Eberhard Karls Universität Tübingen

# Mathematik für Informatiker II

Sommersemester 2019

Dr. Britta Dorn

Mitschrieb von
Felix Pfeiffer

10. Februar 2020

# Inhaltsverzeichnis

# 1 Kurze Wiederholung

## 1.1 Mengen

**Definition 1.1.** *Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterscheidbaren Objekten (Elementen) unserer Anschauung oder unseres Denkens zu einem Ganzen.*

Seien $A$, $B$ Mengen

a) $x \in A$ : $x$ ist Element der Menge $A$
$x \notin A$ : $x$ ist nicht Element der Menge $A$

b) $A = \{a, b, c\}$ : $A$ besteht aus den Elementen $a, b, c$
$= \{c, a, b\}$, d.h. Reihenfolge spielt keine Rolle, Achtung: keine Wiederholungen
$B = \{A, \{1, 2\}, 3\}$
$\mathbb{N} = \{1, 2, 3, ...\}$ Menge der natürlichen Zahlen
$\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ Menge der natürlichen Zahlen mit der Null
$\mathbb{Z} = \{0, -1, 1, -2, 2, ...\}$ Menge der ganzen Zahlen

c) A $:= \{x \mid x$ besitzt die Eigenschaft $E\}A$ besteht aus allen Elementen die $E$ erfüllen
$= \{2, 4, 6, ...\}$
$= \{x \in \mathbb{N} \mid \exists k \in \mathbb{N}$ mit $x = 2 * k\}$
$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ Menge Rationaler Zahlen

d) $\emptyset$ Menge ohne Elemente, leere Menge

e) $|A|$ Anzahl der Elemente von $A$ (Kardinalität, Mächtigkeit von $A$)
z.B. $|\{a, 1, 3\}| = 3, |\emptyset| = 0$

f) $A$ Teilmenge von $B$ ($A \subseteq B$), falls gilt $x \in A \Rightarrow x \in B$
in Worten: jedes Element von $A$ ist auch Element von $B$ ($\forall x \in A : x \in B$)
Dasselbe bedeutet die Notation $B \supseteq A$ ($B$ Obermenge von $A$)
Bsp.: $\emptyset \subseteq \{1, 2\} \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{R}$
Es gilt $\emptyset \subseteq A$ für jede Menge $A$

g) $A, B$ gleich ($A = B$), falls gilt $A \subseteq B$ und $B \subseteq A$

h) $A, B := \{(a, b) \mid a \in A, b \in B\}$, die Menge aller geordneten Paare, heißt kartesisches Produkt von $A$ mit $B$
Dabei legen wir fest, $(a, b) = (a', b')$ (mit $a, a' \in A, b, b' \in B$)
$\Leftrightarrow a = a'$ und $b = b'$
Allgemein für Mengen $A_1, ..., A_n (n \in \mathbb{N})$ :
$A_1 \times A_2 \times ... \times A_n := \{(a_1, a_2, ..., a_n) \mid a_i \in A_i; \forall i = 1, ..., n\}$
die Mengen aller geordneten n-Tupel
Statt $A \times A$ schreiben wir auch $A^2$, und statt $A \times ... \times A$ auch $A^n$

Beispiel:
$A = \{1, 2, 3\}, B = \{3, 4\}$
$(1, 3) \in A \times B$
$(3, 1) \notin A \times B, (3, 1) \in B \times A$
$(3, 3) \in A \times B \in B \times A \in A \times A$
$A \times B = \{(1, 3), (1, 4), (2, 3), ...\}$

i) $A \cap B$

j) $A \cup B$

k) disjunkte Mengen

l) $A \setminus B$

m) $\bar{A}_X$

n) $\mathcal{P}(A)$

i) - n) in Extratutorium besprochen

## 1.2 Logik

**Definition 1.2.** *Eine logische Aussage ist ein Satz, mit dem eindeutig einer der Wahrheitswerte ‚wahr'(1) oder ‚falsch'(0) zugeordnet werden kann.*

Beispiele:

- 2 ist eine ungerade Zahl. **0**
- 2 ist eine Primzahl. **1**
- Ist 2 eine gerade Zahl? **keine Aussage**
- 2. **keine Aussage**
- Es gibt unendlich viele Primzahlen. **1**
- Es gibt unendlich viele Primzahlzwillinge.
  (Primzahlzwillinge: Primzahlen mit Abstand 2, z.B. 5 und 7; 11 und 13) **Aussage, Wahrheitswert unbekannt.**

Aus einfachen Aussagen kann man durch logische Junktoren (Verknüpfungen wie ‚und', ‚oder') kompliziertere bilden (Ausdrücke): Durch Wahrheitstafeln gibt man an, wie der Wahrheitswert der zusammengesetzten Aussage durch die Werte der Teilaussagen bedingt ist.

Beispiel: Negation, $\neg$
Sei $A$ eine Aussage. Die Verneinung von $A$ ist $\neg A$ („nicht $A$") und ist die Aussage, die genau dann wahr ist, wenn $A$ falsch ist.

| $A$ | $\neg A$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

Beispiele:

- $A$: 6 ist durch 3 teilbar. (1)
  $\neg A$: 6 ist nicht durch 3 teilbar. (0)
- $B$: 2,5 ist eine gerade Zahl. (0)
  $\neg B$ 2,5 ist keine gerade Zahl. (1)

Weitere Junktoren:

- **und**, $A \wedge B$: genau dann wahr, wenn $A$ und $B$ gleichzeitig wahr sind,
- **oder**, $A \vee B$: sobald mindestens eine der beiden Aussagen wahr ist, ist die Gesamtaussage wahr.
- **Implikation**, $A \Rightarrow B$: aus $A$ folgt $B$.
- **Äquivalenz**, $A \Leftrightarrow B$: $A$ ist äquivalent zu $B$.

Zwei logische Ausdrücke heißen logisch äquivalent ($\equiv$), wenn sie dieselben Wahrheitstafeln haben.
So kann man zeigen, dass beispielsweise
$A \Rightarrow B$ logisch äquivalent zu $\neg B \Rightarrow \neg A$ ist.
Statt $A \Rightarrow B$ zu beweisen, kann mal also auch $\neg B \Rightarrow \neg A$ (die Kontraposition) zeigen.

Beispiel:

- Pit ist ein Dackel $\Rightarrow$ Pit ist ein Hund. ($A \Rightarrow B$)
- Pit ist ein Hund $\Rightarrow$ Pit ist ein Dackel. ($B \Rightarrow A$, nicht logisch äquivalent zur ersten Aussage)
- Pit ist kein Dackel $\Rightarrow$ Pit ist kein Hund. ($\neg A \Rightarrow \neg B$, nicht logisch äquivalent zur ersten Aussage)
- Pit ist kein Hund $\Rightarrow$ Pit ist kein Dackel. ($\neg B \Rightarrow \neg A$, logisch äquivalent)

Achtung bei der Verneinung von Aussagen:
Gesetze von de Morgan
$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$
$\neg(A \wedge B) \equiv (\neg A \vee \neg B)$

Verneinung von Aussagen mit Quantoren:
$\neg(\forall x \in X : x$ hat Eigenschaft $E) \equiv (\exists x \in X : x$ hat **nicht** Eigenschaft $E)$
Bsp.: $\neg$ (Alle Schafe sind weiß) $\equiv$ Nicht alle Schafe sind weiß (Es gibt (mindestens) ein Schaf, dass nicht weiß ist)
$\neg(\exists x \in X : x$ hat Eigenschaft $E) \equiv (\forall x \in X : x$ hat **nicht** Eigenschaft$E)$

## 1.3 Vollständige Induktion

**Beispiel 1.3.** *Kleiner Gauß*
$1 + 2 + 3 + ... + 100 =?$

$$\begin{array}{rl} & 1 + 2 + 3 + ... + 50 \\ + & 100 + 99 + 98 + ... + 51 \\ \hline & 101 + 101 + 101 + ... + 101 \\ & = 50 * 101 = 5050 \\ & = \frac{100}{2} * 101 \end{array}$$

Allgemein für $n \in \mathbb{N}$ $1 + 2 + ... + n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

Prinzip der vollständigen Induktion

Sei $n_o \in \mathbb{N}$ vorgegeben (oft: $n_0 = 1$)
für $n \geq n_0, n \in \mathbb{N}$, Sei $A(n)$ eine Aussage, die von $n$ abhängt.
Es gelte

(1) $A(n_0)$ ist wahr („Induktionsanfang“)

(2) $\forall n \in \mathbb{N},\, n \geq n_0$ :
Ist $A(n)$ wahr, so ist $A(n+1)$ wahr („Induktionsschritt“)
Dann ist die Aussage $A(n)$ für alle $n \geq n_0$ wahr.

**Beispiel 1.4.** *Kleiner Gauß*

zu zeigen: $1 + 2 + ... + n = \frac{n(n+1)}{2}\ \forall n \in \mathbb{N}$

- Induktionsanfang: zeige $A(1)$ gilt
  $(n = 1)\ 1 = \frac{1(1+1)}{2}$ ist wahr.
- Induktionsvoraussetzung Die Aussage gilt für ein beliebiges aber festes $n \in \mathbb{N}$.
- Indunktionsschritt
  Induktionsvoraussetzung: sei $n \geq 1$
  Es gelte $A(n)$, d.h. $1 + ... + n = \frac{n(n+1)}{n}$
  Induktionsbehauptung: Es gilt $A(n+1)$ d.h. $1 + ... + n + (n+1) = \frac{(n+1)(n+2)}{2}$
  Beweis:

$$
\begin{aligned}
1 + 2 + ... + n + (n+1) &\overset{I.V.}{=} \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n^2 + n + 2n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}
$$

**Beispiel 1.5.** $A(n) : 2^n \geq n\ \forall n \in \mathbb{N} \rightarrow$ *Übungsaufgabe*

**Bemerkung 1.6.** *Für Formeln wie im vorgegebenen Bsp. benutzen wir das Summenzeichen* $\sum$ *(Sigma, großes griechisches S)*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \ \forall n \in \mathbb{N}$$

$$\underset{k=1}{1} + \underset{k=2}{2} + \underset{k=3}{3} + ... + \underset{k=n}{n}$$

weitere Bsp.:

$$\sum_{k=1}^{n} 2k = 2*1 + 2*2 + ... + 2*n$$

$$\sum_{k=4}^{n} 2k = 2*4 + 2*5 + ... + 2*n$$

$$\sum_{k=1}^{3} 7 = 7 + 7 + 7$$

*allg.* $\displaystyle\sum_{k=m}^{n} a_k = a_m + a_{m+1} + ... + a_n$ $(a_m, ..., a_n \in \mathbb{R}$

$k$ heißt Summationsindex

$$\sum_{k=m}^{n} a_k = \sum_{i_m}^{n} a_i \text{usw.}$$

Schreibweisen: $\displaystyle\sum_{k=m}^{n} a_k, \sum_{k\in\mathbb{N}} a_k, \sum_{k=1,k\neq 2}^{4} a_k = a_1 + a_3 + a_4$

für $n < m$ setzt man

$$\sum_{k=m}^{n} a_k = 0(\text{„leere Summe“}), \text{ z.B.} \sum_{k=7}^{3} k = 0$$

<u>Produktzeichen $\prod$ (Pi, großes P)</u>

$$\prod_{k=m}^{n} a_k = a_m * a_{m+1} * ... * a_n$$

für $n < m$ setze $\displaystyle\prod_{k=m}^{n} a_k = 1$ („leeres Produkt“)

## 1.4 Abbildungen

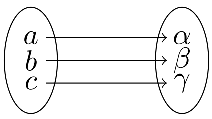
**Definition 1.7.** *Eine Abbildung (oder Funktion)*
$f\colon A \to B$ *besteht aus*

- *zwei Mengen*
  - *$A$, dem Definitionsbereich von $f$*
  - *$B$, dem Bildbereich von $f$*
- *und einer Zuordnungschrift, die jedem Element $a \in A$ genau ein Element $b \in B$, zuordnet.*

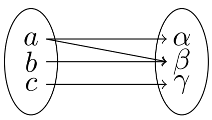
Wir schreiben dann $b = f(a)$, wenn $b$ das Bild oder den Funktionswert von $a$ (unter $f$), und $a$ (ein) Urbild von $b$ (unter $f$).

Notation: $f\colon A \to B$
$\qquad a \mapsto f(a)$

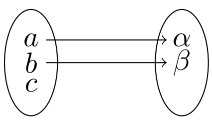
**Beispiel 1.8.** $A = \{a, b, c\}, B = \{\alpha, \beta, \gamma\}$
$f\colon A \to B, a \mapsto \alpha, b \mapsto \beta, c \mapsto \gamma$



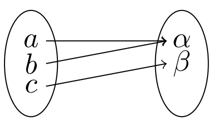

ist eine Funktion
$a$ besitzt das Bild $\alpha$
$\beta$ besitzt das (einzige) Urbild $b$



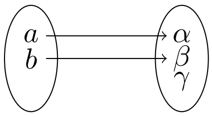

keine Funktion!
Zuordnung von $a$ nicht eindeutig




keine Funktion
$c \in A$ wird nichts zugeordnet.




Funktion in unserem Sinne.
Bild von $a$ unter $f$ ist $\alpha$.
$\alpha \in B$ besitzt Urbilder: $a$ und $b$.




ist eine Funktion
$\gamma \in B$ besitzt unter $f$ kein Urbild.

**Beispiel 1.9.**

a) $A$ Menge
$id_A \colon A \to A$
$x \mapsto x$

b) $f \colon \mathbb{R} \to \mathbb{R}$
$x \mapsto x^2$

c) "$+$„ kann als Abb. aufgefasst werden.
$+\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$(a, b) \mapsto a + b$

**Definition 1.10.**

Sei $f \colon A \to B$
$A_1 \subseteq A, B_1 \subseteq B$ Teilmengen, dann heißt

a) $f(A_1) := \{f(a) \mid a \in A_1\} \subseteq B$
das Bild von $A_1$ (unter $f$)
Bsp.: $f \colon \mathbb{N} \to \mathbb{N}, x \mapsto 2x \quad A_1 = \{1, 3\} \quad f(A_1) = f(1), f(3) = 2, 6$

b) $f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\} \subseteq A$
das Urbild von $B_1$ (unter $f$)
Bsp.: oben: $B_1 = \{8, 14, 100\} \Rightarrow f^(-1)(b_1) = \{4, 7, 50\}$

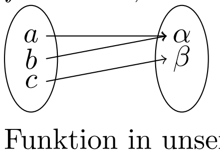
c) $f$ surjektiv, falls gilt: $f(A) = B$
(alle Elemente von $B$ werden getroffen)

d) $f$ injektiv, falls gilt: $a_1, a_2 \in A$ mit $a_1 \neq a_2 \Rightarrow f(a_1) = f(a_2)$
(kein Element von $B$ wird doppelt getroffen)

e) $f$ bijektiv falls $f$ injektiv und surjektiv ist.
(jedes Element wird genau einmal getroffen)

**Beispiel 1.11.**

$A = \{a, b, c\}, B = \{\alpha, \beta, \gamma\}$
$f \colon A \to B, a \mapsto \alpha, b \mapsto \beta, c \mapsto \gamma$




Funktion in unserem Sinne.
Bild von $a$ unter $f$ ist $\alpha$.

Die Simpsons gehen ins Kino. Jedem Familienmitglied wird einer der 100 Kinosessel zugeordnet.
$f\colon$ Simpsons $\to$ Kinosessel
$f$ ist injektiv.

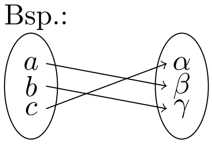
Die Simpsons verteilen eine Schachtel Donuts (20 Stück) unter allen Familienmitgliedern. Jeder bekommt mindestens einen Donut, und am Ende sind alle Donuts verteilt. $f\colon$ Simpsons $\to$ Donuts
$f$ ist surjektiv.

Die Simpsons verteilen eine Schachtel Donuts unter allen Familienmitgliedern. Alle Donuts werden verteilt, aber Maggie bekommt keinen.
$f\colon$ Simpsons $\to$ Donuts
$f$ ist weder injektiv noch surjektiv.

