

# Lineare Algebra I

## Zusammenfassung

Patrick Dondl

7. März 2018

Die Algebra beschäftigt sich mit grundlegenden mathematischen Symbolen und Strukturen sowie den Eigenschaften der dazugehörigen Rechenoperationen. In der linearen Algebra liegt der Fokus auf linearen Abbildungen und linearen Räumen, sogenannten Vektorräumen.

## 0 Lineare Gleichungssysteme und der $\mathbb{R}^n$

In diesem Kapitel verwenden wir vorab elementare Begriffe aus der Mengenlehre. Weiters benutzen wir die reellen Zahlen, geschrieben  $\mathbb{R}$ , mit den bekannten Rechenregeln sowie die natürlichen Zahlen  $\mathbb{N} = \{1, 2, \dots\}$ .

### 0.1 Der $n$ -dimensionale reelle Raum

- Für gegebenes  $n \in \mathbb{N}$  bezeichnen wir mit

$$\mathbb{R}^n = \{x = (x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in \mathbb{R}\}$$

die Menge aller geordneten  $n$ -Tupel reeller Zahlen.

- Wir bezeichnen solche  $n$ -Tupel auch als Vektoren.
- Durch Definition von

$$x + y = (x_1 + y_1, \dots, x_n + y_n) \quad \text{für } x, y \in \mathbb{R}^n$$

und

$$\lambda x = (\lambda x_1, \dots, \lambda x_n) \quad \text{für } x \in \mathbb{R}^n, \lambda \in \mathbb{R}$$

können die Rechenregeln für Vektoren aus denen der reellen Zahlen abgeleitet werden.

- Als Nullvektor  $0$  in  $\mathbb{R}^n$  bezeichnen wir den Vektor, für den alle  $n$  Einträge Null sind.
- Der Sonderfall  $\mathbb{R}^0$  ist die Menge  $\{0\}$ , welche nur das Element  $0$  enthält.

## 0.2 Lineare Gleichungssysteme

- Seien  $m, n \in \mathbb{N}$ . Ein reelles, lineares Gleichungssystem mit  $m$  Gleichungen und  $n$  Unbekannten ist ein Ausdruck der Form

$$\begin{array}{cccccc} a_{1,1}x_1 & +a_{1,2}x_2 & +\dots & +a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & +a_{2,2}x_2 & +\dots & +a_{2,n}x_n & = & b_2 \\ \vdots & & & & & \\ a_{m,1}x_1 & +a_{m,2}x_2 & +\dots & +a_{m,n}x_n & = & b_m \end{array},$$

wobei  $b = (b_1, b_2, \dots, b_m)$  ein Vektor in  $\mathbb{R}^m$  und  $a_{i,j}$  für  $1 \leq i \leq m$ ,  $1 \leq j \leq n$  Zahlen in  $\mathbb{R}$  sind.

- Das Komma zwischen  $i$  und  $j$  in den  $a_{i,j}$  wird gerne auch weggelassen.
- Eine Lösung des obigen Gleichungssystems ist ein Vektor  $\xi = (\xi_1, \dots, \xi_n) \in \mathbb{R}^n$ , welcher, eingesetzt für  $x_j$ ,  $1 \leq j \leq n$ , das Gleichungssystem erfüllt.
- Als Lösungsmenge des Gleichungssystems bezeichnen wir die Menge aller Vektoren  $\xi$ , welche das Gleichungssystem erfüllen.
- Das obige Gleichungssystem lässt sich kurz schreiben als

$$\sum_{j=1}^n a_{i,j}x_j = b_i \quad \text{für } 1 \leq i \leq m.$$

- Noch kürzer ist die Matrixschreibweise

$$Ax = b,$$

wobei  $A$  als *Matrix* des Gleichungssystems bezeichnet wird. Der Vektor  $b$  heißt *rechte Seite* des Gleichungssystems.

- Falls  $m = n$ , so heißt das Gleichungssystem *quadratisch*, falls  $b$  der Nullvektor ist, so heißt das Gleichungssystem *homogen*.
- Wir sagen, dass ein Gleichungssystem (bzw. die dazugehörige Matrix) in *Normalform* ist, falls es die besondere Gestalt

$$\begin{array}{cccccc} x_1 & & +a_{1,k+1}x_{k+1} + \dots & +a_{1,n}x_n & = & b_1 \\ x_2 & & +a_{2,k+1}x_{k+1} + \dots & +a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & \vdots & & \vdots \\ x_k & & +a_{k,k+1}x_{k+1} + \dots & +a_{k,n}x_n & = & b_k \\ & & & 0 & = & b_{k+1} \\ & & & \vdots & & \vdots \\ & & & 0 & = & b_m, \end{array}$$

besitzt.

