Dies ist nur ein studentischer Mitschrieb und erhebt keinen Anspruch auf Korrektheit oder Gleichheit zur Vorlesung!

Lineare Algebra I - gehalten von Gebhard Böckle

Mitschrieb von Anita Ullrich

14. September 2017

Inhaltsverzeichnis

0 Aussagenlogik

Auch in der Mathematik ist die Sprache die Grundlage von allem. Die Sprache der Mathematik besteht aus **Aussagen**. Aussagen sind Sätze, denen man das Prädikat **wahr(w)** oder **falsch(f)** zuordnen kann. Das nennt man den **Wahrheitsgehalt** der Aussage.

Beachte: Sätze oder Alltagssprache sind oft keine Aussagen ("Wie ist das Wetter heute?")

Oft wird von **Axiomen** (Grundaussagen) ausgegangen. Aus diesen kann man nach bestimmten Regeln neue Aussagen bilden. Um diese Regeln einzuführen, verwenden wir **Definitionen** (Vereinbarungen).

Definition 0.1. Seien A und B Aussagen. Dann sind folgende Sätze Aussagen:

a) $\neg A$ "nicht A" (die Negation von A)
b) $A \wedge B$ "A und B"
c) $A \vee B$ "A oder B" (einschließendes oder)

Der Wahrheitsgehalt dieser Aussagen ist durch Wahrheitstabellen beschrieben.

A	$\neg A$
w	f
f	w

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

Beispiel.

3 ist eine Primzahl (w)

3 ist keine Primzahl (f)

Vorsicht: B: alle Primzahlen sind ungerade (f)
$\neg B$: nicht alle Primzahlen sind ungerade (w) oder: wenigstens eine Primzahl ist gerade (w)
falsch ist: $\neg B$: keine Primzahl ist ungerade (f)

Definition 0.2. Sind A und B Aussagen, so auch folgende Sätze:

d) $A \Rightarrow B$: "A impliziert B" oder "aus A folge B" oder "wenn A gilt, dann auch B"
e) $A \Leftrightarrow B$: "A ist äquivalent zu B" oder "A gilt genau dann, wenn B gilt"

Die zugehörige Wertetabellen:

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

Merke:

- Aus einer falschen Aussage folgt alles.
- "Man kann Implikationen und Äquivalenzen mit Wahrheitstafeln nachprüfen" (, im Sinn der folgenden Proposition..)

Proposition 0.3. Für Aussagen A, B, C gelten:

i) $(A \wedge B) \Leftrightarrow (B \wedge A)$; $(A \vee B) \Leftrightarrow (B \vee A)$, d.h. "und" und "oder" sind **kommutativ**.

ii) $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$; $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$, d.h. “und“ und “oder“ sind **assoziativ**.

iii) $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$; $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ (**Distributivität**

iv) $\neg(\neg \mathrm{A}) \Leftrightarrow A$

v) $\neg(A \vee B) \Leftrightarrow (\neg A) \wedge (\neg B)$; $\neg(A \wedge B) \Leftrightarrow (\neg A) \vee (\neg B)$ (**deMorgansche Regel**)

Beweis (zum Teil)**. i)** 1. Teil

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

v) 1. Teil

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$
w	W	W	f	f	f	f
w	f	w	f	f	w	f
f	w	w	f	w	f	f
f	f	f	w	w	w	w

Alles Übrige mit Wahrheitstafeln. □

Proposition 0.4. Für Aussagen A und B gelten:

i) $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$

ii) $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ (**Kontraposition**)

iii) $\neg(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$ (**Widerspruchsbeweis**)

Interpretation.

ii) Um zu zeigen, dass B aus A folgt, kann man alternativ zeigen, dass aus $\neg B$ die Aussage $\neg A$ folgt.

iii) Um $A \Rightarrow B$ zu zeigen, kann man wie folgt vorgehen: A gelte und man nimmt an, dass B falsch ist und dann folgt $\neg(A \Rightarrow B)$ ist falsch, dann folgt $A \Rightarrow B)$ gilt. (Widerspruchsbeweis)

Proposition 0.5. Für Aussagen A, B und C gelten:

i) $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$

ii) $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$

Beweis. Wahrheitstafeln,

Interpretation. ii) sagt: gehe in 2 Schritten vor, um $\Leftrightarrow$ nachzuweisen!

Beweis (von 0.4ii))**.** $(A \Rightarrow B) \Leftrightarrow \neg A \vee B \Leftrightarrow B \vee \neg A \Leftrightarrow \neg(\neg B) \vee (\neg A) \Leftrightarrow (\neg B \Rightarrow \neg A)$ □

1 Mengen, Abbildungen, vollständige Induktion

Wir werden in dieser Vorlesung mit einem "naiven" Mengenbegriff arbeiten.

Definition (Georg Cantor (Ende 19.Jhd.))**.** Eine **Menge** ist eine Zusammenfassung von Objekten unseres Denkens. Diese Objekte heißen **Elemente** von M.
$x \in M$ bedeutet "x ist Element von M".

Bemerkung.

- endliche Mengen werden oft durch eine Aufzählung ihrer Elemente angegeben.
- viele Mengen sind durch ein Bildungsgesetz definiert.

Beispiel.

$$
\begin{aligned}
\mathbb{N} &= \{1, 2, 3, ...\} && \text{(Natürliche Zahlen)}\\
\mathbb{N}_0 &= \{0, 1, 2, 3, ...\} && \text{(natürliche Zahlen und die Null)}\\
\mathbb{Z} &= \{0, \pm 1, \pm 2, ...\} && \text{(ganze Zahlen)}\\
\mathbb{Q} &= \{\tfrac{a}{b} | a, b \in \mathbb{Z},\ b \neq 0\} && \text{(Menge der rationalen Zahlen)}\\
\mathbb{R} & && \text{(reelle Zahlen, siehe Analysis)}\\
\emptyset &= \{\} && \text{(leere Menge)}\\
\mathbb{P} &= \{x \in \mathbb{N} | x\, ist\, Primzahl\} = \{2, 3, 5, 7, ...\}
\end{aligned}
$$

Seien heute im Weiteren M, N Mengen.

Definition 1.1.

a) $x \notin M :\Leftrightarrow x$ liegt nicht in M $(\Leftrightarrow \neg(x \in M))$.
b) $N \subseteq M :\Leftrightarrow$ Jedes Element $x \in N$ liegt auch in M. Man sagt: "N ist Teilmenge von M "oder" M ist Obermenge von N".
c) $N \subset M :\Leftrightarrow N \subseteq M$ und $N \neq M$

Übung. $M = N \Leftrightarrow (M \subseteq N \wedge N \subseteq M)$

Beispiel. $\mathbb{P} \subset \mathbb{N}$

Definition 1.2.

a) $M \cap N := \{x | x \in M \wedge x \in N\}$ $M \cap N$ heißt **Durchschnitt** von M und N.
b) $M \cup N := \{x | x \in M \vee x \in N\}$ "**Vereinigung** von M und N".
c) $M \setminus N := \{x | x \in M \wedge x \notin N\}$ "**Differenz** von M und N" (M ohne N)
d) M und N heißen **disjunkt**$\Leftrightarrow M \cap N = \emptyset$
e) Sind M und N disjunkt, so schreibt man auch $M \,\dot{\cup}\, N$ für $M \cup N$ ("disjunkte Vereinigung")

Beispiel.

$$
\begin{aligned}
&\mathbb{P} \cap \{1, ..., 10\} = \{2, 3, 5, 7\}\\
&\{1, ..., 10\} \setminus \mathbb{P} = \{1, 4, 6, 8, 9, 10\}
\end{aligned}
$$

Beachte:

i) $\Rightarrow, \Leftrightarrow, \Leftarrow, :\Leftrightarrow$ stehen zwischen Aussagen.
ii) $=, :=$ stehen zwischen Mengen oder zwischen Elementen.

Definition 1.3.

a) Für $m \in M$ und $n \in N$ bezeichnet der Ausdruck (m, n) das **geordnete Paar** mit 1. Eintrag m, 2. Eintrag n.
b) Das **Mengenprodukt** von M und N ist $M \times N = \{(m, n)|m \in M, n \in N\}$

Beispiel.

$$\mathbb{R} \times \mathbb{R} = \{(a, b)|a, b \in \mathbb{R}\}\text{“= Punkt der Ebene“}$$
$$\mathbb{R} \times \mathbb{R} \supseteq [0, 1] \times [0, 2]$$
$$[a, b] = \{x \in \mathbb{R}|a \leq x \leq b\}$$

Definition 1.4. Sei $k \in \mathbb{N}$:

a) Ein k**-Tupel** ist eine geordnete Aufzählung $(m_1, ..., m_k)$ von Objekten $m_1, ..., m_k$
b) Sind $M_1, ..., M_k$ Mengen, so ist ihr Mengenprodukt $M_1 \times ... \times M_k = \{(m_1, ..., m_k)|m_1 \in M_1, ..., m_k \in M_k\}$
c) Man schreibt M^k für $M \times ... \times M$ (k Faktoren)

Beispiel. $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ (“Punkte im Raum“)

Definition 1.5.
i) Eine **Abbildung** ist ein Tripel (M, N, f) bestehend aus Mengen M, dem **Definitionsbereich**, und N, dem **Wertebereich**, und einer **Abbildungsvorschrift** f, die jedem $m \in M$ ein Element $f(m) \in N$) zuordnet.
Andere Notation: $f : M \to N$ $\quad M \xrightarrow{f} N \quad$ f
ii) Der **Graph** einer Abbildung $f : M \to N$ ist $Graph(f) := \{(m, f(m))|m \in M\} \subseteq M \times N$

Beispiel. Ist die Menge eine beliebige Menge, so ist $id_M : M \to M, m \mapsto m$ die identische Abbildung.

Sei im Weiteren $f : M \to N$ eine Abbildung.

Definition 1.6.
i) Für $U \subseteq M$ sei $f(U) := \{f(m)|m \in U\}$ das **Bild** von U unter f.
ii) Für $V \subseteq N$ sei $f^{-1}(V) := \{m \in M|f(m) \in V\}$ das **Urbild** von V unter f.

Definition 1.7.
i) f heißt **injektiv** $:\Leftrightarrow$ für jedes $n \in N$ enthält $f^{-1}(\{n\})$ höchstens ein Element.
ii) f heißt **surjektiv** $:\Leftrightarrow$ für jedes $n \in N$ enthält $f^{-1}(\{n\})$ mindestens ein Element.
iii) f heißt **bijektiv** $:\Leftrightarrow$ für jedes $n \in N$ enthält $f^{-1}(\{n\})$ genau ein Element.

Lemma 1.8.
a) f ist injektiv$:\Leftrightarrow$ (für alle $m, m' \in M$ gilt: $f(m) = f(m') \Rightarrow m = m'$)
b) f ist surjektiv$\Leftrightarrow f(M) = N$
c) f ist bijektiv$\Leftrightarrow f$ ist injektiv und surjektiv

Notation.
- $\forall n \in N :$ bedeutet “für alle $n \in N$ gilt“ oder “für jedes $n \in N$ gilt“
- $\exists n \in N :$ bedeutet “es existiert ein $n \in N$, so dass“
- $\exists! n \in N :$ bedeutet “es gibt genau ein $n \in N$, so dass“

Beweis. c) Eine Menge enthält genau ein Element, genau dann, wenn sie mindestens ein Element enthält und höchstens ein Element enthält.
f injektiv und surjektiv $:\Leftrightarrow \forall n \in N : f^{-1}(\{n\})$ enthält mindestens und höchstens ein Element
$\Leftrightarrow \forall n \in N : f^{-1}(\{n\})$ enthält genau ein Element $\Leftrightarrow f$ ist bijektiv

a) "$\Rightarrow$" Sei f injektiv. Seien $m, m' \in M$ und gelte $f(m) = f(m')$.
Setze $n := f(m) \Rightarrow m, m' \in f^{-1}(\{n\}) \overset{f \text{ inj.}}{\Rightarrow} m = m'$, da $f^{-1}(\{n\})$ höchstens einelementig ist.
"$\Leftarrow$" ("Widerspruchsbeweis"): Gelte die rechte Seite der Aussage a).
Annahme: f ist nicht injektiv, d.h. $\exists n \in N : f^{-1}(\{n\})$ enthält nicht kein oder ein Element, d.h.

$$\exists n \in N : \exists m, m' \in M : f^{-1}(\{n\}) \ni m, m' \text{ und } m \neq m'$$

Aber: wegen Aussage rechts: $f(m) = f(m') = n$ impliziert $m = m'$ ↯ Widerspruch zur Annahme!
D.h. die Annahme muss falsch sein. Folglich ist f injektiv.

b) $f(M) = N \Leftrightarrow f(M) \supseteq N$ (Bemerkung: $f(M) \subseteq N$ gilt immer)
$\Leftrightarrow \forall n \in N : n \in f(M) = \{f(m) | m \in M\} \Leftrightarrow \forall n \in N : \exists m \in M : n = f(m)$
$\Leftrightarrow \forall n \in N : \exists m \in M : m \in f^{-1}(\{n\}) \Leftrightarrow \forall n \in N : f^{-1}(\{n\}) \neq \emptyset \Leftrightarrow f$ surjektiv □

Seien weiterhin M, N Mengen und $f : M \to N$ eine Abbildung.

Bemerkung.

i) Für jedes N $\exists!$ Abbildung: $\emptyset \to N$
ii) Falls $M \neq \emptyset$, so existiert keine Abbildung: $M \to \emptyset$

1.1 Verkettung (/Komposition) von Abbildungen

Definition 1.9. Sei $g : L \to M$ eine weitere Abbildung. Die Verkettung "f nach g" ist die Abbildung $f \circ g : L \to N, x \mapsto (f \circ g)(x) := f(g(x))$

Lemma 1.10. Sei $h : K \to L$ eine weitere Abbildung. Dann gilt $(f \circ g) \circ h = f \circ (g \circ h)$ als Abbildung: $K \to N$

Beweis. Es ist nur zu zeigen, dass die Abbildungsvorschriften dieselben sind:
Sei $x \in K : ((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (f \circ h))(x)$ □

Übung. Für $V \subseteq N$ gilt: $(f \circ g)^{-1}(V) = g^{-1}(f^{-1}(V))$

Lemma 1.11.

a) f, g injektiv $\Rightarrow f \circ g$ injektiv
b) f, g surjektiv $\Rightarrow f \circ g$ surjektiv
c) $f \circ g$ surjektiv $\Rightarrow f$ surjektiv

Beweis. c) Seien $x_1, x_2 \in L$ und gelte $g(x_1) = g(x_2)$.
Z: $x_1 = x_2$
Dazu wende f an: $(f \circ g)(x_1) = f(g(x_1)) = f(g(x_2)) = (f \circ g)(x_2 \Rightarrow$ (da $f \circ g$ inj.) $x_1 = x_2$

d) Z: f surjektiv. Sei $n \in N$. Z: $\exists m \in M : f(m) = n$
Wissen: $f \circ g$ surjektiv $\Rightarrow$ $\exists l \in L$ mit $n = (f \circ g)(l) = (f(g(l))$.
Wähle $m := g(l) \Rightarrow n = f(m)$ □

Satz 1.12. Sei $f : M \to N$ eine bijektive Abbildung. Dann existiert genau eine Abbildung $\tilde{f} : N \to M$, mit $\tilde{f} \circ f \overset{\circledast}{=} id_M$ und $f \circ \tilde{f} = id_N$. Man schreib f^{-1} für $\tilde{f}$ und nennt f^{-1} die zu f **inverse Abbildung**.

Beweis. Konstruktion: Sei $n \in N \overset{f \text{ bij.}}{\Rightarrow} f^{-1}(\{n\})$ ist einelementig. Definiere $\tilde{f}(n)$ so, dass $\tilde{f}(\{n\}) = f^{-1}(\{n\}) \rightsquigarrow$ erhalten: $\tilde{f} : N \to M$

$\circledast$ **nachweisen:** Sei $m \in M$. $\tilde{f}(f(m)) = m$. Sei nun $n \in N : f(\tilde{f}(n)) = n$

Eindeutigkeit von $\tilde{f}$: Sei $g : N \to M$ eine Abbildung und $f \circ g = id_N \wedge g \circ f = id_M$. Dann: $\tilde{f} = \tilde{f} \circ id_N = \tilde{f} \circ (f \circ g) = (\tilde{f} \circ f) \circ g \overset{\circledast}{=} id_M \circ g = g$ □

Bemerkung. Gilt $\circledast$ für f und $\tilde{f}$, so sind beide bijektiv.

Induktion: Man kann die natürlichen Zahlen durch folgende Axiome (nach Peano) beschreiben:

P1) $\mathbb{N}_0$ hat ein ausgezeichnetes Element, die Null.
P2) Es gibt eine Abbildung $\nu : \mathbb{N}_0 \to \mathbb{N}_0, n \mapsto \nu(n)$ ($\nu(n)$ der Nachfolger von n)
P3) $0 \notin \nu(\mathbb{N}_0)$ ("0 hat keinen Vorgänger")
P4) ν ist injektiv
P5) Ist $N \subseteq \mathbb{N}_0$ mit $0 \in N$ und $\nu(N) \subseteq N$, so gilt $N = \mathbb{N}_0$
Man definiert: $1 := \nu(0), 2 := \nu(1) = \nu(\nu(0)), ...$

Satz 1.13 (Induktionsprinzip)**.** Sei $A(n)$ eine Aussage für jedes $n \in \mathbb{N}_0$, so dass gilt:

a) $A(n)$ ist wahr.
b) Ist $A(n)$ wahr, so ist $A(\nu(n))$ wahr.

Dann gilt $A(n)$ für alle $n \in \mathbb{N}_0$.

Beweis. Definiere $N := \{n \in \mathbb{N}_0 | A(n) \text{ ist wahr }\}$.
Z: $N = \mathbb{N}_0$
wegen a) und b) gelten: $0 \in N$ und $\nu(N) \subseteq N \Rightarrow N = \mathbb{N}_0$ □

Bemerkung. Man kann "rekursiv" für alle $m \in \mathbb{N}_0$ eine Abbildung $m + \_ : \mathbb{N}_0 \to \mathbb{N}_0, a \mapsto m \cdot a$ definieren. $(m \cdot 0 = 0, m \cdot \nu(n) = m + m \cdot n)$

Definition 1.14.

a) Eine **Relation** auf einer Menge M ist eine Teilmenge $R \subseteq M \times M$
b) An Stelle $(x, y) \in R$ schreibt man oft xRy
c) Eine Relation $R \subseteq M \times M$ heißt **Totalordnung**, schreibe "$\leq$"
   i) $\forall m \in M : m \leq m$
   ii) $\forall m, m' \in M : m \leq m'$ und $m' \leq m \Rightarrow m = m'$
   iii) $\forall m, m' \in M : m \leq m'$ oder $m' \leq m$
   iv) $\forall m, m', m'' : m \leq m'$ und $m' \leq m'' \Rightarrow m \leq m''$
d) Definiere Relation $\leq$ auf $\mathbb{N}_0$ durch: $m \leq m' \Leftrightarrow \exists m \in \mathbb{N}_0 : m' = n + m$

Proposition 1.15. $\leq$ aus d) ist eine Totalordnung auf $\mathbb{N}_0$

1.2 Mächtigkeit (Kardinalität) von Mengen

Für $n \in \mathbb{N}$ sei $\{1, ..., n\} = \{x \in \mathbb{N} | 1 \leq x \leq n\}$

Satz 1.16. Ist $f : \{1, ..., n\} \to \{1, ..., m\}$ eine Bijektion, so gilt $n = m$.

Beweis. Induktion über $n \in \mathbb{N}$
$\mathbf{n = 1}$ (Induktions-Anfang): $f(\{1, ..., n\}) = f(\{1\}) = \{f(1)\} \overset{f \text{ surj.}}{=} \{1, ..., m\} \Rightarrow m = 1$
$\mathbf{n \mapsto n + 1}$ (Induktions-Schritt): Gelte die Aussage für ein beliebiges, aber festes $n \in \mathbb{N}$. Zeige nun, sie gilt auch für $n + 1$:
Sei $f : \{1, ..., n + 1\} \to \{1, ..., m\}$ bij. Sei $m' = f(n + 1)$, definiere

$$g : \{1, ..., m\} \to \{1, ..., m\}, i \mapsto \begin{cases} i & \text{für } i \neq m, m' \\ m & \text{für } i = m' \\ m' & \text{für } i = m \end{cases}$$

Prüfe: g bijektiv, $g \circ f$ ist bijektiv, $g \circ f(n + 1) = m, m > 1 \Rightarrow h : \{1, ..., n\} \to \{1, ..., m - 1\}, i \mapsto g \circ f(i)$ ist bijektiv $\overset{\text{IV}}{\Rightarrow} m - 1 = n \Rightarrow m = n + 1$ □

Proposition 1.17 (Proposition-Definition)**.** Für eine Menge M gilt genau eine der folgenden 3 Aussagen:

a) $M = \emptyset$
b) $\exists n \in \mathbb{N} : \exists$bijektive Abbildung $f : \{1, ..., n\} \to M$
c) es gilt weder a) noch b)

Im Fall b) ist die Zahl $n \in \mathbb{N}$ eindeutig.
Die **Kardinalität** (oder Mächtigkeit) von M ist

$$|M| := \begin{cases} 0 & \text{falls } M = \emptyset \\ n & \text{falls b) gilt} \\ \infty & \text{falls c) gilt} \end{cases}$$

M heißt endlich, falls a) oder b) gilt.

Beweis. i) $\mathbb{Z}$: a) und b) schließen sich gegenseitig aus.
ii) $\mathbb{Z}$: n in b) ist eindeutig.
i) Falls $M = \emptyset$, so existiert keine Abbildung $N \to M = \emptyset$ für $N \neq \emptyset \Rightarrow$ b) gilt nicht.
ii) Seine $\{1, ..., n\} \overset{f}{\to} M$ und $\{1, ..., m\} \overset{g}{\to} M$ beide bijektiv. $\Rightarrow g^{-1} \circ f : \{1, ..., n\} \to \{1, ..., m\}$ ist bijektiv $\overset{1.15}{\Rightarrow} n = m$. □

Fakten:

a) Sei $f : M \to N$ bijektiv. Dann gilt $|M| = |N|$.
b) Sei $f : \{1, ..., m\} \to \{1, ..., n\}$ eine Abbildung:
   i) $n = m \Rightarrow f$ bijektiv
   ii) $n < m \Rightarrow f$ nicht injektiv
   iii) $n > m \Rightarrow f$ nicht surjektiv
c) Sind M und N disjunkt, so gilt $|M \dot{\cup} N| = |M| + |N|$ (unter der Vereinbarung $\infty + \_ = \infty$; $\_ + \infty = \infty$) (oder setze voraus: M, N sind beide endlich).
d) Ist M endlich und $N \subset M$, so ist N endlich und $|N| < |M|$.

e) $|\mathbb{N}_0| = \infty$

f) M, N endlich: $|M \cup N| = |M| + |N| - |N \cap M|$

Definition 1.18. Ist M eine Menge, so heißt $P(M) := \{N | N \subseteq M\}$ die **Potenzmenge** von M.

Beispiel. $P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{2, 1\}\}$

Satz 1.19. M endlich $\Rightarrow |P(M)| = 2^{|M|}$

2 Gruppen und Körper

Definition 2.1. Eine **Gruppe** ist ein Tripel $(G, e, \odot)$ bestehend aus eine Menge G, einem Element $e \in G$ und einer Abbildung $\odot : G \times G \to G$ (einer Verknüpfung), sodass gelten:

$G1)$	$\forall g \in G : g \odot e = g$	(Assoziativität)
$G2)$	$\forall g \in G : \exists h \in G : g \odot e = g$	(Rechtseins)
$G3)$	$\forall g \in G : \exists h \in G : g \odot h = e$	(Rechtsinverses)

Gilt zusätzlich

$G4)$	$\forall g, h \in G : g \odot h = h \odot g$	(Kommutativität)

so heißt G **abelsche Gruppe**.
Wir schreiben oft G für $(G, e, \odot)$. e heißt **neutrales Element** oder (kurz) Eins von G.

Beispiel. a) $(\mathbb{Z}, 0, +)$ ist eine abelsche Gruppe. Das bedeutet: $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b$
$\forall a, b, c \in \mathbb{Z}$:

$G1)$ $(a + b) + c = a + (b + c)$
$G2)$ $a + 0 = a$
$G3)$ $\forall a \in \mathbb{Z} : \exists a' \in \mathbb{Z} : a + a' = 0$ (schreibe $-a$ für a)
$G4)$ $a + b = b + a$

b) $(\mathbb{R}, 0, +)$ ist eine abelsche Gruppe.
c) $(\mathbb{R}^n, \underline{0}, +)$ ist eine abelsche Gruppe für $\underline{0} = (0, ..., 0)$ (n-Tupel): $(a_1, ..., a_n) + (b_1, ..., b_n) := (a_1 + b_1, ..., a_n + b_n)$
d) Sei $\mathbb{R}^x = \mathbb{R} \setminus \{0\}$, dann ist $(\mathbb{R}^x, 1, \cdot)$ eine abelsche Gruppe.
e) $(\{\pm 1\}, 1, \cdot)$ ist eine abelsche Gruppe.
Verknüpfungstafel:

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

Definition 2.2. Für eine Menge M definiere $Bij(M) := \{f : M \to M | f \; ist \; bijektiv\}$

Proposition 2.3. $(Bij(M), id_M, \circ)$ ist eine Gruppe. ($\circ$ ist Verkettung von Abbildungen)

Beweis. G1 gilt: $(f \circ g) \circ h = f \circ (g \circ h)$ gilt $\forall f, g, h \in Bij(M)$ nach Lemma 1.10.
G2: $f \circ id_M = f \quad \forall f \in Bij(M)$
G3: Satz 1.12 $\Rightarrow f \circ f^{-1} = id_M$ □

Definition 2.4. Für $n \in \mathbb{N}$ sei $S_n := Bij(\{1, ..., n\})$. S_n heißt auch **Gruppe der Permutationen** von $\{1, ..., n\}$.

Übung.
i) $|M| \geq 3 \Rightarrow$ Die Gruppe $Bij(M)$ ist nicht abelsch.
ii) M endlich, $|M| = n$. Dann: $|Bij(M)| = n! = 1 \cdot 2 \cdot ... \cdot n$

Proposition 2.5. Für eine Gruppe $(G, e, \odot)$ gelten:

a) $g \odot h = e \Rightarrow h \odot g = e$ für $g, h \in G$

b) $\forall g \in G : e \odot g = g$
c) $\forall g \in G : \exists! h \in G$ mit $g \odot h = e$ (Schreibe später g^{-1} anstelle von diesem eindeutigen h; g^{-1} heißt Inverses zu g)
d) e ist das einzige Element von G, sodass G2 und G3 gelten.
e) $\forall g, h \in G$ gilt: die Gleichung $g \odot x = h$ hat eine eindeutige Lösung, nämlich $x = g^{-1} \odot h$

Beweis. a) Gelte $g \odot h = e$. Sei $k \in G$ rechtsinvers zu h, d.h. $h \odot k = e$. Betrachte nun
$h \odot g \overset{G1+G2}{=} h \odot (g \odot (h \odot k)) \overset{G1}{=} h \odot ((g \odot h) \odot k) \overset{G3}{=} h \odot (e \odot k) \overset{G1}{=} (h \odot e) \odot k \overset{G2}{=} h \odot k \overset{G3}{=} e$

b) Sei h rechtsinvers zu g, d.h. $g \odot h = e$, dann gilt: $e \odot g = (g \odot h) \odot g \overset{G1}{=} g \odot (h \odot g) \overset{a)}{=} g \odot e \overset{G2}{=} g$

c) Seine h, h' rechtsinvers zu g.
Z: $h = h$'
Dazu: $g \overset{G2}{=} h \odot e \overset{G3}{=} h \odot (g \odot h') \overset{G1}{=} (h \odot g) \odot h') \overset{a)}{=} e \odot h' \overset{b)}{=} h'$

d) Seine $e, e' \in G$ Elemente für die G2 und G3 gilt: $e \overset{G2}{=} e \odot e' \overset{b)}{=} e'$

e) $\mathbf{g^{-1} \odot h}$ ist Lösung: $g \odot (g^{-1} \odot h) \overset{G1}{=} (g \odot g^{-1} \odot h \overset{G3}{=} e \odot h \overset{b)}{=} h$
$\exists!$ **Lösung:** Gelte $g \odot x = g \odot x' (= h)$. Verknüpfe von links mit g^{-1}. Nun folgt mit G1 und G2 und b), dass $x = x'$. □

Notation.
a) Wir schreiben meist
  i) G statt $(G, e, \odot)$
  ii) $\cdot$ statt $\odot$, z.B: $gh = g \cdot h = g \odot h$
  iii) Falls G abelsch ist: schreibe $+$ statt $\odot$, dann auch $-g$ statt g^{-1}
b) Sei $a \in G$ und $n \in \mathbb{Z}$, schreibe a^n für

$$\begin{cases} a \cdot ... \cdot a & \text{falls } n > 0 \\ a^{-1} \cdot ... \cdot a^{-1} & \text{falls } n < 0 \\ e & \text{falls } n = 0 \end{cases}$$

Falls $\odot = +$, so gilt $n \cdot a$ statt a^n

Übung. Für alle $m, n \in \mathbb{Z}$ gilt $a^m \cdot a^n = a^{m+n}$

Definition 2.6. Ein **Körper** ist ein Quintupel $(K, 0, 1, +, \cdot)$, oder einfach K, bestehend aus einer Menge K, Elementen $0, 1 \in K$ und Verknüpfungen $+, \cdot : K \times K \to K$, so dass gelten:

$K1)$	$(K, 0, +)$ ist eine abelsche Gruppe.	
$K2)$	$(K \setminus \{0\}, 1, \cdot)$ ist eine abelsche Gruppe.	
$K3)$	$\forall a, b, c \in K : (a + b) \cdot c = a \cdot c + b \cdot c$	(Distributivgesetz)

Beispiel.