Die Simpsons verteile eine Schachtel Donuts unter allen Familienmitgliedern. Jeder bekommt mindestens einen Donut. Den Spinatdonut will aber niemand essen.
$f\colon$ Simpsons $\to$ Donuts
$f$ ist keine Funktion.

**Definition 1.12.**

Sei $f\colon A \to B$ bijektiv
Dann definieren wird die Umkehrfunktion
$f^{-1}\colon B \to A$, indem wir jeden $b \in B$ dasjenige $a \in A$ zuordnen für das $f(a) = b$ gilt.
Bsp.:




$$\begin{aligned} f\colon A &\to B \\ a &\mapsto \beta \\ b &\mapsto \gamma \\ c &\mapsto \alpha \end{aligned}$$

$$\begin{aligned} f^{-1}\colon B &\to A \\ \alpha &\mapsto c \\ \beta &\mapsto a \\ \gamma &\mapsto b \end{aligned}$$

**Definition 1.13.**

Seien $g\colon A \to B \quad f\colon B \to C$ Abbildungen. Dann heißt die Abbildung
$f \circ g\colon A \to C$
$x \mapsto (f \circ g)(x) = f(g(x)) \quad \forall x \in A$
die Hindereinanderausführung oder Komposition von $f$ und $g$ ($f$ nach $g$)

$$\xrightarrow{\quad f \circ g \quad}$$
$$A \overset{g}{\to} B \overset{f}{\to} C$$

Bsp.:

$$\begin{aligned} f\colon \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x+1 \end{aligned}$$

$$\begin{aligned} g\colon \mathbb{R} &\to \mathbb{R} \\ x &\mapsto 2x \end{aligned}$$

$(f \circ g)(x) = f(g(x)) = f(2x) = 2x + 1$
$(g \circ f)(x) = g(f(x)) = g(x+1) = 2x + 2$
$\Rightarrow f \circ g \neq g \circ f$

# 2 Gruppen

**Definition 2.1.** *Verknüpfung, Abgeschlossenheit*

a) Seien $X, Y$ nichtleere Mengen.
Eine Verknüpfung von "$\cdot$" (oder abstrakte Multiplikation) auf $X$ ist eine Abbildung.
$\cdot : X \times X \to Y \quad (a, b) \mapsto a \cdot b$
$a \cdot b$ (oft auch $ab$) heißt Produkt von $a$ und $b$, muss aber nichts mit der übliche Multiplikation von Zahlen zu tun haben.
Beschreibung bei endlichen Mengen oft durch Multiplikationstafeln. siehe Bsp. 2.2a

b) Eine Menge $X \neq \emptyset$ heißt abgeschlossen bezüglich einer Verknüpfung "$\cdot$" falls gilt
$a \cdot b \in X \quad \forall a, b \in X$

**Beispiel 2.2.**

a) $X = \{a, b\}$
$X \times X \to X$
$(a, b) \mapsto a \cdot b$

| $\cdot$ | $a$ | $b$ |
|---|---|---|
| $a$ | $b$ | $b$ |
| $b$ | $a$ | $a$ |

d.h. $a \cdot a = b$
$a \cdot b = b$
...

$\underline{(a \cdot a)} \cdot a = \underline{b} \cdot a = a$
$a \cdot \underline{(a \cdot a)} = a \cdot \underline{b} = b$

b) $X = \{0, 1\}$ ist abgeschlossen bezüglich der üblichen Multiplikation auf $\mathbb{Z}$.
$(0 * 0 = 0 \in X, \quad 0 * 1 = 0 \in X, \quad 1 * 0 = 0 \in X, \quad 1 * 1 = 1 \in X$
nicht abgeschlossen bezüglich der üblichen Addition "$+$"
$0 + 0 = 0 \in X, \quad 0 + 1 = 1 \in X, \quad 1 + 1 = 2 \notin X$
$X = \{1, 2\}$ ist nicht abgeschlossen bezüglich Multiplikation und Addition.

**Definition 2.3.** *Gruppe*

a) Eine Gruppe ist ein Paar $(G, \cdot)$ mit einer Menge $G \neq \emptyset$ und einer Verknüpfung $\cdot : G \times G \to G$ (d.h. $a.b \in G \quad \forall a, b \in G$ d.h. abgeschlossen) die folgende Axiome erfüllt

(1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b \in G$ (Assoziativgesetz)
(2) $\exists e \in G$ mit $a \cdot e = e \cdot a = a \quad \forall a \in G$ (neutrales Element / Einselement)
(3) $\forall a \in G \quad \exists a^{-1} \in G$ mit $a \cdot a^{-1} = a^{-1} \cdot a = e$ (inverses Element / Inverse)

b) Gilt zusätzlich

(4) $a \cdot b = b \cdot a \quad \forall a, b \in G$ (Kommutativgesetz)
so heißt $G$ kommutative oder abelsche Gruppe.

c) Ist $G$ eine edliche Menge, so heißt die Anzahl der Elemente in $G$ die Ordnung von $G$, $|G|$.

d) $(G, \cdot)$ heißt Halbgruppe, falls (1) erfüllt ist.

**Beispiel 2.4.**

a) $(G = \{1\}, \cdot)$ ist abelsche Gruppe $(e = 1, 1^{-1} = 1)$

b) $(\mathbb{Z}, +)$ ist abelsche Gruppe

(1) $a + b) + c = a + (b + c) \quad \forall a, b, c \in \mathbb{Z}$

(2) hier ist $e = 0 \quad a + 0 + 0 + a \quad \forall a \in \mathbb{Z}$

(3) Inverse zu $a$ ist $-a \quad \forall a \in \mathbb{Z} \quad a + (-a) = 0$

(4) $a + b = b + a \quad \forall a, b \in \mathbb{Z}$

c) ebenso sind $(\mathbb{Q}, +), (\mathbb{R}, +)$ abelsche Gruppen

d) $(\mathbb{Z}, \cdot)$ ist keine Gruppe
$e = 1$ ist neutrales Element, aber es gibt kein inverses Element aber (kommutative) Halbgruppe (die auch (2) erfüllt)

e) $G = 2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$ (Menge aller geraden Zahlen)
ist bezüglich + abelsche Gruppe und bezüglich * Halbgruppe

f) $G = 2\mathbb{Z} + 1 := \{2k + 1 \mid k \in \mathbb{Z}\}$ (Menge der ungeraden Zahlen)
$(G, +)$: keine Gruppe, nicht abgeschlossen bezüglich +
$(G, \cdot)$: Halbgruppe

g) weitere Gruppen später

**Satz 2.5.** *Eigenschaften von Gruppen*

Sei $(G, \cdot)$ eine Gruppe, dann gilt

a) Das neutrale Element von $G$ ist eindeutig

b) Für jedes $a \in G$ gibt es eine eindeutige Inverse

c) Für alle $a, b \in G$ gilt $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Beweis

a) Angenommen, $e_1$ und $e_2$ sind neutrale Elemente.
Dann gilt $e_1 = e_1 \cdot e_2 = e_2$ und $a = a \cdot e$

b) Angenommen $a \in G$ besitzt zwei Inversen $x$ und $y$.
Dann ist $x \overset{2.3(2)(3)}{=} x \underbrace{(ay)}_{e} \overset{2.3(1)}{=} \underbrace{(xa)}_{e} y \overset{2.3(2)}{=} y \quad$ (also $x = y$)

c) wir zeigen: Produkt ist $e$
$(a \cdot b)^{-1} \cdot (a \cdot b) = (b^{-1} \cdot a^{-1})(a \cdot b) \overset{2.3(1)}{=} b^{-1} \underbrace{(a^{-1} a)}_{e} b \overset{2.3(2)}{=} b^{-1} b \overset{2.3(2)}{=} e$

$(a \cdot b) \cdot (a \cdot b)^{-1} = ... = e$ (analog)

**Satz 2.6.** *Gleichungen lösen in Gruppen*

Sei $(G, \cdot)$ Gruppe $a, b \in G$

a) $\underbrace{\text{Es gibt genau ein}}_{\exists!}$ $x \in G$ mit $ax = b$ (nämlich $x = a^{-1}b$)

b) Es gibt genau ein $y \in G$ mit $ya = b$ (nämlich $y = ba^{-1}$)

c) Ist $ax = bx$ für ein $x \in G$ dann gilt $a = b$ (Kürzungsregel)

Beweis:

a) Existenz $x = a^{-1}b$ ist Lösung (d.h. zeige, dass $ax = b$ gilt)
$a\underbrace{a^{-1}b}_{x} \overset{2.3(1)}{=} (aa^{-1})b \overset{2.3(2)}{=} e \cdot b = b$

Eindeutigkeit
Es gelte $ax = b$
$\Rightarrow x \overset{2.3(2)}{=} e \cdot x \overset{2.3(3)}{=} (a^{-1}a)x \overset{2.3(1)}{=} a^{-1}(ax) = a^{-1}b$

b) analog (Lösung)

c) Multipliziere von rechts mit $x^{-1}$, gleiches mit $y^{-1}$

**Vorüberlegung 2.7.**

Sei $X = \{a, b, c\}$ Wir betrechten Anordnungen der Elemente von $X$
z.B.: $abc$ oder $bca$
Wie viele unterschiedliche Anordnungen gibt es? 6
Jede Anordnung lässt sich als bijektive Abbildung $\sigma \colon X \to X$ auffassen.

**Definition 2.8.**

a) Eine Permutation ist eine bijektive Abbildung einer endlichen Menge auf sich selbst. Im Allgemeinen verwendet man die Menge $\{1, ..., n\} \to \{1, ..., n\} \quad i \mapsto \sigma(i)$
als Wertetabelle in der Form $\sigma = \begin{pmatrix} 1, & 2, & ..., & n \\ \sigma(1), & \sigma(2), & ..., & \sigma(3) \end{pmatrix}$

b) Mit $S_n$ bezeichnen wir die Menge aller Permutationen von $\{1, ..., n\}$

**Beispiel 2.9.**

a) $x = \{1, 2, 3, 4\}$
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in S_4$

b) indentische Abbildung auf $\{1, ..., n\}$ ist $\sigma = \begin{pmatrix} 1, & 2, & ..., & n \\ 1, & 2, & ..., & n \end{pmatrix}$ $(1 \mapsto 1, 2 \mapsto 2)$

c) $S_1 = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}, S_2 = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$
$S_3 = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}$

**Bemerkung 2.10.**

Es gilt $|S_n| = n! = n * (n-1) + (n-2) + ... * 2 * 1$ (Beweis durch vollständige Induktion, siehe Übungsblatt 3)

**Definition 2.11.** *Produkt von Permutationen*

Wir definieren auf $S_n$ eine Verknüpfung $\circ$ über die Hintereinanderausführung / Komposition: für $\sigma, \tau \in S_n$ sei $(\sigma \circ \tau)(i) = \sigma(\tau(i))$ für $i \in \{1, ..., n\}$

**Bemerkung 2.12.**

$\circ$ ist auf $S_n$ abgeschlossen: Die Verknüpfung zweier Permutationen, ergibt wieder eine Permutation. Das liegt daran dass die komposition bijektiver Abbildungen wieder bijektiv ist
(Mathe 1)

**Beispiel 2.13.**

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3$
$\Rightarrow \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
$\sigma \circ \tau \neq \tau \circ \sigma$ (Kommutativgesetz nicht erfüllt)

**Satz 2.14.**

$(S_n, \circ)$ ist für jedes $n \in \mathbb{N}$ eine Gruppe (die sogenannte "symmetrische Gruppe")
Diese ist für $n \geq 3$ nicht abelsch.
Beweis:

- Assoziativgesetz gilt für die Komposition von Abbildungen
  $((\sigma \circ \tau)\pi)(i) = \sigma(\tau(\pi(i)) = \sigma \circ (\tau \circ \pi)(i)$
- neutrales Element ist die identitäts Abbildung $\epsilon \begin{pmatrix} 1, & 2, & ..., & n \\ 1, & 2, & ..., & n \end{pmatrix}$
  (also $\epsilon(i) = i \quad \forall i \in \{1, ..., n\}$)
  $(\sigma \circ \epsilon)(i) = \underbrace{\sigma(\epsilon(i))}_{i} = \sigma(i)$
  und $(\epsilon \circ \sigma)(i) = \epsilon(\sigma(i)) = \sigma(i) \quad \forall i \in \{1, ..., n\}$
- inverses Element $\sigma = \begin{pmatrix} 1, & ..., & n \\ \sigma(1), & ..., & \sigma(n) \end{pmatrix} \in S_n$
  ist $\sigma^{-1} \quad \sigma(1) \mapsto 1 \ \ ... \ \ \sigma(n) \mapsto n$
  Dann gilt $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \epsilon$
- Kommutativgesetz ist nicht erfüllt, siehe Bsp. 2.13

**Beispiel 2.15.**

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$

$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ $\quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ $\quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $\quad \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $\leftarrow$(“3 komm von 1“)

$\sigma^{-1} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 2 & 4 \end{pmatrix} = \epsilon \quad \sigma \circ \epsilon = \sigma$

Für welche Permutation $x \in S_4$ gilt $\sigma \circ x = \tau$ mit Satz 2.6(a) gilt $x = \sigma^{-1} \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

ebenso löse $x \circ \sigma = \tau$ Satz 2.6(b) $x = \tau \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$

**Erinnerung (Schule) Vorwissen 2.16.**

$25 : 7 = 3$ Rest 4, dh.
$25 = 3 * 7 + 4$ (für Rest gilt: $0 \leq$ Rest $< 7$)
Allgemein kann man zeigen (z.B. mit Induktion) zu gegebenen $n \in \mathbb{N}$ und $m \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ (Ouotient) und $r \in \{0, ..., m-1\}$ (Rest) mit $n = q * m + r$

**Definition 2.17.** *Konguenz, modulo m*

Seien $n, q \in \mathbb{Z}, m \in \mathbb{N} m r \in \{0, ..., m-1\}$ wie eben

a) $r$ heißt Rest bon $n$ modulo $m$, kurz $n \mod m$, $m$ heißt Modul

b) Im Falle $r = 0$ sagen wir auch: $n$ ist durch $m$ teilbar ($m$ teilt $n$), und schreiben $m \mid n$

c) Gilt für $n_1, n_2 \in \mathbb{Z}$: $n_1 \mod m = n_2 \mod m$ (d.h. bei Division durch $m$ lassen $n_1, n_2$ denselben Rest), so sagen wir $n_1$ ist konguent $n_2$ modulo $m$ und schreiben $n_1 \equiv n_2 \mod m$

**Beispiel 2.18.**

$$\begin{aligned}
7 &\mod 3 = 1 && (\text{denn } 7 = 2 * 3 + 1) \\
37 &\mod 7 = 2 && \\
42 &\mod 7 = 0 && (\text{d.h. } 7 \mid 42) \\
-6 &\mod 5 = 4 && (\text{denn } -6 = (-2)5 + 4 \rightarrow \text{ Rest muss } 0 \leq \text{ Rest } < 5 \text{ sein!}) \\
7 &\equiv 1 \mod 3 \\
37 &\equiv 2 \mod 7 \\
-13 &\equiv 1 \mod 7
\end{aligned}$$

**Bemerkung 2.19.**

a) $n_1 \equiv n_2 \mod m \Leftrightarrow \exists q_1, q_2 \in \mathbb{Z}$
$r \in \{0, ..., m-1\}$
mit $n_1 = q_1 m + r$
$n_2 = q_2 m + r$
$\Leftrightarrow n_1 - n_2 = (q_1 - q_2) m$
d.h. $m$ teilt $(n_1 - n_2)$
Also: $n_1 \equiv n_2 \mod m \Leftrightarrow (n_1 - n_2)$ ist durch $m$ teilbar

b) Ist ein Modul $m \in \mathbb{N}$ fest vorgegeben, so ist auf $\mathbb{Z}$ durch $n_1 \sim n_2 :\Leftrightarrow n_1 \equiv n_2 \mod m$ eine Äquivalenzrelation definiert (Mathe 1)
Die Zahlen $0, ..., m-1$ bilden dafür ein vollständiges Repräsentationssystem.

