F_A(e_j) \neq F_B(e_j)$.

□

Bemerkung 3.34.
Sei $f : K^n \to K^m$ linear und $A \in M_{m \times n}(K)$ mit $F_A = f$, so gilt:
Die Spalten von A sind gerade die Bilder der kanonischen Basisvektoren unter $f = F_A$.

Beispiele 3.35.

(1) Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um den Winkel θ um den Nullpunkt.
$f\binom{1}{0} = \binom{\cos\theta}{\sin\theta}$, $f\binom{0}{1} = \binom{-\sin\theta}{\cos\theta}$
$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ mit $f = F_A$.

(2) Spiegelung an der x-Achse:
$g : \mathbb{R}^2 \to \mathbb{R}^2$
$g\binom{1}{0} = \binom{1}{0}$, $g\binom{0}{1} = \binom{0}{-1}$
$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ mit $g = F_B$.

Satz 3.36.
Seien V, W K-VRe.
Dann wird $Hom_K(V, W)$ durch die punktweisen Operationen von + und $\cdot$ selbst zu einem K-VR:
$(f + g)(v) = f(v) + g(v)$
$(a \cdot f)(v) = a \cdot f(v)$ *für* $v \in V$ *und* $a \in K$.

(ohne Beweis)

Bemerkung 3.37.
Die bijektive Abbildung (aus 3.33)
$M_{m\times n}(K) \to Hom_K(V, W)$
$A \mapsto F_A$
ist linear, also ein Isomorphismus.

$A + B = (a_{ij} + b_{ij})$
$F_{A+B} = F_A + F_B$, $F_{A+B}(y) = (A + B)y = Ay + By$.

Satz 3.38.
Für jeden K-VR V ist $End_K(V)$ ein Ring mit Eins id_V.

Beweis:
Das Produkt in $End_K(V)$ ist die Komposition $f \circ g$. Denn die Distributivgesetze $f \circ (g + h) = f \circ g + f \circ h$, d.h. $f(g(v) + h(v)) = f(g(v)) + f(h(v))$ $\forall v \in V$ und $(f + g) \circ h = f \circ h + g \circ h$ ist trivial.

(Identität ist 1)

□

Satz 3.39.
Seien $A \in M_{m\times n}(K)$, $B \in M_{n\times r}(K)$ und seien $F_A : K^n \to K^m$, $F_B : K^r \to K^n$ die entsprechenden linearen Abbildungen. Dann gilt $F_A \circ F_B = F_{AB}$ (als lineare Abbildung $K^r \to K^m$)

Beweis:
Seien $A = (a_{ij})_{1\leqq i\leqq m, 1\leqq j\leqq n}$, $B = (b_{jk})_{1\leqq j\leqq n, 1\leqq k\leqq r}$.
Für $k = 1, \dots r$ gilt
$F_{AB}(e_k) = \sum_{i=1}^{m}(AB)_{ik}e_i = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)e_i$
Andererseits
$F_A \circ F_B(e_k) = F_A\left(\sum_{j=1}^{n} b_{jk}e_j\right) = \sum_{j=1}^{n} bjk \sum_{j=1}^{m} a_{ij}e_i.$

□

Korollar 3.40.
Die Abbildung $M_n(K) \to End_K(K^n), A \to F_A$ ist ein Isomorphismus von Ringen.

Definition 3.41. (Automorphismus)
Sei V ein K-VR. Ein (K-)Endomorphismus f von V heißt ein **Automorphismus** von V, wenn f bijektiv (also ein Isomorphismus) ist.
Die Menge aller Automorphismen von V ist eine Gruppe bezüglich der Komposition, bezeichnet auch als allgemeine lineare Gruppe $GL(V) = GL_K(V)$ von V.

Korollar 3.42.
Sei $n \in \mathbb{N}$

(a) Eine Matrix $A \in M_n(K)$ ist genau dann regulär, wenn $F_A : K^n \to K^n$ bijektiv (also in $GL(K^n)$) ist.

(b) Die Abbildung $GL_n(K) \to GL(K^n)$ ist ein Gruppenhomomorphismus $A \mapsto F_A$.

Beweis:

(a) A regulär $\Leftrightarrow \exists g \in End(K^n) g \circ F_A = id = F_A \circ g$ (nach 3.40)
$\Leftrightarrow F_A$ ist bijektiv.

(b) daher klar aus 3.40

□

Bemerkung 3.43.
Sei $f : V \to W$ eine lineare Abbildung. Für jeden UR W_1 von W ist $f^{-1}(W_1) = \{v \in V : f(v) \in W_1\}$ ein UR von V.
Insbesondere ist $\ker(f) = f^{-1}(\{0\})$ ein UR von V.

Satz 3.44.
Sei $f : V \to W$ eine lineare Abbildung. Dann ist $\dim(V) = \dim(\ker(f)) + \dim(im(f))$.

Beweis:
Sei $(u_i)_{i\in I}$ eine Basis von $\ker(f)$. Sei $(v_j)_{j\in J}$ eine Familie in V, so dass $(f(v_j))_{j\in J}$ eine Basis von $im(f)$ ist.
Behauptung: $\mathcal{B} := (u_i)_{i\in I} \sqcup (v_j)_{j\in J}$ eine Basis von V. ($\Rightarrow$ Aussage des Satzes)

(1) $\mathcal{B}$ ist linear unabhängig:
sei $\sum\limits_{i\in I} a_i u_i + \sum\limits_{j\in J} b_j v_j = 0$ (*) ($a_i, b_j \in K$, f.f.a. $a_i, b_j = 0$)
Anwenden von $f \Rightarrow \sum\limits_{j\in J} b_j f(v_j) = 0$ (**) $\Rightarrow$ alle $b_j = 0$
$\Rightarrow$ alle $a_i = 0$ (*).

(2) $span(\mathcal{B}) = V$. Sei $v \in V$. Dann ist $f(v) = \sum\limits_{j\in J} b_j f(v_j)$ mit geeigneten $b_j \in K$ (f.f.a. $b_j = 0$)
$v - \sum\limits_{j\in J} b_j v_j \in \ker(f)$
$\Rightarrow v - \sum\limits_{j\in J} b_j v_j = \sum\limits_{i\in I} a_i u_i$ mit geeigneten $a \in K \Rightarrow$ OK

□

Korollar 3.45.
Sei $f : V \to W$ linear, sei $\dim(V) = \dim(W) < \infty$
Dann folgt:
f ist injektiv $\Leftrightarrow$ f ist surjektiv $\Leftrightarrow$ f ist bijektiv.

Beweis: f ist injektiv $\Leftrightarrow \ker(f) = 0 = \{0\} \Leftrightarrow \dim(\ker(f)) = 0$
$im(f) = W \Leftrightarrow \dim(W) = \dim(V) = \dim(im(f)) \Leftrightarrow f$ ist surjektiv.

□

Korollar 3.46.
Sind V, W VRe mit $\dim(V) = \dim(W) < \infty$, so ist $V \cong W$ (isomorph).
Insbesondere gilt also $\dim(V) = n > 0 \Rightarrow V \cong K^n$.

Beweis:
Sei $n := \dim(V) = \dim(W)$, sei $(v_1 \ldots v_n)$ eine Basis von V, $(w_1, \ldots, w_n)$ eine Basis von W.
Sei $f : V \to W$ die lineare Abbildung mit $f(v_i) = w_i$, $i = 1, \ldots, n$.
Dann ist f surjektiv $\Rightarrow f$ ist bijektiv (nach 3.45)

□

Bemerkung 3.47.
Für $\dim(V) = \dim(W) = \infty$ werden 3.45 und 3.46 im Allgemeinen falsch.

Korollar 3.48. *(Dimensionsformel)*
Sei V ein VR, seien U_1, U_2 endlich-dimensionale URe von V. Dann gilt:
$\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

Beweis:
Sei $U_1 \oplus U_2 = U_1 \times U_2$ die (externe) direkte Summe, es ist $\dim(U_1 \oplus U_2) = \dim(U_1) + \dim(U_2)$. Betrachte die lineare Abbildung $f : U_1 \oplus U_2 \to U_1 + U_2$, $f(u_1, u_2) := u_1 + u_2$.
f ist surjektiv: weiter gilt: $\ker(f) = \{(x, -x) : x \in U_1 \cap U_2\}$ $(\subset U_1 \oplus U_2)$
Es ist $\ker(\varphi) \cong U_1 \cap U_2$ mittels dem Isomorphismus $(x, -x) \to x$. Die Dimensionsformel 3.44 für f gibt also $\dim(U_1 \oplus U_2) = \dim(\ker(f)) + \dim(im(f))$
$\Rightarrow \dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

□

Korollar 3.49.
Ist $\dim(V) = n < \infty$, so gilt für URe U_1, U_2 von V:
$\dim(U_1 \cap U_2) \geqq \dim(U_1) + \dim(U_2) - n$

Beweis: siehe 3.48

□

Satz 3.50. *(interne, externe Summe)*
Sei V ein VR, sei $(U_i)_{i \in I}$ eine Familie von Unterräumen von V.

Sei $U := \sum_{i \in I} U_i$ (ein UR von V), sei $\bigoplus_{i \in I} U_i$ die externe direkte Summe.

(a) *Die lineare Abbildung $\bigoplus_{i \in I} U_i \to U$, $(u_i)_{i \in I} \to \sum_{i \in I} u_i$, ist surjektiv.*

(b) *Genau dann, wenn ist die Abbildung (a) ein Isomorphismus, wenn die Summe $U = \sum_{i \in I} U_i$ direkt ist.*

Beweis:
folgt direkt aus der Definition.

□

Definition 3.51. (affiner Unterraum)
Sei V ein VR. Eine Teilmenge A von V heißt ein **affiner Unterraum** von V, wenn es einen UR U von V und ein $v \in V$ gibt mit $A := v + U := \{v + u : u \in U\}$.

Bemerkungen und Beispiele 3.52.

1. Für $a, bc \in \mathbb{R}$ ist $A := \{(x, y) \in \mathbb{R}^2 : ax + by = c\}$ ein affiner UR von $\mathbb{R}^2$
   $(a, b) \neq (0, 0)$: $\dim(A) = 1$.
   $(a, b) = 0$: $A = \mathbb{R}^2$ (für $c = 0$), $A = \emptyset$ (für $c \neq 0$).

2. Ein affiner UR A von V ist genau dann ein affiner Unter-VR von V, wenn $0 \in A$

3. Zur besseren Unterscheidung: man sagt oft auch „lineare Unterräume“ „für Untervektorräume“.

Satz 3.53.
Sei U ein linearer UR von V, sei $v \in V$ und $A = v + U$ (affiner UR von V). Dann ist $U = \{x - y : x, y \in A\}$, und $A = (x + U)$ für alle $x \in A$.

der Beweis ist offensichtlich, denn schauen Sie ... ;-)

Beweis:
$(v + u_1) - (v + u_2) = u_1 - u_2$

$v + U = \underbrace{(v + u)}_{\in A} + U$ für jedes $u \in U$.

□

Insbesondere sehen wir: der lineare UR U ist durch den affinen UR $A = v + U$ eindeutig bestimmt.

Definition 3.54. (Translationsraum)
sei A ein affiner UR. Ist $A \neq \emptyset$, so heißt der lineare UR
$T(A) := \{x - y : x, y \in A\}$ von V der **Translationsraum** von A.
Die Dimension von A ist definiert als $\dim(A) := \begin{cases} \dim(T(A)) & \text{, falls } A \neq \emptyset \\ -1 & \text{, falls } A = \emptyset \end{cases}$

Satz 3.55.
Sei $f : V \to W$ eine lineare Abbildung von K-VRen. Für jedes $w \in W$ ist die Urbildmenge $f^{-1}(\{w\}) = \{v \in V : f(v) = w\}$ ein affiner UR von V. Ist $f^{-1}(\{w\}) \neq \emptyset$, so ist $T(f^{-1}(\{w\})) = \ker(f)$.

Beweis:
Ist $w \in im(f)$, etwa $w = f(v)$ mit $v \in V$, so $f^{-1}(\{w\}) = \{v + u : f(u) = 0\} = v + \ker(f)$.
□

Bemerkungen 3.56.

1. Die Bestimmung von $f^{-1}(\{w\})$ zerfällt also in zwei Schritte:

    - Entscheide, ob $w \in im(f)$. Falls ja, finde ein $v \in V$ mit $f(v) = w$.

    - (falls $w \in im(f)$) Bestimme den lineare UR $\ker(f)$ von V; z.B. gebe eine Basis von $\ker(f)$ an.

2. Betrachte insbesondere das Beispiel $F_A : K^n \to K^m$ mit $A = (a_{ij}) \in M_{m \times n}(K)$. Für $u = (u_1, \dots u_m) \in K^m$ sei $\mathcal{L}(A, u) = \{x \in K^n : Ax = u\} = \{x \in K^n : F_A(x) = u\}$ ein affiner UR des K^n.
$\mathcal{L}(A, u)$ ist die Lösungsmenge des linearen Gleichungssystems (*)

    $$\begin{aligned} &a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = u_1 \\ &\vdots \\ &a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = u_m \end{aligned}$$

    Um (*) zu lösen geht man also in zwei Schritten vor:

- Entscheide, ob (*) lösbar ist, und bestimme gegebenenfalls eine Lösung $v = (v_1, \dots v_n)$ von (*).

- Löse das zugehörige **homogene System**, d.h. bestimme $\mathcal{L}(A, 0) = \ker(F_A)$.

Dann ist $\mathcal{L}(A, u) = v + \mathcal{L}(A, 0)$.
Wie man dies konkret macht, siehe unten.

d. Quotienten von Gruppen und Vektorräumen

Definition 3.57. (Relation, Äquivalenzrelation)

(1) Eine **Relation** auf einer Menge X ist eine Teilmenge R von $X \times X$.

(2) R heißt eine **Äquivalenzrelation**, wenn gelten:

   (a) $(x, x) \in R$ (Reflexivität)

   (b) $(x, y) \in R \Rightarrow (y, x) \in R$ (Symmetrie)

   (c) $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$ (Transitivität)

   für alle $x, y, z \in X$.

Beispiele 3.58.

1. Notiere Äquivalenzrelation in der Regel als $\sim$ oder $\approx$, d.h. man schreibt $x \sim y$ für $(x, y) \in R$.

2. Beispiele von Äquivalenzrelationen:

   (a) Identitätsrelation: $x \sim y \Leftrightarrow x = y$

   (b) Allrelation: $x \sim y \; \forall x, y \in X$

   (c) Ist $f : X \to Y$ eine Abbildung von Mengen, so ist auf X eine Äquivalenzrelation $\sim_f$ definiert durch $x_1 \sim_f x_2 :\Leftrightarrow f(x_1) = f(x_2)$

Konstruktion 3.59. (Äquivalenzklasse, Quotientenmenge, Quotientenabbildung)

Sei $\sim$ eine ÄR auf der Menge X.
Für $x \in X$ sei $[x] := \{y \in X : x \sim y\}$, die **Äquivalenzklasse** von x. Für $x, y \in X$ gilt entweder $[x] \cap [y] = \emptyset$ oder $[x] = [y]$.

(Denn: sei $z \in [x] \cap [y]$, dann also $x \sim z \sim y \Rightarrow x \sim y$. Ist $w \in [x]$, so $y \sim x \sim w \Rightarrow y \sim w$, d.h. $w \in [y]$. Also $[x] \subset [y]$, analog $\supset$)
Die Menge X wird also **disjunkt** in Äquivalenzklassen zerlegt.

Die **Quotientenmenge** $X/\sim$ („X modulo $\sim$“) ist definiert als $X/\sim := \{[x] : x \in X\}$ (also $X/\sim \subset \mathcal{P}(X)$).
Die Abbildung $\pi : X \to X/\sim$, $\pi(x) := [x]$, heißt die **Quotientenabbildung**. Für alle $x, y \in X$ gilt $\pi(x) = \pi(y) \Leftrightarrow x \sim y$. (es ist also $\sim = \sim_\pi$, Notation wie in 3.58 3.)

Beispiel 3.60. (Rechtsnebenklasse)
Sei G eine Gruppe, $H \leqq G$ eine Untergruppe. Durch $x \sim y :\Leftrightarrow y^{-1}x \in H$ $(x, y \in G)$ wird auf G eine ÄR $\sim$ definiert:
$x \sim x$: $x^{-1}x = e \in H$
$x \sim y \Rightarrow y^{-1}x \in H \Rightarrow (y^{-1}x)^{-1} = x^{-1}y \in H \Rightarrow y \sim x$
$x \sim y \wedge y \sim z \Rightarrow y^{-1}x, z^{-1}y \in H \Rightarrow (z^{-1}y)(y^{-1}x) \in H \Rightarrow x \sim z$.

Man nennt $[x] = \{y \in G : x^{-1}y \in H\} = \{y \in G : \exists h \in H x^{-1}y = h\}$,
also $[x] = xH := \{y \in G : \exists h \in H : y = xh\}$,
die **Rechtsnebenklasse** von x nach H. Die Quotientenmenge wird als $G/H := \{xH : x \in G\}$ bezeichnet.

Je zwei Nebenklassen xH, yH sind gleichmächtig, denn $H \to xH$, $h \mapsto xh$, ist bijektiv.

Korollar 3.61. *(Satz von Lagrange)*
Sei G eine endliche Gruppe, $H \leqq G$.
Dann ist $|G| = |H| \cdot |G/H|$.
Insbesondere ist $|H|$ ein Teiler von $|G|$.

*Das Gesagte überträgt sich analog auf **Linksnebenklassen** $Hx := \{hx : h \in H\}$ und die Menge $H \setminus G := \{Hx : x \in G\}$ aller Linksnebenklassen.*

Konstruktion 3.62.
Sei jetzt $H = N$ ein Normalteiler von G.
D.h. für alle $x \in G, y \in N$ gilt $xyx^{-1} \in N$, d.h.
$\forall x \in G\ xN = Nx$.

Wir machen die Menge G/N $(= N \setminus G)$ zu einer Gruppe durch folgende Definition:
$xN \cdot yN := (xy)N$ (*)

Dies ist tatsächlich wohldefiniert:
für $x' = xn_1, y' = yn_2$ mit $n_1, n_2 \in N$ ist
$x'y' = xn_1yn_2 = xy\underbrace{(y^{-1}n_1y)}_{inN}n_2 = xyn$ mit $n = y^{-1}n_1yn_2 \in N$ also $(x'y')N = (xy)N$.

Satz 3.63. *(Quotientengruppe)*
Sei G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler. Durch (*) wird G/N selbst zu einer Gruppe, der ***Quotientengruppe*** *„G modulo N".Die Quotientenabbildung $\pi : G \to G/N$, $\pi(g) = gN$ ($g \in G$) ist ein Gruppenepimorphismus, und* $\ker(\pi) = N$.

Beweis:
Dass G/N eine Gruppe ist, ist klar:
Assoziativität aus Assoziativität von G, neutrales Element ist $e \cdot N = N$ und $(xN)^{-1} = x^{-1}N$.
Homomorphie von π gilt nach Definition:
$\pi(xy) = \pi(x) \cdot \pi(y)$ heißt $(xy)N = xN \cdot yN$.
Für $x \in N$:
$\pi(x) = e = 1 \cdot N \in G/N$
$\Leftrightarrow xN = 1 \cdot N = N$
$\Leftrightarrow x \in N$
also $\ker(\pi) = N$.

□

Umgekehrt:

Satz 3.64. *(Homomorphiesatz für Gruppen)*
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, sei $N := \ker(\varphi)$.

(a) Es gibt einen eindeutig bestimmten Homomorphismus $\psi : G/N \to H$ mit $\psi \circ \pi = \varphi$, d.h. derart, dass das Dreieck ... kommutiert; und ψ ist injektiv.

(b) ψ ist Isomorphismus $\Leftrightarrow \varphi$ ist surjektiv.

Beweis:
Wir müssen definieren $\psi(xN) := \varphi(x)$ ($x \in G$).

(a) Wohldefiniertheit:
$xN = yN \Rightarrow y = xn$ mit $n \in N$.

$\Rightarrow \varphi(y) = \varphi(x)\dot{\varphi}(n) \Rightarrow \varphi(y) = \varphi(x)$ (da $\varphi(n) = e$)

ψ Homomorphismus:
$\psi(xN \cdot yN) = \psi(xyN) = \varphi(xy) = \varphi(x) \cdot \varphi(y) = \psi(xN) \cdot \psi(yN)$ - OK.

ψ ist injektiv:
Wir zeigen $\ker(\psi) = \{eN\}$: für $x \in G$ folgt:
$\psi(xN) = e \Rightarrow \varphi(x) = e \Rightarrow x \in \ker(\varphi) = N \Rightarrow xN = eN$ - OK.

(b) ψ ist Isomorphismus $\Leftrightarrow$ ψ ist surjektiv $\Leftrightarrow$ $\forall h \in H\ \exists g \in G\ \psi(gN) = h = V(g)$ $\Leftrightarrow$ φ ist surjektiv.

□

Korollar 3.65.
Für jeden surjektiven Gruppenhomomorphismus $\varphi : G \to H$ ist $H \cong G/\ker(\varphi)$.

(Folgt sofort aus 3.64 (b))

Beispiele 3.66.

1. $\det : GL_2(K) \to K^*$ ist ein surjektiver Gruppenhomomorphismus (3.27) mit Kern $SL_2(K) = \{A \in M_2(K) : \det(A) = 1\}$
   Aus 4.9 folgt also $GL_2(K)/SL_2(K) \cong K^*$.

2. Der Kern des Epimorphismus $\mathbb{C}^* \to \mathbb{R}^*_+$, $z \mapsto |z|$, ist $\mathcal{U} = \{z \in \mathbb{C}^* : |z| = 1\}$.
   Also folgt $\mathbb{C}^*/\mathcal{U} \cong \mathbb{R}^*_+$.

3. $G/\{e\} \cong G$
   $G/G \cong \{e\}$

4. Ist $(G, +)$ eine additiv geschriebene (damit kommutative) Gruppe und $H \leqq G$, so schreibt man die Elemente von G/H als $x + H$ $(x \in G)$, und die Gruppe G/H additiv: $(x + H) + (y + H) = (x + y) + H$.

Bemerkung 3.67. (Quotienten von Ringen)
Sei R ein Ring, sei I ein 2-seitiges Ideal in R. Dann wird die Quotientengruppe R/I der additiven Gruppen zu einem Ring durch die Definition
$(a+I)\cdot(b+I) := ab+I$ $(a,b\in R)$. (wohldefiniert, da I 2-seitiges Ideal)

Die Quotientenabbildung $\pi : R \to R/I$, $\pi(a) = a+I$, ist ein Ringepimorphismus, und es gilt ein zu 3.64 bzw. 3.65 analoger Homomorphiesatz für Ringe.

Beispiel 3.68.
$\mathbb{Z}/\mathbb{Z}n = \{\overline{0},\overline{1},\dots,\overline{n-1}\}$ (siehe 1.3.5) ist der Quotientenring von $R=\mathbb{Z}$ nach dem Ideal $I = n\mathbb{Z}$ $(n\in\mathbb{N})$.

Konstruktion 3.69.
(Sei K ein Körper)
Sei V ein K-VR, sei U ein Unter-VR von V.
Die additive Gruppe $(V/U,+)$ haben wir bereits definiert (als den Quotienten der Gruppe $(V,+)$ nach ihrer Untergruppe U).
Die Elemente von V/U sind die $\overline{v} := v+U$ $(v\in V)$, mit $\overline{v_1} = \overline{v_2} \Leftrightarrow v_1 - v_2 \in U$.
Definiere Skalarmultiplikation $K\times(V/U)\to V/U$ durch
$a\cdot\overline{v} := \overline{av}$ $(a\in K, v\in V)$ (also $a\cdot(v+U) := av+U$). Wegen $KU\in U$ ist dies wohldefiniert. Wir erhalten folgenden Satz:

Satz 3.70. *(Quotienten-Vektorraum)*
Mit diesen Definitionen wird V/U zu einem K-VR, genannt der ***Quotienten-Vektorraum*** *„V modulo U“.*
Die Quotientenabbildung $\pi : V \to V/U$, $\pi(v) = \overline{v} = v+U$, ist K-linear und surjektiv, mit $\ker(\pi) = U$.

□

Satz 3.71. *(Homomorphiesatz)*
Analog zu Gruppen:

Sei $f : V \to W$ eine K-lineare Abbildung von VRen, sei $U := \ker(f)$.

(a) $\exists$ eindeutige lineare Abbildung $g : V/U \to W$, so dass das Dreieck ... kommutiert, und g ist injektiv.

(b) g ist Isomorphismus $\Leftrightarrow$ f ist surjektiv.

Beweis:
$g(\overline{v}) := f(v)$; alles bis auf die Verträglichkeit mit Skalarmultiplikation folgt aus 3.64, letztere ist klar.

□

Korollar 3.72.
Ist $f : V \to W$ ein Epimorphismus von VRen, so ist $V/\ker(f) \cong W$.

Definition 3.73. (Kodimension)
Sei V ein K-VR, sei U ein Unter-VR von V. Dann heißt $codim_V(U) := \dim(V/U)$ die **Kodimension** von U in V.