$(\mathbb{R}, 0, 1, +, \cdot)$ ist ein Körper
$(\mathbb{Q}, 0, 1, +, \cdot)$ ist ein Körper
$(\mathbb{Z}, 0, 1, +, \cdot)$ ist kein Körper
$(\mathbb{F}_2, 0, 1, +, \cdot)$ ist ein Körper für $\mathbb{F}_2 = \{0, 1\}$

$+_{\mathbb{F}_2}$	0	1
0	0	1
1	1	0

Lemma 2.7. Für einen Körper K gelten:

a) $0 \neq 1$
b) $\forall x \in K : 0 \cdot x = x \cdot 0 = 0$
c) $\forall x \in K : 1 \cdot x = x \cdot 1 = x$
d) $\forall a, b \in K : a \cdot b = b \cdot a$

Beweis. a) $1 \in K \setminus \{0\} \Rightarrow 0 \neq 1$

b) $0 \cdot x \overset{K1}{=} (0+0) \cdot x \overset{K3}{=} 0 \cdot x + 0 \cdot x \overset{\text{addiere } -(0 \cdot x)}{\Rightarrow} 0 = 0 \cdot x$. $x \cdot 0 = 0$ ist analog.

c) alls $x \neq 0$: verwende $K2 \Rightarrow 1 \cdot x = x \cdot 1 = x$. Falls $x = 0$: wende b) an.

d) Falls $a \neq 0 \neq b$: wende $K2$ an. Falls $a = 0 \vee b = 0$, wende b) an. □

Notation. Manchmal schreiben wir $0_K, 1_K, +_K, \cdot_K$ an Stelle von $0, 1, +, \cdot$ (analog für Gruppen).

2.1 Primkörper

Ziel: zu jeder Primzahl p existiert ein Körper mit p Elementen. (später: Körper ist eindeutig)

Definition 2.8. Sei $n \in \mathbb{N}$. Eine **Restklasse** modulo n ist eine Teilmenge $m \subseteq \mathbb{Z}$, so dass gelten:

i) $\forall a, b \in M$: n teilt $b - a$
ii) $\forall a \in M : \forall b \in \mathbb{Z} : (n \text{ teilt } (b-a) \Rightarrow b \in M)$
iii) $M = \emptyset$

Die Elemente von M heißen **Vertreter** von M.

Notation.

- Schreibe $n|x$ für "n teilt x"
- Für Restklassen M, N modulo n seien $M \oplus N := \{a + b | a \in M, b \in N\}$ und $M \odot N := \{a \cdot b + k \cdot n | a \in M, b \in N \text{ und } k \in \mathbb{Z}\}$

Satz 2.9. Sei $n \in \mathbb{N}$. Schreibe "Restklasse" für "Restklasse modulo n".

a) Je 2 Restklassen M, N sind disjunkt oder identisch.
b) Jedes $x \in \mathbb{Z}$ liegt in der Restklasse $x + n \cdot \mathbb{Z} := \{x + n \cdot k | k \in \mathbb{Z}\}$.
c) Es gibt genau n Restklassen (modulo n).
d) Sind M, N Restklassen, so auch $M \oplus N$ und $M \odot N$.
e) Sei $\mathbb{Z}/n$ die Menge aller Restklassen. Dann ist $(\mathbb{Z}/n, 0 + n \cdot \mathbb{Z}, \oplus)$ eine abelsche Gruppe.
f) Ist n Primzahl, so ist $(\mathbb{Z}/n, 0 + n \cdot \mathbb{Z}, 1 + n \cdot \mathbb{Z}, \oplus, \odot)$ ein Körper.

Korollar 2.10. Zu jeder Primzahl p gibt es einen Körper mit p Elementen.

Beispiel. Restklassen modulo 3 ($n = 3$):

$$\overline{0} = 0 + 3 \cdot \mathbb{Z} = \{..., -6, -3, 0, 3, 6, ...\}$$
$$\overline{1} = 1 + 3 \cdot \mathbb{Z} = \{..., -5, -2, 1, 4, 7, ...\}$$
$$\overline{2} = 2 + 3 \cdot \mathbb{Z} = \{..., -4, -1, 2, 5, 8, ...\}$$

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

Beweis. a) Zz: $M \cap N \neq \emptyset \Rightarrow M = N$.
Sei $x \in M \cap N$.
$\mathbf{N} \subseteq \mathbf{M}$: Sei $y \in N \overset{\text{i) für } N}{\Rightarrow} n|y - x \overset{\text{ii) für } M}{\Rightarrow} y \in M$
$\mathbf{M} \subseteq \mathbf{N}$: analog.

b) Zz: $M := x + n \cdot \mathbb{Z}$ ist Restklasse.
iii): $x \in M \Rightarrow M \neq \emptyset$
i): Seien $a = x + k \cdot n, b = x + l \cdot n \in M$ $(k, l \in \mathbb{Z})$ $\Rightarrow b - a = (l - k) \cdot n$. Wird von n geteilt.
ii): Seien $a = x + k. \cdot n \in M$ und $b \in \mathbb{Z}$, so dass $n|b - a \Rightarrow b - a = l \cdot n$ für $l \in \mathbb{Z} \Rightarrow b = a + l \cdot n = x + (k + l) \cdot n \in M$

c) Behauptung: Jede Restklasse M enthält ein eindeutiges Element aus $\{0, ..., n-1\} \ni x$
Existenz von x: Sei $y \in M \Rightarrow y + n \cdot |y| \in M \cap \mathbb{N}_0$, denn $y + n \cdot |y| \geq y + |y| \geq 0$. Sei nun $y \in M \cap \mathbb{N}_0$ ein kleinstes Element. (ÜB 2)
Behauptung: $0 \leq y \leq n - 1$, sonst bilde $y - n$. Dies Führt zu Widerspruch.
Eindeutigkeit: Seien $x, x' \in M$ mit $0 \leq x \leq x' \leq n - 1$
Zz: $x' = x$
Wissen: $0 \leq x' - x = k \cdot n \leq n - 1$ für ein $k \in \mathbb{Z} \Rightarrow 0 \leq k < 1 \Rightarrow k = 0 \Rightarrow x' = x$
Behauptung: 1b)$\Rightarrow$ Die Abbildung, die einer Restklasse M (modulo n) das eindeutige element in $M \cap \{0, ..., n-1\}$ zuordnet, ist eine Bijektion: $\{Restklassen\} \to \{0, ..., n-1\}$, d.h. c) gilt.

d) Wissen; nach c) und b), dass alle Restklassen die Form $x + n \cdot \mathbb{Z}$ haben (für ein $x \in \{0, ..., n-1\}$)
Übung:

- $(a + n \cdot \mathbb{Z}) \oplus (b + n \cdot \mathbb{Z} = (a + b) + n \cdot \mathbb{Z}$ ⊛
- $(a + n \cdot \mathbb{Z} \odot (b + n \cdot \mathbb{Z}) = a \cdot b + n \cdot \mathbb{Z}$ ⊛⊛

e) z.B. $0 + n \cdot \mathbb{Z}$ ist die Eins.
$(a + n \cdot \mathbb{Z}) \oplus (0 + n \cdot \mathbb{Z}) \overset{\circledast}{=} (a + (-a)) + n \cdot \mathbb{Z} = 0 + n \cdot \mathbb{Z}$

f) Assoziativität, Kommutativität von 0 mit (⊛⊛), Distributivgesetz mit (⊛) und (⊛⊛) (und verwende Gesetze für $\mathbb{Z}$).
Bleibt Zz: für $a \in \{1, ..., n-1\}$ $\exists b \in \{0, ..., n-1\}$ mit $a + n \cdot \mathbb{Z} \odot b + n \cdot \mathbb{Z} = 1 + n \cdot \mathbb{Z}$.
Dazu zeigen wir: $f_a : \mathbb{Z}/n \to \mathbb{Z}/n, M \mapsto M \odot (a + n \cdot \mathbb{Z})$ ist surjektiv.
Aus den Übungen wissen wir: Sei X eine endliche Menge, $f : X \to X$ injektiv $\Rightarrow f$ ist surjektiv.
Zz: f_a ist injektiv!
Seien $x + n \cdot \mathbb{Z}, x' + n \cdot \mathbb{Z}$ Restklassen mit $(x + n \cdot \mathbb{Z}) \odot (a + n \cdot \mathbb{Z}) = (x' + n \cdot \mathbb{Z}) \odot (a + n \cdot \mathbb{Z}) = a \cdot x' + n \cdot \mathbb{Z}$
$\Rightarrow a \cdot x, a \cdot x'$ sind in derselben Restklasse $\Rightarrow n|(a \cdot x' - a \cdot x) = a \cdot (x' - x)$ und da n eine Primzahl ist
$\Rightarrow n|a$ oder $n|x' - x \overset{0<a<n}{\Rightarrow} n|x' - x \Rightarrow x', x$ in derselben Restklasse. □

Definition 2.11. $p \in \mathbb{N}$ heißt **Primzahl** $\Leftrightarrow p > 1$ und die einzigen Teiler aus $\mathbb{N}$ von p sind 1 und p.

Satz 2.12. p Primzahl $\Rightarrow (\forall a, b \in \mathbb{Z} : p|a \cdot b \Rightarrow p|a \vee p|b)$

Lemma 2.13 (Übung)**.** Sei $\{0\} \subset M \subseteq \mathbb{Z}$, sodass gilt: $\forall a, a' \in M$ gilt $a \pm a' \in M$. Dann folgt:

a) Es gilt $M = m \cdot \mathbb{Z} (= \{m \cdot x | x \in \mathbb{Z}\})$, wobei m das kleinste Element in $M \cap \mathbb{N}$ ist (und $\neq \emptyset$)
b) Falls $M \supseteq p \cdot \mathbb{Z}$ für p eine Primzahl $\Rightarrow M = \mathbb{Z} \vee M = p \cdot \mathbb{Z}$

Beweis (des Satzes mit Lemma)**.** Seien $a, b \in \mathbb{Z}$ mit $p|a \cdot b$. Gelte nun $p \times b$. Betrachte $M := \{x \in \mathbb{Z} | p teilt x \cdot b\}$.
Prüfe $\forall x, x' \in M : x \pm x' \in M$ und $p \cdot \mathbb{Z} \subseteq M$.
Aus dem Lemma folgt nun: $M = \mathbb{Z}$ oder $M = p \cdot \mathbb{Z}$.
Falls $M = p \cdot \mathbb{Z} :\overset{a \in M}{\Rightarrow} \exists k \in \mathbb{Z} : a = p \cdot k$, d.h. $p|a$.
Falls $M = \mathbb{Z} :\overset{1 \in M}{\Rightarrow} p$ teilt $1 \cdot b = b$ ↯ □

Definition 2.14.

a) Eine Relation $R \subseteq M \times M$ (auf M) heißt **Äquivalenzrelation** $\Leftrightarrow$

i)	$\forall x \in M : xRx$	(reflexiv)
ii)	$\forall x, y \in M : xRy \Leftrightarrow yRx$	(symmetrisch)
iii)	$\forall x, y, z \in M : xRy$ und $yRz \Rightarrow xRz$	(transitiv)

b) Schreibe $x / \sim y$ für xRy, falls R Äquivalenzrelation.
c) Die Äquivalenzklasse $x \in M$ ist $[x] := \{y \in M | x\tilde{y}\}$.
d) $M/R := M/\sim := \{[x] | x \in M\}$ heißt Menge der Äquivalenzklassen.

Beispiel. Sei $M = \mathbb{Z}$. Dann ist $R_n = \{(x, y) \in \mathbb{Z}^2 | n$ teilt $x - y\}$ $(n \in \mathbb{N})$ ist eine Äquivalenzrelation auf $\mathbb{Z}$. Äquivalenzklassen zu R_n sind die Restklassen modulo n.

Definition 2.15. $\mathbb{C} := \mathbb{R}^2 = \{(a, b) | a, b \in \mathbb{R}\}$, $0_\mathbb{C} := (0_\mathbb{R}, 0_\mathbb{R})$, $1_\mathbb{C} = (1_\mathbb{R}, 0_\mathbb{R})$.
$+_\mathbb{C} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, ((a, b), (c, d)) \mapsto (a, b) +_\mathbb{C} (c, d) := (a +_\mathbb{R} c, b +_\mathbb{R} d$
$\cdot_\mathbb{C} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}, ((a, b), (c, d)) \mapsto (a, b) \cdot_\mathbb{C} (c, d) := (a \cdot_\mathbb{R} c -_\mathbb{R} b \cdot_\mathbb{R} d, a \cdot_\mathbb{R} d +_\mathbb{R} b \cdot_\mathbb{R} c)$

Satz 2.16. $(\mathbb{C}, 0_\mathbb{C}, 1_\mathbb{C}, +_\mathbb{C}, \cdot_\mathbb{C})$ ist ein Körper, der **Körper der komplexen Zahlen**.
Hinweis: $(a, b) \cdot_\mathbb{C} (a - b) = (a^2 + b^2, 0)$ und $(r, 0) \cdot_\mathbb{C} (c, d) = (r \cdot c, r \cdot d)$

Notation.

- Oft schreibt man i für $(0, 1)$ und $a + b \cdot i$ für (a, b)
- Man identifiziert (oft) $a \in \mathbb{R}$ mit $a + 0 \cdot i = (a, 0) \in \mathbb{C} \Rightarrow \mathbb{R} \subseteq \mathbb{C}$
- $\exists x \in \mathbb{C}$ mit $x^2 = -1_\mathbb{C}$: denn $i^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -(1, 0) = -1_\mathbb{C}$

3 Vektorräume und Unterobjekte

Definition 3.1. Sei $(K, 0_K, 1_K, +_K, \cdot_K)$ ein Körper. Ein **Vektorraum** (VR) über K, oder ein K-VR, ist ein Quadrupel $(V, 0_V, +V, \cdot_V)$ bestehend aus einer Menge V (Menge der Vektoren), einem Element $0_V \in V$ (Nullvektor) und Verknüpfungen

$$+_V : V \times V \to V, (v, w) \mapsto v + w \qquad \cdot_V : K \times V \to V, (\lambda, v) \mapsto \lambda \cdot_V v,$$

sodass gelten:

V1) $(V, 0_V, +_V)$ ist eine abelsche Gruppe.

V2) $\forall \lambda, \mu \in K : \forall v \in V : (\lambda \cdot_K \mu) \cdot_V v = \lambda \cdot_V (\mu \cdot_V v)$ (Assoziativität von $\cdot_V$)

V3) Distributivgesetze:

- $\forall \lambda, \mu \in K : \forall v \in V : (\lambda +_V \mu) \cdot_V v = \lambda \cdot_V v +_V \mu \cdot_V v$
- $\forall \lambda \in K : \forall v, w \in V : \lambda \cdot v(v +_V w) = \lambda \cdot_V v +_V \lambda \cdot_V w$

V4) $\forall v \in V : 1_K \cdot_V v = v$

Notation. Ab nun meist $+, \cdot$ statt $+_K, \cdot_K$ oder $+_V, \cdot_V$ und λv statt $\lambda \cdot v$. Multiplikation bindet enger als Addition ("Punkt vor Strich").

Lemma 3.2. Sei K ein Körper und V ein $K - VR$. Dann gelten $\forall v \in V, \forall \lambda \in K$:

a) $0_K \cdot_V v = 0_V$

b) $\lambda \cdot_V 0_V = 0_V$

c) $\lambda \cdot_V v = 0 \Rightarrow \lambda = 0_K \cdot_V v = 0_V$

d) $(-1) \cdot_V v = -v$

Beweis.

a) $0_K \cdot_V v = (0_K + 0_K) \cdot_V v \overset{V3}{=} 0_K \cdot_V v +_V 0_K \cdot_V v$.
Addiere $-(0_K \cdot_V v)$ und erhalte: $0_V = ... = 0_K \cdot_V v$

b) wie a).

c) Gelte $\lambda \cdot_V v = 0_V$ und $\lambda \neq 0_K$. Multipliziere mit λ^{-1}:

$$0_V \overset{b)}{=} \lambda^{-1} \cdot_V 0_V = \lambda^{-1} \cdot_V (\lambda \cdot_V v) \overset{V2}{=} (\lambda^{-1} \cdot_K \lambda) \cdot_V v = 1_K \cdot v \overset{V4}{=} v$$

d) Übung. □

Beispiel. Sei K ein Körper.

0) $V = \{0_V\}, +_V$ und $\cdot_V$ die einzig möglichen Verknüpfungen → **Null-VR**.

1) $(K^n, \underline{0}, +, \cdot)$ $(n \in \mathbb{N})$ ist ein K-VR für:

$$\begin{aligned} \underline{0} &= (0_K, ..., 0_K) \text{ (n-Tupel)} \\ (\lambda_1, ..., \lambda_n) + (\mu_1, ..., \mu_n) &:= (\lambda_1 + \mu_1, ..., \lambda_n + \mu_n) \\ \lambda \cdot (\mu_1, ..., \mu_n) &= (\lambda \cdot \mu_1, ..., \lambda \cdot \mu n) \text{ für } \lambda, \mu \in K \end{aligned}$$

Prüfe:

V1) $(K^n, \underline{0}, +)$ ist abelsche Gruppe (gilt, da $K0, +)$ ist abelsche Gruppe).

V2)

$$(\lambda\cdot\mu)(\nu_1,...,\nu_n) \overset{Def.}{=} ((\lambda\cdot\mu)\cdot\nu_1,...,(\lambda\cdot\mu)\cdot\nu_n) = (\lambda\cdot(\mu\cdot\nu_1,...,\lambda\cdot(\mu\cdot\nu_n)) \overset{Def.}{=} \lambda\cdot((\mu\cdot\nu_1,...,\mu\cdot\nu_n)) \overset{Def.}{=} \lambda(\mu(\nu_1,...,\nu_n))$$

D.h. $(\lambda\cdot\mu)\cdot\nu = \lambda\cdot(\mu\cdot\nu)$
V4 und V3 analog.

Beispiel. Seien $(V, 0_V, +_V, \cdot_V)$ und $(W, 0_W, +_W, \cdot_W)$ zwei Vektorräume über K. So erhält man einen Vektorraum $V\oplus W$ über K, definiert durch $V\oplus W = (V\times W, \underline{0}, +, \cdot)$ mit

$$\begin{aligned}\underline{0} &= (0_V, 0_W)\\ (v,w)+(v',w') &:= (v +_V v', w +_W w')\\ \lambda\cdot(v,w) &:= (\lambda\cdot_V v, \lambda\cdot_W w) \text{ für } v,v'\in V, w,w'\in W, \lambda\in K\end{aligned}$$

Demnächst: $(K^m, 0, +, \cdot)\oplus(K^n, 0, +, \cdot)$“ = “$(K^{m+n}, 0, +, \cdot)$

3.1 Unterobjekte

Definition 3.3. Sei $(G, e, \cdot_G)$ eine Gruppe $H\subseteq G$ heißt **Untergruppe** $\Leftrightarrow$

i) $e\in H$
ii) $\forall g,h\in H : (g^{-1}\cdot_G h)\in H$

Lemma 3.4. Sei $H\subseteq G$ eine Untergruppe. Dann gelten:

a) $\forall h\in H : h^{-1}\in H$
b) $\forall g,h\in H : (g\cdot_g h)\in H$
c) $(H, e, \cdot_G)$ ist eine Gruppe

Beweis. a) Sei $h\in H$. Wegen $e\in H$, folgt aus ii): $h^{-1}\cdot_G e = h^{-1}\in H$

b) Seien $g,h\in H :\overset{a)}{\Rightarrow} g^{-1}\in H, h\in H \overset{ii)}{\Rightarrow} (g^{-1})^{-1}\cdot h = (g\cdot h)\in H$
c) Aus b) folgt: H ist abgeschlossen unter $\cdot_G$, d.h. ” $\cdot$ ” $: H\times H\to H, (g,h)\mapsto g\cdot_G h$ ist wohldefiniert.
Axiome:
   a) gilt in G, d.h. $\forall g,h,k\in G : (g\cdot h)\cdot k = g\cdot(h\cdot k) \overset{H\subseteq G}{\Rightarrow} \forall g,h,k\in H : (g\cdot h)\cdot k = g\cdot(h\cdot k)$.
   b) $g\cdot e = g\ \forall g\in G \overset{H\subseteq G}{\Rightarrow} h\cdot e = h\ \forall h\in H$
   c) (Rechtsinverses) Wurde in a) gezeigt. □

Merke: Axiome, die nur den Allquantor ($\forall$) enthalten, “vererben sich“ auf Teilmengen. Für $\exists$ geht das nicht! Das muss man prüfen!

Beispiel.
0) Ist G eine Gruppe, so ist $H := \{e\}\subseteq G$ eine Untergruppe.
1) Ist G eine geliebige Gruppe, so ist $g\in G$ bel. $\Rightarrow H = \{g^n | n\in\mathbb{Z}\}\subseteq G$ ist Untergruppe.
2) $\{\sigma\in S_n | \sigma(n) = n\}\subseteq S_n$ ist Untergruppe (und “ = “S_{n-1})

Notation. Sei $f : M\to N$ eine Abbildung und $L\subseteq M$. Die Einschränkung $f|_L$ von f auf (dem Teildefinitionsbereich) L ist die Abbildung $f|_L : L\to f(L), l\mapsto f(l)$.

Beispiel. $H\subseteq G$ Untergruppe $\Rightarrow \cdot_G|_{H\times H} : H\times H\to H$

Definition 3.5. Sei $(K, 0, 1, +, \cdot)$ ein Körper. $L\subseteq K$ heißt **Unterkörper** $\Leftrightarrow$

i) L ist Untergruppe von $(K, 0, +)$
ii) $L \setminus \{0\}$ ist Untergruppe von $(K \setminus \{0\}, 1, \cdot)$

Proposition 3.6. Ist $L \subseteq K$ ein Unterkörper, so gelten:

a) $+_K(L \times L) = L$ (oder $L +_K L = L$) und $\cdot_K(L \times L) = L$ (oder $L \cdot_K L = L$)
b) $(L, 0, 1, +_L|_{L\times L}, \cdot_K|_{L\times L})$ ist ein Körper.

Beweis. a) Verwende Lemma 3.4 für $(K, 0, +), (K \setminus \{0\}, 1, \cdot)$ und $\forall l \in L : 0 \cdot l = l \cdot 0 = 0$.
b) Axiome K1,K2 folgen aus Lemma 3.4. Distributivgesetze in L: Vererben sich von K nach L.

Beispiel. $\mathbb{Q} \subseteq \mathbb{R}$ und $\mathbb{R} \subseteq \mathbb{C}$ sind Unterkörper.

Definition 3.7. Sei K ein Körper und V ein $K - VR$. $U \subseteq V$ heißt **Untervektorraum** (UVR) :$\Leftrightarrow$:

i) $0 \in U$
ii) $\forall \lambda \in K : \forall u \in U : (\lambda \cdot u) \in U$
iii) $\forall u, v \in U : (u + v) \in U$

Beispiel.
0) $\{0_V\} \subseteq V$ ist ein Untervektorraum.
1) Für $u \in V$ ist $\{\lambda \cdot v | \lambda \in K\}$ ein Untervektorraum (verwende $0 \cdot v = 0$ und V2 und V3)).

Proposition 3.8. Seien K ein Körper, V ein K-VR, $U \subseteq V$ ein Untervektorraum. Dann gelten:

a) $+_V(U \times U) = U$ und $\cdot_V(K \times U) = U$
b) $(U, 0, +_V|_{U\times U}, \cdot_V|_{K\times U})$ ist ein K-VR

Beweis. a) $+_V$: es genügt zu zeigen: $(U, 0, +_V|_{U\times U})$ ist eine abelsche Gruppe. Dazu genügt zu zeigen: $U \subseteq V$ und $((V, 0, +))$ ist eine Untergruppe.
Dazu: $u, v \in U \overset{ii)}{\Rightarrow} (-1) \cdot u = -u, v \in U \overset{iii)}{\Rightarrow} ((-u) + v) \in U$ und $0 \in U$ wegen i).
b) V1 wurde im Beweis von a) gezeigt. zu V2-V4: Axiome enthalten nur "$\forall$" $\Rightarrow$ Sie vererben sich auf U. $\square$

Proposition 3.9. Seien K ein Körper, V ein $K - VR$, $U, W \subseteq V$ Untervektorräume. Dann gelten:

a) $U \cap W$ ist ein UVR von V
b) $U + W = \{u + w | u \in U, w \in W\}$ ist ein UVR von V
c) $U \cup W$ ist ein UVR $\Leftrightarrow U \subseteq W$ oder $W \subseteq U$

Beweis (nur b)). i) $0 = (0 + 0) \in U + W$
ii)+iii) Seien $v, v' \in U + w$, d.h. $v = u + w, v' = u' + w'$ mit $u, u' \in U, w, w' \in W$
$\Rightarrow v + v' = (u + w) + (u' + w') = (u + u') + (w + w') \in U + W$. Sei $\lambda \in K$, dann:
$\lambda \cdot v = \lambda(u + w) = \lambda \cdot u + \lambda \cdot w \in U + W$ $\square$

4 Erezeugendensysteme, lineare Unabhängigkeit und Basen

Notation. Sei $u \in \mathbb{N}$, für $i = 1, ..., n$, sei $e_i = (0, ..., 0, 1, 0, ..., 0) \in K^n$, so dass die 1 an i-ter Stelle steht.

Lemma 4.1. $\forall v \in K^n : \exists! \lambda_1, ..., \lambda_n \in K$ mit $v = \sum_{i=1}^{n} \lambda_i \cdot e_i$

Beweis. Seien $\lambda_1, ..., \lambda_n \in K$ und

$$w := \sum_{i=1}^{n} \lambda_i \cdot (0, ..., 0, 1, 0, ..., 0) = \sum_{i=1}^{n} (0, ..., 0, \lambda_i, 0, ..., 0) = (\lambda_1, ..., \lambda_n).$$

Sei $v = (\mu_1, ..., \mu_n) \in K^n$ beliebig, dann:

$$v = \sum_{i=1}^{n} \lambda_i e_i \overset{\circledast}{\Leftrightarrow} (\mu_1, ..., \mu_n) = (\lambda_1, ..., \lambda_n) \Leftrightarrow \forall i = 1, ..., n : \lambda_i = \mu_i$$

$\square$

Im weiteren seien K ein Körper und V ein K-VR.

Definition 4.2.

a) $v \in V$ heißt **Linearkombination** (LK) von $v_1, ..., v_n \in V :\Leftrightarrow \exists \lambda_1, ..., \lambda_n \in K$ mit $v = \sum_{i=1}^{n} \lambda_i v_i$

b) Für $S \subseteq V$: v heißt LK aus $S :\Leftrightarrow \exists n \in \mathbb{N}, \exists v_1, ..., v_n \in S$. v ist LK von $v_1, ..., v_n$.

$$L(S) := \{v \in V | v \text{ ist LK aus } S\} = \text{ die } \textbf{lineare Hülle} \text{ von } S.$$

c) $S \subseteq V$ heißt **Erzeugendensystem** (ES) $\Leftrightarrow V = L(S)$

d) V heißt **endlich erzeugt** $\Leftrightarrow \exists S \subseteq V$ endlich: $V = L(S)$

e) $L(\emptyset) := \{0\}$

Beispiel. $K^n = L(\{e_1, ..., e_n\}) \leftarrow$ in Lemma 4.1.

Lemma 4.3. Sei V ein K-VR, K ein Körper und seien $S; T \subseteq V$, dann gilt:

a) $0 \in L(S)$, $S \subseteq L(S)$

b) Ist $U \subseteq V$ ein UVR, so gilt $L(U) = U$

c) $T \subseteq S \Rightarrow L(T) \subseteq L(S)$

d) $L(S)$ ist ein UVR

e) $L(S)$ ist der kleinste UVR von V, der S enthält.

f) $L(S \cup T) = L(S) + L(T)$

g) $L(L(S)) = L(S)$

Beweis. a) Falls $S = \emptyset \overset{\text{Def.}}{\Rightarrow} L(S) = \{\emptyset\} \ni 0$, $\emptyset = S \subseteq L(S)$.
Falls $S \neq \emptyset$: Für jedes $v \in S$ sind $0 \cdot v, 1 \cdot v$ LK aus $S \Rightarrow 0, v \in L(S) \Rightarrow 0 \subseteq L(S)$, $S \subseteq L(S)$

b) $U \subseteq L(U)$: gilt nach a).
$L(S) \subseteq U$: Seien $v_1, ..., v_n \in U, \lambda_1, ..., \lambda_n \in K \overset{\text{ii) von UVR}}{\Rightarrow} \lambda_1 \cdot v_1, ..., \lambda_n \cdot v_n \in U$
$\overset{\text{iii) von UVR}}{\Rightarrow} \lambda_1 v_1 + \lambda_2 v_2 \in U; \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 \in U$ ... (Induktion) $\rightarrow \lambda_1 v_1 + ... + \lambda_n v_n \in U$

c) Übung.

d) $0 \in L(S)$ nach a); Seien $v = \lambda_1 v_1 + ... + \lambda_n v_n, w = \mu_1 w_1 + ... + \mu_m w_m \in L(S)$ mit $\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_m \in K, v_1, ..., v_n, w_1, ..., w_m \in L(S) \Rightarrow v + w = \lambda_1 v_1 + ... + \lambda_n v_n + \mu_1 w_1 + ... + \mu_m w_m \in L(S)$. Analog $\lambda \cdot v = (\lambda \cdot \lambda_1) v_1 + ... + (\lambda \cdot \lambda_n) v_n \in L(S)$

e) $\not\!Z$: $\forall$ Untervektorräume $U \subseteq V$ mit $S \subseteq U$ gilt $U \supseteq L(S)$
Starte mit $S \subseteq U$. Wende $L(.)$ an $\overset{c)}{\Rightarrow} L(S) \subseteq L(U) \overset{b)}{=} U$

f),g) Übung. $\square$

Definition 4.4. Sei $S \subseteq V$.

a) S heißt **linear abhängig** $:\Leftrightarrow \exists v \in S : v \in L(S \setminus \{v\})$
b) S heißt **linear unabhängig** (l.u.) $:\Leftrightarrow \neg(S$ linear abhängig (l.a.))
c) S heißt **Basis** von V $:\Leftrightarrow S$ ist l.u. und $V = L(S)$, d.h. S ist Erzeugendensystem von V.