- Die ganze Zahl  $k$  bezeichnet man als *Rang* des Gleichungssystems. Es gilt  $0 \leq k \leq \min\{m, n\}$ .
- Die Lösungsmenge eines Gleichungssystems in Normalform lässt sich direkt ableiten:
  - Das Gleichungssystem besitzt genau dann eine Lösung, wenn gilt  $b_{k+1} = \dots = b_m = 0$ .
  - Um die Lösungsmenge zu bestimmen, kann man  $\xi_{k+1}, \dots, \xi_n$  beliebig vorgeben und wählt dann  $\xi_1, \dots, \xi_k$  so, dass gilt

$$\xi_i + \sum_{j=k+1}^n a_{i,j} \xi_j = b_i$$

für  $1 \leq i \leq k$ . Die Lösungsmenge ist damit gegeben durch die Menge

$$\left\{ \left( b_1 - \sum_{j=k+1}^n a_{1,j} \xi_j, \dots, b_k - \sum_{j=k+1}^n a_{k,j} \xi_j, \xi_{k+1}, \dots, \xi_n \right) : \xi_{k+1}, \dots, \xi_n \in \mathbb{R} \right\}$$

- Eine solche Menge, in der  $(n - k)$  Werte frei als Parameter gewählt werden können, heißt  $n$ -parametrig.
- Aus den vorhergehenden Überlegungen folgt unser erstes Lemma  
**Lemma 0.1.** *Eine Matrix in Normalform mit  $m$  Zeilen und  $n$  Spalten, sowie Rang  $k$ , sei gegeben. Dann gilt, dass  $k = n$  genau dann, wenn jedes Gleichungssystem, welches man mit dieser Matrix schreiben kann (d.h.  $Ax = b$  für beliebiges  $b$ ), höchstens eine Lösung besitzt. Weiters gilt, dass  $k = m$  wenn jedes Gleichungssystem, welches man mit dieser Matrix schreiben kann, mindestens eine Lösung besitzt.*

*Beweis.* Folgt aus Betrachtung der Lösungsmenge eines Gleichungssystems in Normalform. Für  $k = n$  kann *kein* Parameter frei vorgegeben werden. Für  $k = m$  ergibt sich keine Bedingung an die rechte Seite  $b$ .  $\square$

- Durch Anwendung von Zeilenoperationen können wir ein Gleichungssystem in ein neues Gleichungssystem überführen.
  - Mit  $Z_i^\lambda$ , wobei  $1 \leq i \leq m$ ,  $\lambda \in \mathbb{R}$ ,  $\lambda \neq 0$ , bezeichnen wir die Operation, bei der die  $i$ -te Zeile des Gleichungssystems mit der Zahl  $\lambda$  multipliziert wird.
  - Mit  $Z_{i,j}^\lambda$ , wobei  $1 \leq i \leq m$ ,  $1 \leq j \leq m$ ,  $\lambda \in \mathbb{R}$ , bezeichnen wir die Operation, bei der das  $\lambda$ -fache der  $i$ -ten Zeile zur  $j$ -ten Zeile hinzuaddiert wird.
  - Diese Zeilenoperationen sind umkehrbar, so ist z.B.  $Z_i^{\frac{1}{\lambda}}$  die Umkehrung von  $Z_i^\lambda$ .
- Aus der Umkehrbarkeit der Zeilenoperationen folgt

**Lemma 0.2.** Die Anwendung von Zeilenoperationen ändert die Lösungsmenge eines linearen Gleichungssystems nicht.

- Dieser Satz (und der dazugehörige Beweis mittels expliziter Konstruktion) ermöglicht die Bestimmung der Lösungsmenge von linearen Gleichungssystemen.

**Satz 0.3.** Jedes lineare Gleichungssystem (bzw. jede Matrix) lässt sich durch die Anwendung von Zeilenoperationen und Vertauschung von Variablen (d.h., Vertauschung von Spalten in der dazugehörigen Matrix) in Normalform überführen.

**Korollar 0.4.** Sei  $A$  eine Matrix mit  $m$  Zeilen und  $n$  Spalten,  $k$  sei der Rang einer Normalform von  $A$ , welche durch Zeilenoperationen und Spaltentausch aus  $A$  entstanden ist. Dann besitzt jedes Gleichungssystem der Form  $Ax = b$  (d.h., jedes lineare Gleichungssystem mit Matrix  $A$ ) entweder keine Lösung oder ein  $n - k$ -parametrisches System von Lösungen. Es gilt  $k = m$  genau dann, wenn jedes Gleichungssystem der Form  $Ax = b$  (mindestens) eine Lösung besitzt. Es gilt  $k = n$  genau dann, wenn jedes Gleichungssystem der Form  $Ax = b$  höchstens eine Lösung besitzt.

**Korollar 0.5.** Jedes homogene lineare Gleichungssystem mit weniger Zeilen als Spalten besitzt mindestens eine nichttriviale (d.h. von Null verschiedene) Lösung. *Bemerkung.* Ein homogenes lineares Gleichungssystem besitzt immer die triviale Lösung  $\xi_1 = \xi_2 = \dots = \xi_n = 0$ .

- Der Begriff der linearen Unabhängigkeit ist zentral in der linearen Algebra.

**Definition 0.6.** Eine Kollektion  $a_1, a_2, \dots, a_n$  von Vektoren in  $\mathbb{R}^m$  heißt *linear unabhängig*, wenn sich keiner der Vektoren als Linearkombination (d.h. als mit reellen Zahlen gewichtete Summe) der anderen Vektoren schreiben lässt.

**Lemma 0.7.** Die Vektoren  $a_1, a_2, \dots, a_n$  sind genau dann linear unabhängig wenn für alle  $\xi_1, \dots, \xi_n \in \mathbb{R}$  gilt, dass aus

$$0 = \xi_1 a_1 + \xi_2 a_2 + \dots + \xi_n a_n$$

schon folgt, dass

$$\xi_1 = \xi_2 = \dots = \xi_n = 0.$$

*Bemerkung.* Ein einzelner Vektor  $a$  ist linear unabhängig, falls  $a \neq 0$ . Die leere Kollektion von Vektoren ( $n = 0$ ) betrachten wir als linear unabhängig.

