Lineare Algebra I, SoSe11

(Prof. Dr. O. Bogopolski)

Dieses Skript basiert teilweise auf dem Skript von Prof. Dr. Fritz Grunewald. Wir betrachten ein breiteres Spektrum von Themen. Definitionen, Beispiele und Beweise werden meistens in einer anderen Weise präsentiert. Beweise werden in diesem Skript nicht aufgeschrieben.

1 Vorlesung

1.1 Mengen

Sei M eine Menge und x ein Objekt. $x \in M$ bedeutet, dass x ein Element von M ist und $x \notin M$ bedeutet, dass x kein Element von M ist.

Beispiele:

1) $\emptyset$ – Die leere Menge.
2) $\{\emptyset\}$ – Die Menge, die die leere Menge als einziges Element enthält.
3) $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Die Elemente dieser Menge sind

$$\begin{aligned} &\emptyset, \\ &\{\emptyset\}, \\ &\{\emptyset, \{\emptyset\}\}. \end{aligned}$$

4) $\{1, 2, a, \text{ein Tisch}, \text{eine Katze}\}$
5) $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ – Die Menge der natürlichen Zahlen.
6) $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ – Die Menge der ganzen Zahlen.

Zwei Arten eine Menge zu beschreiben:

(a) durch Aufzählen ihrer Elemente, so wie in 1)-6).
(b) durch eine Eigenschaft, die ihre Elemente erfüllen, so wie in 7)-10).

7) $\{x \,|\, x \text{ hat die Eigenschaft A}\}$.
8) $\{x \,|\, x \text{ ist eine natürliche Zahl mit } x \leqslant 5\} = \{1, 2, 3, 4, 5\}$.
9) $\{x \,|\, x \text{ ist eine natürliche Zahl und } x = a+b \text{ mit } a \in \{6, 7\}, b \in \{1, 2\}\} = \{7, 8, 9\}$.
10) $\{x \,|\, x \text{ ist ein Tiger und befindet sich im Hörsaal 5D}\}$.

Bezeichnungen = und $\subseteq$:

Zwei Mengen A und B heißen *gleich* (und man schreibt $A = B$), wenn A und B die gleichen Elemente haben. Eine Menge A heißt *Teilmenge* der Menge B (und man schreibt $A \subseteq B$), wenn jedes Element von A auch in B liegt.

$$\text{Es gilt } A = B \text{ genau dann, wenn } A \subseteq B \text{ und } B \subseteq A \text{ ist.}$$

$$\text{Es gilt } \emptyset \subseteq B \text{ für jede Menge } B.$$

Die Ordnung der Elemente in einer Menge ist unwichtig. So ist $\{1, 2, 3\} = \{2, 1, 3\}$.

Operationen mit Mengen:

(a) Vereinigung:

$$A \cup B := \{x \,|\, x \text{ ist ein Element von } A \text{ oder von } B\}.$$

(b) Schnitt:

$$A \cap B := \{x \,|\, x \text{ ist ein Element von } A \text{ und von } B\}.$$

(c) Differenz:

$$A \setminus B := \{x \,|\, x \text{ ist ein Element von } A \text{ aber nicht von } B\}.$$

Beispiele:

$\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}$,
$\{1,2,3\} \cap \{2,3,4\} = \{2,3\}$,
$\{1,2,3\} \setminus \{2,3,4\} = \{1\}$.

Satz 1.1.1 Sind A, B, C Mengen, dann gilt:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Bezeichnung: Sei A eine endliche Menge. Dann bezeichnet $|A|$ die Anzahl der Elemente von A.

Beispiele:

$|\emptyset| = 0$,
$|\{\emptyset\}| = 1$,
$|\{1,2\}| = |\{2,3\}| = |\{3,4\}| = 2$,
$|\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}| = 3$.

Satz 1.1.2 Sind A, B, C endliche Mengen, dann gilt:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Definition 1.1.3 Sei A eine Menge. Die Menge

$$\mathcal{P}(A) := \{X \mid X \subseteq A\}$$

heißt die *Potenzmenge* von A.

Beispiele:

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

Definition 1.1.4 Sei A eine Menge und $k \in \mathbb{N} \cup \{0\}$. Die Menge

$$\mathcal{P}_k(A) := \{X \mid X \subseteq A \text{ und } |X| = k\}$$

heißt die *Menge der k-elementigen Teilmengen* von A.

Beispiele:

$\mathcal{P}_0(\{1,2,3\}) = \{\emptyset\}$,
$\mathcal{P}_1(\{1,2,3\}) = \{\{1\},\{2\},\{3\}\}$,
$\mathcal{P}_2(\{1,2,3\}) = \{\{1,2\},\{1,3\},\{2,3\}\}$,
$\mathcal{P}_3(\{1,2,3\}) = \{\{1,2,3\}\}$,
$\mathcal{P}_4(\{1,2,3\}) = \emptyset$.

Definition 1.1.5 Seien A und B Mengen. Die Menge der Paare

$$A \times B := \{(a,b) \mid a \in A,\, b \in B\}$$

heißt *das direkte Produkt* von A und B.

Beispiele:

Sei $A = \{1,a\}$ und $B = \{1,b\}$. Dann ist $A \times B = \{(1,1),(1,b),(a,1),(a,b)\}$.
Sei $A = \{1,2\}$ und $B = \{1,2,3\}$. Dann ist

$$\begin{aligned} A \times B = \{&(1,1),(1,2),(1,3),\\ &(2,1),(2,2),(2,3)\}. \end{aligned}$$

Satz 1.1.6 Sind A, B endliche Mengen, dann ist das direkte Produkt $A \times B$ endlich und es gilt:

$$|A \times B| = |A| \cdot |B|.$$

Definition 1.1.7 Sei n eine natürliche Zahl und seien $A_1, A_2 \ldots, A_n$ Mengen. Eine Sequenz $(a_1, a_2, \ldots, a_n)$ mit $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$ heißt ein *n-Tupel.* Die Menge

$$A_1 \times A_2 \times \ldots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1,\, a_2 \in A_2, \ldots, a_n \in A_n\}$$

heißt *das direkte Produkt* von $A_1, A_2, \ldots, A_n$.

Satz 1.1.6'. Sei n eine natürliche Zahl. Sind $A_1, A_2, \ldots, A_n$ endliche Mengen, dann ist das direkte Produkt $A_1 \times A_2 \times \ldots \times A_n$ endlich und es gilt:

$$|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|.$$

Bezeichnung. Sei n ine natürliche Zahl und sei A eine Menge. Die Menge

$$A^n := \underbrace{A \times \cdots \times A}_{n \text{ mal}}$$

heißt *n-te Potenz* der Menge A.

2 Vorlesung

2.1 Natürliche Zahlen und Induktion

Axiome 2.1.1 (Peano Axiome)
Die natürlichen Zahlen können durch die folgenden Axiome charakterisiert werden:

1) 1 ist eine natürliche Zahl.

2) Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n', der ebenfalls eine natürliche Zahl ist. `(Es ist gemeint, dass` $n' = n + 1$ `ist.)`

3) Es gibt keine natürliche Zahl, deren Nachfolger 1 ist.

4) Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.

5) Ist S eine Teilmenge von $\mathbb{N}$ und gelten

   (a) $1 \in S$ und

   (b) ist $n \in S$, dann gilt auch $n' \in S$,

   so folgt $S = \mathbb{N}$.

Satz 2.1.2 Für jede endliche Menge M gilt

$$|\mathcal{P}(M)| = 2^{|M|}.$$

Satz 2.1.3 Für alle $n \in \mathbb{N}$ gilt

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Satz 2.1.4 Für alle $n \in \mathbb{N}$ gilt

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

2.2 Binomialkoeffizienten

Definition 2.2.1 Für $n, k \in \mathbb{Z}$ mit $0 \leqslant k \leqslant n$ definieren wir den *Binomialkoeffizient* $\binom{n}{k}$ als

$$\binom{n}{k} := |\mathcal{P}_k(M)|,$$

wobei M eine beliebige n-elementige Menge ist. Mit anderen Wörtern ist $\binom{n}{k}$ die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge M.

Beispiele:

1)
$$\binom{5}{3} = 10.$$
Um das zu beweisen, schreiben wir die alle 3-elementige Teilmengen der Menge $M = \{1, 2, 3, 4, 5\}$ auf:
$$\mathcal{P}_3(M) =$$
$$\{\{1,2,3\},\{1,2,4\},\{1,2,5\},\{1,3,4\},\{1,3,5\},\{1,4,5\},\{2,3,4\},\{2,3,5\},\{2,4,5\},\{3,4,5\}\}.$$

2)
$$\binom{5}{2} = 10.$$
Um das zu beweisen, schreiben wir alle 2-elementigen Teilmengen der Menge $M = \{1, 2, 3, 4, 5\}$ auf:
$$\mathcal{P}_2(M) =$$
$$\{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\}.$$

Bezeichnung. Für $n \in \mathbb{N}$ heißt die Zahl
$$n! = 1 \cdot 2 \cdot \ldots \cdot n$$
n-Fakultät. Zusätzlich definiert man $0! = 1$.

Es gilt $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040$.

Satz 2.2.2 Es gelten:

1)
$$\binom{0}{0} = 1, \quad \binom{n}{0} = 1 \ , \binom{n}{n} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{n-1} = n,$$

2)
$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

3)
$$\binom{n}{k} = \binom{n}{n-k},$$

4)
$$\binom{n}{2} = \frac{n(n-1)}{2}, \qquad \binom{n}{3} = \frac{n(n-1)(n-2)}{6},$$

5) Für $k < n$:
$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}.$$

Pascalsches Dreieck:

$$\begin{array}{ccc}
\binom{0}{0} & & 1 \\
\binom{1}{0}\binom{1}{1} & & 1 \quad 1 \\
\binom{2}{0}\binom{2}{1}\binom{2}{2} & & 1 \quad 2 \quad 1 \\
\binom{3}{0}\binom{3}{1}\binom{3}{2}\binom{3}{3} & = & 1 \quad 3 \quad 3 \quad 1 \\
\binom{4}{0}\binom{4}{1}\binom{4}{2}\binom{4}{3}\binom{4}{4} & & 1 \quad 4 \quad 6 \quad 4 \quad 1 \\
\binom{5}{0}\binom{5}{1}\binom{5}{2}\binom{5}{3}\binom{5}{4}\binom{5}{5} & & 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\dots & & \dots
\end{array}$$

Satz 2.2.3 (**Binomischer Lehrsatz**) Seien $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$. Es gilt:

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + \ldots + \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n}x^ny^0.$$

3 Vorlesung

3.1 Abbildungen

Definition 3.1.1 Eine *Abbildung* f von der Menge X in die Menge Y ist eine Vorschrift, die jedem $x \in X$ genau ein Element $y \in Y$ zuordnet. Man schreibt $f : X \to Y,\ x \mapsto f(x)$.

Beispiele:
(1) $f : \mathbb{N} \to \mathbb{N},\ x \mapsto x^2$.
(2) $g : \{1, 2, 3\} \to \{1, 2, 4\}$,

$$\begin{array}{ccc}
1 & \mapsto & 2 \\
2 & \mapsto & 2 \\
3 & \mapsto & 4
\end{array}$$

(3) $h : \{1, 2, 3\} \to \{1, 2, 4\}$,

$$\begin{array}{ccc}
1 & \mapsto & 2 \\
2 & \mapsto & 1 \\
3 & \mapsto & 4
\end{array}$$

Definition 3.1.2 Sei $A \subseteq X$. Dann heißt $f(A) = \{f(x) \,|\, x \in A\}$ das *Bild* von A.
Sei $B \subseteq Y$. Dann heißt $f^{-1}(B) = \{x \in A \,|\, f(x) \in B\}$ das *Urbild* von B.

Im Beispiel (2) oben: Das Bild von $\{1\}$ ist $\{2\}$; das Urbild von $\{2\}$ ist aber $\{1, 2\}$.

Definition 3.1.3 1) Eine Abbildung $f : X \to Y$ heißt *injektiv*, wenn für alle $x_1, x_2 \in X$ mit $x_1 \neq x_2$ gilt: $f(x_1) \neq f(x_2)$.

2) Eine Abbildung $f : X \to Y$ heißt *surjektiv*, wenn es zu jedem $y \in Y$ mindestens ein $x \in X$ mit $f(x) = y$ gibt.

3) Eine Abbildung heißt *bijektiv*, wenn sie gleichzeitig injektiv und surjektiv ist.

Im Beispiele oben: f ist injektiv, aber nicht surjektiv; g ist nicht injektiv und nicht surjektiv; h ist bijektiv.

Definition 3.1.4 Seien $f : X \to Y$ und $g : Y \to Z$ Abbildungen. Die Verknüpfung $g \circ f$ ist die wie folgt definierte Abbildung: $g \circ f : X \to Z,\ x \mapsto (g(f(x)).$

Beispiel:
$f : \{a, b, c\} \to \{1, 2, 3\}$,

$$\begin{array}{ccc} a & \mapsto & 2 \\ b & \mapsto & 3 \\ c & \mapsto & 3 \end{array}$$

$g : \{1, 2, 3\} \to \{u, v\}$,

$$\begin{array}{ccc} 1 & \mapsto & u \\ 2 & \mapsto & v \\ 3 & \mapsto & v \end{array}$$

$g \circ f : \{a, b, c\} \to \{u, v\}$,

$$\begin{array}{ccc} a & \mapsto & v \\ b & \mapsto & v \\ c & \mapsto & v \end{array}$$

Satz 3.1.5 Sei X eine endliche Menge und $f : X \to X$ eine Abbildung. Dann sind äquivalent:
(a) f ist injektiv.
(b) f ist surjektiv.
(c) f ist bijektiv.

Bemerkung: Für unendliche Mengen ist diese Äquivalenz im allgemeinen falsch. Beispielsweise ist die Abbildung $f : \mathbb{N} \to \mathbb{N},\ x \mapsto x^2$ zwar injektiv, aber nicht surjektiv.

Definition 3.1.6 Sei X eine Menge. Die Abbildung $f : X \to X$, $x \mapsto x$, heißt Identität auf X. Man bezeichnet sie mit id_X.

Satz 3.1.7 Sei $f : X \to Y$ eine Abbildung. Dann sind äquivalent:
(a) f ist bijektiv.
(b) Es existiert eine Abbildung $g : Y \to X$, so dass folgende Formeln gelten:

$$g \circ f = \mathrm{id}_X,$$

$$f \circ g = \mathrm{id}_Y.$$

Behauptung. Seien $f : X \to Y$, $g : Y \to Z$ und $h : Z \to T$ drei Abbildungen. Dann gilt: $h \circ (g \circ f) = (h \circ g) \circ f$.

Tutorium 1

Aufgabe 1:

(a) Aus dem karierten 4×4 Quadrat hat man die obere linke Zelle entfernt. Zeigen Sie, dass sich der Rest in „Eckchen“ aus drei Zellen zerschneiden lässt.

(b) Zeigen Sie die zu (a) analoge Aussage für $2^n \times 2^n$ Quadrate ($n \geqslant 2$), wobei wieder die obere linke Zelle entfernt ist.

Aufgabe 2:
Sei n eine natürliche Zahl. Zeigen Sie, dass $2^{(3^n)} + 1$ durch 3^{n+1} teilbar ist.

Aufgabe 3:
Sei Y die Menge aller **unendlichen** Seqzenzen der Form

$$(a_1, a_2, a_3, \ldots), \text{ mit } a_i \in \{0, 1\} \text{ für alle } i \in \mathbb{N}.$$

Zeiegen Sie:

(a) Es gibt eine injektive Abbildung $\mathbb{N} \to Y$.

(b) Es gibt keine bijektive Abbildung $\mathbb{N} \to Y$.