Beispiel. 1) Sei $S = \{V\} \subseteq V$: S l.a. $\Leftrightarrow v \in L(\emptyset) = \{\} \Leftrightarrow v = 0$

2) Sei $S = \{(1,1,0),(1,0,1),(0,1,1)\} \subseteq \mathbb{R}^3$. **Beh:** S ist l.u.
z.B.: Annahme: $(1,1,0) \in L(\{(1,0,1),(0,1,1)\})$ D.h.

$$\exists \lambda, \mu \in \mathbb{R} : (1,1,0) = \mu(1,0,1) + \lambda(0,1,1) = (\mu, \lambda, \mu + \lambda) \Rightarrow \lambda = 1 = \mu \wedge \lambda + \mu = 0 \quad \lightning$$

Lemma 4.5. Für $S \subseteq V$ sind äquivalent:

a) S ist l.u.
b) Für alle paarweise verschiedenen Vektoren $v_1, ..., v_n \in S$ ($n \in \mathbb{N}$ beliebig) und $\lambda_1, ..., \lambda_n \in K$ gilt: $\sum\limits_{i=1}^{n} \lambda_i v_i = 0 \Rightarrow \lambda_1 = ... = \lambda_n = 0$
c) Jeder Vektor $w \in L(S)$ ist eine eindeute LK aus S, d.h. sind $v_1, ..., v_n \in S$ paarweise verschieden und gelten $w = \lambda_1 v_1 + ... + \lambda_n v_n = \mu_1 v_1 + ... + \mu_n v_n$ (für alle Skalare $\mu_i, \lambda_i \in K$), so gilt: $\lambda_i = \mu_1 \wedge ... \wedge \mu_n = \lambda_n$

Beweisc)$\Rightarrow$b) Wende c) an auf $0 = \sum\limits_{i=1}^{n} \lambda_i v_i = 0 \cdot v_1 + ... + 0 \cdot v_n \overset{c)}{\Rightarrow} \lambda_1 = ... = \lambda_n = 0$

b)$\Rightarrow$a) wir zeigen: $\neg a) \Rightarrow \neg b)$: Sei $v_0 \in S$, so dass $v_0 \in L(S \setminus \{v_0\})$, d.h. $\exists v_1, ..., v_n \in S \setminus \{v_0\}$ paarweise verschieden und $\exists \lambda_1, ..., \lambda_n \in K$ mit $v_0 = \sum\limits_{i=1}^{n} \lambda_i v_i \Rightarrow (-1) \cdot v_0 + \lambda_1 v_1 + ... + \lambda_n v_n = 0$. $\lightning$ Widerspruch zu b).

a)$\Rightarrow$c) Zeige $\neg c) \Rightarrow \neg a)$: Gelte $w = \sum\limits_{i=1}^{n} \lambda_i v_i = \sum\limits_{i=1}^{n} \mu_i v_i$ (mit λ_i, μ_i, v_i wie in c)) und $\exists i_0$ mit $\lambda_{i_0} \neq \mu_{i_0}$. Dann gilt: $(\lambda_{i_0} - \mu_{i_0}) \cdot v_{i_0} = \sum\limits_{i=1, i \neq i_0}^{n} (\mu_i - \lambda_i) \cdot v_i$. Wir wissen: $\lambda_{i_0} - \mu_{i_0} \neq 0$ (in K). Multipliziere mit $\frac{1}{\lambda_{i_0} - \mu_{i_0}} : v_{i_0} = \sum\limits_{i=1, i \neq 0}^{n} (\frac{\mu_i - \lambda_i}{\lambda_{i_0} - \mu_{i_0}}) \cdot v_i \in L(S \setminus \{v\})$, d.h. $\neg a)$ $\square$

Korollar 4.6. $S \subseteq V$ ist Basis $\Leftrightarrow$ Jeder Bektor $v \in V$ ist eindeutige LK aus S.

Beweis. $S \subseteq V$ ist Basis $\Leftrightarrow S$ ist l.u. und $L(S) = V \overset{4.5 \wedge V = L(S)}{\Leftrightarrow}$ Jedes $v \in V$ ist eindeutige LK aus S. $\square$

Korollar 4.7. Sei $S = \{e_1, ..., e_n\} \subseteq K^n$ mit $e_i = (0, ..., 0, 1, 0, ..., 0) \in K^n$, wobei die 1 an i-ter Stelle steht. Dann ist nach Lemma 4.1 S eine Basis von K^n.
Bezeichnung: $\{e_1, ..., e_n\}$ heißt **Standardbasis** von K^n.

Korollar 4.8. Jedes endlich ES $S \subseteq V$ enthält eine Basis $B \subseteq S$ von V.

Beweis. Sei $E := \{T \subseteq S | T$ ist ES von $V\}$. $E \neq \emptyset$, denn $S \in E$. S ist endlich $\Rightarrow$ alle $T \subseteq S$ sind endlich.
Wähle $T \subseteq E$ mit kleinster Kardinalität.
Beh: T ist Basis von V. $\not\!Z$: T ist l.u.
Sonst (T l.a.) $\exists v \in T$ mit

$$v \in L(T \setminus \{v\}) (\Rightarrow L(\{v\}) \subseteq L(T \setminus \{v\})) \Rightarrow L(T \setminus \{v\}) = L(T \setminus \{v\}) + l(\{v\}) \overset{Lemma\ 4.3}{=} L(T \setminus \{v\} \cup \{v\}) = L(T) = V.$$

Aber: $|T \setminus \{v\}| < |T|$, d.h. Widerspruch zur Wahl von T. $\square$

Lemma 4.9. Sei $S \subseteq V$ l.u. und $v \notin L(S) \Rightarrow S \cup \{v\}$ ist l.u.

Beweis. Annahme: $S \cup \{v\}$ ist l.a. $\Rightarrow \exists$ Vektoren $v_1, ..., v_n \in S$ paarweise verschieden und $\lambda, \lambda_1, ..., \lambda_n$ mit $0 = \lambda \cdot v + \lambda_1 \cdot v_1 + ... + \lambda_n \cdot v_n$ und nicht $\lambda = \lambda_1 = ... = \lambda_n = 0$!
Fall 1: $\lambda = 0 \overset{S\,l.u.}{\Rightarrow} \lambda_1 = ... = \lambda_n = 0$ ↯
Fall 2: $\lambda \neq 0 \Rightarrow v = (-\frac{\lambda_1}{\lambda}) \cdot v_1 + ... + (-\frac{\lambda_n}{\lambda}) \cdot v_n \in L(S)$ ist ein Widerspruch zur Voraussetzung $v \notin L(S)$ □

Satz 4.10 (Austauschsatz von Steinitz)**.** Sei $T \subseteq V$ ein ES und $S \subseteq V$ l.u. mit $|S| < \infty$. Dann $\exists \tilde{T} \subseteq T$ mit $|\tilde{T}| = |S|$, so dass $(T \setminus \tilde{T}) \cup S$ ein ES von V.

Korollar 4.11. Sei V endlich erzeugt und $S \subseteq V$ l.u., dann gilt:

a) Für jedes ES T von V gilt: $|T| \geq |S|$ und insbesondere gilt $|S| < \infty$
b) Je zwei Basen von V haben dieselbe Kardinalität

Beweis (von Korollar)**.** Sei nur S endlich. Dazu sei $T \subseteq V$ ein endliches ES mit $m = |T|$.
Steinitz: Annahme: $|S| > m \Rightarrow \exists S_0 \subseteq S$ mit $|S_0| = m + 1$ und S_0 l.u.
Steinitz: $\exists \tilde{T} \subseteq T$ mit $|\tilde{T}| = |S_0|$ und ... $\Rightarrow |S_0| = |\tilde{T}| \leq |T| = m$ ↯

a) es ist noch zu zeigen: Ist T ein unendliches ES von V, so gilt: $|T| \geq |S|$. Dies folgt aus $|T| = \infty > |S|$
b) Seien T, T' Basen von $V \Rightarrow T, T'$ l.u. $\overset{a)}{\Rightarrow} T, T'$ endlich. Nun: T ist ES $\wedge T'$ ist l.u. $\overset{a)}{\Rightarrow} |T| \geq |T'|; T'$ ist ES $\wedge T$ ist l.u. $\overset{a)}{\Rightarrow} |T'| \geq |T| \Rightarrow |T| = |T'| (< \infty)$ □

Definition. Elemente $x_1, ..., x_n$ einer Menge X heißen **paarweise verschieden**$\Leftrightarrow \forall i \neq j : x_i \neq x_j (\Leftrightarrow |\{x_1, ..., x_n\}| = n$

Bemerkung. 4.10 und 4.11 gelten auch für $|S| = \infty$ bzw. V nicht endlich erzeugt. Benötigt "Auswahlaxiom" und "unendliche Mächtigkeit".

Beweis (von 4.10)**.**

1) Beh: Sei $U \subseteq V$ ein UVR, $T \subseteq V$ ein ES, $v \in V \setminus U$. Dann gilt: $\exists t \in T \setminus U$, so dass $T \setminus \{t\} \cup \{v\}$ ein ES ist. Denn: Schreibe $v = \sum\limits_{i=1}^{n} \lambda_i t_i$ mit $t_1, ..., t_n \in T, \lambda_i \in K$ und $t_1, ..., t_n$ seien paarweise verschieden und alle $\lambda_i \neq 0 (v \neq 0)$. Ein $t_{i_0} \notin U$, sonst LK$\in U$, aber $v \notin U \overset{\lambda_{i_0}}{\Rightarrow} t_{i_0} = \frac{1}{\lambda_{i_0}} \cdot v + \sum\limits_{i=1, i \neq i_0}^{n} (\frac{-\lambda_i}{\lambda_{i_0}})$.
$t_i \in L(T \setminus \{t_{i_0}\} \cup \{v\} \Rightarrow T \subseteq L(T \setminus \{t_{i_0}\} \cup \{v\} \Rightarrow V = L(T) \subseteq L(T \setminus \{t_{i_0}\} \cup \{v\}) \subseteq V$
2) Induktion über $N := |S|$. (Der Fall $n = 0, S = \emptyset$ ist klar).
$n \mapsto n + 1$: Gelte 4.10 für alle $S' \subseteq V$ l.u. mit $|S'| = n$. Sei $S \subseteq V$ l.u. mit $|S| = n + 1$. Schreibe $S = S' \cup \{v\}$ mit $|S'| = n$ Induktionsvoraussetzung: $\exists T' \subseteq T$ mit $|T'| = n$ und $T \setminus T' \cup S'$ ist ES von V.
Wende 1) auf $v \in V \setminus L(S)$ an, denn S ist l.u. $\overset{1)}{\Rightarrow} \exists t \in T \setminus T' \cup S' \setminus L(S)$ mit $X = T \setminus T' \cup S' \setminus \{t\} \cup \{v\}$ ist ES. Wegen $t \notin L(S)$ gilt $t \notin S'$, d.h. $t \in T \setminus T' \Rightarrow X = T \setminus (T' \cup \{t\}) \cup (S' \cup \{v\})$. Nenne nun $T' \cup \{t\} =: \tilde{T}$ und $S' \cup \{s\} =: S$. □

Definition 4.12.

a) Sei V ein endlich erzeugter K-VR. Ist $T \subseteq V$ eine Basis, sod efiniert man $dim_K V := |T|$ als die **Dimension** von V.
b) Ist V ein K-VR ohne endliches ES, so setze $dim_K V = \infty$

Notation. Ist K aus dem Kontext klar, so schreibe $dim V$ statt $dim_k V$.

Warnung: $dim_{\mathbb{C}} \mathbb{C} = 1$ aber $dim_{\mathbb{R}} \mathbb{C} = 2$.

Sprechweise: Ein K-VR heißt endlich-dimensional $:\Leftrightarrow dim_K V < \infty (\Leftrightarrow V$ ist endlich erzeugter K-VR)

Korollar 4.13. Sei V ein endlich-dimensionaler $K-VR$, $T \subseteq V$ ein ES, $S \subseteq V$ l.u. Dann gelten:

a) $|S| \leq dimV$ und ($|S| = dimV \Leftrightarrow S$ ist Basis von V)
b) $|T| \geq dimV$ und ($|T| = dimV \Leftrightarrow T$ ist Basis von V)

Beweis. Übung, linke Hälfte aus Kor.4.11, rechte Hälft: Satz von Steinitz.

Satz 4.14 (Basisergänzungssatz)**.** Sei V ein endlich-dimensionaler K-VR. Sei $S \subseteq V$ l.u. Dann gilt: $\exists S' \subseteq V, S \subseteq S'$ und S' ist Basis von V. (d.h. Elemente von $S' \setminus S$ ergänzen S zu eine Basis).

Beweis. Sei $S' \supseteq S$ l.u. und von maximaler Kardinalität (Wissen: S' l.u. $\Rightarrow |S'| \leq dimV$). Annahme: $L(S) \subset V \Rightarrow \exists v \in V, v \notin L(S) \overset{Lemma\ 4.9}{\Rightarrow} S' \cup \{v\}$ ist l.u. $\lightning$,
denn: $|S' \cup \{v\}| = |S'| + 1 > |S'|$, aber S' hat maximale Kardinalität. □

Korollar 4.15. Sei V ein K-VR und $d \in \mathbb{N}$. Gelte $|S| \leq d$ für alle $S \subseteq V$ l.u. Dann gilt: $dimV \leq d$.

Beweis. Mit derselben Idee wie in 4.14.

Korollar 4.16. Sei V ein endlich-dimensionaler $K-VR$ und $W \subseteq V$ ein UVR. Dann gelten:

a) $dimW \leq dimV$
b) $dimW = dimV \Rightarrow W = V$
c) Jede Basis von W lässt sich zu einer Basis von V ergänzen.

Beweis.

c) folgt aus 4.14,
a) folgt aus 4.13, weil Basis von W ist l.u. und in V.
b) ist 4.13 a) 2. Teil.

Erinnerung: Seien M, N endliche Mengen. Dann $|M \cup N| = |M| + |N| - |M \cap N|$

Satz 4.17 (Dimensionsformel für Untervektorräume)**.** Seien V ein endlich-dimensionaler K-VR und $U, W \subseteq V$ UVR'e, dann gilt: $dim(U + W) = dimU + dimW - dim(U \cap W)$

Beweis. Sei $dimV < \infty \overset{4.16}{\Rightarrow} U + W, U, W, U \cap W \subseteq V$ sind endlich-dimensional. Sei B_0 Basis von $U \cap W$. Egänze zu Basis $B_1 \supseteq B_0$ von U. Ergänze zu Basis $B_2 \supseteq B_0$ von W. Behauptung: i) $B_1 \cap B_2 = B_0$ ii) $B_1 \cup B_0$ ist ES von $U + W$ iii) $B_1 \cup B_2 (= B_1 \dot{\cup} B_2 \setminus B_0)$ ist l.u.
Die Behauptung impliziert: $dim(U + W) \overset{ii) \wedge iii)}{=} |B_1 \cup B_2| \overset{Erinn.}{=} |B_1| + |B_2| - |B_1 \wedge B_2| \overset{i)}{=} dimU + dimW - dim(U \cap W)$.

i) Sei $b \in B_1 \cap B_2 \supseteq B_0 \overset{B_1\ l.u.}{\Rightarrow} B_0 \cup \{b\}$ l.u. $\subseteq B_1$ und $\subseteq B_2 \Rightarrow B_0 \cup \{b\}$ ist l.u. von $L(B_1)$ und $L(B_2) \Rightarrow B_0 \cup \{b\} \subseteq U \cap W$ ist l.u. $\Rightarrow |B_0 \cup \{b\}| \leq dimU \cap W = |B_0| \Rightarrow b \in B_0$
ii) $U + W = L(B_1) + L(B_2) = L(B_1 \cup B_2) \Rightarrow B_1 \cup B_2$ ist ES von $U + W$.
iii) $B_1 \cup B_2$ ist l.u., denn: Seien $\lambda_b, b \in B_2 \cup B_1$ Elemente aus V mit $\circledast \sum\limits_{b \in B_1 \cup B_2} \lambda_b \cdot b = 0$ $\underline{zz:}$ alle $\lambda_b = 0$

$\circledast \Rightarrow \sum\limits_{b \in B_1} \lambda_b \cdot b = \sum\limits_{b \in B_2 \setminus B_1} (-\lambda_b) \cdot b =: w \Rightarrow w \in W \cap U \overset{w \in L(B_0) \wedge B_1\ l.u.}{\Rightarrow} \lambda_w = 0\, \forall b \in B_1 \setminus B_0$ (linke Seite $\overset{\circledast}{\Rightarrow} \sum\limits_{b \in B_0} \lambda_b \cdot b = 0 \overset{B_0\ l.u.}{\Rightarrow} \lambda_b = 0\, \forall b \in B_0$, d.h. $\lambda_b = 0\, \forall b \in B_1 \setminus B_0 \cup B_2 \setminus B_0 \cup B_0 = B_1 \cup B_2$ □

Notation. K Körper, V ein $K-VR$, $V_1, ..., v_n \in V$ sind k.u. (bzw. eine Basis) $:\Leftrightarrow \{v_1 ..., v_n\} \subseteq V$ ist l.u. (bzw. Basis) und $v_1, ..., v_n$ sind paarweise verschieden.

Bemerkung. $v_1, ..., v_n \in V$ sind l.u. $\Leftrightarrow$

1) $\forall i = 1...n : v_i \notin L(\{v_1, ..., v_{i-1}, v_{i+1}, ..., v_n\}) \Leftrightarrow$
2) $\forall \lambda_1, ..., \lambda_n \in K : (\sum\limits_{i=1}^{n} \lambda_i v_i = 0 \Rightarrow \lambda_1 = ... = \lambda_n = 0)$

5 Matrizen und Gauß-Elimination

Sei K ein Körper, $m, n \in \mathbb{N}$

Definition 5.1.

a) Eine $m \times n$-Matrix A über K ist eine Tabelle mit m Zeilen und n Spalten und Einträgen aus K:

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

b) Der Eintrag a_{ij} heißt **Matrixkoeffizienten** an der Stelle (i, j)

c) Die Menge aller $m \times n$-Matrizen ist $M_{m\times n}(K)$

d) Eine $1 \times n$-Matrix heßt **Zeilenvektor** der Länge n $\begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix}$. $Z_n(K) := M_{1\times n}(K)$. Eine $m \times 1$-Matrix heißt **Spaltenvektor** der Länge m $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$. $V_m(K) = M_{m\times 1}(K)$

e) Für $A = (a_{ij})$ aus a) heißt $(a_{i1} \dots a_{in})$ die i-te Zeile von A $(i = 1...m)$. Für $j = 1...n$ heißt $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ der j-te Spaltenvektor von A.

Übung. $M_{m\times n}(K)$ ist ein VR über K (der Dimension $m \cdot n$) mit: $(a_{ij})_{i=1...mj=1...n} + (b_{ij})_{\substack{i=1...m \\ j=1...n}} = (a_{ij} + b_{ij})_{\substack{i=1...m \\ j=1...n}}$ und $\lambda \cdot (a_{ij}) := (\lambda \cdot a_{ij})$ für $\lambda \in K$. $(a_{ij}), (b_{ij}) \in M_{m\times n}(K)$.

Hinweis: $M_{m\times n}(K) = Abb(\{1, ..., m\} \times \{1, ..., n\}, K)$

Bemerkung. $Z_n(K)$“ $=$ “$K^n((a_1...a_n))\widehat{=}(a_1, ..., a_n))$

Definition 5.2. Für $A = (a_{ij}) \in M_{e\times m}(K), B = (b_{jk}) \in M_{mxn}(K)$ definiert man $A \cdot B = (c_{ik})_{\substack{i=1...l \\ k=1...n}} \in M_{exn}(K)$ durch $c_{ik} := \sum\limits_{j=1}^{m} a_{ij} \cdot b_{jk}$. D.h. c_{ik} berechnet sich aus Zeile i von A und Spalte k von B: $c_{ik} = (a_{i1} \dots a_{im}) \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{mk} \end{pmatrix} = a_{i1} \cdot b_{1k} + a_{i2} \cdot b_{2k} + a_{im} \cdot b_{mk}$

Beispiel. $\begin{pmatrix} 1 & -3 & 2 \\ 3 & -5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 7 \\ 1 & 12 \end{pmatrix}$ $c_{12} = \begin{pmatrix} 1 & -3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$

Bemerkung. $A \cdot B$ für $A \in M_{exm_1}(K), B \in M_{m_2\times n}(K)$ ist nicht definiert, falls $m_1 \neq m_2$

5.1 Anwendung von Matrizen

Gegeben: $S = \{w_1, ..., w_m\} \subseteq K^n$
Finde a) “einfache Basis“ von $L(S)$ b) eine maximale l.u. Teilmenge $S' \subseteq S$

Gegeben S wie oben, definiere $A := \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix}$, d.h. i-te Zeile von A ist der Vektor w_i (als Zeilenvektor)

Definition 5.3.

a) $A = (a_{ij}) \in M_{m\times n}(K)$ ist in **Zeilenstufenform** (ZSF) $:\Leftrightarrow \exists r \in \{0, ..., m\}, \exists 1 \leq j_1 < j_2 < \cdots < j_r \leq n$, so dass für $i > r$ und $j \in \{1...n\}$ gilt $a_{ij} = 0$ und für $i \in \{1...r\}$ gilt $a_{ij_i} \neq 0$ und $a_{ij} = 0$ für $1 \leq j \leq j_i$

$$\begin{pmatrix}
0 & \dots & 0 & a_{1j_1} & * & \dots & \dots & \dots & \dots & \dots & * \\
0 & \dots & \dots & 0 & a_{2j_2} & * & \dots & \dots & \dots & \dots & * \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \dots & \dots & \dots & \dots & \dots & 0 & a_{rj_r} & * & \dots & * \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0
\end{pmatrix}$$

b) A wie in a) heißt **reduzierte Zeilenstufenform** (red. ZSF) $:\Leftrightarrow$ A hat ZSF (wie in a)) und Pivot-Elemente $a_{ij_i}, i = 1...r$, sind 1 und $a_{kj_i} = 0$ für $k \neq i$ $(i \in \{1...r\}, k \in \{1...m\})$

Beispiel.

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 4 & 0 \end{pmatrix} \text{ hat ZSF.} \qquad \begin{pmatrix} 1 & 2 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ hat reduzierte ZSF (für } K = \mathbb{R})$$

Lemma 5.4. Sei $A \in M_{m\times n}(K)$ mit Zeilen $w_1, ..., w_m$ aus K^n. Ist A in ZSF mit r Zeilen $\neq \underline{0} (\underline{0} = (0...0))$, so ist $w_1, ..., w_r$ eine Basis von $L(\{w_1, ..., w_m\})$

Beweis. Übung.

Gauß-Elimination: Überführt eine beliebige $m \times n$-Matrix durch "elementare Zeilentransformationen" E1-E3 (s.u.) in reduzierte ZSF.

Definition 5.5. E1-E3 sind wie folgt definiert:

E1) Vertausche zwei Zeilen der Matrix.

E2) Addition des Vielfachen einer Zeile zu einer anderen.

E3) Multiplikation einer Zeile mit einem Skalar $\lambda \in K \setminus \{0\}$.

Beispiel.

$$\begin{pmatrix} 2 & 3 & 0 \\ 1 & 1 & 0 \end{pmatrix} \overset{E1}{\rightarrow} \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \end{pmatrix} \overset{E2}{\rightarrow} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \overset{E3}{\rightarrow} \begin{pmatrix} 2 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Lemma 5.6. Seien $A, \tilde{A} \in M_{m\times n}(K)$ mit Zeilen $w_1, ..., w_m$ bzw. $\tilde{w}_1, ..., \tilde{w}_m$. Entsteht $\tilde{A}$ aus A durch wiederholtes Anwenden von E1,E2,E3, so gilt $L(\{w_1, ..., w_m\}) = L(\{\tilde{w}_1, ..., \tilde{w}_m\})$ $\circledast$

Beweis. Induktion über die Anzahl der Anwendungen von E1,E2,E3, es genügt zz: $\circledast$ gilt beim einmaligem Anwenden von E1,E2 oder E3.
zu E1: Vertauschen zweier Zeilen führt zu $S = \tilde{S}$. Die Zeilen insgesamt sind dieselben Mengen.
zu E2: z.B. Addiere $\lambda\cdot$ Zeile i zu Zeile $j \neq i$. $\tilde{w}_k = w_k$ für $k \neq j$, $\tilde{w}_j = w_j + \lambda \cdot w_i (i \neq j) \Rightarrow \tilde{S} \subseteq L(S) \Rightarrow L(\tilde{S}) \subseteq L(L(S)) = L(S)$. umgekehrt: $w_k = \tilde{w}_k$ für $k \neq j, w_j = \tilde{w}_j - \lambda \tilde{w}_i$, wie eben $S \subseteq L(\tilde{S}) \Rightarrow L(S) = L(\tilde{S})$..., E3) analog. $\square$

Satz 5.7. Jede Matrix $A \in M_{m\times n}(K)$ lässt sich durch endlich viele Anwendungen von E1 und E2 (bzw. E1-E3) in (reduzierte) ZSF überführen; durch den Gauß-Algorithmus.

Beweis. Gauß-Algorithmus nur für ZSF mit Induktion über m. $m = 1$ ist klar.
$\underline{m \mapsto m+1:}$ Fall 1: alle $a_{ij_i} = 0$.

Fall 2: Sei j_1 der kleinste Index einer Spalte $\neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Sei $i \in \{1...m\}$, so dass $a_{ij_1} \neq 0$. Vertausche Zeilen 1 und i. So erhalten wir die Matrix

$$\tilde{A} = \begin{pmatrix} 0 & \dots & 0 & \tilde{a}_{1j_1} & \dots & * \\ \vdots & \dots & \vdots & * & \dots & \vdots \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 0 & * & \dots & * \end{pmatrix}$$

für $i = 2...m$. Addiere $(-\frac{\tilde{a}_{ij_1}}{\tilde{a}_{1j_1}})\cdot$ Zeile 1 zu Zeile i (E2) $\rightarrow$ Wir erhalten:

$$\tilde{B} = \begin{pmatrix} 0 & \dots & 0 & \tilde{a}_{1j_1} & * & \dots & * \\ \vdots & \dots & \vdots & 0 & \vdots & \dots & \vdots \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 0 & 0 & * & \dots & * \end{pmatrix}$$

Sei B die $(m-1) \times n$-Matrix bestehend aus den Zeilen $2...m$ von $\tilde{B}$. Wende Induktionsvoraussetzung an, d.h. Gauß-Algorithmus für B. Beachte: Algorithmus für B erhält Nullen der Einträge (i,j) $i = 2...m, j = 1...j_1$ $\square$

Beispiel. $K = \mathbb{Q}$

$$\begin{pmatrix} 0 & 3 & 3 \\ 2 & 4 & 7 \\ 1 & 2 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 5 \\ 2 & 4 & 7 \\ 0 & 3 & 3 \end{pmatrix} \begin{matrix} -2 \\ + \\ \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 5 \\ 0 & 0 & -3 \\ 0 & 3 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 5 \\ 0 & 3 & 3 \\ 0 & 0 & -3 \end{pmatrix} \begin{matrix} \\ \mid \cdot \frac{1}{3} \\ \mid \cdot -\frac{1}{3} \end{matrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} + \\ + \\ -1 \quad -5 \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} + \\ -2 \\ \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Proposition 5.8. Seien $A, \tilde{A} \in M_{mxn}(K)$ mit Zeilen $w_1, ..., w_m$ bzw. $\tilde{w}_1, ..., \tilde{w}_m$. Sei $\tilde{A}$ in ZSF, entsanden aus A durch den Algorithmus im obigen Beweis.
Dann gelten:

a) $\tilde{w}_1, ..., \tilde{w}_r$ ist Basis von $L(\{w_1, ..., w_m\})$ für $r =$Anzahl der Zeilen $\neq (0...0)$ in $\tilde{A}$.
b) Seien $i_1...i_r$ die Nummern der Zeilen, die unter Anwendung von E1 in die Zeilen $1, ..., r$ getauscht wurden. Dann sind $w_{i_1}, ..., w_{i_r}$ eine Basis von $L(\{w_1, ..., w_m\})$

Beweis.

a) Lemma5.4 + Lemma5.6
b) Skizze: Führe Algorithmus durch. Danach streiche alle Zeilen bis auf $i_1, ..., i_r$ in A, und die entsprechenden Zeilen in den Matrizen "zwischen "A und $\tilde{A}$. Man beobachtet, dass die Zeilen $\tilde{w}_1, ..., \tilde{w}_r$ Linearkombinationen von $w_{i1}, ..., w_{ir}$ sind. $\square$

Beispiel.

$$\begin{pmatrix}1&2&3\\2&4&6\\1&2&4\end{pmatrix}\begin{array}{l} {}^{-2}\ {}^{-1}\\ +\\ \quad\ +\end{array} \rightsquigarrow \begin{pmatrix}1&2&3\\0&0&0\\0&0&1\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&2&3\\0&0&1\\0&0&0\end{pmatrix}$$

$r = 2 \Rightarrow \{\begin{pmatrix}1 & 2 & 3\end{pmatrix} = w_1$ und $w_3 = \begin{pmatrix}1 & 2 & 4\end{pmatrix}\}$ ist Basis von $L(\{w_1, w_2, w_3\})$

$A \in M_{m\times n}(K)$ haben Zeilen $w_1, ..., w_m$ und Spalten $v_1, ..., v_n$.

Definition 5.9.

a) $L(\{w_1, ..., w_m\}) \subseteq Z_m(K)$ heißt **Zeilenraum** von A.
b) $dim(L(\{w_1, ..., w_m\}))$ heißt **Zeilenrang** von A.
c) $L(\{v_1, ..., v_n\}) \subseteq V_n(K)$ heißt **Spaltenraum** von A.
d) $dim(L(\{v_1, ..., v_n\}))$ heißt **Spaltenrang** von A.