Korollar 3.74.
Ist $\dim(V) < \infty$, so ist $codim_V(U) = \dim(V) - \dim(U)$.

Beweis:
Wende die Dimensionsformel 3.44 an auf
$\pi : V \to V/U$: $\dim(V) = \underbrace{\dim(\ker(\pi))}_{U} + \underbrace{\dim(im(\pi))}_{V/U}$.

□

Bemerkungen 3.75.

1. Die Elemente von V/U sind genau alle affinen URe A von V mit $T(A) = U$.

2. $V/\{0\} \cong V$
   $V/V \cong \{0\}$

3. Ein Unter-VR H von V heißt eine (**lineare**) **Hyperebene** in V, wenn $codim_V(H) = 1$ ist.
   Beispiel: $V = K^n$, sei $a = (A, \dots, a_n) \neq (0, \dots, 0)$, dann ist $H := \{x = (x_1, \dots, x_n) \in K^n : \sum_{i=1}^{n} a_i x_i = 0\}$ eine Hyperebene in K^n. Denn H ist der Kern der surjektiven linearen Abbildung $K^n \to K$, $x \mapsto \sum_{i=1}^{n} a_i x_i$. ($\Rightarrow codim_{K^n}(H) = \dim(K) = 1$)

Satz 3.76.
Sei V ein VR, seien U, W Unter-VRe von V.

(a) $U/U \cap W \cong (U+W)/W$ *(1. Isomorphiesatz)*

(b) Ist $U \subset W$*, so ist* $(V/U)/(W/U) \cong V/W$ *(2. Isomorphiesatz)*

Betrachte die **Hasse-Diagramme**:

$\vdots$

Beweis:

(a) Die lineare Abbildung $f : U \to (U+W)/W$, $f(u) := u + W$ ist surjektiv, denn das typische Element von $(U+W)/W$ ist $u + w + W = u + W = f(u)$.
Es ist $\ker(f) = \{u \in U : u + W = 0 + W\} = \{u \in U : u \in W\} = U \cap W$. Also nach 3.72:
$(U+W)/W = im(f) \cong U/\ker(f) = U/(U \cap W)$.

(b) Die lineare Abbildung $g : V/U \to V/W$, $g(v+U) := g(v+W)$ $(v \in V)$ ist surjektiv mit $\ker(g) = \{v + U : v \in W\} = W/U$. Nun wende wieder 3.72 an.

□

Korollar 3.77.
Sei U *ein Unter-VR von* V*, sei* W *ein zu* U *komplementärer Unter-VR. Dann ist* $W \cong V/U$*.*

Beweis:
$V = U \oplus W \Rightarrow W = W/\underbrace{(U \cap W)}_{\{0\}} \cong (U+W)/U = V/U$.

Genauer ist also $W \to V/U$, $w \mapsto w + U$, ein Isomorphismus.

□

e. Koordinaten, Basiswechsel, Koordinatentransformation

K ein Körper, VRe seien endlich-dimensional.

Satz 3.78. *(Koordinatensystem, Koordinatenvektor)*
Sei V ein K-VR, $\dim(V) = n < \infty$, sei $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V. Die lineare Abbildung
$\Phi_{\mathcal{B}} : K^n \to V$, $\Phi(x) = \sum\limits_{i=1}^{n} x_i v_i$ ist ein Isomorphismus und heißt das zu $\mathcal{B}$ gehörende ***Koordinatensystem****. Für $v = \sum\limits_{i=1}^{n} x_i v_i$ heißt $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \Phi_{\mathcal{B}}^{-1}(v)$ der* ***Koordinatenvektor*** *von v bezüglich $\mathcal{B}$.*

Definition 3.79. (beschreibende Matrix)
Sei weiter $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V, sei W ein m-dimensionaler VR mit einer Basis $C = (w_1, \dots, w_m)$.
Sei $f : V \to W$ eine lineare Abbildung. Wir drücken $f(v_j)$ $(j = 1, \dots, n)$ durch C aus: $f(v_j) = \sum\limits_{i=1}^{m} a_{ij} w_i$ (mit $a_{ij} \in K$).

Dann heißt die $m \times n$-Matrix $M_C^{\mathcal{B}}(f) := (a_{ij})_{1 \leqq i \leqq m, 1 \leqq j \leqq n} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{nn} \end{pmatrix}$ die f **beschreibende Matrix**.

Satz 3.80.
Die Matrix $A = M_C^{\mathcal{B}}(f)$ ist die eindeutig bestimmte Matrix, für die das Quadrat ... kommutiert, d.h. $f \circ \Phi_{\mathcal{B}} = \Phi_C \circ F_A$.
Die Abbildung $M_C^{\mathcal{B}} : Hom_K(V, W) \to M_{m \times n}(K), f \mapsto M_C^{\mathcal{B}}(f)$ ist ein VR-Isomorphismus.
Insbesondere ist
$\dim_K Hom_K(V, W) = \dim_K(V) \cdot \dim_K(W)$.

Beweis:
Kommutiert das Quadrat, so ist $F_A = \Phi_C^{-1} \circ f \circ \Phi_{\mathcal{B}}$ also ist dadurch A eindeutig bestimmt. Umgekehrt gilt für $A = M_C^{\mathcal{B}}(f) = (a_{ij})$. Es ist für $j = 1, \dots, n$

$(f \circ \Phi_{\mathcal{B}})(e_j) = f(v_j)$, andererseits ist $(\Phi_C \circ F_A)(e_j) = \Phi_C \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = \sum\limits_{i=1}^{m} a_{ij} w_i = f(v_j)$ -

OK.
$M_C^{\mathcal{B}}$ linear ist klar.
Die Umkehrabbildung von $M_C^{\mathcal{B}}$ ist $A \mapsto \Phi_C \circ F_A \circ \Phi_{\mathcal{B}}^{-1}$.

□

Bemerkungen und Beispiele 3.81.

1. Anders gesagt: ist $v \in V$, ist $x = \Phi_{\mathcal{B}}^{-1}(v)$ sein Koordinatenvektor bezüglich $\mathcal{B}$ und ist $x = \Phi_C^{-1}(f(v_j))$ der Koordinatenvektor von $f(v)$ bezüglich C, so ist

   $$y = M_C^{\mathcal{B}}(f) \cdot x.$$

2. **Merkregel:** In der j-ten Spalte von $M_C^{\mathcal{B}}(f)$ stehen die Koeffizienten des Bildes des j-ten Vektors von $\mathcal{B}$, ausgedrückt durch die Basis C.

3. Sei K_m (bzw. K_n) die kanonische Basis von K^m (bzw. K^n); die Koordinatensysteme $\Phi_{K_n} : K^n \to K^n$, $\Phi_{K_m} : K^m \to K^m$ sind die Identitäten. Für jedes $A \in M_{m\times n}(K)$ ist
   $M_{K_m}^{K_n}(F_A) = A$.

4. Sei $\mathbb{R}[x]_d := \{\sum\limits_{i=0}^{d} a_i x^i : a_i \in \mathbb{R}\}$ der $\mathbb{R}$-Vektorraum der Polynome vom Grad $\leqq d$.
   Die Abbildung $D : \mathbb{R}[x]_d \to \mathbb{R}[x]_d, D(f) := f'$, also $D\left(\sum\limits_{i=0}^{d} a_i x^i\right) = \sum\limits_{i=1}^{d} i a_i x^{i-1}$, ist $\mathbb{R}$- linear.
   Bezüglich der Basis $\mathcal{B} = (1, x, x^2, \dots, x^d)$ von $\mathbb{R}[x]_d$ ist

   $$M_{\mathcal{B}}^{\mathcal{B}}(D) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 2 & \dots & 0 \\ 0 & 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & (d-1) \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

5. Für festes $a \in \mathbb{R}$ ist auch $C = (1, x-a, (x-a)^2, \dots, (x-a)^d)$ eine Basis von $\mathbb{R}[x]_d$. (siehe Übungsaufgabe 4.4).
   Die Taylorformel für Polynome sagt: Für $f \in \mathbb{R}[x]_d$ ist
   $f = f(a) + \frac{f'(a)}{1!}(x-a) + \dots + \frac{f^{(d)}(a)}{d!}(x-a)^d = \sum\limits_{i=0}^{d} \frac{f^{(i)}(a)}{i!}(x-a)^i$ wobei $f^{(i)} := \underbrace{D \circ \ldots \circ D}_{i-mal}(f)$. Das bedeutet

$$\Phi_C^{-1}(f) = \left(f(a), \frac{f'(a)}{1!}, \ldots, \frac{f^{(d)}(a)}{d!}\right)^t.$$

Satz 3.82.
$(f, V, W, \mathcal{B}, C$ wie bisher)

Sei $g : U \to V$ weitere lineare Abbildungen, sei $\mathcal{A}$ eine Basis von U. Dann ist $M_C^{\mathcal{A}}(f \circ g) = M_C^{\mathcal{B}}(f) \cdot M_{\mathcal{B}}^{\mathcal{A}}(g)$.

Beweis:
Betrachte ... (mit $r := \dim(U)$), $B := M_{\mathcal{B}}^{\mathcal{A}}(g)$. Es kommutiert jedes der beiden Einzelquadrate (links und rechts). Also kommutiert auch das äußere Rechteck.
Wegen $F_A \circ F_B = F_{AB}$ sind wir fertig nach Satz 3.80.

□

Korollar 3.83.
(vorige Bezeichnungen)

$f : V \to W$ ist Isomorphismus $\Leftrightarrow M_C^{\mathcal{B}}(f)$ regulär ist

Sind diese Bedingungen erfüllt, so ist $M_{\mathcal{B}}^{C}(f^{-1}) = M_C^{\mathcal{B}}(f)^{-1}$.

Beweis:
f ist Isomorphismus $\Leftrightarrow F_A$ ist Isomorphismus $\Leftrightarrow A$ ist regulär (3.42 (a)).
Ist f ein Isomorphismus, so erhalte $M_{\mathcal{B}}^{C}(f^{-1}) = M_C^{\mathcal{B}}(f)^{-1}$ aus 3.82 ($g := f^{-1}$).

□

Korollar 3.84.
Sei V ein VR, sei $\mathcal{B}$ eine Basis von V. Dann ist die Abbildung $M_{\mathcal{B}}^{\mathcal{B}} : End_K(V) \to M_n(K)$ ($n := \dim(V)$) ein Ringisomorphismus, und ihre Restriktion $GL_K(V) \to GL_n(K)$ ist ein Gruppenisomorphismus.

(Dass sie zu Bijektion $GL_K(V) \to GL_n(K)$ einschränkt, folgt aus 3.83) □

Konstruktion 3.85. (Basiswechsel)
Sei $\mathcal{B} = (v_1, \ldots, v_n)$ Basis von V, sei $\mathcal{B}' = (v_1', \ldots, v_n')$ eine zweite Basis von V, sei $\Phi_{\mathcal{B}'} : K^n \to V$ das entsprechende Koordinatensystem.
Nach Satz 3.80 kommutiert das Quadrat ... mit $T := M_{\mathcal{B}'}^{\mathcal{B}}(id_V)$. Also sehen wir:

Definition und Satz 3.86.
$T^{\mathcal{B}}_{\mathcal{B}'} := M^{\mathcal{B}}_{\mathcal{B}'}(id_V)$ heißt die Basiswechselmatrix von $\mathcal{B}$ nach $\mathcal{B}'$.
Sie ist regulär, und ist charakterisiert durch $T^{\mathcal{B}}_{\mathcal{B}'} = (t_{ij})_{1\leqq i,j\leqq n}$ mit $v_j = \sum\limits_{i=1} nt_{ij}v'_j$ $(j = 1,\dots,n)$.
Für jedes $v \in V$ mit Koordinatenvektoren $x = \Phi^{-1}_{\mathcal{B}}(v)$ bezüglich $\mathcal{B}$ und $x' = \Phi^{-1}_{\mathcal{B}'}(v)$ bezüglich $\mathcal{B}'$ ist $x' = T^{\mathcal{B}}_{\mathcal{B}'} \cdot x$. □

Korollar 3.87.
Für je drei Basen $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ von V ist $T^{\mathcal{B}_1}_{\mathcal{B}_3} = T^{\mathcal{B}_2}_{\mathcal{B}_3} \cdot T^{\mathcal{B}_1}_{\mathcal{B}_2}$ und $T^{\mathcal{B}_2}_{\mathcal{B}_1} = \left(T^{\mathcal{B}_1}_{\mathcal{B}_2}\right)^{-1}$.

Beweis:
Spezialfall von 3.82 und 3.83.

□

Korollar 3.88.
Sei $f : V \to W$ eine lineare Abbildung, seien $\mathcal{B}, \mathcal{B}'$ Basen von V, seien $\mathcal{C}, \mathcal{C}'$ Basen auf W. Dann ist $M^{\mathcal{B}'}_{\mathcal{C}'}(f) = T^{\mathcal{C}}_{\mathcal{C}'} \cdot M^{\mathcal{B}}_{\mathcal{C}}(f) \cdot \left(T^{\mathcal{B}}_{\mathcal{B}'}\right)^{-1}$.

Beweis: $\left(T^{\mathcal{B}}_{\mathcal{B}'}\right)^{-1} = T^{\mathcal{B}'}_{\mathcal{B}}$

Rechte Seite:
$M^{\mathcal{C}}_{\mathcal{C}'}(id_W) \cdot M^{\mathcal{B}}_{\mathcal{C}}(f) \cdot M^{\mathcal{B}'}_{\mathcal{B}}(id_V) =$
linke Seite:
$= M^{\mathcal{B}'}_{\mathcal{C}'}(f)$ nach 3.82 und 3.83.

□

Beispiel 3.89.
Betrachte die Basis $\mathcal{B} = (v_1, v_2)$ von $\mathbb{R}^2$ mit $v_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ -3 \end{pmatrix}$, und die kanonische Basis $\mathcal{K} = (e_1, e_2)$ mit $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
Was ist $T^{\mathcal{K}}_{\mathcal{B}}$? Habe $T^{\mathcal{B}}_{\mathcal{K}} = \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix}$.
$T^{\mathcal{K}}_{\mathcal{B}} = \left(T^{\mathcal{B}}_{\mathcal{K}}\right)^{-1} = \frac{1}{-7}\begin{pmatrix} -3 & -1 \\ -1 & 2 \end{pmatrix} = \frac{1}{7}\begin{pmatrix} 3 & 1 \\ 1 & -2 \end{pmatrix}$.
Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um $(0, 0)$ um den Winkel α. Berechne $M^{\mathcal{B}}_{\mathcal{B}}(f)$!
Es ist $M^{\mathcal{B}}_{\mathcal{B}}(f) = T^{\mathcal{K}}_{\mathcal{B}} \cdot M^{\mathcal{K}}_{\mathcal{K}}(f) \cdot T^{\mathcal{B}}_{\mathcal{K}}$.
Es ist $M^{\mathcal{K}}_{\mathcal{M}}(f) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ (3.6)

also nach oben:
$M_{\mathcal{B}}^{\mathcal{B}}(f) = \frac{1}{7}\begin{pmatrix} 3 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix} = \begin{pmatrix} \cos\alpha - \frac{1}{7}\sin\alpha & \frac{10}{7}\sin\alpha \\ -\frac{5}{7}\sin\alpha & \cos\alpha + \frac{1}{7}\sin\alpha \end{pmatrix}.$

f. Rang von Matrizen

K Körper, alle VRe seien endlich dimensional.

Definition 3.90. (Rang)
Sei $f : V \to W$ eine lineare Abbildung.
Dann heißt $rk(f) := \dim(im(f))$ der **Rang** von f.

Lemma 3.91.
Seien $f : U \to V$, und $g : V \to W$ lineare Abbildungen zwischen endlich-dimensionalen K-Vektorräumen.

(a) $rk(g \circ f) \leqq \min\{rk(f), rk(g)\}$.

(b) *g ist injektiv* $\Rightarrow rk(g \circ f) = rk(f)$.

(c) *f ist surjektiv* $\Rightarrow rk(g \circ f) = rk(g)$.

Beweis:

(a) Da die Abbildung der Basisvektoren der Ausgangsmenge ein Erzeugendensystem des Bildes einer Abbildung sind, ist die Dimension des Bildes stets kleiner oder gleich der Dimension der Ausgangsmenge. Damit gilt $rk(g \circ f) \leqq rk(f)$, da das Bild von f die Ausgangsmenge der Abbildung g ist (in $g \circ f$).

Außerdem gilt $rk(g \circ f) \leqq rk(g)$, da die Ausgangsmenge von g (in $g \circ f$) höchstens V sein kann und damit die Dimension des Bildes von $g \circ f$ nicht größer sein kann als die Dimension des Bildes von g.

$\Rightarrow rk(g \circ f) \leqq \min\{rk(f), rk(g)\}$.

(b) Sei g injektiv. $\Rightarrow \dim(im(g)) = \dim(V) \Rightarrow \dim(im(g \circ f)) = \dim(im(f)) \Rightarrow rk(g \circ f) = rk(f)$.

(c) Sei f surjektiv. $\Rightarrow$ für alle $v \in V$ gibt es ein $u \in U$ mit $f(u) = v \Rightarrow$ $im(g \circ f) = im(g) \Rightarrow \dim(im(g \circ f)) = \dim(im(g)) \Rightarrow rk(g \circ f) = rk(g)$

□

Satz 3.92. *(Rangsatz)*
Sei $f : V \to W$ eine lineare Abbildung, sei $r := rk(f)$.
Dann gibt es eine Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V und eine Basis $\mathcal{C} = (w_1, \ldots, w_n)$ von W mit $f(v_j) = \begin{cases} w_j & \text{für } 1 \leqq j \leqq r \\ 0 & \text{für } r+1 \leqq j \leqq n \end{cases}$

Also $M^{\mathcal{B}}_{\mathcal{C}}(f) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$. *(*)*

Beweis:
Sei $(w_1, \ldots, w_r)$ eine Basis von $im(f)$. Wähle $v_j \in V$ mit $f(v_j) = w_j$ $(j = 1, \ldots, r)$.
Sei $\mathcal{U} := span(v_1, \ldots, v_r)$, behaupte $V = U \oplus \ker(f)$.
Sei $v \in V$, dann ist $f(v) = \sum_{i=1}^{r} a_i w_i$ mit geeigneten $a_1, \ldots, a_r \in K$. Also ist $f(v - \sum_{i=1}^{r} a_i v_i) =$ $f(v) - \sum_{i=1}^{r} a_i f(v_i) = 0$ also $v = \underbrace{\sum_{s=1}^{r} a_i v_i}_{\in \mathcal{U}} + \underbrace{\left(v - \sum_{i=1}^{r} a_i v_i\right)}_{\in \ker(f)}$.

$\mathcal{U} \cap \ker(f) = \{0\}$, denn $u = \sum_{i=1}^{r} a_i v_i \in \ker(f) \cap \mathcal{U}$
$\Rightarrow 0 = f(u) = \sum_{i=1}^{r} a_i \underbrace{f(v_i)}_{=w_i} \Rightarrow$ (da $w_1, \ldots, w_r$ linear unabhängig) $a_1 = \ldots = a_r = 0 \Rightarrow$ $u = 0$.

Sei $(v_{r+1}, \ldots, v_n)$ eine Basis von $\ker(f)$, setze $\mathcal{B} := (v_1, \ldots, v_r, v_{r+1}, \ldots, v_n)$.
$\mathcal{B}$ ist Basis von V wegen $V = \mathcal{U} \oplus \ker(f)$.
Wähle $w_{r+1}, \ldots, w_m \in W$, so dass $\mathcal{C} := (w_1, \ldots, w_r, w_{r+1}, \ldots, w_m)$ eine Basis von W ist. Nach Konstruktion haben $\mathcal{B}$ und $\mathcal{B}$ die gewünschte Eigenschaft.

□

Korollar 3.93.
Sei $A \in M_{m \times n}(K)$, sei $r := rk(F_A)$. Dann gibt es reguläre Matrizen $S \in GL_n(K)$, $T \in GL_m(K)$, so dass $T^{-1}AS = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$ *ist.* *(siehe (*))*

Beweis:
zur linearen Abbildung $F_A : K^n \to K^m$, $F_A(x) = Ax$, wähle Basin $\mathcal{B}$ von K^n und $\mathcal{C}$

von K^m, so dass $M^{\mathcal{B}}_{\mathcal{C}}(F_A) = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$ (3.92)

$M^{\mathcal{B}}_{\mathcal{C}}(F_A) = T^{K^n}_{\mathcal{C}} \cdot A \cdot T^{\mathcal{B}}_{K^n}$.
Setze $S := T^{\mathcal{B}}_{K^n}$ und $T := T^{\mathcal{C}}_{K^m}$.

□

Beispiel 3.94.
Sei $A := \begin{pmatrix} 2 & -1 & 1 \\ -4 & 2 & -2 \end{pmatrix} \in M_{2\times 3}(\mathbb{R})$.

Wie findet man $S \in GL_3(\mathbb{R})$, $T \in GL_2(\mathbb{R})$ mit $T^{-1}AS = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$?

Folge dem Beweis von 3.92 (für $f = F_A : \mathbb{R}^3 \to \mathbb{R}^2$):

Es ist $im(F_A) = span\left(\begin{pmatrix} 2 \\ -4 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \end{pmatrix}\right)$, also $rk(F_A) = 1$, und $w_1 := \begin{pmatrix} 2 \\ -4 \end{pmatrix}$ ist eine Basis von $im(F_A)$. Ergänze w_1 zu Basis $\mathcal{C} = (w_1, w_2)$ von $\mathbb{R}^2$, etwa durch $w_2 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Setze $v_1 := \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. Es ist $\ker(F_A) = \left\{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} : 2x_1 - x_2 + x_3 = -4x_1 + 2x_2 - 2x_3 = 0\right\}$
Es ist $\dim(\ker(F_A)) = 3 - 1 = 2$. Wir können etwa (v_2, v_3) als Basis von $\ker(F_A)$ nehmen mit $v_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$. $\mathcal{B} := (v_1, v_2, v_3)$.

$$M^{\mathcal{B}}_{\mathcal{C}}(F_A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = T^{\mathcal{B}}_{\mathcal{C}} \cdot A \cdot T^{\mathcal{B}}_{K^3} = \underbrace{\left(T^{\mathcal{C}}_{K^2}\right)}_{=:T} \cdot A \cdot \underbrace{\left(T^{\mathcal{B}}_{K^3}\right)}_{=:S}.$$

$$T := \begin{pmatrix} 2 & 0 \\ -4 & 1 \end{pmatrix}, S := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Definition 3.95.
Sei $A = (a_{ij}) \in M_{m\times n}(K)$.

(a) Sei $S_j(A) := \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^m$ $(j = 1, \dots, n)$

sei $Z_i(A) := \begin{pmatrix} a_{i1} \\ \vdots \\ a_{in} \end{pmatrix} \in K^n \ (i = 1, \dots, m)$

(b) $span_S(A) := span((S_1(A), \dots, S_n(A)) \subset K^m$,
$span_Z(A) := span(Z_1(A), \dots, Z_m(A)) \subset K^n$.

(c) $srk(A) := \dim span_S(A)$, (Spaltenrang)
$zrk(A) := \dim span_Z(A)$ (Zeilenrang)

Bemerkung 3.96.

1. $span_S(A) = im(F_A)$.
   Insbesondere ist $srk(A) = rk(F_A)$.

2. $span_Z(A) = span_S(A^t)$, also $zrk(A) = srk(A^t)$.

Lemma 3.97.
Sei $A \in M_{m\times n}(K)$, sei $B \in GL_m(K)$, $C \in GL_n(K)$.

(a) $span_Z(BA) = span_Z(A)$, $span_S(AC) = span_S(A)$.

(b) $zrk(BAC) = zrk(A)$, $srk(BAC) = srk(A)$.

Beweis:
Zeige zunächst die Spaltenaussagen. Haben die linearen Abbildungen $K^n \overrightarrow{F_C} K^n \overrightarrow{F_A} K^m \overrightarrow{F_B} K^m$ und F_B, F_C sind Isomorphismen. Es ist $span_S(AC) = im(F_{AC}) = im(F_A \circ F_C) = im(F_A) = span_S(A)$ (nach Lemma 3.91 (c))
Ebenso:
$srk(BAC) = rk(F_B \circ F_A \circ F_C) = rk(F_A) = srk(A)$. (nach Lemma 3.91 (b), (c))

Die Zeilenaussagen erhält man durch Transponieren aus den Spaltenaussagen.
□

Definition und Satz 3.98. *(Rang von Matrizen)*
*Für jede Matrix $A \in M_{m\times n}(K)$ ist $zrk(A) = srk(A)$. Man nennt diese Zahl den **Rang** von A, $rk(A)$.*

Beweis:
Nach 3.93 gibt es $S \in GL_n(K)$, $T \in GL_m(K)$ mit $T^{-1}A = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$ mit $r = rk(F_A) = srk(A)$. Wegen $r = zrk(T^{-1}AS) = zrk(A)$ folgt die Behauptung.