4 Vorlesung

4.1 Gruppen

Satz 4.1.1 Eine Gruppe ist eine nicht-leere Menge G zusammen mit einer Abbildung $* : G \times G \to G$ (`wir werden` $a * b$ `anstatt` $*(a, b)$ `schreiben`), so dass die folgende drei Axiome erfüllt sind:

(1) für alle $a, b, c \in G$ gilt: $a * (b * c) = (a * b) * c$,

(2) es existiert ein $e \in G$, so dass für alle $a \in G$ gilt: $a * e = e * a = a$,

(3) für alle $a \in G$ existiert $b \in G$, so dass $a * b = b * a = e$ gilt.

Behauptung: In jeder Gruppe gibt es nur ein Element, welches das zweite Axiom erfüllt. Außerdem existiert für jedes $a \in G$ genau ein Element b, für welches Axiom (3) erfüllt ist.

Das Element e heißt *neutrales* Element von G und b heißt *inverses* zu a.

Beispiele von Gruppen.

1) $\mathbb{Z}$ mit der Addition $+$.

2) $\mathbb{Q} \setminus \{0\}$ mit der Multiplication $\cdot$.

3) Sei E eine Ebene und $d(x,y)$ der Abstand zwischen den Punkten $x, y \in E$. Eine *Bewegung* von E ist eine Abbildung $f : E \to E$, so dass $d(x,y) = d(f(x), f(y))$ für alle $x, y \in E$ gilt. Beispiele von Bewegungen sind Rotationen und Spiegelungen. Die Komposition von zwei Bewegungen ist wider eine Bewegung.

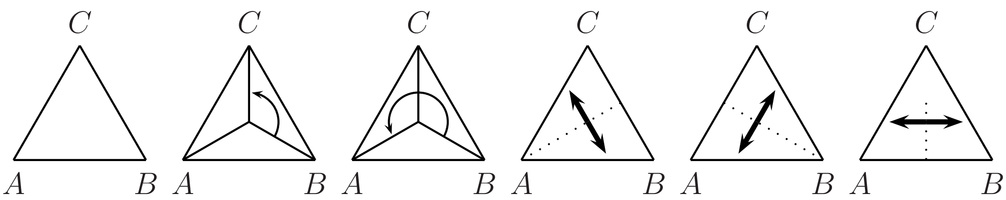
Sei ABC ein gleichseitiges Dreieck in E und sei O seine Mitte. Die Menge aller Bewegungen von E, die das Dreieck auf sich abbilden ist

$$G = \{r_0, r_{120}, r_{240}, l_A, l_B, l_C\},$$

wobei

r_α die Rotation von E um O um α Grad im Gegen-Uhrzeigersinn und

l_X die Spiegelung an der Achse (XO) ist:



r_0 :	r_{120} :	r_{240} :	l_A :	l_B :	l_C :
$A \mapsto A$	$A \mapsto B$	$A \mapsto C$	$A \mapsto A$	$A \mapsto C$	$A \mapsto B$
$B \mapsto B$	$B \mapsto C$	$B \mapsto A$	$B \mapsto C$	$B \mapsto B$	$B \mapsto A$
$C \mapsto C$	$C \mapsto A$	$C \mapsto B$	$C \mapsto B$	$C \mapsto A$	$C \mapsto C$

Diese Menge G zusammen mit der Komposition $\circ$ von Bewegungen ist eine Gruppe. Diese Gruppe heißt *Symmetriegruppe des Dreiecks ABC*.

Beispiel: Wir berechnen die Komposition $l_A \circ l_B$ in den Punkten A, B, C:

$$\begin{aligned} l_A \circ l_B(A) &= l_A(l_B(A)) = l_A(C) = B \\ l_A \circ l_B(B) &= l_A(l_B(B)) = l_A(B) = C \\ l_A \circ l_B(C) &= l_A(l_B(C)) = l_A(A) = A \end{aligned}$$

Es gilt also $l_A \circ l_B = r_{120}$.

5 Vorlesung

Beispiel. Betrachten wir die Menge S_3 aller bijektiven Abbildungen von $\{1,2,3\}$ in $\{1,2,3\}$. Jede solche Abbildung $f : \{1,2,3\} \to \{1,2,3\}$ werden wir in der Form

$$f = \binom{1 \quad\ 2 \quad\ 3}{f(1)\ f(2)\ f(3)}$$

aufschreiben. Dann ist

$$S_3 = \begin{matrix} \{\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ \gamma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & \gamma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \gamma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}. \end{matrix}$$

In der folgenden Tabelle sind die Kompositionen der Elemente aus S_3 angegeben:

$\circ$	id	α	β	γ_1	γ_2	γ_3
id	id	α	β	γ_1	γ_2	γ_3
α	α	β	id	γ_3	γ_1	γ_2
β	β	id	α	γ_2	γ_3	γ_1
γ_1	γ_1	γ_2	γ_3	id	α	β
γ_2	γ_2	γ_3	γ_1	β	id	α
γ_3	γ_3	γ_1	γ_2	α	β	id

Die Menge S_3 zusammen mit der Komposition $\circ$ ist eine Gruppe:

(a) Die Behaputung nach Satz 3.1.7 besagt, dass die Assoziativität gilt.

(b) id ist das neutrale Element.

(c) Die inversen Elemente sind in der folgenden Tabelle angegeben:

a	id	α	β	γ_1	γ_2	γ_3
a^{-1}	id	β	α	γ_1	γ_2	γ_3

Definition 5.1.1 Für jedes $n \in \mathbb{N}$ definieren wir S_n als die Menge aller biektiven Abbildungen von $\{1,2,\dots,n\}$ in $\{1,2,\dots,n\}$. Die Gruppe $(S_n, \circ)$ heißt *Permutationsgruppe* der Menge $\{1,2,\dots,n\}$.

Definition 5.1.2 Sei X eine nicht-leere Menge und sei $S(X)$ die Menge aller biektiven Abbildungen von X in X. Die Gruppe $(S(X), \circ)$ heißt *Permutationsgruppe* der Menge X.

Bemerkung. Es ist klar, dass S_n gleich $S(\{1,2,\dots,n\})$ ist.

Satz 5.1.3 Die Permutationsgruppe $(S(X), \circ)$ ist genau dann kommutativ, wenn $|X| = 1$ oder $|X| = 2$.

Bezeichnung. Sei $(G, *)$ eine Gruppe mit dem neutralen Element e. Für $a \in G$ schreiben wir

$$\begin{array}{ll} a^0 = e, & \\ a^1 = a, & \\ a^2 = a * a, & a^{-2} = a^{-1} * a^{-1}, \\ \dots & \dots \\ a^n = \underbrace{a * a * \dots * a}_{n \text{ mal}}, & a^{-n} = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{n \text{ mal}} \end{array}$$

für $n \in \mathbb{N}$.

Definition 5.1.4 Sei G eine Gruppe mit dem neutralen Element e und sei $a \in G$. Die *Ordnung* von a ist die kleinste natürliche Zahl $n \geqslant 1$, für die $a^n = e$ gilt. Gibt es keine solche Zahl, so sagt man, dass a unendliche Ordnung hat. Die Ordnung von a wird als $\mathrm{Ord}(a)$ bezeichnet. Also ist $\mathrm{Ord}(a) \in \mathbb{N} \cup \{\infty\}$.

Beispiele.

(1) In der Gruppe S_3 haben wir mit den Bezeichnungen aus dem ersten Beispiel dieser Vorlesung:

a	id	α	β	γ_1	γ_2	γ_3
$\mathrm{Ord}(a)$	1	3	3	2	2	2

(2) In der Gruppe $(\mathbb{Z}, +)$ ist $\mathrm{Ord}(z) = \infty$ für alle $z \neq 0$ und $\mathrm{Ord}(0) = 1$.

Satz 5.1.5 Sei $a \in G$ mit $\mathrm{Ord}(a) < \infty$ und sei $m \in \mathbb{N}$. Dann gilt $a^m = e$ genau dann, wenn $\mathrm{Ord}(a)$ ein Teiler von m ist.

Definition 5.1.6 Die *Ordnung* einer Gruppe G ist die Anzahl von Elementen in G und wird mit $|G|$ bezeichnet.

Definition 5.1.7 Sei $(G, *)$ eine Gruppe. Eine nicht-leere Teilmenge U von G heißt *Untergruppe* von G, wenn

(1) für alle $a, b \in U$ gilt $a * b \in U$,

(2) für alle $a \in U$ gilt $a^{-1} \in U$.

Bemerkung. Eine Untergruppe U einer Gruppe $(G, *)$ ist selber eine Gruppe bezüglich $*$.

Tutorium 2

Aufgabe 1: Kleine Gruppen. Zeigen Sie, dass für eine Gruppe $(G, *)$, bis auf Umbenennung der Elemente, gilt:

(a) $|G| = 1 \Rightarrow G = \{e\}$,

(b) $|G| = 2 \Rightarrow G = \{e, a\}$ mit

$*$	e	a
e	e	a
a	a	e

(c) $|G| = 3 \Rightarrow G = \{e, a, b\}$ mit

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Definition:

Zwei Gruppen $(G_1, \bullet)$ und $(G_2, *)$ heißen isomorph, wenn eine Abbildung $\varphi : G_1 \to G_2$ existiert, so dass

(1) φ ist eine Bijektion.

(2) $\varphi(x \bullet y) = \varphi(x) * \varphi(y)$ für alle $x, y \in G_1$.

Beispiel: Sei $(G_1, \bullet)$:

$\bullet$	1	2
1	1	2
2	2	1

und $(G_2, *)$:

$*$	e	a
e	e	a
a	a	e

Dann ist $\varphi : G_1 \to G_2,\ 1 \mapsto e,\ 2 \mapsto a$ eine Abbildung mit den Eigenschaften (1) und (2), also sind G_1 und G_2 isomorph.

Aufgabe 2:

Sei $\mathcal{R}$ die Menge aller Rotationen um eine beliebige Achse, die den Würfel auf sich abbilden. Zeigen Sie:

(a) $\mathcal{R}$ ist bezüglich $\circ$ eine Gruppe mit $|\mathcal{R}| = 24$.

(b) $\mathcal{R}$ ist isomorph zu S_4.

6 Vorlesung

Beispiel. Sei n eine natürliche Zahl. Als $n\mathbb{Z}$ bezeichnen wir die Menge aller ganzen Zahlen, die durch n teilbar sind:

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}.$$

Dann ist $n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$.

Satz 6.1.1 Alle von $\{0\}$ verschiedenen Untergruppen von $\mathbb{Z}$ haben die Gestalt $n\mathbb{Z}$ für ein $n \in \mathbb{N}$.

Definition 6.1.2 Sei $(G, *)$ eine Gruppe und M eine nicht-leere Teilmenge von G. Man sagt, dass G *von M erzeugt ist*, wenn jedes Element $g \in G$ in der Form

$$g = m_1 * m_2 * \cdots * m_k$$

geschrieben werden kann, wobei $m_i \in M$ oder $m_i^{-1} \in M$ für $1 \leqslant i \leqslant k$ und $k \in \mathbb{N}$ ist. In disem Fall schreibt man $\langle M \rangle = G$.

Beispiel. $\mathbb{Z} = \langle 1 \rangle = \langle 37, 7 \rangle$.

Bezeichnung. Seien $n, m \in \mathbb{N}$. Teilen wir m durch n und erhalten einen Rest r, so dass

$$m = qn + r, \quad 0 \leqslant r < n$$

gilt. Den Rest r bezeichnen wir mit $\mathrm{Rest}_n(m)$.

Beispiel. $\mathrm{Rest}_7(37) = 2$, weil $37 = 5 \cdot 7 + 2$ und $0 \leqslant 2 < 7$ ist.

Definition 6.1.3 Sei $n \in \mathbb{N}$. Wir betrachten die Menge $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Wir definieren auf $\mathbb{Z}_n$ eine Verknüpfung $+_n$ durch:

$$i +_n j = \mathrm{Rest}_n(i + j).$$

Satz 6.1.4 $(\mathbb{Z}_n, +_n)$ ist eine Gruppe.

Definition 6.1.5 Die Gruppe $(\mathbb{Z}_n, +_n)$ heißt *Restklassengruppe modulo n*.

Beispiel. Für die Gruppe $(\mathbb{Z}_4, +_4)$ ergibt sich die folgende Verknüpfungstabelle:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Beispiel. Alle Untergruppen von $\mathbb{Z}_{12}$ sind:

$$\begin{aligned}
&\{0\},\\
&\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\},\\
&\{0, 2, 4, 6, 8, 10\},\\
&\{0, 3, 6, 9\},\\
&\{0, 4, 8\},\\
&\{0, 6\}.
\end{aligned}$$

Definition 6.1.6 Seien $(G_1, \diamond)$ und $(G_2, *)$ zwei Gruppen. Eine Abbildung $\varphi : G_1 \to G_2$ heißt *Homomorphismus*, wenn

$$\varphi(x \diamond y) = \varphi(x) * \varphi(y)$$

für alle $x, y \in G_1$ gilt.

Behauptung. Seien $(G_1, \diamond)$ und $(G_2, *)$ zwei Gruppen mit neutralen Elementen e_1, e_2 und sei $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann gilt:
1) $\varphi(e_1) = e_2$,
2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$ für alle $a \in G_1$,

Beispiele.
(a) Folgende Abbildungen sind Homomorphismen:
1) $\varphi : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$.

2) $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_4$
$$\begin{cases} 0 \mapsto 0 \\ 1 \mapsto 2 \end{cases}$$

3) $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2$
$$\begin{cases} 0 \mapsto 0 \\ 1 \mapsto 1 \\ 2 \mapsto 0 \\ 3 \mapsto 1 \end{cases}$$

(b) Folgende Abbildung ist kein Homomorphismus:
$\varphi : \mathbb{Z}_2 \to \mathbb{Z}_4$
$$\begin{cases} 0 \mapsto 1 \\ 1 \mapsto 3 \end{cases}$$

Definition 6.1.7 Seien $(G_1, \diamond)$ und $(G_2, *)$ zwei Gruppen. Eine Abbildung $\varphi : G_1 \to G_2$ heißt *Isomorphismus*, wenn
1) φ eine Bijektion ist,
2) $\varphi(x \diamond y) = \varphi(x) * \varphi(y)$ für alle $x, y \in G_1$ gilt.

Satz 6.1.8 Wenn $\varphi : G_1 \to G_2$ ein Isomorphismus ist, dann ist die inverse Abbildung $\varphi^{-1} : G_2 \to G_1$ auch ein Isomorphismus.

Definition 6.1.9 Zwei Gruppen $(G_1, \diamond)$ und $(G_2, *)$ heißen *isomorph*, wenn ein Isomorphismus $\varphi : G_1 \to G_2$ existiert.

Beispiele. 1) Die Gruppe $(\mathbb{Z}, +)$ und ihre Untergruppe $(2\mathbb{Z}, +)$ sind isomorph.
2) Die Symmetriegruppe eines gleichseitigen Dreiecks und die Permutationsgruppe S_3 sind isomorph.

7 Vorlesung

Definition 7.1.1 Eine Gruppe $(G, *)$ heißt *zyklisch*, wenn ein Element $g \in G$ existiert, so dass $G = \langle g \rangle$ ist. Mit anderen Wörtern ist $G = \{g^i \,|\, i \in \mathbb{Z}\}$.

Beispiele. 1) $(\mathbb{Z}, +)$ ist eine zyklische Gruppe, weil $\mathbb{Z} = \langle 1 \rangle$ ist.
2) $(\mathbb{Z}_n, +_n)$ ist eine zyklische Gruppe für alle $n \in \mathbb{N}$, weil $\mathbb{Z}_n = \langle 1 \rangle$ ist.

Satz 7.1.2 1) Jede unendliche zyklische Gruppe ist zu $(\mathbb{Z}, +)$ isomorph.
2) Jede endliche zyklische Gruppe mit n Elementen ist zu $(\mathbb{Z}_n, +_n)$ isomorph.