**Definition 2.20.**

Gegeben sei ein fester Modul $m \in \mathbb{N}$. Auf den Resten $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ definieren wir Verknüpfungen $\bigoplus$ und $\circledast$ wie folgt:
$r_1 \bigoplus r_2 = (r_1 + r_2)$
$r_1 \circledast r_2 = (r_1 * r_2)$
(Ist der Kontext klar, so benutzen wir auch $+, *$)

**Beispiel 2.21.**

a) $\mathbb{Z} = \{0, 1, 2, 3, 4\}$

| | |
|---|---|
| $2 \bigoplus 1 = 3$ | $2 \circledast 0 = 0$ |
| $2 \bigoplus 2 = 4$ | $2 \circledast 1 = 0$ |
| $2 \bigoplus 3 = 0$ | $2 \circledast 2 = 0$ |
| $2 \bigoplus 4 = 1$ | $2 \circledast 3 = 0$ |
| | $2 \circledast 0 = 0$ |

Bezüglich $\bigoplus$ besitzt jedes Element in Inverses:
Wir bezeichnen das additiv Inverse zu $x \in \mathbb{Z}_m$ mit $-x$ (das mult. Inverse zu $x$ mit $x^{-1}$ wie bisher)
$-0 = 0$
$-1 = 4$
$-2 = 3$
$-3 = 2$
$-4 = 1$
(denn $1 \bigoplus 4 = 0$, $2 \bigoplus 3 = 0$
Bezüglich $\circledast$ besitzt jedes Element (außer 0) ein Inverses:
$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

b) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

| Inverse bzl. $\bigoplus$: | Inverse bzl. $\circledast$: |
|---|---|
| $-0 = 0$ | $1^{-1} = 1$ |
| $-1 = 3$ | $2^{-1} =$ existiert nicht |
| $-2 = 2$ | $3^{-1} = 3$ |
| $-3 = 1$ | |

**Bemerkung 2.22.**

Beachte den Unterschied zwischen $a \mod m$ und $a \equiv b \mod m$ bei festem $m$ ist $a \mapsto a \mod$ Abbildung. $\mathbb{Z} \to \mathbb{Z} = \{0, ..., m-1\}$ $\equiv \mod m$ ist (Äquivalenz) Relation auf $\mathbb{Z}$

**Satz 2.23.** *Rechenregel für mod*

a) Seien $a \equiv a' \mod m$ und $b \mod \equiv b' \mod m \quad (a, a', b, b' \in \mathbb{Z}, m \in \mathbb{N})$
Dann gilt $a \pm b \equiv (a' \pm b') \mod m$ und $a * b \equiv (a' * b') \mod m$

b) Es gilt
$(a \pm b) \mod m = ((a \mod m) \pm (b \mod m)) \mod m$
$(a * b) \mod m = ((a \mod m) * (b \mod m)) \mod m$
(für Beweis a) nutzen)

Nutzen vom Bem. 2.2.3:
Gilt eine Gleichung mit $*, +$ in $\mathbb{Z}$, dann auch in $\mathbb{Z}_m$ mit $\circledast$, $\oplus$
(Achtung nicht mit Division!)

**Beispiel 2.24.**

a) Was ist $11 * 12 * 13 \mod 7$ ?
$11 * 12 * 13 = 1716 \equiv 1 \mod 7$
d.h. $11 * 12 * 13 \mod 7 = 1$
oder $11 * 12 * 13 = 132 * 13 \equiv (-1) * (-1) = 1 \mod 7$
oder $11 * 12 * 13 \equiv 4 * 5 * 6 = 120 \equiv 1 \mod 7$
oder $11 * 12 * 13 \equiv (-3) * (-2) * (-1) = -6 \equiv 1 \mod 7$

b) Welchen Rest lässt $(214\,934)^{57\,891}$ bei division durch 7?
$(214\,934)^{57\,891} = (210\,000 + 49\,000 + 35 + 1)^{57\,891} \equiv (-1)^{57\,891} = -1 \equiv 6 \mod 7$
d.h. Rest ist 6

**Definition 2.25.** *ggT (größter gemeinsamer Teiler), teilerfremd*

Seien $a_1, ..., a_n \in \mathbb{Z}$

a) Ist mindestens ein $a_i \neq 0$, so ist der größte gemeinsame Teiler $ggT(a_1, ..., a_n)$ die größte natürliche Zahl, die alle $a_1, ...a_n$ teilt.

b) Ist $ggT(a_1, ..., a_n) = 1$ so heißen $a_1, ...a_n$ teilerfremd
(Bsp.: $ggT(20, 24) = 4, \quad ggT(20, 23) = 1)$)
Berchnung des $ggT$ zweier Zahlen mittels (Erweitertem) Euklidischen Algorithmus liefert zusätzlich zu $a, b \in \mathbb{Z}$ ganze Zahlen $s, t$ mit $ggT(a, b) = s * a + t * b \to$ Mathe I

**Satz 2.26.**

Sei $m \in \mathbb{N}$

a) $(\mathbb{Z}_m, \bigoplus)$ ist abelsche Gruppe

b) $(\mathbb{Z}_m, \circledast)$ ist i.A. keine Gruppe

Beweis:

a)
- Abgeschlossenheit gilt nach Definition von $\bigoplus$
- Assoziativität/Kommutativität gilt nach Bemerkung 2.23
- neutrales Element ist 0:
  $a \bigoplus 0 = (a+0) \mod m = a \quad \forall a \in \mathbb{Z}_m$
  $0 \bigoplus a$ ebenso
- Inverses Element (vgl. Bsp. 2.21) zu $a \in \mathbb{Z}_m$ ist $m-a$, falls $a \neq 0$ und falls $a = 0$
  denn dann gilt $a \bigoplus (m-a) = (a + (m-a)) \mod m$
  $= m \mod m$
  $= 0$
  (finde die Zahl, die addiert zu $a$ das Modul $m$ ergibt) $\mathbb{Z}_9\colon -3 = 6$

b)
- Abgeschlossenheit gilt wie bei a)
- Assoziativität/Kommutativität gilt wie bei a)
- neutrales Element ist 1 da $(1 * a) \mod m = (a * 1) \mod m$
  $= a \mod m = a \quad \forall a \in \mathbb{Z}$
- Inverses Element:
  0 besitzt keine Inverse (das wäre ein $a \in \mathbb{Z}$ mit $a * 0 \mod m = 1 \rightarrow$ existiert nicht)
  welche Elemente aus $\mathbb{Z}_m$ sind invertierbar? bzgl. $\bigoplus$ (vgl. Bsp. 2.21 b))
  $x \in \mathbb{Z}_m$ invertierbar $\Leftrightarrow \exists y \in \mathbb{Z}_m$

$$
\begin{aligned}
x \in \mathbb{Z}_m \text{ invertierbar } &\Leftrightarrow \exists y \in \mathbb{Z}_m\colon x \bigodot y = 1 \\
&\Leftrightarrow \exists y \in \mathbb{Z}_m\colon (xy) \mod m = 1 \\
&\Leftrightarrow \exists y, q \in \mathbb{Z}\colon xy = q * m + 1 \text{ Rest} \\
&\Leftrightarrow \exists y, q \in \mathbb{Z}\colon xy + (-q)m = 1 \\
&\Leftrightarrow ggT(x, m) = 1
\end{aligned}
$$

Also nur die zu $m$ teilerfremden Elemente sind invertierbar
(vgl. Bsp. 2.21 a) alle in $\mathbb{Z}_5$ (außer 0) b) in $\mathbb{Z}_4$ nur 1 und 3)

**Bemerkung 2.27.** $\mathbb{Z}_m^*$, $\phi(m)$

$\mathbb{Z}_m^* \colon = \{x \in \mathbb{Z} ^| ggT(x, m) = 1\}$ ist eine Gruppe bzl. $\circledast$
$|\mathbb{Z}_m^*| = \phi(m)$ (Phi von $m$, Eulersche $\phi$-Funktion)
Anzahl der zu $m$ teilerfremden Zahlen zwischen 1 und $m$ $\quad (1 \geq z \geq m)$

**Definition 2.28.** *Untergruppen*

$(G, *)$ Gruppe, $\emptyset \neq U \subseteq G$ Teilmege
$U$ heißt Untergruppe von $G(U \leq G)$ falls $U$ bezüglich $*$ selbst eine Gruppe ist.
Insbesondere gilt dann $\forall u, v \in U$ ist $uv \in U, e$ von $G$ ist auch neutrales Element von $U$, Inversen in $U$ sind die gleichen von $G$.
angenommen: $e$ neutrales Element in $G$ aber $F$ neutrales Element in $U, f^{-1}$ Inverse von $f$ in $G$.
Dann ist $f^{-1}f = ff^{-1} = e$ auserdem $ff = f$ (da $f$ neutrales Element) $\Rightarrow f = e * f = (f^{-1}f)f$
$= f^{-1}(ff)$
$= f^{-1}f$
$= e$

**Beispiel 2.29.**

a) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$

b) $(\{-1, 1\}, *) \leq (\mathbb{Q}\backslash\{0\}, *) \leq (\mathbb{R}\backslash\{0\}, *)$

c) $(\{e\}, *)$ ist Untergruppe jeder beliebigen Gruppe mit Verknüpfung * und neutralem Element $e$

d) $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3 \quad \pi = \pi * \pi^{-1}$
$= \pi * \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \epsilon$
$\Rightarrow \{\pi, \epsilon\} \leq S_3$

# 3 Ringe und Körper

**Definition 3.1.** *Ring*

Sei $\mathbb{R} \neq \emptyset$ Menge mit zwei Verknüpfungen $+, *$

a) $(\mathbb{R}, +, *)$ heißt Ring falls gilt

   (1) $(R, +)$ ist abelsche Gruppe
   Das neutrale Element bezeichen wir hier mit 0, das zu $a \in \mathbb{R}$ inverse Element mit $-a$
   (schreibe auch $a - b$ für $a + (-b)$)

   (2) $(R, *)$ ist Halbgruppe (abgeschlossen, Assoziativ)

   (3) Es gelten die Distributivgesetze
   $a * (b + c) = (a * b) + (a * c) = ab + ac$
   $(a + b) * c = (a * c) + (b * c) = ac + bc$

b) $(R, +, *)$ heißt kommutativ, falls $*$ ebenfalls kommutativ ist, allg $a * b = b * a \quad \forall a, b \in R$

c) $(R, +, *)$ heißt Ring mit Eins, falls $(R, *)$ eine Halbgruppe ist, in der ein neutrales Element $1 \neq 0$ existiert mit $a * 1 = 1 * a = 1 \quad \forall a \in R$

d) Ist $(R, +, *)$ Ring mit Eins, so heißen die bezüglich $*$ invertierbaren Elemente Einheiten.
Das zu $a$ bezüglich $*$ inverse Element bezeichnen wir mit $a^{-1}$.
$R^* =$ Menge der Einheiten in $R$.

**Beispiel 3.2.**

a) $(\mathbb{Z}, +, *)$ Kommutativer Ring mit Eins (1)
$\mathbb{Z}^* = \{-1, 1\}$
$(\mathbb{Q}, +, *)$, $(\mathbb{Z}, +, *)$ ebenso
$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$

b) $(\mathbb{Z}, +, *)$ kommutativer Ring ohne Eins

c) trivialer Ring $(\{0\}, +, *)$

d) $m \in \mathbb{Z}$, $m \geq 2$
(alles klar, neu Distributivgesetz folgt aus Bemerkung 2.23)

e) $(\mathbb{R}^n, +, *)$
Allgemein: $R_1, ..., R_n$ Ringe, denn in $R_1 \times ... \times R_n$ Ring

**Satz 3.3.** *Rechnen in Ringen*

Sei $(\mathbb{R}, +, *)$ Ring, $a, b \in R$ Dann gilt

a) $a * 0 = o * a = 0$

b) $(-a) * b = a * (-b) = -(a * b)$

c) $(-a) * (-b) = a * b$

Beweis

a) Es gilz $a * 0 = a * (0 + 0) \overset{3.1(3)}{=} a * 0 + a * 0$
Alternative $-a * 0$ (Beweis von $0 * a$) auf beiden Seiten
erhalte $0 * a = 0$

b) Es gilt $8 - a) * b + a * b \overset{3.1(3)}{=} (-a + a) * b = 0 * b \overset{b)}{=} 0$
Also ist $(-a) * b$ Inverse von $a * b$
$\Rightarrow (-a) * b = -(a * b)$
Analog $a * (-b) = -(a * b)$

c) $$\begin{aligned}(-a) * (-b) &\overset{b)}{=} (-a * (-b)) \\ &\overset{b)}{=} -(-a * b) \\ &\overset{b)}{=} a * b\end{aligned}$$

**Bemerkung 3.4.**

a) In jedem Ring mit Eins sind 1 und -1 Einheiten.
(denn (-1)(-1)=1, d.h. -1 ist eigenes Inverse nach 3.3 c))
Es kann mer geben, es kann auch 1=-1 gelten z.B. in $(\mathbb{Z}_2, \oplus, \circledast)$

b) 0 kann nach 3.3 a) nie Einheit sein (da $1 \neq 0$)

c) In einem kommutativen Ring $R$ gilt der Binomenialsatz $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$
$n \in \mathbb{N}, a, b \in R)$

**Definition 3.5.** *Körper*

Ein kommutativer Ring $(K, +, *)$ mit Eins heißt Körper (engl. field) wenn jedes Element $0 \neq x \in K$ eine Einheit ist, d.h. wenn $K^* = K \backslash \{0\}$ gilt.

**Beispiel 3.6.**

a) $(\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$ Körper
$(\mathbb{Z}, +, *)$ kein Körper

b) $\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m \mid ggT(x, m) = 1\}$ ist Gruppe bezüglich $\circledast$ (vgl. 2.27)
$\Rightarrow (\mathbb{Z}_m, \oplus, \circledast)$ ist genau dann ein Körper wenn $m$ eine Primzahl ist.

**Satz 3.7.** *Rechnen in Körpern, Nullteilerfreiheit*

Sei $(K, +, *)$ ein Körper, $a, b \in K$. Dann gilt $a * b = 0 \Rightarrow a = 0$ oder $b = 0$
Beweis:
"$\Leftarrow$" klar ($0 * b = 0$ oder $a * 0 = 0$, Satz 3.3a))
"$\Rightarrow$" Sei $a * b = 0$, Angenommen $a \neq 0$ (d.h. $a$ besitzt Inverses)
Dann ist $b = 1 * b = (a^{-1} * a) * b = a^{-1} * \underbrace{(a * b)}_{0} = 0 \Rightarrow b$ muss 0 sein

(Gegenbeispiel zum Satz. $(\mathbb{Z}_6, \oplus, \circledast)$ kein Körper. Hier gilt $2 \circledast 3 = 0$ aber weder 2=0 noch 3=0)

**Definition 3.8.** *Polynome über K*

Sei $K$ ein Körper mit 0 und 1

a) Ein Polynom über $K$ ist ein Ausdruck $f = \underbrace{a_0 x^0}_{a_0} + \underbrace{a_1 x^1 * 1}_{a_1 x} + a_n x^n$
   $n \in \mathbb{N}, a_i \in K$ Koeffizienten von $f$ (auch $f(x)$ statt $f$)
   Ist $a_i = 0$, so kann man $0 * x^i$ bei der Beschreibung weglassen.

b) $K[x]$ = Menge aller Polynome über $K$

c) $f, g \in K[x]$ sind gleich wenn gilt $f = 0$ und $g = 0$ oder
   $f = a_0 + a_1 x + ... + a_n x^n$
   $g = b_0 + b_1 x + ... + b_n x^n$
   mit $a_n \neq 0, b_m \neq 0$
   $\Rightarrow n = m$ und $a_i = b_i \quad \forall i \in \{0, .., n\}$

**Beispiel 3.9.**

a) $f(x) = 3x^2 + \frac{2}{3}x - 1 \qquad \in \mathbb{Q}[x], \in \mathbb{R}[x]$

b) $g(x) = x^7 + x^2 + 1 \qquad \in \mathbb{Z}[x]$ (Koeffizienten sind 0 oder 1)

Wir wollen in $K[x]$ wie in einem Ring rechen können. Brauche dazu $+$ und $*$ für Polynome.