□

Korollar 3.99.
Für $A \in M_{m\times n}(K)$ sind äquivalent:

(i) $rk(A) = r$

(ii) $\exists S \in GL_n(K), T \in GL_m(K)$ *mit* $T^{-1}AS = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$.

Korollar 3.100.
Für $A \in M_n(K)$ (quadratisch) sind äquivalent:

(i) $rk(A) = n$

(ii) A ist regulär, d.h. $A \in GL_n(K)$

(iii) die Zeilen von A sind linear unabhängig

(iv) die Spalten von A sind linear unabhängig

Beweis:
(i) $\Rightarrow$ (ii)
Nach 6.10 $\exists S, T \in GL_n(K)$ mit $T^{-1}AS = I_n \Rightarrow A = TS^{-1} \in GL_n(K)$.

(ii) $\Rightarrow$ (i)
$A^{-1} \cdot A = I_n$, nun wieder 3.99.

□

Definition und Satz 3.101.
Für je zwei Matrizen $A, B \in M_{m\times n}(K)$ sind äquivalent:

(i) $rk(A) = rk(B)$

(ii) $\exists S \in GL_n(K), T \in GL_m(K)$ *mit* $B = T^{-1}AS$.

A und B heißen äquivalent, in Zeichen $A \sim B$, *falls (i) und (ii) gelten.*

Bemerkung: $\sim$ ist eine Äquivalenzrelation auf $M_{m\times n}(K)$.

Beweis:
(i) $\Rightarrow$ (ii)
Sei $r := rk(A) = rk(B)$.
Nach 3.99 $\Rightarrow \exists X, \widetilde{X} \in GL_n(K)$, $Y, \widetilde{Y} \in GL_m(K)$:
$Y^{-1}AX = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right) = \widetilde{Y}^{-1}B\widetilde{X}$.
$\Rightarrow B = (\widetilde{Y}Y^{-1}) \cdot A \cdot (X\widetilde{X}^{-1})$
Nimm $X\widetilde{X}^{-1} = S$ und $\widetilde{Y}Y^{-1} = T$.

□

Definition 3.102. (erweiterte Koeffizientenmatrix)
$Ax = u$, $A \in M_{m\times n}(K)$, $u \in K^m$

Die Matrix $(A, u) := \begin{pmatrix} a_{11} & \dots & a_{1n} & u_1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & u_m \end{pmatrix} \in M_{m\times(n+1)}(K)$ heißt die erweiterte Koeffizientenmatrix des Gleichungssystems $Ax = u$.

Es ist $rk(A, u) = rk(A)$ oder $rk(A, u) = a + rk(A)$.

Satz 3.103.

(a) Genau dann ist $Ax = u$ *lösbar (d.h.* $\exists x \in K^n$ *mit* $Ax = u$*), wenn* $rk(A, u) = rk(A)$ *ist.*

(b) Genau dann ist für festes A das System $Ax = u$ *für jedes* $u \in K^m$ *lösbar, wenn gilt:* $rk(A) = m$ *(*$\Leftrightarrow$ *Zeilen von A sind linear unabhängig).*

Beweis:

(a) $Ax = U$ lösbar $\Leftrightarrow u \in im(F_A) = span_S(A)$
$\Leftrightarrow span_S(A, u) = span_S(A) \Leftrightarrow rk(A, u) = rk(A)$.

(b) $\forall u \in K^m \; Ax = u$ lösbar $\Leftrightarrow F_A : K^n \to K^m$ surjektiv $\Leftrightarrow rk(A) = m$.

$\square$

g. Elementare Umformungen von Matrizen, Gauß-Algorithmus

Gegeben sei $A \in M_{m\times n}(K)$, $u \in K^m$.
Studiere das Lineare Gleichungssystem $Ax = u$, und seinen Lösungsraum $\mathcal{L}(A,u) = \{x \in K^n : Ax = u\}$.

Satz 3.104.
Ist $\mathcal{L}(A,u) \neq \emptyset$, so ist $\dim(\mathcal{L}(A,u)) = n - rk(A)$.

Beweis:
$\mathcal{L}(A,u) \neq \emptyset \Rightarrow T(\mathcal{L}(A,u)) = \mathcal{L}(A,0) = \ker(F_A)$.
Habe $\underbrace{\dim(\ker(F_A))}_{\dim(\mathcal{L}(A,u))} + \underbrace{\dim(im(F_A))}_{rk(A)} = n$ $\quad (F_A : K^n \to K^m;$ 3.44$)$

□

Definition 3.105.
Die Matrix A hat Zeilenstufenform (ZSF), wenn A so aussieht:

$$A = \begin{pmatrix} 0 & \dots & 0 & * & \dots & \sharp & \dots & \sharp & \dots & \sharp & \dots & \sharp \\ 0 & \dots & 0 & 0 & \dots & 0 & * & \dots & \sharp & \dots & \dots & \vdots \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \sharp \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \dots & 0 & * & \sharp & \dots & \vdots \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \dots & \vdots & 0 & * & \dots & \sharp \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \vdots & \ddots & \ddots & 0 \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & \dots & 0 \end{pmatrix}$$

mit $*$ = Element $\neq 0$ und $\sharp$ = beliebiges Element.
Also, falls es $1 \leqq k_1 < k_2 < \dots < k_r \leqq n$ gibt mit

(a) $a_{ij} = 0$ für $1 \leqq i \leqq r$, $1 \leqq j < k_i$

(b) $a_i, k_i \neq 0$ für $1 \leqq i \leqq r$

(c) $a_{ij} = 0$ für $r+1 \leqq i \leqq m$, alle $1 \leqq j \leqq n$.

Konstruktion 3.106.
Für solches A gilt $Z_1(A), \dots, Z_r(A)$ sind linear unabhängig und $rk(A) = r$. Wir können $\mathcal{L}(A, u)$ sofort angeben:

(1) Ist $u_i \neq 0$ für ein $i \in \{r+1, \dots, m\}$, so $\mathcal{L}(A, u) = \emptyset$.

(2) Sei $u_{r+1} = \dots = u_m = 0$. Wir können $x_j \in K$ für alle $j \in \{1, \dots, n\} \setminus \{k_1, \dots, k_r\}$ beliebig vorschreiben, und bestimmen zuerst x_{k_r} aus der r-ten Gleichung:
$a_{r,k_r} \cdot x_{k_r} \sum_{j > k_r} a_{rj} x_j = r_r$
dann $x_{k_{r-1}}$ aus der $(r-1)$-ten Gleichung, usw., bis man schließlich x_{k_1} aus der ersten Gleichung erhält.

Um ein beliebiges LGS zu lösen, bringt man es in ZSF. Dies wird wie folgt systematisiert:

Definition 3.107. (elementare Zeilenumformung)
Sei $A \in M_{m \times n}(K)$. Für $1 \leqq k, l \leqq m, k \neq l$ und $\lambda \in K$ sei

(a) $\pi_{kl}(A)$, (b) $q_{kl}^{\lambda}(A)$, (c) δ_k^{λ}

die Matrix, die aus A entsteht durch

(a) Vertauschen der k-ten und l-ten Zeile

(b) Addition des λ-fachen der l-ten Zeile zur k-ten Zeile

(c) Multiplikation der k-ten Zeile mit λ.

Eine **elementare Zeilenumformung** ist der Übergang von A zu einer von $\pi_{kl}(A)$, $q_{kl}^{\lambda}(A)$, $\delta_k^{\lambda}(A)$ $(\lambda \neq 0)$.

Bemerkung 3.108.
Für $1 \leqq k, l \leqq m$, $k \neq l$, sei $\Pi_{kl} = E_{kl} + E_{lk} + \sum_{i \neq k, l, i=1}^{m} E_{ii} \in M_m(K)$.

$\Pi^2 = I_m$. Insbesondere $\Pi_{kl} \in GL_m(K)$.
Weiter setze $Q_{kl}(\lambda) := I_m + \lambda E_{kl}$. Habe $Q_{kl}(\lambda) \cdot Q_{kl}(\mu) = Q_{kl}(\lambda + \mu)$ insbesondere auch $Q_{kl}(\lambda) \in GL_m(K)$. Setze noch $D_k(\lambda) := diag(1, \dots, \underbrace{\lambda}_{k-te \text{ Stelle}}, \dots, 1) \in GL_m(K)$

Lemma 3.109.
Seien $1 \leqq k, l \leqq m$, $k \neq l$, sei $\lambda \in K$.
Für $A \in M_{m\times n}(K)$ ist
$\pi_{kl}(A) = \Pi_{kl} \cdot A$
$q_{kl}(A) = Q_{kl}(\lambda) \cdot A$
$\delta_k^\lambda(A) = D_k(\lambda) \cdot A$

Insbesondere:
Elementare Zeilenumformungen lassen $span_Z(A)$ und $rk(A)$ unverändert.

Beweis:
3.97 (a).

□

Satz 3.110. *(Gauß-Algorithmus)*
Jede Matrix $A \in M_{m\times n}(K)$ kann durch eine endliche Folge von (elementaren Zeilen-)Transformationen π_{kl}, q_{kl}^λ auf ZSF $\widetilde{A}$ gebracht werden. Dabei ist die Zahl der von Null verschiedenen Zeilen von A gleich $rk(A)$.

Beweis:
Die erste von $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ verschiedene Spalte, sei die k_1-te Spalte. Durch eine Zeilenvertauschung erreiche $\widetilde{a_{1,k_1}} \neq 0$ für die neue Matrix $\widetilde{A} = (\widetilde{a_{ij}})$. Erzeuge nun Nullen an den Stellen (i, k_1), $2 \leqq i \leqq m$, durch Addition eines geeigneten Vielfachen von Z_1 zu Z_i. Führe diesen Schritt solange aus, bis ZSF.

□

Korollar 3.111.
Zu jeder Matrix $A \in M_{m\times n}(K)$ gibt es $S \in GL_m(K)$, so dass SA Zeilenstufenform hat.

Beweis:
Ein Algorithmus zum Finden eines solchen S steht im Beweis von 3.110.

□

Bemerkungen 3.112.

1. Bringt man A durch elementare Zeilentransformationen auf ZSF, so bilden die von Null verschiedenen Zeilen von $\widetilde{A}$ eine Basis von $span_Z(A)$.
   $\rightsquigarrow$ Algorithmus: Input: Menge von Vektoren, Output: Basis ihres Spans.

2. Das Verfahren löst beliebige lineare Gleichungssysteme $Ax = u$.
   Bringe A durch elementare Zeilentransformationen π_{ij}, q_{kl}^{λ} auf ZSF $\widetilde{A}$ und führe jede dieser Transformationen auch mit u durch, erhalte $\widetilde{u}$.
   Das neue LGS $\widetilde{A}x = \widetilde{u}$ hat dieselben Lösungen wie $Ax = u$.
   Denn $\exists S \in GL_m(K)$ mit $\widetilde{A} = SA$, $\widetilde{u} = Su$. Das System $\widetilde{A}x = \widetilde{u}$ können wir sofort lösen, siehe 3.106.
   Die Matrix S erhält man explizit dadurch, dass man die Transformationen auf eine weitere Matrix anwendet, beginnend mit I_n.
   Wendet man auch noch δ_k^{λ} an, so lässt sich erreichen, dass an den Stellen $*$ in der ZSF 3.105 jeweils 1 steht.
   Für die konkrete Rechnung ist es oft praktisch, durch weitere q_{kl}^{λ} zu erreichen, dass in den Spalten $k_1, \dots, k_r$ auch über den Elementen $*$ nur Nullen stehen.

3. Beispiel:
   $A = \begin{pmatrix} 0 & -1 & 5 & 3 \\ 3 & 4 & 16 & -2 \\ -2 & -3 & -9 & 3 \end{pmatrix} \in M_{3\times 4}(\mathbb{R})$, sei $u = (u_1, u_2, u_3) \in \mathbb{R}^3$. Löse das LGS $Ax = u$.

   $$\begin{pmatrix} 0 & -1 & 5 & 3 \\ 3 & 4 & 16 & -2 \\ -2 & -3 & -9 & 3 \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

   $q_{23}(1)$

   $$\begin{pmatrix} 0 & -1 & 5 & 3 \\ 1 & 1 & 7 & 0 \\ -2 & -3 & -9 & 3 \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 + u_3 \\ u_3 \end{pmatrix}$$

   π_{12}

   $$\begin{pmatrix} 0 & 1 & 7 & 0 \\ 0 & -1 & 5 & 3 \\ -2 & -3 & -9 & 3 \end{pmatrix}\begin{pmatrix} u_2 + u_3 \\ u_1 \\ u_3 \end{pmatrix}$$

$q_{31}(2)$

$$\begin{pmatrix} 1 & 1 & 7 & 0 \\ 0 & -1 & 5 & 3 \\ 0 & -1 & 5 & 3 \end{pmatrix} \begin{pmatrix} u_2 + u_3 \\ u_1 \\ 2u_2 + 3u_3 \end{pmatrix}$$

$q_{32}(-1)$

$$\begin{pmatrix} 1 & 1 & 7 & 0 \\ 0 & -1 & 5 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} u_2 + u_3 \\ u_1 \\ -u_1 + 2u_2 + 3u_3 \end{pmatrix}$$

$q_{12}(1)$

$$\begin{pmatrix} 1 & 0 & 12 & 3 \\ 0 & -1 & 5 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} u_1 + u_2 + u_3 \\ u_1 \\ -u_1 + 2u_2 + 3u_3 \end{pmatrix}$$

Wir lesen ab:
1) Ist $-u_1 + 2u_2 + 3u_3 \neq 0$, so $\mathcal{L}(A, u) = \emptyset$.

2) Sei $-u_1 + 2u_2 + 3u_3 = 0$. Dann können wir x_3, x_4 frei wählen und erhalten
$x_1 = u_1 + u_2 + u_3 - 12x_3 - 3x_4$
$x_2 = -u_1 + 5x_3 + 3x_4$, also

$$\mathcal{L}(A, u) = \begin{pmatrix} u_1 + u_2 + u_3 \\ -u_1 \\ 0 \\ 0 \end{pmatrix} + span \left\{ \begin{pmatrix} -12 \\ 5 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 3 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Gleichzeitig erfahren wir $rk(A) = 2$, und $\begin{pmatrix} 1 \\ 0 \\ 12 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 5 \\ 3 \end{pmatrix}$ sind Basis von $span_Z(A)$.

$S \in GL_3$, $SA = \widetilde{A}$?

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

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

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

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

Bemerkung 3.113.
Der Gauß-Algorithmus liefert insbesondere auch zu jeder Matrix $A \in M_{m\times n}(K)$ eine Basis von $\ker(F_A)$, $F_A : K^n \to K^m$. Im Beispiel 3.112 z.B. war $\begin{pmatrix} -12 \\ 5 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 3 \\ 0 \\ 1 \end{pmatrix}$ eine Basis von $\ker(F_A)$.

Bemerkung 3.114.
Es ist bei den elementaren Zeilenumformungen **nicht** erlaubt, für zwei Indizes $k \neq l$ gleichzeitig die Transformationen $Z'_k = Z_k + aZ_l$, $Z'_l := Z_l + bZ_k$ vorzunehmen.
Betrachte folgendes Beispiel:
Sei $A = \begin{pmatrix} 1 & 2 & 1 \\ -2 & -4 & 0 \end{pmatrix} \in M_{2\times 3}(\mathbb{R})$.
Habe $rk(A) = 2$. Die nicht erlaubte Operation $\begin{pmatrix} 1 & 2 & 1 \\ -2 & -4 & 0 \end{pmatrix}$ $Z'_1 := Z_1 + \frac{1}{2}Z_2$, $Z'_2 := Z_2 + 2Z_1$.
$\Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix} \to$ falscher Rang!

Bemerkung 3.115.
Seien $U = span(u_1, \dots, u_r)$, $W = span(w_1, \dots, w_s)$ Untervektorräume von K^n. Wie bestimmt man eine Basis von $U \cap W$.

Es genügt, U und W als Lösungsraum von je einem homogenen linearen Gleichungssystem zu schreiben:
dann ist $U \cap W$ der Lösungsraum des zusammengefügten linearen Gleichungssystems.

Sei $U = span(u_1, \dots, u_r)$. Bilde die $r \times n$-Matrix A mit den Zeilen $u_1^t, \dots, u_r^t$. Mit dem Gauß-Algorithmus findet man eine Basis $(v_1, \dots, v_s)$ von $\ker(F_A)$. Sei $B \in M_{s\times n}(K)$ die Matrix mit den Zeilen $v_1^t, \dots, v_s^t$, dann ist $\ker(F_B) = U$.
Denn $0 = u_i^t \cdot v_j = v_j^t \cdot u_i$ $(i = 1, \dots, r; j = 1, \dots, s)$
$\Rightarrow u_i \in \ker(F_B) \Rightarrow U \subset \ker(F_B)$. Andererseits ist $\dim(U) = rk(A)$ und $rk(B) = s = \dim(\ker(F_A)) = n - rk(A) \Rightarrow \dim(U) = n - s = n - rk(B) = \dim(\ker(F_B))$.
Also ist $U = \ker(F_B)$.

Beispiel 3.116.
$U := K\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + K\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \subset K^3$.
Bilde $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, bestimme Basis von $\ker(F_A)$.
Finde: $\ker(F_A) = K\begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$. Setze $B := (-1, 1, 1)$, dann ist also $U = \ker(F_B)$.

Bemerkung 3.117.
Sei $A \in M_n(K)$.
Ist A regulär? Falls ja, wie finde ich A^{-1}.
Antwort:
Mache 2 Spalten von Matrizen M_1, M_2, beginne mit $M_1 = A$ und $M_2 = I_n$.
Durch elementare Zeilentransformationen bringe M_1 auf ZSF, jede dieser Zeilentransformationen wird auch an M_2 ausgeführt.
Ist $rk(\widetilde{A}) = rk(A) < n$, so ist A nicht regulär. Ist $rk(\widetilde{A}) = rk(A) = n$, so ist A regulär, und $\widetilde{A} = \begin{pmatrix} d_1 & \dots & * \\ \vdots & \ddots & \vdots \\ 0 & \dots & d_n \end{pmatrix}$ mit $d_i \neq 0$.
Nach Linksmultiplikation mit der $diag\left(\frac{1}{d_1}, \dots, \frac{1}{d_n}\right)$ erreiche $d_1 = \ldots = d_n = 1$. Durch weitere elementare Zeilentransformationen $q_{ij}(\lambda)$ führt man M_1 schließlich in I_n über. Jetzt ist $M_2 = A^{-1}$, denn $\exists S \in GL_n(K)$ mit $SA = I$ und $SI = M_2 \Rightarrow S = A^{-1}$.

Beispiel 3.118.
Wir betrachten die Matrix $A := \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \in M_3(\mathbb{R})$.

$$\begin{array}{cccccccl} 1 & 2 & 0 & 1 & 0 & 0 & \\ 2 & 1 & 2 & 0 & 1 & 0 & q_{21}(-2) \\ 0 & 2 & 1 & 0 & 0 & 1 & \end{array}$$

$$\begin{array}{cccccc} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & -3 & 2 & -2 & 1 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 \end{array} \quad q_{23}(2)$$

$$\begin{array}{cccccc} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 4 & -2 & 1 & 2 \\ 0 & 2 & 1 & 0 & 0 & 1 \end{array} \quad q_{32}(-2)$$

$$\begin{array}{cccccc} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 4 & -2 & 1 & 2 \\ 0 & 0 & -7 & 4 & -2 & -3 \end{array} \quad q_{12}(-2),\ \delta_3(\tfrac{-1}{7})$$

$$\begin{array}{cccccc} 1 & 0 & -8 & 5 & -2 & -4 \\ 0 & 1 & 4 & -2 & 1 & 2 \\ 0 & 0 & 1 & \frac{-4}{7} & \frac{2}{7} & \frac{3}{7} \end{array} \quad q_{13}(8),\ q_{23}(-4)$$

$$\begin{array}{cccccc} 1 & 0 & 0 & \frac{3}{7} & \frac{2}{7} & -\frac{4}{7} \\ 0 & 1 & 0 & \frac{2}{7} & -\frac{1}{7} & \frac{2}{7} \\ 0 & 0 & 1 & -\frac{4}{7} & \frac{2}{7} & \frac{3}{7} \end{array}$$

Also ist $A^{-1} = \frac{1}{7}\begin{pmatrix} 3 & 2 & -4 \\ 2 & -1 & 2 \\ -4 & 2 & 3 \end{pmatrix}$.

Bemerkung 3.119.
Statt elementarer ZT kann man ebenso elementare Spaltentransformationen (ST) betrachten:

- Addition eines Vielfachen einer Spalte zu einer anderen Spalte,
- Vertauschen von zwei Spalten,
- Multiplikation einer Spalte mit einem $\lambda \neq 0$, $\lambda \in K$.

Diese entsprechen jeweils der Multiplikation von $A \in M_{m\times n}(K)$ mit einer geeigneten Matrix aus $GL_n(K)$ von rechts. Jede Matrix kann durch elementare Spaltentransformationen in Spaltenstufenform gebracht werden.
Der Spaltenspan $span_S$ ändert sich bei elementaren Spaltentransformationen nicht.

Zur Bestimmung von $rk(A)$ kann man elementare ZT und elementare ST beliebig (und abwechselnd) vornehmen.

Beim Lösen eines LGS beschränkt man sich meist auf ZT, da man durch ST auch die Unbekannten ändert.
Zur Bestimmung von A^{-1} kann man statt mit ZT auch mit ST arbeiten, aber nicht beides gleichzeitig:
$SAT = I_n \not\Rightarrow ST = SI_nT$ ist die Inverse von A!

Beispiel 3.120.
Gegeben sei $A \in M_{m\times n}(K)$, gesucht seien $S \in GL_m(K)$, $T \in GL_n(K)$ mit $SAT = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$ (und $r = rk(A)$), siehe Beispiel 3.94.

Lösung:
Mache drei Spalten von Matrizen, genannt M_1, M_2, M_3, beginne mit $M_1 = A$, $M_2 = I_m$, $M_3 = I_n$.

- Mache elementare ZT an M_1 und $M_2 \rightsquigarrow M_1$ in ZSF.
- Spaltenvertauschungen an M_1 und $M_3 \rightsquigarrow \left(\begin{array}{cc|cc} c_1 & * & * & * \\ 0 & c_r & * & * \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$, $c_1, \ldots, c_r \neq 0$.
- elementare ST an M_1 und $M_3 \rightsquigarrow \left(\begin{array}{cc|cc} c_1 & 0 & 0 & 0 \\ 0 & c_r & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$
- Multiplikation mit Diagonalmatrix von links in M_1, M_2.
- Dann ist jetzt $SAT = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$ mit $S = M_2$, $T = M_3$.

4. Determinanten

a. Polynome

Konstruktion 4.1. (Polynom)
Sei A ein kommutativer Ring. Ein **Polynom** (in der Variablen t) über A ist ein formaler Ausdruck
$f = a_m t^m + a_{m-1} t^{m-1} + \ldots a_1 t + a_0$
mit $m \in \mathbb{N}_0$, $a_0, \ldots, a_m \in A$. Wir schreiben formal auch $f = \sum\limits_{i \geqq 0} a_i t^i$, indem wir $a_i = 0$ für $i > m$ setzen.
Zwei Polynome $f = \sum\limits_{i \geqq 0} a_i t^i$ und $g = \sum\limits_{i \geqq 0} b_i t^i$ heißen gleich, falls $a_i = b_i$ für alle $i \geqq 0$ ist.

Die Menge $A[t]$ aller Polynome über A (in t) wird zu einem kommutativen Ring durch die Definitionen

$$\left(\sum_{i \geqq 0} a_i t^i\right) + \left(\sum_{i \geqq 0} b_i t^i\right) := \sum_{i \geqq 0} (a_i + b_i) t^i$$
$$\left(\sum_{i \geqq 0} a_i t^i\right) \cdot \left(\sum_{j \geqq 0} b_j t^j\right) := \sum_{k \geqq 0} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i}\right) t^k$$

(genauer: $A[t]$ ist kommutativer Ring mit Eins)
(Hinweis zum Produkt: $\left(\sum\limits_{i \geqq 0} a_i t^i\right) \cdot \left(\sum\limits_{j \geqq 0} b_j t^j\right) = \sum\limits_{i,j \geqq 0} a_i b_j t^{i+j}$)
Die Null in $A[t]$ ist das Nullpolynom 0, die Eins ist das „konstante“ Polynom 1.
Ist $f = a_m t^m + \ldots + a_1 t + a_0$ mit $a_m \neq 0$, so heißt $m := \deg(f)$ der **Grad** von f, und a_m heißt der **Leitkoeffizient** von f. Man definiert $\deg(0) := -\infty$ (das Polynom 0 hat keinen Leitkoeffizienten).

Konstruktion 4.2.
Ab jetzt sei $A = K$ ein Körper. Dann ist $K[t]$ auch ein K-VR, eine Basis dieses VRs ist z.B. $(t^i)_{i \geqq 0} = (1, t, t^2, t^3, \ldots)$.