Demnächst: Spaltenrang A = Zeilenrang A

Proposition 5.10 (schon gezeigt!)**.**

a) Der Zeilenrang von $A \in M_{m\times n}(K)$ ist unverändert (invariant) unter Anwendung von E1,E2,E3.
b) Der Zeilenrang ist die maximale Anzahl linear unabhängiger Vektoren unter $w_1, ..., w_m$.

6 Strukturerhaltende Abbildungen (Morphismen)

<u>*Definition* 6.1 :</u> Seien $(G, e_G, \circ_G)$ und $(H, e_H, \circ_H)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt <u>*Gruppenhomomorphismus*</u> $\Leftrightarrow \forall g_1, g_2 \in G : \varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$

<u>*Lemma* 6.2 :</u> a) Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, dann gelten:
i) $\varphi(e_G) = e_H$ ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$
b) Sind $\varphi_1 : G_1 \to G_2$ und $\varphi_2 : G_2 \to G_3$ Gruppenhomomorphismen, so auch $\varphi_2 \circ \varphi_1 : G_1 \to G_3$

<u>*Beweis* :</u> a) i) $\varphi(e_G) = \varphi(e_G \circ_G e_G) \overset{Homom.}{=} \varphi(e_G) \circ_H \varphi(e_G)$ Verknüpfe mit $\varphi(e_G)^{-1} (\in H) \Rightarrow e_H = \varphi(e_G)$
ii) $\varphi(g^{-1}) \circ_H \varphi(g) \overset{Homom.}{=} \varphi(g^{-1} \circ_G g) = \varphi(e_G) = e_H$ und $\varphi(g)^{-1}$ ist die eindeutige Lösung von $x \circ \varphi(g) \overset{Lemma\, 2.5}{=} e_H$
b) Übung.

<u>*Definition* 6.12 :</u> Seien $(K, 0_K, 1_K, +_K, \cdot_K)$ und $(L, 0_L, 1_L, +_L, \cdot_L)$ Körper. Eine Abbildung $\varphi : L \to L$ heißt <u>*Körperhomomorphismus*</u> $:\Leftrightarrow$ i) $\forall x, y \in K : \varphi(x +_K y) = \varphi(x) +_L \varphi(y)$
ii) $\forall x, y \in K : \varphi(x \cdot_K y) = \varphi(x) \cdot_L \varphi(y)$
iii) $\varphi(1_K) = 1_L$

<u>*Lemma* 6.13 :</u> (folgt aus 6.2) Für einen Körperhomomorphismus $\varphi : K \to L$ gelten: i) $\varphi(0_K) = 0_L$
ii) $\varphi(-x) = -\varphi(x) \, \forall x \in K$
iii) $\varphi(x^{-1}) = \varphi(x)^{-1} \, \forall x \in K \setminus \{0\}$

<u>*Beispiel* :</u> Folgende Abbildungen sind Körperhomomorphismen: a) $\mathbb{Q} \to \mathbb{R}, q \mapsto q$
b) $\mathbb{R} \to \mathbb{C}, r \mapsto (r, 0)$
c) $\mathbb{C} \to \mathbb{C}, z = (a, b) \mapsto \overline{z} := (a, -b)$

<u>*Beispiel* :</u> Sei G eine Gruppe und $\mathbb{Q}^x = \mathbb{Q} \setminus \{0\}$. Folgende Abbildungen sind Gruppenhomomorphismen: a) $id_G : G \to G, g \mapsto g$
b) $(\{e_G\}, e_G, \circ_G) \to G, e_G \mapsto e_G$
c) $(\mathbb{Q}^x, 1, \cdot) \to (\{\pm 1\}, 1, \cdot), q \mapsto \begin{cases} +1 & q > 0 \\ -1 & q < 0 \end{cases}$
d) $(\mathbb{Z}, 0, +) \to (\mathbb{Z}/n, \bar(0), \overline{+})$ ist ein Gruppenhomomorphismus.

Nächstes Ziel: Der Vorzeichenhomomorphismus $sgn : S_n = Bij(\{1...n\}) \to (\{\pm 1\}, 1, \cdot)$ $n \in \mathbb{N}$
<u>*Notation* :</u> Schreibe $\sigma \in S_n$ als $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ (Wertetabelle)
<u>*Beispiel* :</u> $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

<u>*Definition* 6.3 :</u> Die <u>*Menge der Fehlstände*</u> (Fst.) von $\sigma \in S_n$ ist $F_\sigma := \{(i, j) | 1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)\}$. $l(\sigma) := |F_\sigma| :=$ <u>*Zahl der Fehlstände*</u>.

<u>*Satz* 6.4 :</u> Die Vorzeichenfunktion $\sigma : S_n \to \{\pm 1\}, \sigma \mapsto (-1)^{l(\sigma)}$ ist ein Gruppenhomomorphismus.

<u>*Beispiel* :</u> $l(\sigma) = 1 + 1 + 1 = 3$, $F_\sigma = \{(1, 2), (1, 4), (3, 4)\}$

<u>*Beispiel* :</u> i) $\sigma \in S_n$ gegeben durch $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 \end{pmatrix}$ $F_{\sigma 1} = \{(i, j) | i < j\} = \{(3, 4), (3, 5), (3, 6), (4, 6), (5, 6)\}$, $l(\sigma_1) = |F_\sigma| = 5$. $sgn(\sigma) = (-1)^5 = -1$

ii) $sgn(id) = (-1)^{l(id)} = (-1)^{|F_{id}|} = 1$

<u>*Definition* 6.5 :</u> a) $\sigma \in S_n$ heißt <u>*Transposition*</u> $:\Leftrightarrow \sigma$ genau 2 Elemente aus $\{1...n\}$ vertauscht.

b) Für $1 \leq i < j \leq n$ definiert man die Transposition $\tau_{(i,j)} \in S_n$ durch $\tau_{(i,j)}(k) := \begin{cases} k & \text{falls } k \neq i,j \\ j & \text{falls } k = i \\ i & \text{falls } k = j \end{cases}$

c) Die $\tau_{(i,i+1)} \in S_n$ heißen <u>*Nachbartranspositionen*</u>.

<u>*Bemerkung* :</u> i) $\sigma_1 = \tau_{(3,6)}$
ii) Ist $\tau \in S_n$ eine Transposition $\Rightarrow \tau^2 = \tau \cdot \tau = id$, denn $\tau = \tau_{(i,j)}$, $1 \leq i < j \leq n$.

$$\tau_{(i,j)} \cdot \tau_{(i,j)}(k) = \tau_{(i,j)}(\tau_{(i,j)}(k)) = \begin{cases} \tau_{(i,j)}(k) & \text{falls } \tau_{(i,j)}(k) \neq i,j \widehat{=} k \neq i,j \\ j & \text{falls } \tau_{(i,j)}(k) = i \widehat{=} k = j \\ i & \text{falls } \tau_{(i,j)}(k) = j \widehat{=} k = i \end{cases} = \begin{cases} k & k \neq i,j \\ j & k = j = id \\ i & k = i \end{cases}$$

<u>*Lemma* 6.6 :</u> Zu $\sigma \in S_n \setminus \{id\}$ gibt es Transpositionen $\tau_1, ..., \tau_k$ mit $k \leq n-1$, so dass $\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_k$

<u>*Beweis* :</u> Induktion über n: n=1 gilt, denn $S_1 \setminus \{id\} = \emptyset$
<u>$n \rightsquigarrow n+1$:</u> Sei $\sigma \in S_{n+1} \setminus \{id\}$ Fall 1: $\sigma(n+1) = n+1$ und $\tilde{\sigma} := \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \in S_n \setminus \{id\}$
$\tilde{\sigma} = \tilde{\tau}_1 \circ \tilde{\tau}_2 \circ ... \circ \tilde{\tau}_k$ mit $k \leq n-1$, τ_l's sind Transpositionen aus S_n. $\tilde{\tau}_l := \begin{pmatrix} 1 & 2 & \dots & n & n+1 \\ \tilde{\tau}_l(1) & \tilde{\tau}_l(2) & \dots & \tilde{\tau}_l(n) & n+1 \end{pmatrix} \in$ S_{n+1} und es gilt $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$, $k \leq (n+1) - 2$
Fall 2: $\sigma(n+1) \neq n+1 \rightsquigarrow \tau = \tau_{(\sigma(n+q),n+1)} \in S_{n+1}$
$S_{n+1} \ni \tilde{\sigma} := \tau \circ \sigma \Rightarrow \tilde{\sigma} = \begin{pmatrix} 1 & 2 & \dots & n & n+1 \\ \tilde{\sigma}(1) & \tilde{\sigma}(2) & \dots & \tilde{\sigma}(n) & n+1 \end{pmatrix}$. Auf $\tilde{\sigma}$ wenden wir den gerade bewiesenen Fall 1 an: i) $\tau \circ \sigma = \tilde{\sigma} = \tau_1 \circ ... \circ \tau_k$ mit $k \leq n-1$ $|\tau \cdot \_ \Rightarrow \tau \circ \tau \circ \sigma = \tau \circ \tau_1 \circ ... \circ \tau_k$, $\sigma = \tau \circ \tau_1 \circ ... \circ \tau_k$ $k+1 \leq (n+1) - 1$, was zu zeigen war. oder ii) $\tau \circ \sigma = \tilde{\sigma} = id \rightsquigarrow \sigma = \tau$ $\square$

<u>*Beispiel* :</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \rightsquigarrow \tau_{(1,4)} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. $\tau_{(1,3)} \circ \tau_{(2,4)} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$

<u>*Bemerkung* :</u> $\tau_{(1,2)} \circ \tau_{(1,3)} \circ \tau_{(2,4)} \circ \sigma = id \Rightarrow \sigma = \tau_{(2,4)} \circ \tau_{(1,3)} \circ \tau_{(1,2)}$

<u>*Übung* 6.7 :</u> Jede Transposition ist eine Verkettung von Nachbartranspositionen.

<u>*Beispiel* :</u> $\tau_{(1,3)} = \tau_{(1,2)} \circ \tau_{(2,3)} \circ \tau_{(1,2)}$

<u>*Korollar* 6.8 :</u> (zu Lemma 6.6 und 6.7) Jedes $\sigma \in S_n$ ist ein Produkt von Nachbartranspositionen.

<u>*Lemma* 6.9 :</u> Für $\sigma \in S_n$ und $1 \leq i \leq n-1$ gilt $l(\sigma \circ \tau_{(i,i+1)}) =$
$\begin{cases} l(\sigma) - 1 & \text{falls } (i,i+1) \text{ Fst. von } \sigma \Leftrightarrow \sigma(i) > \sigma(i+1) \\ l(\sigma) + 1 & \text{falls } (i,i+1) \text{ kein Fst. von } \sigma \Leftrightarrow \sigma(i) < \sigma(i+1) \end{cases}$
<u>*Beweis* :</u> Schreibe $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \rightsquigarrow \tilde{\sigma} =$
$\begin{pmatrix} 1 & 2 & 3 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(i-1) & \sigma(i+1) & \sigma(i) & \sigma(i+2) & \dots & \sigma(n) \end{pmatrix}$. Vergleiche F_σ mit $F_{\tilde{\sigma}}$. Seien k,l : $1 \leq k < l \leq n$.
a) <u>$\{k,l\} \cap \{i,i+1\} = \emptyset$:</u> (k,l) Fst. von $\sigma \Leftrightarrow (k,i+1)$ Fst. von $\tilde{\sigma}$
b) <u>$l \in \{i,i+1\}, k < i$:</u> (k,i) Fst. von $\sigma \Leftrightarrow \sigma(k) > \sigma(i) = \tilde{\sigma}(i+1) \Leftrightarrow (k,i+1)$ Fst. von $\tilde{\sigma}$, d.h. (k,i) Fst. von $\sigma \Leftrightarrow (k,i+1)$

Fst. von $\tilde{\sigma}$ und $(k, i+1)$ Fst. von $\sigma \Leftrightarrow (k,i)$ Fst. von $\tilde{\sigma}$
c) $\underline{k \in \{i, i+1\}, l > i+1:}$ analog zu b).
d) $\underline{(k,l) = (i, i+1):}$ $(i, i+1)$ Fst. von $\sigma \Leftrightarrow \tilde{\sigma}(i+1) = \sigma(i) > \sigma(i+1) = \tilde{\sigma}(i) \Leftrightarrow (i, i+1)$ ist kein Fst. von $\tilde{\sigma}$, d.h. bis auf $(k,l) = (i, i+1)$, ist die Anzahl von Fehlständen von σ gleich der Anzahl von Fehlständen von $\tilde{\sigma}$. Dann bleibt $(k,l) = (i, i+1)$ zu untersuchen.
$\cdot$ $(i, i+1)$ Fst. von $\sigma \Rightarrow$ ist kein Fst. von $\tilde{\sigma} \Rightarrow l(\tilde{\sigma}) = l(\sigma) = -1$
$\cdot$ $(i, i+1)$ kein Fst. von $\sigma \Rightarrow$ ist Fs. von $\tilde{\sigma} \Rightarrow l(\tilde{\sigma}) = l(\sigma) + 1$ □

$\underline{\textit{Korollar}\ 6.10:}$ (Ü) σ, i wie im Lemma. Dann ist $sgn(\sigma \circ \tau_{(i,i+1)}) = -sgn(\sigma)$

$\underline{\textit{Lemma}\ 6.11:}$ (Ü) $\forall \sigma \in S_n, \forall \tau_1, ..., \tau_m$ Nachbartranspositionen ist $sgn(\sigma \circ \tau_1 \circ ... \circ \tau_m) = sgn(\sigma) \cdot (-1)^m (= sgn(\sigma) \cdot sgn(\tau_1 \circ ... \circ \tau_m))$

$\underline{\textit{Beweis zu Satz}\ 6.4:}$ Seien $\sigma, \sigma' \in S_n$ $\underline{zz:}$ $sgn(\sigma \circ \sigma') \stackrel{!}{=} sgn(\sigma) \circ sgn(\sigma')$
Schreibe σ' als Produkt (Verkettung) von Nachbartranspositionen. $\sigma' = \tau_1 \circ ... \circ \tau_m$, dann gilt $sgn(\sigma \circ \sigma') = sgn(\sigma \circ \tau_1 \circ ... \circ \tau_m) = sgn(\sigma) \cdot sgn(\sigma')$ □

$\underline{\textit{Definition}\ 6.14:}$ Sei K ein Körper und seien V, W K-Vektorräume. Eine Abbildung $f : V \to W$ heißt $\underline{(K)-linear}$ (oder ein $\underline{K-VR-Homomorphismus}$) $:\Leftrightarrow$ i) $\forall v, w \in V : f(v+w) = f(v) + f(w)$ und ii) $\forall \lambda \in K, v \in V : f(\lambda \cdot v) = \lambda \cdot f(v)$
Die Menge der (K)-linearen Abbildungen von V nach W bezeichnet man mit $Lin(V, W)$ bzw. $(Lin_K(V, W))$.

$\underline{\textit{Facts}:}$ 0) $f : V \to W$ linear $\Rightarrow f(0_V) = 0_W$
1) $id_V : V \to V$ ist linear.
2) Sind $f : U \to V$ und $g : V \to W$ lineare Abbildungen, so auch $g \circ f : U \to W$
3) Ist $f : V \to W$ linear und $U \subseteq V$ ein UVR, so ist $f|_U : U \to W$ linear.

$\underline{\textit{Lemma}\ 6.15:}$ Sei $f : V \to W$ linear. Dann gilt für $n \in \mathbb{N}$, für $\lambda_1, ..., \lambda_n \in K, v_1, ..., v_n \in V : f(\sum\limits_{i=1}^{n} \lambda_i v_i = \sum\limits_{i=1}^{n} \lambda_i f(v_i)$

$\underline{\textit{Beweis}:}$ Induktion über n: $n = 1$ ist klar wegen ii).
$\underline{n \mapsto n+1:}$ $f(\sum\limits_{i=1}^{n+1} \lambda_i v_i) = f(\sum\limits_{i=1}^{n} \lambda_i v_i + \lambda_{n+1} v_{n+1}) \stackrel{i)}{=} f(\sum\limits_{i=1}^{n} \lambda_i v_i) + f(\lambda_{n+1} v_{n+1} \stackrel{Ind.Vor.}{=} \sum\limits_{i=1}^{n} \lambda_i f(v_i) + \lambda_{n+1} f(v_{n+1})$-
□

$\underline{\textit{Bemerkung}:}$ $f : V \to W$ ist linear $\Leftrightarrow \forall \lambda \in K, \forall v_1, v_2 \in V : f(\lambda v_1 + v_2) = \lambda \cdot f(v_1) + f(v_2)$

$\underline{\textit{Korollar}\ 6.16:}$ (Ü) Sei $f : V \to W$ linear und $S \subseteq V$. Dann gilt: $f(L(S)) = L(f(S))$

$\underline{\textit{Beispiel}\ 6.17:}$ Sei W ein K-VR, seine $w_1, ..., w_n \in W$ beliebig. Dann definiert $(\lambda_1, ..., \lambda_n) \mapsto \sum\limits_{i=1}^{n} \lambda_i w_i$ die eindeutige lineare Abbildung $f : K^n \to W$ mit $f(e_i) = w_i$

$\underline{\textit{Beweis}:}$ z.B.: $f(\nu \cdot (\lambda_1, ..., \lambda_n) + (\mu_1, ..., \mu_n)) = f((\nu\lambda_1 + \mu_1, ..., \nu\lambda_n + \mu_n)) \stackrel{Def.}{=} \sum\limits_{i=1}^{n} (\nu \cdot \lambda_i + \mu_i) \cdot w_i = \nu \cdot \sum\limits_{i=1}^{n} \lambda_i w_i + \sum\limits_{i=1}^{n} \mu_i w_i = \nu f(...) + f(...)$ □

$\underline{\textit{Lemma}\ 6.18:}$ Seien V, W VR'e, M eine Menge. Dann gelten: a) $Abb(M, W)$ ist ein K-VR durch $f + g : M \to W, m \mapsto f(m) + g(m), \lambda \cdot f : M \to W, m \mapsto \lambda \cdot f(m)$ für $f, g : M \to W$ und $\lambda \in K$.

b) $Lin(V,W) \subseteq Abb(V,W)$ ist ein UVR. (Ü)

<u>*Lemma* 6.19 :</u> Sei $f : V \to W$ linear, seien $U \subseteq V$ und $X \subseteq W$ UVR'e. Dann gelten: a) $f(U) \subseteq W$ ist UVR
b) $f^{-1}(X) \subseteq V$ ist UVR

<u>*Beweis* :</u> a) $f(U) = f(L(U)) \overset{6.16}{=} L(f(U)) \subseteq W$ ist UVR.
b) Ü. □

<u>*Definition* 6.20 :</u> Für eine lineare Abbildung $f : V \to W$ ist $Kern(f) := f^{-1}(\{0\}) = \{v \in V | f(v) = 0\}$ der <u>*Kern*</u> von f und $Bild(f) = f(V)$ das <u>*Bild*</u> von f.

<u>*Fact* :</u> $Kern(f) \subseteq V$ und $Bild(f) \subseteq W$ sind UVR'e.

<u>*Lemma* 6.21 :</u> Für eine lineare Abbildung $f : V \to W$ gelten: a) f surjektiv $\Leftrightarrow Bild(f) = W$
b) f injektiv $\Leftrightarrow Kern(f) = \{0\}$

<u>*Beweis* :</u> (nur b)) $f : (V, 0, +) \to (W, 0, +)$ als Homom. von Gruppen. In Übung 24: $Kern(f) = \{0\} \Leftrightarrow f$ injektiv. □

<u>*Definition* 6.22 :</u> Sei $f : V \to W$ eine lineare Abbildung. f heißt <u>*Monomorphismus*</u> $:\Leftrightarrow Kern(f) = \{0\}$
b) <u>*Endomorphismus*</u> $:\Leftrightarrow Bild(f) = W$
c) <u>*Isomorphismus*</u> $:\Leftrightarrow f$ ist Monom. $\wedge f$ ist Epim. $\Leftrightarrow f$ ist linear und bijektiv.

<u>*Satz* 6.23(*Dimensionsformel für lineare Abbildungen*) :</u> Sei $f : V \to W$ eine lineare Abbildung und sei V endlich-dimensional. Dann gelten: a) $Bild(f)$ ist endlich-dimensional
b) $dimKern(f) + dimBild(f) = dimV$
c) f ist Monomorphismus $\Leftrightarrow dimBild(f) = dimV$ (aus b) und 6.21)

<u>*Beweis* :</u> $Kern(f) \subseteq V$ ist UVR $\overset{4.16}{\Rightarrow} dimKern(f) \leq dimV < \infty$. Wähle Basis B_0 von $Kern(f)$; ergänze durch $C \subseteq V$ zu Basis $B_0 \dot\cup C$ von V. Schreibe $C = \{w_1, ..., w_m\}$ mit $m = |C|$.
Behauptung 1: $f(w_1), ..., f(w_m)$ sind l.u. (in W). Seien dazu $\lambda_1, ..., \lambda_m \in K$ (bel.), so dass gilt: $0 = \sum_{i=1}^{n} \lambda_i f(w_i \overset{6.15}{=} f(\sum_{i=1}^{m} \lambda_i w_i) \Rightarrow v := \sum_{i=1}^{m} \lambda_i w_i \in Kern(f) = L(B_0) \Rightarrow \exists \mu_b \in K : \sum_{b \in B_0} \mu_b \cdot b = v \Rightarrow 0 = v - v = \sum_{i=1}^{m} \lambda_i w_i + \sum_{b \in B_0} (-\mu_b) \cdot b \overset{B_0 \dot\cup C \text{ Basis}}{\Rightarrow} \lambda_i = 0$ für $i = 1...m$ (und alle $\mu_b = 0$) $\Rightarrow$ Behauptung 1.
Behauptung 2: $\{f(w_1)...f(w_m)\}$ ist ES von $Bild(f)$, denn: $Bild(f) = f(L(B_0 \dot\cup C)) = L(f(B_0) \cup f(C)) = L(f(B_0 \cup C)) = L(f(C)) = L(\{f(w_1), ..., f(w_m)\})$.
<u>*Beh.*1 $\wedge$ *Beh.*2</u> $\Rightarrow f(w_1), ..., f(w_m)$ ist Basis von $Bild(f) \Rightarrow dimBild(f) = m \Rightarrow$ a)
zu b): $dimBild(f) + dimKern(f) = |C| + |B_0| = |C \dot\cup B_0| = dimV$ □

<u>*Satz* 6.26 :</u> Gelte $dimV = dimW < \infty$, dann sind für $f \in Lin(V,W)$ äquivalent:
a) f ist ein Monomorphismus
b) f ist ein Epimorphismus
c) f ist ein Isomorphismus

<u>*Beweis* :</u> a)$\Leftrightarrow$b): a) $\overset{Def.}{\Leftrightarrow} Kern(f) = \{0\} \overset{6.23}{\Leftrightarrow} dimV = dimBild(f) \overset{dimW = dimV}{\Leftrightarrow} Bild(f) = W \Leftrightarrow$ b)
a)$\Leftrightarrow$c): a)$\Rightarrow$a)$\wedge$b)$\overset{Def.}{\Leftrightarrow}$c)$\overset{klar}{\Rightarrow}$a) □

<u>*Definition* 6.27 :</u> a) Eine lineare Abbildung $f : V \to V$ heißt <u>*Endomorphismus*</u>

b) Ein bijektiver Endomorphismus heißt *Automorphismus*
c) $End(V) = Lin(V,V)$ und $Aut(V) = \{f \in End(V) | f \text{ ist bijektiv}\}$.

Korollar 6.28 : Sei V ein endlich-dimensionaler VR. Dann sind für $f \in End(V)$ äquivalent:
a) f ist Monomorphismus
b) f ist Epimorphismus
c) f ist Isomorphismus ($\Leftrightarrow f$ ist Automorphismus)

6.1 Isomorphie von Vektorräumen

Definition 6.24 : K-VR'e V und W heißen *isomorph* (schreibe $V \simeq W$):$\Leftrightarrow \exists$ Isomorphismus $f \in Lin(V,W)$.

Übung 6.35 : i) Ist f Isom. $f : V \to W$, so ist $f^{-1} : W \to V$ K-linearer Isom.
ii) Die Verkettung von Isomorphismen ist ein Isomorphismus.
iii) $f : V \to W$ ist Isom. $\Leftrightarrow \exists g \in Lin(V,W)$ mit $f \circ g = id_W \wedge g \circ f = id_V$
iv) Isomorphie ist eine Äquivalenzrelation auf der Menge aller VR'e.

Sei K ein Körper, V ein K-VR und endlich-dimensional.
Definition 6.29 : a) eine *geordnete Basis* von V ist ein Tupel $\underline{B} = (b-1, ..., b_n) \in V^n$, so dass $b_1, ..., b_n$ eine Basis von V.

b) Für $\underline{B}$ aus a) definiere die Abbildung $\iota\underline{B} : V_n(K) \to V : \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto \sum \lambda_i b_i$

Proposition 6.30 : Ist $\underline{B}$ geordnete Basis von V, so ist $\iota\underline{B}$ ein Isomorphismus. $\iota\underline{B} : V_n(K) \to V, \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto$

$\sum\limits_{=1}^{n} \lambda_i b_i$ ein VR-Isomorphismus.

Beweis : $\iota\underline{B}$ wohldefiniert und linear: siehe Bsp. 6.17.
$\iota\underline{B}$ bijektiv: nach Kor.4.6: Ist $b_1, ..., b_n$ Basis von V, so gibt es $\forall v \in V : \exists!(\lambda_1, ..., \lambda_n) \in K^n$ mit $v = \sum\limits_{i=1}^{n} \lambda_i b_i$

Beachte : $\iota\underline{B}(e_i) = b_i$ für $e_1, ..., e_n$ Standardbasis von $V_n(K)$, $e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, wobei die 1 an i-ter Stelle steht.

Korollar 6.31 : Seien V, W endlich-dimensionale UVR'e über K. Dann gilt: a) $dimV = n \Rightarrow V \simeq V_n(K)$ (vermöge $\iota\underline{B}$ aus 6.30 für geordnete Basis $\underline{B}$ von V)
b) $dimV = dimW \Leftrightarrow V \simeq W$

Beweis zu b) : "$\Rightarrow$ " : Sei $n = dimV = dimW < \infty \overset{a)}{\Rightarrow} V \simeq V_n(K) \simeq W$. Nun: $\simeq$ ist eine Äquivalenzrelation.
"$\Leftarrow$": Wähle Isomorphismus $f : V \to W$. Dimensionsformel ("für f"): $dimV = dimKern(f) + dimBild(f) = 0 + dimW$ $\square$

Lemma 6.32 : (Ü) Seien V, W VR'e über K. Sei $\underline{B} = (b_1, ..., b_n)$ geordnete Basis von V und sei $(w_1, ..., w_n)$ ein Tupel von Vektoren aus W. Dann gelten: a) $\exists! f \in Lin(V, W)$ mit $(f(b_i) = w_i$ für $i = 1...n$
b) Ist $w_1, ..., w_n$ Basis von W, so ist f aus a) ein Isomorphismus.