**Lemma 0.8.** Es seien  $a_1, a_2, \dots, a_n$  linear unabhängige Vektoren und es gelte  $b = \sum_{j=1}^n \lambda_j a_j$ . Dann ist diese Darstellung von  $b$  als Linearkombination der Vektoren  $a_1, a_2, \dots, a_n$  eindeutig.

- Mit den folgenden Aussagen lassen sich gewisse Invarianten von linearen Gleichungssystemen definieren.

**Satz 0.9.** Wenn ein lineares Gleichungssystem durch Zeilenoperationen und Spaltentausch in Normalform gebracht wurde, so erhält man immer denselben Rang.

*Bemerkung.* Damit lässt sich der Rang als Eigenschaft eines Gleichungssystems (oder einer Matrix) definieren.

**Korollar 0.10.** *Wird ein lineares Gleichungssystem nur durch Zeilenoperationen (also ohne Variablentausch) auf Normalform gebracht, so ist die resultierende Matrix eindeutig. Falls das lineare Gleichungssystem lösbar ist, so ist in diesem Fall auch die rechte Seite der Normalform eindeutig bestimmt.*

## 0.3 Elementare Euklidische Geometrie

### 0.3.1 Geraden und Ebenen

- Im Sinne der Geometrie bezeichnen wir in diesem Abschnitt Vektoren in  $\mathbb{R}^n$  auch als Punkte in  $\mathbb{R}^n$ .

- Wir betrachten zunächst Geraden.

**Definition 0.11.** Es sei  $v \neq 0$  ein Vektor in  $\mathbb{R}^n$ . Wir bezeichnen mit  $\mathbb{R}v$  die Menge

$$\mathbb{R}v = \{x \in \mathbb{R}^n : \text{es existiert } \lambda \in \mathbb{R} \text{ mit } x = \lambda v\}$$

**Definition 0.12.** Es seien  $a, v$  Vektoren in  $\mathbb{R}^n$  mit  $v \neq 0$ . Eine Gerade  $g$  im  $\mathbb{R}^n$  ist eine Menge der Form

$$g = \{x \in \mathbb{R}^n : \text{es existiert } \lambda \in \mathbb{R} \text{ mit } x = a + \lambda v\} = a + \mathbb{R}v.$$

Die Menge  $\mathbb{R}v$  heißt in diesem Fall der Richtungsraum von  $g$ .

- Eine Gerade kann auf unterschiedliche Weise dargestellt werden.

**Lemma 0.13.** *Zwei Geraden  $a + \mathbb{R}v$  und  $b + \mathbb{R}w$  sind genau dann gleich (d.h. die Mengen bestehen aus den gleichen Punkten), wenn  $\mathbb{R}v = \mathbb{R}w$  und  $a - b \in \mathbb{R}v$ .*

**Lemma 0.14.** *Durch zwei verschiedene Punkte in  $\mathbb{R}^n$  geht genau eine Gerade.*

**Definition 0.15.** Zwei Geraden heißen parallel, wenn sie die gleichen Richtungsräume haben.

- In ähnlicher Weise lassen sich Ebenen im  $\mathbb{R}^n$  betrachten.

**Definition 0.16.** Es seien  $v$  und  $w$  linear unabhängige Vektoren in  $\mathbb{R}^n$ . Eine affine Ebene  $E$  ist eine Menge der Form  $a + \mathbb{R}v + \mathbb{R}w$ .

**Lemma 0.17.** *Zwei nicht parallele Geraden, die in einer Ebene liegen, schneiden sich.*

### 0.3.2 Das Skalarprodukt in $\mathbb{R}^n$

- Das Skalarprodukt wird sich als sehr nützlich erweisen, um beispielsweise Winkel zwischen Vektoren zu definieren.

**Definition 0.18.** Es seien  $x = (x_1, \dots, x_n)$ ,  $y = (y_1, \dots, y_n)$  Vektoren in  $\mathbb{R}^n$ . Als Skalarprodukt zwischen  $x$  und  $y$  bezeichnen wir den Ausdruck

$$(x, y) = \sum_{j=1}^n x_j y_j$$

**Lemma 0.19.** Das Skalarprodukt in  $\mathbb{R}^n$  ist eine symmetrische, positiv definite Bilinearform, das heißt

1.  $(\lambda x, y) = \lambda(x, y)$ ,
2.  $(x + y, z) = (x, z) + (y, z)$ ,
3.  $(x, y) = (y, x)$ ,
4.  $(x, x) \geq 0$ ,
5.  $(x, x) = 0$  genau dann wenn  $x = 0$ .

*Bemerkung.* Es folgt auch, dass gilt  $(x, \lambda y) = \lambda(x, y)$  und  $(x, y + z) = (x, y) + (x, z)$ .