Für $f = \sum\limits_{i \geqq 0} a_i t^i \in K[t]$ und für $c \in K$ schreibt man $f(c) := \sum\limits_{i \geqq 0} a_i c^i \in K$: man „setzt“ also c für die Variable t „ein “. Ist $f(c) = 0$, so heißt c eine Nullstelle von f.

Es gilt:
$(f + g)(c) = f(c) + g(c)$
$(f \cdot g)(c) = f(c) \cdot g(c)$
$1(c) = 1$.

Also ist die Abbildung $ev_c : K[t] \to K$, $f \mapsto f(c)$ ein Ringhomomorphismus.
(ev_c heißt die **Auswertungs-** oder **Evaluationsabbildung** in $c \in K$)

Satz 4.3.
Seien $f, g \in K[t]$

(a) $\deg(f+g) \leqq \max\{\deg(f), \deg(g)\}$;
ist $\deg(f) \neq \deg(g)$, *so gilt die Gleichheit.*

(b) $\deg(fg) = \deg(f) + \deg(g)$

(c) der Ring $K[t]$ ist nullteilerfrei.

Beweis:
$f = a_m t^m + \dots$
$g = b_n t^n + \dots$
mit $a_m, b_n \neq 0$, die ... bedeuten jeweils Terme von kleinerem Grad.

(a) klar.

(b) $fg = \underbrace{a_m b_n}_{\neq 0} t^{m+n} + \dots\dots$

Das beweist (b), falls $f \neq 0$, $g \neq 0$. Ist $f = 0$ oder $g = 0$, so ist (b) ebenfalls richtig.

(c) folgt aus (b): $f, g \neq 0 \Rightarrow \deg(f), \deg(g) \geqq 0 \Rightarrow \deg(fg) \geqq 0 \Rightarrow fg \neq 0$.

□

Satz 4.4. *(Polynomdivision mit Rest)*
Seien $f, g \in K[t]$, $g \neq 0$. Dann gibt es Polynome $q, r \in K[t]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.
Dadurch sind q und r zudem eindeutig bestimmt.

Beweis:
Existenz: Induktion nach $\deg(f)$

Ist $\deg(f) < \deg(g)$, so setze $q := 0$ und $r := f$. Sei also $\deg(f) = m$, $\deg(g) = n$ mit $m \geqq n$, sei $f = a_m t^m + \ldots + a_0$, $g = b_n t^n + \ldots + b_0$.
Sei $\widetilde{f} := f - \frac{a_m}{b_n} t^{m-n} \cdot g = (a_m t^m + \ldots - \left(\frac{a_m}{b_n} \cdot b_n t^m + \ldots\right)$
Es ist $\deg(\widetilde{f}) < \deg(f) = m$. Nach Induktion gibt es $q_1, r_1 \in K[t]$ mit $\widetilde{f} = q_1 g + r_1$ und $\deg(r_1) < \deg(g)$. Also ist $f = \widetilde{f} + \frac{a_m}{b_n} t^{m-n} \cdot g = \underbrace{\left(q_1 + \frac{a_m}{b_n} t^{m-n}\right)}_{:=q} \cdot g + \underbrace{r_1}_{:=r}$.

Eindeutigkeit:
Sei $f = qg + r = \widetilde{q}g + \widetilde{r}$ mit $q, \widetilde{q}, r, \widetilde{r} \in K[t]$, $\deg(r), \deg(\widetilde{r}) < \deg(g)$.
$\Rightarrow (q - \widetilde{q})g = \widetilde{r} - r$ hat Grad kleiner $\deg(g)$. Daraus folgt $q - \widetilde{q} = 0$, also $q = \widetilde{q}$, also auch $r = \widetilde{r}$.

□

Bemerkung 4.5.
Der Beweis gab einen Algorithmuis zum Finden von q und r. Beispiel: ($K = \mathbb{R}$)
$f := t^4 - 2t^3 - 7$, $g := t^2 + 3$
$\Rightarrow q = t^2 - 2t - 3$, $r = 6t + 2$.

Korollar 4.6.
Sei $f \in K[t]$.

(a) *Ist $c \in K$ mit $f(c) = 0$, so gibt es $g \in K[t]$ mit $f = (t - c) \cdot g$.*

(b) *Ist $f \neq 0$, so hat f höchstens* $\deg(f)$ *viele Nullstellen in K.*

Beweis:

(a) Dividiere f durch $t - c$ mit Rest, erhalte $f = q \cdot (t - c) + r$ mit $\deg(r) \leqq 0$. Einsetzen von c gibt $0 = f(c) = r$.

(b) Induktion nach $n := \deg(f)$. Ist $n \leqq 0$: klar.
Sei $n \geqq 1$, sei c eine Nullstelle von f. Dann ist $f = (t - c)g$ mit $\deg(g) = n - 1$. Nach Induktion hat g höchstens $n - 1$ Nullstellen. Jede Nullstelle $b \neq c$ ist eine Nullstelle von g: $0 = f(b) = \underbrace{(b - c)}_{\neq 0} \cdot g(b) \Rightarrow g(b) = 0$.

□

Bemerkung 4.7.

1. 4.6 (a) sagt: der Kern von $ev_c : K[t] \to K$ ist $K[t] \cdot (t-c) := \{g\dot{(}t-c) : g \in K[t]\}$ das von $t-c$ erzeugte Ideal.

2. Jedes $f \in K[t]$ definiert eine Abbildung $\widetilde{f} : K \to K$, $\widetilde{f} : c \mapsto f(c)$. Eine solche Abbildung heißt eine **Polynomabbildung**.
   Verschiedene Polynome können dieselbe Polynomabbildung induzieren: sei K ein endlicher Körper, sei $f := \prod\limits_{a \in K}(t-a) \in K[t]$. Es ist $f(c) = 0\ \forall c \in K$, also $\widetilde{f} \equiv 0$, obwohl $f \neq 0$ ist. ($\deg(f) = |K|$)
   Andererseits: ist $|K| = \infty$, so gilt: $f \neq g \Rightarrow \widetilde{f} \neq \widetilde{g}$.
   Denn: $\widetilde{f} = \widetilde{g} \Rightarrow f - g \equiv 0$. Wegen $|K| = \infty$ folgt $f - g = 0$ aus 4.6 (b).

b. Vorzeichen von Permutationen

S_n = Gruppe aller Permutationen von $\{1, \dots, n\}$

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

Neutrales Element: $\sigma = id = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$

Definition 4.8.

(a) Für $\sigma \in S_n$ sei $Fix(\sigma) := \{i \in \{1, \dots, n\} : \sigma(i) = i\}$.

(b) $\sigma \in S_n$ heiße eine **Transpostition**, falls $|Fix(\sigma)| = n - 2$

(c) Für $1 \leqq i, j \leqq n$, $i \neq j$, sei τ_{ij} die Transposition, die i und j vertauscht, also

$$\tau(k) = \begin{cases} j & k = 1 \\ i & k = j \\ k & k \notin \{i, j\} \end{cases}$$

Bemerkung 4.9.
Die Transpositionen in S_n sind genau die τ_{ij}, $1 \leqq i, j \leqq n$. Es gibt also genau $\binom{n}{2} = \frac{1}{2}n(n-1)$ Stück.

Satz 4.10.
Jedes $\sigma \in S_n$ ist Produkt von höchstens $n - 1$ Transpositionen.

Beweis: (durch absteigende Induktion nach $|Fix(\sigma)|$):
Durch Induktion zeigen wir für $\sigma \neq id$: σ ist Produkt von höchstens $n - 1 - r$ Transpositionen mit $r := |Fix(\sigma)|$.

Satz ist richtig für $\sigma = id$ (ist Produkt von 0 Transpositionen).
Für $\sigma \neq id$ ist $|Fix(\sigma)| \leqq n - 2$. Für $|Fix(\sigma)| = n - 2$ ist σ eine Transposition. Sei also $r := |Fix(\sigma)| < n - 2$, sei die Aussage für $r + 1, \dots, n - 2, n - 1, n$ schon bewiesen. Wähle i mit $\sigma(i) \neq i$, setze $\tau := \tau_{\sigma(i),i}$ und $\rho := \tau \circ \sigma$. Es ist $\rho(i) = i$ und $\rho(j) = \sigma(j)$ für alle $j \notin \{i, \sigma^{-1}(i)\}$. Also ist $|Fix(\rho)| \geqq r + 1$. Nach Induktion ist also ρ Produkt von $\leqq n - 1 - (r + 1) = n - r - 2$ Transpositionen. Wegen $\sigma = \tau \circ \rho$ ist σ Produkt von $\leqq (n - r - 2) + 1 = n - r - 1$ Transpositionen.

□

Bemerkung 4.11.
Beweis war konstruktiv: will man etwa $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ in Transpositionen zerlegen, so findet man z.B. $\sigma = \tau_{12} \circ \tau_{23}$, oder auch $\sigma = \tau_{23} \circ \tau_{13}$, oder ...
Die Zerlegung in Transpositionen ist also nicht eindeutig.

Definition 4.12.
Sei $\sigma \in S_n$

(a) Ein **Fehlstand** von σ ist ein Paar (i, j) mit $1 \leqq i < j \leqq n$ und $\sigma(i) > \sigma(j)$.

(b) Das **Signum** (oder **Vorzeichen**) von σ ist definiert als $\operatorname{sgn}(\sigma) := (-1)^{f(\sigma)}$, wobei $f(\sigma)$ die Anzahl der Fehlstände von σ ist.

(c) σ heißt **gerade** (bzw. **ungerade**), falls $\operatorname{sgn}(\sigma) = +1$ (bzw. $\operatorname{sgn}(\sigma) = -1$) ist.

Beispiele 4.13.

1. Es ist $f(id) = 0$, also $\operatorname{sgn}(id) = +1$.

2. Sei $i < j$, sei $\tau = \tau_{ij}$. Die Fehlstände von τ sind (i, j), sowie alle (i, k) und (k, j) mit $i < k < j$. Also $f(\tau) = 2(j - i - 1) + 1$, insbesondere $\operatorname{sgn}(\tau) = -1$.
   Jede Transposition ist ungerade.

3. In $S_3 = \{id, \tau_{12}, \tau_{13}, \tau_{23}, \sigma, \sigma^2\}$ mit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$:
   σ hat Fehlstände $(1, 3), (2, 3)$
   σ^2 hat Fehlstände $(1, 2), (1, 3)$. Also σ, σ^2 gerade.

Satz 4.14.
Für alle $\rho, \sigma \in S_n$ gilt:
$\operatorname{sgn}(\rho \circ \sigma) = \operatorname{sgn}(\rho) \cdot \operatorname{sgn}(\sigma)$.

Beweis:
Sei $f = f(\sigma)$ die Anzahl der Fehlstände von σ. Es ist $\prod\limits_{1 \leqq i < j \leqq n} (\sigma(j) - \sigma(i)) = (-1)^f \prod\limits_{1 \leqq i < j \leqq n} (j-$

i).
Also ist $\operatorname{sgn}(\sigma) = \prod\limits_{1 \leqq i < j \leqq n} \frac{\sigma(j)-\sigma(i)}{j-i}$.
Ist auch $\rho \in S_n$, so ist $\operatorname{sgn}(\rho \circ \sigma) = \prod\limits_{i<j} \frac{\rho\circ\sigma(j)-\rho\circ\sigma(i)}{j-i} = \underbrace{\prod\limits_{i<j} \frac{\rho(\sigma(j)) - \rho(\sigma(i))}{\sigma(j)-\sigma(i)}}_{\operatorname{sgn}(\rho)} \cdot \underbrace{\prod\limits_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}}_{\operatorname{sgn}(\sigma)}$

Das linke Produkt auf der rechten Seite ist $\operatorname{sgn}(\rho)$, denn mit $(i,j) \in \{1,\dots,n\}$, $i<j$, durchläuft $\{\sigma(i), \sigma(j)\}$ alle 2-elementigen Teilmengen von $\{1,\dots,n\}$. Die Behauptung folgt deshalb aus $\frac{\rho(a)-\rho(b)}{a-b} = \frac{\rho(b)-\rho(a)}{b-a}$.

□

Hier einige Folgerungen:

Korollar 4.15.
Ist $\sigma = \tau_1 \circ \ldots \circ \tau_r$ mit Transpositionen $\tau_1, \dots, \tau_r$, so ist $\operatorname{sgn}(\sigma) = (-1)^r$.

□

Korollar 4.16.
$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.
Denn: $\sigma \circ \sigma^{-1} = id \Rightarrow \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma^{-1}) = +1$.

□

Korollar 4.17.
Die Abbildung $\operatorname{sgn} : S_n \to \{+1, -1\}$ *ist ein Gruppenhomomorphismus von S_n in die Gruppe* $(\{\pm 1\}, \cdot)$.

□

Definition 4.18.
Der Normalteiler $A_n := \ker(\operatorname{sgn} : S_n \to \{\pm 1\}) = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\}$ von S_n heißt die **alternierende Gruppe**.

Bemerkung 4.19.
Für $n \geqq 2$ ist $\operatorname{sgn} : S_n \to \{\pm 1\}$ surjektiv (z.B. $\operatorname{sgn}(\tau_{12}) = -1$).
Nach dem Homomorphiesatz 3.64 ist also $S_n/A_n \cong \{\pm 1\}$.
Nach Satz von Lagrange (3.61) ist also $|A_n| = \frac{n!}{2}$.
Insbesondere also $A_2 = \{id\}$, $A_3 = \{id, \sigma, \sigma^2\}$ mit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Bequemere Notation für Permutationen:

Definition 4.20.
Sei $2 \leqq r \leqq n$. Eine Permutation $\sigma \in S_n$ heißt ein ***r*-Zykel**, wenn es r paarweise verschiedene Elemente $i_1, \ldots, i_r \in \{1, \ldots, n\}$ gibt mit $\sigma(i_k) = i_{k+1}$ $(k = 1, \ldots, r-1)$, $\sigma(i_r) = i_1$ und $\sigma(j) = j \; \forall j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$.
Man schreibt dann $\sigma =: (i_1 \ldots i_r)$.
Zwei Zykel $(i_1 \ldots i_r)$ und $(j_1 \ldots j_s)$ heißen **disjunkt**, falls $\{i_1 \ldots i_r\} \cap \{j_1 \ldots j_s\} = \emptyset$ ist.

Nebenbemerkung:
Die 2-Zykel sind genau die Transpositionen.

Satz 4.21. *(Zykelzerlegung)*

(a) $\operatorname{sgn}(\sigma) = (-1)^{r-1}$, *falls σ ein r-Zykel ist.*

(b) Sind ρ, σ disjunkte Zykel, so ist $\rho \circ \sigma = \sigma \circ \rho$.

(c) Jedes $\sigma \in S_n$ ist Produkt von paarweise disjunkten Zykeln (von Längen $\geqq 2$), und diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.

Beweis:

(a) $(i_1 \ldots i_r) = (i_1 i_r) \circ \ldots \circ (i_1 i_3) \circ (i_1 i_2)$.

(b) klar

(c) Zeige durch absteigende Induktion nach $|Fix(\sigma)|$:
σ ist Produkt von paarweise disjunkten Zykeln, welche alle zu $Fix(\sigma)$ disjunkt sind. Sei $\sigma \neq id$, sei $i \in \{1, \ldots, n\}$ mit $\sigma(i) \neq i$. Wegen $\langle \sigma \rangle = \{\sigma^k : k \in \mathbb{Z}\}$ endlich, gibt es ein $m \in \mathbb{N}$, $m > 1$, mit $\sigma^m = id$. $\Rightarrow \sigma^m(i) = i$.
Sei $r > 1$ minimal mit $\sigma^r(i) = i$. Dann sind $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{r-1}(i)$ paarweise verschieden, denn $\sigma^\mu(i) = \sigma^\nu(i) \Rightarrow \sigma^{\mu-\nu}(i) = i$.
Für $\rho := (i \, \sigma(i) \ldots \sigma^{r-1}(i))$ ist also $Fix(\rho^{-1} \circ \sigma) = Fix(\sigma) \cup \{i, \sigma(i), \ldots, \sigma^{r-1}(i)\}$.
Insbesondere $|Fix(\rho^{-1} \circ \sigma)| > |Fix(\sigma)|$. Also ist $\rho^{-1} \circ \sigma$ Produkt von paarweise

diskjunkten Zykeln, alle disjunkt zu $Fix(\rho^{-1} \circ \sigma)$.
$\Rightarrow \sigma = \rho \circ (\rho^{-1} \circ \sigma)$ ist Produkt von paarweise disjunkten Zykeln.

$\square$

Bemerkung 4.22.
Die 6 Elemente der S_3 sind $id, (12), (13), (23), (123), (132)$.
Zykel sind invariant unter zyklischer Vertauschung:
$(i_1\, i_2\, i_3 \ldots i_r) = (i_2\, i_3 \ldots i_r\, i_1)$
Einfach, die Zykelzerlegung einer gegebenen Permutation zu finden.
z.B. $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 3 & 8 & 10 & 2 & 6 & 4 & 5 & 1 & 7 \end{pmatrix}$ hat Zerlegung $\sigma = (1\,9)(2\,3\,8\,5)(4\,10\,7)$.
Also $\operatorname{sgn}(\sigma) = (-1) \cdot (-1) \cdot (+1) = +1$.

c. Determinante einer quadratischen Matrix

Bemerkung 4.23.
Seien $x = (x_1, x_2)$ und $y = (y_1, y_2)$ in $\mathbb{R}^2$, sei $P := \{ax + by : 0 \leqq a, b \leqq 1\}$ das von x und y aufgespannte Parallelogramm. Dann gilt für den Flächeninhalt $F(P)$ von P:
$F(P) = |x_1y_2 - x_2y_1| = \left| det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \right|$
Dabei ist det $\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \left\{ \begin{matrix} > 0 \\ < 0 \end{matrix} \right\} \Leftrightarrow \begin{cases} \sphericalangle(x, y) \in]0°, 180°[\\ \sphericalangle(x, y) \in]-180°, 0°[\end{cases}$

Die Determinante einer 2×2-Matrix (über $\mathbb{R}$) lässt sich also als orientierter Flächeninhalte des von den Spalten aufgespannten Parallelogramms interpretieren.
Höhere Dimension: für $v_1, \ldots, v_n \in \mathbb{R}^n$ sei $P := Spat(v_1, \ldots, v_n) := \left\{ \sum\limits_{i=1}^{n} a_i v_i : 0 \leqq a_i \leqq 1 \right\}$.

Notation 4.24.
Sind $v_1, \ldots, v_n \in K^n$, so sei $M(v_1, \ldots, v_n)$ die $m \times n$-Matrix mit den Spalten $v_1, \ldots, v_n$ (in dieser Reihenfolge).

Definition 4.25.
Eine Abbildung $\delta : M_n(K) \to K$ heißt eine **Determinantenabbildung**, wenn gelten:
(D1) δ ist **multilinear** bezüglich der Spalten, d.h.
$\delta(M(v_1, \ldots, av_k + a'v'_k, \ldots, v_n)) = a \cdot \delta(M(v_1, \ldots, v_k, \ldots v_n)) + a' \cdot \delta(M(v_1, \ldots, v'_k, \ldots, v_n))$
$\forall\ v_1, \ldots, v_k, v'_k, \ldots, v_n \in K^n, a, a' \in K$.
(D2) δ ist **alternierend**, d.h. $\delta(A) = 0$, falls A zwei gleiche Spalten hat.
(D3) δ ist **normiert**: $\delta(I_n) = 1$.

Bemerkung:
(D1), (D2) und (D3) wird man erwarten, wenn $|\delta(M(v_1, \ldots, v_n))| = vol_n(Spat(v_1, \ldots, v_n))$ sein soll.

Lemma 4.26.
Sei $\delta : M_n(K) \to K$ eine Determinantenabbildung, sei $\sigma \in S_n$. Für alle $v_1, \ldots, v_n \in K^n$ ist $\delta(M(v_{\sigma(1)}, \ldots, v_{\sigma(n)})) = \mathrm{sgn}(\sigma) \cdot \delta(M(v_1, \ldots, v_n))$.

Beweis:
Wir verwenden nur (D1) und (D2): Es genügt, den Fall $\sigma = \tau$, eine Transposition, zu betrachten (4.10, 4.14).

Sei $\tau = \tau_{kl} = (kl)$ mit $1 \leqq k < l \leqq n$.
$\delta(M(v_1, \ldots, v_{k-1}, v_k + v_l, v_{k+1}, \ldots, v_{l-1}, v_k + v_l, v_{l+1}, \ldots, v_n)) = 0 =$ (D2)
$\underbrace{\delta(M(\ldots, v_k, \ldots, v_k, \ldots))}_{=0} + \delta(M(\ldots, v_k, \ldots, v_l, \ldots)) +$
$\delta(M(\ldots, v_l, \ldots, v_k, \ldots)) + \underbrace{\delta(M(\ldots, v_l, \ldots, v_l, \ldots))}_{=0}$.
$\Rightarrow \delta(M(\ldots, v_k, \ldots, v_l, \ldots)) = \operatorname{sgn}(\tau_{kl}) \cdot \delta(M(\ldots, v_l, \ldots, v_k, \ldots))$

(…: alle anderen Spalten unverändert)

□

Lemma 4.27.
Sei $\delta : M_n(K) \to K$ mit (D1) und (D2). Für $A = (a_{ij}) \in M_n(K)$ ist
$$\delta(A) = \delta(I_n) \cdot \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \cdot \prod_{j=1}^{n} a_{\sigma(j),j} \right).$$
Insbesondere gibt es höchstens eine Determinantenabbildung.

Beweis:
Es ist $A = M(v_1, \ldots, v_n)$ mit $v_j = \sum_{i=1}^{n} a_{ij} e_i$, $(j = 1, \ldots, n)$.
$$\Rightarrow \delta(A) = \delta\left(M\left(\sum_{i_1=1}^{n} a_{i_1,1} e_{i_1}, \ldots, \sum_{i_n=1}^{n} a_{i_n,n} e_{i_n} \right) \right) =$$
$$\sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} a_{i_1,1} \ldots a_{i_n,n} \cdot \underbrace{\delta(M(e_{i_1}, \ldots, e_{i_n}))}_{0 \text{ falls 2 gleiche } i \text{ vorkommen}} =$$
$$\sum_{\sigma \in S_n} a_{\sigma(1),1} \ldots a_{\sigma(n),n} \cdot \underbrace{\delta(M(e_{\sigma(1)}, \ldots, e_{\sigma(n)}))}_{=\operatorname{sgn}(\sigma) \cdot \delta(I_n)} \qquad (i_1, \ldots, i_n) = (\sigma(1), \ldots, \sigma(n))$$

□

Definition 4.28.
Für $A = (a_{ij}) \in M_n(K)$ **definieren** wir die **Determinante** von A durch
$$\det(A) := |A| := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{j=1}^{n} a_{\sigma(j),j}.$$
Wenn es eine Determinantenabbildung δ gibt, so muss $\delta = \det$ sein. (Lemma 4.27).

Satz 4.29.
Die Abbildung $\det : M_n(K) \to K$ hat Eigenschaften (D1), (D2), (D3), ist also eine (die einzige) Determinantenabbildung.

Beweis: (D1) klar (jedes Produkt $\prod_{j=1}^{n} a_{\sigma(j),j}$ enthält aus jeder Spalte genau einen Koeffizienten).

(D3) klar.

(D2):
Sei $A = (a_{ij})$ mit Spalten $S_k(A) = S_l(A)$ (d.h. die k-te und l-te Spalte sind gleich), mit $k < l$. Sei $\tau := \tau_{kl} \in S_n$. Es ist $S_n = A_n \cup A_n\tau$, also:
$\det(A) = \sum_{\sigma\in A_n} \left(a_{\sigma(1),1}\cdots a_{\sigma(n),n} - a_{\sigma\tau(1),1}\cdots a_{\sigma\tau(n),n}\right)$.
Behaupte: $(\ldots) = 0$ (für jedes $\sigma \in A_n$).
Denn alle Faktoren außer in Spalten k und l stimmen in beiden Summanden überein, und $a_{\sigma\tau(k),k} \cdot a_{\sigma\tau(l),l} = a_{\sigma(l),k} \cdot a_{\sigma(k),l} = a_{\sigma(l),l} \cdot a_{\sigma(k),k}$ (da $S_k(A) = S_l(A)$)
□

Bemerkungen und Beispiele 4.30.

(a) (D1) besagt:
$$\begin{vmatrix} a_{11} & \ldots & \lambda a_{1j} + \mu b_{1j} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \ldots & \lambda a_{nj} + \mu b_{nj} & \ldots & a_{nn} \end{vmatrix} =$$
$$\lambda \begin{vmatrix} a_{11} & \ldots & a_{1j} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nj} & \ldots & a_{nn} \end{vmatrix} + \mu \begin{vmatrix} a_{11} & \ldots & b_{1j} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \ldots & b_{nj} & \ldots & a_{nn} \end{vmatrix}$$

(b) Für $n = 2$ stimmt die neue Definition mit der alten (3.14) überein.

(c) Für $n = 3$ gilt (Regel von Sarrus):
$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}.$$

(d) $\det(aA) = a^n \cdot \det(A)$, $A \in M_n(K)$, $a \in K$.