**Definition 3.10.** *Polynomring K[x]*

$K$ Körper, dann wird $K[x]$ zu einem kommutativen Ring mit Eins durch folgende Verknüpfungen:
für $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{j=0}^{m} b_j x^j$ ist $f + g := \sum_{i=0}^{max(m,n)} (a_i + b_j) x^i$
$f * g := (a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m x^m)$
$= \underbrace{a_0 * b_0}_{c_0} + \underbrace{(a_0 b_1 + a_1 b_0) x}_{c_1} + ... + \underbrace{(...) x^{n+m}}_{c_{n+m}}$
$= \sum_{i=0}^{n+m} c_i x^i$
mit $c_i = a_0 b_i + a_1 b_{i-1} + ... + a_i b_0$
$= \sum_{j=0}^{i} a_j b_{j-1}$ (Faltungsprodukt)
(setzt $a_i$ mit $i > n$ bzw. $b_j$ mit $j > m$ gleich 0)

- Einselement: $f = 1 (a_0 = 1, a_i = 0 \quad \forall i \leq 1)$
- Nullelement: $f = 0$

**Bemerkung 3.11.**

$a_0 x, a_2 x^2, ..., a_n x^n$ heißen Monome, $a_n x^n$ heißen Literale von $f = a_0 + a_1 x + ... + a_n x^n (a_n \neq 0)$

**Beispiel 3.12.**

a) in $\mathbb{Q}[x], \mathbb{R}[x]:$ Addition/Multiplikation bekannt

b) in $\mathbb{Z}[x]$: $f = 2x^3 + 1 (= 2x^3 + 0x^2 + x^1 + 1x^0)$
$g = x + 2$
$(\widehat{=}(x-1)$ da $-1 \equiv 2 \mod 3)$
$f + g = 2x^3 + x + \underbrace{(2+1)}_{=0 \mod 3} = 2x^3 + x$
$f * g = 2x^4 + \underbrace{(2*2)}_{\equiv 1 \mod 3} x^3 + x + 2.$
$= 2x^4 + x^3 + x + 2$

c) in $\mathbb{Z}_2[x]$: $f = x^2 + 1, g = x + 1$
$f + f = 0$
$g + g = (x+1)(x+1) = x^2 + x + x + 1 = x^2 + 1$

**Definition 3.13.** *Grad*

Sei $f \neq 0 \in K[x] \quad f = a_0 + a_1 x + ... + a_n x^n$ mit $a_n \neq 0$
Dann heißt $n$ der Grad von $f, grad(f) = n$
$grad(0) := -\infty$
$grad(g) = 0$, falls $g$ konstantes Polynom$\neq 0$ (z.B. $g = 1$)

**Satz 3.14.** *Gradformel*

$K$ Körper $f, g \in K[x]$
Dann ist $grad(f + g) = grad(f) + grad(g)$
(Konvention: $-\infty + (-\infty) = -\infty + n = -\infty$)

Beweis:

- stimmt für $f = 0$ oder $g = 0$
- angenommen, die Leitterme von $f$ bzw. $g$ sind $a_n x^n$ bzw. $b_m x^m (a_n, b_m \neq 0)$ dann ist $grad(f) = n, grad(g) = m$, und $\underbrace{a_n * a_m}_{\neq 0 \text{ (3.7 K Körper nullteilerfrei)}}$ $x^{n+m}$ ist Leitterm von $f * g$
  $\Rightarrow grad(f * g) = n * m$

**Korollar 3.15.**

$K$ Körper, dann gilt dass $K^*[x] = \{f \in K[x] \mid grad(f^{-1} = 0\}$
d.h. nur die konst. Polynom $\neq 0$ sind invertierbar

Beweis:
Inverse zu $f \in K[x]$ sei $f^{-1}$ dann gilt $1 = ff^{-1}$
$0 = grad(1) = f \quad grad(ff^{-1}) \overset{\text{Satz 3.14}}{=} grad(f) + grad(f^{-1})$ d.h. für $f$ konstantes Polynom
weiteres Beispiel für Körper (vgl. Mathe 1)

**Beispiel 3.16.** $\mathbb{C}$

Eine komplexe zahl $z$ ist von der Form $z = a + ib$ mit $a, b \in \mathbb{R}$ und einer "Zahl" $i$ mit $i^2 = -1$ (imaginäre Einheit)
$a=$ heißt Realteil von $z (a = Re(z))$
$b$ heißt Imaginärteil von $z (b = Im(z))$
$\mathbb{C} =$ Menge aller komplexen Zahlen
Für $z = a + ib \in \mathbb{C} \quad |z| = \sqrt{a^2 + b^2}$ Betrag von $z \quad \overline{z} = a - ib$ die zu $z$ Konjugierte
Verknüpfung $+$ und $*$: für $z = a + ib, w = a' + ib' \in \mathbb{C}$
$z + w := (a + a') + i(b + b')$
$z * w := (aa' - bb') + i(ab' + ba')$
Damit ist $\mathbb{C}$ Körper

- AG, KG, DG nachrechnen
- $0 = 0 + i0$
- additiv Inverse $-z = -a - ib = -a + i(-b)$
- $1 = 1 + i0$
- multiplikativ Inverse $z^{-1} = \frac{1}{z} = \frac{1}{a+ib} = \frac{1}{a+ib} * \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2} = \underbrace{\frac{a}{a^2 + b^2}}_{\in \mathbb{R}} + i \underbrace{\frac{b}{a^2 + b^2}}_{\in \mathbb{R}}$

$z = 2 + 3i = 2 + i * 3, \quad Re(z) = 2, \quad Im(z) = 3, \quad \overline{z} = 2 - 3i, \quad |z| = \sqrt{2^2 + 3^2} = \sqrt{13}$
$z * \overline{z} = (2 + 3i)(2 - 3i) = 2^2 + 6i - 6i - 9i^2 = 2 + 9 = 13$

**Bemerkung 3.17.**

Man kann $\mathbb{C}$ veranschaulichen in der "Gaußschen Zahlenebene"
Betrachte $z = a + ib \in \mathbb{C}$ als Punkt $(a \mid b)$ im $\mathbb{R}^2$

# 4 Vektorräume

**Definition 4.1.** *K-Vektorräume*

Gegeben sei eine Menge $V = \emptyset$, dessen Elemente wir Vektoren nennen (bez. mit kleinen lateinischen Buchstaben: $u, v, w, x, y, ...$) ein Körper $K$, dessen Elemente wir Skalare nennen (bez. mit kleinen griechischen Buchstaben: $\alpha, \beta, \lambda, \mu, ...$)
eine Verknüpfung $+ : V \times V \to V$ (Vektoraddition)
und eine Abbildung $* : K \times V \to V$ (Skalare Multiplikation)
$V$ mit $K, +, *$ heißt K-Vektorraum (auch Vektorraum über $K$), wenn gilt:

(1) $(V, +)$ ist abelsche Gruppe
(neutrales Element heißt Nullvektor, bezeichnet mit $\vec{0}$, Inverse zu $v \in V$ bezeichnen wir mit $-v$ $\quad (v + (-v) = \vec{0} \quad \forall v \in V$

(2) Für $*$ gilt für alle $\lambda, \mu \in K, v, w \in V$:

(2.1) $(\lambda \overset{\text{Mult. in } K}{*} \mu) \overset{SkalareMult.}{*} v = \lambda \overset{SkalareMult.}{*} (\mu \overset{SkalareMult.}{*} v)$ (Assoziativgesetz)

(2.2) $(\lambda \overset{\text{Add. in } K}{+} \mu)v = \lambda v \overset{\text{Vektoradd.}}{+} \mu v$ (1. Distributivgesetz)

(2.3) $\lambda(v + w) = \lambda v + \lambda w$ (2. Distributivgesetz)

(2.4) $\overset{\text{Einsel. von } K}{1} * v = v$ (oft: $K = \mathbb{R}$, reeller Vektorraum)

**Beispiel 4.2.**

$K$ beliebiger Körper

$V = K^n := \{\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \mid v_1, ..., v_n \in K\}$ (Raum der Spaltenvektoren der Länge $n$ über $K$)

$\vec{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, für $\lambda \in K, v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in V$ ist $\lambda v = \begin{pmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{pmatrix}$,

$v + w = \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + v_n \end{pmatrix}, -v = \begin{pmatrix} -v_1 \\ \vdots \\ -v_n \end{pmatrix}$

$\lambda v$ geomatrisch

a) bekannt aus Schule: $\mathbb{R}^2, \mathbb{R}^3$

b) $k = \mathbb{Z}_2, V = \mathbb{Z}_2^2 = \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1, x_2 \in \mathbb{Z}_2\}$
$V_1$ hat 4 Elemente $\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \vec{0}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
$\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (d.h.$- \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$)
$\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \vec{0} + v = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \vec{0} \quad 1 * v = v \quad \forall v \in V$

c) $K = \mathbb{Z}_5, V_2 = \mathbb{Z}_5^3 = \{\begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} \mid x_1, x_2, x_3 \in \mathbb{Z}_5\} \quad v = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, w = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} \in V_2$

$-v = \begin{pmatrix} 0 \\ 4 \\ 3 \end{pmatrix}, -w = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}, v + w = v = \begin{pmatrix} 3 \\ 3 \\ 1 \end{pmatrix}$

$1 * w = w, 2 * w = \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}, 3 * w = ...$

$|v| = 5 * 5 * 5 = 5^3 = 125$

**Beispiel 4.3.**

a) trivialer Verktorraum (Nullraum)
$K$ beliebig, $V = \{0\}$
$\vec{0} + \vec{0} = \vec{0}, \lambda \vec{0} = \vec{0}$

b) $\mathbb{R}$ ist ein $\mathbb{R}$-Vektorraum
Vektoren: reelle Zahlen
Skalare: reelle Zahlen

c) Funktionenraum
$M \neq \emptyset$ Menge, $V = \mathscr{F}(M, K) = \{f \mid f\colon M \to K\}$ Menge der auf $M$ definierten Funktionen mit Werten in $K$. (oft: $K = \mathbb{R}, f\colon M \to \mathbb{R}$, reelle Funktion)
Für $f, g \in V, \quad \lambda \in K$ sei $f + g\colon M \to K, (f + g)(x) = (f(x) + g(x) \quad \forall x \in M$
$\lambda * f\colon M \to K, \quad (\lambda f)(x) = \lambda * f(x), \quad \forall x \in M$
Dann ist $V$ mit $K, +, *$ ein Vektorraum. Nullvektor $\vec{0}$ ist $f = 0\colon M \to K, f(x) = 0$ $\forall x \in M$ (Nullfunktion: $f = 0$)

**Satz 4.4.** *Rechnen in Vektorräumen*

Sei $V$ ein K-Vektorraum, $v \in V, \lambda \in K$ Dann:

a) $0 * v = \vec{0}$

b) $\lambda * \vec{0} = \vec{0}$

c) $(-1) + v = -v$

Beweis:

a) (für $\vec{0}$ gilt: $v + (-v) = \vec{0} \quad \forall v \in V \quad (4.1(1))$
jetzt mit $0v$ statt $v$

$$\begin{aligned}
\vec{0} &= 0 * v + (-0v)) \\
&= (0 + 0)v + (-(0v)) \\
&\overset{4.1(2.2)}{=} 0 * v + 0 * v + (-(0v)) \\
&\overset{4.1(1)}{=} 0 * v + (0v + (-(0v)) \\
&= 0 * v + 0 \\
&\overset{4.1(1)}{=} 0 * v
\end{aligned}$$

b) wie a) starte mit $\vec{0} = \lambda * \vec{0} + (-\lambda\vec{0}))$

c) $v + (-1) * v \overset{4.1(2.4)}{=} 1 * v + (-1) * v \overset{4.1(2.2)}{=} (1 + (-1)) * v \overset{\text{Körper}}{=} 0 * v \overset{a)}{=} \vec{0}$ damit folgt c)

**Definition 4.5.** *Unterverktorraum*

Sei $V$ mit $K, +, *$ ein Vektorraum. Eine Teilmenge $U \subseteq V, U \neq \emptyset$ heißt Unter(vektor)raum von $V$, falls $U$ mit $K, +, *$ selbst ein Vektorraum ist.
(Bemerkung: insbesondere muss dann auch $\vec{0} \in U$ gelten)

**Beispiel 4.6.**

$V = \mathbb{R}^2, \quad U = \{\begin{pmatrix} \lambda \\ 0 \end{pmatrix} \mid \lambda \in \mathbb{R}\}$ ist Unterraum von $V$.

**Definition 4.7.** *Unterverktorraum (Klausurrelevant)*

Sei $V$ ein K-Vektorraum. $U \subseteq V$ ist Unterraum von $V$

(1) $\vec{0} \in U$

(2) $u \in U, \lambda \in K \Rightarrow \lambda u \in U$

(3) $u, v \in U \Rightarrow u + v \in U$

Beweis:
"$\Rightarrow$" $U$ ist laut Definition selbst Vektorraum, damit gelten (1), (2), (3)
"$\Leftarrow$" rechne Vektorraum-Eigenschaften aus Definition 4.1 nach.

**Beispiel 4.8.** *(Klausurrelevant)*

a) $V$ ein K-Vektorraum, $\vec{0} \neq u, v \in V \quad (u \neq v)$
Dann ist $G = \{\lambda * v \mid \lambda \in K\}$ ein Unterraum (für $v = 0$ : Nullraum, auch ok.)
$V = \mathbb{R}^2, \mathbb{R}^3$: $G$ ist Gerade durch Nullpunkt aber $G' = \{u + \lambda * v \mid \lambda \in K\}$ kein Unterraum, für $w \neq \mu v \quad (\mu \in K) \quad (\vec{0} \notin G')$
$E = \{\lambda u + \mu v \mid \lambda, \mu \in K\}$ ist Unterraum (Ebene durch $\vec{0}$)

b) $V = \mathbb{R}^3 \quad U_1 = \{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$ ist Unterraum: (benutze 4.7)

(1) $\vec{0} \in U$, denn 0+0-0=0

(2) sei $\lambda \in \mathbb{R}, v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \in U_1$ d.h. $v_1 + v_2 - v_3 = 0$
prüfe: gilt $\lambda v \in U_1$ ?
$\lambda v = \begin{pmatrix} \lambda v_1 \\ \lambda v_2 \\ \lambda v_3 \end{pmatrix}, \lambda v_1 + \lambda v_2 - \lambda v_3 = \lambda \underbrace{(v_1 + v_2 - v_3)}_{0}$ also $\lambda v \in U_1$

(3) Seien $u = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}, v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \in U_1$

d.h. $u_1 + u_2 - u_3 = 0, v - 1 + v_2 - v_3 = 0$ prüfe: gilt auch $u + v \in U_1$?

$u + v = \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ u_3 + v_3 \end{pmatrix}, (u_1 + v_1) + (u_2 + v_2) - (u_3 + v_3) = 0$

$= \underbrace{(u_1 + u_2 - u_3)}_{0} + \underbrace{(v_1 + v_2 - v_3)}_{0} = 0$ also ist $u + v \in U_1$

geometrische Interpretation von $U_1$:

$U_1 = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{pmatrix} \mid x_1, x_2 \in \mathbb{R}\} = \{x_1 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \mid x_1 + x_2 \in \mathbb{R}\}$

d.h. $U_1$ ist die Ebene durch $\vec{0}$ mit Richtungsvektoren $\begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$

c) $U_2 = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \mid x_1 + x_2 - x_3 = 1\}$ ist kein Unterraum $\quad \vec{0} \notin U_2 \quad 0 + 0 - 0 \neq 1$

d) $U_3 = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \mid x_1^2 + x_2^2 + x_3^2 \leq 1\}$ kein Unterraum: $\vec{0} \in U_3$, aber:

z.B. $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in U_3$, aber $2 * \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \notin U_3 \quad (2^2 + 0^2 + 0^2 \nleq 1) \quad$ (d.h. 4.7(2) ist verletzt)

geometrische Interpretation:
$U_3$ ist eine Kugel um 0 mit Radius 1

e) $I \subseteq \mathbb{R}$ Intervall, Mwnge $C(I)$ der stetigen Funktionen auf $I$ ist Unterraum von $\mathscr{F}(I, \mathbb{R})$

Im Folgenden sei $V$ mit $K, +, *$ ein Vektorraum.

