Lineare Algebra 1

Uni Heidelberg

Mit Liebe gemacht von:
Nikolaus Schäfer

Inhaltsverzeichnis

1. Grundlagen

1.1. Naive Aussagenlogik

naive Logik: Wir verwenden die sprachliche Vorstellung (≠ mathematische Logik).

Eine Aussage ist ein festellender Satz, dem genau einer der Wahrheitswerte "$wahr$" oder "$falsch$" zugeordnet werden kann. Aus einfachen Aussagen kann man durch logische Verknüpfungen komplizierte Aussagen bilden. Angabe der zusammengesetzten Aussage erfolgt durch Wahrheitstafeln (liefern Wahrheitswert der zusammengesetzten Aussage aus Wahrheitswerten der einzelnen Aussagen).
Im folgenden seien A, B Aussagen:

Negation(Nicht-Verknüpfung):
Symbol: ¬

Wahrheitstafel:

A	¬ A
w	f
f	w

Bsp.: A: 7 ist eine Primzahl (w)
$\neg A$: 7 ist keine Primzahl (f)

Konjunktion (UND-Verknüpfung):
Symbol: ∧

Wahrheitstafel:

A	B	A ∧ B
w	w	w
w	f	f
f	w	f
f	f	f

Disjunktion (ODER-Verknüpfung):
Symbol: ∨

Wahrheitstafel:

A	B	A ∨ B
w	w	w
w	f	w
f	w	w
f	f	f

Bsp.: A: 7 ist eine Primzahl (w) B: 5 ist gerade (f)

$A \wedge B$: 7 ist eine Primzahl und 5 ist gerade (f)
$A \vee B$: 7 ist eine Primzahl oder 5 ist gerade (w)

Anm.: Es handelt sich um ein "einschließendes oder". "Entweder A oder B" korrespondiert
$(A \vee B) \wedge (\neg(A \wedge B)))$

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

Wahrheitstafel:

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

Sprechweise:
A impliziert B, aus A folgt B, A ist eine hinreichende Bedingung für B (ist $A \Rightarrow B$ wahr, dann folgt aus A wahr, dass auch B wahr ist). B ist eine notwendige Bedingung für A (ist $A \Rightarrow B$ wahr, dann kann A nur dann wahr sein, wenn B wahr ist).

Bsp.: Es seien m.n natürliche Zahlen:
A : m ist gerade
B : $m * n$ ist gerade
Dann ist für alle natürlichen Zahlen m,n die Aussage $A \Rightarrow B$ wahr, dann: Wir nehmen eine Fallunterscheidung vor nach m,n gerade bzw. ungerade:

1. Fall: m gerade, n gerade. Dann ist A wahr, B wahr, d.h. $A \Rightarrow B$ wahr.
2. Fall: m gerade, n gerade. Dann ist A wahr, B wahr, d.h. $A \Rightarrow B$ wahr.
3. Fall: m ungerade, n gerade. Dann ist A falsch, B wahr, d.h. $A \Rightarrow B$ wahr.
4. Fall: m ungerade, n ungerade. Dann ist A falsch, B falsch, d.h. $A \Rightarrow B$ wahr.

Äquivalenz (GENAU-DANN-WENN-VERKNÜPFUNG)
Symbol: $\Leftrightarrow$

Wahrheitstafel:

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

Sprechweise: A gilt genau dann, wenn B gilt; A ist hinreichend und notwendig für B. Die Aussagen $A \Leftrightarrow B$ und $(A \Rightarrow B) \wedge (B \Rightarrow A)$ sind gleichbedeutend.

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

Bsp.: Es sei n eine ganze Zahl

$A : n-2>1$

$B : n>3$

Für alle ganzen zahlen n ist die Äquivalenz $A \Leftrightarrow B$ wahr, denn:

$n-2>1 \Rightarrow n>3$ und $n>3 \Rightarrow n-2>1$

$C : n>0$

$D : n^2>0$

Für $n=-1$ ist die Äquivalenz $C \Leftrightarrow D$ falsch (C falsch, D wahr). Für alle ganzen Zahlen n gilt zumindest die Implikation $C \Rightarrow D$.

Beweisen:

Mathematische Sätze, Bemerkungen, Folgerungen etc. sind meistens in Form wahrer Implikationen formuliert.

Beweisen: Begründen, warum diese Implikation wahr ist.

Beweismethoden für die Implikation $A \Rightarrow B$:

- direkter Beweis ($A \Rightarrow B$)
- Beweis durch Kontraposition ($\neg B \Rightarrow \neg A$)
- Widerspruchsbeweis $\neg(A \wedge \neg B)$

Diese sind äquivalent zueinander:

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

Bsp.: m,n natürlich $A : m^2<n^2$ $B : m<n$ Wir wollen zeigen, dass $A \Rightarrow B$ für alle natürlichen Zahlen m,n wahr ist.

1. Direkter Beweis:
   $A : m^2<n^2 \Rightarrow 0<n^2-m^2 \Rightarrow 0<(n-m)\underbrace{(n+m)}_{>0} \Rightarrow 0<n-m \Rightarrow m<n$

2. Beweis durch Kontraposition:
   $\neg B : m \geq n \overset{*m}{\underset{*n}{\Longrightarrow}} m^2 \geq m*n \wedge m*n \geq n^2 \Rightarrow m^2 \geq n^2 \Rightarrow \neg A$
3. Beweis durch Widerspruch:
   $A \wedge \neg B \Rightarrow m^2 < n^2 \wedge n \leq m \Rightarrow m^2 < n^2 \wedge m*n \leq m^2 \wedge n^2 \leq m*n \Rightarrow m*n \leq m^2 < n^2 \leq m*n \lightning$

Existenz und Allquantor:
$A(x)$ Aussage, die von Variable x abhängt.
$\exists x$: A(x) ist gleichbedeutend mit "Es existiert ein x, für das $A(x)$ wahr ist." (hierbei ist "existiert ein x" im Sinne von "existiert mindestens ein x" zu verstehen).
Bsp.: $\exists$ natürliche Zahl $n : n > 5$ (w)

$\exists! x : A(x)$ ist gleichbedeutend mit "Es existiert genau ein x, für dass $A(x)$ wahr ist."
Bsp.: $\exists!$ natürliche Zahl $n : n + 3 = 8$

$\forall x : A(x)$ ist gleichbedeutend mit "Für alle x ist $A(x)$ wahr"
Bsp.: $\forall$ natürlichen Zahlen n gilt: $4 * n$ ist gerade.

Negation von Existenz- und Allquantor:
$\neg(\exists x : A(x))$ ist äquivalent zu: $\forall x : \neg A(x)$
$\neg(\forall x : A(x))$ ist äquivalent zu: $\exists x : \neg A(x)$
Spezielle Beweistechniken für Existenz- und Allaussagen:

- Angabe eines Beispiels, um zu zeigen, dass eine Existenzaussage wahr ist.
  Bsp.: $\exists$ natürliche Zahl $n : n > 5$ ist wahr, denn für $n = 7$ ist die Aussage $n > 5$ wahr.
- Angabe eines Gegenbeispiels, um zu zeigen, dass eine Aussage falsch ist.
  Bsp.: $\forall$ natürlichen Zahlen $n : n \leq 5$ ist falsch, denn für $n = 7$ ist die Aussage $n \leq 5$ falsch.

1.2. Naive Mengenlehre

Mengenbegriff nach Cantor:
Eine Menge ist eine Zusammenfassung von bestimmten, wohl unterschiedenen Objekten unserer Anschauung und unseres Denkens (die Elemente genannt werden) zu einem Ganzen.

Wir schreiben:
$x \in M$, falls x ein Element von M ist.
$x \notin M$, falls x kein Element von M ist.

Zwei Mengen M, N heißen gleich (Notation: $M = N$), wenn sie die gleichen Elemente besitzen.

Angabe von Mengen:

- Auflisten der Menge: $M = a, b, c, \ldots$
- Beschreibung der Elemente durch Eigenschaften: $M = \{x|E(x)\}$ (Elemente x, für die $E(x)$ wahr)

Bsp.: $\{2,4,6,8\} = \{x|x$ ist eine natürliche Zahl, x ist gerade und $1 < x < 10\}$

Anmerkung:
Bei obiger Schreibweise kommt es nicht auf die Reihenfolge an: $\{1,2,3\} = \{1,3,2\}$
Elemente sind "wohlunterschieden": $\{1,2,2\} = \{1,2\}$
leere Menge: $\emptyset$ (enthält kein Element)
Bsp.: $\{x|x$ ist eine natürliche Zahl und $x < -5\} = \emptyset$

Zahlenbereiche:
$\mathbb{N} := \{1,2,3,\ldots\}$ Menge der natürlichen Zahlen, $\mathbb{N}_0 := \{0,1,2,\ldots\}$
$\mathbb{Z} := \{0,1,-1,2,-2,\ldots\}$ Menge der ganzen Zahlen
$\mathbb{Q} := \{\frac{m}{n}|m \in \mathbb{Z}, n \in \mathbb{N}\}$ Menge der rationalen Zahlen
$\mathbb{R} :=$ Menge der reellen Zahlen

Definition 1.1. A, B Mengen
A heißt Teilmenge von B $(A \subseteq B) \overset{Def.}{\Longleftrightarrow}$ Für alle $x \in A$ gilt $x \in B$ (d.h. jedes Element von A ist auch Element von B)
A heißt echte Teilmenge von B $(A \subseteq B) \overset{Def.}{\Longleftrightarrow} A \subseteq B$ und $A \neq B$

Anmerkung: Offenbar gilt für Mengen $A, B : A = B \Leftrightarrow A \subseteq B$ und $B \subseteq A$, d.h. um zu zeigen, dass $A = B$ ist, zeigt man: Jedes Element aus A liegt in B, und jedes Element aus B liegt in A. Die leere Menge ist Teilmenge jeder Menge.

Beispiel 1.2. $\mathbb{N} \subsetneq \mathbb{N}_0 \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$ (gilt auch mit "$\subsetneq$")

Definition 1.3. A, B Mengen
$A \cap B := \{x|x \in A$ und $x \in B\}$ heißt der Durchschnitt von A und B.
$A \cup B := \{x|x \in A$ oder $x \in B\}$ heißt die Vereinigung von A und B.
$A \backslash B := \{x|x \in A$ und $x \notin B\}$ heißt Differenz von A und B.
Im Fall $B \subseteq A$ nennt man $A \backslash B$ auch das Komplement von B in A und schreibt $C_A(B) = A \backslash B$

Beispiel 1.4.
$A = \{2,3,5,7\}, B = \{3,4,6,7\}$. Dann ist $A \cup B = \{2,3,4,5,6,7\}, A \cap B = \{3,7\}, A \backslash B = \{2,5\}$

Bemerkung 1.5. A, B Mengen
Dann ist $A \cap (B \cup C) = (A \cap B) \cup (A \cap B)$

Bemerkung 1.6. A, B Mengen. Dann sind äquivalent:
(i) $A \cup B = B$

(ii) $A \subseteq B$

Definition 1.7. A, B Mengen
A x $B := \{(a,b) | a \in A, b \in B\}$ heißt das kartesische Produkt von A und B
Hierbei ist $(a,b) = (a',b') \overset{Def.}{\Longleftrightarrow} a = a'$ und $b = b'$.
(a,b) heißt Tupel (geordnetes Paar).

Beispiel 1.8.
(a) $\{1,2\}$ x $\{1,3,4\} = \{(1,1),(1,3),(1,4),(2,1),(2,3),(2,4)\}$
(b) $\mathbb{R}$ x $\mathbb{R} = \{(x,y) | x,y \in \mathbb{R}\} = \mathbb{R}^2$

Definition 1.9. A Menge
$\mathcal{P}(A) := \{M | M \subseteq A\}$ heißt die Potenzmenge von A.

Beispiel 1.10.
$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Definition 1.11. M Menge. Wir setzen:
$$|M| := \begin{cases} n, \text{ falls } M \text{ eine endliche Menge ist und } n \text{ Elemente enthält} \\ \infty, \text{ falls } M \text{ nicht endlich ist} \end{cases}$$
$|M|$ heißt die Kardinalität von M

Beispiel 1.12.
(a) $|\{7,11,16\}| = 3$
(b) $|\mathbb{N}| = \infty$

Bemerkung 1.13.
Für die natürlichen Zahlen gilt das Induktionsaxiom:
Ist $M \subseteq \mathbb{N}$ eine Teilmenge, für die gilt: $1 \in M$ und für alle $n \in M$ gilt: $n \in M \Rightarrow n+1 \in M$, dann $M = \mathbb{N}$

Bemerkung 1.14. (Prinzip der vollständigen Induktion)
Für jedes $n \in \mathbb{N}$ sei eine Aussage $A(n)$ gegeben. Die Aussagen $A(n)$ gelten für alle $n \in \mathbb{N}$, wenn man folgendes zeigen kann:
(IA) $A(1)$ ist wahr
(IS) Für jedes $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$
Der Schritt (IA) heißt Induktionsanfang, die Implikation $A(n) \Rightarrow A(n+1)$ heißt Induktionsschritt.

Beispiel 1.15.
Für $n \in \mathbb{N}$ sei $A(n)$ die Aussage: $1 + \ldots + n = \frac{n(n+1)}{2}$
(IA) $A(1)$ ist wahr, denn $1 = \frac{1(1+1)}{2} = 1$
(IS) zz.: $A(n) \Rightarrow A(n+1)$
Es gelte $A(n)$, d.h. $1 + \ldots + n = \frac{n(n+1)}{2}$ ist wahr. $\Rightarrow 1 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$, d.h. $A(n+1)$ ist wahr.

1.3. Relationen

Definition 1.16. M Menge
Eine Relation auf M ist eine Teilmenge $R \subseteq M$ x M
Wir schreiben $a \sim b \overset{Def.}{\Longleftrightarrow} (a,b) \in R$ ("a steht in Relation zu b")

Anmerkung: Aufgrund der obigen Notation spricht man in der Regel eher von der Relation "$\sim$" auf M als von der Relation $R \subseteq M$ x M.
Anschaulich: Eine Relation auf M stellt eine "Beziehung" zwischen den Elementen von M her. Für $a, b \in M$ gilt entweder $a \sim b$ oder $a \nsim b$, denn: entweder ist $(a.b) \in R$ oder $(a,b) \notin R$.

Beispiel 1.17.
$M = \{1,2,3\}$. Durch $R = \{(1,1),(1,2),(3,3)\} \subseteq M$ x M eine Relation auf M gegeben. Es gilt dann: $1 \sim 1, 1 \sim 2, 3 \sim 3$ (aber z.B.: $1 \nsim 3, 2 \nsim 1, 2 \nsim 2$).

Definition 1.18. M Menge, $\sim$ Relation auf M
$\sim$ heißt:
reflexiv $\Leftrightarrow$ Für alle $a \in M$ gilt: $a \sim a$
symmetrisch $\Leftrightarrow$ Für alle $a, b \in M$ gilt: $a \sim b \Rightarrow b \sim a$
antisymmetrisch $\Leftrightarrow$ Für alle $a, b \in M$ gilt: $a \sim b$ und $b \sim a \Rightarrow a = b$.
transitiv $\Leftrightarrow$ Für alle $a, b, c \in M$ gilt: $a \sim b$ und $b \sim c \Rightarrow a \sim c$
total $\Leftrightarrow$ Für alle $a, b \in M$ gilt: $a \sim b$ oder $b \sim a$

Beispiel 1.19. Sei M die Menge der Studierenden in der LA1-Vorlesung
(a) Für $a, b \in M$ sei $a \sim b \Leftrightarrow a$ hat denselben Vornamen wie b
$\sim$ ist reflexiv, symmetrisch, nicht antisymmetrisch, transitiv, nicht total
(b) Für $a, b \in M$ sei $a \sim b \Leftrightarrow$ Matrikelnummer von a ist $\leq$ als die Matrikelnummer von b
$\sim$ ist reflexiv, nicht symmetrisch, antisymmetrisch, transitiv, total.
(c) Für $a, b \in M$ sei $a \sim b \Leftrightarrow a$ sitzt auf dem Platz rechts von b
$\sim$ ist nicht reflexiv, nicht symmetrisch, antisymmetrisch, nicht transitiv, nicht total

Definition 1.20. M Menge, $\sim$ Relation auf M
$\sim$ heißt eine:
Halbordnung auf $M \Leftrightarrow \sim$ ist reflexiv, antisymmetrisch und transitiv.
Totalordnung auf $M \Leftrightarrow \sim$ ist eine Halbordnung und $\sim$ ist total
In diesen Fällen sagt man auch: Das Tupel $(M, \sim)$ ist eine halbgeordnete bzw. totalgeordnete Menge.

Beispiel 1.21.
(a) $\leq$ auf $\mathbb{N}$ ist eine Totalordnung
(b) Sei $M = \mathcal{P}(\{1,2,3\})$. $\subseteq$ ist auf M eine Halbordnung, aber keine Totalordnung. (es ist z.B. weder $\{1\} \subseteq \{3\}$ noch $\{3\} \subseteq \{1\}$)

Anmerkung: Wegen der Analogie zu $\leq$ auf $\mathbb{N}$ bezeichnen wir Halbordnungen in der Regel mit "$\leq$". (Es ist z.B. weder $\{1\} \subseteq \{3\}$ noch $\{3\} \subseteq \{1\}$)

Definition 1.22. $(M, \leq)$ halbgeordenete Menge, $a \in M$
a heißt:
größtes Element von $M \Leftrightarrow$ Für alle $x \in M$ gilt $x \leq a$
kleinstes Element von $M \Leftrightarrow$ Für alle $x \in M$ gilt $a \leq x$

Bemerkung 1.23. $(M, \leq)$ halbgeordnete Menge
Dann gilt: Existiert in M ein größtes (bzw. kleinstes) Element, so ist dieses eindeutig bestimmt.

Anmerkung: Bemerkung 1.23 sagt nichts darüber aus, ob ein größtes (bzw. kleinstes) Element in M überhaupt existiert.

Beispiel 1.24.
(a) In $(\mathbb{N}, \leq)$ist 1 das kleinstes Element, ein größtes gibt es nicht
(b) In $(\{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\}, \subseteq)$ sind $\{1,2\}, \{1,3\}, \{2,3\}$ maximale Elemente und $\{1\}, \{2\}, \{3\}$ sind minimale Elemente.

Bemerkung 1.25. $(M, \leq)$ halbgeordnete Menge, $a \in M$
Dann gilt: Ist a ein größtes (bzw. kleinstes) Element von M, dann ist a ein maximales (bzw. minimales) Element von M.

Definition 1.26. M Menge, $\sim$ Relation auf M
$\sim$ heißt eine Äquivalenzrelation $\Leftrightarrow$ $\sim$ ist reflexiv, symmetrisch und transitiv.
In dem Fall sagen wir für $a \sim b$ auch: a ist äquivalent zu b.
Für $a \in M$ heißt $[a] := \{b \in M | b \sim a\}$ heißt die Äquivalenzrelation von a.
Elemente aus $[a]$ nennt man Vetreter oder Repräsentanten von a.