(e) $\det(\textit{Dreiecksmatrix}) = a_{11}a_{22}\ldots a_{nn}$.

Satz 4.31.
$\det(A^t) = \det(A)$, $A \in M_n(K)$.

Beweis:
$\det(A) = \sum\limits_{\sigma\in S_n} \operatorname{sgn}(\sigma)\cdot\prod\limits_{j=1}^{n} a_{\sigma(j),j} = \sum\limits_{\rho\in S_n} \operatorname{sgn}(\rho)\cdot\prod\limits_{i=1}^{n} a_{i,\rho(i)} = \det(A^t)$ mit $\rho = \sigma^{-1}$.

□

Die Determinante ist also auch multilinear und alternierend bezüglich der Zeilen, und ist die einzige normierte Abbildung mit dieser Eigenschaft.

Theorem 4.32.
$\forall A, B \in M_n(K)$ *gilt:* $\det(AB) = \det(A)\cdot\det(B)$.

Beweis:
Fixiere A betrachte B als variabel.
Die Abbildung $\delta : M_n(K) \to K$, $\delta(B) := \det(AB)$ hat die Eigenschaften (D1) und (D2). Denn $S_j(AB) = A\cdot S_j(B)$ $(j = 1,\dots,n)$. Nach 4.27 folgt $\det(AB) = \delta(B) = \delta(I_n)\cdot\det(B) = \det(A)\cdot\det(B)$.

□

Korollar 4.33.
Sei $A \in M_n(K)$, sei $\widetilde{A} \in M_n(K)$ aus A durch endlich vielen elementare Zeilen- und Spaltentransformationen vom Typ $q_{kl}(\lambda)$, $q'_{kl}(\lambda)$ gebildet. Dann ist $\det(A) = \det(\widetilde{A})$.

Beweis:
$q_{kl}^{\lambda}(A) = \underbrace{Q_{kl}(\lambda)}_{\det=1}\cdot A$, analog Spalten.

□

Bemerkung 4.34.
Dagegen ändert sich bei einer Permutation σ der Zeilen (oder Spalten) die Determinante um den Faktor $\operatorname{sgn}(\sigma)$.

Beispiel 4.35.
Man berechnet Determinanten im Allgemeinen durch elementare Umformungen:

$$A := \begin{pmatrix} 1 & 5 & 0 & 2 \\ -4 & 0 & 1 & 1 \\ 1 & 3 & 2 & 2 \\ 2 & 0 & -1 & 4 \end{pmatrix} \in M_4(\mathbb{R}).$$

$q_{21}(4), q_{31}(-1), q_{41}(-2)$

$$\begin{pmatrix} 1 & 5 & 0 & 2 \\ 0 & 20 & 1 & 9 \\ 0 & -2 & 2 & 0 \\ 0 & -10 & -1 & 0 \end{pmatrix}$$

π'_{24} (Vertausche S_2 und S_4)

$$\begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 9 & 1 & 20 \\ 0 & 0 & 2 & -2 \\ 0 & 0 & -1 & -10 \end{pmatrix}$$

π_{34}

$$\begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 9 & 1 & 20 \\ 0 & 0 & -1 & -10 \\ 0 & 0 & 2 & -2 \end{pmatrix}$$

$q_{43}(2)$

$$\begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 9 & 1 & 20 \\ 0 & 0 & -1 & -10 \\ 0 & 0 & 0 & -22 \end{pmatrix}$$

Also ist $\det(A) = 1 \cdot 9 \cdot (-1)\dot{(} -22) \cdot (-1)^2 = 198 \quad ((-1)^2$ wegen 2 Vertauschungen)

Korollar 4.36.
Sei $A \in M_n(K)$. Genau dann ist A invertierbar, wenn $\det(A) \neq 0$ ist, und dann gilt $\det(A^{-1}) = \frac{1}{\det(A)}$.

Beweis:
A invertierbar $\Rightarrow A \cdot A^{-1} = I \Rightarrow \det(A) \neq 0$ und $\det(A^{-1}) = \frac{1}{\det(A)}$.
Sei A nicht invertierbar. Also $r := rk(A) < n$. Nach 3.99 ist $A = T^{-1} \cdot diag(1, \dots, 1, 0, \dots, 0) \cdot S$ mit $S, T \in GL_n(K) \Rightarrow \det(A) = 0$.

□

Korollar 4.37.
$\det : GL_n(K) \to K^*$ *ist ein Gruppenhomomorphismus. Sein Kern heißt die spezielle lineare Gruppe:*
$SL_n(K) := \{A \in GL_n(K) : \det(A) = 1\}$.

$SL_n(K)$ ist ein Normalteiler von $GL_n(K)$.

d. Spezielle Determinanten, Entwicklungssatz

Satz 4.38. *(Kästchensatz)*
Sei $A = (a_{ij}) \in M_n(K)$.

(a) *Sei* $A = \left(\begin{array}{c|c} A' & * \\ \hline 0 & A'' \end{array}\right)$ *mit $A' \in M_r(K)$ und $A'' \in M_{n-r}(K)$ (d.h. es gibt $1 \leqq r < n$ mit $a_{ij} = 0$ für $r+1 \leqq i \leqq n$ und $1leqqj < r$), so ist* $\det(A) = \det(A')\dot{\det}(A'')$.

(b) *Analog* $\det\left(\begin{array}{c|c} A' & 0 \\ \hline * & A'' \end{array}\right) = \det(A') \cdot \det(A'')$.

Beweis:

(a) $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{j=1}^{n} a_{\sigma(j),j}$ brauche nur solche σ zu berücksichtigen mit $\sigma\{1, \ldots, r\} = \{1, \ldots, r\}$. für solches σ ist $\sigma\{r+1, \ldots, n\} = \{r+1, \ldots, n\}$. Schreibe $\sigma = (\sigma', \sigma'')$ mit $\sigma' \in S_r$, $\sigma'' \in S_{n-r}$ mit $\sigma'(i) := i$ $(i = 1, \ldots, r)$ und $\sigma''(j) + r = \sigma(j+r)$ $(j = 1, \ldots, n-r)$. Somit $\det(A) = \sum_{\sigma' \in S_r, \sigma'' \in S_{n-r}} \underbrace{\operatorname{sgn}(\sigma') \cdot \operatorname{sgn}(\sigma'')}_{=\operatorname{sgn}(\sigma', \sigma'')} \cdot \prod_{j=1}^{r} a_{\sigma'(j),j} \cdot$
$\prod_{k=1}^{n-r} a_{\sigma''(k)+r,k+r} =.$
$\left(\sum_{\sigma' \in S_r} \operatorname{sgn}(\sigma' \prod_{j=1}^{r} a_{\sigma(j),j}\right) \cdot \left(\sum_{\sigma'' \in S_{n-r}} \operatorname{sgn}(\sigma'') \prod_{k=1}^{n-r} a_{\sigma''(k)+r,k+r}\right) = \det(A') \cdot \det(A'')$.

□

Bemerkung 4.39.
Allgemeine gilt der Satz für größere Kästchenmuster:
det ... = $\det(A_1) \cdot \ldots \cdot \det(A_r)$.

(Beweis durch vollständige Induktion)

Satz 4.40. *(Vandermonde-Determinante)* *Für $a_1, \ldots, a_n \in K$ ist*

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqq i < j \leqq n} (a_j - a_i).$$

Beweis:
Sei $D = D(a_1, \dots, a_n)$ die gesuchte Determinante. Für $j = n, n-1, \dots, 2$ ersetze S_j durch $S_j - a_1 S_{j-1}$. Das ergibt:

$$D = \det\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_1 a_2 & \dots & a_2^{n-1} a_1 a_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n - a_1 & a_n^2 - a_1 a_2 & \dots & a_n^{n-1} a_1 a_n^{n-2} \end{pmatrix} = \prod_{i=2}^{n}(a_i - a_1) \cdot \det\begin{pmatrix} 1 & a_2 & a_2^2 & \dots & a_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-2} \end{pmatrix}$$

Die Behauptung folgt also durch Induktion.

□

Definition 4.41.
Sei $A = (a_{ij}) \in M_n(K)$, seien $i, j \in \{1, \dots, n\}$.

$$\text{Definiere } A_{ij} := \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{pmatrix}$$

Die Matrix $A^\sharp = (a^\sharp_{ij})$ mit $a^\sharp_{ij} := \det(A_{ji})$ (Reihenfolge!) heißt die zu A **komplementäre** (oder **adjunkte**) **Matrix**.

Bemerkung 4.42.
Sei $n > 1$. Es bezeichne A'_{ij} (für $1 \leqq i, j \leqq n$) die $(n-1) \times (n-1)$-Matrix, die aus A durch Streichen der i-ten Zeile und der j-ten Spalte entsteht.
Es gilt $a^\sharp_{ji} = \det(A_{ij}) = (-1)^{i+j} \cdot \det(A'_{ij})$.

Denn durch $j-1$ Spaltenvertauschungen und $i-1$ Zeilenvertauschungen wird aus A_{ij} die Matrix $\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & A'_{ij} \end{array}\right)$. Also $\det(A_{ij} = (-1)^{i-1+j-1} \cdot \det(A'_{ij}) = (-1)^{i+j} \det(A'_{ij})$.

$$\text{Es ist also } A^\sharp = \begin{pmatrix} +\det(A'_{11}) & -\det(A'_{21}) & \dots \\ -\det(A'_{12}) & +\det(A'_{22}) & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Beispiel 4.43.
$n = 2$: $A = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$, $A^\sharp = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$

Satz 4.44.
Sei $A \in M_n(K)$, dann ist $A \cdot A^\sharp = A^\sharp \cdot A = \det(A) \cdot I_n$.

Beweis:
Sei $A = (a_{ij})$, sei $v_j := S_j(A) = \sum\limits_{i=1}^{n} a_{ij}e_i$, und sei $A^\sharp = (a^\sharp_{ij})$. Es ist der (i, j)-Koeffizient von $A^\sharp \cdot A$ gleich

$\sum\limits_{k=1}^{n} a^\sharp_{ik} \cdot a_{kj} = \sum\limits_{k=1}^{n} \det(A_{ki}) \cdot a_{kj} =$

$\sum\limits_{k=1}^{n} \det(M(v_1 - a_{k1}e_k, \dots, \underbrace{e_k}_{\text{Stelle } i}, \dots, v_n - a_{kn}e_k) \cdot a_{kj} =$

$\sum\limits_{k=1}^{n} a_{kj} \cdot \det(M(v_1, \dots, v_{i-1}, e_k, v_{i+1}, \dots, v_n)) =$

$$\det(M(v_1, \dots, v_{i-1}, \underbrace{\sum_{k=1}^{n} a_{kj}e_k}_{=v_j}, v_{i+1}, \dots v_n) =$$

$\det(A) \cdot \delta_{ij}$.

Also gezeigt $A^\sharp \cdot A = \det(A) \cdot I$-
$(A \cdot A^\sharp)^t = (A^\sharp)^t \cdot A^t = \det(A^t) \cdot I = \det(A) \cdot I$.

□

Nebenbemerkung:
$A_{ki} = M(v_1 - a_{k1}e_k, \dots, \underbrace{e_k}_{\text{Stelle } i}, \dots, v_n - a_{kn}e_k)$.

Korollar 4.45.
Ist $\det(A) \neq 0$, *so ist* $A^{-1} = \frac{1}{\det(A)} \cdot A^\sharp$.

Korollar 4.46. *(Entwicklungssatz von Laplace)*
Sei $A = (a_{ij}) \in M_n(K)$. *Für jedes* $j = 1, \dots, n$ *ist* $\det(A) = \sum\limits_{i=1}^{n} (-1)^{i+j} a_{ij} \cdot \det(A'_{ij})$
(Entwickeln nach der j-ten Spalte),
für $i = 1, \dots, n$ *ist* $\det(A) = \sum\limits_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A'_{ij})$.
(Entwickeln nach der i-ten Zeile).

Beweis:
Sei j fest. Der Koeffizient von $A^\sharp \cdot A$ an der Stelle (j, j) ist $\det(A)$ nach 4.44, und ist auch gleich $\sum\limits_{i=1}^{n} a^\sharp_{ji} \cdots a_{ij} = \sum\limits_{i=1}^{n} (-1)^{i+j} \det(A'_{ij}) a_{ij}$.

Analog für Zeilen.

□

Beispiel 4.47.
Entwickeln von $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$ nach der zweiten Zeile gibt:
$-a_{21}(a_{12}a_{33} - a_{13}a_{32}) + a_{22}(a_{11}a_{33} - a_{13}a_{31}) - a_{23}(a_{11}a_{32} - a_{12}a_{31})$.

Beispiel 4.48.
$A = \begin{pmatrix} 1 & 5 & 0 & 2 \\ -4 & 0 & 1 & 1 \\ 1 & 3 & 2 & 2 \\ 2 & 0 & -1 & 4 \end{pmatrix}$.

Entwickle nach der zweiten Spalte - ergibt:
$\det(A) = -5\begin{vmatrix} -4 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & -1 & 4 \end{vmatrix} - 3\begin{vmatrix} 1 & 0 & 2 \\ -4 & 1 & 1 \\ 2 & -1 & 4 \end{vmatrix} = \ldots = 198.$

Satz 4.49. *(Cramer'sche Regel)*
Sei $A = (a_{ij}) \in M_n(K)$ invertierbar, sei $u \in K^n$. Die Lösung der Linearen Gleichungssystems $A \cdot x = u$ ist gegeben durch $x = (x_1, \ldots, x_n)^t$ mit
$x_j = \frac{\det(M(v_1,\ldots,v_{j-1},u,v_{j+1},\ldots,v_n))}{\det(A)}$, mit $v_k :=$ k-te Spalte von A.

Also $x_j = \frac{1}{\det(A)} \cdot \begin{vmatrix} a_{11} & \ldots & u_1 & \ldots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \ldots & u_n & \ldots & a_{nn} \end{vmatrix}$

Beweis:
Es genügt, nachzurechnen, dass $x = (x_1, \ldots, x_n)^t$ eine Lösung ist.

Für $i = 1, \ldots, n$ ist

$$\sum_{j=1}^{n} a_{ij}x_j = \frac{1}{\det(A)} \sum_{j=1}^{n} a_{ij} \underbrace{\sum_{k=1}^{n}(-1)^{j+k}u_k \cdot \det(A'_{kj})}_{\text{Entwicklung nach } j\text{-ten Spalte}} =$$

$$\frac{1}{\det(A)} \sum_{k=1}^{n} u_k \sum_{j=1}^{n} a_{ij} \underbrace{(-1)^{j+k}\det(A'_{kj})}_{a^\sharp_{jk}} =$$

$$\frac{1}{\det(A)} \sum_{k} u_k \cdot \delta_{ik} \cdot \det(A) = u_i.$$

□

Bemerkung 4.50.
Die Formel 4.44 für A^{-1}, sowie die Cramer'sche Regel (4.49), sind für die Rechnung ungenügend.
Vielmehr zeigen sie etwa, dass A^{-1} stetig (sogar differenzierbar, ...) von $A \in GL_n(\mathbb{R})$ abhängt.
Ebenso für Cramer'sche Regel: die Lösung von $Ax = u$ mit invertierbarem A hängt stetig von A und von u ab.

Wir wissen: $\det(A) = 0 \Leftrightarrow rk(A) < n$ (für $A \in M_n(K)$)
Genauer gilt:

Definition 4.51. (Minor) Sei $A \in M_{m\times n}(K)$, sei $r \leqq \min\{m, n\}$.
Jede Determinante
$\det\begin{pmatrix} a_{i_1,j_1} & \dots & a_{i_1,j_r} \\ \vdots & \ddots & \vdots \\ a_{i_r,j_1} & \dots & a_{i_r,j_r} \end{pmatrix}$ mit $1 \leqq i_1 < \ldots \leqq i_r \leqq m$ und $1 \leqq j_1 < \ldots < j_r \leqq n$ heißt ein r-**Minor** (oder r-**reihige Unterdeterminante** von A.

Beispiel 4.52.
Die 1-Minoren sind die a_{ij} : mn Stück.
Die 2-Minoren sind die $\begin{vmatrix} a_{i_1,j_1} & a_{i_1,j_2} \\ a_{i_2,j_1} & a_{i_2,j_2} \end{vmatrix}$ mit $i_1 < i_2$, $j_1 < j_2$.
Das sind $\binom{m}{2} \cdot \binom{n}{2}$ Stück. Allgemeiner gibt es $\binom{m}{r} \cdot \binom{n}{r}$ r-Minoren von A (unter denen natürlich gleiche vorkommen können).

Satz 4.53.
Sei $A \in M_{m\times n}(K)$. Dann ist $rk(A)$ gleich dem maximalen r, für das ein r-Minor $\neq 0$ von A existiert.

Beweis:
Sei $\underbrace{\begin{vmatrix} a_{i_1,j_1} & \dots & a_{i_1,j_r} \\ \vdots & \ddots & \vdots \\ a_{i_r,j_1} & \dots & a_{i_r,j_r} \end{vmatrix}}_{\widetilde{A}} \neq 0.$
Die r Zeilen von $\widetilde{A}$ sind also linear unabhängig.
Erst recht sind also die Zeilen $Z_{i_1}(A), \ldots, Z_{i_r}(A)$ linear unabhängig. $\Rightarrow rk(A) \geqq r$.
Umgekehrt sei $r := rk(A)$- Also hat A linear unabhängige Zeilen, etwa $Z_{i_1}(A), \ldots, Z_{i_r}(A)$ mit $i_1 < \ldots < i_r$. Die $r \times n$-Matrix mit diesen Zeilen hat also Rang r. Also hat sie

auch r linear unabhängige Spalten, etwa die Spalten $j_1 < \ldots < j_r$. Also ist der Minor von A zu den Zeilen $i_1, \ldots, i_r$ und zu den Spalten $j_1, \ldots, j_r$ ungleich 0.

□

Beispiel 4.54.
Seien $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^n$.

Genau dann sind x, y linear abhängig, wenn $x_i y_i = x_j y_j$ gilt $forall 1 \leqq i, j \leqq n$.

Grund: x, y linear abhängig $\Leftrightarrow$ die $n \times 2$-Matrix $\begin{pmatrix} x_1 & y_1 \\ \vdots & \vdots \\ x_n & y_n \end{pmatrix}$ hat Rang $\leqq 1$.

Nach 4.53 ist das äquivalent zu $\begin{vmatrix} x_i & y_i \\ x_j & y_j \end{vmatrix} = 0 \; \forall i \leqq j$.

Bemerkung 4.55.
Für jeden Ring R haben wir den Ring $M_n(R)$ der $n \times n$-Matrizen über R definiert. Kann man eine „sinnvolle " Determinante $\det : M_n(R) \to R$ definieren?

Antwort: Ja, falls R kommutativ ist. Definiere dann $\det(a_{ij}) := \sum\limits_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod\limits_{i=1}^{n} a_i, \sigma(i)$ für $A = (a_{ij}) \in M_n(R)$. Dann bleiben (D1), (D2) und (D3) (siehe 4.25) richtig. Es gilt auch, für $A, B \in M_n(R)$:

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

(2) $A \cdot A^\sharp = A^\sharp \cdot A = \det(A) \cdot I_n$, wobei $A^\sharp$ wie über Körpern definiert wird.

Eine Beweismöglichkeit geht wie folgt:
Beweisidee:
Fasse die Koeffizienten von A und B als formale Unbestimmte auf (1) und (2) sind Polynomgleichungen in diesen Unbestimmten mit ganzen Koeffizienten.
Zwei Polynome über $\mathbb{Z}$ sind genau dann gleich, wenn sie nach Einsetzen beliebiger Wert aus $\mathbb{C}$ für die Variablen stets dasselbe Ergebnis liefern.
Damit sind (1) und (2) auf Fall $R = \mathbb{C}$ zurückgeführt, und damit bewiesen.

Bemerkung 4.56.
Ist R nicht kommutativ, so kann man keine Determinante mit (D1), (D2) und (D3) (siehe 4.25) definieren!

Betrachte $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$: versuche det $:= ad - bc$, aber dann wäre $\det \begin{pmatrix} \lambda a & b \\ \lambda c & d \end{pmatrix} = \lambda ad - b\lambda c \neq \lambda(ad - bc)$ (im Allgemeinen)

e. Ähnlichkeit von Matrizen, Determinante/Spur von Endomorphismen, Orientierung

Alle Vektorräume seien endlich-dimensional

Satz 4.57.
Sei V ein K-VR, $\dim(V) = n$, sei $f \in End(V)$ und $\mathcal{B}$ eine Basis von V. Sei $A := M_{\mathcal{B}}^{\mathcal{B}}(f) \in M_n(K)$.
Für jedes $B \in M_n(K)$ sind äquivalent:

(i) $\exists$ *Basis $\mathcal{C}$ von V mit $B = M_{\mathcal{C}}^{\mathcal{C}}(f)$,*

(ii) $\exists\, S \in GL_n(K)$ *mit $B = SAS^{-1}$.*

Beweis:
(i) $\Rightarrow$ (ii)
$B = SAS^{-1}$ mit $S = T_{\mathcal{C}}^{\mathcal{B}} = M_{\mathcal{C}}^{\mathcal{B}}(id)$.
(denn $S^{-1} = T_{\mathcal{B}}^{\mathcal{C}}$, siehe 3.88)

(ii) $\Rightarrow$ (i)
Definiere $\mathcal{C}$ durch $T_{\mathcal{B}}^{\mathcal{C}} = S^{-1}$; d.h., ist $S^{-1} = (c_{ij})$, so sei $\mathcal{C} = (w_1, \ldots, w_n)$ mit $w_j := \sum_{i=1}^{n} c_{ij} v_i$. (hierbei sei $\mathcal{B} = (v_1, \ldots, v_n)$) Dann ist $B = SAS^{-1} = T_{\mathcal{C}}^{\mathcal{B}} \cdot M_{\mathcal{B}}^{\mathcal{B}}(f) \cdot T_{\mathcal{B}}^{\mathcal{C}} = M_{\mathcal{C}}^{\mathcal{C}}(f)$.
□

Definition 4.58.
Zwei Matrizen $A, B \in M_n(K)$ heißen **ähnlich**, in Zeichen $A \approx B$, falls $\exists S \in GL_n(K)$ mit $B = SAS^{-1}$.

Satz 4.59.
Seien $A, B \in M_n(K)$.

(a) $\approx$ *ist eine Äquivalenzrelation auf $M_n(K)$*

(b) $A \approx B \Rightarrow A \sim B$

(c) $A \approx B \Rightarrow \det(A) = \det(B)$

Beweis:

(a) $A \approx A$, $A \approx B$, etwa $SAS^{-1} = B \Rightarrow A = S^{-1}BS \Rightarrow B \approx A$ und $A \approx B \wedge B \approx C$, etwa $B = SAS^{-1}, C = TBT^{-1}$, dann $C = TSAS^{-1}T^{-1} = (TS)A(TS)^{-1} \Rightarrow A \approx C$.

(b) $A \sim B$ hieß: $\exists\, S, T \in GL_n(K)$ mit $B = SAT^{-1}$. Also $A \approx B \Rightarrow A \sim B$.

(c) $\det(SAS^{-1}) = \det(S) \cdot \det(A) \cdot \det(S)^{-1} = \det(A)$.

□

Bemerkung 4.60.
Ist $f \in End(V)$, $\dim(V) = n$, dann ist $\{M_{\mathcal{B}}^{\mathcal{B}}(f) : \mathcal{B}$ ist Basis von $V\}$ eine volle Ähnlichkeitsklasse (siehe Satz 4.57).

Definition 4.61. (Determinante von Endomorphismen)
($\dim(V) < \infty$) Für $f \in End(V)$ heißt $\det(f) := \det M_{\mathcal{B}}^{\mathcal{B}}(f)$, mit einer beliebigen Basis $\mathcal{B}$ von V, die **Determinante von** f.
Dies ist wohldefiniert (siehe 4.57).

Korollar 4.62.
Seien $f, g \in End(V)$.

(a) $\det(f \circ g) = \det(f) \cdot \det(g)$.

(b) $\det(f) \neq 0 \Leftrightarrow f$ *surjektiv* $\Leftrightarrow f$ *injektiv.*

□

Definition 4.63. (Spur)
Sei $A = (a_{ij}) \in M_n(K)$. Die **Spur** $tr(A)$ von A ist definiert als $tr(A) := \sum_{i=1}^{n} a_{ii}$.

Satz 4.64.
Sei $A, B \in M_n(K)$.

(a) $tr : M_n(K) \to K$ *ist* K*-linear, d.h.* $tr(aA + bB) = a \cdot tr(A) + b \cdot tr(B)$, $(a, b \in K)$.

(b) $tr(A^t) = tr(A)$.

(c) $tr(AB) = tr(BA)$.

Beweis:

(a) klar

(b) klar

(c) Sei $A = (a_{ij}), B = (b_{ij})$. Dann ist $tr(AB) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} b_{ji} \right) = \sum_{j=1}^{n} \sum_{i=1}^{n} b_{ji} a_{ij} = tr(BA)$.

□

Korollar 4.65.
$A \approx B \Rightarrow tr(A) = tr(B)$.