**Definition 0.20.** Als Länge (oder Norm) eines Vektors  $x$  in  $\mathbb{R}^n$  bezeichnen wir den Ausdruck

$$\|x\| = \sqrt{(x, x)}.$$

**Definition 0.21.** Es seien  $x \neq 0, y \neq 0$  Vektoren in  $\mathbb{R}^n$ . Als Winkel zwischen diesen Vektoren bezeichnen wir die Zahl  $\alpha, 0 \leq \alpha \leq \pi$ , für die gilt

$$\cos \alpha = \frac{(x, y)}{\|x\| \|y\|}$$

- Damit diese Definition Sinn ergibt, benötigen wir eine Abschätzung (nachdem der Kosinus ja nur Werte zwischen  $-1$  und  $1$  annimmt).

**Lemma 0.22** (Cauchy-Schwarz'sche Ungleichung). *Es gilt  $(x, y) \leq \|x\| \|y\|$ .*

**Lemma 0.23** (Dreiecksungleichung). *Es gilt  $\|x + y\| \leq \|x\| + \|y\|$ .*

**Korollar 0.24.** *Es seien  $x, y$  Vektoren in  $\mathbb{R}^n$ . Der Ausdruck*

$$d(x, y) = \|x - y\|$$

*definiert eine Metrik (oder einen Abstand), das heißt*

1.  $d(x, y) \geq 0$ ,
2.  $d(x, y) = 0$  genau dann wenn  $x = y$ ,
3.  $d(x, y) = d(y, x)$ ,
4.  $d(x, z) \leq d(x, y) + d(y, z)$ .

## 1 Grundlegende Strukturen

### 1.1 Etwas elementare Aussagenlogik

- Als Aussage im Mathematischen Sinne bezeichnen wir ein sprachliches Gebilde, dem entweder der Wahrheitswert wahr ( $w$ ) oder falsch ( $f$ ) zugeordnet werden kann.
- Mittels einer Wahrheitstabelle lassen sich Aussagen gut darstellen.

	Aussage	wahr/falsch
A	„Es sind mehr als 10 Personen im Rundbau“	w
B	„Es sind weniger als 20 Personen im Rundbau“	f

- Aus gegebenen Aussagen lassen sich neue Aussagen generieren.

**Definition 1.1.**  $A, B$  seien Aussagen.

1. Nicht  $A$ , („ $\neg A$ “) ist die Negation von  $A$ .

$A$	$\neg A$
$w$	$f$
$f$	$w$

2.  $A$  oder  $B$  („ $A \vee B$ “) ist wahr genau dann wenn mindestens eine der Aussagen  $A, B$  wahr ist.  $A$  und  $B$  („ $A \wedge B$ “) ist wahr genau dann, wenn beide Aussagen  $A, B$  wahr sind.

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

3. Aus  $A$  folgt  $B$  („ $A \Rightarrow B$ “) ist wahr, genau dann wenn die Aussage  $A$  die Aussage  $B$  impliziert.  $A$  ist äquivalent zu  $B$  („ $A \Leftrightarrow B$ “) ist wahr, genau dann wenn die Aussage  $A$  die Aussage  $B$  impliziert und die Aussage  $B$  die Aussage  $A$  impliziert.

*Bemerkung.* Um  $A \Rightarrow B$  zu zeigen, kann man annehmen, dass  $A$  wahr ist und muss dann  $B$  folgern.

## 1.2 Mengen und Abbildungen

- Die Frage, was eigentlich genau eine Menge ist, ist schwer zu beantworten. Wir begnügen uns damit, die Existenz einiger bestimmter Mengen anzunehmen und daraus neue Mengen zu generieren.
- Endliche Mengen lassen sich durch Aufzählung ihrer Elemente beschreiben, wir schreiben  $A = \{1, 3, 15, 32\}$ , als die Menge, welche die Zahlen 1, 3, 15 und 32 als Elemente enthält. Wir schreiben  $1 \in A$  für „Die Menge  $A$  enthält das Element 1“.
- Die Reihenfolge der Aufzählung von Elementen ist irrelevant, ebenso werden wiederholte Elemente in der Aufzählung ignoriert. Die Anzahl paarweise verschiedener Elemente einer Menge ist die Mächtigkeit einer Menge.
- Eine wichtige Menge ist die leere Menge  $\emptyset$ , welche keine Elemente enthält.
- Mengen können auch weitere Mengen als Elemente enthalten, beispielsweise ist  $A = \{1, \{1, 3\}, 2\}$  die Menge, welche als Elemente die Zahlen 1 und 2, sowie eine Menge mit den Zahlen 1 und 3 enthält.
- Manche Mengen enthalten alle Elemente einer anderen Menge, man spricht dann von Teilmengen.

- Definition 1.2.**
1. Es seien  $A, B$  Mengen.  $A$  ist eine Teilmenge von  $B$ , falls jedes Element in  $A$  auch in  $B$  enthalten ist. Wir schreiben  $A \subset B$ .
  2. Es gilt  $A = B$ , falls  $A \subset B$  und  $B \subset A$ .
  3. Falls  $A \neq B$ , aber  $A \subset B$ , so sprechen wir von einer echten Teilmenge und schreiben gegebenenfalls  $A \subsetneq B$ .

- Wir nehmen an, dass eine unendliche Menge  $\mathbb{N}$ , die Menge der natürlichen Zahlen,

$$\mathbb{N} = \{1, 2, 3, \dots\},$$

mit den üblichen Rechenregeln existiert, welche die folgende Eigenschaft („Induktionsprinzip“) besitzt:

Sei  $M \subset \mathbb{N}$  und es gelte

1.  $1 \in M$ ,
2. Falls  $n \in M$  so gilt auch  $n + 1 \in M$ .