Beispiel 1.27. M Menge aller Bürgerinnen und Bürger Deutschlands.
Wir definieren für $a, b \in M$: $a \sim b \Leftrightarrow a$ und b sind im selben Jahr geboren.
$\sim$ ist eine Äquivalenzrelation.
Jerome Boateng wurde 1988 geboren.
[Jerome Boateng] = $\{b \in M | b$ ist im selben Jahr geboren wie Jerome Boateng$\}$ = $\{b \in M | b$ wurde 1988 geboren$\}$
Weitere Vertreter von [Jerome Boateng] sind z.B. Mesut Özil und Mats Hummels.
Es ist [Jerome Boateng] = [Mesut Özil] = [Mats Hummels]
Man sieht in diesem Beispiel: Die Menge M zerfällt komplett in verschiedene Äquivalenzklassen:
Jeder Bürger/jede Bürgerin Deutschlands ist in genau einer Äquivalenzklasse enthalten. Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt (haben leeren Durchschnitt).

Bemerkung 1.28. M Menge, $\sim$ Äquivalenzrelation auf M
Dann gilt:
(a) Jedes Element von M liegt in genau einer Äquivalenzklasse.
(b) Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt.
Man sagt auch: Die Äquivalenzklassen bzgl. "$\sim$" bilden eine Partition von M.

Definition 1.29. M Menge, $\sim$ Äquivalenzrelation auf M
$M/\sim := \{[a]|a \in M\}$ (Menge der Äquivalenzklassen) heißt die Faktormenge (Quotientenmenge) von M nach $\sim$.

Beispiel 1.30. $M = \{1, 2, 3, -1, -2, -3\}$
Für $a.b \in M$ setzten wir $a \sim b \Leftrightarrow |a| = |b|$. Das ist eine Äquivalenzrelation auf M.
Es ist $[1] = \{1, -1\}, [2] = \{2, -2\}, [3] = \{3, -3\}$
Somit: $M/\sim := \{[1], [2], [3]\} = \{\{1, -1\}, \{2, -2\}, \{3, -3\}\}$

Anmerkung: Der Übergang zu Äquivalenzklassen soll (für ein jeweils gegebenes Problem) irrelevante Informationen abstreifen.

1.4. Abbildungen

Definition 1.31. M, N Mengen
naive Def.: Eine Abbildung f von M nach N ist eine Vorschrift, die jedem $m \in M$ genau ein Element aus N zuordnet, dieses wird mit $f(m)$ bezeichnet. Notation: $f : M \to N, m \mapsto f(m)$
Zwei Abbildungen $f, g : M \to N$ sind gleich, wenn $f(m) = g(m)$ für alle $m \in M$ gilt.
M heißt die Definitionsmenge von f, N heißt die Zielmenge von f.

formale Def.: Eine Abbildung f von M nach N ist ein Tripel (M, N, G_f), wobei G_f eine Teilmenge von M x N mit der Eigenschaft ist, dass für jedes Element $m \in M$ genau ein Element $n \in N$ mit $(m, n) \in G_f$ existiert (für dieses Element n schreiben wir auch $f(m)$). G_f heißt der Graph von f.

Beispiel 1.32.
(a) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
(b) $f : \mathbb{R} \to \mathbb{R}^2, x \mapsto (x, x + 1)$
(c) M Menge, $id_M : M \to M, m \mapsto m$ heißt die Identität (identische Abb.) auf M.
(d) I, M Mengen. Eine über I induzierte Familie von Elementen von M ist eine Abbildung $m : I \to M$, $i \mapsto m(i) =: m_i$. Wir schreiben für die Familie auch kurz $(m_i)_{i \in I}$. I heißt die Indexmenge der Familie.
(e) Spezialfall von (d): $I = \mathbb{N}, M = \mathbb{R}$. $(m_i)_{i \in \mathbb{N}}$ nennt man auch eine Folge reeler Zahlen.

Anmerkung: Über den Begriff der Familie lassen sich diverse Konstruktionen aus 1.2 verallgemeinern:
Ist $(M_i)_{i \in I}$ eine Familie von Mengen, dann ist:
$\bigcup_{i \in I} M_i := \{x|$ Es gibt ein $i \in I$ mit $x \in M_i\}$
$\bigcap_{i \in I} M_i := \{x|$ Für alle $i \in I$ ist $x \in M_i\}$
$\prod_{i \in I} M_i := \{(x_i)_{i \in I} | x_i \in M_i$ für alle $i \in I\}$

Definition 1.33. M, N Mengen, $f : M \to N$ Abb.
Sind $m \in M$, $n \in N$ mit $n = f(m)$, dann nennen wir n das Bild von m unter f, und wir nennen m ein Urbild von n unter f.

Anmerkung: In obiger Situation ist das Bild von m unter f eindeutig bestimmt (nach Def. einer Abb.). Urbilder sind im Allgemeinen nicht eindeutig bestimmt, und im allgemeinen besitzt nicht jedes Element aus N ein Urbild:
$f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, dann ist $4 = f(2) = f(-2)$, d.h. 2 und -2 sind Urbilder von 4, das Element -5 hat kein Urbild unter f, denn es existiert kein $x \in \mathbb{R}$ mit $x^2 = -5$.

Definition 1.34. M, N Mengen, $f : M \to N$ Abb., $A \subseteq M$, $B \subseteq N$
$f(A) := \{f(a) | a \in A\} \subseteq N$ heißt das Bild von A unter f
$f^{-1}(B) := \{m \in M | f(m) \in B\} \subseteq M$ heißt das Urbild von B unter f

Beispiel 1.35. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$
$f(\{1,2,3\}) = \{1,4,9\}$
$f^{-1}(\{4,-5\}) = \{2,-2\}$, $f^{-1}(\{4\}) = \{2,-2\}$, $f^{-1}(\{-5\}) = \emptyset$
$f(\mathbb{R}) = \{x^2 | x \in \mathbb{R}\} = \{x \in \mathbb{R} | x \geq 0\} =: \mathbb{R}_{\geq 0}$

Definition 1.36. M, N Mengen, $f : M \to N$ Abb., $A \subseteq M$
$f|_A : A \to N$, $m \mapsto f(m)$ heißt die Restriktion (Einschränkung) von f auf A.
Ist $B \subseteq N$ mit $f(A) \subseteq B$, dann setzen wir $f|_A^B : A \to B$, $m \mapsto f(m)$
Ist $f(M) \subseteq B$, dann setzen wir $f|^B := f|_M^B : M \to B$, $m \mapsto f(m)$

Definition 1.37. L, M, N Mengen, $f : L \to M$, $g : M \to N$
$g \circ f : L \to N$, $x \mapsto (g \circ f)(x) := g(f(x))$ heißt die Komposition (Hintereinanderausführung) von f und g.

Beispiel 1.38. $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$
$\Rightarrow g \circ f : \mathbb{R} \to \mathbb{R}$, $x \mapsto g(f(x)) = g(x^2) = x^2 + 1$

Bemerkung 1.39. L, M, N, P Mengen, $f : L \to M$, $g : M \to N$, $h : N \to P$
Dann gilt: $h \circ (g \circ f) = (h \circ g) \circ f$, d.h. die Verknüpfung von Abbildungen ist assoziativ.

Definition 1.40. M, N Mengen, $f : M \to N$
f heißt injektiv $\Leftrightarrow$ Für alle $m_1, m_2 \in M$ gilt: $f(m_1) = f(m_2) \Rightarrow m_1 = m_2$
$\Leftrightarrow$ Für alle $m_1, m_2 \in M$ gilt: $m_1 \neq m_2 \Rightarrow f(m_1) \neq f(m_2)$
f heißt surjektiv $\Leftrightarrow$ Für jedes $n \in N$ existiert ein $m \in M$ mit $f(m) = n$
$\Leftrightarrow f(M) = N$
f heißt bijektiv $\Leftrightarrow$ f ist injektiv und surjektiv.

Beispiel 1.41.
(a) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ ist:

- nicht injektiv, denn: $f(2) = f(-2)$, aber $2 \neq -2$
- nicht surjektiv, denn es existiert kein $m \in \mathbb{R}$ mit $f(m) = -1$
- nicht bijektiv

(b) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$, $x \mapsto x^2$ ist:

- injektiv, denn für $m_1, m_2 \in \mathbb{R}_{\geq 0}$ gilt: $f(m_1) = f(m_2) \Rightarrow m_1^2 = m_2^2 \overset{m_1, m_2 \geq 0}{\Longrightarrow} m_1 = m_2$
- nicht surjektiv, denn es existiert kein $m \in \mathbb{R}_{\geq 0}$ mit $f(m) = -1$
- nicht bijektiv

(c) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$ ist:

- injektiv (wie bei (b))
- surjektiv, denn: Für $m \in \mathbb{R}_{\geq 0}$ ist $f(\sqrt{m}) = (\sqrt{m})^2 = m$
- bijektiv

Bemerkung 1.42. M, N Mengen, $f : M \to N$, $g : N \to M$ mit $g \circ f = id_M$
Dann ist f injektiv und g surjektiv.

Bemerkung 1.43. M, N Mengen, $f : M \to N$
Dann sind äquivalent:
(i) f ist bijektiv
(ii) Zu jedem $n \in N$ gibt es genau ein $m \in M$ mit $f(m) = n$
(iii) Es gibt genau eine Abb. $g : N \to M$ mit $g \circ f = id_M$ und $f \circ g = id_N$
In diesem Fall bezeichnen wir die Abb. $g : N \to M$ aus (iii) mit f^{-1} und nennen f^{-1} die Umkehrabbildung von f. Sie ist gegeben durch $f^{-1} : N \to M$, $n \mapsto$ das eindeutig bestimmte Element $m \in M$ mit $f(m) = n$.

Beispiel 1.44.
Im Beispiel 1.41(c) haben wir gesehen: $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$ ist bijektiv. Die Umkehrabbildung ist gegeben durch: $f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto \sqrt{x}$

Bemerkung 1.45. M, N Mengen, $f : M \to N$
Dann gilt:
(a) f injektiv $\Leftrightarrow$ Es existiert $g : N \to M$ mit $g \circ f = id_M$
(b) f surjektiv $\Leftrightarrow$ Es existiert $g : N \to M$ mit $f \circ g = id_N$

Bemerkung 1.46. L, M, N Mengen, $f : L \to M$, $g : M \to N$
Dann gilt: g, f beide injektiv (bzw. surjektiv bzw. bijektiv) $\Rightarrow g \circ f$ injektiv (bzw. surjektiv bzw. bijektiv).

Definition 1.47. M, N Mengen
M, N heißen gleichmächtig $\Leftrightarrow$ Es gibt eine bijektive Abbildung $f : M \to N$

Bemerkung 1.48. M, N endliche Mengen mit $|M| = |N|$, $f : M \to N$
Dann sind äquivalent:
(i) f ist injektiv
(ii) f ist surjektiv
(iii) f ist bijektiv

1.5. Gruppen

Definition 1.49. M Menge
Eine Verknüpfung (innere Verknüpfung) auf M ist eine Abb. $* : M \text{ x } M \to M$.
Anstelle von $*(a,b)$ schreiben wir $a * b$.

Beispiel 1.50.
$+ : \mathbb{R} \text{ x } \mathbb{R} \to \mathbb{R}, (a,b) \mapsto a+b$
$\cdot : \mathbb{R} \text{ x } \mathbb{R} \to \mathbb{R}, (a,b) \mapsto a \cdot b$
sind Verknüpfungen.

Definition 1.51.
Ein Monoid ist ein Tupel $(M,*)$, bestehend aus einer Menge M und einer Verknüpfung: $* : M \text{ x } M \to M$, welche folgenden Bedingungen genügt:
(M1) Die Verknüpfung ist assoziativ, d.h. für alle $a,b,c \in M$ ist $(a*b)*c = a*(b*c)$
(M2) Es existiert ein neutrales Element e in M, d.h. ein Element $e \in M$ mit $e*a = a = a*e \ \forall a \in M$

Beispiel 1.52.
(a) $(\mathbb{N}_0,+),(\mathbb{Z},+)$ sind Monoide (neutrales Element:0)
(b) $(\mathbb{N},+)$ ist kein Monoid (es existiert kein neutrales Element)
(c) $(\mathbb{N},\cdot),(\mathbb{Z},\cdot)$ sind Monoide (neutrales Element:1)

Bemerkung 1.53. $(M,*)$ Monoid
Dann gibt es genau ein neutrales Element.

Definition 1.54. $(M,*)$ Monoid mit neutralem Element e, $a \in M$
Ein Element $b \in M$ heißt ein Inverses zu $a \Leftrightarrow a*b = e = b*a$

Beispiel 1.55.
In $(\mathbb{Z},+)$ ist -2 ein Inverses zu 2, denn $-2+2 = 0 = 2+(-2)$
In $(\mathbb{N}_0,+)$ existiert kein Inverses zu 2, denn es existiert kein $n \in \mathbb{N}_0$ mit $2+n = 0 = n+2$
In $(\mathbb{Z},\cdot)$ existiert kein Inverses zu 2, denn es existiert kein $n \in \mathbb{Z}$ mit $2 \cdot n = 1 = n \cdot 2$

Bemerkung 1.56. $(M,*)$ Monoid, $a \in M$
Dann gilt: Besitzt a ein Inverses, dann ist dieses eindeutig bestimmt.

Definition 1.57. Eine Gruppe ist ein Tupel $(G,*)$, bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \to G$, sodass gilt:
(G1) $(G,*)$ ist ein Monoid
(G2) Jedes Element aus G besitzt ein Inverses.
In diesem Fall schreiben wir a' für das nach Bemerkung 1.56 eindeutig bestimmte Inverse eines Elements $a \in G$.

Beispiel 1.58.
(a) $(\mathbb{Z},+)$ ist eine Gruppe, denn: $(\mathbb{Z},+)$ ist ein Monoid, und für $a \in \mathbb{Z}$ ist $-a$ das inverse Element: $a+(-a) = 0 = (-a)+a$
(b) $(\mathbb{Z},\cdot)$ ist keine Gruppe, denn das Element $2 \in \mathbb{Z}$ hat kein Inverses (vgl. 1.52).
(c)$(\mathbb{Q}\backslash\{0\},\cdot)$ ist eine Gruppe, denn: $(\mathbb{Q}\backslash\{0\},\cdot)$ ist ein Monoid (mit neutralem Element 1), und für jedes Element $a \in \mathbb{Q}\backslash\{0\}$ existiert ein $b \in \mathbb{Q}\backslash\{0\}$ mit $a \cdot b = 1 = b \cdot a$, nämlich $b = \frac{1}{a}$

Bemerkung 1.59. $(G,*)$ Gruppe mit neutralem Element E, $a,b,c \in G$. Dann gilt:
(a) (Kürzungsregel) $a*b = a*c \Rightarrow b = c$
$a*c = b*c \Rightarrow a = b$
(b) $a*b = e \Rightarrow b = a'$
(c) $(a')' = a$
(d) (Regel von Hemd und Jacke) $(a*b)' = b'*a'$

Definition 1.60.
$(M,*)$ Monoid/Gruppe heißt kommutativ (abelsch) $\Leftrightarrow \forall a,b \in M$ gilt $a*b = b*a$

Beispiel 1.61.
Alle bisher betrachteten Beispiele von Monoiden bzw. Gruppen sind abelsch.

Bemerkung 1.62. M Menge
Wir setzen $S(M) := \{f : M \to M | f \text{ ist bijektiv}\}$. Dann ist $(S(M),\cdot)$ eine Gruppe, die symmetrische Gruppe auf M.

Definition 1.63. $n \in \mathbb{N}$
$S_n := S(\{1,...,n\}) = \{\pi : \{1,...,n\} \to \{1,...,n\} | \pi \text{ ist bijektiv}\}$
$(S_n,\circ)$ heißt die symmetrische Gruppe auf n Ziffern. Elemente aus S_n heißen Permutationen.
Wir schreiben Permutationen $\pi \in S_n$ in der Form: $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$

Beispiel 1.64. In S_3 ist:
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

d.h., $(S_3,\circ)$ ist nicht abelsch.

1.6. Restklassen

Motivation: Im täglichen Leben verwendet man zur Bestimmung von Uhrzeiten das Rechnen "modulo 24": z.B. 22 Uhr + 7 h = 5 Uhr. Wir wollen dies mathematisch präzisieren und verallgemeinern.

Bemerkung 1.65. $n \in \mathbb{N}$
Dann ist durch: $a \sim b \Leftrightarrow$ Es existiert ein $q \in \mathbb{Z}$ mit $a - b = qn$ eine Äquivalenzrelation auf $\mathbb{Z}$ gegeben.
Anstelle von $a \sim b$ schreiben wir auch $a \equiv b \pmod{n}$ ("a kongruent b modulo n").
Die Äquivalenzklasse von $a \in \mathbb{Z}$ ist durch $\overline{a} := \{b \in \mathbb{Z} | b \equiv a \pmod{n}\} = a + n \cdot \mathbb{Z} := \{a + nq | q \in \mathbb{Z}\}$ gegeben und heißt die Restklasse von a modulo n.
Die Menge aller Restklassen modulo n wird $\mathbb{Z}/n\mathbb{Z}$ bezeichnet ("$\mathbb{Z}$ modulo $n\mathbb{Z}$").
Es ist $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ und die Restklassen $\overline{0}, \overline{1}, ..., \overline{n-1}$ sind paarweise verschieden.

Beispiel 1.66.
$n = 3$: $a \equiv b \pmod{3} \Leftrightarrow$ Es existiert ein $q \in \mathbb{Z}$ mit $a - b = 3q$.
z.B.: $11 \equiv 5 \pmod{3}$, denn $11 - 5 = 6 = 2 \cdot 3$.
$7 \not\equiv 2 \pmod{3}$, denn $7 - 2 = 5$, und es gibt kein $q \in \mathbb{Z}$ mit $5 = 3q$.
$\overline{b} = \{a \in \mathbb{Z} | a \equiv 0 \pmod{3}\} = \{a \in \mathbb{Z} |$ Es ex. $q \in \mathbb{Z}$ mit $a = 3q\} = 3\mathbb{Z} = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$
$\overline{1} = \{a \in \mathbb{Z} | a \equiv 1 \pmod{3}\} = \{a \in \mathbb{Z} |$ Es ex. $q \in \mathbb{Z}$ mit $a - 1 = 3q\} = 1 + 3\mathbb{Z}$
$\overline{2} = \{a \in \mathbb{Z} | a \equiv 2 \pmod{3}\} = \{a \in \mathbb{Z} |$ Es ex. $q \in \mathbb{Z}$ mit $a - 2 = 3q\} = 2 + 3\mathbb{Z}$
$\overline{3} = \{a \in \mathbb{Z} | a \equiv 3 \pmod{3}\} = \{a \in \mathbb{Z} |$ Es ex. $q \in \mathbb{Z}$ mit $a - 3 = 3q\}$
$= \{a \in \mathbb{Z} |$ Es ex. $q \in \mathbb{Z}$ mit $a = 3(q+1) = 3\mathbb{Z}\} = \overline{0}$
$\overline{4} \equiv \overline{1}, \overline{5} \equiv \overline{2}, \overline{-1} \equiv \overline{2}$ etc.

Bemerkung 1.67. $n \in \mathbb{N}$
Wir definieren eine Verknüpfung (Addition) auf $\mathbb{Z}/n\mathbb{Z}$ wie folgt:
Für $a, b \in \mathbb{Z}/n\mathbb{Z}$ setzen wir $\overline{a} + \overline{b} = \overline{a + b}$. Dann gilt $(\mathbb{Z}/n\mathbb{Z}, +)$ ist eine abelsche Gruppe.