Beweis:
$B = SAS^{-1}$ mit $S \in GL_n(K)$. Es ist $tr(B) = tr(S \cdot AS^{-1}) = tr(AS^{-1} \cdot S) = tr(A)$.

□

Definition 4.66.
Sei V ein K-VR, $f \in End(V)$.
Dann heißt $tr(f) := tr\left(M_{\mathcal{B}}^{\mathcal{B}}(f)\right)$, mit einer beliebigen Basis $\mathcal{B}$ von V, die **Spur** von f.
(wie gezeigt hängt dies nicht von der Wahl von $\mathcal{B}$ ab)

Korollar 4.67.
Für $f, g \in End(V)$ gilt:

(a) $tr(af + bg) = a \cdot tr(f) + b \cdot tr(g)$ $(a, b \in K)$.

(b) $tr(f \circ g) = tr(g \circ f)$.

□

Bemerkung 4.68.

1. Ein Endomorphismus $p \in End(V)$ heißt eine **Projektion**, falls $p \circ p = p$ ist. Siehe Klausur 1.
   $V = \ker(p) \oplus im(p)$, und es ist $p(x) = x\ \forall x \in im(p)$. Wähle Basis $\mathcal{B}$ von V gemäß $\mathcal{B} = (u_1, \ldots, u_r, v_1, \ldots, v_s)$ mit $u_1, \ldots, u_r \in \ker(p)$, $v_1, \ldots, v_s \in im(p)$.
   $$\text{Dann } M^{\mathcal{B}}_{\mathcal{B}}(p) = \left(\begin{array}{ccc|ccc} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ \hline & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{array}\right)$$
   Wir sehen: $tr(p) = \dim(im(p)) = rk(p)$.

2. Die Frage, ob zwei Matrizen A, B ähnlich sind, ist im Allgemeinen subtil. Notwendige Kriterien sind: A, B haben gleichen Rang, Determinante, Spur. Im Allgemeinen sind diese aber noch nicht hinreichend, z.B. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, nicht ähnlich, da $SI_nS^{-1} = I_n$.

3. $(K = \mathbb{R})$ Sei $f \in End(\mathbb{R}^n)$, $f = F_A$ mit $A \in M_n(\mathbb{R})$. Dann kann $|\det(f)|$ als der Faktor interpretiert, um den f Volumina im $\mathbb{R}^n$ verzerrt.
   Sind $v_1, \ldots, v_n \in \mathbb{R}^n$, ist $S := spat(v_1, \ldots, v_n) = \{\sum\limits_{i=1}^{n} \lambda_i v_i : 0 \leqq \lambda_i \leqq 1\}$, so ist $f(S) = \{\sum\limits_{i=1}^{n} \lambda_i f(v_i) : \forall i, 0 \leqq \lambda_i \leqq 1\} = spat(f(v_1), \ldots, f(v_n))$.
   Heuristisch hatten wir uns überlegt:
   $vol_n(S) = |\det(P)|$ wobei $P := M(v_1, \ldots, v_n)$ sei (Matrix mit Spalten $v_1, \ldots, v_n$)
   $M_n(f(v_1), \ldots, f(v_n)) = A \cdot M(v_1, \ldots, v_n) = AP$.
   Also $vol_n f(S) = |\det(AP)| = |\det(A)| \cdot |\det(P)| = |\det(f)| \cdot vol_n(S)$.

Definition 4.69. (orientiert)
(sei $K = \mathbb{R}$)
Sei V ein endlich-dimensionaler $\mathbb{R}$-VR.

(a) Ein $f \in Aut_{\mathbb{R}}(V)$ heißt **orientierungstreu**, falls $\det(f) > 0$ ist , und **orientierungsumkehrend**, falls $\det(f) < 0$.

(b) Zwei Basen $\mathcal{B} = (v_1, \ldots, v_n)$, $C(w_1, \ldots, w_n)$ von V heißen **gleich orientiert**, falls der Automorphismus f von V mit $f(v_i) = w_i$ $(i = 1, \ldots, n)$ orientierungstreu ist.
Andernfalls ($\det(f) < 0$) heißen $\mathcal{B}$ und C **entgegengesetzt orientiert**.

Beispiel 4.70.

1. Sind $\mathcal{B}$, C und f wie in 4.69 (b), so ist $M^{\mathcal{B}}_{C}(f) = I$. Also ist $M^{C}_{C}(f) = M^{\mathcal{B}}_{C}(f) \cdot M^{C}_{\mathcal{B}}(id) = T^{C}_{\mathcal{B}}$.
   Daher sind $\mathcal{B}$ und C genau dann gleich orientiert, wenn $\det\left(T^{C}_{\mathcal{B}}\right) > 0$.

2. Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um $(0, 0)$ um den Winkel α. Bezüglich Basis $\mathcal{K}_2$ von $\mathbb{R}$ hat f die Matrix $\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$, also $\det(f) = 1 > 0$ also ist f orientierungstreu.

   Ist $f : \mathbb{R}^2 \to \mathbb{R}^2$ eine Spiegelung, etwa (v_1, v_2) Basis von $\mathbb{R}^2$ mit $f(v_1) = v_1, f(v_2) = -v_2$, so ist $\det(f) = -1 < 0$. Also ist f orientierungsumkehrend.

3. Eine Basis (v_1, v_2) von $\mathbb{R}^2$ hat genau dann die selbe Orientierung wie die kanonische Basis, wenn gilt:
   $\sphericalangle(v_1, v_2) \in]0°, 180°[$.

Satz 4.71.
Die Gleichorientiertheit von Basen eines $\mathbb{R}$-Vektorraums V ($\dim V < \infty$) ist eine Äquivalenzrelation.

□

Definition 4.72. (Orientierung)
Sei V ein $\mathbb{R}$-VR, $\dim(V) < \infty$. Eine **Orientierung** von V ist eine Äquivalenzklasse von Basen von V bezüglich gleicher Orientierung.

Korollar 4.73.
V hat genau zwei verschiedene Orientierungen (falls $V \neq \{0\}$).

□

5. Eigenwerte

a. Definition, Beispiele

Definition 5.1. (Eigenwert, Eigenvektor)
Sei $f \in End_K(V)$. Eine Zahl $\lambda \in K$ heißt ein **Eigenwert** von f, wenn es ein $v \neq 0$ in V gibt mit $f(v) = \lambda v$. Jedes solche $v \neq 0$ heißt ein **Eigenvektor** von f (zu Eigenwert λ). Die Menge

$$Eig(f;\lambda) := \{v \in V : f(v) = \lambda v\}.$$

ist ein Unter-VR von V, genannt der **Eigenraum von** f zum Parameter λ.
Die Eigenwerte λ von f sind also genau die λ mit $Eig(f;\lambda) \neq \{0\}$.

Korollar 5.2.
Genau dann ist $\lambda \in K$ ein Eigenwert von f, wenn $\ker(f - \lambda \cdot id_V) \neq 0$ ist.
Insbesondere: ist $\dim(V) < \infty$, so gilt:
λ ist Eigenwert von f $\Leftrightarrow$ $\det(f - \lambda \cdot id) = 0$.

Beispiel 5.3.

1. Ist $f \in End(V)$ eine Projektion, d.h. ist $f \circ f = f$, so hat f genau die beiden Eigenwerte (EW) 0 und 1 (sofern $f \neq 0, f \neq id$). Denn $V = \ker(f) \oplus im(f)$ mit $f|_{im(f)} = id$.
   Also ist $Eig(f;0) = \ker(f)$, $Eig(f;1) = im(f)$.

2. Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um $(0,0)$ um Winkel α. Für $\alpha \notin \mathbb{Z} \cdot \pi$ hat f keine Eigenwerte.
   Denn bezüglich $\mathcal{K}_2$ hat f die Matrix $A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ und $\det(\lambda \cdot I - A) = \begin{vmatrix} \lambda - \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \lambda - \cos(\alpha) \end{vmatrix} = \lambda^2 - 2\lambda\cos(\alpha) + 1 = (\lambda - \cos(\alpha))^2 + \sin^2(\alpha) > 0.$

3. Sei V der $\mathbb{R}$-VR aller beliebig oft differenzierbaren Abbildungen $f : \mathbb{R} \to \mathbb{R}$. ($\dim_{\mathbb{R}}(V) = \infty$!)
   Die Ableitung $D : V \to V$, $D(f) = f'$, ist ein Endomorphismus von V. Jedes $\lambda \in \mathbb{R}$ ist Eigenwert von D:
   Für $f(x) := e^{\lambda x}$ ist $f'(x) = \lambda e^{\lambda x} = \lambda f(x)$, also $D(f) = \lambda f$.

Lemma 5.4.
Seien $\lambda_1, \ldots, \lambda_r \in K$ paarweise verschieden.
Sei V ein K-VR, $f \in End(V)$. Dann ist die Summe $\sum_{i=1}^{r} Eig(f; \lambda_r)$ (von Untervektorräumen von V) direkt.

Beweis:
Seien $v_i \in Eig(f; \lambda_i)$ $(i = 1, \ldots, r)$ mit $v_1 + \ldots + v_r = 0$. Zu zeigen ist $v_1 = \ldots = v_r = 0$.
Angenommen, dies ist falsch, wähle ein Gegenbeispiel mit minimalem r. Dann ist $v_i \neq 0$ für jedes $i = 1, \ldots, r$. Anwendung von f gibt

$$\lambda_1 v_1 + \ldots + \lambda_r v_r = 0 \tag{1}$$

Multipliziere $\sum v_i = 0$ mit λ_1 und ziehe die erhaltene Gleichung von (1) ab:
Erhalte $(\lambda_2 - \lambda_1)v_2 + \ldots + (\lambda_r - \lambda_1)v_r = 0$.
Wegen $\lambda_i - \lambda_1 \neq 0$ $(i = 2, \ldots, r)$ ist das eine kürzere Relation, Widerspruch zur Minimalität.

□

Korollar 5.5.
Ist $\dim(V) = n < \infty$, so hat $f \in End(V)$ höchstens n verschiedene Eigenwerte.

□

Definition 5.6.
Sei $\dim(V) < \infty$. Sei $f \in End(V)$.
f heißt **diagonalisierbar**, wenn es eine Basis $\mathcal{B}$ von V gibt, so dass $M_{\mathcal{B}}^{\mathcal{B}}(f)$ eine Diagonalmatrix ist.
Äquivalent ist: V hat eine Basis aus Eigenvektoren von f.

Korollar 5.7.
Sei $f \in End(V)$. Genau dann ist f diagonalisierbar, wenn $V = \sum_{\lambda \in K} Eig(f; \lambda)$ ist.

Beweis:
Nach Lemma 5.4 ist die Summe direkt.

□

Zusatz:
Ist $\dim(V) = n < \infty$, und hat f n verschiedene Eigenwerte, so ist f diagonalisierbar.
Folgt sofort aus 5.7.

Beispiele 5.8.
Eine Drehung in $\mathbb{R}^2$ ist (für $\alpha \neq \mathbb{Z}\pi$) nicht diagonalisierbar. Eine Spiegelung im $\mathbb{R}^2$ ist diagonalisierbar. Eine Projektion ($p^2 = p$) ist diagonalisierbar.

Bemerkung 5.9.
Diese Konzepte übertragen sich in offensichtlicher Weise auf quadratische Matrizen $A \in M_n(K)$:
A heißt diagonalisierbar, wenn $F_A : K^n \to K^n, x \mapsto Ax$ ein diagonalisierbarer Endomorphismus von K^n ist.
Dies ist äquivalent dazu, dass A zu einer Diagonalmatrix ähnlich ist.
Mit Eigenvektoren bzw. Eigenwerten von A meint man Eigenvektoren bzw. Eigenwerte von F_A.
(EV: $0 \neq x \in K^n$ mit $Ax = \lambda x$)
Ist A diagonalisierbar, und ist $(v_1, \ldots, v_n)$ eine Basis von K^n aus EVen von A, so ist $S^{-1}AS = diag(\lambda_1, \ldots, \lambda_n)$, wobei $S := M(v_1, \ldots, v_n)$.
(v_i sei EV zu λ_i)

b. Das charakteristische Polynom

Sei $\dim(V) = n < \infty$, $f \in End(V)$.

Genau dann ist $\lambda \in K$ EW von f, wenn $\det(\lambda \cdot id_V - f) = 0$ ist.

Definition 5.10.
Für $A \in M_n(K)$ heißt $P_A(t) := \det(t \cdot I_n - A) \in K[t]$ das **charakteristische Polynom von** A.

Hierbei ist $t \cdot I_n - A \in M_n(K[t])$. Siehe Bemerkung 4.55.

Bemerkungen und Beispiele 5.11.

1. Ist $A = (a_{ij}) \in M_n(K)$, so ist $P_A(t) = \begin{vmatrix} t - a_{11} & \dots & -a_{11} \\ -a_{21} & & -a_{2n} \\ \vdots & & \vdots \\ -a_{n1} & \dots & t - a_{nn} \end{vmatrix}$
2. Ist $A = \begin{pmatrix} d_1 & & * \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ Dreiecksmatrix, so ist $P_A(t) = \begin{vmatrix} t - d_1 & & * \\ & \ddots & \\ 0 & & t - d_n \end{vmatrix} = (t - d_1) \cdots (t - d_n)$.
   Allgemeiner gilt der Kästchensatz 4.38 für das charakteristische Polynom,

Korollar 5.12.
Sei $A \in M_n(K)$, sei $\lambda \in K$. Genau dann ist λ ein Eigenwert von A, wenn $P_A(\lambda) = 0$.

□

Satz 5.13.
Ist $A \in M_n(K)$, so ist $P_A(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ mit $a_0, a_1, \ldots, a_{n-1} \in K$. Dabei gilt $a_0 = (-1)^n \cdot \det(A)$ und $a_{n-1} = -tr(A)$.

Beweis:
$a_0 = P_A(0) = \det(0 \cdot I_n - A) = \det(-A) = (-1)^n \cdot \det(A)$. Es ist $P_A(t)$ normiert vom Grad n, denn in der Determinante $P_A(t) = \det(tI_n - A)$ kommt der Summand $\prod_{i=1}^n (t - a_{ii})$

vor. In allen anderen Summanden kommt t in höchstens $n-2$ Faktoren vor. Also ist $P_A(t) = t^n - \left(\sum_{i=1}^{n} a_{ii}\right) t^{n-1} +$ (Terme mit kleineren Potenzen von t).

$\square$

Beispiel 5.14.
Für $A \in M_2(K)$ ist $P_A(t) = t^2 - tr(A) \cdot t + det(A)$.

Satz 5.15.
$A, B \in M_n(K)$, $A \approx B \Rightarrow P_A(t) = P_B(t)$.

Beweis:
$B \approx A$ hieß: $B = SAS^{-1}$ mit $S \in GL_n(K)$. Also ist $P_B(t) = \det(t \cdot I_n - SAS^{-1}) = \det(S \cdot (tI_n - A) \cdot S^{-1}) = \det(S) \cdot P_A(t) \cdot \det(S)^{-1} = P_A(t)$.
(vergleiche 4.55) $\square$

Bemerkung 5.16.
Die Umkehrung von 5.15 ist falsch.
z.B. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ haben $P_A(t) = P_B(t)$, aber $A \not\approx B$ (vergleiche 4.67).

Definition 5.17. (charakteristisches Polynom von Endomorphismen)
Sei $f \in End(V)$. Dann heißt $P_f(t) := P_A(t)$, für $A := M_{\mathcal{B}}^{\mathcal{B}}(f)$ mit $\mathcal{B}$ beliebige Basis von V, das **charakteristische Polynom von** f.
Nach 5.15 hängt die Definition nicht von $\mathcal{B}$ ab.
Es ist klar, dass die zu 5.13 analogen Aussagen für $P_f(t)$ gelten.

Anwendung über $\mathbb{R}$:

Satz 5.18.
Sei V ein $\mathbb{R}$-VR, $\dim(V)$ sei ungerade und sei $f \in End(V)$. Dann hat f einen Eigenwert.

Beweis:
$P_f(t)$ ist ein normiertes Polynom von ungeradem Grad ($= \dim(V)$) über $\mathbb{R}$. Also $P_f(t) = t^n + \ldots$, n ungerade. Es ist $\lim_{x \to -\infty} P_f(x) = -\infty$, $\lim_{x \to +\infty} P_f(x) = +\infty$. Nach dem Zwischenwertsatz folgt: $\exists x \in \mathbb{R}$ mit $f(x) = 0$.

$\square$

Für $\dim(V)$ gerade ist der Satz im Allgemeinen falsch (Bsp. 5.3).

Notation 5.19.
Für Polynome $p, q \in K[t]$ schreibt man $p|q$ („p teilt q"), falls $\exists f \in K[t]$ mit $q = p \cdot f$.

Definition 5.20. (Vielfachheit von Nullstellen)
Sei $p \in K[t]$, $p \neq 0$.

(a) Für $\lambda \in K$ heißt $\mu(p;\lambda) := \max\{k \geqq 0 : (t-\lambda)^k | p\}$ die **Vielfachheit** der Nullstelle λ von p.

(b) p **zerfällt in Linearfaktoren**, falls $\exists c, \lambda_1, \dots, \lambda_n \in K$ mit $p = c \cdot (t-\lambda_1) \cdots (t-\lambda_n)$.

Es gilt: $p(\lambda) = 0 \Rightarrow \mu(p;\lambda) \geqq 1$ (4.6). Allgemeiner:

Lemma 5.21.
Ist $p = (t-\lambda)^k \cdot q$ mit $k \geqq 0$ und $q \in K[t]$, und ist $q(\lambda) \neq 0$, so ist $\mu(p;\lambda) = k$.

Beweis:
$\mu(p;\lambda) \geqq k$ klar.
Angenommen, $\mu(p;\lambda) \geqq k+1$. Dann ist $p = (t-\lambda)^{k+1} \cdot \widetilde{q}$ mit $\widetilde{q} \in K[t]$.
Kürzen durch $(t-\lambda)^k$ (erlaubt, da $K[t]$ nullteilerfrei) gibt $q(t) = (t-\lambda) \cdot \widetilde{q}(t) \Rightarrow q(\lambda) = 0$, Widerspruch.

□

Definition 5.22. (geometrische, algebraische Vielfachheit)
Sei $f \in End(V)$, sei $\lambda \in K$. Dann heißt
$\mu_g(f;\lambda) := \dim(Eig(f;\lambda))$ die geometrische Vielfachheit,
$\mu_a(f;\lambda) := \mu(P_f;\lambda)$ die algebraische Vielfachheit des Eigenwertes λ von f.
Analog definiert man für $A \in M_n(K)$ die Vielfachheiten $\mu_g(A;\lambda)$ und $\mu_a(A;\lambda)$.

Satz 5.23.
Sei $f \in End(V)$, sei U ein Untervektorraum von V mit $f(U) \subset U$. Sei $f|_U : U \to U$ und $\overline{f} : V/U \to V/U$, $\overline{f}(v+U) := f(v) + U$ die von f induzierten Endomorphismen. Dann ist $P_f(t) = P_{f|_U}(t) \cdot P_{\overline{f}}(t)$.
Insbesondere ist $P_{f|_U}(t)$ ein Teiler von $P_f(t)$.

Beweis:
Sei $(v_1, \dots, v_m)$ eine Basis von U, ergänze sie zu einer Basis $\mathcal{B} := (v_1, \dots, v_m, v_{m+1}, \dots, v_n)$

von V. Dann ist $\mathcal{C} := (\overline{v_{m+1}}, \dots, \overline{v_n})$ eine Basis von V/U. Es ist $M^{\mathcal{B}}_{\mathcal{B}} = \left(\begin{array}{c|c} B & * \\ \hline 0 & C \end{array}\right)$, wobei $B \in M_m(K)$ die Matrix von $f|_U$ bezüglich $(v_1, \dots, v_m)$ und C die Matrix von $\overline{f}$ bezüglich $\mathcal{C}$ ist. Kästchensatz (4.38) $\Rightarrow P_f(t) = P_B(t) \cdot P_C(t)$. Dies ist die Behauptung.

□

Satz 5.24.
Sei $f \in End(V)$, sei $\lambda \in K$.

(a) $\mu_g(f;\lambda) = \dim(V) - rk(\lambda \cdot id_V - f)$.

(b) $\mu_a(f;\lambda) \geqq \mu_g(f;\lambda)$.

(c) λ ist Eigenwert von $f \Leftrightarrow \mu_a(f;\lambda) \geqq 1 \Leftrightarrow \mu_g(f;\lambda) \geqq 1$.

Beweis:

(a) klar: $\underbrace{\dim(\ker(\lambda \cdot id_V - f))}_{=\mu_g(\dots)} + \underbrace{\dim(im(\lambda \cdot id_V - f))}_{=rk(\dots)} = \dim(V)$

(b) Sei $U := Eig(f;\lambda)$. Wende Satz 5.23 an: es ist $f(U) = \lambda U \subset U$.
Es folgt: $P_{f|_U}(t) | P_f(t)$. Also $(t-\lambda)^{\mu_g(f;\lambda)} | P_f(t)$, also folgt $\mu_a(f;\lambda) \geqq \mu_g(f;\lambda)$.

(c) λ ist Eigenwert von $f \Leftrightarrow Eig(f;\lambda) \neq \{0\} \Leftrightarrow \mu_g(f;\lambda) \geqq 1$.
Andererseits: λ ist EW von $f \Leftrightarrow P_f(\lambda) = 0 \Leftrightarrow t - \lambda | P_f(t) \Leftrightarrow \mu_a(f;\lambda) \geqq 1$.

□

Bemerkung: Im Allgemeinen kann $\mu_a > \mu_g$ gelten, z.B. für $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ und $\lambda = 0$: $P_A(t) = t^2$, $\mu_a(A;0) = 2$, aber $\mu_g(A;0) = 1$.

Korollar 5.25.
Für $f \in End(V)$ sind äquivalent:

(i) f *ist diagonalisierbar,*

(ii) $P_f(t)$ *zerfällt in Linearfaktoren, und für jeden EW* λ *von* f *(mit* $\mu_a(f;\lambda) \geqq 2$*) ist* $\mu_a(f;\lambda) = \mu_g(f;\lambda)$*.*

Beweis:
(i) $\Rightarrow$ (ii) klar.

(ii) $\Rightarrow$ (i):
Gelte (ii). Der Untervektorraum $\bigoplus\limits_{\lambda\in K} Eig(f;\lambda)$ (Summe ist direkt nach 5.4) hat Dimension $\sum\limits_{\lambda \text{EW von } f} \mu_g(f;\lambda) \underbrace{=}_{(*)} \sum\limits_{\lambda \text{EW von } f} \mu_a(f;\lambda) \underbrace{=}_{(**)} \dim(V)$.
Also ist $V = \bigoplus\limits_{\lambda \text{EW von } f} Eig(f;\lambda)$, d.h. es gilt (i).

Zu (*): $\mu_g(f;\lambda) = \mu_a(f;\lambda)$ gilt auch, wenn $\mu_a(f;\lambda) \leqq 1$ ist: das folgt aus 5.24 (b) und (c).

Zu (**): da $P_f(t)$ nach Voraussetzung zerfällt, gilt (**).

$\square$

Beispiele 5.26.

1 $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ist nicht diagonalisierbar.

2 Sei $A := \begin{pmatrix} 1 & 0 & 0 \\ 3 & -5 & -3 \\ -3 & 6 & 4 \end{pmatrix} \in M_3(K)$. Ist A diagonalisierbar?

Es ist $P_A(t) = (t-1)\cdot(t^2+t-2) = (t-1)^2(t+2)$.
Also Eigenwerte $\lambda_1 = 1$, $\lambda_2 = -2$, $\mu_a(A;1) = 2$, $\mu_a(A;-2) = 1 \Rightarrow \mu_g(A;-2) = 1$.
Um $\mu_g(A;1)$ auszurechnen, berechnen wir $rk(I-A)$:
$I - A = \begin{pmatrix} 0 & 0 & 0 \\ -3 & 6 & 3 \\ 3 & -6 & -3 \end{pmatrix}$. Also ist $rk(I-A) = 1$. (sei $char(K) \neq 3$)
Also $\mu_g(A;1) = 3 - 1 = 2 \Rightarrow A$ ist diagonalisierbar nach Korollar 5.25.

Frage: Wie bestimmt man $S \in GL_3(K)$ mit $S^{-1}AS = diag(1,1,-2)$?

Antwort:

Berechne Basen der Eigenräume von A: man findet $Eig(A;1)$ hat Basis $\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $Eig(A;-2)$ hat Basis $\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$.

$$\Rightarrow S := \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

Bemerkung 5.27.
Wie entscheidet man, ob eine Matrix $A \in M_n(K)$ diagonalisierbar ist, und wie findet man gegebenenfalls eine Diagonalisierung von A?

1. Berechne $P_A(t)$ (cahrakteristisches Polynom von A), prüfe, ob $P_A(t)$ in Linearfaktoren zerfällt. Falls nein, ist A nicht diagonalisierbar.