7 Darstellungsmatrizen (lineare Abbildungen)

<u>*Spezialfall* :</u> Sei $e_1, ..., e_n \in V_n(K)$ die Standardbasis. Für $f \in Lin(V_n(K), V_m(K))$ definiere $Mat(f) := (f(e_1)...f(e_n)) \in M_{mxn}(K)$

<u>*Lemma* 7.1 :</u> a) $Mat : Lin(V_n(K), V_m(K)) \to M_{mxn}(K), f \mapsto Mat(f)$ ist ein VR-Isomorphismus.
b) $\forall \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in V_n(K)$ gilt $f(\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}) = Mat(f) \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in V_m(K)$
c) Es gilt $A = Mat(f) \Leftrightarrow \forall \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in V_n(K) : f(\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}) = A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$

<u>*Beweis* :</u> a) i) Mat ist linear: Seien $f, g \in Lin(V_n(K), V_m(K))$. $Mat(f+g)$ hat j-te Spalte $(f+g)(e_j) = f(e_j) + g(e_j)$. $Mat(f) + Mat(g)$ hat j-te Spalte $f(e_j) + g(e_j)$. analog $\lambda \cdot f$
ii) Mat injektiv: wegen 6.32 ist f eindeutig bestimmt.
iii) Mat surjektiv: wegen 6.32(/6.17) eindeutige lineare Abbildung.
b) $f(\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}) = f(\sum_{i=1}^{n} \lambda_i e_i) \overset{f\ lin.}{=} \sum_{i=1}^{n} \lambda_i f(e_i) = ((f(e_1)...f(e_n)) \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = Mat(f) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$
c) " $\Rightarrow$ " ist b). " $\Leftarrow$ " $A \cdot \_$ ist lineare Abbildung. (Ãœbung, siehe unten). $A \cdot e_j$ =Spalte von $A = A \cdot e_j = f(e_j)$ =Spalte j von $Mat(f)$ □

<u>*Beispiel* :</u> $V_n(K) \to V_m(K) \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_5 \end{pmatrix} \mapsto \sum \lambda_i w_i$. Dann: $Mat(f) = \begin{pmatrix} w_1 & \dots & w_n \end{pmatrix}$ $(w_i \in V_m(K))$

<u>*Korollar* 7.2 (Verkettungsregel für Mat):</u> Für lineare Abbildungen $f : V_n(K) \to V_m(K), g : V_m(K) \to V_l(K)$ gilt: $Mat(g \circ f) = Mat(g) \cdot Mat(f)$

<u>*Beweis* :</u> Für $v = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in V_n(K)$ gilt: $Mat(g \circ f) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \overset{7.1b)}{=} (g \circ f)(v) = g(f(v)) = Mat(g) \cdot f(v) =$
$Mat(g) \cdot Mat(f) \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \overset{7.1c)}{\Rightarrow} Mat(g) \cdot Mat(f) = Mat(g \circ f)$ □

<u>*Korollar* 7.3 :</u> $dim Lin(V_n(K), V_m(K)) = dim M_{mxn}(K) = m \cdot n$

<u>*Beweis* :</u> $Lin(V_n(K), V_m(K)) \overset{7.1a)}{\simeq} M_{mxn}(K) \simeq Abb(\{1...m\} \times \{1...n\}, K) \leftarrow$ hat Dimension $n \cdot m$. Nun: 6.31 □

<u>*Lemma* 7.4 :</u> (Ü) Seien U, V, W, X K-VR'e und $f : W \to X$ und $h : U \to V$ lineare Abbildungen. Dann gelten:
a) $l_f : Lin(V, W) \to Lin(V, X), g \mapsto f \circ g$ ist lineare Abbildung.
b) $r_h : Lin(V, W) \to Lin(U, W), g \mapsto g \circ h$ ist lineare Abbildung.
c) Ist f ein Isom., so auch l_f
d) Ist h ein Isom., so auch r_h

<u>*Korollar* 7.5 :</u> Für $A, A' \in M_{mxn}(K)$, $B, B' \in M_{exm}(K)$ gelten: a) $(B + B') \cdot A = B \cdot A + B' \cdot A$
b) $B \cdot (A + A') = B \cdot A + B \cdot A'$

c) Für $\lambda \in K : \lambda \cdot (B \cdot A) = (\lambda \cdot B) \cdot A = B \cdot (\lambda \cdot A)$

<u>*Beweis* :</u> z.B. a) wähle $g, g' \in Lin(V_m(K), V_l(K)), h \in Lin(V_n(K), V_m(K))$, so dass $Mat(g) = B$; $Mat(G') = B', Mat(h) = A \overset{7.4b)}{\Rightarrow} (g + g') \circ h = g \circ h + g' \circ h \overset{Mat\,lin.}{\Rightarrow} Mat((g + g') \circ h) = Mat(g \circ h) + Mat(g' \circ h) \overset{7.2}{\Rightarrow} Mat(g + g') \cdot Mat(h) = Mat(g) \cdot Mat(h) + Mat(g') \cdot Mat(h)$ $\square$

<u>*Allgemeiner Fall ("Darstellungsmatrizen")* :</u> Seien V, W K-VR'e mit geordneten Basen $\underline{B} = (b_1, ..., b_n)$ bzw. $\underline{C} = (c_1, ..., c_m)$. Für $f : V \to W$ betrachte

$$\begin{array}{ccccc} V & \xrightarrow{f} & W & \to f(b_j) \\ {}^\iota\underline{B}\uparrow & & \uparrow{}^\iota\,\underline{C} & \\ V_n(K) & & V_m(K) & \to \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} \end{array}$$

<u>*Lemma* 7.6 :</u> Die folgenden Abbildungen sind VR-Isomorphismen: a) $Lin(V, W) \to Lin(V_n(K), V_m(K)), f \mapsto {}^\iota\underline{C}^{-1} \circ f \circ {}^\iota\,\underline{B}$
b) $Mat^{\underline{C}}_{\underline{B}} : Lin(V, W) \to M_{mxn}(K), f \mapsto Mat^{\underline{C}}_{\underline{B}}(f) := Mat({}^\iota\underline{C}^{-1} \circ f \circ {}^\iota\underline{B})$ ($Mat^{\underline{C}}_{\underline{B}}(f)$ heißt <u>*Darstellungsmatrix*</u> von f bezüglich $\underline{B}$ und $\underline{C}$)

<u>*Beweis* :</u> a) Anwendung von 7.4c) und d); beachte ${}^\iota\underline{B}, {}^\iota\,\underline{C}^{-1}$ sind Isomorphismen.
b) $Mat^{\underline{C}}_{\underline{B}}$ ist die Verkettung der VR-Isomorphismen.

<u>*Korollar* 7.7 :</u> $dimLin(V, W) = dimV \cdot dimW$ falls V und W endlich-dimensionale K-VR'e.

<u>*Direkte Beschreibung von* $Mat^{\underline{C}}_{\underline{B}}(f)$:</u> Für $j = 1...n$ liegt $f(B_j) \in L(\{c_1, ..., c_m\}) \overset{C\ Basis}{\Rightarrow} \exists!(a_{1j}, ..., a_{mj}) \in K^m$ mit $f(b_j) = \sum_{i=1}^{m} a_{ij} \cdot c_i$

<u>*Proposition* 7.8 :</u> $Mat^{\underline{C}}_{\underline{B}}(f) = (a_{ij})_{\substack{i=1...m \\ j=1...n}} \in M_{mxn}(K)$

<u>*Beweis* :</u> Spalte j von $Mat({}^\iota\underline{C}^{-1} \circ f \circ {}^\iota\underline{B})$ $(= Mat^{\underline{C}}_{\underline{B}}(f)) = ({}^\iota\underline{C}^{-1} \circ f \circ {}^\iota\underline{B}(e_j) = {}^\iota\,\underline{C}^{-1}(f(b_j))$ =der Spaltenvektor $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix} \in V_m(K)$ mit ${}^\iota\underline{C} \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix} = \sum_{i=1}^{m} \mu_i c_i = f(b_j) \overset{C\ Basis}{\Rightarrow} \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ =Spalte j von A. $\square$

<u>*Bemerkung* :</u> a) Sind $\underline{E}_n$ und $\underline{E}_m$ die Standardbasen von $V_n(K)$ bzw. $V_m(K)$, so gilt: $Mat = Mat^{\underline{E}_m}_{\underline{E}_n}$
b) Formale Schreibweise in (7.8): $(f(b_1)...f(b_n)) = f(\underline{B} = \underline{C} \cdot A$ $(A = Mat^{\underline{C}}_{\underline{B}}(f))$

<u>*Proposition* 7.9 (*Verkettung von Darstellungsmatrizen*) :</u> Seien V, W, X K-VR'e und endlich-dimensional, mit geordneten Basen $\underline{B}$ von $V, \underline{C}$ von $W, \underline{D}$ von X. Dann gilt für $f \in Lin(V, W)$ und $g \in Lin(W, X)$: $\circledast\circledast = Mat^{\underline{D}}_{\underline{B}}(g \circ f) = Mat^{\underline{D}}_{\underline{C}}(g) \cdot Mat^{\underline{C}}_{\underline{B}}(f) = \circledast$

<u>*Beweis* :</u> Betrachte

$$\begin{array}{ccccc} V & \xrightarrow{f} & W & \xrightarrow{g} & X \\ \simeq\uparrow^\iota\,\underline{B} & & \simeq\uparrow^\iota\,\underline{C} & & \simeq\uparrow^\iota\,\underline{D} \\ V_n(K) & & V_m(K) & & V_l(K) \end{array} .$$

$\circledast = Mat({}^\iota\underline{D}^{-1} \circ g \circ {}^\iota\underline{C}) \cdot Mat({}^\iota\underline{C}^{-1} \circ f \circ {}^\iota\underline{B}) \overset{7.2}{=} Mat({}^\iota\underline{D}^{-1} \circ g \circ {}^\iota\underline{C} \circ {}^\iota\underline{C}^{-1} \circ f \circ {}^\iota\underline{B}) = Mat({}^\iota\underline{D}^{-1} \circ f \circ f \circ {}^\iota\underline{B}) = \circledast\circledast$ $\square$

<u>*"Formaler Beweis"* :</u> Schreibe $A = Mat^{\underline{C}}_{\underline{B}}(f), A' = Mat^{\underline{D}}_{\underline{C}}(g)$
$f(B) = \underline{C} \cdot A$" $\overset{g\ anw.}{\Rightarrow}$ "$g(f(\underline{B})) = g(\underline{C} \cdot A) \overset{\ddot{U}}{=} g(\underline{C}) \cdot A \overset{7.8}{\Rightarrow} Mat^{\underline{D}}_{\underline{B}}(g \circ f) = A' \cdot A$ $\square$

$\underline{Spezialfall:}$ $V = W$ endlich-dimensionale VR'e mit Basen $\underline{B}$ und $\underline{C}$ von V. Dann heißt $Mat^{\underline{C}}_{\underline{B}}(id_V) =: A$ $\underline{Basiswechselmatrix}$ (von $\underline{B}$ nach $\underline{C}$).

$\underline{Proposition\,7.10:}$ Sei $n = dimV$. Schreibe $v \in V$ als $v = \sum\limits_{i=1}^{n} \lambda_i b_i = \sum\limits_{i=1}^{n} \mu_i c_i$. Dann gilt: $A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$

$\underline{Beweis:}$ Schreibe $v = \begin{pmatrix} b_1 & \dots & b_n \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$ (formal). Form gilt: $\underline{B} = id_V(\underline{B} = Mat^{\underline{C}}_{\underline{B}}(id_V) \cdot \underline{C} = \underline{C} \cdot A \Rightarrow v =$ $\underline{B} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \underline{C} \cdot (A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}) = \underline{C} \cdot \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} \overset{\underline{C}\ Basis}{\Rightarrow} A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$ $\square$

$\underline{Bemerkung:}$ Koordinatn (bzw. Koeffizienten) von v sind Spaltenvektoren. Geordnete Basen sind "Zeilen-Tupel".

7.1 Eigenschaften von Basiswechselmatrizen

$\underline{Proposition\,7.11:}$ Für $A \in M_{nxn}(K)$ (quadratische Matrix), sind äquivalent: a) $Spaltenrang(A) = n$
b) $l_A : V_n(K) \to V_n(K), v \mapsto A \cdot v$ ist Isom.
c) $\exists A' \in M_{nxn}(K) : A \cdot A' = 1_n$
d) $\exists A' \in M_{nxn}(K) : A' \cdot A = 1_n$ für $1_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \in M_{nxn}(K)$.
Die Matrizen in c),d) sind eindeutig und dieselben.

$\underline{Beweis:}$ a) $\Leftrightarrow$ $Bild(l_A) = l_A(L(\{e_1, ..., e_n\})) = L(\{Ae_1, ..., Ae_n\}) = V_n(K)$, da $A \cdot e_j$ =Spalte j von A.$\Leftrightarrow$ l_A ist Epim.$\overset{l_A\ Endom.}{\Leftrightarrow}$ l_A ist Isom.
b) $\Rightarrow$ c)$\wedge$d): l_A Isom. $\Rightarrow \exists g \in Lin(V_n(K), V_n(K)) : g \circ l_A = id_{V_n(K)} = l_A \circ g \overset{Mat\ anw.}{\Rightarrow} Mat(g) \cdot Mat(l_A) \overset{7.2}{=}$ $Mat(id_{V_n(K)}) = 1_n = A \cdot Mat(g) = A \cdot A' = A' \cdot A$
d)$\Rightarrow$b): Aus d) folgt: $l_{A'} \circ l_A = l_{1n} = id_{V_n(K)} \Rightarrow$ inj.$\Rightarrow$ l_A ist injektiv, d.h. ein Monom. $\overset{l_A\ Endom.}{\Rightarrow}$ l_A ist Isom., d.h. b) gilt. c)$\Rightarrow$b) ist analog.
Zusatz: Eindeutigkeit von A' folgt aus b)$\Rightarrow$c)$\wedge$d), denn $A' = Mat(l_a^{-1})$ und l_A^{-1} ist eindeutig. $\square$

$\underline{Definition\,7.12:}$ i) $A \in M_{nxn}(K)$ heißt $\underline{invertierbar}$ $\Leftrightarrow$ a)-d) aus 7.11 gelten.
ii) Schreibe A^{-1} für die Matrix A' aus c) (oder d)).
iii) $GL_n(K) := \{A \in M_{nxn}(K) | A \text{ ist invertierbar}\}$

$\underline{ddotU:}$ $(GL_n(K), 1_n, \cdot)$ ist eine Gruppe, nicht abelsch für $n \geq 2$

$\underline{Satz\,7.13:}$ Sei $\underline{C} = (c_1, ..., c_n)$ geordnete Basis von V. Dann gilt:
a) Für $\underline{B}$ eine geordnete Basis von V ist $Mat^{\underline{C}}_{\underline{B}}(id_V) \in GL_n(K)$
b) Für $A \in GL_n(K)$ ist $\underline{C} \cdot A =: \underline{B}$ eine geordnete Basis von V.
(Ü) c) $GL_n(K) \to \{\text{geordnete Basen von } V\}, A \mapsto \underline{C} \cdot A$ ist eine Bijektion.

$\underline{Lemma\,7.14:}$ Seien V,W endlich-dimensionale K-VR'e mit geordneten Basen $\underline{B}$ und $\underline{C}$ und $f : V \to W$

linearer Isom. Dann ist $Mat^{\underline{C}}_{\underline{B}}(f)$ invertierbar.

<u>*Beweis* :</u> Sei $n = dimV = dimW$. $Mat^{\underline{C}}_{\underline{B}}(f) \in M_{nxn}(K)$ und $Mat^{\underline{B}}_{\underline{C}}(f^{-1}) \cdot Mat^{\underline{C}}_{\underline{B}}(f) \overset{7.9}{=} Mat^{\underline{B}}_{\underline{B}}(f^{-1} \circ f) = Mat^{\underline{B}}_{\underline{B}}(id_V) = 1_n$ $\square$

<u>*Beweis von* 7.13 :</u> a) Wende 7.14 an auf $V = W$ und $f = id_V$
b) $\underline{B} := \underline{C} \cdot A \overset{\cdot A^{-1}}{\Rightarrow} \underline{B} \cdot (A^{-1}) = \underline{C} \Rightarrow \{c_1, ..., c_n\} \in L(\underline{B}) \Rightarrow V = L(\{c_1, ..., c_n\})$ ist Teilmenge von $L(\{b_1, ..., b_n\}) \subseteq V \Rightarrow \{b_1, ..., b_n\}$ ist ES von V mit $v > dimV$ Elementen.$\Rightarrow \{b_1, ..., b_n\}$ ist Basis. $\square$

8 Dualräume und lineare Funktionale

Sei V ein VR über K, K ein Körper.
<u>*Motivation :*</u> Ein UVR $U \subseteq V$ lässt sich auf (mindestens) 2 Arten beschreiben:
a) Als lineare Hülle einer Teilmenge $S \subseteq V$
b) Falls $V = V_n(K)$ und $a_i = (a_{i1}, ..., a_{in}) \in Z_n(K), i = 1...m$,so ist die <u>*Nullstellenmenge*</u> linearer Gleichungen $\{v \in V_n(K) | a_i \cdot v = 0, i = 1...m\} \subseteq V$ ein UVR.

<u>*Definition :*</u> i) $V^* := Lin_K(V, K)$ heißt <u>*Dualraum*</u> von V
ii) Die Elemente $\xi \in V^*$ heißen <u>*lineare Funktionale*</u> (Linearformen).

V^* übernimmt "Funktion"von $Z_n(K)$ im Vergleich zu $V_n(K)$: Ist $S^* \subseteq V^*$, so ist $\{v \in V | \xi(v) = 0 \forall \xi \in S^*\} \subseteq V$ ein UVR.

<u>*Nachbemerkung zu Mat_B^C und $GL_n(K)$:*</u> i) Ess gibt keine Standard-Definition von Mat_B^C: Vorsicht!
ii) <u>*Bsp :*</u> $V = W = V_n(K)$. $\underline{E} = (e_1, ..., e_n)$ Standardbasis, $\underline{B} = (b_1, ..., b_n)$ beliebige Basis $A = Mat_{\underline{B}}^{\underline{E}}(id_V) =?$
Spalte j von $A = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$ erfüllt: $b_j = id_V(b_j) = \sum\limits_{i=1}^{n} a_{ij} \cdot e_i = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$, d.h. $A = (b_1 ... b_n)$. Frage nun: $Mat_{\underline{E}}^{\underline{B}}(id_V) =?? = A^{-1} \leftarrow$ in 3. VL!

<u>*zu Dualräumen :*</u> <u>*Proposition 8.2 :*</u> a) V^* ist ein VR über K, (denn $V^* = Lin_K(V, K)$)
b) $dimV < \infty \Rightarrow dimV^* = dimV$
c) $(V_n(K))^* = Lin(V_n(K), V_1(K)) \overset{Mat\,\simeq}{\rightarrow} Mat_{1xn}(K) = Z_n(K)$ ist ein Isom.

<u>*Beweis :*</u> b) $dimV^* = dim(Lin(V, K)) \overset{7,7}{=} dim_K V \cdot dim_K K = dimV \cdot 1$
c) Folgt direkt aus 7.1 $\square$

Funktional zu Zeilenvektor $z = (a_1 ... a_n) \in Z_n(K)$ unter 8,2c)?

Sei $\xi \in V^*$ beliebig und $e_1 ... e_n$ Standardbasis von $V_n(K) \Rightarrow Mat(\xi) = (\xi(e_1) \dots \xi(e_n)) \Rightarrow \xi(\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}) =$
$\xi(\sum\limits_{i=1}^{n} \lambda_i e_i) \overset{\xi\ lin.}{=} \sum\limits_{i=1}^{n} \lambda_i \xi(e_i) \overset{falls\ Mat(\xi)=z}{=} \sum\limits_{i=1}^{n} \lambda_i a_i = (a_1 ... a_n) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$

Sei $\underline{B} = (b_1, ..., b_n)$ geordnete Basis von $V \Rightarrow$ für $i = 1...n \exists!$ lineare Abbildung $b_i^* : V \to K$, so dass $b_j \mapsto \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$

<u>*Lemma 6.25 :*</u> <u>*Bsp :*</u> Ist $e_1 ... e_n$ Standardbasis von $V_n(K)$, so gilt: $e_i^* = (0 \dots 010 \dots 0)$

<u>*Proposition 8.3 :*</u> $\underline{B}^* := (b_1^*, ..., b_n^*)$ ist Basis von V^*, die <u>*Dualbasis*</u> zu $\underline{B} = (b_1, ..., b_n)$ (Basis von V)

<u>*Beweis :*</u> $dimV^* = n$, nach 8.2a) $\Rightarrow$ genügt zz: $b_1^*, ..., b_n^*$ sind l.u.
Seien $\lambda_1, ..., \lambda_n \in K$, so dass $\xi = \sum\limits_{i=1}^{n} \lambda_i b_i^* = 0$ (d.h. ξ ist die Null-Abbildung). Berechne $0 = \xi(b_j) = \sum\limits_{i=1}^{n} \lambda_i b_i^*(b_j) = \lambda_j \cdot 1 + 0 + ... + 0 \Rightarrow$ alle $\lambda_j = 0$ $\square$

$\underline{Definition\, 8.4:}$ Der $\underline{Bidualraum}$ von V ist $V^{**} := (V^*)^*$.

$\underline{"Bsp:":}$ Der Dualraum von $Z_n(K)$ ist $V_n(K)$, indem man $\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix} \in V_n(K)$ das Funktional $Z_n(K) \to K; (a_1...a_n) \mapsto (a_1....a_n)\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix}$ $\Rightarrow$ Bidual von $V_n(K) \simeq$ Dual von $Z_n(K) \simeq V_n(K)$

$\underline{Satz\, 8.5:}$ (Ü) Sei $b_V : V \to Lin(V^*, K) = V^{**}, v \mapsto (b_V(v) : \xi \in V^* \mapsto \xi(v))$. Dann gelten: a) $b_V(v)$ ist in der Tat linear.
b) $b_V : V \to V^{**}$ ist linear.
c) Gilt $dim < \infty$, so ist b_V ein Isom.

$\underline{Definition\, 8.6:}$ Seien $S \subseteq V$ und $T \subseteq V^*$ Teilmengen. Definiere $Am(S) = \{\xi \in V^* | \xi(v) = 0 : \forall v \in S\}; Null(T) := \{v \in V | \xi(v) = 0 : \forall \xi \in T\}$ als $\underline{Annulator}$ von S bzw. $\underline{Nullraum}$ von T.

$\underline{Bsp:}$ $U := L(\{\begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\0\end{pmatrix}\}) \subseteq V_3(K) \Rightarrow Ann(U) = L(\{\begin{pmatrix}1 & 1 & 1\end{pmatrix}\}) \subseteq Z_3(K)$. Sei $\xi = (\begin{pmatrix}\lambda_1 & \lambda_2 & \lambda_3\end{pmatrix})$, benötigen $\xi \cdot \begin{pmatrix}1\\0\\-1\end{pmatrix} = 0$ und $\xi \cdot \begin{pmatrix}1\\-1\\0\end{pmatrix} = 0$

$\underline{Lemma\, 8.7:}$ (Ü) a) $Ann(S) \subseteq V^*$ und $Null(T) \subseteq V$ sind UVR'e.
b) $S' \subseteq S \subseteq V \Rightarrow Ann(S') \supseteq Ann(S)$, analog für $T' \subseteq T \subseteq V^* : Null(T') \supseteq Null(T)$
c) $Ann(S) = Ann(L(S))$ und $Null(T) = Null(L(T))$

$\underline{Beweis:}$ $\underline{z.B.:}$ a) Teil 2: $\underline{Behauptung:}$ $Null(T)$ ist UVR von V.
i) $0 \in Null(T)$, denn $\xi(0) = 0\, \forall \xi \in V^*$
ii) Seien $v, w \in Null(T)$ und $\lambda \in K$. Sei $\xi \in T$ beliebig. $\underline{Dann\, gilt:}$ $\xi(\lambda \cdot v + w) = \lambda \cdot \xi(v) + \xi(w) = 0 + 0 \Rightarrow (\lambda \cdot v + w) \in Null(T)$ $\square$

Sei $X \subseteq V^*$. Gelte $dimV < \infty$. Wir haben: $\begin{matrix} V & \supseteq & Null(X) \\ b_V \downarrow & & \\ V^{**} & \supseteq & Ann(X) \end{matrix}$ dann gilt: $X \subseteq V^*$.

$\underline{Lemma\, 8.8:}$ Gelte $dimV < \infty$. Sei $X \subseteq V^*$. Dann gilt: a) $b_V(Null(X)) = Ann(X)$
b) $b_V|_{Null(X)} : Null(X) \to Ann(X)$ ist Isom.

$\underline{Beweis:}$ a): $Ann(X) = \{w \in V^{**} | w(\xi) = 0\, \forall \xi \in X\}$. ($b_V : V \to V^{**}$ ist Isom., also bijektiv)$\Rightarrow w = b_V(v)$ für eindeutiges $v \in V$)$\Rightarrow Ann(X) = \{b_V(v) | v \in V, (b_V(v))(\xi) = 0\, \forall \xi \in X\} = \{b_V(v) | v \in V, \xi(v) = 0\, \forall \xi \in X\} = b_V(\{v \in V | \xi(v) = 0\, \forall \xi \in X\})$
b) Abbildung surjektiv nach a). Abbildung ist Einschränkung der injektiven Abbildung b_V, also injektiv. $\square$

$\underline{Satz\, 8.9 \text{ (Dimensionsformeln für Nullraum und Annulator)}:}$ Gelte $dimV < \infty$. Seien $U \subseteq V$ und $X \subseteq V^*$ UVR'e. Dann gilt:
a) $dimU + dimAnn(U) = dimV$
b) $dimX + dim(Null(X)) = dimV (= dimV^*)$
c) $Null(Ann(U)) = U$
d) $Ann(Null(X)) = X$

Beweis : a) Sei $\underline{B} = (b_1, ..., b_n)$ geordnete Basis von V, so dass $S = \{b_1, ..., b_m\}$ eine Basis von U (Basis-Ergänzungssatz). Sei $\underline{B}^* = (b_1^*, ..., b_n^*)$ die Dualbasis zu $\underline{B}$ (von V^*).
Behauptung : $T = \{b_{m+1}^*, ..., b_n^*\}$ ist Basis von $Ann(U)$:
1.Schritt: $Ann(U) = Ann(S)$, denn 8.7c): $Ann(S) = Ann(L(S))$
2.Schritt: Schreibe $\xi \in V^*$ als $\xi = \sum_{j=1}^{n} \mu_j \cdot b_j^*$

$\xi \in Ann(U) = Ann(S) \Leftrightarrow \forall i = 1...m : \xi(b_i) = 0 \Leftrightarrow \forall i = 1...m : 0 = \sum_{i=1}^{n} \mu_j \cdot b_j^*(b_i) = \mu_i \Leftrightarrow \mu_1 = \cdots == \mu_m = 0 \Leftrightarrow \xi \in L(\{b_{m+1}^*, b_n^*\})$. D.h. T ist ES von $Ann(U)$. T ist l.u., denn T ist Teilmenge der Basis $b_1^*, ..., b_n^*$
Beh. $\Rightarrow dimU + dimAnn(U) = |S| + |T| = m + (n - m) = n = dimV$
b) aus a) folgt: $dimX + dimAnn(X) = dimV^* = dimV$
c) Wie in a) zeigt man: $\{b_{m+1}^*, ..., b_n^*\}$ ist Basis von $Ann(U) \Rightarrow \{b_1, ..., b_m\}$ ist Basis von $Null(Ann(U))$ □

8.1 Die duale Abbildung

Sei $f : V \to W$ eine lineare Abbildung. Ist $\xi : W \to K$ ein lineares Funktional, so auch $\xi \circ f : V \to K$.

Lemma 8.10 : $f^* : W^* \to V^*, \xi \mapsto f^*(\xi) := \xi \circ f$ ist lineare Abbildung.

Beweis : zz: $\forall \lambda \in K, \forall \xi, \eta \in W^* : f^*(\lambda \cdot \xi + n) \overset{!}{=} \lambda \cdot f^*(\xi) + f^*(\eta)$ linke Seite$= f^*(\lambda \cdot \xi + \eta) = (\lambda \cdot \xi + \eta) \circ f \overset{7.4}{=} \lambda \cdot (\xi \circ f) + \eta \circ f$ =rechte Seite. □

"Visualisierung" :
$$\begin{array}{ll} W & \\ \downarrow \xi & \overset{f^*}{\mapsto} f^*(\xi) = \xi \circ f \\ K & \end{array}$$

Definition 8.11 : f^* heißt die zu f *duale Abbildung*.

Lemma 8.12 : Für $f \in Lin(V, W)$ und $g \in Lin(W, X)$ gilt $(g \circ f)^* = f^* \circ g^*$

Beweis : Sei $\xi \in X^*$. Dann gilt: $(g \circ f)^*(\xi) \overset{Def.}{=} \xi \circ (g \circ f) = (\xi \circ g) \circ f \overset{Def.}{=} f^*(\xi \circ g) \overset{Def.}{=} f^*(g^*(\xi)) = (f^* \circ g^*)(\xi)$ □

Darstellungsmatrix von f^* : *Definition 8.13 :* Sei $A = (a_{ij})_{j=1...m}^{i=1...m} \in M_{mxn}(K)$. Definiere $\tilde{a}_{ij} = a_{ji}$ für $substacki = 1...mj = 1...n$. Dann heißt $A^t := (\tilde{a}_{ij})_{j=1...n}^{i=1...m}$ die zu A *transponierte Matrix*

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

Lemma 8.14 : Seien $\underline{B} = (b_1, ..., b_n)$ bzw. $\underline{C} = (c_1, ..., c_m)$ geordnete Basen von V bzw. W mit Dualbasen $\underline{B}^*$ von V^* und $\underline{C}^*$ von W^*. Dann gilt für $f \in Lin(V, W) : \tilde{A} = Mat_{\underline{C}^*}^{\underline{B}^*}(f^*) = (Mat_{\underline{B}}^{\underline{C}}(f))^t = A^t$

Beweis : $A = (a_{ij}{}_{j=1...n}^{i=1...m}$ erfülllt: $f(b_j) = \sum_{k=1}^{m} a_{kj} \cdot c_k$ für $j = 1...n.\tilde{A} = (\tilde{a}_{ij})_{j=1...m}^{i=1...n}$ erfüllt: $f^*(c_i^*) = \sum_{k=1}^{n} \tilde{a}_{ki} \cdot b_k^*$ für $i = 1...m$. Wende c_i^* an: $c_i^*(f(b_j)) = \sum_{k=1}^{m} a_{kj} \cdot c_i^*(c_k) = a_{ij} + 0 + ... + 0$. Wende $f^*(c_i^*)$ auf b_j an: $f^*(c_i^*))(b_j) = c_i^*(f(b_j))$ □

Korollar 8.15 : Für $A \in M_{mxn}(K)$ und $B \in M_{exm}(K)$ gilt: $(B \cdot A)^t = A^t \cdot B^t$

Beweis : 1. Möglichkeit: Matrixeinträge vergleichen (Indexschlacht)
2. Sei $\underline{E}$ die Standardbasis von $V_?(K)$ für $? \in \{l, m, n\}$. Sei $l_A : V_n(K) \to V_m(K), v \mapsto A \cdot v$ und $l_B : V_m(K) \to V_l(K), w \mapsto B \cdot w$. Dann gilt: $A = Mat^{m}_{\underline{E}_n}(l_A)$. $B = Mat^{\underline{E}_n}_{\underline{E}_m}(l_B)$, $B \cdot A = Mat^{\underline{E}_l}_{\underline{E}_n}(l_B \circ l_A) \Rightarrow$ $(B \cdot A)^t = (Mat^{\underline{E}_l}_{\underline{E}_n}(l_B \circ l_A))^t = Mat^{\underline{E}^*_n}_{\underline{E}^*_l}((l_B \circ l_A)^*) \overset{8.10}{=} Mat^{\underline{E}^*_n}_{\underline{E}^*_l}(l^*_A \circ l^*_B) \overset{7.9}{=} Mat^{\underline{E}^*_m}_{\underline{E}^*_m}(l^*_B \overset{8.10}{=} A^t \cdot B^t$ □

Satz 8.16 : Für endlich-dimensionale VR'e V, W und $f \in Lin(V, W)$ gelten: a) $Bild(F) = Null(Kern(f^*))$
b) $Bild(^* = Ann(Kern(f))$
c) $dimBild(f) = dimBild(f^*)$

Vorbereitung :Lemma 8.17 : Unter den Voraussetzungen von 8.16 sei: $f^* : W^* \to V^*$ dual zu f und $f^{**} : V^{**} \to W^{**}$ dual zu f^*.