Beispiel 1.68.
Wir fassen die Ergebnisse der Verknüpfung "+" in einer Verknüpfungstafel zusammen:

$n = 3$:

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

$n = 4$:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Definition 1.69. $(G, *), (H, \circledast), \phi : G \to H$ Abb.
φ heißt ein Gruppenhomormophismus $\Leftrightarrow \forall a, b \in G$ gilt: $\varphi(a * b) = \varphi(a) \circledast \varphi(b)$
φ heißt ein Gruppenisomorphismus $\Leftrightarrow \varphi$ ist ein bijektiver Gruppenhomomorphismus.

Beispiel 1.70.
(a) φ: $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 2a$ ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$, denn:
$\varphi(a+b) = 2(a+b) = 2a+2b = \varphi(a)+\varphi(b)$ für alle $a, b \in \mathbb{Z}$.
φ ist aber kein Gruppenisomorphismus, denn: φ ist nicht surjektiv ($1 \notin im(\varphi) = \varphi(\mathbb{Z})$).

(b) $n \in \mathbb{N}$. Dann ist $q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \overline{a}$ ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}/n\mathbb{Z}, +)$, denn: $\forall a, b \in \mathbb{Z}$ ist $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b)$ φ ist kein Gruppenisomorphismus, denn φ ist nicht injektiv ($\varphi(0) = \overline{0} = \overline{n} = \varphi(n)$, aber $0 \neq n$).

(c) $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto a+1$ ist kein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$, denn: $\varphi(2+6) = \varphi(8) = 9$, aber $\varphi(2) + \varphi(6) = 3 + 7 = 10$.

(d) $\exp : \mathbb{R} \to \mathbb{R}_{>0} := \{x \in \mathbb{R} | x > 0\}$, $x \mapsto \exp(x) = e^x$ ist ein Gruppenismorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}_{>0}, \cdot)$, denn:
(1) $\exp(a+b) = \exp(a)\exp(b)$ $\forall a, b \in \mathbb{R}$
(2) exp ist bijektiv (vgl. Ana 1 VL).

Bemerkung 1.71. $(G, *)$, $(H, \circledast)$ Gruppen mit neutralen Elementen e_G bzw. e_H, $\varphi : G \to H$ Gruppenhomomorphismus. Dann gilt:
(a) $\varphi(e_G) = e_H$
(b) $\forall a \in G$ ist $\varphi(a') = \varphi(a)'$ (hierbei bezeichnet ' das Inverse)
(c) Ist φ ein Gruppenismorphismus, dann ist $\varphi^{-1} : H \to G$ ebenfalls ein Gruppenisomorphismus.
$(G, *)$, $(H, \circledast)$ heißen isomorph $\Leftrightarrow$ Es existiert ein Gruppenisomorphismus $\psi : G \to H$. Wir schreiben dann $(G, *) \cong (H, \circledast)$.

1.7. Ringe und Körper

Definition 1.72. Ein Ring ist ein Tripel $(R, +, \cdot)$, bestehend aus einer Menge R und zwei Verknüpfungen:
$+ : R \times R \to R$, $(a, b) \mapsto a + b$ (gennant Addition)
$\cdot : R \times R \to R$, $(a, b) \mapsto ab$ (gennant Multiplikation)
welche den folgenden Bedingungen genügen:
(R1) $(R, +)$ ist eine abelsche Gruppe
(R2) $(R, \cdot)$ ist ein Monoid
(R3) Es gelten die Distributivgesetze, d.h für alle $a, b, c \in R$ ist $a \cdot (b+c) = a \cdot b + a \cdot c$, $(a+b) \cdot c = a \cdot c + b \cdot c$
Ein Ring heißt kommutativ $\Leftrightarrow$ Die Multiplikation ist kommutativ, d.h. $a \cdot b = b \cdot a$ für alle $a, b \in \mathbb{R}$.

Anmerkung:

- ohne Klammerung gilt die Kovention "$\cdot$" vor "+", "$\cdot$" wird häufig weggelassen.
- Das neutrale Element bzgl. "+" bezeichnen wir mit 0_R (Nullelement), das neutrale Element bzgl. "$\cdot$" mit 1_R (Einselement). Das zu $a \in R$ bzgl. "+" inverse Element bezeichnen wir mit $-a$, für $a+(-b)$ schreiben wir $a-b$. Existiert zu $a \in R$ ein Inverses bzgl. "$\cdot$", so bezeichnen wir dieses mit a^{-1}
- Wir schreiben häufig verkürzend "R Ring" statt "$(R,+,\cdot)$ Ring"
- In der Literatur wird gelegentlich die Forderung der Existenz eines neutralen Elements bzgl. "$\cdot$" weggelassen, "unser" Ringbegriff entspricht dort dem Begriff "Ring mit Eins".

Beispiel 1.73.
(a) $(\mathbb{Z},+,\cdot)$ ist ein kommutativer Ring.
(b) Nullring $(\{0\},+,\cdot)$ mit $0+0=0$, $0\cdot 0=0$ ist ein kommutativer Ring (hier ist Nullelement = Einselement = 0). Wir bezeichnen den Nullring kurz mit 0.

Bemerkung 1.74. R Ring. Dann gilt:
(a) $0_R \cdot a = 0_R = a \cdot 0_R$ für alle $a \in R$.
(b) $a\cdot(-b) = -ab = (-a)\cdot b$ für alle $a,b \in R$.
(c) Ist $R \neq 0$, dann ist $1_R \neq 0_R$.

Bemerkung 1.75. $n \in \mathbb{N}$. Für $\overline{a},\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ setzen wir $\overline{a}+\overline{b} := \overline{a+b}$, $\overline{a}\cdot\overline{b} := \overline{ab}$
Dann ist $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ ein kommutativer Ring.

Anmerkung: Wenn wir ab jetzt vom Ring $\mathbb{Z}/n\mathbb{Z}$ sprechen, dann meinen wir $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ mit den obigen Verknüpfungen.

Beispiel 1.76. (Verknüpfungstafeln für $\mathbb{Z}/n\mathbb{Z}$)

n=3:

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

n=3:

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

n=4:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

n=4:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

In $\mathbb{Z}/4\mathbb{Z}$ ist $\overline{2}\cdot\overline{2} = \overline{0}$, aber $\overline{2} \neq \overline{0}$.

Definition 1.77. Ein Integritätsbereich ist ein kommutativer Ring $(R,+,\cdot)$ mit $R \neq 0$, in dem gilt:
Für alle $a,b \in R$ gilt: $a\cdot b = 0_R \Rightarrow a = 0_R$ oder $b = 0_R$
(bzw. äquivalent dazu: $a \neq 0_R$ und $b \neq 0_R \Rightarrow ab \neq 0_R$)

Beispiel 1.78. $\mathbb{Z}/3\mathbb{Z}$ ist ein Integritätsbereich, $\mathbb{Z}/4\mathbb{Z}$ ist kein Integritätsbereich, denn $\overline{2}\cdot\overline{2} = \overline{0}$, aber $\overline{2} \neq \overline{0}$.

Bemerkung 1.79. $n \in \mathbb{N}$. Dann sind äquivalent:
(i) $\mathbb{Z}/n\mathbb{Z}$ ist ein Integritätsbereich
(ii) n ist eine Primzahl.

Definition 1.80. Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$, in dem gilt:
$K \neq 0$ und jedes Element $a \in K, a \neq 0$ besitzt ein Inverses in K bzgl. "$\cdot$", d.h. es existiert $b \in K$ mit $ab = 1_K$.
Wir setzen $K^* := K\backslash\{0\}$.

Beispiel 1.81.
(a) $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ sind Körper (mit den übl $+, \cdot$)
(b) $\mathbb{Z}/3\mathbb{Z}$ ist ein Körper (betr. Verknüpfungstafel)
(c) $\mathbb{Z}/4\mathbb{Z}$ ist kein Körper: Das Element $\overline{2}$ besitzt kein Inverses bzgl "$\cdot$".

Bemerkung 1.82. K Körper. Dann gilt:
(a) $0_K \neq 1_K$
(b) K ist ein Integritätsbereich
(c) $(K^*, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_K.

Bemerkung 1.83. R Integritätsbereich, der nur endlich viele Elemente hat. Dann ist R ein Körper.

Folgerung 1.84. $n \in \mathbb{N}$. Dann sind äquivalent:
(i) $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper
(ii) n ist eine Primzahl.

Notation: p Primzahl. Mann nennt $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ auch den endlichen Körper mit p Elementen.

Definition 1.85. R Ring

$$char(R) := \begin{cases} 0, \text{ falls } 1_R + \cdots + 1_R \neq 0_R \text{ für alle } n \in \mathbb{N} \\ \min\{n \in \mathbb{N} | \underbrace{1_R + \cdots + 1_R}_{n-\text{mal}} = 0_R\}, \text{ sonst} \end{cases}$$

heißt die Charaktersitik von R.

Beispiel 1.86.
(a) $char(\mathbb{Z}) = char(\mathbb{Q}) = char(\mathbb{R}) = 0$
(b) $char(\mathbb{Z}/n\mathbb{Z}) = n$, denn: $\underbrace{\overline{1} + \cdots + \overline{1}}_{n-\text{mal}} = \overline{n} = \overline{0}$, und $\underbrace{\overline{1} + \cdots + \overline{1}}_{m-\text{mal}} = \overline{m} \neq \overline{0}$ für $m \in \{1, \ldots, n-1\}$

Bemerkung 1.87. R Integritätsbereich
Dann ist $char(R) = 0$ oder $char(R)$ ist eine Primzahl.

Folgerung 1.88. K Körper
Dann ist $char(K) = 0$ oder $char(K)$ ist eine Primzahl.

Beispiel 1.89. p Primzahl, dann ist $char(\mathbb{F}_p) = p$.

1.8. Polynome

Definition 1.90. (naive Def.) K Körper
Ein Polynom in der Variablen t über K ist ein Ausdruck der Form:
$f = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ mit $n \in \mathbb{N}_0$ (d.h. insbesondere: nur endlich viele Summanden), $a_0, \ldots a_n \in K$ ("fehlende" $a_{i's} = 0$, ebenso setzen wir $a_{n+1} = \cdots = a_{n+2} = 0$). Die a_i heißen die Koeffizienten von f.
$\deg(f) := \begin{cases} -\infty, \text{ falls } f = 0 \text{ (d.h. alle Koeffizienten = 0)} \\ max\{k \in \mathbb{N}_0 | a_k \neq 0\}, \text{ falls } f \neq 0 \end{cases}$ heißt der Grad von f.
Für $f \neq 0$ heißt $l(f) := a_{\deg(f)}$ der Leitkoeffizient von f, $l(0) := 0$. f heißt normiert $\Leftrightarrow l(f) = 1$
Hierbei sind zwei Polynome $f = a_n t^n + \cdots + a_0$, $g = b_m t^m + \cdots + b_0$ gleich ($f = g$)
$\Leftrightarrow \deg(f) = \deg(g) =: r$ und $a_r = b_r, \ldots, a_1 = b_1, a_0 = b_0$.

Beispiel 1.91.
(a) $f = \frac{3}{4}X^2 - 7X + \frac{1}{2} \in \mathbb{Q}[X] \Rightarrow \deg(f) = 2, l(f) = \frac{3}{4}$, f ist nicht normiert.
(b) $f = X^5 - \frac{1}{3}X + \frac{2}{5} \in \mathbb{Q}[X] \Rightarrow \deg(f) = 5, l(f) = 1$, f ist normiert.

Bemerkung 1.92. K Körper, $f, g \in K[t]$, $f = a_n t^n + \cdots + a_1 t + a_0$, $g = b_m t^m + \cdots + b_1 t + b_0$
Wir setzen $r := max\{m, n\}$ und definieren:
$f + g := (a_r + b_r)t^r + \cdots + (a_1 + b_1)t + (a_0 + b_0)$
$f \cdot g := c_{n+m}t^{n+m} + \cdots + c_1 t + c_0$, $c_k := \sum_{i,j \in \mathbb{N}_0, i+j=k} a_i b_j$
Mittels der Verknüpfung $+, \cdot$ wird die Menge aller Polynome über K in der Variablen t (=: $K[t]$) zu einem kommutativen Ring, dem Polynomring über K in der Variablen t.

Bemerkung 1.93. K Körper, $f, g \in K[t]$. Dann gilt:
(a) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
(b) $\deg(fg) = \deg(f) + \deg(g)$
(Hierbei setzt man formal für $n \in \mathbb{N} : -\infty < n$, $n + (-\infty) = -\infty = (-\infty) + n, (-\infty) + (-\infty) = -\infty$).

Folgerung 1.94. K Körper
Dann ist $K[t]$ ein Integritätsbereich.

Anmerkung: $K[t]$ ist kein Körper: Das Polynom $t \in K[t]$ besitzt kein Inverses bzgl. "$\cdot$", denn: Wäre $f \in K[t]$ invers zu t, dann wäre $f \cdot t = 1 \Rightarrow 0 = \deg(1) = \deg(f \cdot t) = \deg(f) + \deg(t) = \deg(f) + 1 \Rightarrow \deg(f) = -1 \lightning$

Satz 1.95. (Polynomdivision)
K Körper, $f, g \in K[t], g \neq 0$
Dann existieren eindeutig bestimmte Polynome $q, r \in K[t]$ mit
$f = qg + r$ und $\deg(r) < \deg(g)$.

Definition 1.96. $f \in K[t]$, $f = a_n t^n + \cdots + a_1 t + a_0$, $\lambda \in K$
Wir setzen $f(\lambda) := a_n \lambda^n + \cdots + a_1 \lambda + a_0 \in K$
λ heißt Nullstelle von $f \Leftrightarrow f(\lambda) = 0$

Bemerkung 1.97. K Körper, $f \in K[t], \lambda \in K$ Nullstelle von f
Dann gibt es in $K[t]$ ein eindeutig bestimmtes Polynom q mit $f = (t-\lambda)q$.
Es ist $\deg(q) = \deg(f) - 1$.

Folgerung 1.98. K Körper, $f \in K[t]$, $f \neq 0$, $n := \deg(f)$
Dann besitzt f in K höchstens n Nullstellen.

Definition 1.99. K Körper, $f \in K[t]$, $f \neq 0$, $\lambda \in K$
$\mu(f,\lambda) := \max\{e \in \mathbb{N}_0 |$ Es existiert ein $g \in K[t]$ mit $f = (t-\lambda)^e g\}$ heißt die Vielfachheit der Nullstelle λ von f.

Anmerkung:

- Es ist $\mu(f,\lambda) = 0 \Leftrightarrow f(\lambda) \neq 0 \Leftrightarrow \lambda$ keine Nullstelle von f.
  (denn: $f(\lambda) = 0 \overset{1.97}{\Longleftrightarrow}$ Es existiert $q \in K[t]$ mit $f = (t-\lambda)q \Leftrightarrow \mu(f,\lambda) \neq 0$)
- Die Vielfachheit von λ gibt an, wie oft der Linearfaktor $t-\lambda$ in f vorkommt.
- Sind $\lambda_1, \ldots, \lambda_m \in K$ sämtliche verschiedene Nullstellen von f und ist $e_i := \mu(f,\lambda_i)$, $i = 1, \ldots, m$, dann ex. ein Polynom $g \in K[t]$ mit $f = (t-\lambda_1)^{e_1} \cdot \ldots \cdot (t-\lambda_m)^{e_m} g$ und den Eigenschaften, dass g in K keine NS besitzt, und dass $\deg(g) = \deg(f) - (e_1 + \cdots + e_m)$.
- "bester Fall": $\deg(g) = 0$ ("f zerfällt in Linearfaktoren"):
  Dann ex. $a \in K\backslash\{0\}, \lambda_1, \ldots, \lambda_m \in K$ paarweise verschieden, $e_1, \ldots, e_n \in \mathbb{N}$ mit $f = a(t-\lambda_1)^{e_1} \cdot \ldots \cdot (t-\lambda_m)^{e_m}$, $e_1 + \cdots + e_m = \deg(f)$
  alternative Darstellung: $f = a(t-\tilde{\lambda}_1) \cdot \ldots \cdot (t-\tilde{\lambda}_n), n = \deg(f), \tilde{\lambda}_1, \ldots \tilde{\lambda}_n$ nicht notwendig verschieden.

Satz 1.100. (Fundamentalsatz der Algebra)
Jedes Polynom $f \in \mathbb{C}[t]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle.

Folgerung 1.101. $f \in \mathbb{C}[t]$, $f \neq 0$
Dann zerfällt f in Linearfaktoren.

Definition 1.102. K Körper, $f \in K[t]$
f induziert eine Abbildung $\tilde{f} : K \to K, \lambda \mapsto f(\lambda)$
$\tilde{f}$ heißt die Polynomfunktion zum Polynom f.

Beispiel 1.103. Es ist wichtig, zwischen dem Polynom $f \in K[t]$ und der dazugehörigen Polynomfunktion $\tilde{f} : K \to K$ zu unterscheiden:
Sei $f = t^2 + t \in \mathbb{F}_2[t]$. Dann ist $f(\overline{0}) = \overline{0}^2 + \overline{0} = \overline{0}$, $f(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{0}$, d.h. $\tilde{f} : \mathbb{F}_2 \to \mathbb{F}_2$ ist die Nullabbildung, aber f ist nicht das Nullpolynom.

Bemerkung 1.104. K Körper mit unendlich vielen Elementen
Dann ist die Abb. $\sim: K[t] \to \mathrm{Abb}(K,K) := \{g : K \to K$ Abbildung$\}$
$f \mapsto \tilde{f}$
injektiv, d.h.: Ist K unendlich und sind $f_1, f_2 \in K[t]$, dann gilt: $f_1 = f_2 \Leftrightarrow \tilde{f}_1 = \tilde{f}_2$.

Anmerkung:

- Lässt man in 1.104 die Voraussetzung "K hat unendlich viele Elemente" weg, wird die Aussage falsch: siehe Bsp. 1.103
- Mit dem Wissen von 1.103/1.104 im Hintergrund bezeichnet man die vom Polynom f induzierte Polynomfunktion mit f anstelle von $\tilde{f}$

2. Vektorräume

In diesem Kapitel sei K stets ein Körper.