Definition 7.1.3 Seien $(G_1, \diamond)$ und $(G_2, *)$ zwei Gruppen mit neutralen Elementen e_1 und e_2. Sei $\varphi : G_1 \to G_2$ ein Homomorphismus.
Der *Kern* von φ ist die Menge $\ker(\varphi) = \{x \in G_1 \,|\, \varphi(x) = e_2\}$.
Das *Bild* von φ ist die Menge $\mathrm{im}(\varphi) = \{\varphi(x) \,|\, x \in G_1\}$.

Satz 7.1.4 Seien $(G_1, \diamond)$ und $(G_2, *)$ zwei Gruppen und $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann ist äquivalent:
(a) φ ist injektiv.
(b) $\ker(\varphi) = \{e_1\}$, wobei e_1 das neutrale Element von G_1 ist.

Satz 7.1.5 Seien $(G_1, \diamond)$ und $(G_2, *)$ zwei Gruppen mit neutralen Elementen e_1, e_2 und sei $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann gilt:

1) $\ker(\varphi)$ ist eine Untergruppe von G_1,
$\mathrm{im}(\varphi)$ ist eine Untergruppe von G_2,

2) wenn $a \in G_1$ eine endliche Ordnung hat,
dann ist $\mathrm{Ord}(\varphi(a))$ ein Teiler von $\mathrm{Ord}(a)$,

3) wenn φ ein Isomorphismus ist,
dann gilt: $\mathrm{Ord}(\varphi(a)) = \mathrm{Ord}(a)$ für alle $a \in G_1$.

Definition 7.1.6 Sei $(G, *)$ eine Gruppe, H eine Untergruppe und $g \in G$. Die Menge

$$gH = \{g * h \,|\, h \in H\}$$

heißt die *linke Nebenklasse* von H in G bzgl. g. Die Menge

$$\{gH \,|\, g \in G\}$$

ist die Menge aller linken Nebenlassen von H in G.

Beispiel. Sei $G = S_3 = \{\mathrm{id}, \alpha, \beta, \gamma_1, \gamma_2, \gamma_3\}$ (siehe erstes Beispiel von Vorlesung 5) und $H = \{\mathrm{id}, \gamma_1\}$. Wir schreiben alle linken Nebenlassen von H in G auf:

$$\begin{aligned} \mathrm{id}H &= \{\mathrm{id}, \gamma_1\} = N_1, & \gamma_1 H &= \{\gamma_1, \mathrm{id}\} = N_1, \\ \alpha H &= \{\alpha, \gamma_3\} = N_2, & \gamma_2 H &= \{\gamma_2, \beta\} = N_3, \\ \beta H &= \{\beta, \gamma_2\} = N_3, & \gamma_3 H &= \{\gamma_3, \alpha\} = N_2. \end{aligned}$$

Definition 7.1.7 Sei H eine Untergruppe einer Gruppe G. Die Anzahl der linken Nebenklassen von H in G heißt der *Index von H in G* und wird mit $|G : H|$ bezeichnet.

Satz 7.1.8 (Lagrange) Sei H eine Untergruppe einer endlichen Gruppe G. Dann ist $|H|$ ein Teiler von $|G|$. Genauer gilt

$$|G| = |H| \cdot |G : H| \,.$$

Folgerung 7.1.9 Sei a ein Element einer endlichen Gruppe G. Dann ist die Ordnung von a ein Teiler der Ordnung von G.

Tutorium 3

Aufgabe 1:

Berechnen Sie alle Homomorphismen von $\mathbb{Z}_6$ nach $\mathbb{Z}_{15}$.

Aufgabe 2 (Warum die Gruppe S_n so wichtig ist):

Sei G eine endliche Gruppe mit n Elementen. Beweisen Sie, dass es einen injektiven Homomorphismus $\varphi : G \to S_n$ gibt.

Aufgabe 3:

Berechnen Sie (1 2 3 4 5) (4 3 1 2) (3 6) (2 3 5) (1 4 2 6) in der symmetrischen Gruppe S_6.

8 Vorlesung

Definition 8.1.1 Eine Permutation $\sigma \in S_n$ heißt k-Zyklus, wenn verschiedene Zahlen $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ existieren, so dass

$$\begin{aligned} &\sigma(i_j) = i_{j+1} && \text{für } 1 \leqslant j < k, \\ &\sigma(i_k) = i_1 && \text{und} \\ &\sigma(x) = x && \text{für alle } x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}. \end{aligned}$$

Schreibweise: $\sigma = (i_1 i_2 \ldots i_k)$. Die Zahl k heißt die *Länge* von σ.

Bemerkung. Es ist klar, dass $(i_1 i_2 \ldots i_k) = (i_2 i_3 \ldots i_k i_1) = \cdots = (i_k i_1 i_2 \ldots i_{k-1})$ ist.

Definition 8.1.2 Zwei Zyklen $(i_1 i_2 \ldots i_k)$ und $(j_1 j_2 \ldots j_l)$ heißen *unabhängig*, wenn

$$\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_l\} = \emptyset.$$

Bemerking. Zwei unabhängige Zyklen σ, τ kommutieren, d.h. $\sigma\tau = \tau\sigma$.

Satz 8.1.3 Jede Permutation $\sigma \in S_n$ kann als Produkt (Komposition)

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k,$$

geschrieben werden, so dass $\sigma_1, \sigma_2, \dots, \sigma_k$ unabhängige Zyklen sind. Dieses Produkt ist bis auf eine Permutation der $\sigma_1, \dots, \sigma_k$ eindeutig.

Beispiele. 1) $(62475) \circ (193) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 1 & 7 & 6 & 2 & 5 & 8 & 3 \end{pmatrix}$

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 9 & 2 & 6 & 7 & 4 & 5 & 8 & 3 \end{pmatrix} = (293) \circ (46) \circ (57)$

Definition 8.1.4 Eine Transposition in S_n ist ein Zyklus der Form (i, j) für $i, j \in \{1, 2, \dots, n\}$ mit $i \neq j$.

Satz 8.1.5 Die symmetrische Gruppe S_n ist von allen ihren Transpositionen erzeugt:

$$S_n = \langle \{(ij) \,|\, 1 \leqslant i < j \leqslant n\} \rangle.$$

Definition 8.1.6 Sei $\sigma \in S_n$ und $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$, wobei $\sigma_1, \sigma_2, \dots, \sigma_k$ unabhängige Zyklen sind. Wir defineren eine Zahl (*Signum* von σ):

$$\operatorname{sign}(\sigma) = (-1)^{L(\sigma)},$$

wobei

$$L(\sigma) = (\text{Länge}(\sigma_1) - 1) + \dots + (\text{Länge}(\sigma_k) - 1)$$

ist. Zusätzlich setzen wir $\operatorname{sign}(\mathrm{id}) = 1$.

Lemma 8.1.7 Sei $\sigma \in S_n$ und sei (ij) eine Transposition aus S_n. Dann gilt

$$\operatorname{sign}(\sigma \circ (ij)) = -\operatorname{sign}(\sigma).$$

Satz 8.1.8 Sei $\sigma, \tau \in S_n$. Dann gilt

$$\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau).$$

Folgerung 8.1.9 . Die Abblildung $\operatorname{sign} : S_n \to \{-1, 1\}$ ist ein Homomorphismus. Hier ist die Gruppe $\{-1, 1\}$ bezüglich Multiplikation betrachtet und sie ist zu der Gruppe $\mathbb{Z}_2$ bezüglich Addition isomorph.

Definition 8.1.10 Eine Permutation $\sigma \in S_n$ heißt *gerade*, wenn $\operatorname{sign}(\sigma) = 1$ ist und sie heißt *ungerade*, wenn $\operatorname{sign}(\sigma) = -1$ ist.

Bemerkung. Alle gerade Permutationen in S_n bilden eine Untergruppe. Diese Untergruppe heißt *alternierende Gruppe des Grades* n und wird als A_n bezeichnet. Es ist klar, dass $A_n = \ker(\operatorname{sign})$.

Satz 8.1.11 Sei $n \geqslant 2$. Dann hat die Untergruppe A_n Index 2 in S_n.

$$S_n = A_n \bigcup \; (12) \circ A_n$$

ist die Zerlegung von S_n in zwei Nebenklassen von A_n. Die Nebenklasse $(12) \circ A_n$ entsteht aus allen ungeraden Permutationen.

Tutorium 4

Aufgabe 1
Zeigen Sie den folgenden Satz.
Satz: Wenn τ ein k-Zyklus aus S_n ist, dann ist $\sigma\tau\sigma^{-1}$ für beliebige $\sigma \in S_n$ ebenfalls ein k-Zyklus. Genauer gilt für einen k-Zyklus $\tau = (i_1\ i_2\ \dots\ i_k)$ und $\sigma \in S_n$:

$$\sigma\tau\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_k))\,.$$

Aufgabe 2
Beweisen Sie, dass $S_n = \langle (1\ 2\ \dots\ n)\,, (1\ 2) \rangle$ gilt.

Aufgabe 3
Zeigen Sie den folgenden Satz.
Satz (Polya): Sei M eine beliebige Menge von Transpositionen aus der symmetrischen Gruppe S_n. Dann gilt die folgende Äquvialenz:

$$\langle M \rangle = S_n \quad \Leftrightarrow \quad \Gamma_M \text{ ist zusammenhängend.}$$

Dabei ist Γ_M der Graph mit $\{1, 2, \dots, n\}$ als Menge der Eckpunkte bei dem zwei Eckpunkte i, j genau dann durch eine Kanten verbunden sind, wenn $(i\ j) \in M$. Ein Graph heißt *zusammenhängend*, wenn je zwei Eckpunkte durch einen Weg verbunden werden können.

Aufgabe 4 (Quaternionen)
Wir definieren auf der Menge

$$\text{Quat} = \{1, i, j, k, -1, -i, -j, -k\}$$

eine Verknüpfung durch die folgenden Bedingungen:

- 1 ist neutrales Element,
- -1 wird mit den Elementen aus Quat auf die natürliche Weise multipliziert,
- $i^2 = j^2 = k^2 = -1$,
- $ij = k, \quad ji = -k,$
  $jk = i, \quad kj = -i,$
  $ki = j, \quad ik = -j.$

Diese Verknüpfung macht Quat zu einer Gruppe. Geben Sie alle Untergruppen dieser Gruppe an.

9 Vorlesung

Definition 9.1.1 Eine nicht-leere Menge K zusammen mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring*, wenn folgende Axiome erfüllt sind:

A1. $a + (b + c) = (a + b) + c$ für alle $a, b, c \in K$

A2. Es gibt ein Element $0 \in K$ mit $0 + a = a + 0 = a$ für alle $a \in K$.

A3. Für jedes $a \in K$ existiert ein $b \in K$, so dass $a + b = b + a = 0$ gilt.
(Das Element b wird als $-a$ bezeichnet.)

A4. $a + b = b + a$ für alle $a, b \in K$.

M1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in K$ (Assoziativität).

D1. $c \cdot (a + b) = c \cdot a + c \cdot b$ für alle $a, b, c \in K$ (linkes Distributivgesetz).

D2. $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in K$ (rechtes Distributivgesetz).

Definition 9.1.2 Ein Ring K heißt *kommutativ*, wenn $a \cdot b = b \cdot a$ für alle $a, b \in K$.
Ein Element $e \in K$ heißt *Einselelement* des Ringes K, wenn $e \cdot a = a \cdot e = a$ für alle $a \in K$.

Bemerkung. Wenn der Ring $(K, +, \cdot)$ ein Einselelement hat, dann ist dieses eindeutig bestimmt und wird mit 1 bezeichnet.

Beispiele.
1) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselelement 1.
2) $(n\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring und hat für $n > 1$ kein Einselement.
3) $(\mathbb{Q}, +, \cdot)$ ist ein kommutativer Ring mit Einselelement 1.
4) $(\mathbb{R}, +, \cdot)$ ist ein kommutativer Ring mit Einselelement 1.
5) Wir betrachten die Menge K der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Für $f, g \in K$ definieren wir die Funktionen $f + g$ und $f \cdot g$ durch

$$\begin{aligned} (f + g)(x) &:= f(x) + g(x) \text{ für alle } x \in \mathbb{R}, \\ (f \cdot g)(x) &:= f(x) \cdot g(x) \quad \text{ für alle } x \in \mathbb{R}. \end{aligned}$$

Mit diesen Verknüpfungen wird K zu einem kommutativen Ring mit der Funktion $1_{\mathbb{R}} : \mathbb{R} \to \mathbb{R},\ x \mapsto 1$ als Einselement.
6) Sei n eine natürliche Zahl. Die Menge $\mathbb{Z}_n = \{0, 1, \ldots, n\}$ wird zusammen mit der Verknüpfung $+_n$ als Addition und der durch

$$x \bullet_n y := \text{Rest}_n(i \cdot j)$$

definierten Verknüpfung als Multiplikation zu einem kommutativen Ring mit Einselement 1. Der Ring $(\mathbb{Z}_n, +_n, \bullet_n)$ heißt Restklassenring modulo n.
Die Verknüpfungstabellen für $n = 4$ sind:

$+_n$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\bullet_n$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

7) Sei $(K, +, \cdot)$ ein Ring. Wir definieren auf der Menge

$$M(2, K) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K \right\}$$

der 2×2-Matrizen die Verknüpfungen $+$ und $\cdot$ durch

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix},$$
$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

Man kann beweisen, dass $M(2, K)$ ein Ring ist. Falls K ein Einselement 1 besitzt, so ist die Matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ das Einselemet von $M(2, K)$.

Definition 9.1.3 Sei $(K, +, \cdot)$ ein Ring. Eine nicht-leere Teilmenge $U \subseteq K$ heißt *Unterring*, wenn folgende Axiome erfüllt sind.

U1. Aus $a, b \in U$ folgt $a + b \in U$.

U2. Aus $a \in U$ folgt $-a \in U$.

U3. Aus $a, b \in U$ folgt $a \cdot b \in U$.

Bemerkung. Es ist klar, dass U1 und U2 implizieren $0 \in U$. Mit den Verknüpfungen $+, \cdot$ ist U ein Ring.

Definition 9.1.4 Sei $(K, +, \cdot)$ ein kommutativer Ring. Eine nichtleere Teilmenge I von K heißt *Ideal*, wenn

1) Aus $a, b \in I$ folgt $a - b \in I$.

2) Aus $a \in I$ und $b \in K$ folgt $a \cdot b \in I$. (Achtung: $b \in K$!)

Bemerkung. $\{0\}$ und K sind Ideale in dem Ring K.

Satz 9.1.5 Für jede natürliche Zahl n ist $n\mathbb{Z}$ ein Ideal in dem Ring $\mathbb{Z}$.
Jedes Ideal $I \neq \{0\}$ in dem Ring $\mathbb{Z}$ hat die Form $n\mathbb{Z}$ für eine natürliche Zahl n.

10 Vorlesung

Definition 10.1.1 Seien $a, b \in \mathbb{Z}$. Die Zahl b heißt *Teiler* von a, wenn eine Zahl c existiert. so dass $a = b \cdot c$ gilt. Schreibweise: $b \,|\, a$.

Definition 10.1.2 Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Eine Zahl $c \in \mathbb{N}$ heißt *größter gemeinsamer Teiler* (kurz $\mathrm{ggT}(a, b)$) von a und b, wenn folgendes gilt:
1) $c \,|\, a$ und $c \,|\, b$,
2) wenn $d \in \mathbb{Z}$ ist und $d \,|\, a$ und $d \,|\, b$, dann gilt $d \,|\, c$.