2. $P_A(t)$ zerfalle in Linearfaktoren. (Diese Zerlegung sei bekannt). Berechne $\mu_g(A;\lambda)$ für jede Nullstelle λ von $P_A(t)$ mit $\mu_a(A;\lambda) \geqq 2$. Falls $\mu_g(A;\lambda) = \mu_a(A;\lambda)$ für diese λ ist, so ist A diagonalisierbar, ansonsten nicht. (NB: $\mu_g(A;\lambda) = n - rk(A - \lambda \cdot I_n)$)

3. Um $S \in GL_n(K)$ mit $S^{-1}AS =$ Diagonalmatrix zu finden, bestimme zu jedem Eigenwert λ von A eine Basis von $Eig(A;\lambda) = \ker(A - \lambda \cdot I_n)$. Sei S die Matrix mit all diesen Basisvektoren als Spalten, dann ist $S^{-1}AS$ eine Diagonalmatrix.

Definition 5.28. (trigonalisierbar)

(a) Ein Endomorphismus $f \in End(V)$ heißt **trigonalisierbar**, falls es eine Basis $\mathcal{B}$ von V gibt, so dass $M_{\mathcal{B}}^{\mathcal{B}}(f)$ eine Dreiecksmatrix ist.

(b) $A \subset M_n(K)$ heißt **trigonalisierbar**, falls $\exists S \in GL_n(K)$, so dass $S^{-1}AS$ eine Dreiecksmatrix ist.

Satz 5.29.
$f \in End(V)$ ist genau dann trigonalisierbar, wenn $P_f(t)$ in Linearfaktoren zerfällt.

Beweis:
„Nur dann“: klar!
„Dann“:
es zerfalle $P_f(t)$ in Linearfaktoren. Induktion nach $\dim(V)$.
Fall $\dim(V) = 1$, ist trivial.
Aussage sei schon für $\dim(V) \leqq n-1$ bewiesen, sei $\dim(V) = n$.
Sei λ ein Eigenwert von f, sei u ein Eigenvektor von f bezüglich λ: $f(u) = \lambda u$, $u \neq 0$.
Sei $U := Ku$, sei $\overline{f} \in End(V/U)$ der von f induzierte Endomorphismus: $\overline{f}(v+U) = f(v) + U$.
Nach Satz 5.23 ist $P_f(t) = (t-\lambda) \cdot P_{\overline{f}}(t)$.
Es folgt: $P_{\overline{f}}(t)$ zerfällt in Linearfaktoren. Nach Induktionsannahme ist also $\overline{f}$ trigonalisierbar. Es gibt also eine Basis $\mathcal{C} := (v_2 + U, \dots, v_n + U)$ von V/U, so dass $C := M^{\mathcal{C}}_{\mathcal{C}}(\overline{f})$ eine obere Dreiecksmatrix ist.

Damit ist $\mathcal{B} := (u) \sqcup \mathcal{C} = (u, v_2, \dots, v_n)$ eine Basis von V, und $M^{\mathcal{B}}_{\mathcal{B}}(f) = \left(\begin{array}{c|c} \lambda & * \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right)$
ist obere Dreiecksmatrix (weil C Dreiecksmatrix), wie gewünscht.

□

Definition 5.30.
Ein Körper K heißt **algebraisch abgeschlossen**, wenn die folgenden äquivalenten Bedingungen gelten.

(i) Jedes $f \in K[t]$ mit $\deg(f) \geqq 1$ hat eine Nullstelle in K;

(ii) jedes $f \in K[t]$ mit $\deg(f) \geqq 1$ zerfällt in Linearfaktoren.

Beweis:
(i) $\Rightarrow$ (ii):
wähle $\lambda \in K$ mit $f(\lambda) = 0$, dann ist $f = (t-\lambda) \cdot g$ mit $\deg(g) < \deg(f)$, nun mache mit g weiter.

□

Beispiele 5.31.
$K = \mathbb{Q}$, $K = \mathbb{R}$ sind nicht algebraisch abgeschlossen. (z.B. hat $t^2 + 1$ keine Nullstellen in K). Ein endlicher Körper K ist niemals algebraisch abgeschlossen: das Polynom $f := 1 + \prod_{a \in K}(t-a)$ hat $\deg(f) = |K|$ und erfüllt $f(a) = 1\ \forall a \in K$.

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen (Fundamentalsatz der Algebra - Beweis irgendwann später mal).

Korollar 5.32.
Jede Matrix $A \in M_n(\mathbb{C})$ ist trigonalisierbar.

□

c. Minimalpolynom, Satz von Cayley-Hamilton

Definition 5.33.
Sei $A \in M_n(K)$. Definiere A^i $(i \geqq 0)$ induktiv durch $A^0 := I$, $A^{i+1} := A \cdot A^i$ $(i \geqq 0)$. Für $p = \sum_{i=0}^{m} a_i t^i$ sei $p(A) := \sum_{i=0}^{m} a_i A^i \in M_n(K)$: wir haben die Matrix A in das Polynom $p = p(t)$ eingesetzt.

Analog für $f \in End(V)$: $f^0 := id_V$, $f^{i+1} := f \circ f^i$ $(i \geqq 0)$. Für $p = p(t)$ wie oben definiere $p(f) := \sum_{i=0}^{m} a_i f^i \in End(V)$.

Lemma 5.34.
Sei $A \in M_n(K)$.

(a) *Die Einsetzabbildung $K[t] \to M_n(K)$, $p \mapsto p(A)$ ist ein Ringhomomorphismus. Ihr Bild ist der Teilring $K[A] := \{p(A) : p \in K[t]\}$ von $M_n(K)$; dieser Teilring ist kommutativ.*

(b) *Für $S \in GL_n(K)$ und $p \in K[t]$ ist $p(SAS^{-1}) = S \cdot p(A) \cdot S^{-1}$.*
Insbesondere ist $K[SAS^{-1}] = S \cdot K[A] \cdot S^{-1}$.

Beweis:

(a) Kommutativität: $p_1(A) \cdot p_2(A) = (p_1 p_2)(A) = (p_2 p_1)(A) = p_2(A) \cdot p_1(A)$.

(b) $(SAS^{-1})^i = \underbrace{(SAS^{-1}) \cdot (SAS^{-1}) \cdots (SAS^{-1})}_{i \text{ Faktoren}} = S \cdot A^i \cdots S^{-1}$.

Ist $p(t) = \sum_{i=0}^{m} a_i t^i$, so also $p(SAS^{-1}) = \sum_{i=0}^{m} a_i (SAS^{-1})^i = S \cdot \left(\sum_{i=0}^{m} a_i A^i \right) S^{-1} = S \cdot p(A) \cdot S^{-1}$.

□

Analoges Lemma für Endomorphismen.

Definition und Satz 5.35.
Sei $A \in M_n(K)$, sei V ein K-VR ($\dim(V) < \infty$) und $f \in End(V)$.

(a) *Es gibt ein eindeutig bestimmtes normiertes Polynom $q(t), q \neq 0$, kleinsten Grades mit $q(A) = 0$.*

(b) *Es gibt ein eindeutig bestimmtes normiertes Polynom $q(t), q \neq 0$, kleinsten Grades mit $q(f) = 0$.*

(c) *Das Polynom q wie in (a) bzw. (b) heißt das **Minimalpolynom** Q_A von A bzw. Q_f von f.*

Vorbemerkung:
Gibt es ein $p \in K[t]$ mit $\deg(p) = d$ und $p(A) = 0$, so gibt es auch ein *normiertes* solches Polynom: nämlich $\widetilde{p} := \frac{1}{a} \cdot p$, wobei a der Leitkoeffizient von p sei.

Beweis:
Die $n^2 + 1$ Matrizen $I, A, A^2, \ldots, A^{n^2}$ sind linear abhängig.
Also gibt es ein Polynom $p \in K[t], p \neq 0$, mit $\deg(p) \leqq n^2$ und $p(A) = 0$.
Es gibt also auch ein Polynom p kleinsten Grades mit dieser Eigenschaft (nach Vorbemerkung können wir p normiert annehmen).
Sei $\widetilde{p} \in K[t]$ normiert mit $\widetilde{p}(A) = 0$ und $\deg(\widetilde{p}) = \deg(p)$, zu zeigen: $\widetilde{p} = p$.
Für das Polynom $p - \widetilde{p}$ gilt: $\deg(p - \widetilde{p}) < \deg(p) = \deg(\widetilde{p})$, und $(p - \widetilde{p})(A) = p(A) - \widetilde{p}(A) = 0$.
Also ist $p - \widetilde{p} = 0$ (wegen der Minimalität von p), also $p = \widetilde{p}$.

□

Beispiele 5.36.

1. Ist $f = c \cdot id_V$, so ist $Q_f(t) = t - c$.

   Ist f eine Projektion (d.h. $f^2 = f$), so ist $Q_f(t) = t^2 - t$ (außer falls $f = 0$ oder $f = id$).

2. Ist $f \in End(V)$ und $\mathcal{B}$ eine Basis von V, so ist $Q_f = Q_A$ für $A = M_{\mathcal{B}}^{\mathcal{B}}(f)$.

Lemma 5.37.
Sei $A \in M_n(K)$, sei Q_A das Minimalpolynom.

(a) *Ist $p \in K[t]$ mit $p(A) = 0$, so ist $Q_A | p$.*

(b) *Ist $B \approx A$, so ist $Q_B(t) = Q_A(t)$.*

Beweis:

(a) Sei $p(A) = 0$. Division mit Rest gibt $p = q \cdot Q_A + r$ mit $q, r \in K[t]$ und $\deg(r) < \deg(Q_A)$. Einsetzen von A gibt $\underbrace{p(A)}_{=0} = q(A) \cdot \underbrace{Q_A(A)}_{=0} + r(A)$
$\Rightarrow r(A) = 0$. Wegen $\deg(r) < \deg(Q_A)$ ist $r = 0$.

(b) klar aus 3.58, oder mit Lemma 5.34.

□

Theorem 5.38. *(Cayley-Hamilton)*
Für jedes $A \in M_n(K)$ ist $p_A(A) = 0$.
($p_A :=$ charakteristisches Polynom von A)
Dieselbe Aussage für $f \in End(V)$.

Beweis:
Jede Matrix $C \in M_n(K[t])$ hat eine eindeutige Darstellung $C = \sum_{i=0}^{m} t^i C_i$ mit $m \in N_0$, Matrizen $C_0, \ldots, C_m \in M_n(K)$. Wir schreiben $(t \cdot I_n - A)^\sharp$ in dieser Weise: $(t \cdot I_n - A)^\sharp = \sum_{i=0}^{m} t^i B_i$ mit $B_i \in M_n(K)$, $i = 0, \ldots, m$.
$(t \cdot I_n - A)^\sharp \cdot (t \cdot I_n - A) = \det(t \cdot I_n - A) \cdot I_n = P_A(t) \cdot I_n$ (4.55). Das bedeutet $(t^m B_m + \ldots + tB_1 + B_0)(tI_n - A) = t^n(a_n I) + \ldots + t(a_1 I) + (a_0 I))$, wobei $P_A(t) = a_n t^n + \ldots + a_1 t + a_0$ sei.

Multipliziere aus, ordne nach Potenzen von t, und vergleiche: dies ergibt $m + 1 = n$ (sei $B_m \neq 0$) und

(1) $B_{n-1} = a_n I$ (t^n)

(2) $-B_i A + B_{i-1} = a_i I$ $(t^i, i = 1, \dots, n-1)$

(3) $-B_0 A = a_0 I$ (t^0)

Multipliziere (1) mit A^n, (2) mit A^i, (3) mit $A^0 = I$: und addiere die Gleichungen.
Die rechte Seite ist $p_A(A)$.
Die linke Seite ist $B_{n-1}A^n + (-B_{n-1}A + B_{n-2})A^{n-1} + \ldots + (-B_1 A + B_0)A - B_0 A = 0$.

□

Zum Satz von Cayley-Hamilton ist folgende Formulierung äquivalent:

Korollar 5.39.
Für jede Matrix $A \in M_n(K)$ ist $Q_A(t) | P_A(t)$.

□

Bemerkung 5.40.
Über $K = \mathbb{C}$ können wir einen leichteren Beweis von Cayley-Hamilton (5.38) geben:
Sei $A \in M_n(\mathbb{C})$. Es genügt, dies für A = Dreiecksmatrix zu zeigen. Denn es gibt $S \in GL_n(K)$ mit $S^{-1}AS =: \widetilde{A}$ Dreiecksmatrix, und es ist $P_A(t) = P_{\widetilde{A}}(t)$, also $P_A(A) = P_{\widetilde{A}}(A) = P_{\widetilde{A}}(S\widetilde{A}S^{-1}) = S \cdot \underbrace{P_{\widetilde{A}}(\widetilde{A})}_{=0 \text{ n.V.}} \cdot S^{-1}$

Ist A diagonalisierbar, so ist Cayley-Hamilton klar:
$A = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$, $P_A(t) = \prod_{i=1}^{n}(t - a_i)$, also $P_A(A) = (A - a_1 I) \cdots (A - a_n I) =$
$$\begin{pmatrix} 0 & & & \\ & * & & \\ & & \ddots & \\ & & & * \end{pmatrix}\begin{pmatrix} * & & & \\ & 0 & & \\ & & \ddots & \\ & & & * \end{pmatrix} \cdots \begin{pmatrix} * & & & \\ & \ddots & & \\ & & * & \\ & & & 0 \end{pmatrix} = 0.$$
Also ist Cayley-Hamilton auch richtig für diagonalisierbares A.

Die Abbildung $M_n(\mathbb{C}) \to M_n(\mathbb{C}), A \mapsto P_A(A)$. ist stetig. Ist jetzt A eine Dreiecksmatrix, so lässt sich A beliebig gut durch diagonalisierbare Matrizen approximieren.
$A = (a_{ij}) \Rightarrow \forall \varepsilon > 0\ \exists B(b_{ij})$ diagonalisierbar mit $|a_{ij} - b_{ij}| < \varepsilon\ \forall i, j$.

Denn: $A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$. Ändere die Diagonalelemente so ab, dass sie paarweise verschieden werden, diese Matrix ist dann diagonalisierbar.
Aus Stetigkeitsgründen folgt also $P_A(A) = 0$ für die Dreiecksmatrix A.

(K beliebig)

Korollar 5.41.
Sei $A \in M_n(K)$, sei $Q_A(t)$ das Minimalpolynom. Dann ist $\deg(Q_A) \leqq n$, und der K-VR $K[A]$ hat die Dimension $\dim(K[A]) = \deg(Q_A)$.

Beweis:
erste Aussage:
folgt aus $Q_A | P_A$ und $\deg(P_A) = n$.

zweite Aussage:
$K[A]$ wird als K-VR erzeugt von den $A^i, i \geqq 0$. Wegen $Q_A(A) = 0$ sind $I, A, A^2, \ldots, A^d$ $(d := \deg(Q_A))$ linear abhängig, aber $I, A, \ldots, A^{d-1}$ sind linear unabhängig. Also ist $I, A, \ldots, A^{d-1}$ eine Basis von $K[A]$.

□

Bemerkung 5.42.

1. Wir haben bereits gesehen, dass $\deg(Q_A) < n$ sein kann, für $A \in M_n(K)$. (z.B. Projektionen).

2. Ist A invertierbar, so können wir A^{-1} als Polynom in A schreiben:
   Sei $P_A(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$, es ist $a_0 = (-1)^n \det(A) \neq 0$. Aus $P_A(A) = 0$ folgt also $A(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1 I) = -a_0 I$
   $\Rightarrow A^{-1} = \frac{1}{-a_0}(A^{n-1} + a_{n-1}A^{n-2} + \ldots + a_1 I)$.

   Für $n = 2$ bedeutet das $A^{-1} = \frac{1}{\det(A)}(tr(A) \cdot I - A)$.

d. Jordansche Normalform

Stets: V ein K-Vektorraum, $\dim(V) < \infty$.

Definition 5.43.
Sei $f \in End(V)$. Ein Unter-VR U von V heißt f-**invariant**, wenn $f(U) \subset U$ ist.

Bemerkung 5.44.
Nützlichkeit von f-invarianten UR:
Sei U f-invariant, sei $\mathcal{F}$ eine Basis von U, ergänzt zu einer Basis $\mathcal{B} = \mathcal{F} \sqcup \mathcal{G}$ von V. Dann ist $M^{\mathcal{B}}_{\mathcal{B}}(f) = \left(\begin{array}{c|c} B & * \\ \hline 0 & * \end{array}\right)$ mit $B = M^{\mathcal{F}}_{\mathcal{F}}(f|_U)$.

Beispiele von f-invarianten UR: die $U = Eig(f, \lambda)$ oder $U = im(f)$.
Allgemeiner:

Lemma 5.45.
Sei $f \in End(V)$, sei auch $g \in End(V)$ mit $f \circ g = g \circ f$. Dann sind die Unterräume $\ker(g)$ *und $im(g)$ f-invariant.*

Beweis:
$\ker(g)$: ist $u \in \ker(g)$, so $g(f(u)) = f(g(u)) = 0$, also $f(u) \in \ker(g)$.
$im(g)$: ist $u = g(v) \in im(g)$, mit $v \in V$, so $f(u) = f(g(v)) = g(f(v)) \in im(g)$.

$\square$

Definition 5.46.
Ein Endomorphismus $f \in End(V)$ heißt **nilpotent**, falls ein $k \in \mathbb{N}$ existiert mit $f^k = 0$.
Das kleinste solche k heißt der **Nilpotenzindex** von f.

(die analoge Definition für Matrizen)

Beispiel 5.47.

1. $A := \begin{pmatrix} 6 & -4 \\ 9 & -6 \end{pmatrix}$ hat $A^2 = 0$, also ist A nilpotent vom Index 2.

2. Ist $f \in End(V)$ und $A = M^{\mathcal{B}}_{\mathcal{B}}(f)$ mit einer Basis $\mathcal{B}$ von V, so gilt: f ist nilpotent $\Leftrightarrow$ A ist nilpotent.

3. $A, B \in M_n(K)$ mit $A \approx B$, so gilt: A ist nilpotent $\Leftrightarrow$ B ist nilpotent.

Lemma 5.48.
Sei $\dim(V) = n < \infty$, *sei* $f \in End(V)$. *Genau dann ist* f *nilpotent, wenn* $M_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{pmatrix} 0 & & & * \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}$ *für eine geeignete Basis* $\mathcal{B}$ *von* V *ist. In diesem Fall ist* $f^n = 0$.

Beweis:
„$\Leftarrow$“: Sei $M_{\mathcal{B}}^{\mathcal{B}}(f) = (a_{ij}) =: A$ mit $a_{ij} = 0$ für $i \geqq j$, dann ist A^n.
Klar mit Cayley-Hamilton, oder direkt: $A^n =: (b_{ij})$ mit $b_{ij} = \sum_{k_1=1}^{n} \dots \sum_{k_{n-1}=1}^{n} \underbrace{a_{i,k_1} \cdot a_{k_1,k_2} \cdots a_{k_{n-1},j}}_{=0} = 0$ (ansonsten müsste $i < k_1 < \ldots < k_{n-1} < j$ sein, also $j - i \geqq n$).

„$\Rightarrow$“: sei f nilpotent, Induktion nach $\dim(V)$.
$\dim(V) = 1$: klar. Sei also $\dim(V) = n > 1$. Sei $f^k = 0$ und $f^{k-1} neq 0$ (also $k =$Nilpotenzindex von f).
Sei $U := \ker(f^{k-1})$. Es ist $U \neq V$ (wegen $f^{k-1} \neq 0$) und $f(V) \subset U$, denn $0 = f^k = f^{k-1} \circ f$. Insbesondere ist $f(U) \subset U$, und $f|_U \in End(U)$ ist nilpotent.
Nach Induktionsannahme gibt es also eine Basis $\mathcal{F}$ von U, so dass $M_{\mathcal{F}}^{\mathcal{F}}(f|_U) =: B = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$ ist.
Ergänze $\mathcal{F}$ zu einer Basis $\mathcal{B} = \mathcal{F} \sqcup \mathcal{G}$ von V, dann $M_{\mathcal{B}}^{\mathcal{B}}(f) = \left(\begin{array}{c|c} B & * \\ \hline 0 & 0 \end{array}\right)$.

□

In Sprache der Matrizen: $A \in M_n(K)$ ist genau dann nilpotent, wenn $A \approx \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$ ist; dann gilt $A^n = 0$.

Korollar 5.49.
Sei $\dim(V) = n$ *und* $f \in End(V)$. *Dann gilt:*
f *ist nilpotent* $\Leftrightarrow$ $f^n = 0 \Leftrightarrow P_f(t) = t^n$.

Beweis:
f ist nilpotent $\Rightarrow P_f(t) = t^n$ (5.48)
$P_f(t) = t^n \Rightarrow f^n = 0$ (Cayley-Hamilton)
$f^n = 0 \Rightarrow f$ ist nilpotent.

□

Lemma 5.50.
Sei $\dim(V) = n < \infty$*, sei* $f \in End(V)$*.*
Sei $r := \mu_a(f; 0)$*.*

(a) *Es gibt eine Zahl* $0 \leqq d \leqq r$*, so dass gelten:*

(1) $\{0\} = \ker(f^0) \subsetneq \ker(f) \subsetneq \ker(f^2) \subsetneq \ldots \subsetneq \ker(f^d) = \ker(f^{d+1}) = \ldots$

(2) $V = im(f^0) \supsetneq im(f) \supsetneq im(f^2) \supsetneq \ldots \supsetneq im(f^d) = im(f^{d+1}) = \ldots$

Wir setzen $U := \ker(f^d)$ *und* $W := im(f^d)$*. Es gelten weiter:*

(b) $\dim(U) = r$, $\dim(W) = n - r$;

(c) $V = U \oplus W$;

(d) *U und W sind f-invariant, und* $f|_U \in End(U)$ *ist nilpotent, und* $f|_W \in End(W)$ *ist bijektiv.*

Beweis:
Setze $U_i := \ker(f^i)$ $(i = 0, 1, 2, \ldots)$.
Habe also $\{0\} = U_0 \subset U_1 \subset U_2 \subset \ldots$. Wegen $\dim(V) < \infty$ kann nur endlich oft $\neq$ gelten. Für alle $i \geqq 1$ gilt $U_i = f^{-1}(U_{i-1})$, denn für $v \in V$ gilt: $v \in f^{-1}(U_{i-1}) \Leftrightarrow f(v) \in U_{i-1} \Leftrightarrow f^{i-1}(f(v)) = 0 \Leftrightarrow v \in U_i$.
Daraus folgt: ist $U_i = U_{i+1}$ für ein i, so ist auch $U_i = U_{i+1} = U_{i+2} = \ldots$
Daher gibt es ein $d \geqq 0$ mit (1). Für die $W_i := im(f^i)$ gilt $\dim(U_i) + \dim(W_i) = n$; wegen $V \supset W_1 \supset W_2 \supset \ldots$ muss also (2) gelten.

Es ist klar, dass $d \leqq \dim(U_d)$ ist. Wir setzen $U := U_d$, $W := W_d$. U, W sind f-invariant (nach Lemma 5.45), und $f|_U$ ist nilpotent wegen $(f|_U)^d = 0$.
Wegen $f(W) = W_{d+1} = W_d = W$ ist $f|_W \in End(W)$ surjektiv, also auch bijektiv (da

$\dim(W) < \infty$). Also ist $U \cap W = \ker(f^d) \cap W = \{0\}$. Wegen $\dim(U) + \dim(W) = \dim(V)$ folgt $V = U \oplus W$.

Zu zeigen bleibt $\dim(U) = r$ ($\Rightarrow r = \dim(U) \geqq d$).
Es ist $P_f(t) = P_{f|_U}(t) \cdot P_{f|_W}(t)$ (siehe 5.23). Wegen $f|_U$ nilpotent ist $P_{f|_U}(t) = t^{\dim(U)}$ (siehe 5.49), wegen $f|_W$ injektiv ist t kein Teiler von $P_{f|_W}(t)$. ($P_{f|_W}(0) = \pm\det(f|_W) \neq 0$)
Also ist $r = \mu_a(f;0) = \dim(U)$.

□

Korollar 5.51. *(Verallgemeinerung von 5.50)*
Sei $\dim(V) = n$, *sei* $f \in End(V)$, *sei* $\lambda \in K$ *und sei* $r := \mu_a(f;\lambda)$. *Für die Unterräume* $U(\lambda) := \ker((f - \lambda id)^r)$ *und* $W(\lambda) := im((f - \lambda id)^r)$ *von* V *gilt:*

(a) $U(\lambda) \oplus W(\lambda) = V$,

(b) $U(\lambda)$ *und* $W(\lambda)$ *sind* f*-invariant,*

(c) $\dim(U(\lambda)) = r$, $\dim(W(\lambda)) = n - r$,

(d) $P_{f|_{U(\lambda)}}(t) = (t - \lambda)^r$, *und* λ *ist kein Eigenwert von* $f|_W$.

Beweis:
Sei $g := f - \lambda id$, dann ist $P_g(t) = \det(t \cdot id - g) = \det((t + \lambda) \cdot id - f) = P_f(t + \lambda)$.
Habe $P_f(t) = (t - \lambda)^r \cdot Q(t)$ mit $Q(t) \neq 0 \Rightarrow P_g(t) = t^r \cdot \underbrace{Q(t + \lambda)}_{=:\widetilde{Q}(t)}$ mit $\widetilde{Q}(0) = Q(\lambda) \neq 0$.