2.1. Vektorräume

Definition 2.1.
Ein K-Vektorraum ist ein Tripel $(V, +, \cdot)$, bestehend aus einer Menge V, einer Verknüpfung $+ : V \times V \to V$, $(v, w) \mapsto v + w$ (genannt Addition)
und einer äußeren Verknüpfung $\cdot : K \times V \to V$, $(\lambda, v) \mapsto \lambda \cdot v$ (genannt skalare Multiplikation)),
welche folgenden Bedingungen genügen:
(V1) $(V, +)$ ist eine abelsche Gruppe
(V2) Die skalare Multiplikation ist in folgender Weise mit den anderen Verknüpfungen (auf V und K) verträglich: Für alle $\lambda, \mu \in K, v, w \in V$ ist:
$(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
$\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$
$\lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$
$1 \cdot v = v$

Anmerkung:

- Es ist wichtig, zwischen Addition "+" und sklarer Multiplikation "$\cdot$" auf V und Addition und Multiplikation in K zu unterscheiden: In der Gleichung $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ sind etwa die Verknüpfungen wie folgt zu verstehen:
  $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
  (Addition in K) (skal. Mul) (skal. Mul.) (Addition in V) (skal. Mul.)
- Das neutrale Element bzgl. "+" auf V bezeichnen wir mit 0_V (Nullvektor), das Inverse zu $v \in V$ bzgl. "+" mit $-v$. Das Zeichen "$\cdot$" für die skalare Multiplikation lassen wir ab jetzt meistens weg und schreiben λv statt $\lambda \cdot v$ (für $\lambda \in K, v \in V$)

Beispiel 2.2.
(a) $n \in \mathbb{N}$, $K^n := \{(x_1, \ldots, x_n) | x_1, \ldots, x_n \in K\}$ mit
$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$
$\lambda \cdot (x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n)$, $(\lambda \in K, (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n)$
ist ein K-VR, der sogenannte Standardvektorraum über K.
Die Axiome rechnet man nach, exemplarisch: Sind $\lambda, \mu \in K$, $(x_1, \ldots, x_n) \in K^n$, dann ist: $(\lambda + \mu) \cdot (x_1, \ldots, x_n) =$
$((\lambda + \mu)x_1, \ldots, (\lambda + \mu)x_n) = (\lambda x_1 + \mu x_1, \ldots, \lambda x_n + \mu x_n)$
$= (\lambda x_1, \ldots, \lambda x_n) + (\mu x_1, \ldots, \mu x_n) = \lambda(x_1, \ldots, x_n) + \mu(x_1, \ldots, x_n)$
Der Nullvektor ist gegeben durch $0_{K^n} = (0, \ldots, 0)$, für $x = (x_1, \ldots, x_n)$ ist $-x = (-x_1, \ldots, -x_n)$.

(b) $\mathbb{C}$ ist ein $\mathbb{R}$-VR bzgl. + = übliche Addition auf $\mathbb{C}$,
skalare Mul. $\cdot : \mathbb{R} \times \mathbb{C} \to \mathbb{C}$, $\lambda \cdot (a + i \cdot b) := \lambda a + i\lambda b$

(c) $K[t]$ Polynomring über K in der Variablen t wird zum K-VR durch + = Addition von Polynomen, skalare Mul. $\cdot : K \times K[t] \to K[t]$, $\lambda \cdot (a_n t^n + \cdots + a_1 t + a_0) := \lambda a_n t^n + \cdots + \lambda a_1 t + \lambda a_0$

(d) M Menge
Abb $(M, K) := \{f : M \to K \text{ Abb}\}$ wird zum K-VR durch die folgenden Verknüpfungen:
Addition: Zu $f, g \in$ Abb.(M, K) wird $f + g := M \to K$ definiert über:
$(f + g)(x) := f(x) + g(x)$ für $x \in M$
skalare Mult.: Zu $\lambda \in K$, $f \in$ Abb(M, K) wird $\lambda f : M \to K$ definiert über:
$(\lambda f)(x) := \lambda f(x)$ für $x \in M$
("punktweise Addition und skalare Multiplikation")

Bemerkung 2.3. V K-VR. Dann gilt:
(a) $0_K \cdot v = 0_V$ für alle $v \in V$
(b) $\lambda \cdot 0_V = 0_V$ für alle $\lambda \in K$
(c) $\lambda \cdot v = 0_v \Rightarrow \lambda = 0_K$ oder $v = 0_V$
(d) $(-1_K) \cdot v = -v$ für alle $v \in V$

Definition 2.4. V K-VR, $U \subseteq V$
U heißt Untervektorraum (K-Untervektorraum), kurz: UVR, von V
$\Leftrightarrow$ die folgenden Bedingungen sind erfüllt:
(U1) $U \neq \emptyset$
(U2) $v, w \in U \Rightarrow v + w \in U$ (d.h. U ist abgeschlossen bzgl. Addition)
(U3) $v \in U, \lambda \in K \Rightarrow \lambda v \in U$ (d.h. U ist abgeschlossen bzgl. skal. Mult.)

Bemerkung 2.5. V K-VR, $U \subseteq V$
Dann sind äquivalent:
(i) U ist ein UVR von V
(ii) Addition und skal. Mult. auf V induzieren durch Einschränkung auf U Verknüpfungen
$+ : U \times U \to U$, $\cdot : K \times U \to U$, und bzgl. dieser Verknüpfungen ist U ein K-VR.

Beispiel 2.6.
(a) $K = \mathbb{R}$, $V = \mathbb{R}^2$
Es sei $U = \{(x_1, x_2) \in \mathbb{R}^2 | x_1 - 2x_2 = 0\}$ (ist ein UVR)
(b) $K = \mathbb{R}$, $V = \mathbb{R}^2$
Es sei $U = \{(x_1, x_2) \in \mathbb{R}^2 | x_1 - 2x_2 = 1\}$ Es ist $(0,0)(= 0_V) \notin U$, also: U ist kein UVR von $V = \mathbb{R}^2$.
(c) $K = \mathbb{R}, V = \mathbb{R}^2$
Es sei $U = \{(x_1, x_2) \in \mathbb{R}^2 | x_1 \geq 0 \text{ und } x_2 \geq 0\}$
U ist kein UVR von V, denn: $(5,2) \in U$, aber $(-1) \cdot (5,2) = (-5,-2) \notin U$
(d) $V = K[t]$
Es sei $U = \{f \in K[t] | \deg(f) \leq 2\} = \{f \in K[t] |$ Es ex. $a_0, a_1, a_2 \in K$ mit $f = a_2 t^2 + a_1 t + a_0\}$ (ist UVR)
(e) V K-VR. Dann sind $\{0\}$, V UVR von V ("triviale UVR")
$\{0\}$ heißt der Nullvektorraum (Nullraum)

Bemerkung 2.7. V K-VR, I Indexmenge, $(U_i)_{i \in I}$ Familie von UVR von V (d.h. für jedes $i \in I$ ist ein UVR U_i von V gegeben). Dann gilt:
$U := \bigcap_{i \in I} U_i$ ist ein UVR von V.
Mit anderen Worten: Der Durchschnitt von UVRen von V ist wieder ein UVR von V.

Beispiel 2.8. Die Vereinigung von UVR ist im Allgemeinen kein UVR: z.B.: $K = \mathbb{R}$, $V = \mathbb{R}^2$
$U_1 = \{(x_1, x_2) \in \mathbb{R}^2 | x_1 = x_1\}$
$U_2 = \{(x_1, x_2) \in \mathbb{R}^2 | 2x_1 = x_2\}$
Aber: $U_1 \cup U_2$ ist kein UVR von $\mathbb{R}^2$, denn: $(1,1) \in U_1 \subseteq U_1 \cup U_2$, $(2,4) \in U_2 \subseteq U_1 \cup U_2$
aber: $(1,1) + (2,4) = (3,5) \notin U_1 \cup U_2$

Definition 2.9. V K-VR, $(v_1, \ldots, v_r)$ endl. Familie von Vektoren aus V
$\text{Lin}((v_1, \ldots, v_r)) := \{\alpha v_1 + \cdots + \alpha v_r | \alpha_1, \ldots, \alpha_r \in K\}$
heißt die lineare Hülle (das Erzeugnis) der Familie $v_1, \ldots v_r$
$v \in V$ heißt Linearkombination von $v_1, \ldots v_r \Leftrightarrow v \in \text{Lin}((v_1, \ldots, v_r)) \Leftrightarrow$ Es ex. $\alpha_1, \ldots, \alpha_r \in K$ mit $v = \alpha_1 v_1 + \ldots \alpha_r v_r$

Beispiel 2.10.
(a) $V = \mathbb{R}^3$, $K = \mathbb{R}$
$v \in V$ $v \neq 0 \Rightarrow \text{Lin}((v)) = \{\alpha v | \alpha \in \mathbb{R}\}$ = Gerade durch 0 und v
$v, w \in V$, $v \neq 0 \Rightarrow \text{Lin}((v,w)) = \{\alpha_1 v + \alpha_2 w | \alpha_1, \alpha_2 \in \mathbb{R}\} = \begin{cases} \text{Gerade durch } 0, v \text{ , falls } w \in \text{Lin}((v)) \\ \text{Ebene durch } 0, v, w \text{ , falls } w \notin \text{Lin}((v)) \end{cases}$

(b) $V = K^n$ als K-VR

$e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$

i-te Stelle

$$\begin{aligned}\mathrm{Lin}((e_1, \ldots, e_n)) &= \{\alpha_1 e_1 + \cdots + \alpha_n e_n | \alpha_1, \ldots, \alpha_n \in K\} \\ &= \{(\alpha_1, 0, \ldots, 0) + (0, \alpha_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, \alpha_n) | \alpha_1, \ldots, \alpha_n \in K\} \\ &= \{(\alpha_1, \ldots, \alpha_n) | \alpha_1, \ldots, \alpha_n \in K\} \\ &= K^n\end{aligned}$$

Definition 2.11. V K-VR, $(v_i)_{i \in I}$ Familie von Vektoren aus V

$\mathrm{Lin}((v_i)_{i \in I}) := \{ \sum_{i \in I} \alpha_i v_i | \alpha_i \in K$ für alle $i \in I, \alpha_i = 0$ für fast alle $i \in I\}$

heißt lineare Hülle (das Erzeugnis) der Familie $(v_i)_i \in I$

Hierbei bedeutet "$\alpha_i = 0$ für fast alle $i \in I$": Es gibt nur endlich viele $i \in I$ mit $\alpha_i \neq 0$, d.h. die auftretenden Summen sind endliche Summen.

Falls $I = \emptyset$, setzen wir $\mathrm{Lin}((v_i)_{i \in \emptyset}) := \{0\}$.

Anmerkung: Ein Element $v \in V$ ist genau dann in $\mathrm{Lin}((v_i)_{i \in I})$ enthalten, wenn es eine endl. Teilmenge $\{i_1, \ldots, i_r\} \subseteq I$ und Elemente $\alpha_{i_1}, \ldots, \alpha_{i_r} \in K$ gibt mit $v = \alpha_{i_1} v_{i_1} + \cdots + \alpha_{i_r} v_{i_r}$

Insbesondere ist $\mathrm{Lin}((v_i)_{i \in I}) = \bigcup_{J \subseteq I \text{ endlich}} \mathrm{Lin}((v_i)_{i \in J})$

Beispiel 2.12. $V = K[t]$ als K-VR

Es ist $\mathrm{Lin}((t^n)_{n \in \mathbb{N}_0}) = \{ \sum_{i \in \mathbb{N}_0} \alpha_i t^i | \alpha_i \in K, \alpha_i = 0$ für fast alle $i \in \mathbb{N}_0\} = K[t]$

Bemerkung 2.13. V K-VR, $(v_i)_{i \in I}$ Familie von Vektoren aus V

Dann gilt:

(a) $\mathrm{Lin}((v_i)_{i \in I})$ ist ein UVR von V

(b) Ist $U \subseteq V$ ein UVR mit $v_i \in U$ für alle $i \in I$, dann ist $\mathrm{Lin}((v_i)_{i \in I}) \subseteq U$, d.h. $\mathrm{Lin}((v_i)_{i \in I})$ ist das bzgl. "$\subseteq$" kleinste Element der Menge derjenigen UVR von V, die alle $v_i, i \in I$, enthalten.

(c) $\mathrm{Lin}((v_i)_{i \in I}) = \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U \text{ für alle } i \in I} U$

Notation: Ist $M \subseteq V$, dann setzen wir $\mathrm{Lin}(M) := \mathrm{Lin}((m)_{m \in M})$ (kleinster UVR von V, der alle Elemente aus M enthält)

Vorteil der Definition von Lin(...) für Familien von Vektoren: Bei Familien ist es sinnvoll zu sagen, dass ein Vektor mehrfach vorkommt (im Gegensatz zu Mengen), darüber hinaus haben die Vektoren der Familie $(v_i)_{i \in I}$ im wichtigen Spezialfall $I = \{1, \ldots, n\}$, Familie $(v_1, \ldots, v_n)$ eine natürliche Reihenfolge. Diese geht verloren, wenn man die Menge $\{v_1, \ldots, v_n\}$ betrachtet (z.B. in $\mathbb{R}^2$: $\{e_1, e_2\} = \{e_2, e_1\}$, aber $(e_1, e_2) \neq (e_2, e_1)$)

Definition 2.14. V K-VR, $(v_1, \dots v_r)$ endl. Familie von Vektoren aus V
$(v_1, \dots, v_r)$ linear unabhängig $\Leftrightarrow$ Sind $\lambda_1, \dots \lambda_r \in K$ mit $\lambda_1 v_1 + \dots + \lambda_r v_r = 0$, dann folgt $\lambda_1 = \dots = \lambda_r = 0$
Mit anderen Worten: Der Nullvektor lässt sich nur auf triviale Weise aus der Familie $(v_1, \dots, v_r)$ linear kombinieren. $(v_1, \dots, v_r)$ heißt linear abhängig $\Leftrightarrow$ $(v_1, \dots, v_r)$ ist nicht linear unabhängig $\Leftrightarrow$ Es ex. $\lambda_1, \dots, \lambda_r \in K$ mit $(\lambda_1, \dots, \lambda_r) \neq (0, \dots, 0)$ und $\lambda_1 v_1 + \dots + \lambda_r v_r = 0$

$(v_i)_{i \in I}$ Familie von Vektoren aus V
$(v_i)_{i \in I}$ heißt linear unabhängig $\Leftrightarrow$ Jede endl. Teilfamilie von $(v_i)_{i \in I}$ ist linear unabhängig, d.h. für jede endl. Teilmenge $J \subseteq I$ ist $(v_i)_{i \in J}$ linear unabhängig.
$(v_i)_{i \in I}$ heißt linear abhängig $\Leftrightarrow$ $(v_i)_{i \in I}$ ist nicht linear unabhängig
$\Leftrightarrow$ Es ex. eine endl. Teilfamilie $(v_i)_{i \in J}$ von $(v_i)_{i \in I}$, die linear abhängig ist.
$\Leftrightarrow$ Es gibt eine endl. Teilmenge $J = \{i_1, \cdots r\} \subseteq I, \lambda_{i_1}, \dots, \lambda_{i_r} \in K$ mit $(\lambda_{i_1}, \dots, \lambda_{i_r}) \neq (0, \dots, 0)$ und $\lambda_{i_1} v_{i_1} + \dots + \lambda_{i_r} v_{i_r} = 0$
$M \subseteq V$ heißt linear (un-)abhängig $\Leftrightarrow$ $(m)_{m \in M}$ ist linear (un-)abhängig.

Beispiel 2.15.
(a) $V = K^n$ als K-VR.
Die Familie $(e_1, \dots, e_n)$ (vgl. 2.10) ist linear unabhängig, denn:
Sind $\lambda_1, \dots, \lambda_n \in K$ mit $\lambda_1 e_1 + \dots + \lambda_n e_n = 0$, dann ist

$$\underbrace{\underbrace{\lambda_1(1,0,\dots,0)}_{=(\lambda_1,0,\dots,0)} + \underbrace{\lambda_2(0,,1,0,\dots,0)}_{=(0,\lambda_2,0,\dots,0)} + \dots + \underbrace{\lambda_n(0,\dots,0,1)}_{=(0,\dots,0,\lambda_n)} = 0}_{=(\lambda_1,\dots,\lambda_n)} \quad \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n = 0.$$

(b) $K = \mathbb{R}$, $V = \mathbb{R}^2$
Die Familie $((1,-1),(0,2),(1,2))$ ist linear abhängig, denn: $2 \cdot (1,-1) + 3 \cdot (0,2) - 2 \cdot (1,2) = 0$, es gibt also eine nichttriviale Linearkombination der Null aus den Vektoren der Familie.
(c) $V = K[t]$ als K-VR
Die Familie $(t^n)_{n \in \mathbb{N}_0}$ ist linear unabhängig, denn: Sei $J = \{n_1, \dots, n_r\} \subseteq \mathbb{N}_0$ eine endliche Teilmenge von $\mathbb{N}_0$, und sind $\lambda_{n_1}, \dots, \lambda_{n_r} \in K$, dann folgt aus $\lambda_{n_1} t^{n_1} + \dots + \lambda_{n_r} t^{n_r} = 0$ sofort: $\lambda_{n_1} = \dots = \lambda_{n_r} = 0$ (vgl. Def. von "=" von Polynomen)
Also: Jede endl. Teilfamilie von $(t^n)_{n \in \mathbb{N}_0}$ ist linear unabhängig, also ist $(t^n)_{n \in \mathbb{N}_0}$ linear unabhängig.

Bemerkung 2.16. V K-VR, $(v_i)_{i \in I}$ Familie von Vektoren aus V
Dann sind äquivalent:
(i) $(v_i)_{i \in I}$ ist linear unabhängig
(ii) Jeder Vektor $v \in \text{Lin}((v_i)_{i \in I})$ lässt sich in eindeutiger Weise aus Vektoren der Familie $(v_i)_{i \in I}$ linear kombinieren.

Bemerkung 2.17. V K-VR. Dann gilt:
(a) Ist $v \in V$, dann gilt: (v) linear unabhängig $\Leftrightarrow v \neq 0$
(b)Gehört der Nullvektor zu einer Familie, dann ist sie linear abhängig.
(c) Kommt der gleiche Vektor in einer Familie mehrfach vor, so ist sie linear abhängig.
(d) Ist $r \geq 2$, so gilt: Die Familie $(v_1, \ldots, v_r)$ von Vektoren aus V ist linear abhängig $\Leftrightarrow$ Es ex. ein $i \in \{1, \ldots, r\}$, so dass v_i Linearkombination von $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_r$ ist.

2.2. Basis und Dimension

In diesem Abschnitt sei V stets ein K-VR.

Definition 2.18. $(v_i)_{i \in I}$ Familie von Vektoren aus V
$(v_i)_{i \in I}$ heißt ein Erzeugendensystem (ES) von $V \Leftrightarrow V = \text{Lin}((v_i)_{i \in I})$
V heißt endlich erzeugt $\Leftrightarrow V$ besitzt ein endliches Erzeugendensystem (d.h. es ex. eine endliche Familie $(v_1, \ldots, v_n)$ von Vektoren aus V mit $V = \text{Lin}((v_1, \ldots, v_n))$).
$(v_i)_{i \in I}$ heißt eine Basis von $V \Leftrightarrow (v_i)_{i \in I}$ ist ein linear unabhängiges ES von V. Ist $B = (v_1, \ldots, v_n)$ eine endl. Basis von V, dann heißt n die Länge von B.