Dann gilt bereits  $M = \mathbb{N}$ .

- Durch Erweiterung von Zahlbereichen lassen sich aus  $\mathbb{N}$  auch die Mengen der ganzen Zahlen  $\mathbb{Z}$ , der rationalen Zahlen  $\mathbb{Q}$  und der reellen Zahlen  $\mathbb{R}$ , sowie der komplexen Zahlen  $\mathbb{C}$  erzeugen.
- Es sei  $M$  eine Menge, und  $E$  eine Eigenschaft, von der für jedes Element in  $M$  überprüft werden kann, ob die Eigenschaft für dieses Element zutrifft. Man kann nun aus  $M$  eine Teilmenge mit den Elementen erzeugen, welche die Eigenschaft  $E$  besitzen. Wir schreiben

$$X = \{x \in M : x \text{ besitzt die Eigenschaft } E\}$$

- Aus gegebenen Mengen lassen sich neue Mengen erzeugen.

**Definition 1.3.**  $X$  und  $Y$  seien Mengen.

1. Die Vereinigung  $X \cup Y$  ist die Menge der Elemente, welche in  $X$  oder in  $Y$  (oder in beiden) sind.
2. Der Schnitt  $X \cap Y$  ist die Menge der Elemente, welche sowohl in  $X$  als auch in  $Y$  sind.
3. Falls  $X \subset Y$ , so ist die Differenzmenge  $Y \setminus X$  die Menge der Elemente, welche in  $Y$  aber nicht in  $X$  enthalten sind.
4. Das kartesische Produkt  $X \times Y$  ist die Menge der geordneten Tupel aus Elementen in  $X$  und in  $Y$ ,  $X \times Y = \{(x, y) : x \in X, y \in Y\}$ .

*Bemerkung.* · Der bereits bekannte euklidische Raum  $\mathbb{R}^2$  ist nichts anderes als das kartesische Produkt von  $\mathbb{R}$  mit sich selbst, also  $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ .

- Diese Operationen lassen sich auch mehrmals nacheinander ausführen. Im Fall des kartesischen Produktes verkürzen wir  $((x_1, x_2), x_3)$  zu  $(x_1, x_2, x_3)$ .



- Abbildungen können Beziehungen zwischen Mengen darstellen.

**Definition 1.4.**  $X$  und  $Y$  seien Mengen. Eine Abbildung  $f$  von  $X$  nach  $Y$  ist eine Vorschrift, die jedem Element  $x$  in  $X$  genau ein Element  $f(x)$  in  $Y$  zuordnet. Wir schreiben

$$f: X \rightarrow Y, \quad x \mapsto f(x).$$

**Definition 1.5.** Zwei Abbildungen  $f: X \rightarrow Y$  und  $g: X \rightarrow Y$  heißen gleich, falls gilt  $f(x) = g(x)$  für alle  $x \in X$ .

- Mittels Abbildungen können auch (Teil-)Mengen transportiert werden.

**Definition 1.6.** Es seien  $X, Y$  Mengen,  $f: X \rightarrow Y$  eine Abbildung. Weiters sei  $N \subset X$ ,  $M \subset Y$ .

1.  $f(N) = \{y \in Y : \text{es existiert ein } x \in N \text{ mit } y = f(x)\} \subset Y$ , das Bild von  $N$ ,
2.  $f^{-1}(M) = \{x \in X : f(x) \in M\}$ , das Urbild von  $M$ .

- Besonders wichtige Arten von Abbildungen bekommen Namen.

**Definition 1.7.** Es seien  $X, Y$  Mengen,  $f: X \rightarrow Y$  eine Abbildung.

1. Die Abbildung  $f$  heißt injektiv, falls für  $x, \hat{x}$  aus  $X$  mit  $f(x) = f(\hat{x})$  schon folgt, dass  $x = \hat{x}$ .
2. Die Abbildung  $f$  heißt surjektiv, falls gilt  $f(X) = Y$ .
3. Die Abbildung  $f$  heißt bijektiv, falls sie sowohl injektiv als auch surjektiv ist.

*Bemerkung.* Für bijektive Abbildungen  $f: X \rightarrow Y$  gilt, dass die Menge  $f^{-1}(\{y\})$  mit  $y \in Y$  immer genau ein Element enthält. Wir definieren dann eine Abbildung  $f^{-1}: Y \rightarrow X$ , wobei  $f^{-1}(y) = x$ , so dass  $y = f(x)$ .

**Satz 1.8.** Sei  $X$  eine endliche Menge,  $f: X \rightarrow X$  ein (Selbst-)abbildung der Menge  $X$ . Dann sind die folgenden Aussagen äquivalent:

1.  $f$  ist injektiv,
2.  $f$  ist surjektiv,
3.  $f$  ist bijektiv.

- Man kann Abbildungen auch nacheinander ausführen.

**Definition 1.9.** Es seien  $X, Y$  und  $Z$  Mengen,  $f: X \rightarrow Y$  und  $g: Y \rightarrow Z$  Abbildungen. Dann definiert

$$g \circ f: X \rightarrow Z \quad x \mapsto (g \circ f)(x) = g(f(x))$$

eine neue Abbildung, die Komposition von  $f$  und  $g$ .

*Bemerkung.* Die Komposition ist assoziativ, aber nicht kommutativ.