**Definition 4.9.** *Linearkombination, lineare Unabhänigkeit*

a) Seien $v_1, ..., v_m \in V$ ein Vektor $v \in V$ heißt Linearkombination (LK) von $v_1, ..., v_m$, wenn es Skalare $\lambda_1, ..., \lambda_m$ gibt mit $v = \lambda_1 * v_1 + ... + \lambda_m * v_m \in K \quad (\sum_{i=0}^{m} \lambda_i v_i)$

b) $v_1, ..., v_m \in V$ heißen linear abhänig (l.a.) wenn es $\lambda_1, .., \lambda_m \in K$ gibt, nicht alle gleich 0 so dass $\lambda_1 v_1 + ... + \lambda_m v_m = \vec{0}$ gilt.

c) analog nennt man die Menge $\{v_1, ..., v_m\}$ l.a./l.u.
$\emptyset$ definieren wir als l.u.

**Bemerkung 4.10.**

$v_1, ..., v_m \in V$ sind also l.u. wenn aus $\sum_{i=0}^{m} = \vec{0}$ folgt dass $\lambda_1 = ... = \lambda_m = 0$ gilt. (d.h. $\vec{0}$ lässt sich nur auf triviale Weise $0 * v_1 + ... + 0 * v_m$ als LK darstellen)

**Beispiel 4.11.**

a) $V = K^n$, jedes $v \in V$ ist LK von $e_1, ..., e_n$ ("kanonische Einheitsvektoren"), wobei

$$e_i = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \leftarrow i \qquad \text{z.B.} \begin{pmatrix} 3 \\ 7 \\ -1 \end{pmatrix} = 3 * \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}}_{e_1} + 7 * \underbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}}_{e_2} - 1 * \underbrace{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}}_{e_3}$$

$$e_1, ..., e_n \text{ sind l.u.} \qquad \lambda_1 * \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \lambda_2 * \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \lambda_n * \begin{pmatrix} 0 \\ 0 \\ \vdots \\ n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ d.h. } \lambda_1 = 0, \lambda_2 = 0, \lambda_n = 0$$

b) $V = \mathbb{R}^2$ über $\mathbb{R}$: $v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ sind l.u.

Seien $\lambda_1, \lambda_2 \in \mathbb{R}$ mit $\lambda_1 v_1 + \lambda_2 v_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} + \begin{pmatrix} \lambda_1 \\ 2\lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} \lambda_1 + \lambda_2 \\ \lambda_1 + 2\lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

aus I $\lambda_1 = -\lambda_2$

in II $-\lambda_2 + 2\lambda_2 = 0 \Rightarrow \lambda_2 = 0$ in I $\Rightarrow \lambda_1 = 0$

c) $\begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$ sind l.a. in $\mathbb{Z}_5^3$, denn $1 * \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix} + 2 * \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

(sehen, oder nachrechnen wie in b))

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

**Bemerkung 4.12.**

a) $\vec{0}$ ist linear abhänig, wähle beliebiges $\lambda \in K$, dann $\lambda * \vec{0} = \vec{0}$

b) Ist von den Vektoren $v_1, ..., v_m \in V$ einer $\vec{0}$, so sind $v_1, ..., v_m$ l.a.
(z.B. $v_1 = \vec{0}$, dann ist $1 * \vec{0} + 0 * v_2 + ... + 0 * v_m = \vec{0}$)

c) ein einzelner Vektor $V \neq \vec{0}, v \in V$ ist l.u.
angenommen es gibt $\lambda \neq 0 \in K$ mit $\lambda v = \vec{0}$ dann ist
$v \overset{4.1(2.1)}{=} 1v \overset{\text{Körper } \lambda \neq 0}{=} (\frac{1}{\lambda}\lambda)v \overset{4.1(2.1)}{=} \frac{1}{\lambda}(\lambda v) = \frac{\lambda}{\lambda}\vec{0} \overset{\text{Satz 4.1b}}{=} \vec{0}$

**Beispiel 4.13.**

$V = \mathscr{F}(\mathbb{R}, \mathbb{R})$

a) $f, g \colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = x, g(x)x^2 \quad \forall x \in \mathbb{R}$ sind l.u. denn:
Seien $\lambda_1, \lambda_2 \in \mathbb{R}$ mit $\lambda_1 f + \lambda_2 f \equiv 0 \quad$ (Nullfunktion)
$\Rightarrow \lambda_1 x + \lambda_2 x^2 = 0 \quad \forall x \in \mathbb{R}$ also auch für z.B. $x = 1$, d.h. $\lambda_1 + \lambda_2 = 0$ und für $x = -1$, d.h. $-\lambda_1 + \lambda_2 = 0 \Rightarrow \lambda_1 = \lambda_2 = 0$

b) $f(x) = sin^2 x, g(x) = cos^2 x, h(x) = 3$ sind l.a. denn
$1 * f(x) + 1 * g(x) - \frac{1}{3} h(x) \vec{0}$
$sin^2 x + cos^2 x - 1 = 0 \quad \forall x \in \mathbb{R}$

**Bemerkung 4.14.**

Unendlich viele Vektoren aus $V$ heißen l.u., wenn es endlich viele (verschiedene) von ihnen l.u. sind.
Bsp.: in $\mathscr{F}(\mathbb{R}, \mathbb{R})$ sind die Monome $1, x, x^2, x^3, ...$ l.u. denn sei $x^{k1}, x^{k2}, ..., x^{kr}$ eine endliche Auswahl dieser Vektoren ($k_i \in \mathbb{N}_0$ alle verschieden) mit $\sum_{j=0}^{r} \lambda_j x^{kj} \equiv 0$
(d.h.: $0 \quad \forall x \in \mathbb{R}) \Rightarrow \lambda_1 = ... = \lambda_r = 0$
(da ein reelles Polynom $p(x)$ nur endlich viele Nullstellen besitzt, es se denn $p(x) \equiv 0$)

**Definition 4.15.** *Dimension*

Sei $n \in \mathbb{N}$

a) Falls es in $V \quad n$ l.u. Vektoren gibt, aber je $n + 1$ Vektoren aus $V$ l.u. sind, so heißt $n$ die Dimension von $V$ ($dim\, V = n$)
Für den Nullraum $V = \{\vec{0}\}$ setzen wir $dim\, V = 0$

b) Gibt es in $V$ zu jedem $m \in \mathbb{N}$ (mindestens) $m$ l.u. Vektoren, so heißt $V$ unendlich dimensional (denn $V = \infty$)
($dim\, V$ ist also die maximalzahl l.u. Vektoren in $V$)

**Beispiel 4.16.**

$dim \mathscr{F}(\mathbb{R}, \mathbb{R}) = \infty$, denn für jedes $m \in \mathbb{N}$ sind $1, x, x^2, ..., x^m$ l.u. (Bem./Bsp. 4.14)

**Definition 4.17.** *Basis*

Die Vektoren $v_1, ... v_m \in V$ (oder auch die Menge $B = \{v_1, ..., v_m\} \in V$) heißen Basis von $V$, falls sich jeder Vektor $w \in V$ eindeutig als LK von $v_1, ..., v_m$ darstellen lässt, also

(1) $\forall w \in V \quad \exists \lambda_1, ..., \lambda_m \in K$ mit $\sum_{i=1}^{m} \lambda_i v_i$

(2) gilt zusätzlich $w = \sum_{i=1}^{m} \mu_i v_i$ mit $\mu_i, ..., \mu_m \in K$, so folgt $\mu_1 = \lambda_1, ..., \mu_m = \lambda_m$

**Beispiel 4.18.**

a) $e_1, ..., e_n$ Basis von $\mathbb{R}^n(K^n)$ "Kanonische Basis"

b) $v_1 = \begin{pmatrix}1\\1\end{pmatrix}, v_2 = \begin{pmatrix}0\\1\end{pmatrix}$ bilden Basis von $\mathbb{R}^2$ z.B. ist $\begin{pmatrix}5\\7\end{pmatrix} = 5 * \begin{pmatrix}1\\1\end{pmatrix} + 2 * \begin{pmatrix}0\\1\end{pmatrix}$, allgemein:
sei $w = \begin{pmatrix}w_1\\w_2\end{pmatrix} \in \mathbb{R}^2$ beliebig

(1) $w = \underbrace{w_1}_{=\lambda_1} \begin{pmatrix}1\\1\end{pmatrix} + \underbrace{w_2 - w_1}_{=\lambda_2} \begin{pmatrix}0\\1\end{pmatrix}$ (darstellbar)

(2) sei $w = \mu_1 \begin{pmatrix}1\\1\end{pmatrix} + \mu_2 \begin{pmatrix}0\\1\end{pmatrix}$, d.h. $\begin{pmatrix}w_1 = \mu_1 + \mu_2 * 0\\ w_2 = \mu_1 + \mu_2\end{pmatrix} \Rightarrow \mu_1 = w_1 = \lambda_1, \mu_2 = w_2 - \mu_1 = w_2 - w_1 = \lambda_2$ (Eindeutigkeit)

**Bemerkung 4.19.** *Koordinaten, geordnete Basis*

Sei $B = \{v_1, ..., v_n\}$ eine Basis von $V$, $w \in V$. Seien $\lambda_1, ..., \lambda_n$ die (eindeutig bestimmten!) Skalare mit $w = \lambda_1 v_1 + ... + \lambda_n v_n$. Dann ordnen wir $w$ den Vektor $\begin{pmatrix}\lambda_1\\ \vdots \\ \lambda_n\end{pmatrix} \in K^n$ zu.

(Koordinatenvektor von $w$ bezüglich $\tilde{B}$, mit $\tilde{B} = (v_1, ..., v_n)$ geordnete Basis von $V$ $\lambda_1, ..., \lambda_n$ Koordinaten von $w$)
Im Bsp. 4.18 b) ist $\begin{pmatrix}w_1\\ w_2 - w_1\end{pmatrix}$ der Koordinatenvektor von $w$ bezüglich $\tilde{B} = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$
Beachte: Hier spielt die Reihenfolge, in der die Basisvektoren aufgelistet werden, eine Rolle!
$\rightarrow$ geordnete Basis, Schreibweise als Tupel $(..., ..., ...)$ statt Menge $\{..., ..., ...\}$ speziell von $V = K^n$ für die kanonische Basis $\tilde{B} = (e_1, ..., e_n)$ spricht man von kartesischen Koordinaten.
z.B. Koordinaten $v = \begin{pmatrix}7\\-3\\0\end{pmatrix}$ bezüglich $\tilde{B}$ sind $\begin{pmatrix}7\\-3\\0\end{pmatrix}$

**Satz 4.20.** *1. Zusammenhang Dimension / Basis*

Gegeben sei $V$ mit $dmi\, V = n \in \mathbb{N}$ $v_1, ..., v_n$ l.u. (existiert nach Definition von $dim\, V$)
$\Rightarrow \{v_1, ..., v_n\}$ Basis
Beweis:

(1) $w \in V$ beliebig $\Rightarrow v_1, ..., v_n, w$ sind $n + 1$ Vektoren, also l.a. nach Definition 4.15
$\Rightarrow \exists \lambda_1, ..., \lambda_n, \lambda \in K$, nicht alle gleich 0, mit $\lambda_1 v_1 + ... + \lambda_n, v_n + \lambda_w = \vec{0}$
Nun ist $\lambda \neq 0$ (sonst $\lambda_1 v_1 + ... + \lambda_n v_n = 0$, nicht alle $\lambda_i = 0$, also $v$ l.a)
$\Rightarrow w \frac{-\lambda_1 v_1}{\lambda} - ... - \frac{\lambda_n v_n}{\lambda}$ d.h. $w$ ist LK von $v_1, ..., v_n$

(2) Sei $w = \sum_{i=0}^{n} \underbrace{(\lambda_i - \mu_i) v_i}_{=0\, \forall i \text{ da } v_1 \text{ l.a.}} \Rightarrow \lambda_i = \mu_i \quad \forall i$

**Satz 4.21.**

Gegeben seien $m$ Vektoren $v_1, ..., v_m$. Dann sind je $m + 1$ LK von $v_1, ..., v_m$ l.a.
Beweis: Vollständige Induktion nach $m$

**Beispiel 4.22.** *Bsp. 4.18 a) genauer*

$V = K^n$ über $K$: $e_1, ..., e_n$ sind l.u. (Bsp. 4.11 a)) jeder Vektor $v \in V$ ist LK von $e_1, .., e_n$ (4.11 a))

$n+1$ Vektoren aus $V$ sind also $n+1$ LK von $e_1, ..., e_n \overset{4.21}{\Rightarrow}$ l.a. $\Rightarrow dim\, V = n$ und (Satz 4.20) $e_1, ..., e_n$ bilden Basis $K^n$

**Satz 4.23.** *2. Zusammenhang Dimension / Basis*

Sei $B = \{v_1, ..., v_n\}$ Basis von $V \Rightarrow v_1, ..., v_n$ l.u. und $dim\, V = n$
Beweis:

(1) jedes $v \in V$, also auch $\vec{0}$ (lässt sich eindeutig als LK von $v_1, ..., v_n$ schreiben (Definition Basis)
$\Rightarrow$ triviale Darstellung $\vec{0} = 0 + v_1 + ... + 0 * v_n$ einzig mögliche
$\Rightarrow v_1, ..., v_n$ l.u.

(2) nach (1) gibt es $n$ l.u. Vektoren in $V$, je $n+1$ Vektoren sind $n+1$ LK von $v_1, ..., v_n$ nach 4.21 l.a.
$\Rightarrow dim\, V = n$

**Korollar 4.24.**

Je zwei Basen eines n-dimensionalen Vektorraums bestehen aus gleich vielen, nämlich $n$ Vektoren.

**Satz 4.25.** *Austauschlemma*

Sei $B = \{v_1, ..., v_n\}$ Basis von $V$, sei $\vec{0} \neq w \in V, w = \sum_{i=0}^{n} \lambda_i v_i$. Ist $\lambda_j \neq 0$ für ein $j \in \{1, ..., n\}$, so bilden die Vektoren $v_1$ bis $v_{j-1}, w, v_{j+1}, ..., v_n$ ebenfalls eine Basis von $V$.
(d.h. kann $v_j$ gegen $w$ austauschen wenn $\lambda_j \neq 0$ in LK von $w$)
Beweis:
Sei o.B.d.A. (ohne Beschränkung der Allgemeinheit) $\lambda_1 \neq 0$
wir zeigen: $w_1, v_1, ..., v_n$ sind l.u. (das genügt nach Satz 4.20 und 4.23)
Sei dazu $\mu_1 w + \mu_2 v_2 + ... + \mu_n v_0 = \vec{0} \quad (\mu_i \in K)$
$\Rightarrow \underbrace{\mu_1 \lambda_1 v_1}_{=0} + (\underbrace{\mu_1 \lambda_2 v_2}_{=0}) v_2 + ... + (\mu_1 \lambda_n + \mu_n) v_n = \vec{0}$
$\Rightarrow \mu_1 = 0 \Rightarrow \lambda_1 \neq 0 \quad \mu_2 = \mu_3 = ... = \mu_n = 0 \Rightarrow$ Beh.

**Satz 4.26.** *Steinitz'scher Austauschsatz*

$v_1, ..., v_n$ Basis von $V$. Sei $w_1, ..., w_m \in V$ l.u. $(\Rightarrow m \leq n)$
Dann kann man aus den $n$ Vektoren $v_1, ..., v_n n-m$ Stück auswählen, die zusammen mit $w_1, ..., w_m$ eine Basis von $V$ bilden.
Beweis: wende Satz 4.25 sukzessive an:

1) $w_1 \in V$, d.h. $w_1 = \sum_{j=1}^{n} \lambda_j v_j$, wären alle $\lambda_j = 0$, so wäre $w_1 = \vec{0}$, dann aber (Bem 4.12) $w_1, ..., w_m$ nicht l.u. Also mindestens ein $\lambda_j$ ist $\neq 0$, o.B.d.A. $\lambda_1 \neq 0$
$\Rightarrow$ kann $v_1$ austauschen, 4.25 $w_1, v_2, ..., v_n$ Basis von $V$.