Dann gelten: a) Im Diagramm $\begin{array}{ccc} V & \overset{f}{\to} & W \\ b_V \downarrow & & \downarrow b_W \\ V^{**} & \overset{f^{**}}{\to} & W^{**} \end{array}$ gilt $b_W \circ f = f^{**} \circ b_V$

b) (Ü) Für $Kern(f) \subseteq V$ und $Kern(f^{**}) \subseteq V^{**}$ gilt: $b_V|_{Kern(f)} : Kern(f) \to Kern(f^{**})$ ist ein Isom.
c) (Ü) Analog ist $b_W|_{Bild(f)} : Bild(f) \to Bild(f^{**})$ ein Isom.

Beweis : a) zz: $\forall \xi \in W^* : \forall v \in V : ((b_W \circ f)(v))(\xi) \overset{!}{=} ((f^{**} \circ b_V)(v))(\xi)$. linke Seite= $(b_W(f(v))(\xi) \overset{Def.}{=} \xi(f(v))$. rechte Seite= $(f^{**}(b_V(v))(\xi) = (b_V(v) \circ f^*)(\xi) = b_V(v)(f^*(\xi)) = (f^*(\xi))(v) = (\xi \circ f)(v) = \xi(f(v))$ □

Beweis zu 8.16 : a) " $\subseteq$ " : Sei $f(v) \in Bild(f)$, d.h. $v \in V$, zz: $f(v) \in Null(Kern(f^*))$, also zz: $\forall \xi \in Kern(f^*) : \xi(f(v)) = 0!$, aber: $\xi(f(v)) = (\xi \circ f)(v) = (f^*(\xi))(v) \overset{\xi \in Kern(f^*}{=} 0(v) = 0$
c) " $\leq$ ": $dimBild(f) \leq dimNull(Kern(f^*)) \overset{Satz\,8.9:}{=} dimV^* - dimKern(f^*) \overset{Satz\,6.23:}{d} imBild(f^*)$
b) " $\subseteq$ ": Analog zu a).
c) " $\leq$ " folgt: $dimBild(f) = dim(Null(Kern(f))) \overset{a)\subseteq}{\Rightarrow} Bild(f) = Null(Kern(f^*))$ (da " $\subseteq$ " bekannt).
b) " $\supseteq$ ": wie a) " $\supseteq$ ". □

Definition 8.18 : Für $f \in Lin(V, W)$, definiere den Rang von f als $Rang(f) := dimBild(f)$

Bemerkung : Für $f \in Lin(V_n(K), V_m(K))$ mit $A = Mat(f)$ gilt $Rang(f)$ =Spaltenrang(A), denn der Spaltenraum von $A = L(\{A \cdot e_1, ..., A \cdot e_n\}) = L(\{f(e_1), ..., f(e_n)\}) = f(L(\{e_1, ..., e_n\})) = f(V_n(K)) = Bild(f)$ □

Korollar 8.19 : Für $A \in M_{mxn}(K)$ gilt Spaltenrang(A)=Zeilenrang(A). (in Zukunft schreiben wir nur noch Rang$A$).

Beweis : Spaltenrang$(A) \overset{Bem.}{=}$ Rang$(l_A) = dimBild(l_A) \overset{8.18}{=} dimBild(l^*_a)$ =Spaltenrang(A^t) =Zeilenrang(A) □

9 Lineare Gleichungssysteme

<u>*Definition* 9.1 :</u> Ein <u>*Lineares Gleichungssystem*</u> (LGS) in m Gleichungen und n Variablen $x_1, ..., x_n$ (über K) ist ein Schema: $\begin{matrix} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{matrix} = \circledast$ mit $b_i, a_{ij} \in K$ für $i = 1...m, j = 1...n$. Das LGS heißt <u>*homogen*</u> $\Leftrightarrow b_1 = \cdots = b_m = 0$, sonst <u>*inhomogen*</u>. Der <u>*Lösungsraum*</u> von $\circledast$ ist $\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in V_n(K) |$ die Gleichungen $\circledast$ sind erfüllt für $x_1, ..., x_n\}$.

sei $A = (a_{ij})_{j=1...n}^{i=1...m} \in M_{mxn}(K)$, sei $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in V_m(K)$. Dann gilt: $\circledast$ ist äquivalent zu $A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = b$

<u>*Definition* 9.2 :</u> $\mathbb{L}(A, b) = \{x \in V_n(K) | A \cdot x = b\}$ heißt <u>*Lösungsraum*</u> von $\circledast$. Sei $l_A : V_n(K) \to V_m(K), v \mapsto A \cdot v$ und seien $z_1, ..., z_m \in Z_n(K)$ die Zeilen von A ($z_i = i$-te Zeile)

<u>*Satz* 9.3 :</u> a) Ist $\circledast$ homogen, so gelten: $\mathbb{L}(A, 0) \stackrel{i)}{=} Kern(l_A) \stackrel{ii)}{=} Null(\{z_1, ..., z_m\})$
iii) $dim\mathbb{L}(A, 0) = n - Rang(A) = n - dimL(\{z_1, ..., z_n\})$
b) Sei $\circledast$ beliebig (im Allgemeinen homogen). Dann gelten:
i) $\circledast$ hat Lösung $\Leftrightarrow Rang(A) = Rang(A|b)$
ii) Ist $x_0 \in \mathbb{L}(A, b)$, so gilt $\mathbb{L}(A, b) = \{x + x_0 | x \in \mathbb{L}(A, 0)\}$

<u>*Notation* :</u> Wir schreiben $A|b$ für die um die Spalte b verlängerte Matrix A.

<u>*Beweis* :</u> a) i) $\mathbb{L}(A, 0) = \{x \in V_n(K) | A \cdot x = 0\} = Kern(l_A)$
ii) Definition von $Null(\{z_1, ..., z_n\}) = \{v \in V_n(K) | z_i \cdot v = 0$ für $i = 1...m\}$
iii) $dim\mathbb{L}(A, 0) \stackrel{i)}{=} dimKern(l_A) = dimV_n(K) - dimBild(l_A) = n - Rang(A)$. $Null(\{z_1, ..., z_n\}) = Null(L(\{z_1, ..., z_n\})$.
Nun Dimensionsformel für Nullraum.
b) i) $\circledast$ hat Lösung $\Leftrightarrow \exists x_1, ..., x_n \in K$ mit $x_1a_1 + ... + x_na_n = b$ für $a_1...a_n$ die Spalten von $A \Leftrightarrow b \in L(\{a_1, ..., a_n\})$ =Spaltenraum(A)$\Leftrightarrow$Spaltenraum($A|b$) =Spaltenraum(A) $\Leftrightarrow$ Rang($A|b$)=Rang(A)
iii) zz: $x \in \mathbb{L}(A, 0) \Leftrightarrow x + x_0 \in \mathbb{L}(A, b)$
"$\Rightarrow$" $A \cdot (x + x_0) = A \cdot x + A \cdot x_0 = A \cdot x + b = b$ falls $x \in \mathbb{L}(A, 0)$
"$\Leftarrow$" $A \cdot x = A \cdot (x + x_0 - x_0) = A \cdot (x + x_0) - A \cdot x_0 = b - b = 0$, falls $x + x_0 \in \mathbb{L}(A, b)$ $\square$

<u>*Korollar* 9.4 :</u> Falls $RangA = n$. Dann gelten:
i) $\mathbb{L}(A, 0) = \{0\} (\subseteq V_n(K))$ und $|\mathbb{L}(A, b)| \leq 1 \; \forall b \in V_m(K)$
ii) Falls zusätzlich $m = n$, so gilt: $|\mathbb{L}(A, b)| = 1 \; \forall b \in V_n(K) = V_m(K)$

<u>*Beweis* :</u> i) Folgt aus $dim\mathbb{L}(A, 0) = n - RangA = n - n = 0$ und 9.3b) für $\mathbb{L}(A, b)$
ii) Falls $m = n$: $n = Spaltenrang(A) \leq Spaltenrang(A|b) \leq n = Spaltenrang(A)$ $\square$

<u>*Lemma* 9.5 :</u> (Ü) a) Für $C \in GL_m(K)$ gilt: $\mathbb{L}(C \cdot A, C \cdot b) = \mathbb{L}(A, b)$
b) Elementare Zeilentransformationen angewandt auf A (oder $A|b$) lassen sich durch Linksmultiplikation $C \cdot A$ (oder $C \cdot (A|b)$) für elementare Matrizen in $GL_n(K)$ beschreiben.

<u>*Bsp* :</u> $K = \mathbb{R}$

$$\begin{matrix} x_1 & & +x_3 & =2 & & =4 \\ 3x_1 & +4x_2 & +7x_3 & =0 & oder & =10 \end{matrix} \rightsquigarrow A = \begin{pmatrix} 1 & 0 & 1 \\ 3 & 4 & 7 \\ 2 & 4 & 6 \end{pmatrix}, b_1 = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, b_2 = \begin{pmatrix} 4 \\ 10 \\ 8 \end{pmatrix}$$
$$\begin{matrix} 2x_1 & +4x_2 & +6x_3 & =0 & & =6 \end{matrix}$$

$$(A|b_1|b_2) = \begin{pmatrix} 1 & 0 & 1 & | & 2 & | & 4 \\ 3 & 4 & 7 & | & 0 & | & 10 \\ 2 & 4 & 6 & | & 0 & | & 6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 1 & | & 2 & | & 4 \\ 0 & 4 & 4 & | & -6 & | & -2 \\ 0 & 4 & 4 & | & -4 & | & -2 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 1 & | & 2 & | & 4 \\ 0 & 4 & 4 & | & -6 & | & -2 \\ 0 & 0 & 0 & | & 2 & | & 0 \end{pmatrix}$$

I $Rang(A|b_1) = 3 \geq Rang(A) \Rightarrow \mathbb{L}(A, b_1) = \emptyset$

II $Rang(A|b_2) = 2 = Rang(A) \Rightarrow \mathbb{L}(A, b_2) \neq \emptyset$

$\Rightarrow$ Lösung finden in II: $\begin{pmatrix} 1 & 0 & 1 & | & 4 \\ 0 & 1 & 1 & | & -\frac{1}{2} \end{pmatrix}$ eine Lösung $\begin{pmatrix} 4 \\ -\frac{1}{2} \\ 0 \end{pmatrix} = x_0; \mathbb{L}(-\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}) = L(\{\begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}\})$

$\Rightarrow \mathbb{L}(A, b_2) = \{\begin{pmatrix} 4 \\ -\frac{1}{2} \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}\}\lambda \in \mathbb{R}$

<u>*Lemma* 9.6 :</u> Gelte $Rang(A) = n$ für $A \in M_{nxn}(K)$. Ist $(1_n|B)$ die reduzierte ZSF aus dem Gauß-Algorithmus zu $(A|1_n)$, so gilt $B = A^{-1}$

<u>*Beweis* :</u> i) $Rang(A) = n \Rightarrow$ red. ZSF zu A aus Gauß-Algorithmus ist $1_n \rightarrow$ wende Gauß auf $(A|1_n)$ an: erhalte red. ZSF der Form $(1_n|B)$

ii) Nach 9.5 $\exists C \in GL_n(K)$ mit $C(A|1_n)) = (1_n|B) \Rightarrow C \cdot A = 1_n$ und $C \cdot 1_n = B$, d.h. $B \cdot A = 1_n \overset{A\ quadratisch}{\Rightarrow} B = A^{-1}$

alternativ: $(A|1_n)$ codiert das simultane LGS $A \cdot x_1 = e_1, ..., A \cdot x_n = e_n \Rightarrow (x_1, ..., x_n) = A^{-1}$ $\square$

<u>*Nachtrag* :</u> Sei $C \in M_{nxn}(K)$. Dann gilt: C invertierbar $\Leftrightarrow C^t$ invertierbar. Beweis 1. Lösung: C invertierbar $\Leftrightarrow Spaltenrang(C) = n \Leftrightarrow Zeilenrang(C^t) = n \Leftrightarrow (C^t)$

2. Lösung: C invertierbar $\Leftrightarrow D \in M_{nxn}(K)$ mit $C \cdot D = 1_n \Rightarrow D^t \cdot C^t = (C \cdot D)^t = 1_n \Rightarrow C^t$ invertierbar.

Man kann auch elementare <u>$Spaltentransformationen$</u> definieren:

E1') Vertausche 2 Spalten

E2') Addiere Vielfaches einer Spalte zu einer anderen.

E3') Multiplikation einer Spalte mit Skalar $\lambda \neq 0$

$\rightarrow$ damit kann man reduzierte Spaltenstufenform von Matrizen erhalten. (red.SSF)

<u>*Lemma* 9.5 :</u> Elementare Spaltentransformationen lassen sich durch Rechtsmultiplikation mit invertierbaren Matrizen beschreiben.

Warnung: Spaltenoperationen änderen die Lösungsräume LGS!

<u>*Definition* 9.7(Ähnlichkeit und Äquivalenz) :</u> a) $A, A' \in M_{mxn}(K)$ heißen äquivalent. (schreibe $A \sim A'$):$\Leftrightarrow$ <u>$\exists B \in GL_n(K), C \in GL_m(K)$ mit $A' = C \cdot A \cdot B$</u>

b) $A, A' \in M_{nxn}(K)$ heißen <u>*ähnlich*</u>(schreibe $A \approx A'$) $\Leftrightarrow \exists B \in GL_n(K)$ mit $A' = B^{-1} \cdot A \cdot B$

<u>*Übung* :</u> Ähnlichkeit definiert eine Äquivalenzrelation auf $M_{nxn}(K)$ und Äquivalenz definiert eine Äquivalenzrelation auf $M_{mxn}(K)$

Satz 9.8 : Seien $A, A' \in M_{mxn}(K)$. Dann gelten: a) $A \sim \begin{pmatrix} 1_r & \vdots & 0 \\ \dots & \dots & \dots \\ 0 & \vdots & 0 \end{pmatrix} \in M_{mxn}(K)$ für $r = Rang(A)$

b) $A \sim A' \Leftrightarrow Rang(A) = Rang(A')$

Beweis : a) Äquivalenz bleibt erhalten unter elementaren Zeilen- und Spaltentransformationen (Lemma 9.5,9.5'). $A \overset{Gauss}{\rightsquigarrow} A'' = \begin{pmatrix} 0 & \dots & 0 & 1 & X & \dots & \dots & \dots & X \\ 0 & \dots & \dots & 0 & 1 & X & \dots & \dots & X \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & 0 & 1 & X & \dots & X \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$

$\overset{E1'-E3'}{\rightsquigarrow} \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & 1 & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \end{pmatrix} \overset{E1'}{\rightsquigarrow} \left(\begin{array}{c|c} \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} & 0 \\ \hline 0 & 0 \end{array}\right) = A'''$. Damit wurde $A \sim A''$ gezeigt.

b) " $\Leftarrow$ " folgt aus a). " $\Rightarrow$ " Ü.

$Rang(C \cdot A) = Rang(A) = Rang(A \cdot B)$ für B, C invertierbar, d.h. in Äquivalenzklassen ist der Rang konstant.

Korollar 9.9 : Jede Matrix aus $GL_n(K)$, d.h. jede Matrix in $M_{nxn}(K)$ mit $Rang = n$ ist ein Produkt von Elementarmatrizen.

Proposition 9.10 (Interpretation von Ähnlichkeit und Äquivalenz) : Seien V, W VR'e (über K) mit geordneten Basen $\underline{B} = (b_1, ..., b_n)$ bzw. $\underline{C} = (c_1, ..., c_m)$. Dann gilt:

a) Sei $f \in Lin(V, W)$ und $A = Mat_{\underline{B}}^{\underline{C}}(f) \in M_{mxn}(K)$. Dann gilt: $A' \sim A$ (für $A' \in M_{mxn}(K)$) $\Leftrightarrow \exists$Basen $\underline{B}', \underline{C}'$ von V bzw. W: $A' = Mat_{\underline{B}'}^{\underline{C}'}(f)$

b) Sei $f \in End(V)$ und sei $A = Mat_{\underline{B}}^{\underline{B}}(f) \in M_{nxn}(K)$. $A' \approx A$ (für $A' \in M_{nxn}(K)$) $\Leftrightarrow \exists$ Basen $\underline{B}'$ von V mit $A' = Mat_{\underline{B}'}^{\underline{B}'}(f)$.

Bemerkung : Normalformen unter Ähnlichkeit sind nicht so leicht zu erhalten, siehe dann in LA2: über $\mathbb{C}$: Jordanform zu A. Für "einfache"A: erhalte "einfache "Normalfform $A \approx \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$, $d_i \in K$ für $\underline{B}'$ Basis aus "Eigenvektoren ".

Beweis zu 9.10 : Verkettungsformel: $Mat_{\underline{B}'}^{\underline{C}'}(f) = Mat_{\underline{C}}^{\underline{C}'}(id_W) \cdot Mat_{\underline{B}}^{\underline{C}}(f) \cdot Mat_{\underline{B}'}^{\underline{B}}(id_V)$

a) " $\Leftarrow$ ": Basiswechselmatrizen sind invertierbare Matrizen!

" $\Rightarrow$ ": Jede invertierbare Matrix definiert Basiswechselmatrix, z.B.: Sei $D \in GL_m(K)$, definiere $\underline{C} := \underline{C} \cdot D^{-1} \Rightarrow \underline{C} = \underline{C}' \cdot D$ und daher $Mat_{\underline{C}}^{\underline{C}'}(id_V) = D$

c) Spezialfall von Beweis von a) für $W = V, \underline{C}" = \underline{B}"$ und $"\underline{C}' = "\underline{B}'$, denn: $(Mat_{\underline{B}'}^{\underline{B}}(id_V))^{-1} = Mat_{\underline{B}}^{\underline{B}'}(id_V)$
□

weitere Anwendungen des Gauß-Algorithmus :

Finde Basis zu i) $X = L(\{z_1, ..., z_m\}) \subseteq Z_n(K)$ zu gegebenen $z_1, ..., z_m \in Z_n(K)$

ii) $U = L(\{v_1, ..., v_n\}) \subseteq V_m(K)$ zu gegebenen $v_1, ..., v_n \in V_m(K)$

iii) $Kern(l_A)$ zu $l_A : V_n(K) \to V_m(K), v \mapsto A \cdot v; A \in M_{mxn}(K)$
iv) $Bild(l_A)$ zu $l_A : V_n(K) \to V_m(K), v \mapsto A \cdot v; A \in M_{mxn}(K)$
v) $U + W$ für $W = L(\{w_1, ..., w_s\}) \subseteq V_n(K), U$ wie oben, $w_j \in V_n(K)$
vi) $Null(X) \subseteq V_n(K)$
vii) $Ann(U) \subseteq Z_m(K)$
viii) $U \cap W \subseteq V_n(K)$
Nochmals zu i): Sei $\tilde{A}$ die red. ZSF zu $A = (v_1| \dots |v_n) \in M_{nxn}(K)$. Seien $1 \leq j_1 < j_2 < \cdots < j_r \leq n$ die Indizes der Pivotspalten von $\tilde{A}$. $\Rightarrow \{v_{j_1}, v_{j_2}, ..., v_{j_r}\}$ ist Basis von $U = Spaltenraum(A)$.

10 Determinanten

$\underline{Definition\,10.1:}$ Seien V, W K-VR'e, $n \in \mathbb{N}$. a) $f : V^n = V \times \cdots \times V \to W$ heißt $\underline{n-linear}$ $:\Leftrightarrow f$ ist in jedem Argument linear $:\Leftrightarrow \forall j = 1...n \forall (v_1, ..., v_{n-1}) \in V^{n-1}$ ist die Abbildung $V \to W, v \mapsto f(v_1, ..., v_{j-1}, v, v_j, ..., v_{n-1})$ linear.
b) Eine n-lineare Abbildung $f : V^n \to W$ heißt $\underline{n-linearform}$ $:\Leftrightarrow W = K$
c) Ist $f : V^n \to W$ n-linear, so heißt f $\underline{alternierend}$ $:\Leftrightarrow \forall (v_1, ..., v_n) \in V$ gilt: $v_i = v_j$ für ein Paar $1 \leq i < j \leq n$, so dass $f(v_1, ..., v_n) = 0$
d) $Lin_n(V, W)$ sei die Menge aller n-linearen Abbildungen $f : V^n \to W$
e) $Alt_n(V, W)$ sei die Menge aller alternierenden Abbildungen $f : V^n \to W$

$\underline{Lemma\,10.2:}$ (Ü) $Alt(V, W) \subseteq Lin_n(V, W)$ sind UVR'e von $Abb(V^n, W)$
$\underline{Motivation:}$ Sei $V = \mathbb{R}^n$ zu $(v_1, ..., v_n) \in V^n$. Sei $PE(v_1, ..., v_n) = \{\sum\limits_{i=1}^{n} \lambda_i \cdot v_i | 0 \leq \lambda_i \leq 1 \forall i = 1...n\}$ das zugeörige Parallelepided ($n = 3$ Spat, $n = 2$ Parallelogramm)

$\underline{gesucht:}$ a) Eine Abbildung $D_{\underline{E}} : V^n \to \mathbb{R}$ mit $D_{\underline{E}}(v_1, ..., v_n) =$"orientiertes"Volumen von $PE(v_1, ..., v_n)$
b) Eine Abbildung $det : End_{\mathbb{R}}(\mathbb{R}^n) \to \mathbb{R}$, so dass für jede $\mathbb{R}$-lineare Abbildung $f : \mathbb{R}^n \to \mathbb{R}^n$ der Wert $det(f)$ die Volumenänderung unter f misst, d.h. $D_{\underline{E}}(f(v_1), ..., f(v_n)) = det(f) \cdot D_{\underline{E}}(v_1, ..., v_n) = \pm$Volumen$(PE(f(v_1), ..., f(v_n)) \; \forall (v_1, ..., v_n) \in V^n$

Eigenschaften von $D_{\underline{E}} : (n-2)$ i) $D_{\underline{E}}(\lambda \cdot v_1, v_2) = \lambda \cdot D_{\underline{E}}(v_1, v_2) = D_{\underline{E}}(v_1, \lambda \cdot v_2)$
ii) $D_{\underline{E}}(v_1 + w_1, v_2) = D_{\underline{E}}(v_1, v_2) + D_{\underline{E}}(w_1, v_2)$ analog im 2. Argument.
iii) $D_{\underline{E}}(v, v) = 0$. Allgemeines n: $D_{\underline{E}} \in Alt_n(\mathbb{R}^n, \mathbb{R})$

$\underline{Wiederholung:}$ K ein Körper. $\underline{Charakteristik}$ von K ist $Char(K) := min\{n \in \mathbb{N} | 1_K + ... + 1_K = 0_K\}$, wobei: $min\emptyset := 0$
In Ü: $Char(K) \neq 0 \Rightarrow Char(K)$ ist Primzahl!

$\underline{Lemma\,10.3:}$ Seien V, W K-VR'e und $f \in Lin_n(V, W)$ a) $f \in Alt_n(V, W) \Rightarrow \circledast \forall \sigma \in S_n : \forall (v_1, ..., v_n) \in V^n :$ $f(v_{\sigma(1)}, ..., v_{\sigma(n)}) = sgn(\sigma) \cdot f(v_1, ..., v_n)$
b) Falls $Char(K) \neq 2$, so gilt $Alt_n(V, W) = \{f \in Lin_n(V, W) | f$ erfüllt $\circledast\}$

$\underline{Beweis:}$ a) Ü: Es genügt $\circledast$ für Nachbartranspositionen zu zeigen. (S_n wird erzeugt durch Nachbartranspositionen). Sei also $\sigma = \tau_{(i,i+1)}$ für $i \in \{1, ..., n-1\}$ $\underline{zz:}$$f(v_1, ..., v_{i-1}, v_{i+1}, v_i, v_{i+2}, ..., v_n) = (-1) \cdot f(v_1, ..., v_{i-1}, v_i, v_{i+1}, ..., v_n)$. Fixiere $v_1, ..., v_{i-1}, v_{i+2}, ..., v_n$. Setze $g(v, w) = f(v_1, ..., v_{i-1}, v, w, v_{i+2}, ..., v_n)$.
g 2-linear (bilinear), da f n-linear. g ist alternierend, d.h. $\forall v \in V : g(v, v) = 0$, denn f ist alternierend.
$\underline{zz:}$$g(v, w) = -g(w, v) :=^{g\,altern.} g(v + w, v + w) \overset{g\,2-lin.}{=} g(v, v + w) + g(w, v + w) \overset{g\,2-lin.}{=} g(v, v) + g(v, w) + g(w, v) + g(w, w) \overset{g\,altern.}{=} g(v, w) + g(w, v) = 0 \Rightarrow -g(w, v) = g(v, w)$ $\square$
b) Sei $(v_1, ..., v_n) \in V^n$ mit $v_i = v_j$ und $1 \leq i < j \leq n$. f erfüllt $\circledast$.
$\underline{zz:}$ $Char(K) \neq 2 \Rightarrow f(v_1, ..., v_n) = 0$
Dazu: Sei $\sigma = \tau_{(i,j)} : f(v_1, ..., v_n) = f_{\sigma(1)}, ..., v_{\sigma(n)}) = sgn(\tau_{(i,j)}) \cdot f(v_1, ..., v_n) \Rightarrow 2 \cdot f(v_1, ..., v_n) = 0 \overset{Char(k)\neq 2}{\Rightarrow}$ $f(v_1, ..., v_n) = 0$ $\square$

$\underline{Lemma\,10.4:}$ Sei $\underline{B} = (b_1, ..., b_n)$ Basis von V, für $(v_1, ..., v_n) \in V^n$. Schreibe $v_i = \sum\limits_{i=1}^{n} \lambda_{ij} b_j$ für eindeutige $\lambda_{ij} \in K$. Dann gilt:
a) Für $f ß Lin_n(V, W)$ gilt: $f(v_1, ..., v_n) = \sum\limits_{j_1=1}^{n} \sum\limits_{j_2=1}^{n} ... \sum\limits_{j_n=1}^{n} \lambda_{1_{j1}} \lambda_{2_{j2}} ... \lambda_{n_{jn}} f(b_{j1}, ..., b_{jn})$
b) Für $f \in Alt_n(V, W)$ gilt: $f(v_1, ..., v_n) = \sum\limits_{\sigma \in S_n} \lambda_1 \sigma(1) .... \lambda_n \sigma(n) \cdot sgn(\sigma) f(b_1, ..., b_n)$

Beweis : a) Verwende n-Linearität in allen Argumenten, z.B.: $f(v_1, ..., v_{i-1}, \sum\limits_{j=1}^{n} \lambda_i j_i f(v_1, ..., v_{i-1}, b_j, v_{i+1}, ..., v_n)$
b) f alternierend $\Rightarrow f(b_{j1}, ..., b_{jn}) = 0$, falls $j_1, ..., j_n$ nicht paarweise verschieden sind! Falls $j_1, ..., j_n$ paarweise verschieden $\Rightarrow \{1, ..., n\} \to \{1, ..., n\}$ ist Permutation und erhalten so alle Permutationen in S_n genau 1-mal! Schreibe $j_1 = \sigma(1), ..., j_n = \sigma(n)$ für $\sigma \in S_n \Rightarrow f(v_1, ..., v_n) = \sum\limits_{\sigma \in S_n} \lambda_1 \sigma(1) \lambda_2 \sigma(2) ... \lambda_n \sigma(n) f(b_{\sigma(1)}, ..., b_{\sigma(n)}) = sgn(\sigma) f(b_1, ..., b_n)$ □

Lemma 10.4$\frac{1}{2}$: Sei $A_n := Kern(sgn : S_n \to \{\pm 1\}$ und sei $\tau \in S_n$ eine Transposition und $n \geq 2$. Dann (Ü!):
i) $A_n \to A_n \cdot \tau, \sigma \mapsto \sigma \cdot \tau$ ist bijektiv.
ii) $S_n = A_n \dot\cup A_n \cdot \tau$
iii) $|S_n| = n!, |A_n| = \frac{1}{2} n!$

Korollar 10.5 : Sei $\underline{B} = (b_1, ..., b_n)$ Basis von V. Für $(v_1, ..., v_n) \in V^n$ definiere $(\lambda_{ij}) \in M_{nxn}(K)$ durch $\sum\limits_{j=1}^{n} \lambda_{ij} \cdot b_j = v_i$. Dann:
a) $D_{\underline{B}} : V^n \to K, (v_1, ..., v_n) \mapsto \sum\limits_{\sigma \in S_n} sgn(\sigma) \lambda_{1\sigma(1)} ... \lambda_{n\sigma(n)}$ liegt in $Alt_n(V, K)$
b) $D_{\underline{B}}$ ist Basis des K-VR $Alt_n(V, K)$ und $D_{\underline{B}}(b_1, ..., b_n) = 1 \rightsquigarrow$ Lösung der 1. Frage der Motivation zu Kapitel 10.