Satz 10.1.3 Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann existiert $\mathrm{ggT}(a, b)$ und ist eindeutig bestimmt. Außerdem existiern $x, y \in \mathbb{Z}$, so dass gilt:

$$ax + by = \mathrm{ggT}(a, b).$$

Satz 10.1.4 (Euklidischer Algorithmus). Seien $a_0, a_1 \in \mathbb{N} \setminus \{0\}$. Wir teilen a_0 durch a_1 mit dem Rest a_2. Danach teilen a_1 durch a_2 mit dem Rest a_3 u.s.w. bis wir den Rest 0 bekommen:

$$\begin{array}{lll}
a_0 & = q_1 a_1 + a_2, & 0 \leqslant a_2 < a_1 \\
a_1 & = q_2 a_2 + a_3, & 0 \leqslant a_3 < a_2 \\
\ldots & & \\
a_{i-1} & = q_i a_i + a_{i+1}, & 0 \leqslant a_{i+1} < a_i \\
\ldots & & \\
a_{n-1} & = q_n a_n + a_{n+1}, & 0 \leqslant a_{n+1} < a_n \\
a_n & = q_{n+1} a_{n+1} + \mathbf{0}. &
\end{array}$$

Dann ist der letzte von Null verschiedene Rest a_{n+1} gleich $\mathrm{ggT}(a, b)$.

Beispiel. Wir wenden den euklidischen Algorithmus auf die Zahlen 1022 und 318 an:

$$\begin{array}{rl}
1022 = & 3 \cdot 318 + 68 \\
318 = & 4 \cdot 68 \;\; + 46 \\
68 = & 1 \cdot 46 \;\; + 22 \\
46 = & 2 \cdot 22 \;\; + 2 \\
22 = & 11 \cdot 2 \;\;\; + 0
\end{array}$$

Es gilt also $\mathrm{ggT}(1022, 318) = 2$.
Nun bestimmen wir ganze Zahlen x, y mit $2 = x \cdot 1022 + y \cdot 318$, indem wir obige Gleichungen in umgekehrter Reihenfolge benutzen:

$$\begin{aligned}
2 &= 1 \cdot 46 - 2 \cdot 22 = 1 \cdot 46 - 2 \cdot (68 - 1 \cdot 46) = -2 \cdot 68 + 3 \cdot 46 \\
&= -2 \cdot 68 + 3 \cdot (318 - 4 \cdot 68) = 3 \cdot 318 - 14 \cdot 68 = 3 \cdot 318 - 14(1022 - 3 \cdot 318) \\
&= \underbrace{-14}_{=x} \cdot 1022 + \underbrace{45}_{=y} \cdot 318.
\end{aligned}$$

Definition 10.1.5 Seien K_1, K_2 zwei Ringe. Eine Abbildung $\varphi : K_1 \to K_2$ heißt *Homomorphismus*, wenn gilt:
1) $\varphi(a + b) = \varphi(a) + \varphi(b)$,
2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Beispiel. 1) Die Abbildung

$$\begin{aligned}\mathrm{Rest}_n : \mathbb{Z} &\to \mathbb{Z}_n,\\ x &\mapsto \mathrm{Rest}_n(x)\end{aligned}$$

ist ein Ringhomomorphismus.

2) Sei F der Ring der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Dann ist die Abbildung $\varphi : F \to \mathbb{R}$, $f \mapsto f(1)$, ein Homomorphismus.

Satz 10.1.6 Sei $\varphi : K_1 \to K_2$ ein Ringhomomorphismus. Dann gilt:

1) Das Bild von φ
$$\mathrm{im}\,(\varphi) = \{\varphi(x) \,|\, x \in K_1\}$$
ist ein Unterring in K_2.

2) Der Kern von φ
$$\ker\,(\varphi) = \{x \in K_1 \,|\, \varphi(x) = 0\}$$
ist ein Unterring in K_1. Der Kern ist sogar ein Ideal in K_1.

Satz 10.1.7 Sei $\varphi : K_1 \to K_2$ ein Ringhomomorphismus. Dann gilt:

1) $\varphi(0) = 0$,

2) φ ist injektiv genau dann, wenn $\ker(\varphi) = \{0\}$.

Definition 10.1.8 Seien K_1, K_2 zwei Ringe. Eine Abbildung $\varphi : K_1 \to K_2$ heißt Isomorphismus, wenn φ ein bijektiver Ringhomomorphismus ist.

Beispiele. 1) Der Kern des Homomorphismus $\mathrm{Rest}_n : \mathbb{Z} \to \mathbb{Z}_n$ ist $n\mathbb{Z}$.

2) Der Kern des Homomorphismus $\mathbb{Z}_9 \to \mathbb{Z}_3$, $x \mapsto \mathrm{Rest}_3(x)$, ist das Ideal $\{0, 3, 6\}$ des Ringes $\mathbb{Z}_9$. Dieser Kern ist zu dem Ring $\mathbb{Z}_3$ isomorph.

Tutorium 5

Aufgabe 1(Chamäleons)

Auf einer Insel leben 45 Chamäleons, von denen 13 blau, 15 grün und 17 gelb sind. Treffen sich zwei Chamäleons verschiedener Farbe, so wechseln sie ihre Farbe in die dritte Farbe. Zeigen Sie, dass es hierdurch nicht möglich ist, dass irgendwann alle Chamäleons der Insel gelb sind.

Aufgabe 2 (Chinesischer Restklassensatz)

Finden Sie mit dem folgenden Satz eine ganze Zahl x, die die Kongruenzen

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \end{cases}$$

erfüllt.

Satz: Seien $m_1, m_2, \ldots, m_s$ paarweise teilerfremde ganze Zahlen. Dann existiert für jedes Tupel $(x_1, x_2, \ldots, x_s) \in \mathbb{Z}^s$ eine ganze Zahl x, so dass die folgenden Kongruenzen erfüllt sind:

$$\begin{cases} x \equiv x_1 \pmod{m_1}, \\ x \equiv x_2 \pmod{m_2}, \\ \ldots \\ x \equiv x_s \pmod{m_s}. \end{cases}$$

Setzen wir $m = m_1 m_2 \ldots m_s$. Ist x_0 eine beliebige Lösung, so ist die Menge aller ganzzahligen Lösungen gleich $\{x_0 + km \mid k \in \mathbb{Z}\}$. Dabei kann eine solche Lösung mit der Formel

$$x_0 := \sum_{i=1}^{s} c_i \frac{m}{m_i} x_i$$

bestimmt werden, wobei c_i invers (bzgl. Multiplikation) zu m/m_i im Ring $\mathbb{Z}_{m_i}$ ist.

Aufgabe 3 (Restklassenring modulo n)

Sei $n \in \mathbb{N}$, $n \geqslant 2$. Zeigen Sie, dass in $\mathbb{Z}_n$ die folgende zwei Aussagen äquivalent sind:

(1) Jedes von 0 verschiedene Element hat bzgl. $\bullet$ ein Inverses.

(2) n ist eine Primzahl.

Beispiele:

In $\mathbb{Z}_5$:

x	1	2	3	4
x^{-1}	1	3	2	4

In $\mathbb{Z}_4$:

x	1	2	3
x^{-1}	1	$\nexists$	3

11 Vorlesung

Definition 11.1.1 Eine nichtleere Menge K zusammen mit zwei Verknüpfungen $+$ und $\cdot$ heißt ein *Körper*, wenn
1) $(K, +)$ eine kommutative Gruppe ist,
2) $(K \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist,
3) die Distributivgesetze gelten.

Etwas ausführlicher:
A1) für alle $a, b, c \in K$ gilt: $a + (b + c) = (a + b) + c$,
A2) es existiert ein Element $0 \in K$, so dass für alle $a \in K$ gilt: $a + 0 = 0 + a = a$,
A3) für alle $a \in K$ existiert ein $b \in K$ mit $a + b = b + a = 0$,
A4) für alle $a, b \in K$ gilt: $a + b = b + a$,
B1) für alle $a, b, c \in K \setminus \{0\}$ gilt: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
B2) es existiert ein Element $1 \in K\setminus\{0\}$, so dass für alle $a \in K\setminus\{0\}$ gilt: $a \cdot 1 = 1 \cdot a = a$,
B3) für alle $a \in K \setminus \{0\}$ existiert ein $b \in K \setminus \{0\}$ mit $a \cdot b = b \cdot a = 1$,
B4) für alle $a, b \in K \setminus \{0\}$ gilt: $a \cdot b = b \cdot a$,
D1) für alle $a, b, c \in K$ gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$,
D2) für alle $a, b, c \in K$ gilt: $(a + b) \cdot c = a \cdot c + b \cdot c$.

Beispiele.
1) $(\mathbb{Q}, +, \cdot)$,
2) $(\mathbb{R}, +, \cdot)$,
3) $(\mathbb{Z}_2, +_n, \bullet_n)$.

Satz 11.1.2 Der Restklassenring $(\mathbb{Z}_n, +_n, \bullet_+)$ ist ein Körper genau dann, wenn n eine Primzahl ist.

Definition 11.1.3 Wir definieren $+$ und $\cdot$ auf der Menge $\mathbb{C} = \{(a, b) \,|\, a, b \in \mathbb{R}\}$ durch

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2),\\ (a_1, b_1) \cdot (a_2, b_2) &= (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2).\end{aligned}$$

Satz 11.1.4 $(\mathbb{C}, +, \cdot)$ ist ein Körper. Sein Nullelement ist (0,0) und sein Einselelement ist $(1, 0)$. Sei $(a, b) \neq (0, 0)$ ein von null verschiedenes Element. Dann ist

$$(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}).$$

das inverse Element zu (a, b).

Definition 11.1.5 Der Körper $(\mathbb{C}, +, \cdot)$ heißt *Körper der komplexen Zahlen.*

Algebraische Form der komplexen Zahlen.
Die Abbildung

$$\begin{aligned} \mathbb{R} &\to \mathbb{C} \\ r &\mapsto (r, 0). \end{aligned}$$

ist injektiv. Deshalb identifizieren wir 1 mit $(1, 0)$ und allgemeiner $r \in \mathbb{R}$ mit $(r, 0) \in \mathbb{C}$. Das Paar $(0, 1)$ wird mit i bezeichnet. Dann gilt $i^2 = -1$ und

$$(a, b) = (a, 0) + (0, b) = a + ib.$$

$a + ib$ heißt die *algebraische Form* der komplexen Zahl (a, b). Für $z = a + ib$ heißt a der *reelle Teil* von z, und b der *imaginäre Teil* von z. Man schreibt $a = \operatorname{Re} z$ und $b = \operatorname{Im} z$. Es gilt

$$z = \operatorname{Re} z + i \operatorname{Im} z.$$

Für die algebraische Form haben wir die folgenden Gesetze:

$$\begin{aligned} (a_1 + ib_1) + (a_2 + ib_2) &= (a_1 + a_2) + i(b_1 + b_2), \\ (a_1 + ib_1) \cdot (a_2 + ib_2) &= (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2). \end{aligned}$$

Trigonometrische Form der komplexen Zahlen.
Sei $z = a + ib$ eine von null verschiedene komplexe Zahl in der algebraischen Form. Mit der Bezeichnungen $r = \sqrt{a^2 + b^2}$, $x = \frac{a}{\sqrt{a^2+b^2}}$ und $y = \frac{b}{\sqrt{a^2+b^2}}$ haben wir

$$z = r(x + iy).$$

Da $x^2 + y^2 = 1$ ist, existiert ein Winkel $\varphi \in [0, 2\pi)$, so dass $x = \cos\varphi$ und $y = \sin\varphi$ gelten. Dann gilt:

$$z = r \cdot (\cos\varphi + i \sin\varphi).$$

Das ist die *trigonometrische Form* der komplexen Zahl z. Die reelle Zahl r heißt *Absolutbetrag* von z und wird mit $|z|$ bezeichnet. Die Zahl φ heißt *Argument* von z und wird mit $\arg(z)$ bezeichnet. Es gilt:

$$z = |z|(\cos(\arg(z)) + i \sin(\arg(z))).$$

Für $z = 0$ setzen wir $|z| = 0$ und $\arg(z) = 0$.

Beispiele.

1)

$$\frac{2 - i3}{4 - i5} = \frac{(2 - i3) \cdot (4 + i5)}{(4 - 5i) \cdot (4 + i5)} = \frac{23 - i2}{41} = \frac{23}{41} - i\frac{2}{41}.$$

2)

$$1 + i\sqrt{3} = 2 \cdot \Big(\frac{1}{2} + i\frac{\sqrt{3}}{2}\Big) = 2 \cdot (\cos\frac{\pi}{3} + i \sin\frac{\pi}{3}).$$

Satz 11.1.6 Seien $z_1 = r_1(\cos\varphi_1 + i \sin\varphi_1)$ und $z_2 = r_2(\cos\varphi_2 + i \sin\varphi_2)$ zwei komplexe Zahlen in der trigonometrischen Form. Dann gilt:

$$z_1z_2 = r_1r_2(\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)).$$

Also werden, bei der Multiplikation von z_1 und z_2, die Absolutbetäge multipliziert und ihre Argumente addiert (modulo 2π).

Definition 11.1.7 Sei $z = a+ib$ eine komplexe Zahl in der algebraischen Form. Die Zahl $\overline{z} = a - ib$ heißt *komplex Konjugierte* zu z.

Behauptung. Es gelten die folgenden Formeln:

$$\begin{aligned}
&\overline{\overline{z}} = z,\\
&\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2},\\
&\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\\
&|\overline{z}| = |z|,\\
&\arg(\overline{z}) = 2\pi - \arg(z) \quad \text{für} \quad z \notin \mathbb{R},\\
&\overline{z} \cdot z = |z|^2.
\end{aligned}$$

Eine Konstruktion eines Körper der Ordnung 4.
Wir betrachten die folgende Menge von Polynomen mit Koeffizienten in $\mathbb{Z}_2$:

$$K := \{ax + b \mid a, b \in \mathbb{Z}_2\} = \{0, 1, x, x+1\}.$$

Auf dieser Menge wird durch

$$(ax + b) \oplus (cx + d) := \mathrm{Rest}_2(a + c)x + \mathrm{Rest}_2(b + d)$$

eine Addition definiert. Eine Multiplikation $\odot$ definieren wir in drei Schritten:

<u>Schritt 1.</u> (Polynommultiplikation):
Berechne $p_1 = (ax + b) \cdot (cx + d) = acx^2 + (ad + bc)x + bd.$

<u>Schritt 2.</u> (Reduktion von p_1 zu einem Polynom ohne quadratischen Term):
Subtrahiere von p_1 das Polynom $ac(x^2 + x + 1)$ und erhalte ein Polynom $p_2 = (ad + bc - ac)x + (bd - ac)$.

<u>Schritt 3.</u> (Reduktion der Koeffizienten von p_2 modulo 2):
Setze $(ax + b) \odot (cx + d) := \mathrm{Rest}_2(ad + bc - ac)x + \mathrm{Rest}_2(bd - ac)$.

Mit den Verknüpfungen $\oplus$ und $\odot$ wird K zu einem Körper, welcher 4 Elemente enthält. Dabei ist $0x + 0$ das Nullelement und $0x + 1$ das Einselement.

12 Vorlesung

Definition 12.1.1 Sei $(K, +, \cdot)$ ein Körper. Eine nicht-leere Menge V zusammen mit zwei Verknüpfungen

$$\begin{aligned} + : \quad & V \times V \to V \quad \text{(Vektoraddition)}, \\ \cdot : \quad & K \times V \to V \quad \text{(Skalarmultiplikation)} \end{aligned}$$

heißt ein *Vektorraum über K* (oder *K-Vektorraum*), wenn folgende Axiome erfüllt sind:

(VA1) $(u + v) + w = u + (v + w)$ für alle $u, v, w \in V$,

(VA2) Es gibt ein $0_V \in V$ mit $0_V + v = v + 0_V = v$ für alle $v \in V$,

(VA3) Zu jedem $v \in V$ gibt es ein $-v \in V$ mit $v + (-v) = 0_V$,

(VA4) $u + v = v + u$ für alle $u, v \in V$,

(VS1) $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$ für alle $\lambda, \mu \in K$ und $v \in V$,

(VS2) $1_K \cdot v = v$ für alle $v \in V$

(VS3) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ für alle $\lambda, \mu \in K$ und $v \in V$,

(VS4) $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$ für alle $\lambda, \mu \in K$ und $v \in V$.

Beispiele. Sei K ein Körper.