**Definition 1.10.** Die Abbildung

$$\text{Id}_X: X \rightarrow X, \quad x \mapsto x$$

heißt Identitätsabbildung auf  $X$ .

**Lemma 1.11.** *Es seien  $X$  und  $Y$  nichtleere Mengen,  $f: X \rightarrow Y$  eine Abbildung. Dann gilt*

1.  *$f$  ist genau dann injektiv, wenn eine Abbildung  $g: Y \rightarrow X$  existiert mit  $g \circ f = \text{Id}_X$ ,*
2.  *$f$  ist genau dann surjektiv, wenn eine Abbildung  $g: Y \rightarrow X$  existiert mit  $f \circ g = \text{Id}_Y$ ,*
3.  *$f$  ist genau dann bijektiv, wenn eine Abbildung  $g: Y \rightarrow X$  existiert mit  $g \circ f = \text{Id}_X$  und  $f \circ g = \text{Id}_Y$ . In diesem Fall gilt  $g = f^{-1}$ .*

– Das kartesische Produkt haben wir bereits kennen gelernt. Es ist nützlich zur Definition einer Reihe anderer Strukturen und Objekte.

**Definition 1.12.** Es sei  $f: X \rightarrow Y$  eine Abbildung,  $X, Y$  Mengen. Der Graph von  $f$  ist die Menge

$$\Gamma_f = \{(x, f(x)) \text{ für } x \in X\} \subset X \times Y.$$

–

**Definition 1.13.** Seien  $X, Y$  Mengen. Mit  $\text{Abb}(X, Y)$  bezeichnen wir die Menge aller Abbildungen von  $X$  nach  $Y$ .

*Bemerkung.* Alle surjektiven Abbildungen von  $X$  nach  $Y$  lassen sich nun beispielsweise schreiben als  $\{f \in \text{Abb}(X, Y) : f \text{ surjektiv}\}$ .

**Definition 1.14.** Es seien  $X, Y$  Mengen. Wir sagen  $X$  besitzt die selbe Mächtigkeit wie  $Y$ , falls eine bijektive Abbildung von  $X$  nach  $Y$  existiert.

*Bemerkung.* Für endliche Mengen gilt  $\#X = n$  genau dann wenn  $X$  gleichmächtig wie  $\{1, 2, \dots, n\}$ .

**Definition 1.15.** Mit  $2^X$  bezeichnen wir die Potenzmenge von  $X$ , d.h. die Menge aller Teilmengen von  $X$ .

**Satz 1.16.** *Es sei  $M$  eine endliche Menge,  $\#M = n$  mit  $n \in \mathbb{N} \cup \{0\}$ . Dann gilt  $\#2^M = 2^n$ .*

*Beweis.* Mittels Induktion. □

– Das kartesische Produkt zweier Mengen ist nützlich, um zum Beispiel den Graphen einer Funktion zu definieren.

**Definition 1.17.** Es sei  $f: X \rightarrow Y$  eine Funktion. Als Graph von  $f$  bezeichnen wir die Menge

$$\Gamma_f = \{(x, f(x)) \in X \times Y\}.$$

– Insbesondere wichtig sind Relationen zwischen Elementen einer Menge.

**Definition 1.18.** Eine Teilmenge  $R \subset X \times X$  bezeichnen wir als Relation und schreiben

$$x \sim y \text{ falls } (x, y) \in R.$$

Wir sagen dann, dass  $x$  in Relation steht mit  $y$ .

**Definition 1.19.** Eine Relation auf  $X$  heißt Äquivalenzrelation, falls gilt

1.  $x \sim x$  „Reflexivität“,
2.  $x \sim y \Rightarrow y \sim x$  „Symmetrie“,
3.  $x \sim y$  und  $y \sim z \Rightarrow x \sim z$  „Transitivität“,

für alle  $x, y, z \in X$ .

**Definition 1.20.** Es sei  $X$  eine Menge mit Äquivalenzrelation  $\sim$ . Eine Menge  $A \subset X$  heißt Äquivalenzklasse, falls gilt

1.  $A \neq \emptyset$ ,
2.  $x, y \in A \Rightarrow x \sim y$ ,
3.  $x \in A, y \in X, x \sim y \Rightarrow y \in A$ .

**Proposition 1.21.** Es sei  $X$  eine Menge mit Äquivalenzrelation  $\sim$ . Dann gehört jedes Element  $a \in X$  zu genau einer Äquivalenzklasse. Insbesondere sind zwei Äquivalenzklassen entweder gleich oder disjunkt.

### 1.3 Gruppen

- Eine Verknüpfung ist ein mathematisches Objekt, das elementare Rechenoperationen verallgemeinert.

**Definition 1.22.** Es sei  $G$  eine Menge. Eine Verknüpfung ist eine Abbildung

$$*: G \times G \rightarrow G \quad *: (a, b) \mapsto *(a, b).$$

*Bemerkung.* Wir schreiben üblicherweise  $a * b$  für  $*(a, b)$ , eventuell auch  $a \cdot b$  oder  $ab$ .

**Definition 1.23.** Es sei  $G$  eine Menge,  $*$  eine Verknüpfung auf  $G$ .  $(G, *)$  heißt Gruppe, falls gilt

1.  $(a * b) * c = a * (b * c)$  (Assoziativgesetz),
2. Es existiert ein  $e \in G$ , so dass
  - a)  $e * a = a$  für alle  $a \in G$ ,
  - b) zu jedem  $a \in G$  existiert  $a' \in G$  mit  $a' * a = e$ .