Beispiel 2.19.
(a) Die Familie $(e_1, \ldots, e_n)$ ist eine Basis des K-VR K^n, da $\text{Lin}((e_1, \ldots, e_n)) = K^n$ (vgl. 2.10(b)) und somit $(e_1, \ldots, e_n)$ ES des K^n, und $(e_1, \ldots, e_n)$ linear unabhängig nach 2.15(a). Die Länge der Basis $(e_1, \ldots, e_n)$ ist n. $(e_1, \ldots, e_n)$ heißt die kanonische Basis oder Standardbasis des K^n.
(b) Die Familie $(t^n)_{n \in \mathbb{N}_0}$ ist eine Basis des K-VR $K[t]$, denn: $\text{Lin}((t^n)_{n \in \mathbb{N}_0}) = K[t]$ nach Bsp. 2.12, $(t^n)_{n \in \mathbb{N}_0}$ ist linear unabhängig nach 2.15(c)
(c) $((1,-1),(0,2),(1,2))$ ist ein ES des $\mathbb{R}$-VR $\mathbb{R}^2$, denn für jedes $(x_1, x_2) \in \mathbb{R}^2$ ist $(x_1, x_2) = x_1(1,-1) + \frac{x_1+x_2}{2}(0,2) \in \text{Lin}((1,-1),(0,2),(1,2))$. $((1,-1),(0,2),(1,2))$ ist jedoch keine Basis des $\mathbb{R}^2$, da linear abhängig nach 2.15(b)
(d) Die leere Familie () ist eine Basis des Nullraums $\{0\}$: vgl. 2.11 und Anm. nach 2.14

Anmerkung: Jeder Vektorraum V besitzt ein ES, denn es ist $V = \text{Lin}((v)_{v \in V})$

Satz 2.20. $V \neq \{0\}$, $B = (v_1, \ldots, v_n)$ endliche Familie von Vektoren aus V
Dann sind äquivalent:
(i) B ist eine Basis von V, d.h. ein linear unabhängiges ES von V
(ii) B ist ein unverkürzbares ES von V, d.h. B ist ein ES und für jedes $r \in \{1, \ldots, n\}$ ist $(v_1, \ldots, v_{r-1}, v_{r+1}, \ldots, v_n)$ kein ES von V mehr.
(iii) Zu jedem $v \in V$ gibt es eindeutig bestimmte $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$
(iv) B ist unverlängerbar linear unabhängig, d.h. B ist linear abhängig und für jedes $v \in V$ ist die Familie $(v_1, \ldots, v_n, v)$ linear abhängig.

Folgerung 2.21. (Basisauswahlsatz)
Besitzt V ein endliches ES $(v_1, \ldots, v_n)$, dann kann man aus diesem eine Basis auswählen, d.h. es gibt eine Teilmenge $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, so dass $(v_{i_1}, \ldots, v_{i_r})$ eine Basis von V ist. Insbesondere besitzt jeder endlich erzeute Vektorraum eine Basis.

Folgerung 2.22. Jeder endlich erzeugte K-VR besitzt eine Basis von endlicher Länge.

Satz 2.23. (Austauschlemma)
V endl. erzeugter K-VR, $B = (v_1, \ldots, v_r)$ von V, $\lambda_1, \ldots, \lambda_r \in K$, $w = \lambda_1 v_1 + \cdots + \lambda_r v_r$
Dann gilt: Ist $k \in \{1, \ldots, r\}$ mit $\lambda_k \neq 0$, dann ist $B' := (v_1, \ldots, v_{k-1}, w, v_{k+1}, \ldots, v_r)$ ebenfalls eine Basis von V (d.h. man kann v_k gegen w austauschen).

Satz 2.24. (Austauschsatz) V endl. erzeugter K-VR, $(w_1, \ldots, w_n)$ linear unabhängige Familie in V.
Dann gilt:
(a) Ist $B = (v_1, \ldots, v_r)$ eine Basis von V, dann ist $r \geq n$.
(b) Es gibt Indizes $i_1, \ldots, i_n \in \{1, \ldots, r\}$ der Art, dass man aus der Basis $B = (v_1, \ldots, v_r)$ von V nach Austausch von v_{i_1} gegen w_1, v_{i_2} gegen $w_2, \ldots, v_{i_n}$ gegen w_n wieder eine Basis von V erhält. Nummeriert man B so rum, dass $i_1 = 1, i_2 = 2, \ldots, i_n = n$ ist, bedeutet dies, dass $B^* := (w_1, \ldots, w_n, v_n + 1, \ldots, v_r)$ eine Basis von V ist.

Folgerung 2.25. Es gilt:
(a) Ist V endlich erzeugt, dann ist jede Basis von V von endlicher Länge, und je zwei Basen von V haben dieselbe Länge.
(b) Ist V nicht endlich erzeugt, dann ex. für V keine Basis von endlicher Länge.

Definition 2.26.
$\dim_K V := \begin{cases} r, \text{ falls } V \text{ endlich erzeugt, } r \text{ Länge einer(jeder) Basis von } V \\ \infty, \text{ falls } V \text{ nicht endlich erzeugt} \end{cases}$ heißt die Dimension von V über K. Ist $\dim_K V \in \mathbb{N}_0$, dann heißt V endlichdimensional über K.

Beispiel 2.27.
(a) $V = K^n$ Die Standardbasis $(e_1, \ldots, e_n)$ von K^n hat Länge n, d.h. $\dim_K K^n = n$. Insbesondere hat jede Basis von K^n die Länge n.
(b) In $K[t]$ ist die Familie $(t^n)_{n \in \mathbb{N}_0}$ eine Basis unendlicher Länge (vgl. Bsp 2.19(b)). Wäre $K[t]$ endlichdimensional über K, dann wäre jede Basis von $K[t]$ als K-VR von endlicher Länge. Also: $\dim_K K[t] = \infty$
(c) $\dim_{\mathbb{C}} \mathbb{C} = 1$ (siehe(a)), aber: $\dim_{\mathbb{R}} \mathbb{C} = 2$ (denn:$(1, i)$ ist eine Basis von $\mathbb{C}$ als $\mathbb{R}$-VR)

Folgerung 2.28. V endlichdimensionaler K-VR, $U \subseteq V$ UVR von V
Dann gilt:
(a) U ist endlichdimensional
(b) $\dim_K U \leq \dim_K V$
(c) Es ist $U = V \Leftrightarrow \dim_K U = \dim_K V$

Satz 2.29. (Basisergänzungssatz)
V endlich dimensionaler K-VR, $(u_1, \ldots, u_n)$ linear unabhängige Familie in V
Dann ex. $u_{n+1}, \ldots, u_r \in V, r = \dim V$, so dass $B = (u_1, \ldots, u_n, u_{n+1}, \ldots, u_r)$ eine Basis von V ist (d.h.$(u_1, \ldots, u_n)$ kann zu einer Basis ergänzt werden).

Satz 2.30. (Zornsches Lemma)
Jede induktiv geordnete nichtleere Menge $(M, \leq)$ besitzt ein maximales Element. Hierbei heißt eine halbgeordnete Menge $(M, \leq)$ induktiv geordnet $\Leftrightarrow$ Jede Teilmenge $T \subseteq M$, für die $(T, \leq)$ totalgeordnet ist, besitzt eine obere Schranke in $(M, \leq)$, d.h. es ex. ein $S \in M$ mit $t \leq S$ für alle $t \in T$.

Anmerkung: Das Zornsche Lemma ist äquivalent zum Auswahlaxiom.

Satz 2.31. $(u_j)_{j \in J}$ linear unabhängige Familie in V
Dann kann $(u_j)_{j \in J}$ zu einer Basis von V ergänzt werden, d.h. es ex. eine Menge I mit $J \subseteq I$ und eine Familie $(v_i)_{i \in I}$ mit $v_j = u_j$ für alle $j \in J$, so dass $(v_i)_{i \in I}$ eine Basis von V ist. Insbesondere besitzt jeder K-VR eine Basis.

Anmerkung: Der Satz "Jeder VR hat eine Basis" ist äquivalent zum Auswahlaxiom.

2.3. Matrizen

In diesem Abschnitt seien $m, n, r \in \mathbb{N}$
Frage: Gegeben sei ein UVR $U = \text{Lin}((v_1, \ldots, v_m)) \subseteq K^n$. Wie bestimmt man effizient eine Basis von U?

Definition 2.32.
Eine $m \times n$-Matrix mit Einträgen aus K ist eine Familie $(a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{m1}, \ldots, a_{mn})$ von minimalen Elementen aus K, die wir in der Form

$$(a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

(kurz: (a_{ij}) wenn m, n klar sind) schreiben. Die Menge aller $m \times n$-Matrizen mit Einträgen aus K bezeichnen wir mit $M(m \times n, K)$.
Für $A = (a_{ij})$ wie oben heißen $a_i := (a_{i1}, \ldots, a_{in})$, $i = 1, \ldots, m$ die Zeilen der Matrix A. Im Folgenden fassen wir die Zeilen von A als Elemente von K^n auf: $a_i = (a_{i1}, \ldots, a_{in})$.
$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in M(m \times 1, K)$, $j = 1, \ldots, n$ heißen die Spalten der Matrix A.

Bemerkung 2.33. Es gilt:

(a) $M(m\times n,K)$ ist bzgl. der Verknüpfungen:

$+ : M(m\times n,K)\times M(m\times n,K)\to M(m\times n,K), (a_{ij})+(b_{ij}) := (a_{ij}+b_{ij})$

$\cdot : K\times M(m\times n,K)\to M(m\times n,K), \lambda\cdot(a_{ij}) := (\lambda a_{ij})$

ein K-VR. Es ist $\dim_K M(m\times n,K) = m\cdot n$

(b) Durch:

$\cdot : M(m\times n,K)\times M(n\times r,K)\to M(m\times r,K)$

$(a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}\cdot(b_{jk})_{\substack{1\le j\le n\\ 1\le k\le r}} := (c_{ik})_{\substack{1\le i\le m\\ 1\le k\le r}}$

mit $c_{ik} := \sum_{j=1}^{n} a_{ij}b_{jk}$ ist die Multiplikation von Matrizen erklärt.

$$m \text{ Zeilen}\left\{\underbrace{\begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in}\end{pmatrix}}_{n \text{ Spalten}}\cdot\underbrace{\begin{pmatrix} b_{1k}\\ \vdots\\ b_{nk}\end{pmatrix}}_{r \text{ Spalten}}\right\} n \text{ Zeilen} = \underbrace{\begin{pmatrix} c_{ik}\end{pmatrix}}_{r \text{ Spalten}}\Big\} m \text{ Zeilen}$$

Für diese gilt:

Sind $A_1, A_2\in M(m\times n,K)$, $B_1, B_2\in M(n\times r,K)$, $C\in M(r\times s,K), \lambda\in K$, dann ist

$A\cdot(B_1+B_2) = A\cdot B_1 + A\cdot B_2$, $(A_1+A_2)B = A_1B + A_2B$

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

$A(BC) = (AB)C$

$E_m\cdot A = A\cdot E_n = A$.

Hierbei ist für $l\in\mathbb{N}$ $E_l := \begin{pmatrix} 1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}\in M(l\times l,K)$ die $l\times l$- Einheitsmatrix über K.

(c) $M(n\times n,K)$ ist bzgl.

$+,\cdot : M(n\times n,K)\times M(n\times n,K)\to M(n\times n,K)$ ("+" siehe (a), "$\cdot$" siehe (b))

ein Ring (Einselement: E_n). Für $n>1$ ist dieser Ring nicht kommutativ.

Definition 2.34. $A\in M(n\times n,K)$

A heißt invertierbar $\Leftrightarrow$ Es ex. ein $B\in M(n\times n,K)$ mit $AB = BA = E_n$.

Bemerkung 2.35. Es gilt:

$GL(n,K) := \{A\in M(n\times n,K)\,|\,A \text{ ist invertierbar}\}$ ist bzgl. der Matrizenmultiplikation eine Gruppe, die sogenannte allgemeine lineare Gruppe. Das neutrale Element ist E_n, das zur $A\in GL(n,K)$ inverse Element bezeichnen wir mit A^{-1}.

Definition 2.36. $A \in M(m \times n, K)$ mit Zeilen $a_1, \ldots, a_m \in K^n$
Unter elementaren Zeilenummformungen von A verstehen wir die folgenden Umformungen von A:

1. Multiplikation der i-ten Zeile mit $\lambda \in K^* = K \setminus \{0\}$
$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} \rightsquigarrow \begin{pmatrix} \vdots \\ \lambda a_i \\ \vdots \end{pmatrix}$$
2. Addieren der j-ten Zeile zur i-ten Zeile, $i \neq j$
$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \rightsquigarrow \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$
3. Addition des λ-fachen der j-ten Zeile zur i-ten Zeile, $\lambda \in K^*$, $i \neq j$
$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \rightsquigarrow \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$
4. Vertauschen der i-ten Zeile mit der j-ten Zeile, $i \neq j$
$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \rightsquigarrow \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$

Anmerkung:

- Typ 3,4 kann man durch Kombinationen von Umformungen von Typ 1,2 erhalten.
- Analog zu den elementaren Zeilenumformungen definiert man elementare Spaltenumformungen in naheliegender Weise
- Elementare Zeilenumformungen erhält man durch Multiplikation von A mit sogenannten Elementarmatrizen von links, elementare Spaltenumformungen durch Multiplikation von Elementarmatrizen von rechts.

Definition 2.37. $A \in M(m \times n, K)$ mit Zeilen $a_1, \ldots, a_m \in K^n$
$ZR(A) := \text{Lin}((a_1, \ldots, a_m)) \subseteq K^n$ heißt der Zeilenraum von A.

Beispiel 2.38. $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M(2\times 3, \mathbb{Q}) \Rightarrow ZR(A) = \text{ Lin}((1,2,3),(4,5,6)) \subseteq \mathbb{Q}^3$

Bemerkung 2.39. $A, B \in M(m\times n, K)$
Dann gilt: Ist B aus A durch eine endliche Folge elementaren Zeilenumformungen entstanden, dann ist $ZR(B) = ZR(A)$

Definition 2.40. $A = (a_{ij}) \in M(m\times n, K)$
A ist in Zeilenstufenform (ZSF) $\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(Z1) Es gibt eine Zahl $r \in \mathbb{N}_0$ mit $0 \le r \le m$, so dass in den Zeilen mit Index 1 bis r jeweils nicht nur Nullen stehen, und in den Zeilen mit den Indizes $r+1$ bis m stehen nur Nullen.
(Z2) Setzen wir für i mit $1 \le i \le r$ $_{ji} := \min\{j \in \{1,\dots,n\} | a_{ij} \neq 0\}$, dann gilt: $j_1 < j_2 < \dots < j_r$ (Stufenbedingung)
Visualisierung:

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

Die Elemente $a_{1j_1}, \dots, a_{rj_r}$ heißen die Pivots von A (* in Skizze).

Beispiel 2.41.

$$A = \begin{pmatrix} 0 & ③ & 1 & 0 & 4 & \\ 0 & 0 & 0 & ② & 3 & 4 \\ 0 & 0 & 0 & 0 & ⑥ & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

ist in ZSF. Es ist $r = 3$, $j_1 = 2$, $j_2 = 4$, $j_3 = 5$, Pivots: $a_{12} = 3$, $a_{24} = w$, $a_{35} = 6$.

Satz 2.42. $A \in M(m\times n, K)$
Dann lässt sich A durch endlich viele elementare Zeilenumformungen in eine Matrix B in ZSF umformen:

$$B = \begin{pmatrix} b_{1j_1} & * & \dots & \dots & \dots & \dots & * \\ & b_{2j_2} & * & \dots & \dots & \dots & * \\ & & & & & & \vdots \\ & & & & & b_{rj_r} & * \\ & 0 & & & & & \end{pmatrix} \begin{matrix} \} \text{r Zeilen} \\ \\ \\ \\ \} \text{m-r} \end{matrix}$$

Die ersten r Zeilen von B bilden eine Basis von $ZR(A)$.

Satz 2.43.
Eingabe: $W = \text{Lin}((v_1, \ldots, v_m)) \subseteq K^n$
Ausgabe: Eine Basis $(w_1, \ldots, w_r)$ von W
Durchführung:

1. Bilde aus den Zeilenvektoren $v_1, \ldots, v_m$ die Matrix $A \in M(m \times n, K)$
2. Bringe die Matrix A durch elementare Zeilenumformungen auf ZSF B:

$$B = \begin{pmatrix} * & & & \\ & * & & \\ & & \ddots & \\ & & & * \\ & & & \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} \text{r Nichtnullzeilen} \\ \left.\vphantom{\begin{matrix}a\\a\end{matrix}}\right\} \text{m-r Nullzeilen} \end{matrix}$$

3. Die Familie $(w_1, \ldots, w_r)$ der ersten r Zeilenvektoren von B ist eine Basis von W.

Beispiel 2.44. $W = \text{Lin}((0,0,3,-1),(0,1,2,0),(0,3,0,2)) \subseteq \mathbb{R}^4$

$$A = \begin{pmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 3 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & -6 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$\Rightarrow ((0,1,2,0),(0,0,3,-1))$ ist eine Basis von W, insbesondere ist $\dim W = 2$.

Definition 2.45. $A = (a_{ij}) \in M(m \times n, K)$

$A^t := \begin{pmatrix} a_{11} & \ldots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \ldots & a_{mn} \end{pmatrix} \in M(n \times m, K)$ heißt die zu A transponierte Matrix.

Bemerkung 2.46. $A, A_1, A_2 \in M(m \times n, K), B \in M(n \times r, K), \lambda \in K$.
Dann gilt:
(a) $(A_1 + A_2)^t = A_1^t + A_2^t$
(b) $(\lambda A)^t = \lambda A^t$
(c) $(A^t)^t = A$
(d) $(AB)^t = B^t A^t$

Definition 2.47. $A \in M(m \times n, K)$
Zeilenrang $(A) := \dim_K ZR(A)$ heißt der Zeilenrang von A.
$SR(A) := ZR(A^t) \subseteq K^m$ heißt der Spaltenraum von A
Spaltenrang $(A) := \dim_K SR(A)$ heißt der Spaltenrang von A

Beispiel 2.48. Wir betrachten die Matrix A aus Bsp 2.44

$A = \begin{pmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \in M(3\times 4, \mathbb{R})$, nach Bsp 2.44 ist Zeilenrang$(A) = \dim ZR(A) = 2$

$A^t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \in M(4\times 3, \mathbb{R}) \Rightarrow SR(A) := \text{ Lin}((0,0,0),(0,1,3),(3,2,0),(-1,0,2))$

Wir bestimmen eine Basis von $SR(A)$:

$$A^t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 2 & 6 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$\Rightarrow ((-1,0,2),(0,1,3))$ ist eine Basis von $SR(A) \Rightarrow$ Spaltenrang$(A) = 2$.
In diesem Beispiel ist also Zeilenrang(A) = Spaltenrang(A)

2.4. Summen von Untervektorräumen

In diesem Abschnitt sei V stets ein K-VR

Definition 2.49. $U_1, \ldots, U_r \subseteq V$ UVR
$U_1 + \ldots + U_r := \{u_1 + \ldots + u_r | u_1 \in U_1, \ldots, u_r \in U_r\} \subseteq V$ heißt die Summe von $U_1, \ldots, U_r$. Für $U_1 + \ldots + U_r$ schreiben wir auch $\sum_{i=1}^{r} U_i$

Bemerkung 2.50. $U_1, \ldots, U_r \subseteq V$ UVR
Dann gilt:
(a) $U_1 + \ldots + U_r = \text{ Lin}(U_1 \cup \ldots \cup U_r)$, d.h. $U_1 + \ldots + U_r$ ist der kleinste UVR von V, der alle Elemente aus $U_1, \ldots, U_r$ enthält.
(b) Sind $U_1, \ldots, U_r$ endlich-dimensional, dann ist auch $U_1 + \ldots + U_r$ endlichdimensional, und es ist $\dim(U_1 + \ldots + U_r) \leq \dim(U_1) + \ldots + \dim(U_r)$

Beispiel 2.51.
(a) $K = \mathbb{R}$, $V = \mathbb{R}^2$, $U_1 = \text{ Lin}((1,-1))$, $U_2 = \text{ Lin}((1,1))$
$\Rightarrow U_1 + U_2 = \text{ Lin}((1,-1),(1,1)) = \mathbb{R}^2$
(b) $K = \mathbb{R}$, $V = \mathbb{R}^3$, $U_1 = \text{ Lin}((e_1, e_2))$ (="$x_1 - x_2$−Ebene"), $U_2 = \text{ Lin}((e_2, e_3))$ (="$x_2 - x_3$−Ebene") $\Rightarrow$ $U_1 + U_2$ enthält e_1, e_2, e_3 also $U_1 + U_2 = \mathbb{R}^3 \Rightarrow \dim(U_1 + U_2) = 3 < \underbrace{\dim(U_1)}_{=2} + \underbrace{\dim(U_2)}_{=2} = 4$

Satz 2.52. $U_1, U_2 \subseteq V$ endlichdimensionale UVR
Dann gilt: $\dim(U_1 + U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2)$

Definition 2.53. $U_1, \ldots, U_r \subseteq V$ UVR
V heißt direkte Summe von $U_1, \ldots, U_r \Leftrightarrow V = U_1 + \ldots + U_r$ und $U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\}$

Notation: $V = U_1 \oplus \ldots \oplus U_r = \bigoplus_{i=1}^{r} U_i$

Anmerkung: Spezialfall: $r = 2$:
$V = U_1 \oplus U_2 \Leftrightarrow V = U_1 + U_2$ und $U_1 \cap U_2 = \{0\}$. In diesem Fall ist $\dim(V) = \dim(U_1) + \dim(U_2)$
Ist $r \geq 3$, dann genügt für $V = U_1 \oplus \ldots \oplus U_r$ nicht, zu fordern, dass $V = U_1 + \ldots + U_r$ und $U_i \cap U_j = \{0\}$ für $i \neq j$:
z.B.: $K = \mathbb{R}$, $V = \mathbb{R}^2$, $U_1 = \text{ Lin}((e_1))$, $U_2 = \text{ Lin}((e_2))$, $U_3 = \text{ Lin}((1,1))$
Dann $V = U_1 + U_2 + U_3$ und $U_i \cap U_j = \{0\}$ für $i \neq j$, aber $U_1 \cap \underbrace{(U_2 + U_3)}_{=\mathbb{R}^2} = U_1 \neq \{0\}$, d.h die Summe ist nicht direkt.