1) $V = K^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, x_2, \ldots, x_n \in K \right\}$ mit den Verknüpfungen

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \text{ und } \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

2) Sei M eine beliebige nicht-leere Menge. Wir setzen

$$V = \{f : M \to \mathbb{R} \mid f \text{ ist eine Abbildung}\}.$$

Für $f, g \in V$ wird die Funktion $f + g$ definiert durch

$$(f + g)(m) = f(m) + g(m) \text{ für alle } m \in M.$$

Für $f \in V$ und $\lambda \in K$ wird die Funktion $\lambda \cdot f$ definiert durch

$$(\lambda \cdot f)(m) := \lambda f(m) \text{ für alle } m \in M.$$

3) $K[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \mid a_n, \ldots, a_0 \in K,\ \ n \in \mathbb{N} \cup \{0\}\}$
Die übliche Addition von zwei Polynomen und die Multiplikation eines Polynome mit einem Element aus K machen $K\,[x]$ zu einem Vektorraum.

Satz 12.1.2 Sei K ein Körper und V ein K-Vektorraum. Dann gelten:

(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) $\lambda \cdot v = 0_V$ gilt genau dann, wenn $\lambda = 0_K$ oder $v = 0_V$,

(d) $(-1) \cdot v = -v$ für alle $v \in V$.

Definition 12.1.3 Sei K ein Körper und V ein K-Vektorraum. Eine nicht-leere Teilmenge $U \subset V$ heißt *Untervektorraum von V*, falls

(UV1) $u + v \in U$ für alle $u, v \in U$,

(UV2) $-u \in U$ für alle $u \in U$,

(UV3) $\lambda \cdot u \in U$ für allle $\lambda \in K$ und $u \in U$.

Bemerkung. Aus den Axiomen (UV1) und (UV2) folgt $0_V \in U$. Ein Untervektorraum eines Vektorraums über K ist ein Vektorraum über K.

Beispiel. Sei K ein Körper und seien $\lambda_1, \lambda_2 \in K$. Dann ist

$$U_{(\lambda_1,\lambda_2)} = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in K^2 \ \middle| \ \lambda_1 x_1 + \lambda_2 x_2 = 0_V \right\}$$

ein Untervektorraum von K^2.

Satz 12.1.4 Für $\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ gilt $U_{(\lambda_1,\lambda_2)} = \{k \cdot \begin{pmatrix} \lambda_2 \\ -\lambda_1 \end{pmatrix} \mid k \in K\}$.

Satz 12.1.5 Die Untervektorräume von $V = K^2$ sind

(1) $\{0_{K^2}\}$,

(2) K^2,

(3) $U_{(\lambda_1,\lambda_2)}$ für $\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Beweis: Sei $\{0_V\} \neq U \neq K^2$ ein Untervektorraum in K^2. Wir wählen $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} a \\ b \end{pmatrix} \in U$. Ohne Beschränkung der Allgemeinheit können wir $b \neq 0$ voraussetzen (Fall $a \neq 0$ lässt sich analog betrachten). Mit der Bezeichnung $a_1 = \frac{a}{b}$ ist $\frac{1}{b} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a_1 \\ 1 \end{pmatrix} \in U$. Wir beweisen nun, dass alle Vektoren $\begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \in U$ die Form $k \cdot \begin{pmatrix} a_1 \\ 1 \end{pmatrix}$ für ein $k \in K$ haben. Es gilt

$$U \ni \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} - b_2 \cdot \begin{pmatrix} a_1 \\ 1 \end{pmatrix} = \begin{pmatrix} a_2 - b_2 a_2 \\ b_2 - b_2 \end{pmatrix} = \begin{pmatrix} a_2 - b_2 a_1 \\ 0 \end{pmatrix}.$$

Wenn $a_2 - b_2 a_1 = 0$ ist, dann setze $k := b_2$. Wir werden nun zeigen dass $a_2 - b_2 a_1 \neq 0$ nicht möglich ist. In diesem Fall wäre nämlich

$$U \ni \frac{1}{a_2 - b_2 a_1} \cdot \begin{pmatrix} a_2 - b_2 a_1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Da $\begin{pmatrix} a_1 \\ 1 \end{pmatrix} \in U$ würde zusätzlich folgen:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_1 \\ 1 \end{pmatrix} - a_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in U,$$

also $\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in U$ und damit $K^2 = U$, ein Widerspruch.

Satz 12.1.6 Seien $\lambda_1, \lambda_2, \mu_1, \mu_2 \in K$ mit $\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Dann sind die folgenden zwei Aussagen äquivalent:

(a) $U_{(\lambda_1,\lambda_2)} = U_{(\mu_1,\mu_2)}$.

(b) Es existiert ein $c \in K \setminus \{0\}$ mit $c \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}$.

Definition 12.1.7 Sei V ein K-Vektorraum und $M = \{v_1, \ldots, v_n\} \subseteq V$ eine endliche Menge von Vektoren aus V. Die *lineare Hülle von* M ist

$$\mathcal{L}(M) := \{\lambda_1 \cdot v_1 + \ldots + \lambda_n \cdot v_n \mid \lambda_1, \ldots, \lambda_n \in K\} \subseteq V.$$

Wir setzen auch $\mathcal{L}(\emptyset) = \{0_V\}$.

Satz 12.1.8 (a) Für jede endliche Menge M ist $\mathcal{L}(M)$ ein Untervektorraum von V.

(b) $\mathcal{L}(M)$ ist der kleinste Untervektorraum, der M enthält.

(c) Es gilt:

$$\mathcal{L}(M) = \bigcap_{\substack{U \text{ ist ein UVR von } V \\ M \subseteq U}} U$$

13 Vorlesung

Definition 13.1.1 Sei V ein K-Vektorraum. Eine endliche Teilmenge $M \subseteq V$ heißt *Erzeugendensystem* von V, falls $\mathcal{L}(M) = V$.
Ein K-Vektorraum V heißt *endlich erzeugt*, falls es eine endliche Teilmenge $M \subseteq V$ gibt, so dass $\mathcal{L}(M) = V$.

Beispiele.

1) $V = K^n$ ist endlich erzeugt. Ein Erzeugendensystem ist $M = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$.

2) $V = K[x]$ ist nicht endlich erzeugt.

3) Die Vektoren $\begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ bilden ein Erzeugendensystem von $\mathbb{R}^2$.

Definition 13.1.2 Eine endliche Menge $M = \{v_1, \ldots, v_n\}$ von Vektoren aus dem K-Vektorraum V heißt *linear unabhängig*, falls aus $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0_V$ mit $\lambda_1, \ldots, \lambda_n \in K$ folgt, dass $\lambda_1 = \ldots = \lambda_n = 0_K$. Außerdem ist $M = \emptyset$ linear unabhängig. Nicht linear unabhängig wird auch *linear abhängig* genannt.

Beispiele.

1) In $V = K^2$ ist $M = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ linear unabhängig. Analog für K^n.

2) In $V = K^2$ ist die Menge $M = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix} \right\}$ linear abhängig.

3) Die Vektoren $\begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ bilden ein Erzeugendensystem von $\mathbb{R}^2$.

Bemerkung. Ist $M \subseteq V$ linear unabhängig, dann gilt dies auch für jede Teilmenge von M.

Definition 13.1.3 Eine endliche Menge $M \subseteq V$ heißt *Basis* von V, falls

1) M ist ein Erzeugendensystem von V,
2) M ist linear unabhängig.

Der Vektorraum $V = \{0_V\}$ hat die Basis $B = \emptyset$.

Bemerkung.

1) K^n hat eine Basis für jedes $n \in \mathbb{N}$.

2) Ist $M = \{v_1, \ldots, v_n\}$ eine Basis von V, dann lässt sich jeder Vektor $v \in V$ in eindeutiger Weise als Linearkombination der $v_1, \ldots, v_n$ schreiben:

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n.$$

Satz 13.1.4 (Basisexistenzsatz) Jeder endlich erzeugte Vektorraum besitzt eine Basis.

Satz 13.1.5 (Austauschsatz von Steinnitz) Sei $\{v_1, \ldots, v_k\}$ linear unabhängig in V und sei $\{u_1, \ldots, u_n\}$ eine Basis von V. Dann ist $n \geqslant k$ und es existieren $u_{i_1}, \ldots, u_{i_k} \in B$, so dass

$$B' = B \setminus \{u_{i_1}, \ldots, u_{i_k}\} \cup \{v_1, \ldots, v_k\}$$

auch eine Basis von V ist.

14 Vorlesung

Satz 14.1.1 (Ergänzungssatz) Sei V ein endlich erzeugter K-Vektorraum und $L \subseteq V$ eine endliche, linear unabhängige Teilmenge. Dann gibt es eine Basis B von V mit $L \subseteq B$. Insbesondere ist $|L| \leqslant \dim_K V$.

Folgerung 14.1.2 Sei V ein endlich erzeugter K-Vektorraum und $U \subseteq V$ ein Untervektorraum. Dann ist U auch endlich erzeugt und es gilt:

$$\dim_K(U) \leqslant \dim_K(V).$$

Die Gleichheit $\dim_K(U) = \dim_K(V)$ gilt genau dann, wenn $U = V$ ist.

Definition 14.1.3 Seien U_1, U_2 Untervektorräume von V. Dann ist

$$U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$$

ebenfalls ein Untervektorraum, genannt die *Summe* von U_1 und U_2. Eine solche Summe heißt *direkte Summe* (in Zeichen $U_1 \oplus U_2$), wenn einer der folgenden äquivalenten Bedingungen erfüllt ist:

1) $U_1 \cap U_2 = \{0_V\}$.

2) Jedes $u \in U_1 + U_2$ wird eindeutig als $u = u_1 + u_2$ mit $u_1 \in U_1$, $u_2 \in U_2$ geschrieben.

Beispiele.

1) $\mathcal{L}(v_1, \ldots, v_n) + \mathcal{L}(u_1, \ldots, u_m) = \mathcal{L}(v_1, \ldots, v_n, u_1, \ldots, u_m)$.

2) Seien $U_1 = \mathcal{L}(v_1, v_2)$, $U_2 = \mathcal{L}(u_1, u_2)$ Untervektorräume in $\mathbb{R}^3$, wobei

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix},\ v_2 = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix},\ u_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix},\ u_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$$

ist. Dann ist $U_1 + U_2 = \mathbb{R}^3$ und diese Summe nicht direkt, weil der Vekrtor $\begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix}$ in $U_1 \cap U_2$ liegt.

3) Seien $U_1 = \mathcal{L}(v)$, $U_2 = \mathcal{L}(u)$ Untervektorräume in $\mathbb{R}^3$, wobei

$$v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ u = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$$

ist. Dann ist die Summe von U_1 und U_2 direkt: $U_1 + U_2 = U_1 \oplus U_2$.

Satz 14.1.4 (Dimensionsformel)
Sei V ein endlich erzeugter Vektorraum und U_1, U_2 Untervektorräume von V. Dann gilt

$$\dim(U_1 + U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2).$$

Tutorium 6

Aufgabe 1:

In $\mathbb{R}^3$ sei $v_1 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, $u_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}$. Bestimmen Sie eine Basis des Schnittes von

$$\mathcal{L}(v_1, v_2) = \{\alpha_1 v_1 + \alpha_2 v_2 \mid \alpha_1, \alpha_2 \in \mathbb{R}\} \text{ und } \mathcal{L}(u_1, u_2) = \{\beta_1 u_1 + \beta_2 u_2 \mid \beta_1, \beta_2 \in \mathbb{R}\}.$$

Lösung: Der Vektor $\beta_1 u_1 + \beta_2 u_2 \in \mathcal{L}(u_1, u_2)$ liegt genau dann in $\mathcal{L}(v_1, v_2)$ und somit im Schniit, wenn es $\alpha_1, \alpha_2 \in \mathbb{R}$ gibt, mit $\alpha_1 v_1 + \alpha_2 v_2 = \beta_1 u_1 + \beta_2 u_2$. Die letzte Gleichung ist äquivalent zu

$$\left\{\begin{array}{rl} -\alpha_1 + \alpha_2 - \beta_1 - 2\beta_2 = & 0 \\ \alpha_2 + \beta_1 + \beta_2 = & 0 \\ \alpha_1 \quad - \beta_1 - 3\beta_2 = & 0 \end{array}\right.$$

und durch Addition der ersten zur letzen Gleichung äquivalent zu

$$\left\{\begin{array}{rl} -\alpha_1 + \alpha_2 - \beta_1 - 2\beta_2 = & 0 \\ \alpha_2 + \beta_1 + \beta_2 = & 0 \\ \alpha_2 - 2\beta_1 - 5\beta_2 = & 0 \end{array}\right.$$

und durch Addition des (-1)-fachen der zweiten Gleichung zur dritten zu

$$\left\{\begin{array}{rl} -\alpha_1 + \alpha_2 - \beta_1 - 2\beta_2 = & 0 \\ \alpha_2 + \beta_1 + \beta_2 = & 0 \\ -3\beta_1 - 6\beta_2 = & 0 \end{array}\right.$$

Das letzte Gleichungssystem besitzt nun genau dann eine Lösung, wenn $-3\beta_1 - 6\beta_2 = 0$, also $\beta_1 = -2\beta_2$ gilt. In diesem Fall kann man nämlich α_2 so wählen, dass die zweite Gleichung erfüllt ist und anschließend α_1 so, dass auch die erste Gleichung erfüllt ist. Die Vektoren im Schnitt sind also genau die Vektoren $\beta_1 u_1 + \beta_2 u_2$ für die $\beta_1 = -2\beta_2$ gilt, d.h. der Schnitt ist gleich

$$\{-2\beta_2 u_1 + \beta_2 u_2 \mid \beta_2 \in \mathbb{R}\} = \{\beta_2(-2u_1 + u_2) \mid \beta_2 \in \mathbb{R}\} = \left\{ \beta_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \mid \beta_2 \in \mathbb{R} \right\} = \mathcal{L}(\underbrace{\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}}_{=:b})$$

und $\{b\}$ ist eine Basis des Schnittes.

Aufgabe 2:

Seien $f(x) = x^3 + x + 2$, $g(x) = 2x^2 - x - 3$ zwei Polynome in $\mathbb{Z}[x]$. Bestimmen Sie mit Hilfe des euklidischen Algrithmus für Polynome den ggT von $f(x)$ und $g(x)$.

15 Vorlesung

Sei K ein assoziativer, kommutativer Ring mit 1, z.B. ein Körper, $\mathbb{Z}$ oder $\mathbb{Z}[X]$.

Definition 15.1.1 Seien $m, n \in \mathbb{N}$. Eine $m \times n$-Matrix mit *Einträgen* in K ist eine Tabelle:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

mit $a_{ij} \in K$. Die Matrix A hat m *Zeilen* und n *Spalten.*

Bezeichnung: $M(m, n, K) = \{A \mid A \text{ ist eine } m \times n\text{-Matrix mit Einträgen in } K\}$.
Schreibweise: $A = (a_{ij})$.

Die Matrizen $E_n := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ und $\mathbb{O}_n := \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$ aus $M(n, n, K)$ heißen *Einheits-* und *Nullmatrix.* Die Matrix $E_{ij}(\alpha)$, deren Eintrag in der i-ten Zeile und j-ten Spalte gleich α ist und deren anderen Einträge wie in E_n sind, heißt *Elementarmatrix.*

Die Matrix D aus $M(n, n, K)$ mit $D_{ij} = 0$ für alle $i \neq j$ heißt *Diagonalmatrix.* Also ist
$D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}$ für einige $d_1, d_2, \dots, d_n$ aus K.

Beispiel. Für $n = 3$ ist $E_{23}(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}$.