*Bemerkung.*  $e$  wird neutrales Element der Gruppe genannt,  $a'$  inverses Element zu  $a$ .

**Definition 1.24.** Eine Gruppe  $(G, *)$  heißt abelsch, falls die Verknüpfung kommutiert, d.h.  $a * b = b * a$  für alle  $a, b \in G$ .

**Proposition 1.25.** Es sei  $(G, *)$  eine Gruppe. Dann gilt

- Das neutrale Element  $e$  ist eindeutig bestimmt und es gilt auch  $a * e = a$  für alle  $a \in G$ ,
- Das inverse Element  $a'$  zu  $a$  ist für jedes  $a \in G$  eindeutig bestimmt und es gilt auch  $a * a' = e$  für alle  $a \in G$ .

*Bemerkung.* 1. Das Inverse zu  $a$  bezeichnen wir als  $a^{-1}$ . Es gilt

$$a^{-1} * a = a * a^{-1} = e, \quad (a^{-1})^{-1} = a, \quad (a * b)^{-1} = b^{-1} * a^{-1}$$

2. Es gilt

$$a * \tilde{x} = a * x \Rightarrow \tilde{x} = x \text{ und } \tilde{y} * a = y * a \Rightarrow \tilde{y} = y.$$

**Definition 1.26.** Es sei  $(G, *)$  eine Gruppe,  $a \in G$ . Als Rechts- bzw. Linkstranslation bezeichnen wir die Abbildungen

$$\begin{aligned}\tau_a: G &\rightarrow G, x \mapsto x * a, \\ {}_a\tau: G &\rightarrow G, x \mapsto a * x.\end{aligned}$$

**Lemma 1.27.** *Es sei  $(G, *)$ . Dann sind die Abbildungen  $\tau_a$  und  ${}_a\tau$  für jedes  $a \in G$  bijektiv. Sei andererseits  $G$  eine Menge mit assoziativer Verknüpfung  $*$ . Falls sowohl  $\tau_a$  als auch  ${}_a\tau$  surjektiv sind, so ist  $(G, *)$  bereits eine Gruppe.*

**Definition 1.28.** Es sei  $(G, *)$  eine Gruppe,  $G' \subset G$ .  $G'$  heißt Untergruppe von  $G$ , falls gilt

$$a, b \in G' \Rightarrow a * b \in G' \text{ und } a^{-1} \in G'.$$

**Definition 1.29.** Es seien  $(G, \cdot)$ ,  $(H, \odot)$  Gruppen. Eine Abbildung  $\phi: G \rightarrow H$  heißt (Gruppen-)Homomorphismus, falls gilt

$$\phi(a \cdot b) = \phi(a) \odot \phi(b) \quad \text{für alle } a, b \in G.$$

*Bemerkung.* Ein bijektiver Homomorphismus heißt Isomorphismus.

**Proposition 1.30.** *Es sei  $(G, *)$  eine Gruppe  $G'$  eine Untergruppe. Dann gilt  $(G', *)$  ist eine Gruppe.*

**Proposition 1.31.** *Es seien  $(G, \cdot)$ ,  $(H, \odot)$  Gruppen. Die Abbildung  $\phi: G \rightarrow H$  sei ein Homomorphismus. Dann gilt*

1.  $\phi(e) = e'$  mit neutralen Elementen  $e \in G$ ,  $e' \in H$ ,
2.  $\phi(a^{-1}) = \phi(a)^{-1}$  für alle  $a \in G$ ,

3. *Ist  $\phi$  ein Isomorphismus, so ist auch  $\phi^{-1}: H \rightarrow G$  ein Isomorphismus.*

*Beispiel.* Wir betrachten die Gruppe  $(\mathbb{Z}, +)$ . Es sei  $m \in \mathbb{N}$ . Dann ist  $(m\mathbb{Z}, +)$  mit  $m\mathbb{Z} = \{m \cdot a : a \in \mathbb{Z}\}$  eine Untergruppe. Für  $r \in \{0, 1, \dots, m-1\}$  schreiben wir  $r + m\mathbb{Z} = \{r + m \cdot a : a \in \mathbb{Z}\}$ , die Restklassen modulo  $m$ . Jedes  $a \in \mathbb{Z}$  gehört genau zu einer solchen Restklasse (Division mit Rest!), die Menge der Restklassen bezeichnen wir mit  $\mathbb{Z}/m\mathbb{Z}$ . Wir schreiben  $a \equiv b \pmod{m}$  falls  $a$  und  $b$  zur selben Restklasse gehören. Es sei  $\bar{a}$  die zu  $a$  gehörige Restklasse. Auf diesen Restklassen definieren wir nun eine Addition  $\bar{a} + \bar{b} = \overline{a + b}$ .

*Proposition.* *Diese Addition ist Wohldefiniert, das heißt das Ergebnis hängt nicht von der Wahl der jeweiligen Repräsentanten ab.*

*Satz.* *Die Restklassen modulo  $m$  bilden eine abelsche Gruppe. Die Abbildung*

$$\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, \quad a \mapsto a + m\mathbb{Z}$$

*ist ein surjektiver Homomorphismus.*

## 1.4 Ringe und Körper

– Wir benötigen auch eine Struktur für Mengen mit zwei Verknüpfungen.