2) $w_2 \in V$, d.h. $w_2 = \sum_{j=2}^{n} \mu_j v_j$ wären $\mu_2 = ... = \mu_n = 0$, so wäre $w_2 = \mu_1 * w_1$, also $w_1, w_2$ l.a Also: mindestens ein $\mu_j (j = \{2, ..., n\} \neq 0$, o.B.d.A. $\mu_2 \neq 0$.
$\Rightarrow$ kann $v_2$ austauschen, 4.25 $w_1, w_2, v_3, ..., v_n$ Basis von $V$

3) usw.

**Korollar 4.27.** *Basisergänzungssatz*

$V$ endl. $dim$ VR. Jede l.u. Teilmenge von $V$ lässt sich zur Basis von $V$ ergänzen.
Beweis: wähle bel. Basis von $V$ und tausche mittels Satz 4.26 aus.

**Beispiel 4.28.**

$V = \mathbb{R}^4$

$$u_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, u_2 = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^4$$

$u_1, u_2$ sind l.u.
Wie kann man $u_1, u_2$ zu einer Basis von $\mathbb{R}^4$ ergänzen?
Austauschsatz (4.24/4.26/4.27)
$\{e_1, e_2, e_3, e_4\}$ Kanonische basis von $V$ $\quad u_1 = 1 * e_1 + 2 * e_2 + 0 * e_3 + 1 * e_4$
$\Rightarrow \{u_1, e_2, e_3, e_4\}$ Basis von $V$ ($e_1$ gegen $u_1$ getauscht)
$u_2 = 0 * v_1 + 2 * e_2 + 1 * e_3 + 0 * e_4$
$\Rightarrow \{u_1, e_2, u_2, e_4\}$ Basis von $V$ ($e_3$ gegen $u_2$ getauscht)

**Definition 4.29.** *erzeugter UR*

Sei $V$ K-VR, $M \subseteq V$

a) Der vom $M$ erzeugte oder aufgespannte Unterraum $< M >_K$ (oder nur $< M >$) ist die Menge aller endl. LK, die man mit Vektoren aus $M$ bilden kann,
also $< M >_K := \{\sum_{j=1}^{m} \lambda_i v_i \mid \lambda_i \in K, v \in M, n \in \mathbb{N}\}$
$< \emptyset >_K := \{\vec{0}\}$ für $M = \{v_1, ..., v_n\}$ schreiben wir auch $< v_1, ..., v_n >_K$

b) Ist $V =< M >_K$ so heißt $M$ ein Erzeugendensystem von $V$.

**Bemerkung 4.30.**

a) $< M >_K$ ist tatsächlich ein UR (wegen 4.7), und zwar der kleinste, der $M$ enthält:
$M \subseteq < M >_K$ gilt, und $U$ ein UR von $V$ mit $m \subseteq U$, so enthält $U$ alle endl. LK von El. aus $M$.
(4.7) $\Rightarrow < M >_K \subseteq U$
$\Rightarrow U$ kann nicht kleiner als $< M >_K$ sein.

b) Nach unseren Sätzen über $dimV$ gilt $dim(< v_1, ..., v_m >_K) \leq m$, und
$dim(< v_1, ..., v_m >_K) = m$ wenn $v_1, ..., v_m$ l.u. sind.

c) Man nennt $M \subseteq V$ eine Basis von $V$ wenn $< M >_K = V$ gilt und $M$ l.u. ist.
Dieser "neue"Basisbegriff stimmt im Falle $dimV < \infty$ mit dem bisherigen überein, gilt aber auch für $dimV = \infty$
z.B. ist damit $M = \{1, x, x^2, ...\}$ eine Basis von $\{p \colon \mathbb{R} \to \mathbb{R}, p \text{ ist Polynom } \} \subseteq \mathscr{F}(\mathbb{R}, \mathbb{R})$.

**Satz 4.31.** *Schnitt und Summe von UR*

$V$ ein k-VR, $U_1, U_2$ Unterraum von $V$

a) $U_1 \cap U_2 := \{u \in V \mid u \in U_1$ und $U_2\}$ (Durch)schnitt von $U_1$ und $U_2$ ist UR von $V$

b) $U_1 + U_2 := \{u_1 + u_2 \mid u_2 \in U_1, u_2 \in U_2\}$ Summe von $U_1, U_2$ ist UR von $V$
Beweis: prüfe UR-Kriterien (4.7)

   a) in moodle

   b) (1) $\vec{0} \in U_1 + U_2 \quad \vec{0} = \vec{0} + \vec{0}$

      (2) sei $v \in U_1 + U_2$, d.h. $v = u_1 + u_2$
      $\lambda \in K$, dann ist $\lambda v = \lambda(u_1 + u_2) = \underbrace{\lambda u_1}_{\in U_1} + \underbrace{\lambda u_2}_{\in U_2} \in U_1 + U_2$

      (3) seien $v = \underbrace{u_1}_{\in U_1} + \underbrace{u_1}_{\in U_1} \quad w = \underbrace{u_1}_{\in U_1} + \underbrace{u_1}_{\in U_1} \in U_1 + U_2$

**Bemerkung 4.32.**

a) 4.31 a) gilt auch für unendlich viele UR, b) für endlich viele

b) $U_1 \cup U_2$ ist im Allgemeinen kein UR

c) Der Schnitt zweier UR ist nie leer ($\vec{0}$ ist in jedem UR)

**Beispiel 4.33.**

$v, w \in \mathbb{R}^2, v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, w = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$
$G_1 =< v >_{\mathbb{R}}= \{\lambda v \mid \lambda \in \mathbb{R}\}$
$G_2 =< w >_{\mathbb{R}}= \{\mu w \mid \mu \in \mathbb{R}\}$
Geraden durch $\vec{0}$, sind UR

a) $G_1 + G_2 = \{\lambda v + \mu w \mid \lambda, \mu \in \mathbb{R}\}$
Ebene durch $\vec{0}$, ist UR (hier ganz $\mathbb{R}^2$)

b) $G_1 \cap G_2 = \{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$

**Satz 4.34.** *Dimensionsformel für Unterräume*

$V$ K-VR, $dimV$ endlich ($< \infty$)
$U, W$ Unterräume von $V$, dann gilt $dim(U + W) = dimU + dimW - dim(U \cap W)$
(insbesondere: falls $U \cap W = \{\vec{0}\}$, dann nur Summe)

# 5 Matritzen und Lineare Gleichungssysteme

**Definition 5.1.**

a) Seien $m.n \in \mathbb{N}, K$ Körper
Eine $m \times n$ Matrix $A$ über $K$ ist ein rechteckiges Schema
$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$
mit $m$ Zeilen und $n$ Spalten und Einträgen $a_{ij}(1 \leq i \leq m, 1 \leq j \leq n) \in K$
Schreiweise $A = (a_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \quad A = (a_{ij})$

b) $M_{m,n}(K) =$ Menge aller $m \times n$ Matritzen über $K$
$M_n(K) =$ Menge aller $n \times n$ Matritzen über $K$ (quadratische Matritzen)

c) Ist $A \in M_{m,n}(K)$ so erhält man die zu $A$ transponierte Matrix $A^T_{n,m}(K)$
$$A^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & \vdots \\ \vdots & & \ddots & \vdots \\ a_{nm} & \cdots & \cdots & a_{mn} \end{pmatrix}$$, indem man Zeilen und Spalten der Matrix tauscht.
Bsp.: $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 4 \\ 3 & 6 \end{pmatrix}$
Es gilt $(A^T)^T = A$

d) $1 \times n-$Matrix: Zeilenvektor der Länge $n$
$m \times 1-$Matrix: Spaltenvektor der Länge $m$
$$0 = 0_{m,n} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ (alle } a_{ij} = 0)$$
$$E = E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix} \quad n \times m \text{ Einheitsmatrix}$$
(also $E_n = (\delta_{ij})$ mit $\delta_{ij} = \{\substack{1 \cdots i=j \\ 0 \cdots i \neq j}\}$)

e) $M_{m,n}(K)$ lässt sich zu einem K-VR machen, Vektoren sind Matritzen. Brauche Addition und Skalare Multiplikation für $A(a_{ij}), B(b_{ij}) \in M_{m,n}(K)$ (beide vom selben Typ) und $\lambda \in K$ ist.
$A + B := (a_{ij} + b_{ij})_{\substack{i \in 1,\ldots,m \\ j \in 1,\ldots,n}}$ und
$\lambda * A := (\lambda * a_{ij})_{\substack{i \in 1,\ldots,m \\ j \in 1,\ldots,n}}$
$Mm, n(K)$ ist damit VR, Vektoren sind Matritzen, $\vec{0}$ ist 0 (Nullmatrix)

Basis wäre z.B.: $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}, \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & 1 \end{pmatrix}$

$dim(M_{m,n}(K)) = m * n$

f) Für $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in M_{m,n}(K)$ und $B = (b_{jk})_{\substack{j=1,\dots,n \\ k=1,\dots,l}} \in M_{n,l}(K)$ ist das Matrixpordukt $A * B$ definiert durch $A * B = (c_{ik})_{\substack{i=1,\dots,m \\ k=1,\dots,l}} \in M_{m,l}(K)$
$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + ... + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk}$ ($i$-te Zeile von $A$, $k$-te Spalte von $B$)
$A * B$ ist nur deff., wenn Anzahl der Spalten von $A$ = Anzahl der Zeilen von $B$ ist.

g) $M_n(K)$ bildet mit $+, *$ ein Ring mit Eins $(E_n)$
$A \in M_n(K)$ heißt Invertierbar falles es $\exists A^{-1} \in M_n(K)$ mit $AA^{-1} = A^{-1}A = E_n$

**Beispiel 5.2.**

a) $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & 1 \end{pmatrix} \in M_{2,3}(\mathbb{R})$

$A + B = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, 3 * B = \begin{pmatrix} 0 & 0 & -9 \\ 3 & 0 & 3 \end{pmatrix}, A * B$ nicht def.

$B^T = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ -3 & 1 \end{pmatrix} \in M_{3,\mathbb{R}}, A * B^T = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 2 \end{pmatrix} * \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -9 & 4 \\ -6 & 1 \end{pmatrix} \in M_{2,2}(\mathbb{R})$

$B^T * A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ -3 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 2 \\ 0 & 0 & 0 \\ -2 & -6 & -7 \end{pmatrix} \in M_{3,3}(\mathbb{R})$

Matrixmultiplikation ist i.A. nicht kommutativ (auch für $M_n(K)$!)

b) $A = \begin{pmatrix} 1 & 2 & 0 \end{pmatrix} \in M_{1,3}(\mathbb{Z}_3), B = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} \in M_{3,1}(\mathbb{Z}_3)$

$A * B = \begin{pmatrix} 1 & 2 & 0 \end{pmatrix} * \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} = 0 \in M_{1,1}(\mathbb{Z}_3)$

$B * A = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 2 & 1 & 0 \\ 1 & 2 & 0 \end{pmatrix} \in M_{3,3}(\mathbb{Z}_3)$

**Bemerkung 5.3.** *Rechenregeln (wie bisher in Ringen/Vektorräumen)*

$A, A_1, A_2 \in M_{m,n}(K)$
$B, B_1, B_2 \in M_{n,p}(K)$
$C \in M_{p,q}$
$\lambda \in K$

a) $(A * B) * C = A * (B * C)$

b) $(A_1 + A_2) * B = A_a * B + A_2 * B$

c) $A(B_1 + B_2) = A * B_1 + A * B_2$

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

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

**Definition 5.4.** *LGS*

a) Allg. Form eines linearen Gleichungsystems (LGS) über Körper $K$

$$\circledast \begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{12}x_2 + ... + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{12}x_2 + ... + a_{mn}x_n = b_n \end{cases}$$

$m$ Gleichungen, $n$ Unekannte $x_1, ..., x_n$, Koeffizienten $a_{ij} \in K$
rechte Seite: $b_1, ..., b_m \in K$

b) LGS heißt homogen, falls $b_1 = ... = b_m = 0$, sonst inhomogen

c) setzt man $A = \begin{pmatrix} a_1 & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(K)$ (Koeffizientenmatrix), $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m$,

so lässt sich $\circledast$ in Matrixform schreiben als $Ax = b$ $\quad (x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix})$

d) sind $s_1, ..., s_n$ Spalten von $A$, so lässt sich $\circledast$ in Spaltenform schreiben als $x_1 * s_1 + ... + x_n s_n = b$
$x_n\,(\,) + ... + x_n\,(\,) = (\,)$
Beachte: Ein homogenes LGS hat immer mindestens eine Lösung nämlich $\vec{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$,
$(x_1 = ... = x_n = 0)$, die triviale Lösung (Null-Lösung)

**Bemerkung 5.5.**

Aus 5.4 c) ergibt sich dass $\delta\colon {}^{K^n \to K^m}_{x \mapsto Ax}$ für $A \in M_{m,n}(K), x \in K^n$ eine Abbildung ist, die Vektoren (aus $K^n$) auf Vektoren (aus $K^n$) abbildet. (Bsp.: Folien)

**Satz 5.6.**

a) Die Menge der Lösungen des homogenen LGS $Ax = \vec{0}$ bildet ein Vektorraum von $K^n$.

b) Ist das inhomogene LGS $Ax = b$ lösbar und $x_0 \in K^n$ irgendeine spezielle Lösung, so erhält man alle Lösungen $\{x \in K^n \mid Ax = b\}$ durch $\{x_0 + y \mid Ay = 0\}$
Ist also $U$ der lösbare Raum des zugehörigen LGS $Ax = \vec{0}$, so ist die Lösungsmenge von $Ax = b$ vo der Form $x_0 + U$.
(Das nennt man einen affinen UR, UR $U$ verschoben um $x_0$)

Beweis:

a) mit UR Kriterium 4.7

   (1) $\vec{0}$ ist Lösung

   (2) sind $x_1, x_2$ Lösung, dann gilt $Ax_1 = \vec{0}, Ax_2 = \vec{0} \Rightarrow \vec{0} = Ax_1 + Ax_2 \overset{5.2c)}{=} A(x_1 + x_2)$ d.h. $x_1 + x_2$ ist Lösung

   (3) analog, benutze 5.3 d)

b) Sie $Ax_0 = b$
Ist $Ay = \vec{0}$, dann $A(x_0 + y) \overset{5.3c)}{=} \underbrace{Ax_0}_{=b} + \underbrace{Ay_0}_{=0} = b$ (d.h. $x_0 + y$ löst inh. LGS)
umgekehrt:
$Ax = b$
$\Rightarrow \underbrace{Ax}_{=b} + \underbrace{Ax_0}_{=b} = A(x - x_0) = \vec{0}$, also $(x - x_0) \in U$
wegen $x = x_0 + \underbrace{(x - x_0)}_{\in U}$ ist $x \in x_0 + U$

**Fragen 5.7.**

- Wann hat $Ax = b$ mindestens/genau eine Lösung?
- Wie groß ist die $dim$ des Lösungsraums von $Ax = 0$?
- Wie bestimmt man alle Lösungen von $Ax = b$?