Beispiel 2.54. (vgl. Bsp 2.51)
(a) $K = \mathbb{R}$, $V = \mathbb{R}^2$, $U_1 = \text{ Lin}((1,-1)$, $U_2 = \text{ Lin}((1,1)) \Rightarrow V = U_1 \oplus U_2$
(b) $K = \mathbb{R}$, $V = \mathbb{R}^3$, $U_1 = \text{ Lin}((e_1, e_2))$, $U_2 = \text{ Lin}((e_2, e_3)) \Rightarrow V = U_1 + U_2$, aber die Summe ist nicht direkt, denn: $e_2 \in U_1 \cap U_2$

Bemerkung 2.55. $U_1, \ldots, U_r \subseteq V$ Dann sind äquivalent:
(i) $V = U_1 \oplus \ldots \oplus U_r$
(ii) Für jedes $v \in V$ existiert ein bestimmtes $u_i \in U_i, i = 1, \ldots, r$ mit $v = u_1 + \ldots + u_r$

Satz 2.56. V endlichdimensionaler K-VR, $U_1, \ldots U_r \subseteq V$ UVR
Dann sind äquivalent;
(i) $V = U_1 \oplus \ldots \oplus U_r$
(ii) Für alle Basen $B_i = (v_1^{(i)}, \ldots, v_{s_i}^{(i)})$ von U_i, $i = 1, \ldots, r$ ist $B := (v_1^{(1)}, \ldots, v_{s_1}^{(1)}, \ldots, v_1^{(r)}, \ldots, v_{s_r}^{(r)})$ eine Basis von V.
(iii) Es gibt Basen $B_i = (v_1^{(i)}, \ldots, v_{s_i}^{(i)})$ von U_i, $i = 1, \ldots, r$, sodass $B := (v_1^{(1)}, \ldots, v_{s_1}^{(1)}, \ldots, v_1^{(r)}, \ldots, v_{s_r}^{(r)})$ eine Basis von V ist.
(iv) $V = U_1 + \ldots + U_r$ und $\dim V = \dim U_1 + \ldots + \dim U_r$.

Satz 2.57. $U \subseteq V$ UVR
Dann ex. ein UVR $W \subseteq V$ mit $V = U \oplus W$. W heißt ein Komplement zu U in V.

Anmerkung: W in 2.57 ist im allgemeinen nicht eindeutig bestimmt: z.B.: $K = \mathbb{R}$, $V = \mathbb{R}^2$, $U = \text{ Lin}((e_1)) \Rightarrow$ $V = U \oplus \text{ Lin}((e_2)) = U \oplus \text{ Lin}((1,1))$

3. Lineare Abbildungen

In diesem Kapitel sei K stets ein Körper.

3.1. Lineare Abbildungen

In diesem Abschnitt seien U, V, W stets K-VR.

Definition 3.1. $f : V \to W$ Abb.
f heißt K-lineare Abbildung (Homomorphismus von K-VR, kurz: lineare Abbildung)
$\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(L1) $f(\underbrace{u+v}_{\text{Addition in } V}) = \underbrace{f(u)+f(v)}_{\text{Addition in } W}$ für alle $u, v \in V$
(L2) $f(\underbrace{\lambda v}_{\text{skal. Mult. in } V}) = \underbrace{\lambda f(v)}_{\text{skal. Mult. in } W}$ für alle $v \in V, \lambda \in K$

Beispiel 3.2.
(a) $A = (a_{ij} \in M(m \times n, K)$ Wir schreiben die Elemente von K^n als Spaltenvektoren und betrachten die Abb.:
$\tilde{A} : K^n \to K^m$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto Ax$
Es gilt für $u, v \in K^n, \lambda \in K : \tilde{A}(u+v) = A(u+v) = Au + Av = \tilde{A}(u) + \tilde{A}(v)$, $\tilde{A}(\lambda v) = A \cdot (\lambda v) = \lambda(Av) = \lambda \tilde{A}(v)$.
Wegen $\tilde{A}(e_i) = A \cdot e_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}$ stehen in den Spalten von A genau die Bilder der kanon. Basisvektoren $e_1, \ldots, e_n$ von K^n unter $\tilde{A}$
Sind $A \in M(m \times n, K), B \in M(n \times r, K), x \in K^r$, dann ist:
$\widetilde{AB}(x) = (AB)(x) = A(Bx) = A \cdot \tilde{B}(x) = \tilde{A}(\tilde{B}(x)) = (\tilde{A} \circ \tilde{B})(x)$, d.h. die Verknüpfung $\tilde{A}, \tilde{B}$ entspricht der Multiplikation der Matrizen $A, B : \tilde{A} \circ \tilde{B} = \widetilde{AB}$.
(b) Wir betrachten die Abb. $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}$
Diese ist linear nach (a), beschreibt Spiegelung an der x_1-Achse.
(c) Sei $V = \{f : (0,1) \to \mathbb{R} | f \text{ ist differenzierbar}\}$ (ist ein $\mathbb{R}$-VR)
$' : V \to \{g : (0,1) \to \mathbb{R} \text{ Abb.}\}$, $f \mapsto f'$ ist eine lineare Abb., denn es gilt für $f, g \in V$, dass $(f+g)' = f' + g'$, $(\lambda f)' = \lambda f'$ $(\lambda \in \mathbb{R})$.

Bemerkung 3.3. $f : V \to W$ lineare Abb.
Dann gilt:
(a) $f(0) = 0$
(b) $f(\lambda_1 v_1 + \ldots + \lambda_n v_n) = \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n)$ für alle $v_1, \ldots, v_n \in V$, $\lambda_1, \ldots, \lambda_n \in K$
(c) $V' \subseteq V$ UVR $\Rightarrow f(V') \subseteq W$ ist UVR

(d) $W' \subseteq W$ UVR $\Rightarrow f^{-1}(W') \subseteq V$ ist UVR
(e) $(v_i)_{i\in I}$ linear abhängige Familie in $V \Rightarrow (f(v_i)_{i\in I})$ linear abhängige Familie in W
(f) $V' = \text{Lin}((v_i))_{i\in I} \Rightarrow f(V') = \text{Lin}((f(v_i))_{i\in I})$
(g) W endlichdimensional $\Rightarrow f(V)$ endlichdimensionaler UVR von W mit $\dim f(V) \leq \dim W$

Bemerkung 3.4. $f : V \to W$, $g : U \to V$ lineare Abb.
Dann ist $f \circ g : U \to W$ eine lineare Ab..

Definition 3.5. $Hom_K(V,W) := \{f : V \to W | f \text{ ist } K\text{-linear}\}$
Eine K-lineare Abb. $f : V \to V$ heißt ein Endomorphismus von V.
$End_K(V) := \{f : V \to V | f \text{ ist Endomorphismus}\} = Hom_K(V,V)$

Bemerkung 3.6. Es gilt:
(a) $Hom_K(V,W)$ ist bzgl.
$+ : Hom_K(V,W) \times Hom_K(V,W) \to Hom_K(V,W)$, $(f,g) \mapsto f+g$ mit $(f+g)(v) := f(v)+g(v)$ für $v \in V$
$\cdot : K \times Hom_K(V,W) \to Hom_K(V,W)$, $(\lambda, f) \mapsto \lambda f$ mit $(\lambda f)(v) := \lambda f(v)$ für $v \in V$,
ein K-VR.
Nullvektor ist die Nullabb. $0 : V \to W$ mit $0(v) = 0$ für alle $v \in V$. (b) $End_K(V)$ ist bzgl.
$+ : End_K(V) \times End_K(V) \to End_K(V)$, $(f,g) \mapsto f+g$
$\circ : End_K(V) \times End_K(V) \to End_K(V)$, $(f,g) \mapsto f \circ g$
ein Ring, Einselement ist id_V.

Definition 3.7. Eine bijektive K-lineare Abb. $f : V \to W$ heißt ein Isomorphismus von V nach W.
Eine bijektive K-lineare Abb. $f : V \to V$ heißt ein Automorphismus von V.
$Iso_K(V,W := \{f : V \to W | f \text{ ist ein Isomorphismus}\}$
$Aut_K(V) := \{f : V \to V | f \text{ ist ein Automorphismus}\} = Iso_K(V,V)$

Bemerkung 3.8. $f : V \to W$ lineare Abb.
Dann gilt: Ist f ein Isomorphismus, dann ist auch $f^{-1} : W \to V$ ein Isomorphismus. Existiert zwischen V und W ein Isomorphismus, dann nennen wir V, W isomorph (Notation $V \cong W$)

Definition 3.9. $f : V \to W$ lineare Abb.
$im(f) := f(V)$ heißt das Bild von f.
$\ker(f) := f^{-1}(\{0\}) = \{v \in V | f(v) = 0\}$ heißt der Kern von f.

Bemerkung 3.10. $f : V \to W$ lineare Abb.
Dann gilt:
(a) $im(f) \subseteq W$ und $ker(f) \subseteq V$ sind UVR.
(b) f surjektiv $\Leftrightarrow im(f) = W$
(c) f injektiv $\Leftrightarrow \ker(f) = \{0\}$
(d) f injektiv und $(v_i)_{i\in I}$ linear unabhängige Familie in $V \Rightarrow ((f(v_i))_{i\in I})$ ist linear unabhängig.

Definition 3.11. $f : V \to W$ lineare Abb.
$\text{Rang}(f) := \dim(im(f))$ heißt der Rang von f.

Beispiel 3.12. $A \in M(m \times n, K)$
Wir betrachten die zu A gehörende lineare Abb. $\tilde{A} : K^n \to K^m$, $x \mapsto Ax$
Wegen $K^n = \text{Lin}((e_1, \ldots, e_n))$ folgt aus 3.3(f): $im(\tilde{A}) = \text{Lin}((\tilde{A}(e_1), \ldots, \tilde{A}(e_n)))$
Nach 3.2(a) sind $\tilde{A}(e_1), \ldots, \tilde{A}(e_n)$ genau die Spalten von A, d.h.: $\text{Rang}(\tilde{A}) = \dim(im(\tilde{A})) = \dim SR(A) =$ Spaltenrang (A)

Satz 3.13. (Dimensionsformel für lineare Abb.)
V endlichdimensionaler K-VR, $f : V \to W$ lineare Abb.
$(v_1, \ldots, v_k)$ Basis von $\ker(f)$, $(w_1, \ldots, w_r)$ Basis von $im(f)$ (beachte: $im(f)$ endlichdimensional wegen 3.3(f)). Für $i = 1, \ldots, r$ sei $u_i \in V$ mit $f(u_i) = w_i$
Dann ist $A := (u_1, \ldots, u_r, v_1, \ldots, v_k)$ eine Basis von V. Insbesondere ist $\dim V = \dim(\ker(f)) + \dim(im(f))$

Folgerung 3.14. V, W endlichdimensionale K-VR
Dann sind äquivalent:
(i) $V \cong W$
(ii) $\dim V = \dim W$

Folgerung 3.15. $n, m \in \mathbb{N}$
Dann gilt: $K^n \cong K^m \Leftrightarrow n = m$

Folgerung 3.16. V endlichdimensionaler K-VR. Dann gilt:
Es existiert ein $n \in \mathbb{N}_0$ mit $V \cong K^n$

Folgerung 3.17. V, W endlichdimensionale K-VR mit $\dim V = \dim W$, $f : V \to W$ lineare Abb.
Dann sind äquivalent:
(i) f injektiv
(ii) f surjektiv
(iii) f bijektiv

3.2. Faktorräume und der Homomorphiesatz

In diesem Abschnitt seien V, W stets K-VR

Definition 3.18. $A \subseteq V$
A heißt ein affiner Unterraum von $V \Leftrightarrow$ Es gibt ein $a \in V$ und einen UVR $U \subseteq V$, sodass $A = a + U := \{a + u | u \in U\}$ ist oder $A = \emptyset$.

Anmerkung:

- affine Unterräume von V entstehen (mit Ausnahme von $\emptyset$) durch "Parrallelverschiebung" von UVR von V.
- Ist $A = a + U$ mit $a \notin U$, dann $0 \notin a + U$, d.h. A ist in diesem Fall kein UVR von V

Bemerkung 3.19. $a \in V, U \subseteq V$ UVR, $A = a + U$
Dann gilt:
(a) Für jedes $b \in A$ ist $A = b + U$
(b) Ist $\tilde{a} \in V$, $\tilde{U} \subseteq V$ UVR mit $\tilde{a} + \tilde{U} = a + U$, dann ist $U = \tilde{U}$ und $a - \tilde{a} \in U$.
Mit anderen Worten: Zu einem affinen Unterraum $A = a + U$ ist der UVR U eindeutig bestimmt, der "Aufhängepunkt" a kann beliebig in A gewählt werden. Wir setzen $\dim A := \dim U$, $\dim \emptyset := -1$.

Beispiel 3.20.
UVR U im $\mathbb{R}$-VR $\mathbb{R}^2$:
$\dim U = 0 : \{0\}$
$\dim U = 1 : \ \mathrm{Lin}((v)), v \neq 0$ (Ursprungsgerade)
$\dim U = 2 : \mathbb{R}^2$
affine UR A in $\mathbb{R}^2$:
$\dim A = -1 : \emptyset$
$\dim A = 0 : \{a\}$ (Punkte) $a \in \mathbb{R}^2$
$\dim A = 1 : a + \ \mathrm{Lin}((v))$, a, $v \in \mathbb{R}^2$, $v \neq 0$ (Geraden)
$\dim A = 2 : \mathbb{R}^2$

Definition 3.21. $f : V \to W$ lineare Abb., $w \in W$
$f^{-1}(\{w\}) = \{v \in V | f(v) = w\}$ heißt die Faser von f über w.

Anmerkung:

- Ist $A \in M(m \times n, K)$, so erhalten wir eine lineare Abb. $\tilde{A} : K^n \to K^m$, $x \mapsto Ax$. Für $b \in K^m$ ist $\tilde{A}^{-1}(\{b\}) = \{x \in K^n | Ax = b\}$ genau die Lösungsmenge des linearen Gleichungssystems $Ax = b$.
- Durch $v_1 \sim_f v_2 \Leftrightarrow f(v_1) = f(v_2)$ ist eine Äquivalenzrelation aus V erklärt, die Äquivalenzklassen von $v \in V$ ist gegeben durch $\{u \in V | f(u) = f(v)\} = f^{-1}(\{f(v)\})$. Somit sind die nichtlerren Fasern von f genau die Äquivalenzklassen bzgl. "$\sim_f$". Insbesondere ist V die Vereinigung der Fasern von f, je zwei Fasern von f sind gleich oder disjunkt.

Satz 3.22. $f : V \to W$ lineare Abb., $w \in W$
Dann gilt:
$$f^{-1}(\{w\}) = \begin{cases} u + \ker(f), \text{ falls } w \in im(f) \text{ (hierbei } u \in f^{-1}(\{w\})) \\ \emptyset, \text{ falls } w \notin im(f) \end{cases}$$
Somit ist die Faser von f über w ein affiner UR von V mit
$$\dim f^{-1}(\{w\}) = \begin{cases} \dim \ker(f) = \dim V - \dim im(f), \text{ falls } w \in im(f) \\ -1, \text{ falls } w \notin im(f) \end{cases}$$
Insbesondere haben alls nichtleeren Fasern von f dieselbe Dimension.

Beispiel 3.23. $K = \mathbb{R}, V = \mathbb{R}^2$

Wir betrachten die Abb. $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix}$

f ist linear, und es ist $im(f) = \text{ Lin}((e_1))$, $\ker(f) = \text{ Lin}((e_2))$, und für $w = \lambda e_1 = \begin{pmatrix} \lambda \\ 0 \end{pmatrix} \in im(f)$ ist $f^{-1}(\{w\}) =$

$f^{-1}(\{\begin{pmatrix} \lambda \\ 0 \end{pmatrix}\}) = \begin{pmatrix} \lambda \\ 5 \end{pmatrix} + \ker(f) = \begin{pmatrix} \lambda \\ 5 \end{pmatrix} + \text{ Lin}((e_2))$

bel. El. aus $f^{-1}(\{\begin{pmatrix} \lambda \\ 0 \end{pmatrix}\})$ ↛

Ziel: Wir haben gesehen, dass der Kern einer linearen Abb. $f : V \to W$ ein UVR von V ist, und dass für jedes $w \in W$ die Faser von f über w ein affiner UR von V ist. Wir wollen nun zu einem gegebenen UVR $U \subseteq V$ einen UR W und eine lineare Abb. $f : V \to W$ konstruieren, sodass $U = \ker(f)$ ist (bzw. dass ein gegebener affiner UR von V eine Faser von f ist)

Bemerkung 3.24. $U \subseteq V$ UVR

Dann ist durch $a \sim_U b \Leftrightarrow a - b \in U$ eine Äquivalenzrelation auf V gegeben. Anstelle von $a \sim_U b$ schreiben wir auch $a \equiv b \pmod{U}$ ("a kongruent b modulo U").

Die Äquivalenzklasse von $a \in V$ ist durch $\overline{a} := a + U$ gegeben und heißt Restklasse von a modulo U. Die Menge aller Äquivalenzklassen modulo U bezeichnen wir mit V/U.