Definition 15.1.2
1. Addition von Matrizen und Skalarmultiplikation:
Sei $\lambda \in K$ und $(a_{ij}), (b_{ij}) \in M(n, m, K)$. Dann definiere

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \text{ und } \lambda \cdot (a_{ij}) = (\lambda \cdot a_{ij}).$$

2. Multiplikation von Matrizen:
Seien $m, n, k \in \mathbb{N}$. Sei A eine $m \times n$- und B eine $n \times k$-Matrix über K. Dann ist das Produkt $A \cdot B$ definiert und ergibt die folgende $m \times k$-Matrix über K:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \dots & b_{1k} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nk} \end{pmatrix} = \begin{pmatrix} c_{11} & \dots & c_{1k} \\ \vdots & \ddots & \vdots \\ c_{m1} & \dots & c_{mk} \end{pmatrix},$$

wobei $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}$ für $1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k$
(„i-te Zeile von A mal j-te Spalte von B“).

Beispiele:

$$\begin{pmatrix}1&2\\3&4\end{pmatrix}+\begin{pmatrix}2&0\\3&1\end{pmatrix}=\begin{pmatrix}3&2\\6&5\end{pmatrix},\ 2\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}2&4\\6&8\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\cdot\begin{pmatrix}7&8\\1&2\\-3&-5\end{pmatrix}=\begin{pmatrix}1\cdot7+2\cdot1+3\cdot(-3)&1\cdot8+2\cdot2+3\cdot(-5)\\4\cdot7+5\cdot1+6\cdot(-3)&4\cdot8+5\cdot2+6\cdot(-5)\end{pmatrix}=\begin{pmatrix}0&-3\\15&12\end{pmatrix}$$

Satz 15.1.3 (Eigenschaften des Matrixproduktes)
Für $B, B_1, B_2 \in M(m,n,K)$, $A, A_1, A_2 \in M(n,k,K)$ und $\lambda \in K$ gelten

(1) $B\cdot(A_1+A_2) = B\cdot A_1 + B\cdot A_2$,

(2) $(B_1+B_2)\cdot A = B_1\cdot A + B_2\cdot A$,

(3) $(\lambda\cdot B)\cdot A = \lambda\cdot(B\cdot A) = B\cdot(\lambda\cdot A)$.

Satz 15.1.4 (Assoziativität des Matrizenprodukts)
Seien $A \in M(m,n,K)$, $B \in M(n,k,K)$ und $C \in M(k,l,K)$. Dann gilt

$$(A\cdot B)\cdot C = A\cdot(B\cdot C).$$

Satz 15.1.5 Die Menge $M(n,n,K)$ mit der Matrizenaddition und Multiplikation ist ein Ring mit der Nullmatrix $\mathbb{O}_n$ und der Einheitsmatrix E_n als Null- und als Einselement.

Definition 15.1.6 Eine quadratische Matrix $A \in M(n,n,K)$ heißt *invertierbar*, falls es eine Matrix $B \in M(n,n,K)$ gibt, so dass $A\cdot B = B\cdot A = E_n$. Wir definieren $\mathrm{GL}(n,K) := \{A \in M(n,n,K) \mid A \text{ ist invertierbar}\}$.

Bemerkung. Nach dem Satz 15.1.4 ist $\mathrm{GL}(n,K)$ eine Gruppe.
Beipsiele:

(1) Für $A=\begin{pmatrix}1&2\\3&4\end{pmatrix}\in M(2,2,\mathbb{R})$ ist $A^{-1}=\begin{pmatrix}-2&1\\\frac{3}{2}&-\frac{1}{2}\end{pmatrix}$.

(2) $A=\begin{pmatrix}1&-1\\1&-1\end{pmatrix}$ ist nicht invertierbar.

(3) In $M(2,2,\mathbb{Z}_5)$ ist $\begin{pmatrix}1&2\\3&4\end{pmatrix}^{-1}=\begin{pmatrix}3&1\\4&2\end{pmatrix}$.

Satz 15.1.7 Eine Matrix $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in M(2,2,K)$ ist genau dann invertierbar, wenn $ad-bc\neq 0$. In diesem Fall ist $A^{-1}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$.

16 Vorlesung

Behauptung 16.1.1 Sei $A \in M(n,m,K)$.

(a) Sei $E_{ij}(\alpha) \in M(n,n,K)$ mit $i \neq j$. Dann ist $E_{ij}(\alpha)A$ wohldefiniert und

$$\begin{aligned}&(\text{die } i\text{-te Zeile von } E_{ij}(\alpha)\cdot A)\\ =\,&(\text{die } i\text{-te Zeile von } A)+\alpha\cdot(\text{die } j\text{-te Zeile von } A).\end{aligned}$$

Alle anderen Zeilen von A bleiben unverändert.

(b) Sei $E_{ij}(\alpha) \in M(m,m,K)$ mit $i \neq j$. Dann ist $A \cdot E_{ij}(\alpha)$ wohldefiniert und

$$\begin{aligned}&(\text{die } j\text{-te Spalte von } A\cdot E_{ij}(\alpha))\\ =\,&(\text{die } j\text{-te Spalte von } A)+\alpha\cdot(\text{die } i\text{-te Spalte von } A).\end{aligned}$$

Alle anderen Spalten von A bleiben unverändert.

Beispiel.

$$\begin{pmatrix}1&0&0\\0&1&2\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}=\begin{pmatrix}1&2&3\\18&21&24\\7&8&9\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\0&1&2\\0&0&1\end{pmatrix}=\begin{pmatrix}1&2&7\\4&5&16\\7&8&25\end{pmatrix}$$

Satz 16.1.2 Jede Matrix $A \in M(n,n,K)$ kann als Produkt

$$A = B_s \cdot \ldots \cdot B_2 \cdot B_1 \cdot \mathbf{D} \cdot C_1 \cdot C_2 \cdot \ldots \cdot C_t$$

dargestellt werden, wobei $B_1,\ldots,B_s,C_1,\ldots,C_t$ Elementarmatrizen aus $M(n,n,K)$ und $\mathbf{D}$ eine Diagonalmatrix aus $M(n,n,K)$ ist.

Beispiel. $A = \begin{pmatrix}1&2&3\\-1&0&2\\0&4&7\end{pmatrix} = E_{21}(-1)\cdot E_{32}(2)\cdot\begin{pmatrix}1&0&0\\0&2&0\\0&0&-3\end{pmatrix}\cdot E_{23}\left(\frac{5}{2}\right)\cdot E_{13}(3)\cdot E_{12}(2)$

17 Vorlesung (Eliminationsverfahren von Gauß)

Wir betrachten das Gleichungssystem

$$\begin{cases} a_{11}x_1 \ + \ldots + a_{1n}x_n = b_1 \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases}$$

Hierzu heißt $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$ die *Koeffizientenmatrix* und mit $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ als Vektor der rechten Seiten heißt $A|B = \left(\begin{array}{ccc|c} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{array}\right)$ die *erweiterte Koeffizientenmatrix.*

Elementare Zeilenumformungen:

(T1) Multiplikation der i-ten Gleichung mit $\lambda \neq 0$.

(T2) Addition des λ-fachen der i-ten Gleichung zur k-ten Gleichung mit $i \neq k$.

(T3) Vertauschung zweier Gleichungen.

Das Ziel ist es, das System mit Hilfe der elementaren Zeilenumformungen (T1)-(T3) in die *Zeilenstufenform* zu brignen: In dieser Form wird die Anzahl der links stehenden Nullen innerhalb der linken Seite von Zeile zu Zeile größer. Die Nullzeile darf am Ende öfter auftauchen.

$$\left(\begin{array}{ccc|c} * & & \text{etwas} & b'_1 \\ & * & & \vdots \\ & & * & b'_r \\ & \text{Nullen} & & b'_{r+1} \\ & & & \vdots \\ & & & b'_m \end{array}\right)$$

Dabei sind $*$ Elemente ungleich 0.

Behauptung 17.1.1 Wenn eine der Zahlen $b'_{r+1}, \ldots, b'_m$ ungleich 0 ist, dann hat das System keine Lösung, sonst gibt es Lösungen und man kann alle Lösungen leicht aufschreiben.

Beispiel. Wir lösen das folgende Gleichungssystem:

$$\begin{cases} x_1 + 2x_2 + 3x_3 - x_4 + \quad x_5 = \ 1 \\ 2x_1 + 4x_2 + 0x_3 + x_4 + 11x_5 = \ 8 \\ 4x_1 + 8x_2 + 6x_3 - x_4 + 13x_5 = 10 \end{cases}$$

Durch Addition des (-2)-fachen der ersten Gleichung zur zweiten und des (-4)-fachen der ersten Gleichungen zur dritten erhält man:

$$\begin{cases} x_1 + 2x_2 \ + \ 3x_3 - \ x_4 + \ x_5 = 1 \\ \qquad\qquad - \ 6x_3 + 3x_4 + 9x_5 = 6 \\ \qquad\qquad - \ 6x_3 + 3x_4 + 9x_5 = 6 \end{cases}$$

Dies ist noch keine Zeilenstufenform. Diese erhält man aber durch Addition des (-1)-fachen der zweiten Zeile zur dritten:

$$\left\{\begin{array}{l} x_1 + 2x_2 + 3x_3 - x_4 + x_5 = 1 \\ \qquad\qquad - 6x_3 + 3x_4 + 9x_5 = 6 \end{array}\right. \tag{1}$$

Die Unbekannten, die in der Zeilenstufenform nicht am Anfang einer Zeile stehen, heißen *Parameter-Unbekannten*. Sie dürfen beliebige Werte annehmen:

$$x_2 := \lambda_2,\ x_4 := \lambda_4\ x_5 := \lambda_5.$$

Alle anderen Unbekannten lassen sich nun leicht aus diesen Werten berechnen. Dazu werden nacheinander die Gleichungen aus (1) in umgekehrter Reihenfolge benutzt:

$$\begin{aligned} x_3 &= \tfrac{6-3x_3-9x_5}{-6} = \tfrac{6-3\lambda_4-9\lambda_5}{-6} = -1 + \tfrac{1}{2}\lambda_4 + \tfrac{3}{2}\lambda_5 \\ x_1 &= 1 - x_5 + x_4 - 3x_3 - 2x_2 = 1 - \lambda_5 + \lambda_4 - 3\left(-1 + \tfrac{1}{2}\lambda_4 + \tfrac{3}{2}\lambda_5\right) - 2\lambda_2 \\ &= 4 - 2\lambda_2 - \tfrac{1}{2}\lambda_4 - \tfrac{11}{2}\lambda_5 \end{aligned}$$

Die Menge der Lösungen ist also

$$\left\{ \begin{pmatrix} 4 - 2\lambda_2 - \frac{1}{2}\lambda_4 - \frac{11}{2}\lambda_5 \\ \lambda_2 \\ -1 + \frac{1}{2}\lambda_4 + \frac{3}{2}\lambda_5 \\ \lambda_4 \\ \lambda_5 \end{pmatrix} \in \mathbb{R}^5 \ \middle|\ \lambda_2, \lambda_4, \lambda_5 \in \mathbb{R} \right\}.$$

18 Vorlesung (Determinanten)

Ist $A \in M(n,n,K)$, so bezeichnen wir mit $a_1, \ldots, a_n$ die Zeilenvektoren von A:

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \text{ mit } a_i = (a_{i1} \ \ldots \ a_{in}).$$

Definition 18.1.1 Eine Abbildung $\det : M(n,n,K) \to K, A \mapsto \det A$ heißt Determinante, falls folgendes gilt:

(D1) det ist *linear* in jeder Zeile, d.h. für jeden Index $1 \leqslant i \leqslant n$ und alle $\lambda \in K$ gilt

$$\text{(a)}\ \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i + a_i' \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i' \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} \quad \text{und}$$

$$\text{(b)}\quad \det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \lambda\cdot a_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \lambda\cdot\det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}.$$

(D2) det ist *alternierend*, d.h. hat A zwei gleiche Zeilen, so ist $\det A = 0$.

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

Eine andere Schreibweise für die Determinante ist

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \det\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

Satz 18.1.2 Eine Determinante $\det\colon M(n,n,K) \to K$ hat die folgenden weiteren Eigenschaften:

(D4) Für jedes $\lambda \in K$ gilt $\det(\lambda\cdot A) = \lambda^n \cdot \det(A)$.

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

(D6) Ist $\lambda \in K$ und entsteht B aus A durch Addition des λ-fachen der j-ten Zeile zur i-ten Zeile mit $i \neq j$, so ist $\det B = \det A$.

(D7) Entsteht B aus A durch eine Zeilenvertauschung, so ist $\det B = -\det A$.

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

(D9) Sei $n \geqslant 2$ und $A \in M(n,n,K)$ von der Gestalt

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

wobei A_1, A_2 quadratische Matrizen sind, dann gilt

$$\det A = \det A_1 \cdot \det A_2.$$

Satz 18.1.3 Für $A, B \in M(n,n,K)$ gilt $\det(A\cdot B) = \det A \cdot \det B$.

19 Vorlesung

Satz 19.1.1 (Leibniz-Formel)
Ist $n \geqslant 1$, so gibt es genau eine Determinante

$$\det : M(n,n,K) \to K$$

und zwar ist für $A = (a_{ij}) \in M(n,n,K)$:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}.$$

Beispiele.

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

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

$$\begin{aligned} = \quad & \operatorname{sign}(\mathrm{Id})\, a_{11}a_{22}a_{33} + \operatorname{sign}((1\ 2\ 3))\, a_{12}a_{23}a_{31} + \operatorname{sign}((1\ 3\ 2))\, a_{13}a_{21}a_{32} \\ & + \operatorname{sign}((1\ 3))\, a_{13}a_{22}a_{31} + \operatorname{sign}((1\ 2))\, a_{12}a_{21}a_{33} + \operatorname{sign}((2\ 3))\, a_{11}a_{23}a_{32} \\ = & \, a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \end{aligned}$$

Bezeichnung Sei $A \in M(n,n,K)$. Wir bezeichnen mit $A'_{ij} \in M(n-1,n-1,K)$ die Matrix, die man aus A durch Streichen der i-ten Zeile und der j-ten Spalte erhält. Wir nennen diese Matrix die *Komplementare* Matrix zur Stelle i,j.

Satz 19.1.2 (Erster Entwichklungssatz von Laplace)
Ist $n \geqslant 2$ und $A \in M(n,n,K)$, so gilt für jedes $i \in \{1,\ldots,n\}$

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

(Entwicklung nach der i-ten Zeile) und für jedes $j \in \{1,\ldots,n\}$

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

(Entwicklung nach der j-ten Spalte). Dabei bezeichnet A'_{ij} jeweils die oben definierte ij-Streichungsmatrix.

Beispiele.

(1) Entwicklung nach der ersten Zeile:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 0 & -1 \\ 2 & 1 & 3 \end{vmatrix} = 1 \cdot \begin{vmatrix} 0 & -1 \\ 1 & 3 \end{vmatrix} - 2 \cdot \begin{vmatrix} 4 & -1 \\ 2 & 3 \end{vmatrix} + 3 \cdot \begin{vmatrix} 4 & 0 \\ 2 & 1 \end{vmatrix} = 1 \cdot 1 - 2 \cdot 14 + 3 \cdot 4 = -15$$

(2) Entwicklung nach der zweiten Zeile:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 0 & -1 \\ 2 & 1 & 3 \end{vmatrix} = -4 \cdot \begin{vmatrix} 2 & 3 \\ 1 & 3 \end{vmatrix} + 0 \cdot \begin{vmatrix} 1 & 3 \\ 2 & 3 \end{vmatrix} - (-1) \cdot \begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix} = -4 \cdot 3 + 0 \cdot (-3) - (-1) \cdot (-3) = -15$$

(3) Entwicklung nach der zweiten Spalte:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 0 & -1 \\ 2 & 1 & 3 \end{vmatrix} = -2 \cdot \begin{vmatrix} 4 & -1 \\ 2 & 3 \end{vmatrix} + 0 \cdot \begin{vmatrix} 1 & 3 \\ 2 & 3 \end{vmatrix} - 1 \cdot \begin{vmatrix} 1 & 3 \\ 4 & -1 \end{vmatrix} = -2 \cdot 14 - 1 \cdot (-13) = -15$$

20 Vorlesung

Satz 20.1.1 (Zweiter Entwichklungssatz von Laplace)
Sei $n \geqslant 2$, $A \in M(n, n, K)$.