Korollar 10.6 : $d \in Alt_n(V, K) \setminus \{0\}$, und $n = dim V, (b_1, ..., b_n) \in V^n$. Dann gilt: $(b_1, ..., b_n)$ ist Basis von $V \Leftrightarrow d(b_1, ..., b_n) \neq 0$

Beweis : " $\Rightarrow$ " : Sei $(b_1, ..., b_n)$ Basis $\Rightarrow d = d(b_1, ..., b_n) \cdot D_{\underline{B}}$ (siehe obiger Beweis). Wissen $d, D_{\underline{B}} \neq 0 \Rightarrow d(b_1, .., b_n) \neq 0$
" $\Leftarrow$ " : (Ü) $f \in Alt_n(V, W)$ und $v_1, ..., v_n$ l.a. $\Rightarrow f(v_1, ..., v_n) = 0$ (also $d(b_1, ..., b_n) \neq 0 \Rightarrow b_1, ..., b_n$ sind l.u.) □

Definition 10.7 : Für $d \in Alt_n(V, K)$ sind $f \in Lin(U, V)$. Definiere $f^\circ(d) : U^n \to K, (u_1, ..., u_n) \mapsto d(f(u_1), ..., f(u_n))$

Bemerkung : $f^\circ(D_{\underline{B}})(v_1, ..., v_n) = D_{\underline{B}}(f(v_1), ..., f(v_n)) = ... \cdot D_{\underline{B}}(v_1, ..., v_n)$

Lemma 10.8 : a) $f^\circ(d) \in Alt_n(U, K) \forall d \in Alt_n(V, K)$
b) $f^\circ : Alt_n(V, K) \to Alt_n(U, K), d \mapsto f^\circ(d)$ ist linear.
c) Ist $g : X \to U$ linear, so gilt: $g^\circ(f^\circ(d)) = (f \circ g)^\circ(d)$

Beweis : a) $f^\circ(d)$ n-linear, denn: Seien $u_1, ..., u_{i-1}, u_{i+1}, ..., u_n \in U$ fest. $u \in U$ variabel.$\Rightarrow u \mapsto f()$ und $v \mapsto d(f(u_1), ..., f(u_{i-1}), v, f(u_{i+1}), ..., f(u_n))$ sind linear $\Rightarrow$ deren Verkettung:
$u \mapsto d(f(u_1), ..., f(u_{i-1}), f(u), f(u_{i+1}), ..., f(u_n))$ d.h. $u \mapsto (f^\circ(d))(u_1, ..., u_{i-1}, u, u_{i+1}, ..., u_n)$ ist lienar.
alternierend: Seien $u_1, ..., u_n \in U$ mit $u_i = u_j$ für ein Paar $1 \leq i < j \leq n \Rightarrow f(u_1), ..., f(u_n) \in V$ und $f(u_i) = f(u_j) \Rightarrow 0 = d(f(u_1), ..., f(u_n)) = (f^\circ(d))(u_1, ..., u_n)$
b),c) Ü. □

Korollar 10.9 : Gelte $dim V = n \Rightarrow$ Für $f \in End(V)$ und $d \in Alt_n(V, K) \setminus \{0\}$ gelten:
a) $f^\circ(d) \in Alt_n(V, K) = K \cdot d$, d.h. $\exists! \lambda_f \in K$ mit $\lambda_f \cdot d$
b) λ_f ist unabhängig von d.

Definition 10.10 : Die *Determinante* von $f \in End(V)$ ist $det(f) := \lambda_f$, d.h. $det : End_K(V) \to K$

Beweis : a) $f^\circ(d) \in Alt_n(V,K)$ nach 10.8. $d \neq 0 \Rightarrow d \in Alt_n(V,K)$ ist Basis nach 10.5$\Rightarrow$ erhalte eindeutiges $\lambda \cdot f$
b) Sei $d \in Alt_n(V,K)\backslash\{0\}$ beliebig $\Rightarrow \exists \mu \in K : d' = \mu \cdot d \Rightarrow f^\circ(d') = f^\circ(\mu \cdot d) \overset{f^\circ\ lin.}{=} \mu \cdot f^\circ(d) \overset{a)}{=} \mu \cdot \lambda_f \cdot d = \lambda_f \cdot d'$
$\square$

Proposition 10.11 : Sei $\underline{B} = (b_1, ..., b_n)$ geordnete Basis von V, seien $f, g \in End(V)$ und $\lambda \in K$. Dann gelten: a) $det(f \circ g) = det(f) \cdot det(g)$
b) $det(f) = D_{\underline{B}}(f(b_1), ..., f(b_n))$
c) $det(\lambda \cdot f) = \lambda^n \cdot det(f)$
d) $f \in Aut(V) \Leftrightarrow det(f) \neq 0$
e) $det|_{Aut(V)} : Aut(V) \to K$ ist Gruppenhomom.

Beachte : b) $\Rightarrow det(id_V) = 1$, e) $\Rightarrow det(f^{-1}) = det(f)^{-1}$

10.1 Die Determinante einer quadratischen Matrix

Zu $A = (a_{ij}) \in M_{nxn}(K)$ betrachte $f = l_{A^t} : V_n(K) \to V_n(K), v \mapsto A^t \cdot v$

Definition 10.12 : $det(A) := |A| := det(l_{A^t}$ heißt *Determinante* von A.

Proposition 10.13 : Es gelten: a) $det(AB) = det(A) \cdot det(B)$ für $A, B \in M_{nxn}(K)$
b) $det(A) = \sum\limits_{\sigma \in S_n} sgn(\sigma) \cdot a_{1\sigma(1)} ... a_{n\sigma(n)}$

Beweis : a) $|A \cdot B| = det(l_{(AB)^t}) = det(l_{B^t} \circ l_{A^t}) \overset{10.11a)}{=} det(l_{B^t}) \cdot det(l_{A^t}) = |A \cdot B|$ $\square$
b) $|A| = det(f) \overset{10.11b)}{=} D_{\underline{E}}(f(e_1), ..., f(e_n)) = D_{\underline{E}}(\sum\limits_{i_k=1}^{n} a_{1_{i1}} e_{i1}, ..., \sum\limits_{i_n=1}^{n} a_{n_{in}} e_{in}) \overset{10.4}{=} \sum\limits_{\sigma \in S_n} a_{1\sigma(1)} \cdot ... \cdot a_{n\sigma(n)} \cdot sgn(\sigma) \cdot D_{\underline{E}}(e_1, ..., e_n)$ $\square$

Bemerkung : Im weiteren und auch zuvor: $\sum$ =Standardbasis von $V_n(K)$ (Spaltenvektoren) und $\underline{E}^*$ ist Dualbasis von $Z_n(K)$.

Lemma 10.14 : Seien $z_1, ..., z_n$ die Zeilen von A. Dann gilt $det \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = D_{\underline{E}} * (z_1, ..., z_n)$, insbesondere ist $(z_1, ..., z_n) \mapsto det \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ alternierend und (K-)n-linear.

Beweis : $det(z_1, ..., z_n)^t = det(l_{(z_1 t ... z_n t)}) \overset{10.5}{=} D_{\underline{E}}(z_1^t, ..., z_n^t)$. Sei $g : Z_n(K) \to V_n(K), z \mapsto z^t$ (VR-Isom.)$\Rightarrow$
$\circledast = (g^\circ(D_{\underline{E}}))(z_1, ..., z_n)$. Behauptung: $g^\circ(D_{\underline{E}} = D_{\underline{E}^*}$ in $Alt_n(Z_n(K), K)$ genügt zu zeigen: $(g^\circ(D_{\underline{E}}))(e_1^*, ..., e_n^* \overset{!}{=} D_{\underline{E}^*}(e_1^*, ..., e_n^*) = 1$, da $g^\circ(D_{\underline{E}}) = \mu \cdot D_{\underline{E}^*}$ für $\mu \in K$
zu ! : $(g^\circ(D_{\underline{E}}))(e_1^*, ..., e_n^*) = D_{\underline{E}}((e_1^*)^t, ..., (e_n^*)^t) = D_{\underline{E}}(e_1, ..., e_n) = 1$ $\square$

Korollar 10.15 : Entsteht $\tilde{A}$ aus A durch anwenden von E1-E3 (Zeilentransformationen) so gilt:

$$det(\tilde{A}) = \begin{cases} -det(A) & \text{für E1 (vertausche verschiedene Zeilen)} \\ det(A) & \text{für E2} \\ \lambda \cdot det(A) & \text{für E3 (Mult. 1Zeile mit } \lambda \neq 0) \end{cases}$$

__*Beweis*:__ a) Tausche Zeile i mit Zeile $j, i \neq j$. Sei $\tau = \tau_{(i,j)}$. Dann gilt: $det(\tilde{A}) = D_{\underline{E}^*}(z_1, ..., z_i + z_j \cdot \mu, ..., z_n) = D_{\underline{E}^*}(z_1, ..., z_n) = (-1) \cdot det(A)$
b) E2: Addiere Zeile $j \cdot \mu$ zu Zeile i. $det(\tilde{A}) = D_{\underline{E}^*}(z_1, ..., z_i + z_j \cdot \mu, ..., z_n) = D_{\underline{E}^*}(z_1, ..., z_n) + D_{\underline{E}^*}(z_1, ..., z_i, ..., z_j, ..., z_n) \cdot \mu = det(A)$ etc. $\square$

__*Korollar* 10.16 :__ Für $A \in M_{nxn}(K)$ gilt $|A^t| = |A|$

__*Beweis*:__ 1) Die Aussage gilt für elementare Matrizen. (wegen 10.15) z.B: $det(S^{(i,j)}) = -1 = det(S^{(j,i)^t})$ oder $(S^{(i,j)^t} = S^{(i,j)}$! Analog für übrige $A_\lambda^{(i,j)}$ bzw. $M_\lambda^{(i)}$. Beachte $det(A_\lambda^{(i,j)}) \overset{10.15}{=} 1$ (E2 in 10.15)
2) Falls A in $GL_n(K)$, schreibe $A = A_1 \cdot ... \cdot A_5$ mit A_i elementar. $det(A^t) = det(A_5^t \cdot A_{5-1}^t \cdot ... \cdot A_1^t) = det(A_5^t) \cdot ... \cdot det(A_1^t) \overset{1)}{=} det(A_1) \cdot .... \cdot det(A_5) = det(A)$
3) Für $A \in M_{nxn}(K) \setminus GL_n(K) :\Rightarrow A$ und A^t haben nicht vollen Rang $\Rightarrow l_{A^\circ}, l_A$ nicht invertierbar $\Rightarrow det(A) = det(l_{A^t}) = 0 = det(l_A) = det(A^t)$ $\square$

__*Korollar* 10.17 :__ (Ü) a) $V^n \to K, (v_1, ..., v_n) \mapsto det(v_1, ..., v_n)$ ist in $Alt_n(V_n(K), K)$
b) Analogen zu 10.15 gilt für elementare Spaltentransformationen.
c) (wie im Bsp.) $det \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} = a_1 \cdot ... \cdot a_n$ (auch falls ein $a_i = 0$!)

10.2 Laplace-Entwicklung

Für $A \in M_{nxn}(K)$ und $i, j \in \{1, ..., n\}$. Sei $A_{i,j} \in M_{n-1xn-1}(K)$ die durch Streichen von Zeile i und Spalte j entstehende Matrix.

__*Lemma* 10.18 :__ (Ü) Sei $A \in M_{nxn}(K)$ mit Zeile i von der Form $\begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \end{pmatrix} \Rightarrow det(A) = (-1)^{i+j} det(A_{i,j})$

__*Satz* 10.19 Laplace'scher Entwicklungssatz :__ Für $i, j \in \{1, ..., n\}$ gelten a) $det(A) = \sum\limits_{j=1}^{n} a_{ij}(-1)^{i+j}|A_{ij}|$ (Zeilenentwicklung)
b) $det(A) = \sum\limits_{i=1}^{n} a_{ij}(-1)^{i+j}|A_{ij}|$ (Spaltenentwicklung)

__*Beweis*:__ nur a): Sei $A = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ (z_1 ist Zeile l von A)$\Rightarrow |A| = D_{\underline{E}^*}(z_1, ..., z_{i-1}, \sum\limits_{j=1}^{n} a_{ij} \cdot e_j^*, z_{i+1}, ..., z_n) = \sum\limits_{j=1}^{n} a_{ij} \cdot D_{\underline{E}^*}(z_1, ..., z_{i-1}, e_j^*, z_{i+1}, ..., z_n) = \sum\limits_{j=1}^{n} a_{ij} | \circledast_j | \overset{\ddot{U}}{=} \sum\limits_{j=1}^{n} (-1)^{i+j}|A_{ij}| \cdot a_{ij}$ $\square$

__*Korollar* 10.20 :__ Für $k \neq i$ gilt $\sum\limits_{j=1}^{n} a_{kj}(-1)^{i+j} det(A_{i,j}) = 0$

__*Beweis*:__ Schreibe $A = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$, d.h. z_j =Zeile l von A. $det \begin{pmatrix} z_1 \\ \vdots \\ z_{i-1} \\ z_k \\ z_{i+1} \\ \vdots \\ z_n \end{pmatrix} = \sum\limits_{j=1}^{n} a_{kj}(-1)^{i+j} det(A_{i,j})$. Zeile i =Zeile

k (und $k \neq i$) und $Z_n(K)^n \to K, (w_1, ..., w_n) \mapsto det \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$ ist alternierend. $\square$

<u>*Definition* 10.21 :</u> Für $A \in M_{nxn}(K)$ sei die <u>*Adjunkte*</u>$Adj(A) \in M_{nxn}(K)$ die Matrix $((-1)^{i+j} det(A_{j,i}))_{i,j=1...n}$

<u>*Satz* 10.22 :</u> $A \cdot Adj(A) = det(A) \cdot 1_n$. Gilt also $det(A) \neq 0$, so erhält man $A^{-1} = \frac{1}{det(A)} \cdot Adj(A)$

<u>*Korollar* 10.23 (Regel von Cramer) :</u> Sei $A \in M_{nxn}(K)$ mit Spalten $a_1, ..., a_n \in V_n(K)$. Sei $b \in V_n(K)$. Falls $det(A) \neq 0$, so gelten: a) $|\mathbb{L}(A, b)| = 1$

b) Ist $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ die Lösung aus a), so gilt $x_i = \frac{det(a_1...a_{i-1} b a_{i+1}....a_n)}{det(a_1...a_n)}$

<u>*Beweis* :</u> a) $det(A) \neq 0 \Rightarrow Rang(A) = n \overset{9.4b)}{\Rightarrow} |\mathbb{L}(A, b)| = 1$

b) $A \cdot x = b$ bedeutet: $x_1 a_1 + x_2 a_2 + ... + x_n a_n = b \circledast \Rightarrow det(a_1...a_{i-1} b a_{i+1}...a_n) = \sum_{j=1}^{n} x_j det(a_1...a_{i-1} a_j a_{i+1}...a_n) = x_i \cdot 0 + ... + 0 x_{i-1} + x_j \cdot det(A) + 0 + ... + 0$ $\square$

<u>*Proposition* 10.24 :</u> Sei V K-VR mit geordneter Basis $\underline{B} = (b_1, ..., b_n)$ und sei $f \in End(V)$. Dann gilt: $det(f) = det(Mat_{\underline{B}}^{\underline{B}}(f))$

<u>*Korollar* 10.25 :</u> a) $det(Mat_{\underline{B}}^{\underline{B}}(f))$ ist unabhängig von $\underline{B}$. (Klar!)

b) Ähnliche Matrizen haben dieselbe Determinante. (Klar!) (Ü)

<u>*Beweis* 10.24 :</u> Betrachte $\begin{array}{ccc} V & \overset{f}{\to} & V \\ \uparrow^{\iota} \underline{B} & & \downarrow^{\iota} \underline{B}^{-1} \\ V_n(K) & \overset{g}{\to} & V_n(K) \end{array}$ und beachte $d := ({}^{\iota}\underline{B}^{-1})^{\circ}(D_{\underline{E}}) \in Alt_n(V, K)$.

1) $det(f) = det(g)$: $det(g) \cdot D_{\underline{E}} = g^{\circ}(D_{\underline{E}}) = ({}^{\iota}\underline{B}^{-1} \circ f \circ^{\iota} \underline{B})^{\circ}(D_{\underline{E}}) =^{\iota} \underline{B}^{\circ} \circ f^{\circ} \circ ({}^{\iota}\underline{B}^{-1})^{\circ}(D_{\underline{E}}) =^{\iota} \underline{B}^{\circ} \circ f^{\circ}(d) =^{\iota} \underline{B}^{\circ}(det(f) \cdot d) = det(f) \cdot^{\iota} \underline{B}^{\circ}({}^{\iota}\underline{B}^{-1})^{\circ}(D_{\underline{E}}) = det(f) \cdot D_{\underline{E}}$

2) Sei $A := Mat_{\underline{B}}^{\underline{B}}(f) = Mat(g)$, so dass $g = l_A$. Dann $det(A) = det(A^t) = det(l_{(A^t)^t}) = det(l_A) = det(g) = det(f)$ $\square$

11 Das Charakteristische Polynom und Eigenwerte

Sei K ein Körper.
$\underline{Definition\, 11.1:}$ a) Ein $\underline{Polynom}$ über K ist eine Folge $(a_n)_{n\geq 0}$ mit $a_n \in K$. $\forall n$ und $\exists n_0 : \forall n \geq n_0 : a_n = 0$
b) $P = (0, 0, 0, ...)$ heißt $\underline{Nullpolynom}$ (schreibe $P = 0$)
c) Für Polynome $P = (a_n)_{n\geq 0}$ und $Q = (b_n)_{n\geq 0}$ über K seien $P+Q := (a_n+b_n)_{n\geq 0}$. $P\cdot Q := (\sum\limits_{k=0}^{n} a_k \cdot b_{n-k})_{n\geq 0}$

$$\underline{Grad}P := \begin{cases} -\infty & P = 0 \\ max\{n \in \mathbb{N}_0 | a_n \neq 0\} & P \neq 0 \end{cases}$$

Falls $P \neq 0$ nenne $a_{Grad\, P}$ den $\underline{Leitkoeffizienten}$ von P, nenne P $\underline{normiert}$, wenn Leitkoeffizient=1.
d) Schreibe $K[T]$ für die Menge aller Polynome über K (in den Variablen T)$\rightsquigarrow$ alternative Notation für $(a_n)_{n\geq 0}$ ist $\sum\limits_{n\geq 0} a_n T^n = a_0 + a_1 T + ... + a_m T^m$

$\underline{Bemerkung:}$ $(K[T], 0, 1, +, \cdot)$ $(1 = (1, 0, 0, ..., 0))$ ist ein $\underline{Ring}$: Es gelten Axiome eines Körpers, bis auf Elemente in $K[T] \setminus \{0\}$ müssen kein Inverses bezüglich $\cdot$ haben.

$\underline{Definition\, 11.2:}$ Sei $P = (a_n) \in K[T]$ a) $P(.) : K \to K, \lambda \mapsto \sum\limits_{n\geq 0} a_n \lambda^n$ heißt $\underline{Auswertungsabbildung}$ zu P.
b) $\lambda \in K$ heißt $\underline{Nullstelle}$ von $P :\Leftrightarrow P(\lambda) = 0$

$\underline{Lemma\, 11.3:}$ (Ü) seien P, Q (Polynome) $\in K[T]$ und $\lambda \in K$. Dann: a) $(P + Q)(\lambda) = P(\lambda) + Q(\lambda)$
b) $GradP \cdot Q = GradP + GradQ$, hierbei gelte $-\infty + x = x + (-\infty) = -\infty + (-\infty) = -\infty$ $(x \in \mathbb{N}_0)$
c) $P \cdot Q = 0 \Leftrightarrow P = 0 \vee Q = 0$
d) $\exists!$Polynom $S \in K[T]$, so dass $P = (T - \lambda) \cdot S + P(\lambda)$
e) $GradP > GradQ \Rightarrow$ Leitkoeffizient von $P + Q$ =Leitkoeffizient von P.

$\underline{Bemerkung:}$ Polynomdivision gilt für Polynome P, Q beliebig.

$\underline{Satz\, 11.4:}$ Sei $P \in K[T] \setminus \{0\}$. Dann existiert $k \in \mathbb{N}_0, \lambda_1, ..., \lambda_k \in K$ paarweise verschieden, $n_1, ..., n_k \in \mathbb{N}$ und $Q \in K[T]$, so dass $P = Q \cdot \prod_{j=1}^{k}(T - \lambda_j)^{n_j}$ und Q hat keine Nullstelle in K. Dabei ist Q eindeutig und $(\lambda_1 n_1), ..., (\lambda_k n_k)$ sind eindeutig bis auf Permutationen.

$\underline{Definition\, 11.5:}$ n_i heißt $\underline{Vielfachheit}$ der Nullstellen λ_i.

$\underline{Beweis:}$ Existenz: Indukton über $GradP$. $GradP = 0 \Rightarrow P = a_0 = Q, k = 0$. $n = GradP, n \mapsto n + 1 : P$ hat keine Nullstellen in $K \Rightarrow Q := P, k = 0$.
Fall: P hat Nullstellen in K, diese seien $\lambda \overset{11.3}{\Rightarrow} P = (T - \lambda) \cdot P_1 + 0$ für eindeutiges Polynom P_1 vom $Gradn$.
Nun Ind.Vor: auf P_1 anwenden und sauber "Buch halten".
Eindeutigkeit; (Ü)

$\underline{Korollar\, 11.5:}$ a) Sei $P \in K[T] \setminus \{0\}$. Dann ist die Zahl der Nullstellen von P in K höchstens $GradP$.
b) Ist K ein unendlicher Körper, so gibt für $P, Q \in K[T] : P = Q \Leftrightarrow P(.) = Q(.) (\Leftrightarrow P(\lambda) = Q(\lambda) \forall \lambda \in K)$

$\underline{Beweis:}$ a) Schreibe $P = Q \cdot \prod_{i=1}^{k}(T - \lambda_i)^{k_i}$ wie in 11.4 $\Rightarrow$ Nullstellen von P sind $\lambda_1, ..., \lambda_k$ und $GradP = GradQ + \sum\limits_{i=1}^{k} n_i \geq 0 + \sum\limits_{i=1}^{k} 1 = k$ =Anzahl der Nullstellen.
b) $P = Q \Leftrightarrow P - Q = 0$. Also zz: $P = 0 \Leftrightarrow P(.)$ ist die Nullabbildung.
" $\Rightarrow$ " Klar. " $\Leftarrow$ " Annahme: $P \neq 0 \overset{a)}{\Rightarrow} P$ hat höchstens $GradP$ Nullstellen. Andererseits: P =Nullabbildung.$\Rightarrow$ alle Elemente von K sind Nullstellen von $P \Rightarrow |K| \leq GradP$ ist Widerspruch zu K unendlich. $\square$

$\underline{Bemerkung:}$ $\cdot$ Gilt $GradP, GradQ \leq n$ und $|K| > n$, so folgt $P = Q \Leftrightarrow P(.) = Q(.)$
$\cdot$ Eventuell in LA 2: $L[T] \to Abb(K,K), p \mapsto p(.)$ ist ein Ringhomomorphismus.

$\underline{Satz\ 11.7:}$ (ohne Beweis) a) $\mathbb{C}$ ist algebraisch abgeschlossen (auch in Funktheo 1)
b) Jeder Körper ist Unterkörper eines algebraisch abgeschlossenen Körpers
c) Jeder algebraisch abgeschlossene Körper ist unendlich.

$\underline{Definition\ 11.12\ \text{Charakteristisches Polynom}):}$ Sei V ein K-VR mit Basis $\underline{B}, f \in End(V), A = Mat_{\underline{B}}^{\underline{B}}(f)$.
Definiere $P_{ij} := \begin{cases} T - a_{ii} & i = j \\ -a_{ij} & i \neq j \end{cases}$ in $K[T]$ und $P_f := P_A := \sum_{\sigma \in S_n} sgn(\sigma) \cdot P_{1\sigma(1)} \cdot \ldots \cdot p_{n\sigma(n)} \overset{11.3e)}{\Rightarrow} GradP_f =$Grad von Summand für $\sigma = id = n$ und Leitkoeffizient von $P_f =$Leitkoeffizient von $sgn(\sigma) \cdot P_{11} \cdot \ldots \cdot P_{nn} =$Leitkoeffizient von $1 \cdot (T - a_{11}) \cdot \ldots \cdot (T - a_{nn}) = 1$
b) $P_{ij}(\lambda) =$Koeffizient an (i,j) von $C := Mat_{\underline{B}}^{\underline{B}}(\lambda \cdot id_V - f) = \lambda \cdot Mat_{\underline{B}}^{\underline{B}}(id_V) - Mat_{\underline{B}}^{\underline{B}}(f) \overset{11.3}{\Rightarrow} P_f(\lambda) = \sum_{\sigma \in S_n} sgn(\sigma) \cdot P_{1\sigma(1)}(\lambda) \cdot \ldots \cdot P_{n\sigma(n)}(\lambda) = \sum_{\sigma \in S_n} sgn(\sigma) \cdot c_{1\sigma(1)} \cdot \ldots \cdot c_{n\sigma(n)} \overset{Leibniz}{=} det(C) = det(\lambda id_V - f)$
c) Beweis nur für K mit $|K| > n$. Nach b) und a): $P_f \in K[T], GradP = n$ und $P_f(\lambda) = det(\lambda \cdot id_V - f) \forall \lambda \in K$.
Sei jetzt $A' = Mat_{\underline{B'}}^{\underline{B'}}(f)$ bezüglich Basis $\underline{B'}$ von $V \overset{a),b)}{\Rightarrow} P_{A'} \in K[T], GradP_{A'} = n, P_{A'}(\lambda) = det(\lambda id_V - f) \forall \lambda \in K \Rightarrow P_f(\lambda) = P_{A'}(\lambda) \forall \lambda \in K$ $(|K| \geq n+1)$ und $GradP_{A'} = GradP_f = n \Rightarrow P_{A'} = P_f$
d) Folgt aus b) und 10.4, da $\lambda \cdot id_V - f \in End(V)$ ist invertierbar$\Leftrightarrow det(\lambda id_V - f) \neq 0 \overset{b)}{\Leftrightarrow} P_f(\lambda) \neq 0$ $\square$

$\underline{Berechnung\ von\ P_f:}$ Berechne allgemeine Formel von $P_f(\lambda)$ für $\lambda \in K$ beliebig (unter der Annahme, dass K unendlich ist) mit Gauß (oder Sarrus oder...). Ersetze λ durch T. Tatsächlich berechne direkt mit T. $P_f(\lambda) = det(\lambda id_V - f)$!

$\underline{Definition\ 11.15:}$ Sei V ein VR der Dimension $n \in \mathbb{N}, f \in End(V)$. $v \in V$ heißt $\underline{Eigenvektor}$ zu $f \Leftrightarrow v \neq 0, \exists \lambda \in K$ mit $f(v) = \lambda \cdot v$

$\underline{Definition\ 11.16:}$ a) $A = (a_{ij}) \in M_{nxn}(K)$ heißt $\underline{Diagonalmatrix} \Leftrightarrow a_{ij} = 0 \forall i \neq j \Leftrightarrow A = \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_{nn} \end{pmatrix}$
b) $f \in End(V)$ heißt $\underline{diagonalisierbar} \Leftrightarrow \exists$Basis $\underline{B}$ von V, so dass $Mat_{\underline{B}}^{\underline{B}}(f)$ ist Diagonalmatrix.

$\underline{Satz\ 11.17:}$ $f \in End(V)$ ist diagonalisierbar$\Leftrightarrow V$ besitzt Basis $\underline{B}$ aus Eigenvektoren.

$\underline{Beweis:}$ " $\Rightarrow$ " sei $\underline{B}$ Basis, so dass $Mat_{\underline{B}}^{\underline{B}}(f) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ gilt $(\lambda_1, ..., \lambda_n \in K) \Rightarrow$ Betrachte i-te Spalte $\Rightarrow f(b_i) = \lambda_i b_i$, da $b_i \neq 0$, haben Basis aus Eigenvektoren.
" $\Leftarrow$ " Sei $\underline{B} = (b_1, ..., b_n)$ Basis aus Eigenvektoren. Gelte $f(b_i) = \lambda_i b_i$ für geeignetes $\lambda_i \in K \Rightarrow Mat_{\underline{B}}^{\underline{B}}(f) =$
$\begin{pmatrix} \lambda_1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & 0 & \vdots & \vdots \\ \vdots & \vdots & \lambda_i & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \ldots & \lambda_n \end{pmatrix}$ ist Diagonalmatrix. $\square$

$\underline{Beachte:}$ i) $v \in V$ ist Eigenvektor $\Leftrightarrow v \neq 0 \wedge \exists \lambda \in K.\ f(v) = \lambda \cdot id_V(v) \Leftrightarrow v \neq 0 \wedge \exists \lambda \in K$ mit

$(\lambda \cdot id_V - f)(v) = 0 \Leftrightarrow \exists \lambda \neq 0 : v \in Kern(\lambda id_V - f) \setminus \{0\}$
ii) $Kern(\lambda id_V - f) \supset \{0\} \Leftrightarrow \lambda \cdot id_V - f$ kein Monomorphismus $\Leftrightarrow \lambda id_V - f$ ist nicht invertierbar$\Leftrightarrow 0 = det(\lambda id_V - f) = P_f(\lambda)$

Lemma 11.18 : a) $v \in V$ ist EV zu $f \Rightarrow \exists!$ EW λ von f mit $f(v) = \lambda \cdot v$
b) Ist λ ein EW von f in K, so existiert ein EV v zu f mit $f(v) = \lambda \cdot v$

Definition 11.19 : $E_f(\lambda) := \{v \in V | f(v) = \lambda v\} = Kern(\lambda id_V - f)$ heißt Eigenraum zu $\lambda \in K$

Bemerkung : a) $E_f(\lambda) \supset \{0\} \Leftrightarrow \lambda$ ist EW zu f
b) Menge aller EV'en zu $f = \overset{\cup}{\lambda \in K, EW\ zu\ f}\ (E_f(\lambda) \setminus \{0\}) \Rightarrow$Bestimmung aller EV'en: i) Berechne P_f
ii) Berechne die Nullstellen von P_f in K.
iii) $\forall EV'e\lambda$ von f berechne $Kern(\lambda id_V - f)$

Definition 11.20 : $\mu_f(\lambda) :=$ Vielfachheit von λ als Nullstelle von P_f

Bemerkung : $\mu_f(\lambda) = 0$ falls λ kein EW zu f, sonst: $1 \leq \mu_f(\lambda) \leq n$

Lemma 11.21 : $dim E_f(\lambda) \leq \mu_f(\lambda)$

Satz 11.22 : Für $f \in End(V)$. V endlich-dimensionaler K-VR, sind äquivalent:
a) f ist diagonalisierbar
b) i) P_f zerfällt in Linearfaktoren (in $K[T]$)$\wedge$ ii) $\forall$ EWλ von f gilt $dim E_f(\lambda) = \mu_f(\lambda)$
c) $\sum\limits_{\lambda \in K} dim E_f(\lambda) = dim V$

Definition 11.23 : a) UVR'e$U_1, ..., U_k$ von V heißen l.u. $:\Leftrightarrow \forall (u_1, ..., u_k) \in U_1 \times ... \times U_k : u_1 + ...u_k = 0 \Rightarrow (u_1, ..., u_k) = (0, ..., 0)$. in Diesem Fall schreiben wir $U_1 \oplus U_2 \oplus ... \oplus U_k$ für $L(U_1 \cup U_2 \cup .... \cup U_k)$
b) UVR'e $U_1, ..., U_k$ von V bilden Zerlegung von $V \Leftrightarrow U_1, ..., U_k$ sind k.u. und $U_1 \oplus ... \oplus U_k = V$

Bemerkung : Sind $u_1, ..., u_n \in V$ l.u.„ so sind $U_1 = K \cdot u_1, ..., U_k = K \cdot u_k$ l.u.. Bilden $u_1, ..., u_k$ Basis von V, so bilden $K \cdot u_1, ..., K \cdot u_k$ eine Zerlegung von V.