Satz 3.25. $U \subseteq V$ UVR

Wir definieren Verknüpfungen

$+ : V/U \times V/U \to V/U, \overline{a} + \overline{b} := \overline{a+b}$

$\cdot : K \times V/U \to V/U, \lambda \cdot \overline{a} := \overline{\lambda a}$

Dann gilt:

(a) V/U wird mit der obigen Addition und skalaren Multiplikation zu einem K-VR, dem Faktorvektorraum (Faktorraum, Quotientenvektorraum) von V modulo U. Der Nullvektor in V/U ist $\overline{0} = 0 + U = U$.

(b) Die Abbildung $\pi : V \to V/U$, $a \mapsto \overline{a}$ ist eine surjektive lineare Abbildung mit $\ker(\pi) = U$. π heißt die kanonische Projektion von V nach V/U.

(c) Ist V endlichdimensional, dann ist $\dim_K V/U = \dim_K V - \dim_K U$.

Folgerung 3.26. $U \subseteq V$. Dann sind äquivalent:

(i) U ist UVR von V.

(ii) Es gibt einen K-VR W und eine lineare Abb. $f : V \to W$ mit $\ker(f) = U$ Ist V endlichdimensional, dann kann man in diesem Fall W auch endlichdimensional mit $\dim W \leq \dim V$ wählen.

Folgerung 3.27. $A \subseteq V$. Dann sind äquivalent:

(i) A ist ein affiner Unterraum von V

(ii) Es gibt einen K-VR W, eine lineare Abb. $f : V \to W$ und ein $w \in W$ mit $A = f^{-1}(\{w\})$. Ist V endlichdimensional, dann kann man in diesem Fall auch W endlichdimensional wählen mit $\dim W \leq \dim V$ (außer im Fall $A = \emptyset, V = \{0\}$)

Anmerkung: Philosophie hinter 3.26/3.27: UVR = Kerne von linearen Abb., affine UR = Fasern linearer Abbildungen.

Satz 3.28. (Homomorphiesatz) $f : V \to W$ lineare Abb.
Dann induziert f einen Isomorphismus $\overline{f} : V/\ker(f) \to im(f)$, $\overline{v} \mapsto f(v)$
d.h.: $V/\ker(f) \cong im(f)$.

Folgerung 3.29. $f : V \to W$ lineare Abb.
Dann lässt sich f schreiben als $f = i \circ \overline{f} \circ \pi$, wobei $\pi : V \to V/\ker(f)$, $v \mapsto \overline{v}$ (kanonische Projektion), $\overline{f}$: Abb. aus 3.28, $i : im(f) \to W$, $w \mapsto w$ Inklusion. Man sagt auch: Das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ V/\ker(f) & \xrightarrow[\overline{f}]{} & im(f) \end{array}$$

kommutiert. Hierbei ist π surjektiv, $\overline{f}$ ein Isomorphismus, i ist injektiv.

3.3. Lineare Gleichungssysteme

In diesem Abschnitt seien stets $m, n \in \mathbb{N}$, $A = (a_{ij}) \in M(m \times n, K)$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m$

Ziel: Bestimme alle $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ mit $Ax = b$, d.h. löse das lineare Gleichungssystem $Ax = b$, explizit:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

Die Matrix A induziert eine lineare Abb. $\tilde{A} : K^n \to K^m$, $x \mapsto Ax$, d.h.: Bestimmung der Lösungsmenge von $Ax = b$ korrespondiert zur Bestimmung der Faser $\tilde{A}^{-1}(b)$.

Definition 3.30.
Das LGS $Ax = b$ heißt homogen $\Leftrightarrow b = 0$
inhomogen $\Leftrightarrow b \neq 0$
Das LGS $Ax = 0$ heißt das zu $Ax = b$ gehörige homogene LGS. A heißt die Koeffizientenmatrix des LGS $Ax = b$.
Lös$(A, b) := \{x \in K^n | Ax = b\} = \tilde{A}^{-1}(b)$ heißt der Lösungsraum des LGS $Ax = b$. Insbesondere ist Lös$(A, 0) = \ker(\tilde{A})$.

Satz 3.31. Es gilt:
(a) Lös$(A,0) \subseteq K^n$ ist ein UVR der Dimension $n - \text{Rang}(A)$
(b)Lös$(A,b) \subseteq K^n$ ist ein affiner Unterraum von K^n. Ist Lös$(A,b) \neq \emptyset$, dann hat dieser die Dimension $n - \text{Rang}(A)$
(c) Ist Lös$(A,b) = \emptyset$ und $v \in$ Lös(A,b), dann ist Lös$(A,b) = v +$Lös$(A,0)$

Anmerkung: Lös$(A,0)$ enthält immer die triviale Lösung 0, nichttriviale Lösung von $Ax = 0$ gibt es wegen (a) genau dann, wenn Rang$(A) < n$ ist.

Definition 3.32.

$$A|b := \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix} \subseteq M(mx(n+1), K)$$

heißt die erweiterte Koeffizientenmatrix des LGS $Ax = b$.

Satz 3.33. Es sind äquivalent:
(i) Lös$(A,b) \neq \emptyset$, d.h. das LGS $Ax = b$ besitzt eine Lösung.
(ii) Rang(A) = Rang$(A|b)$.

Folgerung 3.34. Es sind äquivalent:
(i) Das LGS $Ax = b$ besitzt genau eine Lösung.
(ii) Rang(A) = Rang$(A|b) = n$

Ziel: Algorithmus zur Bestimmung von Lös(A,b).

Definition 3.35.
A ist in strenger Zeilenstufenform (SZSF) $\Leftrightarrow$ A ist in ZSF mit Pivotspalten bei $j_1, \dots, j_r$ und es gilt:
(SZ1) $a_{aj_1} = \dots = a_{rj_r} = 1$
(SZ2) $a_{ij_k} = 0$ für alle $k \in \{1, \dots, r\}$, $i \in \{1, \dots, k-1\}$
Visualisierung:

$$\begin{array}{c} \begin{array}{ccccccccc} j_1 & & j_2 & & j_3 & & & & j_r \end{array} \\ \left(\begin{array}{ccccccccc} 1 & * & 0 & * & 0 & & & & 0 \\ & & 1 & * & 0 & * & & & \vdots \\ & & & & 1 & & & & \vdots \\ & & & & & & \ddots & & 0 \\ & & & & & & & & 1 \end{array}\right) \end{array}$$

Satz 3.36.
A lässt sich durch elementare Zeilenumformungen auf SZSF bringen.

Anmerkung: Die strenge ZSF von A ist eindeutig bestimmt (vgl. Blatt 11, ZA5).

Bemerkung 3.37. $C \in M(m \times n, K)$, $d \in K^m$

Ist $C|d$ durch eine Folge elementarer Zeilenumformungen aus $A|b$ entstanden, dann ist Lös(C,d) = Lös(A,b).

Satz 3.38. (Gauß-Algorithmus zur Lösung homogener LGS)

Eingabe: $A \in M(m \times n, K)$

Ausgabe: eine Basis von Lös$(A,0)$

Durchführung:

1. Bringe die Matrix A durch elementare Zeilenumformungen auf SZSF S:

$$S = \begin{array}{c} \begin{array}{ccccccccc} j_1 & & j_2 & & j_3 & & & & j_r \end{array} \\ \left(\begin{array}{ccccccccc} 1 & * & 0 & * & 0 & & & 0 & \\ & & 1 & * & 0 & * & & \vdots & \\ & & & & 1 & & & \vdots & * \\ & & & & & & \ddots & 0 & \\ & & & & & & & 1 & \end{array}\right) \end{array}, \quad r = \text{Zeilenrang}(A)$$

2. Sei $B \in M(r \times (n-r), K)$, die aus S durch Streichen der Spalten mit den Indizes $j_1, \ldots, j_r$ und der Zeilen mit den Indizes $r+1, \ldots, m$ entsteht. Seien $k_1 < k_2 < \ldots < k_{n-r}$ mit $\{1, \ldots, n\} = \{j_1, \ldots, j_r, k_1, \ldots, k_{n-r}\}$

3. Eine Basis von Lös$(A,0)$ ist gegeben durch $(w_1, \ldots, w_{n-r})$, wobei $w_i = \begin{pmatrix} w_{i1} \\ \vdots \\ w_{in} \end{pmatrix} \in K^n$ für $i = 1, \ldots, n-r$

wie folgt gegeben ist:

$$\begin{pmatrix} w_{ij_1} \\ \vdots \\ w_{ij_r} \end{pmatrix} = \text{i-te Spalte von } -B, \quad \begin{pmatrix} w_{ik_1} \\ \vdots \\ w_{ik_{n-r}} \end{pmatrix} = e_i \in K^{n-r}$$

Folgerung 3.39.

Es gilt: Zeilenrang(A) = Spaltenrang(A) = Rang(A)

Beispiel 3.40.

Sei $A = \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \in M(3\times 4, \mathbb{R})$, gesucht ist eine Basis von $\text{Lös}(A,0) \subseteq \mathbb{R}^4$

$$A \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & -3 \\ \hline 0 & 0 & 0 & 0 \end{array}\right)$$

Insbesondere ist $\text{Rang}(A) = 2$, $\dim \text{Lös}(A,0) = 4 - \text{Rang}(A) = 2$.

Es ist $j_1 = 1$, $j_2 = 2$. Wegen $\{1,2,3,4\} = \{j_1, j_2, k_1, k_2\}$ und $k_1 < k_2$ ist $k_1 = 2, k_2 = 4$

Es ist $B = \begin{pmatrix} 2 & 6 \\ 0 & -3 \end{pmatrix}$, $-B = \begin{pmatrix} -2 & -6 \\ 0 & 3 \end{pmatrix}$

Eine Basis von $\text{Lös}(A,0)$ ist gegeben durch (w_1, w_2), mit $w_1 = \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $w_2 = \begin{pmatrix} -6 \\ 0 \\ 3 \\ 1 \end{pmatrix}$

Satz 3.41. (Gauß-Algorithmus zur Lösung inhomogener LGS)

Eingabe: $A \in M(m\times n, K), b \in K^m, b \neq 0$

Ausgabe: $\text{Lös}(A,b)$

Durchführung:

1. Bringe die Matrix $A|b$ durch elementare Zeilenumformungen auf SZSF $S|s$::

$$S|s = \begin{array}{c} \begin{matrix} j_1 & & j_2 & & j_3 & & & j_r & \end{matrix} \\ \left(\begin{array}{cccccccc} 1 & * & 0 & * & 0 & & 0 & s_1 \\ & & 1 & * & 0 & * & \vdots & \vdots \\ & & & & 1 & & \vdots & * \\ & & & & & \ddots & 0 & \vdots \\ & & & & & & 1 & s_r \\ & & & & & & & 0 \\ & & & & 0 & & & \vdots \\ & & & & & & & 0 \end{array}\right) \end{array} \in M(m\times(n+1), K),\ r = \text{Rang}(A|b)$$

2. Falls $j_r = n+1$, dann ist $\text{Lös}(A,b) = \emptyset$.

3. Falls $j_r < n+1$, dann ist eine spezielle Lösung von $Ax = b$ gegeben durch $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$, wobei

$\begin{pmatrix} v_{j_1} \\ \vdots \\ v_{j_r} \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_r \end{pmatrix}$, $v_i = 0$ für $i \in \{1,\ldots,n\}\backslash\{j_1,\ldots,j_r\}$.

Es ist $\text{Lös}(A,b) = v + \text{Lös}(A,0)$, wobei man $\text{Lös}(A,0)$ mittels 3.38 bestimmt.

Beispiel 3.42.

Wir betrachten das LGS $Ax = b$ mit $A = \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \in M(3\times 4, \mathbb{R})$, $b = \begin{pmatrix} 4 \\ 6 \\ 9 \end{pmatrix} \in \mathbb{R}^3$ (vgl. Bsp 3.40)

$$A|b = \begin{pmatrix} 2 & 4 & 2 & 6 & 4 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rightsquigarrow \left(\begin{array}{cc|ccc} 1 & 2 & 0 & 6 & 1 \\ 0 & 0 & 1 & -3 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Es ist $\operatorname{Rang}(A|b) = \operatorname{Rang}(A) = 2$, insbesondere ist $\operatorname{Lös}(A, b) \neq \emptyset$, dim $\operatorname{Lös}(A, b) = 4 - \operatorname{Rang}(A) = 2$. Es ist $j_1 = 1$, $j_2 = 3$. Eine spezielle Lösung von $Ax = b$ ist nach 3.41 gegeben durch $v = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ Nach Bsp 3.40 ist

$$\operatorname{Lös}(A, b) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \operatorname{Lin}\left(\begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -6 \\ 0 \\ 3 \\ 1 \end{pmatrix}\right) = \left\{ \begin{pmatrix} 1 - 2\lambda - 6\mu \\ \lambda \\ 1 + 3\mu \\ \mu \end{pmatrix} \mid \lambda, \mu \in \mathbb{R} \right\}$$

3.4. Lineare Abbildungen und Matrizen

In diesem Abschnitt seien V, W endlichdimensionale K-VR.

Satz 3.43. $v_1, \ldots, v_r \in V, w_1, \ldots, w_r \in W$. Dann gilt:
(a) Ist $(v_1, \ldots, v_r)$ eine Basis von V, dann gibt es genau eine lineare Abb. $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \ldots, r$. Diese Abb. hat die folgenden Eigenschaften:

- $im(f) = \operatorname{Lin}((w_1, \ldots, w_r))$, insbesondere f surjektiv $\Leftrightarrow (w_1, \ldots, w_r)$ ES von W
- f injektiv $\Leftrightarrow (w_1, \ldots, w_r)$ linear unabhängig

f Isomorphismus $\Leftrightarrow (w_1, \ldots, w_r)$ Basis von W

Folgerung 3.44. $B = (v_1, \ldots, v_n)$ Basis von V
Dann gibt es genau einen Isomorphimus $\underline{\overline{\phi}}_B : K^n \to V$ von K-VR mit $\underline{\overline{\phi}}_B(e_i) = v_i$ für $i = 1, \ldots, n$
$\underline{\overline{\phi}}_B$ heißt das durch B bestimmte Koordinatensystem von V.

ist $v = \lambda_1 v_1 + \ldots + \lambda_n v_n \in V$, dann nennt man $\underline{\overline{\phi}}_B^{-1}(v) = \lambda_1 e_1 + \ldots + \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in K^n$ die Koordinaten von v bzgl. B.

Satz 3.45. $A = (v_1, \ldots, v_n)$ Basis von V, $B = (w_1, \ldots w_m)$ Basis von W
Dann gilt:
(a) Für jede lineare Abb. $f : V \to W$ gibt es genau eine Matrix $A = (a_{ij}) \in M(m \times n, K)$, sodass $f(v_j) = \sum_{i=1}^{m} a_{ij} w_i$ für $j = 1, \ldots, n$
$M_B^A(f) := A$ heißt die Darstellungsmatrix von f bzgl. der Basen A und B. In der j-ten Spalte von $M_B^A(f)$ stehen die Koordinaten von $f(v_j)$ bzgl. der Basis B von W (für $j = 1, \ldots, n$)
(b) Die aus (a) erhaltene Abb.
$M_B^A : Hom_K(V, W) \to M(m \times n, K)$, $f \mapsto M_B^A(f)$ ist ein Isomorphismus von K-VR.
Insbesondere ist im Fall $V = W$, $A = B$ die Abb.
$M_B : End_K(V) \to M(n \times n, K)$, $f \mapsto M_B(f) := M_B^B(f)$ ein Isomorphismus von K-VR.

Folgerung 3.46. Die Abb.
$M_{(e_1,\ldots,e_n)}^{(e_1,\ldots,e_n)} : Hom_K(K^n, K^m) \to M(m \times n, K)$ ist ein Isomorphismus von K-VR mit Umkehrabbildung:
$\sim : M(m \times n, K) \to Hom_K(K^n, K^m)$, $A \mapsto \tilde{A}$
Insbesondere ist $\sim$ ebenfalls ein Isomorphismus.

Beispiel 3.47.
$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{R})$. Es ist $M_{e_1,e_2}^{e_1,e_2}(\tilde{A}) = A$.
Es sei $A = (\binom{-1}{1}, \binom{1}{1})$, $B = (\binom{2}{-1}, \binom{1}{-1})$

$$\tilde{A}(\tbinom{-1}{1}) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = -\begin{pmatrix} 2 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\tilde{A}(\tbinom{1}{1}) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 5\begin{pmatrix} 2 \\ -1 \end{pmatrix} - 7\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\Rightarrow M_B^A(\tilde{A}) = \begin{pmatrix} -1 & 5 \\ 1 & -7 \end{pmatrix}$$

Wir haben einen Basiswechsel durchgeführt.

Folgerung 3.48. $A \in M(n \times n, K)$. Dann sind äquivalent:
(i) $A \in Gl(n, K)$
(ii) Es gibt ein $B \in M(n \times n, K)$ mit $AB = E_n = BA$
(iii) Es gibt ein $B \in M(n \times n, K)$ mit $AB = E_n$
(iv) Es gibt ein $B \in M(n \times n, K)$ mit $BA = E_n$
(v) $\tilde{A} : K^n \to K^n$ ist ein Isomorphismus
(vi) Rang$(A) = n$

Folgerung 3.49.
Es gilt: $\dim_K Hom_K(V, W) = \dim_K(V) \cdot \dim_K(W)$.

Folgerung 3.50. $U \subseteq K^n$. Dann sind äquivalent:
(i) U ist UVR von K^n
(ii) Es gibt ein $m \in \mathbb{N}$ und ein $A \in M(m \times n, K)$, sodass $U =$ Lös$(A, 0)$

Folgerung 3.51. $U \subseteq K^n$. Dann sind äquivalent:
(i) U ist ein affiner UR von K^n
(ii) Es gibt $m \in \mathbb{N}$, $A \in M(m \times n, K)$, $b \in K^m$, sodass $U = \text{Lös}(A, b)$.

Anmerkung: Philosophie hinter 3.50/3.51: affine UR von K^n = Lösungsräume von LGS (in n Variablen) über K, UVR von K^n = Lösungsräume homogener LGS (in n Variablen) über K.