(a) Seien $i, k \in \{1, \ldots, n\}$ zwei verschiedene Indizes. Dann gilt:

$$\sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A'_{kj} = 0.$$

(b) Seien $j, k \in \{1, \ldots, n\}$ zwei verschiedene Indizes. Dann gilt:

$$\sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A'_{ik} = 0.$$

Beispiel. Für $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 0 & -1 \\ 2 & 1 & 3 \end{pmatrix}$ gilt nach 20.1.1(a) für $i = 2, k = 3$:

$$(-1)^{2+1} \cdot 4 \cdot \begin{vmatrix} 2 & 3 \\ 0 & -1 \end{vmatrix} + (-1)^{2+2} \cdot 0 \cdot \begin{vmatrix} 1 & 3 \\ 4 & -1 \end{vmatrix} (-1)^{2+3} \cdot (-1) \cdot \begin{vmatrix} 1 & 2 \\ 4 & 0 \end{vmatrix}.$$

Satz 20.1.2 (Anwendung zur Berechnung der inversen Matrix)
Sei $A \in M(n, n, K)$. Dann hat A genau dann eine Inverse, wenn $\det A \neq 0$. In diesem Fall gilt:

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} (-1)^{1+1} \det(A'_{11}) & \ldots & (-1)^{1+n} \det(A'_{n1}) \\ \vdots & \ddots & \vdots \\ (-1)^{n+1} \det(A'_{1n}) & \ldots & (-1)^{n+n} \det(A'_{nn}) \end{pmatrix}.$$

Elementare Zeilentransformationen einer Matrix:

(Z1) Multiplikation der i-ten Zeile mit $\lambda \neq 0$.

(Z2) Addition des λ-fachen der i-ten Zeile zur k-ten Zeile mit $i \neq k$.

Satz 20.1.3 (Ein praktisches Verfahren für die Berechnung von A^{-1} falls $\det A \neq 0$)
Sei $A \in M(n,n,K)$ mit $\det A \neq 0$. Forme die Matrix $(A \mid E_n) \in M(n,2n,K)$ durch elementare Zeilenumtransformationen so um, dass im linken Teil die Einheitsmatrix steht. Dann steht im rechten Teil die Matrix A^{-1}.

Beispiel. Um die Inverse von $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ zu berechnen, starten wir mit:

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right).$$

Addition des (-3)-fachen der ersten Zeile zur Zweiten:

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

Addition der zweiten Zeile zu Ersten:

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

Multiplikation der zweiten Zeile mit $-1/2$:

$$\left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right)$$

Also ist die inverse Matrix $\begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$.

Satz 20.1.4 (Cramersche Regel)
Wir betrachten das System

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \ldots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n. \end{cases}$$

Dieses schreiben wir kurz als $A \cdot X = B$ mit

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} = (a^{(1)}\ a^{(2)}\ \ldots\ a^{(n)}),\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

wobei $a^{(1)}, \ldots, a^{(n)}$ die Spalten der Matrix A sind. Wenn $\det A \neq 0$, dann gilt für jedes $i \in \{1, \ldots, n\}$:

$$x_i = \frac{\det\left(a^{(1)}\ \ldots\ a^{(i-1)}\ B\ a^{(i+1)}\ \ldots\ a^{(n)}\right)}{\det A}.$$

Die Matrix im Zähler ist die Matrix A, bei der die i-te Spalte durch B ersetzt wurde.

Beispiel. Für $\begin{cases} x_1 + 2x_2 = 7 \\ 3x_1 + 5x_2 = 18 \end{cases}$ ist

$$x_1 = \frac{\begin{vmatrix} 7 & 2 \\ 18 & 5 \end{vmatrix}}{\begin{vmatrix} 1 & 2 \\ 3 & 5 \end{vmatrix}} = \frac{35-36}{5-6} = 1 \text{ und } x_2 = \frac{\begin{vmatrix} 1 & 7 \\ 3 & 18 \end{vmatrix}}{\begin{vmatrix} 1 & 2 \\ 3 & 5 \end{vmatrix}} = \frac{18-21}{5-6} = 3.$$

21 Vorlesung

Definition 21.1.1 Sei K ein Körper und U, V zwei K-Vektorräume. Eine Abbildung $\varphi : U \to V$ heißt *lineare Abbildung*, falls

(1) $\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2)$ für alle $u_1, u_2 \in U$,

(2) $\varphi(\lambda \cdot u) = \lambda \cdot \varphi(u)$ für alle $\lambda \in K$ und $u \in U$.

Bemerkung. Die Bedingungen (1)-(2) sind dem volgenden Bedingung äquivalent:
Für alle $u_1, u_2 \in U$ und $\lambda_1, \lambda_2 \in K$ gilt $\varphi(\lambda_1 u_1 + \lambda_2 u_2) = \lambda_1 \cdot \varphi(u_1) + \lambda_2 \cdot \varphi(u_2)$.

Beispiele.

1) Wir betrachten K als Vektorraum über K. Sei $a \in K$ und $\varphi_a : K \to K$ definiert durch $\varphi_a(x) = a \cdot x$ für alle $x \in K$. Dann ist φ_a linear.

2) Sei V ein K-Vektorraum und $M = \{v_1, \ldots, v_n\} \subseteq V$ eine endliche Menge von Vektoren. Wir definieren $\varphi_M : K^n \to V$ durch

$$\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \mapsto k_1 v_1 + \ldots + k_n v_n.$$

Dann ist φ_M linear.

3) Sei $V = \mathbb{R}^2$ und $M = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix} \in \mathbb{R}^2 \right\}$. Dann ist $\varphi_M : \mathbb{R}^3 \to \mathbb{R}^2$,

$$\begin{pmatrix} k_1 \\ k_2 \\ k_3 \end{pmatrix} \mapsto k_1 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} + k_2 \cdot \begin{pmatrix} -1 \\ 3 \end{pmatrix} + k_3 \cdot \begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} k_1 - k_2 + 4k_3 \\ 2k_1 + 3k_2 + 5k_3 \end{pmatrix},$$

linear.

Behauptung. Sei $\varphi : U \to V$ eine lineare Abbildung. Es gelten

(1) $\varphi(0_U) = 0_V$,

(2) $\varphi(-u) = -\varphi(u)$ für alle $u \in U$.

Definition 21.1.2 Sei $\varphi : U \to V$ eine lineare Abbildung. Wir definieren das *Bild von* φ:

$$\mathrm{Im}(\varphi) = \{v \in V \mid \exists u \in U \text{ mit } \varphi(u) = v\}$$

und den *Kern von* φ:

$$\mathrm{Ker}(\varphi) = \{u \in U \mid \varphi(u) = 0_V\}.$$

Satz 21.1.3 Sei $\varphi : U \to V$ eine lineare Abbildung. Dann gelten:

(1) $\operatorname{Im}(\varphi) \subseteq V$ und $\operatorname{Ker}(\varphi) \subseteq U$ sind Untervektorräume.

(2) φ ist genau dann surjektiv, wenn $\operatorname{Im}(\varphi) = V$ ist.

(3) φ ist genau dann injektiv, wenn $\operatorname{Ker}(\varphi) = 0_V$ ist.

Satz 21.1.4 (Im-Ker-Formel) Sei U ein endlich erzeugter und V ein beliebiger K-Vektorraum. Sei $\varphi : U \to V$ eine lineare Abbildung. Dann sind $\operatorname{Im}(\varphi)$ und $\operatorname{Ker}(\varphi)$ endlich erzeugt und es gilt:

$$\dim_K(U) = \dim_K(\operatorname{Ker}(\varphi)) + \dim_K(\operatorname{Im}(\varphi)).$$

Satz 21.1.5 (Existenz und Eindeutigkeitssatz für lineare Abbildungen)
Sei U ein K-Vektorraum mit Basis $\{u_1, \ldots, u_n\}$. Weiter sei V ein K-Vektorraum und $v_1, \ldots, v_n$ beliebige Elemente aus V. Dann gibt es eine eindeutig bestimmte lineare Abbildung

$$\varphi : U \to V \text{ mit } \varphi(u_1) = v_1, \ldots, \varphi(u_n) = v_n.$$

Satz 21.1.6 Sei $\varphi : U \to V$ eine bijektive lineare Abbildung. Dann ist auch φ^{-1} linear.

Definition 21.1.7 Seien U und V zwei K-Vektorräume. Eine Abbildung $\varphi : U \to V$ heißt *Isomorphismus*, falls

(1) φ ist bijektiv und

(2) φ ist eine lineare Abbildung.

U und V heißen *isomorph*, falls es einen Isomorphismus $\varphi : U \to V$ gibt.

Satz 21.1.8 Zwei endlich erzeugte K-Vektorräume U, V sind genau dann isomorph, wenn $\dim U{=}\dim V$.

22 Vorlesung

Definition 22.1.1 Sei $A \in M(n, m, K)$. Der *Zeilenrang* von A, bezeichnet als $\operatorname{ZRang}(A)$, ist die maximale Anzahl an linear unabhhängigen Zeilen von A. Z.B. ist

$$\operatorname{ZRang}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \end{pmatrix} = 2.$$

Analog wird der Spaltenrang von A definiert und mit $\operatorname{SRang}(A)$ abgekürzt. Mit anderen Worten: Sei $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (b_1 \ \ldots \ b_m)$, wobei a_i die i-te Zeile und b_j die j-te Spalte von A sind. Dann ist

$$\operatorname{ZRang}(A) = \dim \mathcal{L}(a_1, \ldots, a_n) \text{ und } \operatorname{SRang}(A) = \dim \mathcal{L}(b_1, \ldots, b_m).$$

Satz 22.1.2 Die elementaren Zeilenumformungen (Z1), (Z2) verändern den Zeilenrang von A nicht:

(Z1) Für $\lambda \in K$ und $i \neq j$ gilt $\text{ZRang}\begin{pmatrix} a_1 \\ \dots \\ a_i \\ \dots \\ a_j \\ \dots \\ a_n \end{pmatrix} = \text{ZRang}\begin{pmatrix} a_1 \\ \dots \\ a_i + \lambda a_j \\ \dots \\ a_j \\ \dots \\ a_n \end{pmatrix}$

(Z2) Für $\lambda \neq 0$ gilt $\text{ZRang}\begin{pmatrix} a_1 \\ \dots \\ a_i \\ \dots \\ a_n \end{pmatrix} = \text{ZRang}\begin{pmatrix} a_1 \\ \dots \\ \lambda a_i \\ \dots \\ a_n \end{pmatrix}$

Methode: Um den Zeilenrang einer Matrix A zu bestimmmen formt man diese zunächst durch elementare Zeilentransformationen zu einer Matrix A' in Zeilenstufenform um. Hat A' dann r Nicht-Nullzeilen, so gilt:

$$\text{ZRang}(A) = \text{ZRang}(A') = r.$$

Satz 22.1.3

(a) Zeilentransformationen verändern weder Zeilen noch Spaltenrang.

(b) Spaltentransformationen verändern weder Zeilenrang noch Spaltenrang.

Satz und Definition 22.1.4 Es gilt $\text{ZRang}(A) = \text{SRang}(A)$. Diese Zahl heißt *Rang* von A und wird als $\text{Rang}(A)$ bezeichnet.

Folgerung 22.1.5

(a) $\text{Rang}(A)$=$\text{Rang}(A^T)$.

(b) Sei $A \in M(n, m, K)$. Dann ist $\text{Rang}(A) \leqslant \min(n, m)$.

Satz 22.1.6 Sei $A \in M(n, n, K)$. Dann ist

$$\det A \neq 0 \;\Leftrightarrow\; \text{Rang}(A) = n.$$

Satz 22.1.7 Sei $A \in M(m, n, K), B \in M(n, k, K)$. Dann ist

$$\text{Rang}(A \cdot B) \leqslant \text{Rang}(A),\ \text{Rang}(B).$$

Satz 22.1.8 Sei $A \in M(m, n, K)$, $B \in M(n, n, K)$, $C \in M(m, m, K)$ und sei $\det B \neq 0$, $\det C \neq 0$. Dann gilt:

(a) $\text{Rang}(A \cdot B)$ =$\text{Rang}(A)$,

(b) $\text{Rang}(C \cdot A)$ =$\text{Rang}(A)$.

Definition 22.1.9 Sei $A \in M(n, m, K)$ und sei $1 \leqslant k \leqslant \min\{n, m\}$. Wählen wir k Zeilen und k Spalten von A. Die Einträge, die auf dem Schnitt dieser Zeilen und Spalten stehen, bilden eine $k \times k$-Teilmatrix von A. Die Determinante einer solchen Teilmatrix heißt k-*Minor* von A.

Beispiel. Die Anzahl der 2-Minoren der Matrix $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}$ ist 18. Einer von diesen ist

$$\det \begin{pmatrix} a_{22} & a_{24} \\ a_{32} & a_{34} \end{pmatrix} = a_{22} \cdot a_{34} - a_{24} \cdot a_{32}.$$

Bemerkung. Für $A \in M(n, m, K)$ ist die Anzahl der $k \times k$-Teilmatrizen gleich $\binom{n}{k} \cdot \binom{m}{k}$.

Satz 22.1.10 Für $A \in M(n, m, K) \setminus \{0\}$ gilt:

$$\mathrm{Rang}(A) = \max\{k \in \mathbb{N} \mid A \text{ besitzt einen von 0 verschiedenen } k\text{-Minor}\}.$$

23 Vorlesung

Wir betrachten ein homogenes lineares Gleichungssystem über K

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m, \end{cases}$$

kurz $A \cdot X = B$. Die Menge aller Lösungen dieses Systems bezeichnen wir als $\text{Lös}(AX = B)$.

Satz 23.1.1 Das System $A \cdot X = B$ ist genau dann lösbar, wenn $\mathrm{Rang}(A) = \mathrm{Rang}(A \mid B)$ ist.

Satz 23.1.2 Sei $X^{(0)}$ eine Lösung des Systems $AX = B$. Dann ist

$$\text{Lös}(AX = B) = X^{(0)} + \text{Lös}(AX = 0).$$

Satz 23.1.3 Wir betrachten ein *homogenes* lineares Gleichungssystem über K

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0, \end{cases}$$

kurz $A \cdot X = 0$. Dann ist die Menge aller Lösungen:

$$\text{Lös}(AX = 0) = \{x \in K^n \mid Ax = 0\}$$

ein Untervektorraum von K^n. Dieser hat die Dimension $n - r$, wobei $r = \mathrm{Rang}(A)$ ist.

Definition 23.1.4 Sei $AX = 0$ ein homogenes lineares Gleichungssystem über K. Eine Basis von dem Vektorraum $\text{Lös}(AX = 0)$ heißt *Fundamentalsystem* von Lösungen des Systems $AX = 0$.

Vorgehensweise (zur Berechnung eines Fundamentalsystems):
Im ersten Schritt bringen wir das homogene lineare Gleichungssystem $AX = 0$ auf Zeilenstufenform. Hier gibt es $r = \text{Rang}(A)$ führende Unbekannte und $(n - r)$ Parameterunbekannte. Wir erstellen nun eine Tabelle mit $n - r$ Zeilen und n Spalten, wobei die j-te Spalte für die Unbekannte x_j steht. In der i-ten Zeile wird der i-te Parameterunbekannte als 1 und alle weiteren Parameterunbekannten als 0 gewählt. Mit Hilfe des Gleichungssystems berechnen sich hieraus die führenden Unbekannten. In den Zeilen dieser Tabelle steht nun ein Fundamentalsystem von Lösungen.