Also ist $r = \mu(g;0)$. Wende nun 5.50 an auf g: es ist $\ker(g^r) = \ker((f - \lambda id)^r) = U(\lambda)$, $im(g^r = W(\lambda)$ und wir erhalten alle Aussagen aus 5.50 für g.

Nebenbemerkung:
Erhalte: $U(\lambda)$, $W(\lambda)$ sind g-invariant $\Rightarrow$ auch f-invariant).

□

Definition 5.52. (Hauptraum)
Sei $\dim(V) = n$, sei $f \in End(V)$.
Für $\lambda \in K$ heißt $Hau(f;\lambda) := \ker((f - \lambda id)^n)$ der **Hauptraum** von f zum Parameter λ.
Es ist also $Hau(f;\lambda) = \ker((f - \lambda id)^k)$ für alle $k \geqq r = \mu_a(f;\lambda)$.

SATZ 5.53. *(Hauptraumzerlegung)*
Sei $f \in End(V)$, sei $P_f(t) = \prod_{i=1}^{k}(t-\lambda_i)^{r_i}$ mit $\lambda_1, \ldots, \lambda_k \in K$ paarweise verschieden, und $r_i \in \mathbb{N}$. Dann gilt:

(a) $V = Hau(f;\lambda_1) \oplus \ldots \oplus Hau(f;\lambda_k)$,

(b) *Die $Hau(f;\lambda_i)$ sind f-invariant,*

(c) $\dim(Hau(f;\lambda_i)) = r_i$ $(i = 1, \ldots, k)$

(d) *$f|_{Hau(f;\lambda_i)}$ hat charakteristisches Polynom $(t-\lambda_i)^{r_i}$ $(i = 1, \ldots, k)$.*

Bezüglich einer geeigneten Basis hat f also folgende Matrix (*):

$$\begin{pmatrix} \boxed{\begin{matrix}\lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_1\end{matrix}} & & & 0 \\ & \boxed{\begin{matrix}\lambda_2 & & * \\ & \ddots & \\ 0 & & \lambda_2\end{matrix}} & & \\ & & \ddots & \\ 0 & & & \boxed{\begin{matrix}\lambda_k & & * \\ & \ddots & \\ 0 & & \lambda_k\end{matrix}} \end{pmatrix}$$

Dabei hat das i-te Kästchen die Größe $r_i \times r_i$ $(i = 1, \ldots, k)$.

BEWEIS:
(b) und (c) wurden in 5.51 bewiesen.
(a) folgt aus (b) und folgendem allgemeineren Lemma.

□

Lemma 5.54.
$f \in End(V)$, $\lambda_1, \ldots, \lambda_k \in K$ paarweise verschieden. Dann ist die Summe $\sum\limits_{i=1}^{k} Hau(f;\lambda_i)$ direkt.

Beweis:
Das Lemma ist analog zu 5.4, und sein Beweis ist ebenfalls:
Seien $x_i \in Hau(f;\lambda_i)$ $(i = 1, \ldots, k)$ mit $x_1 + \ldots + x_k = 0$. Zu zeigen: Jedes $x_i = 0$.
Angenommen falsch, sei $x_1 + \ldots + x_k = 0$ von minimaler Länge k mit $x_1 \neq 0, \ldots, x_k \neq 0$.Anwenden von $(f - \lambda_1 id)^n$ (mit $n = \dim(V)$) auf die Gleichung gibt neue Identität $y_2 + \ldots + y_k = 0$, mit $y_i := (f - \lambda_1 id)^n(x_i)$ $(i = 2, \ldots, k)$.
Die $Hau(f;\lambda_i)$ sind invariant unter f, also auch unter $(f - \lambda_1)^n$, also ist $y_i \in Hau(f;\lambda_i)$, $i = 2, \ldots, k$.
Da $f|_{Hau(f;\lambda_i)}$ nur den Eigenwert λ_i hat, ist $y_i \neq 0$ für $i = 2, \ldots, k$. $\Rightarrow$ Widerspruch zur minimalen Wahl der Gleichung $\sum x_i = 0$.

□

Korollar 5.55. *(Jordan-Chevalley Zerlegung)*
Sei $A \in M_n(K)$, so dass $P_A(t)$ in Linearfaktoren zerfällt. Dann gibt es eine diagonalisierbare Matrix D und eine nilpotente Matrix M mit $A = D + N$ und $DN = ND$.

Beweis:
Nach 5.53 gibt es $S \in GL_n(K)$, so dass $\widetilde{A} := S^{-1}AS$ aus 5.53 (d) hat. Setze $\widetilde{D} := diag(\underbrace{\lambda_1, \ldots, \lambda_1}_{r_1}, \ldots, \underbrace{\lambda_k, \ldots, \lambda_k}_{r_k})$ und $\widetilde{N} := \widetilde{A} - \widetilde{D}$. Dann ist $\widetilde{N}$ nilpotent, und $\widetilde{D}\widetilde{N} = \widetilde{N}\widetilde{D}$ (klar aus Kätchenweiser Argumentation). Setze $D := S\widetilde{D}S^{-1}$ und $N := S\widetilde{N}S^{-1}$, dann D diagonalisierbar, N nilpotent, $A = D + N$ und $DN = S\widetilde{D}S^{-1}\dot{S}\widetilde{N}S^{-1} = S\widetilde{D}\widetilde{N}S^{-1} = S\widetilde{N}\widetilde{D}S^{-1} = S\widetilde{N}S^{-1} \cdot S\widetilde{D}S^{-1} = ND$.

□

Bemerkung 5.56.

1. Um die Jordan-Chevalley-Zerlegung von A zu bestimmen, genügt es im Allgemeinen *nicht*, A in Dreiecksform zu bringen, und dann A in Diagonale und Rest zu zerlegen. Beispiel:
   $A := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$; für $D := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, $N := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ ist $DN \neq ND$.

   Um die Jordan-Chevalley-Zerlegung von A zu bestimmen, geht man wie folgt vor:

zerlege $P_A(t)$ in Linearfaktoren, und berechne Basen der Haupträume $Hau(A;\lambda_i)$. Beispiel: nochmal A wie oben. $\Rightarrow P_A(t) = (t-1)^2(t-2)$. Man findet $Hau(A;1) = \ker((A-I)^2)$ mit Basis (e_1, e_2), und $Hau(A;2) = Eig(A;2)$ mit Basisvektor $e_1 + e_3$.

Sei $S = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ die Matrix mit diesen Basisvektoren als Spalten, dann gilt $S^{-1}AS = \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 2 \end{array}\right)$ die Gestalt (*) aus 5.53. Daher ist die Jordan-Chevalley-Zerlegung $A = D+N$ von A gegeben durch $D = S\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}S^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, $N = SE_{12}S^{-1} = E_{12} = A - D$.

2. Man kann zeigen, dass die Jordan-Chevalley-Zerlegung $A = D + N$ von A eindeutig bestimmt ist.

3. Insbesondere haben wir jetzt auch gesehen, wie man eine Matrix trigonalisiert (wenn $P_A(t)$ in Linearfaktoren zerlegt; sonst nicht möglich).

Notation 5.57. (Jordan-Kästchen)

Für $\lambda \in K$ und $m \in \mathbb{N}$ heißt die Matrix $J_m(\lambda) := \begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} = \lambda I + \sum_{i=1}^{m-1} E_{i,i+1} \in M_m(K)$ heißt **Jordan-Kästchen** (der Größe m zum Parameter λ).

Satz 5.58.
Sei $f \in End(V)$ mit $P_f(t) = (t-\lambda)^n$ für ein $\lambda \in K$. Bezüglich einer geeigneten Basis von V wird f dann durch eine Matrix der Gestalt $\begin{pmatrix} \boxed{J_{m_1}(\lambda)} & & 0 \\ & \ddots & \\ & & \boxed{J_{m_r}(\lambda)} \end{pmatrix}$ beschrieben mit $m_1 \geqq \ldots \geqq m_r \geqq 1$ (und $\sum_{i=1}^{r} m_i = n$).
Unter dieser Bedingung sind r und $m_1, \ldots, m_r$ sogar eindeutig bestimmt.

Beweis:
Sei O.E. $\lambda = 0$ (ansonsten ersetze f durch $g := f - \lambda \cdot id$). Also ist f nilpotent,

sei d der Nilpotenzindex von f: $f^d = 0 \neq f^{d-1}$. Wir übernehmen aus Beweis von 5.50: $U_i := \ker(f^i), i = 0, 1, 2, \ldots$; es ist $\{0\} = U_0 \subsetneq U_1 \subsetneq \ldots \subsetneq U_d = V$; die U_i sind f-invariant, und $U_i = f^{-1}(U_{i-1})$ $(i = 1, \ldots, d)$.
Sei L_d ein Untervektorraum von V mit $(V =)U_d = L_d \oplus U_{d-1}$.
Es folgt $f(L_d) \subset U_{d-1}$, und $L_d \cap f^{-1}(U_{d-2}) = L_d \cap U_{d-1} = \{0\}$. Insbesondere also $f(L_d) \cap U_{d-2} = \{0\}$.
Daher gibt es einen UR L_{d-1} von U_{d-1} mit $f(L_d) \subset L_{d-1}$ und $U_{d-1} = L_{d-1} \oplus U_{d-2}$.
Induktiv finden wir so für jedes $i = d, d-1, d-2, \ldots, 1$ einen UR L_i von U_i mit $U_i = L_i \oplus U_{i-1}$ und $f(L_{i+1}) \subset L_i$ (für $i < d$). Insbesondere ist $L_1 = U_1$, und somit haben wir
$V = U_d$
$= U_{d-1} \oplus L_d$
$= U_{d-2} \oplus L_{d-1} \oplus L_d$
$= \ldots$
$= L_1 \oplus L_2 \oplus \ldots \oplus L_d$.

Wegen $L_1 = \ker(f)$ ist die Restriktion von f auf $L_2 \oplus \ldots \oplus L_d$ injektiv.

Sei $\mathcal{B}$ eine Basis von L_d. Dann ist $f(\mathcal{B}_d)$ eine linear unabhängige Familie in L_{d-1}. Wähle Familie $\mathcal{B}_{d-1}$, so dass $f(\mathcal{B}_d) \sqcup \mathcal{B}_{d-1}$ eine Basis von L_{d-1} ist. Fahre so fort, und erhalte folgende Basen der L_i (**):

$$\begin{array}{ll} L_d: & \mathcal{B}_d \\ L_{d-1}: & f(\mathcal{B}_d) \sqcup \mathcal{B}_{d-1} \\ \vdots & \vdots \\ L_1: & f^{d-1}(\mathcal{B}_d) \sqcup f^{d-2}(\mathcal{B}_{d-1}) \sqcup \ldots \sqcup f(\mathcal{B}_2) \sqcup \mathcal{B}_1 \end{array}$$

Die Gesamtheit aller dieser Vektoren (**) bildet eine Basis von V. Für jeden Vektor v aus $\mathcal{B}_i$ $(i = 1, \ldots, d)$ ist nun $C_v := (f^{i-1}(v), \ldots f(v), v)$ die Basis eines f-invarianten Unterraums $W(v)$ von V, denn $f^i(v) = 0$. Die Matrix von $f|_{W(v)}$ bezüglich C_v ist
$\begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} = J_i(0)$. Die Gesamtheit der Vektoren in (**) können wir also so anordnene, dass f bezüglich dieser Basis von V eine Matrix wie gewünscht erhätlt: beginne mit den Familien C_v für v in $\mathcal{B}_d$, nimm dann die C_v für v in $\mathcal{B}_{d-1}$, usw.
Die so erhaltene Matrix von f hat genau $s_i := |\mathcal{B}_i|$ viele Jordankästchen $J_i(0)$, für $i = 1, \ldots, d$. Es ist $|\mathcal{B}_i| = \dim(L_i) - \dim(L_{i+1})$ nach Konstruktion. Andererseits ist $\dim(L_i) \dim(U_i) - \dim(U_{i+1})$. Somit ist
$s_i = \dim(U_i) - \dim(U_{i-1}) - \dim(U_{i+1}) + \dim(U_i) = 2\dim(U_i) - \dim(U_{i-1}) - \dim(U_{i+1})$.
Wegen $\dim(U_i) \ker(f^i)$ hängen die s_i nur von f ab, sond also eindeutig bestimmt.
$\square$

Theorem 5.59. *(Jordan'sche Normalform)*
Sei $f \in End(V)$, und $P_f(t)$ zerfalle in Linearfaktoren. Dann gibt es eine Basis von V, bezüglich der f beschrieben wird durch eine Matrix $\begin{pmatrix} \boxed{J_{m_1}(\lambda_1)} & & 0 \\ & \ddots & \\ & & \boxed{J_{m_r}(\lambda_r)} \end{pmatrix}$ *mit $r, m_1, \dots, m_r \in \mathbb{N}$ und $\lambda_1, \dots, \lambda_r \in K$.*

Die Folge der Paare $(m_1, \lambda_2), \dots, (m_r, \lambda_r)$ ist bis auf Permutation eindeutig bestimmt.

Zusatz 5.60.
Ist $\lambda \in K$ ein Eigenwert von f, und setzt man $r_i(\lambda) := rk((f - \lambda id)^i)$ $(i = 0, 1, 2, \dots)$, so ist für $m \geqq 1$ die Anzahl s_m der Jordan-Kästchen $J_m(\lambda)$ der Größe m gegeben durch

$$\boxed{s_m = r_{m-1}(\lambda) - 2r_m(\lambda) + r_{m+1}(\lambda)}$$

Beweis:
Siehe Beweis von 5.58: Mit $U_i := \ker((f - \lambda id)^i)$ hatten wir gesehen $s_m = 2\dim(U_m) - \dim(U_{m-1}) - \dim(U_{m+1})$. Wegen $r_i(\lambda) = \dim(V) - \dim(U_i)$ folgt die Behauptung.
□

Bemerkung 5.61.

1. Das Zerfallen von $P_f(t)$ ist natürlich auch notwendig für die Existenz der Jordan-Normalform von f.

2. Es zerfalle $P_A(t)$ (für gegebene Matrix $A \in M_n(K)$). Will man nur die Jordan-Normalform von A ausrechnen, muss man folgendes tun:
   $P_A(t)$ berechnen und in seine LInearfaktoren zerlegen. Für jede Nullstelle λ von $P_A(t)$ (mit $\mu_a(A; \lambda) \geqq 2$) bestimmt man die Ränge von $((A - \lambda I)^i)$ für $i = 1, 2, \dots, \mu_a(A; \lambda)$.
   Daraus liest man die Größen der Jordankästchen zum Eigenwert λ ab, siehe Zusatz 5.60.

   Will man auch eine zugehörige Transformationsmatrix bestimmen, muss man Basen der Haupträume von A finden, und dabei wie im Beweis von 5.58 vorgehen:

Beispiel 5.62.

Gegeben sei $A := \begin{pmatrix} 0 & -1 & 1 \\ 0 & 1 & 0 \\ -1 & -1 & 2 \end{pmatrix} \in M_n(K)$.

Man findet $P_A(t) = (t-1)^3$ und $A - I = \begin{pmatrix} -1 & -1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & 1 \end{pmatrix}$ und $(A-I)^2 = 0$. Also ist $rk(A-I) = 1$ und $rk((A-I)^2) = 0$.

Man liest aus $rk(A-I) = 1$ schon ab, dass es genau $2 = \dim(\ker(A-I))$ Jordan-Kästchen gibt. Also ist die Jordan-Normalform von A gleich $B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Um eine konkrete Matrix $S \in GL_3(K)$ mit $S^{-1}AS = B$ zu bestimmen, gehen wir wie im Beweis von 5.58 vor:

sei $g := F_{A-I}$, sei $U_1 = \ker(g)$, $U_2 = \ker(g^2)$. Man findet $U_1 = \{x \in K^3 : x_1 + x_2 = x_3\}$ und $U_2 = K^3$, also $\dim(U_1) = 2$, $\dim(U_2) = 3$. Man startet mit einem Vektor $v \in U_2$, $v \notin U_1$, etwa $v = e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, und bildet $g(v) = -e_1 - e_3 = \begin{pmatrix} -1 \\ 0 \\ -1 \end{pmatrix} \in U_1$. Ergänze $g(v)$ zu einer Basis von U_1, etwa durch $w := e_2 + e_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$. Dann ist $(g(v), v, w)$ eine Basis von K^3, bezüglich der F_A die Matrix B hat. Es ist also $B = S^{-1}AS$ mit $S = M(g(v), v, w) = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 1 \end{pmatrix}$.

Wir können damit sofort beliebige Potenzen von A ausrechnen: es ist

$$A^n = (SBS^{-1})^n = S \cdot B^n S^{-1} = S \cdot \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot S^{-1} = \begin{pmatrix} 1-n & -n & n \\ 0 & 1 & 0 \\ -n & -n & 1+n \end{pmatrix}$$

Korollar 5.63.

Zwei Matrizen $A, B \in M_n(K)$ mit zerfallenden charakteristischen Polynomen sind genau dann ähnlich, wenn sie bis auf Permutation der Kästchen dieselbse Jordan-Normalform haben.

Beweis:

$A \approx B \Leftrightarrow A, B$ beschreiben denselben Endomorphismus bezüglich geeigneter Basen.

Die Behauptung folgt also aus 5.59.

□

Bemerkung 5.64.

1. Sei $n \in \mathbb{N}$. Zu jeder endlichen Folge $(m_1, \lambda_1), \dots, (m_r, \lambda_r)$ von Paaren mit $r \in \mathbb{N}$, $m_1, \dots, m_r \in \mathbb{N}$ mit $n = m_1 + \dots m_r$ und $\lambda_1, \dots, \lambda_r \in \mathbb{C}$ gehört eine Ähnlichkeitsklasse von $M_n(\mathbb{C})$. Zwei solche Folgen bestimmen genau dann dieselbe Ähnlichkeitsklasse, wenn sie bis auf Vertauschen gleich sind.

2. Die Ähnlichkeitsklassen von nilpotenten $n \times n$-Matrizen sind also eine Bijektion zur Menge aller Tupel $(m_1, \dots, m_r)$ mit $r \geqq 1$ und $m_1 \geqq \dots \geqq m_r$ und $\sum_{i=1}^{r} m_i = n$. Ein solches Tupel heißt eine **Partition** von n:
   man schreibt $p(n)$ für die Anzahl der Partitionen von n:

n	$p(n)$	Partitionen
1	1	(1)
2	2	$(2), (1,1)$
3	3	$(3), (2,1), (1,1,1)$
4	5	$(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$
5	7	
6	11	
7	15	

Bemerkungen 5.65.
Weitere Anwendungen:

1. Berechnung der Potenzen A^n von A in geschlossener Form. Das ist leicht, wenn A ein Jordan-Kästchen ist. Der allgemeine Fall wird durch Transformation in Jordan-Normalform erledigt, siehe Beispiel 5.62.

2. An der Jordan-Normalform liest man das Minimalpolynom von A ab und sieht genau, wo der Unterschied zum charakteristischen Polynom liegt: es zerfalle $P_A(t)$ in Linearfaktoren, sei $\lambda \in K$ ein fester Eigenwert von A. Es seien $J_{m_1}(\lambda), \dots, J_{m_r}(\lambda)$ die Jordan-Kästchen zum Eigenwert λ, mit $m_1 \geqq \dots \geqq m_r$. Dann gilt:

   - $P_A(t)$ enthält den Faktor $t - \lambda$ mit der genauen Vielfachheit $\mu_a(A; \lambda) = m_1 + \dots + m_r$.

- $Q_A(t)$ (= Minimalpolynom von A) enthät den Faktor $t - \lambda$ mit der genauen Vielfachheit m_1 (Grund: das Minimalpolynom von $J_m(\lambda)$ ist $(t-\lambda)^m$)
- $r = \mu_g(A; \lambda)$.

Also gilt: genau dann ist $P_A(t) = Q_A(t)$, wenn es zu jedem Eigenwert λ von A nur ein Jordan-Kästchen gibt, oder (äquivalent) genau dann, wenn alle Eigenräume von A (höchstens) eindimensional sind.

Bemerkung 5.66.
Sei $K = \mathbb{R}$ oder $K = \mathbb{C}$. Für jede Matrix $A = (a_{ij}) \in M_n(K)$ schreiben wir $||A|| : \max\limits_{i,j=1,\dots,n} |a_{ij}|$.
Die ist eine Vektorraum-Norm auf $M_n(K)$, d.h. es gelten
$||A|| \geqq 0$, und $||A|| > 0$ für $A \neq 0$;
$||\lambda A|| = |\lambda| ||A||$, für $\lambda \in K$;
$||A + B|| \leqq ||A|| + ||B||$.

Für $A, B \in M_n(K)$ ist $||A \cdot B|| \leqq n \cdot ||A|| \cdot ||B||$.

Definition 5.67.
Die Exponentialfunktion für Matrizen ist definiert durch
$\exp(A) := \sum\limits_{k=0}^{\infty} \frac{1}{k!} A^k$, für $A \in M_n(\mathbb{C})$.

Satz 5.68.
Seien $A, B \in M_n(K)$.

(a) Die Reihe $\exp(A) = \sum\limits_{k=0}^{\infty} \frac{1}{k!} A^k$ *konvergiert koeffizientenweise absolut, und es gilt* $||exp(A) - I|| \leqq \frac{1}{n}(e^{n||A||} - 1)$.

(b) $\exp(A)$ *ist invertierbar, und* $\exp(A)^{-1} = \exp(-A)$.

(c) $\det(\exp(A)) = e^{tr(A)}$.

(d) Für $S \in GL_n(K)$ ist $\exp(SAS^{-1}) = S \cdot \exp(A) \cdot S^{-1}$.

(e) *Ist* $AB = BA$, *so ist* $\exp(A + B) = \exp(A) \cdot \exp(B)$.

Beweis:
Es ist $\|A^k\| \leqq n^{k-1}\|A\|^k$, für alle $k \geqq 1$.

(a) Also ist $\|\exp(A) - I\| \leqq \sum\limits_{k=1} \infty \frac{1}{k!}\|A^k\| \leqq \frac{1}{n} \sum\limits_{k=1} \infty \frac{1}{k!}(n\|A\|)^k = \frac{1}{n}(e^{n\|A\|} - 1) < \infty$.

(b)

(c) Es genügt, Dreiecksmatrizen zu betrachten (siehe (d)).
Dann klar: Sind $\lambda_1, \dots, \lambda_n$ die Diagonalelemente von A, so sin $e^{\lambda_1}, \dots, e^{\lambda_n}$ die Diagonalelemente von $\exp(A) \Rightarrow \det(\exp(A)) = \prod e^{la_i} = e^{tr(A)}$.

(d) klar. Insbesondere folgt: $A \approx B \Rightarrow \exp(A) \approx \exp(B)$. Deshalb genügt es zu (c), Dreiecksmatrizen zu betrachten.

Sei $AB = BA$. Man zeige zunächst $(A + B)^n = \sum\limits_{k=0}^{n} \binom{n}{k} A^k B^{n-k}$.
Daraus folgt (e) wie für komplexe Zahlen.

□

Bemerkung 5.69.

1. Ist $AB \neq BA$, so ist im Allgemeinen $\exp(A + B) \neq \exp(A) \cdot \exp(B)$.
Beispiel:
$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, es ist $\exp(A) = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}$, $\exp(B) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, also $\exp(A) \cdot \exp(B) = \begin{pmatrix} e & e \\ 0 & 1 \end{pmatrix}$, aber $\exp(A + B) \neq \exp(A) \cdot \exp(B)$.

2. Berechnung von $\exp(A)$: mit Hilfe der Jordan-Chevalley Zerlegung $A = D + N$ von A:
Für Diagonalmatrizen D (und damit auich für diagonalisierbare Matrizen) ist $\exp(D)$ leicht zu berechnen: $\exp(diag(\lambda_1, \dots, \lambda_n))) = diag(e^{\lambda_1}, \dots, e^{\lambda_n})$.
Für nilpotentes N ist die Reihe $\exp(N) = \sum\limits_{k=0}^{n} \frac{1}{k!} N^k$ eine endliche Reihe, also ebenfalls berechenbar. Wegen $DN = ND$ ist also $\exp(A) = \exp(D) \cdot \exp(N)$.

Beispiel 5.70.
Sei A wie in 5.62. Berechne $\exp(zA)$ für jedes $z \in \mathbb{C}$. Mit S wie dort ist $zA = S \cdot z(I+N) \cdot S^{-1}$ mit $N = E_{12}$ (also $N^2 = 0$). Also ist $\exp(zA) = S \cdot (\exp(zI) \cdot \exp(zN)) \cdot S^{-1} = S \cdot e^z \begin{pmatrix} 1 & z & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot S^{-1} = e^z \cdot \begin{pmatrix} 1-z & -z & z \\ 0 & 1 & 0 \\ -z & -z & 1+z \end{pmatrix}$