Bemerkung 3.52. $f : V \to W$ lineare Abbildung. Dann gibt es Basen A von V, B von W mit $M_B^A(f) = \begin{pmatrix} E_r & \\ & 0 \end{pmatrix}$, $r = \text{Rang}(f)$

3.5. Basiswechsel

In diesem Abschnitt seien V, W endlichdimensionale K-VR

Bemerkung 3.53. $f : V \to W$ lineare Abb., A Basis von V, B Basis von W. Dann gilt:

Das Diagramm $\begin{array}{ccc} K^n & \xrightarrow{\underline{\phi}_A} & V \\ \downarrow{\scriptstyle \widetilde{M_B^A(f)}} & & \downarrow{\scriptstyle f} \\ K^m & \xrightarrow{\underline{\phi}_B} & W \end{array}$ ist kommutativ, d.h. $\underline{\phi}_B \circ \widetilde{M_B^A(f)} = f \circ \underline{\phi}_A$ (Hierbei sind $\underline{\phi}_A, \underline{\phi}_B$ Koordinatensysteme von V bzgl. A bzw. von W bzgl. B) Insbesondere ist $\widetilde{M_B^A(f)} = \underline{\phi}_B^{-1} \circ f \circ \underline{\phi}_A$

Bemerkung 3.54. A, A' Basen von V, $n = \dim(V)$
$T_{A'}^A := M_{A'}^A(id_V) \in M(n \times n, K)$ heißt die Transformationsmatrix des Basiswechsels von A nach A'.
Es gilt:
(a) $T_{A'}^A \in Gl(n, K)$
(b) $\widetilde{T_{A'}^A} = \underline{\phi}_{A'}^{-1} \circ \underline{\phi}_A$
(c) $T_{A'}^A = (T_A^{A'})^{-1}$

Beispiel 3.55. $K = \mathbb{R}, V = \mathbb{R}^2$, $A = (\binom{-1}{1}, \binom{1}{1})$, $B = (\binom{2}{-1}, \binom{1}{-1})$. Gesucht ist $T_B^A = M_B^A(id_{\mathbb{R}^2})$
Es ist $\binom{-1}{1} = 0 \cdot \binom{2}{-1} + (-1) \cdot \binom{1}{-1}$, $\binom{1}{1} = 2 \cdot \binom{2}{-1} + (-3) \cdot \binom{1}{-1} \Rightarrow T_B^A = \begin{pmatrix} 0 & 2 \\ -1 & -3 \end{pmatrix}$

Satz 3.56. U, V, W endlichdimensionale K-VR mit Basen A, B, C, $g : U \to V$, $f : V \to W$ lineare Abb.
Dann gilt: $M_C^A(f \circ g) = M_C^B(f) \cdot M_B^A(g)$

Folgerung 3.57. A, B, C Basen von V. Dann gilt:
(a) $T_C^A = T_C^B \cdot T_B^A$
(b) $M_B : End_K(V) \to M(n \times n, K)$, $f \mapsto M_B(f) = M_B^B(f)$ ist ein Isomorphismus von Ringen, d.h. M_B ist bijektiv, $M_B(f+g) = M_B(f) + M_B(g)$, $M_B(f \circ g) = M_B(f) M_B(g)$, $M_B(id_V) = E_1$ für alle $f, g \in End_K(V)$.

Satz 3.58. (Transformationsformel) $f : V \to W$ lineare Abb., A, A' Basen von V, B, B' Basen von W.
Dann gilt: $M_{B'}^{A'}(f) = T_{B'}^B M_B^A(f) T_A^{A'}$
Setzen wir $A := M_B^A(f)$, $B := M_{B'}^{A'}(f)$, $S := T_{B'}^B$, $T := T_{A'}^A$, dann gilt also $B = SAT^{-1}$.

Beispiel 3.59. $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in M(2\times 2, \mathbb{R})$, $A = (\binom{-1}{1}, \binom{1}{1})$, $B = (\binom{2}{-1}, \binom{1}{-1})$
Gesucht ist $M_B^A(\tilde{A})$. Nach 3.58 ist:

$$M_B^A(\tilde{A}) = T_B^{(e_1,e_2)} \underbrace{M_{(e_1,e_2)}^{(e_1,e_2)}(\tilde{A})}_{=A} T_{(e_1,e_2)}^A = T_B^{(e_1,e_2)} A T_{(e_1,e_2)}^A = (T_{(e_1,e_2)}^B)^{-1} A T_{(e_1,e_2)}^A$$

$$T_{(e_1,e_2)}^A = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, T_{(e_1,e_2)}^B = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\Rightarrow M_B^A(\tilde{A}) = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = \ldots = \begin{pmatrix} -1 & 5 \\ 1 & -7 \end{pmatrix}$$

Folgerung 3.60. A, B Basen von V, $f \in End_K(V)$
Dann gilt: $M_B(f) = T_B^A M_A(f) T_A^B$
Setzen wir $A := M_A(f)$, $B := M_B(f)$, $S := T_B^A$, dann gilt also $B = SAS^{-1}$

Definition 3.61. $A, B \in M(m\times n, K)$
A, B heißen äquivalent ($A \sim B$) $\Leftrightarrow$ Es ex. $S \in Gl(m,K)$, $T \in Gl(n,K)$ mit $B = SAT^{-1}$.

Bemerkung 3.62.
Äquivalenz von Matrizen ist eine Äquivalenzrelation auf $M(m\times n, K)$.

Bemerkung 3.63. $A, B \in M(m\times n, K)$ A Basis von K^n, B Basis von K^m, $f : K^n \to K^m$ lineare Abb. mit $M_B^A(f) = A$.
Dann sind äquivalent:
(i) $A \sim B$, d.h. existieren $S \in Gl(m,K)$, $T \in Gl(n,K)$ mit $B = SAT^{-1}$
(ii) Es exisitieren Basen A' von K^n, B' von K^m mit $M_{B'}^{A'}(f) = B$ (d.h. A, B beschreiben bzgl. geeigneter Paare von Basen dieselbe lineare Abbildung)
(iii) Rang(A) = Rang(B)
Insbesondere ist jede Matrix aus $M(m\times n, K)$ vom Rang r äquivalent zu $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$

Definition 3.64. $A, B \in M(n\times n, K)$
A, B heißen ähnlich $\Leftrightarrow$ Es ex. ein $S \in Gl(n,K)$ mit $B = SAS^{-1}$ (Notation: $A \approx B$)

Bemerkung 3.65.
Ähnlichkeit von Matrizen ist ein Äquivalenzrelation.

Bemerkung 3.66. $A, B \in M(n\times n, K)$, A Basis von K^n, $f : K^n \to K^n$ lineare Abb. mit $M_A(f) = A$
Dann sind äquivalent:
(i) $A \approx B$
(ii) Es existiert eine Basis B von K^n mit $M_B(f) = B$ (d.h. (A, B beschreiben bzgl. geeigneter Basen denselben Endomorphismus)

Anmerkung: Einen möglichst einfachen Vertreter der Ähnlichkeitsklasse von A zu finden, ist eine schwierige Aufgabe (LA2, Jordansche Normalformen).

3.6. Determinanten

In diesem Abschnitt sei $n \in \mathbb{N}$

Ziel: Ordne jeder Matrix aus $M(n \times n, K)$ eine Element aus K zu, dass genau dann = 0 ist, wenn die Matrix nicht invertierbar ist. Die Zuordnungen soll mehreren Bedingungen genügen.

Definition 3.67.

Eine Abb. $\det : M(n \times n, K) \to K,\ A \mapsto \det A$ heißt Determinante $\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:

(D1) det ist linear in jeder Zeile, d.h. ist $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in M(n \times n, K)$ mit Zeilen $a_1, \ldots, a_n$, dann gilt für jedes $i \in \{1, \ldots, n\}$:

(D1a) ist $a_i = a_i' + a_i''$, dann ist $\det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_i' \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_i'' \\ \vdots \\ a_n \end{pmatrix}$

(D1b) Ist $a_i = \lambda a_i'$ mit $\lambda \in K$, dann ist $\det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} = \lambda \det \begin{pmatrix} a_1 \\ \vdots \\ a_i' \\ \vdots \\ a_n \end{pmatrix}$

(D2) det ist alternierend, d.h.: Hat $A \in M(n \times n, K)$ zwei gleiche Zeilen, dann ist $\det A = 0$

(D3) det ist normiert, d.h. $\det E_n = 1$

Weitere Schreibweise: Für $A = (a_{ij})$ schreiben wir auch $\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix} := \det \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$

Satz 3.68. $\det : M(n\times n, K) \to K$ sei eine Determinante, $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, $B \in M(n\times n, K)$

Dann gilt:

(D4) $\det(\lambda A) = \lambda^n \det(A)$

(D5) Ist eine Zeile von A gleich Null, dann ist $\det A = 0$

(D6) $\det \underbrace{\begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix}}_{\text{i-te und j-te Zeile vertauscht für } i \neq j} = -\det(A)$,

d.h. bei Zeilenumformung vom Typ 4 wird das Ergebnis mit -1 multipliziert.

(D7) $\det \begin{pmatrix} a_1 \\ \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_n \end{pmatrix} = \det A$ für $i \neq j, \lambda \in K$, d.h. det ist invariant unter Zeilenumformungen vom Typ 3.

(D8) Ist A eine obere Dreiecksmatrix, d.h. $A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$, dann ist $\det A = \lambda_1 \cdot \ldots \cdot \lambda_n$.

Analog für untere Dreiecksmatrix

(D9) Ist $n \geq 2$ und A von der Gestalt $A = \begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix}$ mit $A_1 \in M(r\times r, K), A_2 \in M(s\times s, K), r+s = n$, dann ist $\det A = \det(A_1) \cdot \det(A_2)$

(D10) $\det A = 0 \Leftrightarrow \text{Rang}(A) < n$ (d.h. $\det A \neq 0 \Leftrightarrow A \in Gl(n, K)$)

(D11) $\det(AB) = \det(A) \cdot \det(B)$. Insbesondere ist $\det(A^{-1}) = \det(A)^{-1}$

Anmerkung: Wir müssen immer noch zeigen, dass es überhaupt Abbildungen $det : M(n\times n, K) \to K$ gibt die (D1)-(D8) erfüllen. Wir werden dies tun, indem wir eine explizite Formel angeben (Leibniz-Formel).

Definition 3.69. $\sigma \in S_n$

$sgn(\sigma) := \prod_{1\leq i\leq j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$ heißt das Signum von σ.

σ heißt gerade $\Leftrightarrow sgn(\sigma) = 1$, σ heißt ungerade $\Leftrightarrow sgn(\sigma = -1)$

$(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ mit $i < j$ und $\sigma(i) > \sigma(j)$ heißt ein Fehlstand von σ.

Bemerkung 3.70. Es gilt:

(a) $sgn : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus von $(S_n, \circ)$ nach $(\{\pm 1\}, \cdot)$ d.h. $sgn(\sigma \circ \tau) = sgn(\sigma) \circ sgn(\tau)$ für alle $\sigma, \tau \in S_n$.

(b) $sgn(\sigma^{-1}) = sgn(\sigma)$ für alle $\sigma \in S_n$

(c) Es ist $sgn(\sigma) = \begin{cases} +1, \text{ wenn } \sigma \text{ eine gerade Anzahl von Fehlständen hat} \\ -1, \text{ wenn } \sigma \text{ eine ungerade Anzahl an Fehlständen hat} \end{cases}$

$= (-1)^k$, k Anzahl der Fehlstände von σ

Definition 3.71.

$\tau \in S_n$ heißt Transposition $\Leftrightarrow$ es ex. $a, b \in \{1, \ldots, n\}$, $a \neq b$ mit $\tau(a) = b$ $\tau(b) = a$ und $\tau(c) = c$ für alle $c \in \{1, \ldots, n\} \backslash \{a, b\}$.

Bemerkung 3.72. $n \geq 2$ Dann gilt:

(a) für jedes $\sigma \in S_n$ existieren Transpositionen $\tau_1, \ldots, \tau_k \in S_n$ mit $\sigma = \tau_1 \circ \ldots \circ \tau_k$ d.h. jedes Element aus S_n kann (auf nicht notwendig eindeutige Weise!) als Produkt von Transpositionen geschreiben werden.

(b) Ist $\tau \in S_n$ eine Transposition, dann ex. ein $\sigma \in S_n$ mit $\tau = \sigma \circ \delta \circ \sigma^{-1}$, wobei $\delta = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}$

Folgerung 3.73. $n \geq 2$. Dann gilt:

(a) Ist $\tau \in S_n$ eine Transposition, dann ist $sgn(\tau) = -1$

(b) Ist $\sigma \in S_n$, $\sigma = \tau_1 \circ \ldots \circ \tau_k$ mit Transpositionen $\tau_1, \ldots, \tau_k \in S_n$, dann ist $sgn(\sigma) = (-1)^k$

Folgerung 3.74. $\det : M(n \times n, K) \to K$ sei eine Determinante, $\sigma \in S_n$

Dann gilt: $\det \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix} = sgn(\sigma)$

Bemerkung 3.75. $A_n := \{\sigma \in S_n | sgn(\sigma) = 1\}$ ist eine Gruppe bzgl. "$\circ$", die sogenannte alternierende Gruppe.

Beispiel 3.76. Es ist $S_3 = \{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$

Es ist $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, d.h. $sgn(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}) = (-1)^2 = 1$

(vgl. Def. sgn: $sgn(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}) = \prod_{1 \leq i \leq j \leq 3} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{3-2}{2-1} \cdot \frac{1-2}{3-1} \cdot \frac{1-3}{3-2} = 1$)

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, d.h. $sgn(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}) = 1 \Rightarrow A_3 = \{id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$.

Bemerkung 3.77. $n \geq 2, \pi \in S_n \backslash A_n$. Dann gilt:

(a) $S_n = A_n \cup A_n\pi$, $A_n \cap A_n\pi = \emptyset$. Hierbei ist $A_n\pi := \{\sigma \circ \pi | \sigma \in A_n\}$

Also: $S_n = A_n \dot{\cup} A_n\pi$

(b) $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

Satz 3.78.
Es gibt genau eine Determinante $\det : M(n\times n, K) \to K$
Diese ist durch $\det(A) = \sum_{\sigma\in S_n} sgn(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ für $A = (a_{ij}) \in M(n\times n, K)$ (Leibniz-Formel) gegeben.

Satz 3.79. $A \in M(n\times n, K)$
Dann gilt: $\det(A^t) = \det(A)$

Satz 3.80. (Algorithmus)
Eingabe: $A \in M(n\times n, K)$
Ausgabe: $\det(A)$
Durchführung:
1. Bringe A durch elementare Zeilen- u. Spaltenumformungen vom Typ III, IV auf obere Dreiecksgestalt:

$$B = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

2. Ist k die Zahl der benötigten Vertauschungen von Zeilen u. Spalten, dann ist $\det(A) = (-1)^k \lambda_1 \cdot \cdots \cdot \lambda_n$.

Definition 3.81. $A(a_{ij}) \in M(n\times n, K)$

$$A_{ij} := \begin{pmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & & & 0 & & & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & & & \vdots & & & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{pmatrix} \leftarrow \text{i-te Zeile}$$
$$\uparrow \text{j-te Zeile}$$

$a^{\#}_{ij} := \det(A_{ji}) \in K$
$A^{\#} := (a^{\#}_{ij}) \in M(n\times n, K) = (\det(A_{ij}))^t$ heißt die zu A komplementäre Matrix.

$$A'_{ij} := \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nn} \end{pmatrix} \in M((n-1)\times(n-1), K)$$

Beispiel 3.82. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2\times 2, \mathbb{R})$

$A_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, A_{12} = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, A_{21} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, A_{22} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$A^{\#} = \begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix}^t = \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$

Bemerkung 3.83. $A \in M(n\times n, K), i, j \in \{1, \ldots, n\}$ Dann gilt:
$\det(A_{ij}) = (-1)^{i+j} \det(A'_{ij})$

Bemerkung 3.84. $A = (a^1, \ldots, a^n) \in M(n\times n, K)$ mit Spaltenvektoren $a^1, \ldots, a^n, e^i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$

Dann gilt: $\det(A_{ij}) = \det((a^1, \ldots, a^{j-1}, e^i, a^{j+1}, \ldots, a^n))$ durch Addition von geeigneten Vielfachen der j-ten Spalte in A_{ij} über ("i-te Zeile ausräumen") $\overset{\text{D7}}{\Longrightarrow}$ Beh.

Satz 3.85. $A \in M(n\times n, K)$
Dann gilt: $A \cdot A^{\#} = \det(A) \cdot E_n = A^{\#} A$

Satz 3.86. (Entwicklungssatz von Laplace) $n \geq 2$, $A \in M(n\times n, K)$. Dann gilt:
Für jedes $i \in \{1, \ldots, n\}$ ist $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A'_{ij})$ (Entwicklung nach i-ten Zeile) und für jedes $j \in \{1, \ldots, n\}$ ist $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A'_{ij}$ (Entwicklung nach j-ter Spalte)

Beispiel 3.87.

$$\det\begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} = (-1)^{1+2} \cdot 2 \cdot \det\begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} + (-1)^{2+2} \cdot 1 \cdot \det\begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} + (-1)^{3+2} \cdot 0 \cdot \det\begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} = 0 +$$
$$\det\begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} + 0 = (-2) \cdot 1 - 3 \cdot (-1) = 1$$

Satz 3.88. $A \in Gl(n, K)$. Dann gilt:
$A^{-1} = \frac{1}{\det(A)} A^{\#} = \frac{1}{\det(A)} B^t$, wobei $B = (\det(A_{ij})) = ((-1)^{i+j} \det(A'_{ij})$

Beispiel 3.89. Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2, K)$

$$\Rightarrow A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^t = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Satz 3.90. (Cramersche Regel)

$A = (a^1, \ldots, a^n) \in Gl(n, K)$, $b \in K^n$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$

Sei die eindeutig bestimmte Lösung des LGS $Ax = b$ (es ist $x = A^{-1}b$) Dann: Für jedes $i \in \{1, \ldots, n\}$ ist $x_i = \frac{\det(a^1, \ldots, a^{i-1}, b, a^{i+1}, \ldots, a^n)}{\det(A)}$

Beispiel 3.91. Wir betrachten das reelle 3×3 LGS

$$\underbrace{\begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}}_{=:b}$$ Nach Bsp. 3.87 ist $\det(A) = 1$

$$\Rightarrow x_1 = \det\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = 1 \cdot \det\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -3$$

$$x_2 = \det\begin{pmatrix} -2 & 1 & 3 \\ -1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix} = 1 \cdot (-1) \det\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} + 1 \cdot 1 \cdot \det\begin{pmatrix} -2 & 1 \\ -1 & 2 \end{pmatrix} = 5 + (-3) = 2$$

$$x_3 = \det\begin{pmatrix} -2 & 2 & 1 \\ -1 & 1 & 2 \\ -1 & 0 & 0 \end{pmatrix} = 1 \cdot (-1) \cdot \det\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = -3$$

$$\Rightarrow Ls(A, b) = \{\begin{pmatrix} -3 \\ 2 \\ -3 \end{pmatrix}\}$$

Anmerkung: In der Praxis findet die Cramersche Regel wegen der vielen zu berechnenden Determinanten kaum Anwendung.

Bemerkung 3.92. V endlichdimensionaler K-VR, $f \in End_K(V)$

Wir wählen eine Basis B von V und setzen $\det(f) := \det(M_B(f))$

Dann gilt:

(a) $\det(f)$ ist wohldefiniert.

(b) f ist ein Isomorphismus $\Leftrightarrow \det(f) \neq 0$

Anmerkung: Ist R ein kommutativer Ring, dann kann man (in Analogie zu $M(n \times n, K)$ für einen Körper K) den Ring $M(n \times n, R)$ der $n \times n$-Matrizen mit Einträge in R betrachten.

Im Beweis von 3.77 wird nicht dividiert.

Somit: Definiert man $\det : M(n \times n, R) \to R$ durch $\det(A) = \sum_{\sigma \in S_n} sgn(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}$ für $A = (a_{ij})$ dann sind D1-D3 (für R statt K) erfüllt. (und man kann zeigen: D4-D9, D11 sind erfüllt, $\det(A) = \det(A^t)$, $A \cdot A^{\#} = A^{\#} \cdot A = \det(A) E_n$, Entwicklungssatz von Laplace).