Beispiel. Wir berechnen ein Fundamentalsystem von Lösungen für das reelle Gleichungssystem

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ 2x_1 + 2x_2 + 4x_3 + 2x_4 + 6x_5 = 0. \end{cases}$$

Dieses brignen wir in Zeilenstufenform:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ \qquad\qquad 2x_3 \qquad + 4x_5 = 0. \end{cases}$$

Nun sind x_1, x_3 die führenden Unbekannten und x_2, x_4, x_5 die Parameterunbekannten.

x_1	x_2	x_3	x_4	x_5
-1	1	0	0	0
-1	0	0	1	0
1	0	-2	0	1

Ein Fundamentalsystem ist also:

$$\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

24 Vorlesung

24.1 Eigenwerte und Eigenvektoren

Definition 24.1.1 (Eigenwerte und Eigenvektoren für Matrizen)

Sei $A \in M(n,n,K)$. Ein $\lambda \in K$ heißt *Eigenwert von A*, wenn es ein $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$ mit $v \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ gibt, so dass folgendes gilt:

$$A \cdot v = \lambda \cdot v.$$

Jedes $v \in K^n \setminus \{0_{K^n}\}$ mit $A \cdot v = \lambda \cdot v$ heißt *Eigenvektor von A zum Eigenwert λ*.

Beispiele.

(a) Für $A = \begin{pmatrix} 5 & -1 \\ 3 & 1 \end{pmatrix}$ ist $v = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ ein Eigenvektor zum Eigenwert 2 und $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ein Eigenvektor zum Eigenwert 4.

(b) Für $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ sind $\begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix}$ Eigenvektoren zum Eigenwert 0 und $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ ist Eigenvektor zum Eigenwert 6.

Bemerkung. Sei $A \in M(n,n,K)$. Wir definieren eine Abbildung $\varphi : K^n \to K^n$ durch $\varphi(X) = A \cdot X$ für $X \in K^n$. Dann ist diese Abbildung linear.

Definition 24.1.2 Sei V ein K-Vektorraum und sei $\varphi : V \to V$ eine lineare Abbildung. Ein $\lambda \in K$ heißt *Eigenwert von φ*, wenn ein $v \in V \setminus \{0\}$ existiert, so dass

$$\varphi(v) = \lambda \cdot v.$$

Jedes $v \in V \setminus \{0\}$ mit $\varphi(v) = \lambda \cdot v$ heißt *Eigenvektor von φ zum Eigenwert λ*.

Bemerkung. Wenn v ein Eigenvektor von φ zum Eigenwert λ ist, dann auch $k \cdot v$ (für alle $k \in K \setminus \{0\}$).

Geometrische Interpretation: Sei v ein Eigenvektor von φ zum Eigenwert λ. Dann ist die Gerade $\mathcal{L}(v) = \{k \cdot v \mid k \in K\}$ *φ-invariant*, d.h. $\varphi(\mathcal{L}(v)) \subseteq \mathcal{L}(v)$.

Lemma 24.1.3 Sei $B \in M(n,n,K)$. Dann hat die Gleichung $BX = 0$ genau dann eine nichttriviale Lösung (d.h. $\neq 0$), wenn $\det(B) = 0$ gilt.

Definition 24.1.4 Sei $A \in M(n, n, K)$. Das charakteristisches Polynom von A ist das Polynom

$$\chi_A(\lambda) = \det(A - \lambda \cdot E_n) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{vmatrix}.$$

Beispiel. Für $A = \begin{pmatrix} 1 & 0 & 2 \\ 3 & -1 & 4 \\ 2 & 1 & 5 \end{pmatrix}$ ist $A - \lambda \cdot E_n = \begin{pmatrix} 1-\lambda & 0 & 2 \\ 3 & -1-\lambda & 4 \\ 2 & 1 & 5-\lambda \end{pmatrix}$ und

$$\begin{aligned} \det(A - \lambda \cdot E_3) &= (1-\lambda)(-1-\lambda)(5-\lambda) + 3 \cdot 2 \cdot 1 + 2 \cdot 0 \cdot 4 \\ &= -2 \cdot (-1-\lambda) \cdot 2 - 3 \cdot 0 \cdot (5-\lambda) - 1 \cdot 4 \cdot (1-\lambda) \\ &= (-\lambda^3 + 5\lambda^2 + \lambda - 5) + 6 + (4 + 4\lambda) - (4 - 4\lambda) = -\lambda^3 + 5\lambda^2 + 9\lambda + 1. \end{aligned}$$

Bemerkung. $\chi_A(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_0$, wobei

$$\begin{aligned} a_n &= (-1)^n \\ a_{n-1} &= (-1)^{n-1}(a_{11} + \ldots + a_{nn}) \\ a_{n-2} &= (-1)^{n-2}(\text{Summe aller 2-Hauptminoren von } A) \\ &\dots \\ a_0 &= \det A. \end{aligned}$$

Dabei ist ein k-Hauptminor von A die Determinante einer $k \times k$-Teilmatrix, bei der die gewählten Spalten und Zeilenindices übereinstimmen (vgl. Def 21.1.9).

Satz 24.1.5 Sei $\alpha \in K$. Dann ist α genau dann ein Eigenwert von A, wenn α eine Nullstelle von $\chi_A(\lambda)$ ist.

Satz 24.1.6 Jedes Polynom $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ mit Koeffizienten in einem Körper K und $a_n \neq 0$ hat nicht mehr als n Nullstellen in K.
Ist $K = \mathbb{C}$, dann gilt

$$f(x) = a_n(x - \lambda_1)^{k_1}(x - \lambda_2)^{k_2} \ldots (x - \lambda_s)^{k_s},$$

wobei $\lambda_1, \lambda_2, \ldots, \lambda_s \in \mathbb{C}$ – alle verschiedene Nullstellen von $f(x)$ sind, $k_1, k_2, \ldots, k_s \in \mathbb{N}$ und $s \leqslant n$ ist. Die Zahl k_i heißt *Vielfaches der Nullstelle* λ_i. Wenn wir jede Nullstelle λ_i nicht einmahl, sondern k_i mal zählen, dann ist die gesammte Anzahl von Nullstellen n.

Wie sucht man Eigenwerte und Eigenvektoren von A?

(1) Eigenwerte sind die Nullstellen von $\chi_A(\lambda)$. Seien $\lambda_1, \ldots, \lambda_k$ diese Nullstellen.

(2) Für jedes λ_i ist das System $AX = \lambda_iX$ zu lösen. Dieses ist äquivalent zu

$$(A - \lambda_iE_n)X = 0.$$

Man finde ein Fundamentalsystem $v_1, \ldots, v_p$ von Lösungen dieses Systems. Dann sind die Eigenvektoren zum Eigenwert λ_i die nichttrivialen Linearkombinationen dieser Vektoren, also die Vektoren in $\mathcal{L}(v_1, \ldots, v_p) \setminus \{0\}$.

Definition 24.1.7 Zwei Matrizen $A, B \in M(n, n, K)$ heißen *ähnlich*, falls eine invertierbare Matrize $T \in M(n, n, K)$ mit $B = T^{-1}AT$ existiert.

Satz 24.1.8 Wenn A und B ähnliche Matrizen sind, dann gilt $\chi_A(\lambda) = \chi_B(\lambda)$.

25 Vorlesung

Definition 25.1.1 Seien $\varphi : V \to V$ eine lineare Abbildung und λ ein Eigenwert von φ. Die Menge $\operatorname{Eig}(\varphi, \lambda) := \{v \in V \mid \varphi(v) = \lambda v\}$ heißt *Eigenraum* von φ bezüglich λ.

Bemerkung. $\operatorname{Eig}(\varphi, \lambda)$ ist ein Untervektorraum von V.

Satz 25.1.2 Sei $\varphi : V \to V$ eine lineare Abbildung und seien $v_1, \dots, v_k$ Eigenvektoren von φ mit den zugehörigen Eigenwerten $\lambda_1, \dots, \lambda_k$. Sind die Eigenwerte $\lambda_1, \dots, \lambda_k$ verschieden, dann sind die Vektoren $v_1, \dots, v_k$ linear unabhängig.

Definition 25.1.3 Seien $V_1, V_2, \dots, V_k$ Untervektorräume von V. Dann heißt die Summe $W = V_1 + \cdots + V_k$ *direkt*, falls jeder Vektor $v \in W$ eindeutig in der Form $v = v_1 + \cdots + v_k$ mit $v_i \in V_i$, $i = 1, \dots, k$, geschrieben werden kann.
Wenn die Summe direkt ist, bezeichnen wir sie als $V_1 \oplus \cdots \oplus V_k$ oder $\bigoplus\limits_{i=1}^{k} V_i$.

Satz 25.1.4 Seien $V_1, V_2, \dots, V_k$ Untervektorräume von V. Die folgenden Aussagen sind gleichwertig:

(1) Die Summe $V_1 + \cdots + V_k$ ist direkt.

(2) Aus $v_1 + \cdots + v_k = 0$ mit $v_1 \in V_1, \dots, v_k \in V_k$ folgt $v_1 = \cdots = v_k = 0$.

(3) Für alle $i = 1, \dots, k$ gilt $V_i \cap \sum\limits_{j \neq i} V_j = \{0\}$.

(4) $\dim(V_1 + \cdots + V_k) = \dim V_1 + \cdots + \dim V_k$.

Satz 25.1.5 Seien $\lambda_1, \dots, \lambda_k$ verschiedene Eigenwerte von φ. Dann ist die Summe $\operatorname{Eig}(\varphi, \lambda_1) + \ldots + \operatorname{Eig}(\varphi, \lambda_k)$ direkt.

Folgerung 25.1.6 Es gilt $\sum\limits_{i=1}^{k} \dim \operatorname{Eig}(\varphi, \lambda_i) \leqslant n$.

Definition 25.1.7 Eine Matrix $A \in M(n, n, K)$ heißt *diagonalisierbar*, wenn eine invertierbare Matrix $T \in M(n, n, K)$ existiert, so dass

$$T^{-1} \cdot A \cdot T = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Satz 25.1.8 Sei $A \in M(n,n,K)$. Dann sind die folgenden Aussagen gleichwertig:

(a) A ist diagonalisierbar.

(b) Es existieren n Eigenvektoren von A die eine Basis von K^n bilden.

(c) $\sum\limits_{\lambda \in \mathrm{EW}(A)} \dim \mathrm{Eig}(A,\lambda) = n$.

(d) $\bigoplus\limits_{\lambda \in \mathrm{EW}(A)} \mathrm{Eig}(A,\lambda) = K^n$.

Bemerkung: Falls (b) gilt und $t^{(1)}, \ldots, t^{(n)} \in K^n$ eine Basis aus Eigenvektoren von A ist, dann gilt

$$T^{-1} \cdot A \cdot T = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \text{ wobei } T = \begin{pmatrix} t^{(1)} & \ldots & t^{(n)} \end{pmatrix}$$

die Matrix mit den Spalten $t^{(1)}, \ldots, t^{(n)}$ ist und $\lambda_1, \ldots, \lambda_n$ die zugehörigen Eigenwerte sind.

26 Vorlesung

Definition 26.1.1 Seien $\{e_1, \ldots, e_n\}$ und $\{e'_1, \ldots, e'_n\}$ zwei Basen eines Vektorraumes V über K. Sei

$$\begin{aligned} e'_1 &= t_{11}e_1 + \cdots + t_{1n}e_n \\ &\ldots \\ e'_n &= t_{n1}e_1 + \cdots + t_{nn}e_n. \end{aligned}$$

Die Matrix $T = \begin{pmatrix} t_{11} & \ldots & t_{n1} \\ \vdots & \ddots & \vdots \\ t_{1n} & \ldots & t_{nn} \end{pmatrix}$ heißt *Übergangsmatrix* von e zu e'.

Satz 26.1.2 Seien $\{e_1, \ldots, e_n\}$ und $\{e'_1, \ldots, e'_n\}$ zwei Basen eines Vektorraumes V über K. Ist T die Übergangsmatrix von e zu e', dann ist T invertierbar und die Übergangsmatrix von e' zu e gleich T^{-1} ist.

Definition 26.1.3 Sei V ein K-Vektorraum, sei $\varphi : V \to V$ eine lineare Abbildung und sei $e = \{e_1, \ldots, e_n\}$ eine Basis von V. Wir stellen $\varphi(e_1), \ldots, \varphi(e_n)$ in der Basis $\{e_1, \ldots, e_n\}$ dar:

$$\begin{aligned} \varphi(e_1) &= a_{11}e_1 + \ldots + a_{1n}e_n \\ &\ldots \\ \varphi(e_n) &= a_{n1}e_1 + \ldots + a_{nn}e_n. \end{aligned}$$

Die Matrix $[\varphi]_e^e = \begin{pmatrix} a_{11} & \ldots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \ldots & a_{nn} \end{pmatrix}$ heißt die *Darstellungsmatrix* von φ bezüglich der Basis e.

Merkregel: In der i-ten **Spalte** der Darstellungsmatrix $[\varphi]_e^e$ stehen die Koeffizienten von $\varphi(e_i)$ bzgl. der Basis e.

Beispiele.

(1) Für $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + 2x_2 \\ 3x_1 + 4x_2 \end{pmatrix}$ und $e = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ ist
$$[\varphi]_e^e = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

(2) Für $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + 2x_2 \\ 3x_1 + 4x_2 \end{pmatrix}$ und $e' = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ ist
$$[\varphi]_{e'}^{e'} = \begin{pmatrix} -2 & -4 \\ 3 & 7 \end{pmatrix}.$$

Satz 26.1.4 Sei $\varphi : V \to V$ eine lineare Abbildung und seien $e = \{e_1, \dots, e_n\}$ und $e' = \{e'_1, \dots, e'_n\}$ zwei Basen von V. Dann gilt:
$$[\varphi]_{e'}^{e'} = T^{-1} \cdot [\varphi]_e^e \cdot T,$$
wobei T die Übergangsmatrix von e zu e' ist.

Satz 26.1.5 In der Situation von Definition 26.1.1 sei
$$v = x_1 e_1 + \ldots + x_n e_n = x'_1 e'_1 + \ldots + x'_n e'_n \in V.$$
Dann gilt für die Koordinatenvektoren
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = T \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}.$$

Zusatzinformation (wird nicht in der Klausur gefragt)

Definition 26.1.6 Seien U, V zwei K-Vektorräume, $\dim_K(U) = n$ und $\dim_K(V) = m$. Sei $B_1 = \{u_1, \dots, u_n\}$ eine Basis von U und $B_2 = \{v_1, \dots, v_m\}$ eine Basis von V. Sei $\varphi : U \to V$ eine lineare Abbildung. Wir stellen $\varphi(u_1), \dots, \varphi(u_n)$ in der Basis $\{v_1, \dots, v_m\}$ dar:
$$\begin{aligned} \varphi(u_1) &= a_{11} v_1 + \ldots + a_{1m} v_m \\ &\cdots \\ \varphi(u_n) &= a_{n1} v_1 + \ldots + a_{nm} v_m. \end{aligned}$$
Die Matrix $[\varphi]_{B_1}^{B_2} = \begin{pmatrix} a_{11} & \dots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1m} & \dots & a_{nm} \end{pmatrix}$ heißt die *Darstellungsmatrix* von φ bezüglich der Basen $B_1 \subseteq U$, $B_2 \subseteq V$.

Merkregel: In der i-ten **Spalte** der Darstellungsmatrix $[\varphi]_{B_1}^{B_2}$ stehen die Koeffizienten von φ(i-ter Vektor von B_1) bzgl. der Basis B_2.

Satz 26.1.7 Seien U, V, W drei Vektorräume über K mit den Basen $B_1 = \{u_1, \dots, u_n\}$, $B_2 = \{v_1, \dots, v_m\}$, $B_3 = \{w_1, \dots, w_k\}$ und seien $\varphi : U \to V$, $\psi : V \to W$ zwei lineare Abbildungen. Für die Darstellungsmatrix der linearen Abbildung $\psi \circ \varphi$ bezüglich der Basen B_1 und B_3 gilt dann
$$[\psi \circ \varphi]_{B_1}^{B_3} = [\psi]_{B_2}^{B_3} \cdot [\varphi]_{B_1}^{B_2}.$$