Diese Fragen lassen sich mittels des Gauß-Algorithmus beantworten ($\rightarrow$ Folien) bis 5.13 a)

**Beispiel 5.13.**

a) $$\begin{pmatrix} 0 & 2 & 1 \\ 3 & 2 & 2 \\ 6 & 4 & 4 \end{pmatrix} \xrightarrow{I \leftrightarrow II} \begin{pmatrix} 3 & 2 & 2 \\ 0 & 2 & 1 \\ 6 & 4 & 4 \end{pmatrix} \xrightarrow{I * \frac{1}{3}} \begin{pmatrix} 1 & \frac{2}{3} & \frac{2}{3} \\ 0 & 2 & 1 \\ 6 & 4 & 4 \end{pmatrix} \xrightarrow[III: I*6-III]{II:OK} \begin{pmatrix} 1 & \frac{2}{3} & \frac{2}{3} \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{II * \frac{1}{2}} \begin{pmatrix} 1 & \frac{2}{3} & \frac{2}{3} \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix}$$
$rang = 2$ (2 Stufen)

**Definition 5.14.**

Der Zeilensprung einer Matrix $A$ ist die Maximalzahl l.u. Zeilen von $A$. D.h. sind $z_1, ..., z_m$ die Zeilen von $A$, da. Zeilenrang=$dim < z_1, ..., z_m >_K$
Analog: Spaltenrang
Es gilt Zeilenrang($A$)=Spaltenrang($A^T$)

**Satz 5.15.**

Elementare Zeilenumformungen (ZUF) ändern den Zeilenrang und den Spaltenrang
Beweis: (Zeilenrang)

(1) $< z_1, ..., z_m >=< z_1, z_2 + \lambda z_1, ..., z_m >$ $\quad (\lambda \in K)$

(2) $< z_1, ..., z_m >=< \lambda z_1, z_2, ..., z_m >$ $\quad \lambda \neq 0$

(3) $< z_1, ..., z_m =< z_2, z_1, ..., z_m >$

**Bemerkung 5.16.**

Bei einer Matrix in Zeilenstufenform ist der Rang direkt ablesbar: er ist die Anzahl der Zeilen $\neq \vec{0}$.
Der Gauß-Algorithmus (5.12) liefert also (wegen 5.15) ein einfaches Verfahren zur Rangbestimmung.
(Bsp.: Matrix im Bsp. 5.13 a) hat Rang 3, in 5.13 b) Rang 2)

**Satz 5.17.**

Für jede Matrix $A \in M_{m,n}(K)$ gilt Zeilenrang($A$)=Spaltenrang($A$)
Beweis: Bringe Matrix $A$ auf Zeilenstufenform (mit 5.12). Sei $r$ die Anzahl der Stufen, dann sind die Stufenspalten $s_{j1}, ..., s_{jr}$ l.u.
Also: Spaltenrag($A$)≥Zeilenrang($A$)=Spaltenrang($A^T$)≥Zeilenrang($A^T$)=Spaltenrang($A$)
⇒ überall gilt Gleichheit ⇒ Beh.

**Definition 5.18.**

Für $A \in M_{m,n}(K), B \in M_{n,p}(K)$ gilt $rg(AB) \geq rg(A)$, $rg(AB) \geq rg(B)$
Beweis:

$$B = (b_1, ..., b_p) \Rightarrow A*B = (A*b_1, ..., A*b_p) \text{ und } A*b_k = (a_1, ..., a_n) \underbrace{\begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix}}_{\text{Spalte } b_k} = b_{1k}*a_1 + ... + b_{nk}*a_n$$

$$\Rightarrow \qquad \underbrace{A * b_k}_{\text{ist LK von Spalten von } A} \qquad \forall K \in \{1, ..., p\}$$

$\Rightarrow rg(AB) \geq dim < a_1, ..., a_n > \overset{5.17}{=} rg(A)$
$rg(AB) = rg((AB)^T) = rg(B^T A^T) \geq rg(B^T) \overset{5.17}{=} rg(B)$

**Beispiel 5.19.**

Gauß-Algorithmus zur Lösung von LGS → Folien

**Korollar 5.20.**

a) $Ax = b$ ist genau dann lösbar, wenn $rb(a, b) = rg(A)$

b) $Ax = b$ ist genau dann eindeutig lösbar wenn $rg(A, b) = rg(A) = n$
($n$ = Anzahl der Unbekannten)

c) Dimension des Lösungsraums von $Ax = \vec{0}$ ist $n - rg(A)$
($\underbrace{x_{r+1}, ..., x_n}_{n-r \text{ Stück}}$ sind frei wählbar)
Beweis: folgt aus 5.29

**Definition 5.21.**

Der Lösungsraum eines homogenen LGS $Ax = \vec{0}$ wird auch als Kern von $A$ bezeichnet. $kerA$
(Es gilt also $dim\, kerA)n - rg(A))$

**Beispiel 5.22.** *LGS über $\mathbb{R}$*

a) $x_1 + 2x_2 + x_3 + x_4 = 0$
$x_1 - x_2 + 2x_3 - x_4 = 0$
$(A,b) = \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 1 & -1 & 2 & -1 & 0 \end{array}\right) \xrightarrow{II:\, I*(-1)+II} \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & -3 & 1 & -2 & 0 \end{array}\right)$
$\xrightarrow{II:\, II*\frac{1}{3}} \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & -\frac{1}{3} & \frac{2}{3} & 0 \end{array}\right)$
$r = 2 \quad (x_3, x_4,$ sind frei wählbar ("freie"Variablen))
$rg(A.b) = 2 < n = 4 \Rightarrow kerA =$ Lösungsraum $U$ de LGS ist 2-dimensional
$dimU = n - rg(A)$
Wie sieht der Lösungsraum genau aus? Gib eine Basis von $U$ an. Wähle $x_3, x_4$ frei. (möglichst geschickt)
$x_3 = 0, x_4 = 1$ gibt $x_2 = -\frac{2}{3}, x_1 = 0 + \frac{3}{4} + 0 - 1 = \frac{1}{3}$
$\Rightarrow v_1 = \begin{pmatrix} \frac{1}{3} \\ -\frac{2}{3} \\ 0 \\ 1 \end{pmatrix}$ ist 1. Basisvektor von $U$
$x_3 = 1, x_4 = 0$ gibt $x_2 = \frac{1}{3}, x_1 = -\frac{2}{3} - 1 = -\frac{5}{3}$
$v_2 = \begin{pmatrix} -\frac{5}{3} \\ \frac{2}{3} \\ 1 \\ 0 \end{pmatrix}$ ist 2. Basisvektor von $U$

$$\Rightarrow U =< v_1, v_2 >_{\mathbb{R}} =< \begin{pmatrix} 1 \\ -2 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} -5 \\ 2 \\ 3 \\ 0 \end{pmatrix} >_{\mathbb{R}} = \{\alpha * \begin{pmatrix} 1 \\ -2 \\ 0 \\ 3 \end{pmatrix} + \beta * \begin{pmatrix} -5 \\ 2 \\ 3 \\ 0 \end{pmatrix} \mid \alpha, \beta \in \mathbb{R}\}$$

b) $x_1 + 2x_2 + x_3 + x_4 = 7$
$x_1 - x_2 - 2x_3 - x_4 = -2$
(inhomogenes LGS, das zu homogene LGS aus Teil a))
$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 7 \\ 1 & -1 & 2 & -1 & -2 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 7 \\ 0 & -3 & 1 & -2 & -9 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 7 \\ 0 & 1 & -\frac{1}{3} & \frac{2}{3} & 3 \end{array}\right)$
spezielle Lösung $x_0$:
z.B. $x_3 = 0, x_4 = 0$ (frei wählen)
$\Rightarrow x_2 = 3$
$x_1 = 7 - 2 * 3 = 1$ gibt $x_0 = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}$
Allg. Lösung hat die Form:

$$\begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix} + \underbrace{U}_{\text{von a)}} = \{ \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix} + \alpha * \begin{pmatrix} 1 \\ -2 \\ 0 \\ 3 \end{pmatrix} + \beta * \begin{pmatrix} -5 \\ 2 \\ 3 \\ 0 \end{pmatrix} \mid \alpha, \beta \in \mathbb{R}\}$$

**Bemerkung 5.23.**

Sei $V = \mathbb{R}^2, U =< \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 7 \\ -1 \end{pmatrix}, \begin{pmatrix} -2 \\ -4 \\ 0 \end{pmatrix} >_{\mathbb{R}}$ UR von $V$

Wie viele l.u. Vektoren enthält $U$? (was ist $dimU$? Basis von $U$?)

Dies lässt sich nun einfach mit 5.12 beatnworten:

$$dimU = rg \begin{pmatrix} 2 & 0 & 2 & -2 \\ 1 & 3 & 7 & 4 \\ 1 & -1 & -1 & 0 \end{pmatrix} \underbrace{=}_{\substack{II:\, II*(-2)+I \\ III:\, III*(-2)+I}} rg \begin{pmatrix} 2 & 0 & 2 & -2 \\ 0 & -6 & -12 & 6 \\ 0 & 2 & 4 & -2 \end{pmatrix}$$

$$\underbrace{=}_{III:\, 3*III+II} rg \begin{pmatrix} 2 & 0 & 2 & -2 \\ 0 & -6 & -12 & 6 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 2$$

Also gibt es 2 l.u. Vektoren in $U$, die den Stufenspalten entsprechen $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ -1 \end{pmatrix}$

Diese bilden Basis von $U$

weiteres Bsp.:

$V = \{p \mid p\text{Polynom vom Grad} \leq 2\} \subseteq \mathscr{F}(\mathbb{R}, \mathbb{R})$

$U =< 3x, 4x^2 + 2x + 2, 2x^2 + x + 1 >\subseteq V$

$dimU$? Basis von $U$

Erstelle Matrix aus Koodinatenvektoren bezgl. (geordneter) Basis $(1, x, x^2)$ von $V$:

$$dimU = rg \begin{pmatrix} 0 & 2 & 1 & 1 \\ 3 & 2 & 1 & 0 \\ 0 & 4 & 2 & 2 \end{pmatrix} = rg \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 4 & 2 & 2 \\ 0 & 2 & 1 & 1 \end{pmatrix} = rg \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 4 & 2 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 2$$

Basis von $U = \{3x, 4x^2 + 2x + 2\}$

**Bemerkung 5.24.**

Gegeben ist das LGS (*) $Ax = b$ mit $A \in M_n(K), b \in K^n, rg(A) = n$.

Nach 5.21 b) besitzt (*) genau einen Vektor $x \in K^n$ als Lösung, dieser kann mittels 5.12/5.20 gefunden werden.

Statt nur auf Zeilenstufenform kann man $(A, b)$ durch elementare ZUF auch auf die Form $(E_n, b\prime)$ bringen. Dann ist $b\prime$ genau der gesuchte Lösungsvektor $x$.

Bsp.: $2x_1 + x_2 = 10$

$x_1 + 3_2 = 15$

$$(A, b) = \left(\begin{array}{cc|c} 2 & 1 & 10 \\ 1 & 3 & 15 \end{array}\right) \xrightarrow{II:\, I-2*II} \left(\begin{array}{cc|c} 2 & 1 & 10 \\ 0 & -5 & -20 \end{array}\right) \xrightarrow{II:\, II*(-\frac{1}{5})} \left(\begin{array}{cc|c} 2 & 1 & 10 \\ 0 & 1 & 4 \end{array}\right)$$

$$\xrightarrow{I:\, I-II} \left(\begin{array}{cc|c} 2 & 0 & 6 \\ 0 & 1 & 4 \end{array}\right) \xrightarrow{II:\, I*\frac{1}{2}} \left(\begin{array}{cc|c} 1 & 0 & 3 \\ 0 & 1 & 4 \end{array}\right)$$

Ähnlich lässt sich die Inverse $A^{-1} \in M_n(K)$ einer Matrix $A \in M_n(K)$ berechnen. (falls $A$ invertierbar ist)

Gegeben sei die Gleichung $A * x = E_n \quad (A * A^{-1} = E_n)$ mit $A, E_n \in M_n(K)$ gesucht ist die Matrix $X (= A^{-1}) \in M_n(K)$

Bringe die erweiterte Koeffizientenmatrix $A, E_n)$ mittels Gauß-Algoritmus (5.12) auf die Form $(E_n, E_n\prime)$. Dann ist $E_n\prime$ genau die gesuchte Lösungsmatrix $X$ (also $A^{-1}$)

Bsp.: $A = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \in M_2(\mathbb{R})$, gesucht $A^{-1}$ mit $AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{array}\right) \xrightarrow{II:\,2*II} \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 2 & 6 & 0 & 2 \end{array}\right) \xrightarrow{II:\,I-II} \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 0 & -5 & 1 & -2 \end{array}\right)$$

$$\xrightarrow{II:\,II*(-\frac{1}{5})} \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{array}\right) \xrightarrow{I:\,I-II} \left(\begin{array}{cc|cc} 2 & 0 & \frac{6}{5} & -\frac{2}{5} \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{array}\right) \xrightarrow{I:\,I*\frac{1}{2}} \left(\begin{array}{cc|cc} 1 & 0 & \frac{3}{5} & -\frac{1}{5} \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{array}\right)$$

Test: $A * A^{-1} = A^{-1} * A = E_n$

Das führt zu folgendem Satz.

**Satz 5.25.** *Charakterisierung invertierbarer Matritzen*

$A \in M_n(K)$ ist invertierbar $\Leftrightarrow rg(A) = n$.

Beweis: $\Rightarrow$ Sei $A$ invertierbar. Dann gilt $n = rg(E_n) = rg(A * A^{-1}) \overset{5.19}{\geq} rg(A) \geq$ (größer geht nicht, $A \in M_n(K)) \Rightarrow rg(A) = n)$

$\Leftarrow$ folgt aus Bem. 5.25

# 6 Determinante

**Definition 6.1.**

$A \in M_{n-1}(K) \quad i,j \in \{1,...,n\}$
$A_{ij} \in M_{n-1}(K)$ sei die Matrix, die man aus $A$ durch streichen der $i$-ten Zeile und der $j$-ten Spalte erhält.
(z.B. $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, A_{1,1} = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix}, A_{3,2} = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}$)

**Definition 6.2.** *Determinante*

(rekursive Definition)
$A \in M_n(K)$
$n = 1 : A = (a)$, dann ist $det(A) := a$
$n > 1 : det(A) := \sum_{j=1}^{n} (-1)^{1+j} a_{ij} * det(A_{1j})$
$= a_{11} * det(A_{11}) - a_{12} * det(A_{12}) + a_{13} * det(A_{13}) - ... + / - a_{1n} * det(A_{1n})$
$det(A)$ heißt Determinante von $A$
(Formel heißt auch Ëntwicklung nach der 1. Zeile")

**Beispiel 6.3.**

a) $det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} * a_{22} - a_{12} * a_{21}$

b) $det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$
$= a_{11} * (a_{22} * a_{33} - a_{23} * a_{32}) - a_{12} * (a_{21} * a_{33} - a_{23} * a_{31}) + a_{13} * (a_{21} * a_{32} - a_{22} * a_{31})$
Regel von Sarrus

c) für $n \times n$ Matrix ermittle i.A. $n!$ Summanden

d) Ist $A$ eine obere oder untere Dreiecksmatrix, so lässt sich $det(A)$ einfach berechnen:
$A = \begin{pmatrix} a_{11} & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & a_{nm} \end{pmatrix}, det(A) = a_{11} * a_{12} * ... * a_{nm}$
klar für $n = 1 : A(0)$
$n > 1 :\ det \begin{pmatrix} a_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nm} \end{pmatrix} = a_{11} * det \begin{pmatrix} a_{12} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nm} \end{pmatrix}$
Induktion $\Rightarrow$ Behauptung

e) damit ist klar $det(E_n) = 1$
Man kann Def. 6.2 verallgemeinern und folgenden Satz zeigen

**Satz 6.4.** *Entwicklungssatz von Laplace*

$A \in M_n(K)$

a) Entwicklung nach der $i$-ten Zeile für $i \in \{1, ..., n\}$ gilt $det(A) = \sum_{j=1}^{n}(-1)^{i+j} a_{ij} * det(A_{ij})$

b) Entwicklung nach der $j$-ten Spalte für $j \in \{1, ..., n\}$ gilt $det(A) = \sum_{i=1}^{n}(-1)^{i+j} a_{ij} * det(A_{ij})$

**Beispiel 6.5.**

$A = \begin{pmatrix} 2 & 1 & 1 \\ -1 & 0 & 3 \\ 2 & 0 & 4 \end{pmatrix} \in M_3(\mathbb{R}) \qquad \begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$
mit Def. 6.2 Entwicklung nach 1. Zeile:
$det(A) = 2 * det \begin{pmatrix} 0 & 3 \\ 0 & 4 \end{pmatrix} - 1 * det \begin{pmatrix} -1 & 2 \\ 3 & 4 \end{pmatrix} + 1 * det \begin{pmatrix} -1 & 0 \\ 2 & 0 \end{pmatrix} = 2 * 0 - 1(-10) + 1 * 0 = 10$
oder Entwicklung nach 3. Zeile:
$det(A) = 2 * det \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} - 0 * det(...) + 4 * det \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} = 2 * 3 - 0 * ... + 4 * 1 = 10$
oder (besser) Entwicklung nach 2. Spalte:
$det(A) = -1 * det \begin{pmatrix} -1 & 3 \\ 2 & 4 \end{pmatrix} + 0 * det(...) - 0 * det(...) = -1 * (-10) = 10$
Also: Geschickt nach einer Zeile oder Spalte zu entwickeln, in der viele Nullen stehen.
Falles es nur wenig Nullen gibt: zuerst Gauß anwenden. (Achtung: *det* ändert sich evtl.)