Lemma 11.24 : Seien $U_1, ..., U_k$ l.u. UVR'e von V, sei B_i Basis von $U_i, i = 1...k$. Dann gelten:
a) $B_1, ..., B_k$ sind paarweise disjunkt und $B = \bigcup\limits_{i=1}^{k} B_i$ ist Basis von $U_1 \oplus ... \oplus U_k$
b) Bilden $U_1, ..., U_k$ eine Zerlegung von V, so ist B (aus a)) Basis von V.

Beweis : b) folgt direkt aus a) under der Definition von Zerlegung.
a) B ist ES von $U_1 \oplus ... \oplus U_k$: Denn $L(U_1 \cup ... \cup U_k) = L(B_1 \cup ... \cup B_k)$.
B ist l.u. (und B_i paarweise disjunkt): Gelte $0 = \sum\limits_{b \in B_i} \lambda_b \cdot b = 0$ für $i = 1...k \Rightarrow \lambda_b = 0 \forall b \in B_i \forall i = 1...k \Rightarrow$ Behauptung. $\square$

Korollar 11.25 : Seien $U_1, ..., U_k$ l.u. UVR'e von V. Dann gelten:
a) $dim U_1 \oplus ... \oplus U_k = \sum\limits_{i=1}^{k} dim U_i$ (denn $|B| = \sum\limits_{i=1}^{k} |B_i|$ im Lemma)
b) $U_1, ..., U_k$ bilden Zerlegung von $V \Leftrightarrow \sum\limits_{i=1}^{k} dim U_i = dim V$

Lemma 11.26 : Für $f \in End(V)$ $(dim V < \infty)$ seien $\lambda_1, ..., \lambda_k \in K$ paarweise verschiedene Eigenwerte von f. Dann sind $E_f(\lambda_1), ..., E_f(\lambda_k)$ l.u. UVR'e von V.

Beweis : Sei $v_i \in E_f(\lambda_i)$ für $i = 1...k$. Gelte $v_1 + ... + v_k = 0$. zz: $v_1 = ... = v_n = 0$
Definiere $f_i \in End(V)$ durch $f_i := (\lambda_1 \cdot id_V - f) \circ ... \circ (\lambda_{i-1} id_V - f) \circ (\lambda_{i+1} id_V - f) \circ ... \circ (\lambda_k id_v - f)$ $\Rightarrow$Für einen EV w zu f mit $f(w) = \lambda \cdot W$ gilt $f_i(w) = (\lambda_1 - \lambda)...(\lambda_{i-1} - \lambda)(\lambda_{i+1} - \lambda)...(\lambda_k - \lambda) \cdot w \Rightarrow 0 = f_i(0) = f_i(v_1 + ... + v_k) = \sum_{l=1}^{k} f_i(v_l) = \sum_{l=1}^{k} (\lambda_1 - \lambda_l)...(\lambda_{i-1} - \lambda_l)(\lambda_{i+1} - \lambda_l)...(\lambda_k - \lambda_l) \cdot v_l = 0 + ... + 0 + (\lambda_1 - \lambda_i)...(\lambda_{i-1} - \lambda_i)(\lambda_{i+1} - \lambda_i)...(\lambda_k - \lambda_i) v_i + 0 + ... + 0 + 0$. D.h. $0 = (Skalar \neq 0) \cdot v_i \Rightarrow v_i = 0$ □

Beachte : $f_i|_{E_f(\lambda_1) \oplus ... \oplus E_f(\lambda_k)}$ ist surjektive lineare Abbildung. $E_f(\lambda_1) \oplus ... \oplus E_f(\lambda_k) \to E_f(\lambda_i)$

Beweis von Satz : a)$\Rightarrow$b): Wähle $\underline{B}$ Basis von V mit $Mat^{\underline{B}}_{\underline{B}}(f) = \begin{pmatrix} \mu_1 & & 0 \\ & \ddots & \\ 0 & & \mu_n \end{pmatrix}$. Umordnen der $\mu_i \Rightarrow Mat^{\underline{B}}_{\underline{B}}(f) = Diag(\lambda_1, ..., \lambda_1, \lambda_2, ..., \lambda_2, ..., \lambda_k, ..., \lambda_k)$ wobei $\lambda_1, ..., \lambda_k$ paarweise verschieden. n_i =Vielfachheit mit der λ_i in der Diagonalmatrix auftritt und $n_1 + ... + n_k = n$

$$\Rightarrow P_f = det \begin{pmatrix} T - \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & T - \lambda_1 & & & & \\ & & & \ddots & & & \\ & & & & T - \lambda_k & & \\ & & & & & \ddots & \\ & & & & & & T - \lambda_k \end{pmatrix} = (T - \lambda_1)^{n_1} \cdot ... \cdot (T - \lambda_k)^{n_k} \Rightarrow \mu_f(\lambda_i) = n_i$$

zerfällt in Linearfaktoren und $E_f(\lambda) = Kern(Diag(\lambda_i - \lambda_1, ..., \lambda_i - \lambda_1, ..., \lambda_i - \lambda_{i-1}, \lambda_i - \lambda_{i-1}, 0, ..., 0$,Einträge $\neq 0). \Rightarrow dim E_f(\lambda) = \mu_f(\lambda_i \; \forall i = 1...k)$

b)$\Rightarrow$c): $\sum_{\lambda \in K} dim E_f(\lambda) = \sum_{\lambda \in K} dim E_f(\lambda) = \sum_{i=1}^{k} \mu_f(\lambda_i) = Grad P_f = dim V$

c)$\Rightarrow$a): Seien $\lambda_1, ..., \lambda_n$ die paarweise verschiedenen EW'e von f. Sei B_i Basis von $E_f(\lambda_i)$. c)$\Rightarrow \sum dim(E_f(\lambda_i) = dim V$. 11.26: $\Rightarrow E_f(\lambda_1), ..., E_f(\lambda_k)$ sind l.u. $\overset{11.25}{\Rightarrow} v = E_f(\lambda_1) \oplus ... \oplus E_f(\lambda_k)$ und 11.24: $B = B_1 \dot\cup B_2 \dot\cup ... \dot\cup B_k$ ist Basis von V von EV'en zu $f \Rightarrow f$ diagonalisierbar. □

Bemerkung : $det(f - \lambda \cdot id_V) = (-1)^{dim V} \cdot det(\lambda \cdot id_v - f)$

Bemerkung : Es gilt stets $\sum_{\lambda \in K} dim E_f(\lambda) \leq dim V$ (zu 11.22). Denn: $\sum_{\lambda \in K} dim E_f(\lambda \leq \sum_{\lambda \in K} \mu_f(\lambda) = \sum_{\lambda \in K} \mu_f(\lambda) \leq Grad(P_f) = dim V$

Korollar 11.27 : Für $f \in End(V)$ $(dim V < \infty)$ gilt: Hat f $dim V$ verschiedene Eigenwerte, so ist f diagonalisierbar.

Beweis : Ist $\lambda \in K$ ein EW zu f, so gilt $dim E_f(\lambda) \geq 1 \Rightarrow \sum_{\lambda \in K} dim E_f(\lambda) \geq \sum_{\lambda \in K} 1 \geq dim V \Rightarrow f$ ist diagonalisierbar. □

12 Euklidische und unitäre Vektorräume

Sei $K \in \{\mathbb{R}, \mathbb{C}\}$. $\underline{Ziel:}$ Zusatzstruktur eines Skalarproduktes auf einem K-VR $\rightsquigarrow$anschaulich: Können Längen und Winkel "messen".
$\underline{Wiederholung:}$ $\cdot\ \mathbb{R} \subseteq \mathbb{C} = \mathbb{R} + i \cdot \mathbb{R}$ identifiziere $a \in \mathbb{R}$ mit $a + i \cdot 0 \in \mathbb{C}$
$\cdot\ \overline{} : \mathbb{C} \to \mathbb{C}, z = a + i \cdot b \mapsto \overline{z} = a - i \cdot b$ ist komplexe Konjugation, wobei $\mathbb{R} = \{z \in \mathbb{C} | \overline{z} = z\}$
Für $z = a + i \cdot b$, mit $a, b \in \mathbb{R}$. i) $|z| = \sqrt{a^2 + b^2}$ und $|z|^2 = z \cdot \overline{z}$
ii) $|z| = 0 \Leftrightarrow z = 0$
iii) $Re(z) := a = \frac{1}{2}(z + \overline{z})$ und $Im(z) := b = \frac{1}{2i}(z - \overline{z})$

$\underline{Lemma\ 12.1:}$ (Ü) Seien $z, w \in \mathbb{C}$ beliebig, dann gilt: a) $|z \cdot w| = |z| \cdot |w|$
b) Ist $\underline{arg(z)}$ der Winkel zwischen z und $\mathbb{R}_{\geq 0}$, so gilt $arg(z \cdot w) = arg(z) + arg(w) - \begin{cases} 0 & arg(z) \neq arg(w) < 2\pi \\ 2\pi & arg(z) \neq arg(w) \geq 2\pi \end{cases}$
c) $\forall z \in \mathbb{C} \exists \lambda \in \mathbb{C}$ mit $|\lambda| = 1$, so dass $|z| = \lambda \cdot z$ (falls $z \neq 0 : \lambda = \frac{\overline{z}}{|z|}$)

$\underline{Definition\ 12.2:}$ Seien V, W K-VR'e, $K \in \{\mathbb{R}, \mathbb{C}\}$. Eine Abbildung $f : V \to K$ heißt $\underline{c-linear}$ $:\Leftrightarrow$ $\forall v_1, v_2 \in V$ und $\lambda \in K : f(v_1 + v_2) = f(v_1) + f(v_2) \wedge f(\lambda \cdot v_1) = \overline{\lambda} \cdot f(v_1)$

$\underline{Bemerkung:}$ Für $K = \mathbb{R}$ gilt linear=c-linear.

$\underline{Definition\ 12.3:}$ Sei V ein K-VR. Eine Abbildung $< .,. >: V \times V \to K, (v, w) \mapsto < v, w >$ heißt:
a) $\underline{symmetrische\ Bilinearform}$ (SBF), falls $K = \mathbb{R}$; $\underline{Hermitesche\ Form}$ (HF) falls $K = \mathbb{C}$ sofern gelten:
(S-H-1): $\forall w \in V$ ist $V \to K, v \mapsto < v, w >$ linear
(S-H-2): $\forall v \in V$ ist $V \to K, w \mapsto < v, w >$ c-linear
(S-H-3) $\forall v, w \in V :< v, w >= \overline{< v, w >}$
b) $\underline{Skalarprodukt}$ $\Leftrightarrow < .,. >$ ist SBF bzw. HF und es gilt (P) $\forall v \in V \setminus \{0\} :< v, v > \in \mathbb{R}_{\geq 0} = \{r \in \mathbb{R} | r > 0\}$
c) Ist $< .,. >$ ein Skalarprodukt auf V, so heißt $(V, < .,. >)$ $\underline{Euklidischer}$ $(K = \mathbb{R})$ bzw. $\underline{unitärer}$ $(K = \mathbb{C})$ Vektorraum. Falls $dimV < \infty$, nennen wir $(V, < .,. >)$ einen endlich-dimensionalen $\underline{Hilbertraum}$ (HR).

$\underline{Beispiel:}$ $V = V_n(K), < .,. >: V_n(K) \times V_n(K) \to K, (v, w) \mapsto v^t \cdot \overline{w}$ ist ein Skalarprodukt.

Sei im weiteren stets $(V, < .,. >)$ ein unitärer/Euklidischer Vektorraum.
$\underline{Definition\ 12.4:}$ a) Für $v \in V$ heißt $||v|| = \sqrt{< v, v >}$ die $\underline{Normlänge}$ von V.
b) Ist $(V, < .,. >)$ ein Euklidischer Vektorraum und sind $\overline{u, w \in V \setminus \{0\}}$, so heißt $\varphi \in [0, \pi]$ der $\underline{Winkel}$ zwischen v und $w \Leftrightarrow cos\varphi = \frac{<v,w>}{||v|| \cdot ||w||} \in [-1, 1]$
c) $v, w \in V$ heißen $\underline{orthogonal}$ $\Leftrightarrow < v, w >= 0$

$\underline{Lemma\ 12.5:}$ Für $v, w \in V$ und $\lambda \in K$ gelten: a) $||\lambda \cdot v|| = |\lambda| \cdot ||v||$
b) $v = 0 \Leftrightarrow ||v|| = 0$
c) $v \neq 0 \Rightarrow ||\frac{1}{||v||} \cdot v|| = 1$
d) $||v \pm w||^2 = ||v||^2 + ||w||^2 \pm 2 \cdot Re < v, w >$

$\underline{Beweis:}$ a) $||\lambda \cdot v|| = \sqrt{< \lambda v, \lambda v >} \overset{SH1}{=} \sqrt{\lambda < v, \lambda v >} \overset{SH2}{=} \sqrt{\lambda \overline{\lambda} < v, v >} = \sqrt{|\lambda|^2 ||v||^2} = |\lambda| ||v||$
b) folgt aus (P) und $< 0, 0 >= 0$
c) folgt aus a) und b)
d) $||v \pm w||^2 =< v \pm w, v \pm w > \overset{SH1,SH2}{=} < v, v > \pm < v, w > \pm < w, v > + < w, w >= ||v||^2 + ||w||^2 \pm (< v, w > + \overline{< v, w >}) = ||v||^2 + ||w||^2 \pm 2 \cdot Re < v, w >$ □

$\underline{Satz\ 12.6:}$ a) (Cauchy-Schwartz-Ungleichung): $\forall v, w \in V : | < v, w > | \leq ||v|| \cdot ||w||$

b) (Dreiecksungleichung) $\forall v, w \in V : ||v + w|| \leq ||v|| + ||w||$

<u>*Beweis :*</u> <u>a) $\Rightarrow$ b) :</u> 12.5$\Rightarrow$ $||v+w||^2 = ||v||^2 + ||w||^2 + 2 \cdot Re < v, w > \leq ||v||^2 + ||w||^2 + 2| < v, w > | \leq ||v||^2 + ||w||^2 + 2 \cdot ||v|| \cdot ||w|| = (||v|| + ||w||)^2 \overset{\checkmark}{\Rightarrow} ||v + w|| \leq ||v|| + ||w||$
a) Falls $< v, w >= 0 \Rightarrow$ Aussage klar. Im weiteren $< v, w > \neq 0 \Rightarrow v, w \neq 0 \Rightarrow ||v||, ||w|| > 0$. Dividiere Ungleichung durch $||v|| \cdot ||w|| (> 0) \Rightarrow \frac{|<v,w>|}{||v|| \cdot ||w||} \leq 1 \Rightarrow | < \frac{1}{||v||} \cdot v, \frac{1}{||w||} \cdot w > | \leq 1 \Rightarrow$ <u>$zz:$</u> $\forall v, w \in V$ mit $||v|| = ||w|| = 1$ gilt $| < v, w > | \leq 1$.
Wähle $\lambda \in \mathbb{C}$ mit $|\lambda| = 1$,so dass $\lambda\cdot < v, w >= | < v, w > | \in \mathbb{R}_{\geq 0}$, d.h. $| < v, w > | =< \lambda \cdot v, w >= Re < \lambda \cdot v, w > \Rightarrow 0 \leq ||\lambda \cdot v - w||^2 = ||\lambda \cdot v||^2 - 2 \cdot Re < \lambda v, w > + ||w||^2 \Rightarrow 2| < v, w > | = 2 \cdot Re < \lambda v, w > \leq ||v||^2 + ||w||^2 = 2 \Rightarrow | < v, w > | \leq 1$ □

<u>*Definition* 12.7(Darstellungsmatrizen zu einem Skalarprodukt) :</u> Sei V ein endlich-dimensionaler K-VR mit Basis $\underline{B} = (b_1, ..., b_n)$ und sei $< ., . >$ eine SBF/HF. Dann heißt $Mat_{\underline{B}}(< ., . >) = (< b_i, b_j >)_{i,j \in \{1,...,n\}} \in M_{nxn}(K)$ Darstellungsmatrix von $< ., . >$ bezüglich $\underline{B}$

<u>*Proposition* 12.8 :</u> Haben $v, w \in V$ die Koordinaten $(\lambda_1, ..., \lambda_n)$ bzw. $(\mu_1, ..., \mu_n)$ bezüglich $\underline{B}$ (d.h. $v = \sum\limits_{i=1}^{n} \lambda_i b_i, w = \sum\limits_{i=1}^{n} \mu_i b_i$), so gilt $< v, w >= (\lambda_1, ..., \lambda_n) \cdot Mat_{\underline{B}}(< ., . >)(\overline{\mu_1}, ..., \overline{\mu_n})^t$
<u>*Beweis :*</u> $< \sum\limits_{i=1}^{n} \lambda_i b_i, \sum\limits_{j=1}^{n} \mu_j b_j >= \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} \lambda_i \overline{\mu_j} < b_i, b_j >=$ rechte Seite. □

<u>*Definition* 12.9 :</u> Sei $A = (a_j) \in M_{nxn}(K)$. a) A heißt <u>*symmetrisch*</u> $:\Leftrightarrow A = A^t (\Leftrightarrow a_{ij} = a_{ji}, \forall i, j \in \{1...n\})$
b) $\overline{A} = (\overline{a}_{ij}) \in M_{nxn}(K), A^* = A^{-t} (\Rightarrow A^* = A^t$ falls $K = \mathbb{R})$
c) A heißt <u>*hermitesch*</u> $\Leftrightarrow A = A^*$

<u>*Beispiel* :</u> $\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$ ist hermitesch, nicht symmetrisch.

<u>*Proposition* 12.10 :</u> Sei V ein K-VR mit Basis $\underline{B} = (b_1, ..., b_n)$. Dann ist die folgende Abbildung wohl-definiert und bijektiv: $\{< ., . >: V \times V \to K | < ., . >$ eine $\overset{SBF}{HF}\} \to \{A \in M_{nxn}(K) | A = A^*\}, < ., . > \mapsto Mat_{\underline{B}}(< ., . >)$.
Umkehrabbildung: $(< ., . >: (\sum \lambda_i b_i, \sum \mu_j b_j) \mapsto (\lambda_1, ..., \lambda_n) \cdot A \cdot \begin{pmatrix} \overline{\mu_1} \\ \vdots \\ \overline{\mu_n} \end{pmatrix}) \hookleftarrow A$

<u>*Beweis :*</u> (Ü) wohl-definiert: <u>$zz:$</u> $Mat_{\underline{B}}(< ., . >)$ ist hermitesch! □

<u>*Proposition* 12.11 :</u> Sei V ein K-VR mit Basis $\underline{B} = (b_1, ..., b_n)$. Sei $(a_{ij} \in M_{nxn}(K)$ hermitesch. Dann gilt: $< ., . >_A$ ist Skalarprodukt$\Leftrightarrow \forall k = 1, ..., n$ gilt $det((a_{ij})_{i,j=1...k}) \in \mathbb{R}_{\geq 0}$

<u>*Lemma* 12.12 :</u> Sei V ein VR über K mit Basen $\underline{B} = (b_1, ..., b_n)$ und $\underline{C}$ und sei $< ., . >$ SBF/HF und sei $T := Mat_{\underline{B}}^{\underline{C}}(id_V)$, dann gilt: $Mat_{\underline{B}}(< ., . >) = T^t \cdot Mat_{\underline{C}}(< ., . >) \cdot \overline{T}$

<u>*Beweis* :</u> Schreibe $v, w \in V$ als $v = (b_1, ..., b_n) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \sum \lambda_i b_i, w = (b_1, ..., b_n) \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} = \underline{mu}$. Definition von T: $\underline{B} = \underline{C} \cdot T \Rightarrow v = \underline{B} \cdot \underline{\lambda} = \underline{C} \cdot (T \cdot \underline{\lambda}, w = \underline{B} \cdot \underline{\mu} = \underline{C} \cdot (T \cdot \underline{\mu})$, d.h. v, w haben die Koordinaten $T \cdot \underline{\lambda}$ bzw. $T \cdot \underline{\mu}$ bezüglich $\underline{C}$.
Wir erhalten: $< v, w >= \underline{\lambda}^t \cdot Mat_{\underline{B}}(< ., . >) \cdot \overline{\underline{\mu}}$ und $< v, w >= (T \cdot \lambda)^t \cdot Mat_{\underline{C}}(< ., . >) \cdot (T \cdot \underline{\mu}) = (\lambda^t (T^t Mat_{\underline{C}}(< ., . >) \overline{T}) \overline{\underline{\mu}}) \Rightarrow$ Behauptung. □

$\underline{Lemma\,12.13:}$ (Ü) $det(\overline{A}) = \overline{det(A)}$ für $A \in M_{nxn}(K)$

$\underline{Korollar\,12.14:}$ (Ü) Unter den Voraussetzungen von 12.12 gilt: $det(Mat_{\underline{B}}(<.,.>)) = det(Mat_{\underline{C}}(<.,.>)) \cdot |det(T)|^2$

$\underline{Bemerkung:}$ $det(Mat_{\underline{B}}(<.,.>))$ heißt $\underline{Diskriminante}$ von $<.,.>$ bezüglich $\underline{B}$.

Sei ab nun $(V, <.,.>)$ ein endlich-dimensionaler Hilbertraum.
$\underline{Definition\,12.15:}$ Vektoren $v_1, ..., v_r \in V$ heißen i) $\underline{orthogonal}$ $\Leftrightarrow \forall i \neq j : v_i \perp v_j (:\Leftrightarrow < v_i, v_j >= 0)$
ii) $\underline{orthonormal}$ $:\Leftrightarrow v_1, ..., v_r$ sind orthogonal und $||v_i|| = 1$ für $i = 1...r$
iii) $\underline{Orthonormalbasis}(ONB):\Leftrightarrow v_1, ..., v_r$ sind orthonormal und bilden Basis.

$\underline{Lemma\,12.16:}$ Ist $\underline{C}$ eine Basis von V, so gilt: $\underline{C}$ ist ONB$\Leftrightarrow \forall i, j \in \{1...n\} :< c_i, c_j >= \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \Leftrightarrow$ $Mat_{\underline{C}}(<.,.>) = 1_n$

$\underline{Lemma\,12.17:}$ Sind $v_1, ..., v_r \in V$ orthonormal, so sind sie l.u.

$\underline{Beweis:}$ Setze an: $\sum\limits_{i=1}^{r} \lambda_i v_i = 0$ für $\lambda_1, ..., \lambda_r \in K$ (zz:alle $\lambda_i = 0$). Bilde $< ., v_j) : 0 = \sum\limits_{i=1}^{r} \lambda_i < v_i, v_j >= \lambda_j \Rightarrow$ Behauptung. $\square$

$\underline{Lemma\,12.18 \text{ (Gram-Schmidt-Verfahren)}:}$ Sei $\underline{B} = (b_1, ..., b_n)$ Bassi von V. Definiere rekursiv: $c'_i := b_i - \sum\limits_{j=1}^{i-1} < b_i, c_j > \cdot c_j$ und $c_j = \frac{1}{||c'_i||} \cdot c'_i$ für $i = 1...n$. Dann sind $c_1, ..., c_n$ wohl-definiert und bilden ONB von V.

$\underline{Korollar\,12.19:}$ Jeder endlich-dimensionale HR besitzt eine ONB.

$\underline{Korollar\,12.20:}$ Ist $\underline{B}$ Basis von V, so gilt $det(Mat_{\underline{B}}(<.,.>)) \in \mathbb{R}_{\geq 0}$

$\underline{Korollar\,12.21:}$ Voraussetzungen wie in 12.20. Sei $A := Mat_{\underline{B}}(<.,.>) =: (a_{ij})$. Dann gilt $det((a_{ij})_{i,j=1...k}) \in \mathbb{R}_{\geq 0}\ \forall k = 1...n$

$\underline{Beweis:}$ Definiere $V_k := L(\{b_1, ..., b_k\}) \subseteq V$ (UVR),$<.,.>_k :=<.,.> |_{V_k \times V_k} : V_k \times V_k \to K$
(Ü) $<.,.>_k$ Skalarprodukt auf V_k.
Sei $\underline{B}_k = (b_1, ..., b_k)$ von $V_k \Rightarrow Mat_{\underline{B}_k}(<.,.>_k) = (a_{ij})_{i,j=1...k} \Rightarrow$ Behauptung. $\square$

$\underline{Beweis\ von\,12.18:}$ Induktion über $i \in \{1...n\}$ zeige: $c'_i \neq 0, c_1, ..., c_i$ sind orthonormal, bilden ONB von $L(\{b_1, ..., b_i\}) =: V_i$ (UVR von V)
IA: i=1: $c'_1 = b_1 \neq 0$ (da $\underline{B}$ Basis). $c_1 = \frac{1}{||b_1||} \cdot b_1 \Rightarrow ||c_1|| = 1$ und c_1 ist ONB von V_1
IS: i$\mapsto$i+1: $c'_{i+1} = b_{i+1} - \sum\limits_{j=1}^{i} < b_{i+1}, c_j > \cdot c_j$. Falls $c'_{i+1} = 0$, so folgt $b_{i+1} \in L(\{c_1, ..., c_n\}) \overset{IV}{=} L(\{b_1, ..., b_i\}) = V_i$. Widerspruch zu $b_1, .., b_n$ l.u.!
$\Rightarrow$ wir können c_{i+1} bilden.
Orthonormalität? $< c_{i+1}, c_{i+1} >= 1$ nach Def. $< c_j, c'_j >= \begin{cases} 1 & j = j' \\ 0 & j \neq j' \end{cases}$ für $1 \leq j, j' \leq i$ nach IV. Nun: für $1 \leq j' \leq i :< c'_{i+1}, c_j >=< b_{i+1}, c'_j > - \sum\limits_{j=1}^{i} < b_{i+1}, c_j > \cdot < c_j, c'_j >=< b_{i+1}, c'_j > - < b_{i+1}, c'_j >< c_j, c'_j >= 0$. D.h. $c'_{i+1} \perp c_j$ für $j = 1...i$, d.h. $c_1, ..., c_{i+1}$ sind orthonormal in $V_{i+1} \Rightarrow c_1, ..., c_{i+1}$ ist Basis von V_{i+1} $\square$

<u>*Beweis von* 12.11 :</u> Sei V ein K-VR mit Basis $\underline{B} = \{b_1, ..., b_n\}$, erfülle $A = (a_{ij}) \in M_{nxn}(K)$ die Bedingung der rechten Seite von 12.11. Sei $< .,. >:=< .,. >_{A,B}$, d.h. $< \sum_{i=1}^{n} \lambda_i b_i, \sum_{j=1}^{n} \mu_j b_j >= \sum_{i,j=1}^{n} \lambda_i \overline{\mu_i} a_{ij}$.
Induktion über $n = dimV$: IA: n=1: $A = (a_{11}$ mit $a_{11} \in \mathbb{R}_{\geq 0}$. Neue Basis $c_1 := \frac{1}{\sqrt{a_{11}}} b_1 \Rightarrow Mat_{\underline{C}}(< .,. >) = (1) \Rightarrow < .,. >$ ist positiv definit.
IS: n$\mapsto$ n+1: IV$\Rightarrow$ Für $V_n := L(\{b_1, ..., b_n\})$ ist $< .,. > |_{V_n \times V_n} : V_n \times V_n \to K$ ist positiv definit.
Denn: $Mat_{(b_1,...,b_n)}(< .,. >_n) = (a_{ij})_{i,j=1...n}$($\Rightarrow$Können IV anwenden)
Wähle ONB $c_1, ..., c_n$ von V_n, ergänze durch $c_{n+1} := b_{n+1}$ zu Basis von V.

Basiswechsel: $Mat_{\underline{C}}(< .,. >) = \begin{pmatrix} 1 & & 0 & a_{1,n+1} \\ & \ddots & & \vdots \\ 0 & & 1 & \vdots \\ a'_{n+1,1} & \dots & \dots & a_{n+1,n+1} \end{pmatrix} =: A'$. Wissen: $A' = T^t \cdot A \cdot \overline{T}$für $T \in GL_{n+1}(K) \Rightarrow (A')^* = A'$ (d.h. A' ist hermitesch).
Alternativ: $< .,. >$ ist HF bzw. SBF $\Rightarrow$ Darstellungsmatrix ist hermitesch. A' hermitesche$\Rightarrow a'_{n+1,n+1} \in \mathbb{R}$ und $a'_{n+1,i} = \overline{a'_{i,n+1}}$ für $i = 1...n+1$
Induktion mit Laplace (Ü): $det(A') = a'_{n+1,m+1} - \sum_{j=1}^{n} |a_{n+1,j}|^2$

Sei $v = \sum_{i=1}^{n+1} \lambda_i c_i \Rightarrow < v, v >= (\lambda_1, ..., \lambda_{n+1}) A' \begin{pmatrix} \overline{\lambda_1} \\ \vdots \\ \overline{\lambda_{n+1}} \end{pmatrix} = \sum_{i=1}^{n} |\lambda_i|^2 + a'_{n+1,n+1} |\lambda_{n+1}|^2 + \sum_{i=1}^{n} (\lambda_{n+1} \overline{\lambda_i} a_{n+1,i} + \lambda_i \overline{\lambda_{n+1}} \overline{a_{n+1,i}}) = \sum_{i=1}^{n} |\lambda_i + \lambda_{n+1} a_{n+1,i}| = 0$ für $i = 1...n$ und $|\lambda_{n+1}| = 0 \Leftrightarrow \lambda_1 = ... = \lambda_{n+1} = 0$ $\square$

<u>Ende</u>
Und viel Spaß und Erfolg in LA 2! ;)