**Bemerkung 6.6.**

Aus 6.4 folgt $det(A) = det(A^T)$

**Satz 6.7.** *Eigenschaften der Determinante*

$A, B \in M_n(K) \quad s_1, ..., s_n$ Spalten von $A$
$s_i \in K^n, \lambda \in K$
Also $A = \{s_1, ..., s_n)$

(D1) $det(s_1, ..., s_i + s_i\prime, ..., s_n) = det(s_1., , , s_1, ..., s_n) + det(s_1, ..., s_i\prime, ..., s_n)$

(D2) Beim vertauschen zweier Spalten von $A$ ändert sich das Vorzeichen von $det(A)$

(D3) $det(s_1, ..., \lambda s_i, ..., s_n) = \lambda * det(s_1, ..., s_i, ..., s_n)$

(D4) $det(\lambda * A) \overset{D3}{=} \lambda^n * det(A)$

(D5) Ist eine Spalten von $A$ gleich $\vec{0}$, so ist $det(A) = 0$ (folgt aus D3)

(D6) Besitzt $A$ zwei identische Spalten, so ist $det(A) = 0$
(vertausche id Spalte, erhalte Matrix $A\prime(= A)$.
Nach D2: $detA = -detA\prime = -detA$, dies ist nur möglich wenn $det(A) = 0$)

(D7) $det(s_1, ..., s_i + \lambda s_j, ..., s_n) = det(A) \quad (i \neq j)$ mit (D1,D2, D6)

(D8) $det(A * B) = det(A) * det(B)$

Analog mit Zeilen statt Spalten

**Bemerkung 6.8.**

Also: Erzeuge mit Gauß viele Nulleinträge (D2, D3 ($det$ ändert sich) D7 ($det$ bleibt)), entwickle nach guter Zeile/Spalte. (oder: bringe Matrix auf obere/untere Dreiecks-Form)

z.B. $det \begin{pmatrix} 0 & 1 & 2 \\ -2 & 0 & 3 \\ 0 & -2 & 3 \end{pmatrix} \overset{D2}{=} -det \begin{pmatrix} -2 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & -2 & 3 \end{pmatrix} \overset{D7}{\underset{III:\, 2II+III}{=}} -det \begin{pmatrix} -2 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 7 \end{pmatrix}$

$= -(-2 * 1 * 7) = 14$

**Satz 6.9.** *Charakterisierung invertierbarer Matritzen über Determinante*

$A \in M_n(K)$ ist invertierbar $\Leftrightarrow det(A) \neq 0$

In diesem Fall gilt: $det(A^{-1}) = (detA)^{-1} \quad (= \frac{1}{detA}$ in $\mathbb{R})$

Beweis "$\Rightarrow$"Sei $A$ invertierbar $\exists A^{-1}$ mit $A * A^{-1} = E_n \Rightarrow det(A * A^{-1}) = det(E_n) = 1$

$= det(A) * det(A^{-1})$ (D8)

$\Rightarrow det(A) \neq 0 \quad det(A^{-1}) = \frac{1}{det(A)} = ((det(A))^{-1})$

"$\Leftarrow$"(mit Kontraposition:) Sei $A$ nicht invertierbar $\overset{\text{Satz 5.26}}{\Rightarrow} rg(A) < n \Rightarrow$ Spalten von $A$ sind l.a.

d.h. $\exists i$ mit $s_i = \sum_{k=1}^{n} \lambda_k s_k$

($s_i$ als LK der restlichen Spalten)

$\Rightarrow det(A) \overset{D7}{=} det(s_1, ..., \underbrace{s_i - \sum \lambda_k s_k}_{i}, ..., s_n) = det(s_1, ..., \vec{0}, ..., s_n) \overset{D5}{=} 0$

**Bemerkung 6.10.**

Für $A \in M_2(K)$ lässt sich $A^{-1}$ auch schnell mittels Determinante berechnen:

Es gilt: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K) \Rightarrow A^{-1} = \frac{1}{detA} * \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \qquad \frac{1}{detA} = (detA)^{-1}$

# 7 Eigenwerte und Eigenvektoren

Sei $A \in M_n(K)$. Ein Skalar $\lambda \in K$ heißt Eigenwert von $A$ wenn es einen Vektor $\vec{0} \neq x \in K^n$ gibt ("nichttrivial"d.h. $\neq \vec{0}$) mit $Ax = \lambda x$.
(d.h. der Vektor wird von $A$ nur um $\lambda$ gestreckt und sonst nicht verändert)
Jedes solche $x$ heißt ein zu $\lambda$ gehöriger Eigenvektor von $A$,
und $Eig(\lambda) = Eig_A(\lambda) = \{x \in K^n \mid Ax = \lambda x\}$ (alle zu $\lambda$ geh. EV und der Nullvektor $\vec{0}$) der $\lambda$ zugeordnete Eigenraum.

**Satz 7.1.**

$\lambda \in K$ ist Eigenwert von $A \in M_n(K) \Leftrightarrow det(A - \lambda E_n) = 0$, und die zu $\lambda$ gehörenden Eigenvektoren sind genau die nichttrivialen Lösungen des homogenen LGS $[A - \lambda E_n]x = \vec{0}$
also: $Eig_A(\lambda))ker(A - \lambda E_n)$
Beweis: $(x \neq \vec{0})$ $\quad Ax = \lambda x \Leftrightarrow Ax = \lambda E_n\, x \Leftrightarrow (A - \lambda E_n)x = \vec{0}$
Also: $\lambda$ Eigenwert von $A$
$\Leftrightarrow (A - \lambda E_n)x = \vec{0}$ hat noch weitere Lösungen als $x = \vec{0}$
$\overset{Kor. 5.21}{\Leftrightarrow} rg(A - \lambda E_n) < n$
$\overset{5.26}{\Leftrightarrow} (A - \lambda E_n)$ nicht invertierbar
$\overset{6.9}{\Leftrightarrow} det(A - \lambda E_n) = 0$
$x$ Eigenvektor $\Leftrightarrow x \neq \vec{0}$ und $(A - \lambda E_n)x = \vec{0}$

**Bemerkung 7.2.**

$\lambda \in K$ ist Eigenwert von $A \Leftrightarrow det(A - \lambda E_n) = 0$
$Eig_A(\lambda) = ker(A - \lambda E_n)$

**Definition 7.3.**

Für $A \in M_n(K)$ heißt $P_A(\lambda) := det(A - \lambda E_n)$ das charakteristische Polynom von $A$

**Beispiel 7.4.**

$A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} \in M_2(\mathbb{R})$
Eigenwerte, Eigenvektoren, $Eig(A)$, $P_A(\lambda)$?
$A - \lambda E_2 = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1-\lambda & 1 \\ -2 & 4-\lambda \end{pmatrix}$
$P_A(\lambda) = det \begin{pmatrix} 1-\lambda & 1 \\ -2 & 4-\lambda \end{pmatrix} = (1-\lambda)(4-\lambda) - (1) + (-2) = \lambda^2 - 5\lambda + 6 = /\lambda - 2)(\lambda - 3)$
Eigenwerte von $A$:
$\lambda \in W$ von $A \Leftrightarrow P_A(\lambda) = 0 \overset{7.2}{\Leftrightarrow} \lambda = 2$ oder $\lambda = 3$
d.h. $\lambda_1 = 2, \lambda_2 = 3$ Eigenwerte von $A$
Eigenvektoren von $A$:
$x$ ist EV zu $\lambda_1 = 2 \Leftrightarrow x \neq 0$ und $(A - \lambda_1 E_2)x = \vec{0}$, also $\begin{pmatrix} 1-2 & 1 \\ -2 & 4-2 \end{pmatrix} x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
$\Leftrightarrow \begin{pmatrix} -1 & 1 \\ -2 & 2 \end{pmatrix} x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (z.B. $x = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, welche noch?)

Eigenraum von $A$:
$Eig_A(\lambda_1) = ker \begin{pmatrix} -1 & 1 \\ -2 & 2 \end{pmatrix} =< \begin{pmatrix} 1 \\ 1 \end{pmatrix} >_{\mathbb{R}}$
$x$ ist EV von $\lambda_2 = 3 \Leftrightarrow x \neq \vec{0}$ und $(A - \lambda_2 E_2)x = \vec{0}$ also $\begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix} x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
$Eig_A(\lambda_2) = ker \begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix} =< \begin{pmatrix} 1 \\ 2 \end{pmatrix} >_{\mathbb{R}}$

**Anwendungen 7.5.**

a) Matrixpotenzen
Berechne $A^{2019} = \underbrace{A * A * ... * A}_{2019 \text{ mal}}$ für $A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$ aus Bsp. 7.4
Es gilt: $S := \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ (linke Spalte Eigenvektor zu $\lambda_1$, rechte Spalte EV zu $\lambda_2$)
$S^{-1} \underbrace{=}_{\text{Formel 6.10 } (detS = 1)} \frac{1}{1} * \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$ dann ist $A = S * \underbrace{\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}}_{=D \text{ Diagonalmatrix}} * S^{-1}$
$\Rightarrow A^{2019} = (SDS^{-1} =^{2019}= (SD \underbrace{S^{-1})(S}_{=E_2} D \underbrace{S^{-1})...(S}_{=E_2} DS^{-1})$
$= SD^{2019}S^{-1}$
$S \begin{pmatrix} 2^{2019} & 0 \\ 0 & 3^{2019} \end{pmatrix} S^{-1}$

b) -Schwingungen, Eigenfrequenz (Tacoma Bridge)
- Googles PageRang Algo.
- Hauptachsentransformation, PCA (Eigenfaces)

**Bemerkung 7.6.**

Für $A \in M_n(K)$ ist $P_A(\lambda) = det(A - E_n) = det \begin{pmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1m} \\ \vdots & a_{22} - \lambda & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{nm} & & & a_{nm} - \lambda \end{pmatrix}$
ein Polynom von Grad $N$ (folgt aus Definition der Determinante) die Nulstellen von $P_A(\lambda)$ sind EW von $A$.
$K = \mathbb{R} :\leq n$ Eigenwerte
$K = \mathbb{C}$: hier gilt der sog. "Fundamentalsatz der Algebra": jedes Polynom $p(\lambda) \sum_{k=0}^{n} a_k \lambda^k$ $(a_k \in \mathbb{C})$ vom Grad $n$ (d.h. $a_n \neq 0$) besitzt genau $n$ Nullstellen in $\mathbb{C}$ genauer $\exists \lambda_1, ..., \lambda_n \in \mathbb{C}$ mit $p(\lambda) = a_n \lambda - \lambda_1)...(\lambda - \lambda_n)$.
Von den Zahlen $\lambda_1, ..., \lambda_n$ können auch einige gleich sein, daher präziser formuliert: $\exists l \in \mathbb{N}, \lambda_1, ..., \lambda_l \in \mathbb{C}$ mit $\lambda_i \neq \lambda_j (i \neq j)$ und $\exists n_1, ..., n_l \in \mathbb{N}$ und $p(\lambda) = a_n(\lambda - \lambda_1)^{n_1}...(\lambda - \lambda_l)^{n_l}$.
Die Zahl $n_j$ nennt man dann die algebraische Vielfachheit vin $\lambda_j$.

**Beispiel 7.7.**

a) $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, p_A(\lambda) = det \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = \lambda^2 + 1 = (\lambda + i)(\lambda - i)$
$\Rightarrow$ Eigenwerte: $\lambda_1 = i, \lambda_2 = -i$
Eigenvektoren:
zu $\lambda_1 = i$: löse $\begin{pmatrix} -1 & -1 \\ 1 & -i \end{pmatrix} x = \vec{0}$ $\quad \left(\begin{array}{cc|c} -1 & -1 & 0 \\ 0 & 0 & 0 \end{array}\right)$
$Eig_A(\lambda_1) =< \begin{pmatrix} 1 \\ -i \end{pmatrix} >$
zu $\lambda_2 = -i$: löse $\begin{pmatrix} i & -1 \\ 1 & i \end{pmatrix} x = \vec{0}$
$Eig_A(\lambda_2) =< \begin{pmatrix} 1 \\ i \end{pmatrix} >$

b) $A = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ 1 & 0 & 0 \end{pmatrix} p_A = det \begin{pmatrix} 2-\lambda & 0 & -1 \\ 0 & 2-\lambda & -1 \\ 1 & 0 & -\lambda \end{pmatrix}$
$= (2-\lambda) * det \begin{pmatrix} 2-\lambda & -1 \\ 0 & -\lambda \end{pmatrix} - 1 * det \begin{pmatrix} 0 & 2-\lambda \\ 1 & 0 \end{pmatrix} = ... = (2-\lambda)(\lambda-1)$
$\Rightarrow \lambda_1 = 2$ ist EW mit algebraischer Vielfachkeit 1
$\lambda_2 = 1$ ist EW mit algebraischer Vielfachkeit 2
$Eig_A(\lambda_1 = 2) = ker \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & 0 & -2 \end{pmatrix} = ker \begin{pmatrix} 1 & 0 & -2 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}$ ($x_2$ frei, setze $x_1 = 1$, rechne: $x_3 = 0, x_1 = 0$)
$=< \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} >$
$Eig_A(\lambda_2 = 1) = ker \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 1 & 0 & -1 \end{pmatrix} = ker \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$ ($x_2$ frei)
$=< \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} >$

**Definition 7.8.** *Diagonalisierbarkeit*

Eine Matrix $A \in M_n(K)$ heißt diagonalisierbar, wenn eine invertierbare Matrix $S \in M_n(K)$ existiert, so dass $A = SDS^{-1}$ gilt, wobei $D = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$ Diagonalmatrix ist.
(Die $\lambda_i$ sind gerade die EW von $A$. Es gilt dann auch $D = S^{-1}AS$)
Ist jede Matrix diagonalisierbar?

**Satz 7.9.** *Spektralsatz*

a) $A \in M_n(K)$ ist diagonalisierbar $\Leftrightarrow$ Es gibt $n$ l.u. Eigenvektoren von $A$

b) Besitzt $A$ $n$ verschiedene EW, so ist $A$ diagonalisierbar.
($A$ diagonalisierbar $\Leftrightarrow$ $A$ besitzt $n$ verschiedene EW)

Beweis:

a) $A$ diagonaliierbar, d.h. $\exists S$ invertierbar mit $S^{-1}AS = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$

$\overset{\text{Mult. mit } S \text{ von links}}{\Leftrightarrow} AS = S * \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$

Sei $S = (\underbrace{s_1, ..., s_n}_{\text{Spalten}}$

Für die $i$-te Spalte $s_i$ von $S$ gilt dann $As_i = \lambda_i s_i \quad (i = 1, ..., n)$

Also ist $s_i$ EV zum EW von $A$.

$S$ ist invertierbar $\Leftrightarrow$ Spalten $s_1, ..., s_n$ l.u

b) Zeige per Induktion, dass die zugehörigen EV l.u. sind, Beh. folgt aus Teil a)

**Bemerkung 7.10.** *zu 7.9 b)*

Es gibt auch diagonalisierbare Matritzen, die nicht $n$ verschiedene EW haben!
z.B.: $E_n$: ist bereits in Diagonalform

$$E_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}}_{S} \underbrace{\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}}_{S^{-1}}$$

$\lambda_1 = 1$ ist $n$-facher EW

EV sind die kanonischen Einheitsvektoren $(1 - \lambda)^n = 0$