**Definition 1.32.** Es sei  $R$  eine Menge mit den Verknüpfungen

$$\begin{aligned} +: R \times R &\rightarrow R, & +(a, b) &\mapsto a + b, \\ \cdot: R \times R &\rightarrow R, & \cdot(a, b) &\mapsto a \cdot b. \end{aligned}$$

$(R, +, \cdot)$  heißt Ring, falls gilt

1.  $(R, +)$  ist eine abelsche Gruppe,
2. die Multiplikation  $\cdot$  ist assoziativ,
3. es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

*Bemerkung.* Ein Ring heißt kommutativ, falls die Multiplikation kommutiert. Das neutrale Element der Addition in einem Ring bezeichnen wir als Nullelement  $0$ . Falls ein Element  $1 \in R$  existiert, mit  $1 \cdot a = a \cdot 1 = a$  für jedes  $a \in R$ , so bezeichnen wir dieses als Einselement.

**Proposition 1.33.** *Es sei  $(R, +, \cdot)$  ein Ring mit Nullelement  $0$ . Dann gilt für jedes  $a \in R$*

$$0 \cdot a = a \cdot 0 = 0.$$

**Definition 1.34.** 1. Es sei  $(R, +, \cdot)$  ein Ring und  $R' \subset R$ .  $R'$  heißt Unterring, falls  $R'$  eine Untergruppe bezüglich der Addition ist, und gilt  $a \cdot b \in R'$  für alle  $a, b \in R'$ .

2. Es seien  $(R, +, \cdot)$  und  $(S, \oplus, \odot)$  Ringe. Eine Abbildung  $\phi: R \rightarrow S$  heißt (Ring-)Homomorphismus, wenn für alle  $a, b \in R$  gilt  $\phi(a + b) = \phi(a) \oplus \phi(b)$  und  $\phi(a \cdot b) = \phi(a) \odot \phi(b)$ .

**Definition 1.35.** Eine Menge  $K$  mit zwei Verknüpfungen  $+: K \times K \rightarrow K$  und  $\cdot: K \times K \rightarrow K$  heißt Körper, wenn gilt

1.  $(K, +)$  ist eine abelsche Gruppe (mit neutralem Element  $0$  und inversem Element  $-a$  zu  $a$ ).
2. Es sei  $K^* = K \setminus \{0\}$ . Dann gilt, dass  $a \cdot b \in K^*$  für alle  $a, b \in K^*$  und  $(K^*, \cdot)$  ist eine abelsche Gruppe (mit neutralem Element  $1$  und inversem Element  $\frac{1}{a}$  zu  $a$ ).
3. Es gelten die Distributivgesetze  $a \cdot (b + c) = a \cdot b + a \cdot c$  und  $(a + b) \cdot c = a \cdot c + b \cdot c$ .

**Proposition 1.36.** *In einem Körper gelten die folgenden Rechenregeln:*

- $1 \neq 0$ ,
- $0 \cdot a = a \cdot 0 = 0$ ,
- $a \cdot b = 0 \Rightarrow a = 0$  oder  $b = 0$ ,
- $a \cdot (-b) = -(a \cdot b)$  und  $(-a) \cdot (-b) = a \cdot b$ ,

$$\cdot \quad x \cdot a = \tilde{x} \cdot a \text{ für } a \in K^* \Rightarrow x = \tilde{x}.$$

*Beispiel.* 1.  $\mathbb{R}$  und  $\mathbb{Q}$  mit der üblichen Addition und Multiplikation sind Körper.

2. Die komplexen Zahlen  $\mathbb{C}$  sind ein Körper.

**Definition 1.37.** Ein Ring  $(R, +, \cdot)$  heißt nullteilerfrei, falls für alle  $a, b \in R$  gilt  $a \cdot b = 0 \Rightarrow a = 0$  oder  $b = 0$ .

**Satz 1.38.** Der Restklassenring  $Z/m\mathbb{Z}$  ist genau dann nullteilerfrei, wenn  $m$  eine Primzahl ist.

*Bemerkung.* Jeder Körper ist ein abelscher nullteilerfreier Ring.

**Satz 1.39.** Ein nullteilerfreier, kommutativer Ring  $K$  mit endlich vielen Elementen und Eins ist ein Körper.

*Bemerkung.* Es sei  $R$  ein Ring. Für  $n \in \mathbb{N}$  und  $x \in R$  schreiben wir  $n \cdot x = x + x + \dots + x$  ( $n$ -mal).

**Definition 1.40.** Es sei  $R$  ein Ring mit Einselement 1 (ein unitärer Ring). Die Charakteristik von  $R$  ist definiert durch

$$\chi(R) = \begin{cases} 0 & \text{falls } n \cdot 1 \neq 0 \text{ für alle } n \in \mathbb{N}. \\ \min\{n \in \mathbb{N} : n \cdot 1 = 0\} & \text{sonst.} \end{cases}$$

**Lemma 1.41.** Es sei  $K$  ein Körper. Dann ist  $\chi(K)$  entweder Null oder eine Primzahl.

## 2 Vektorräume

### 2.1 Definition und grundlegende Eigenschaften

- Wir haben bereits den  $\mathbb{R}^n$  kennengelernt und werden nun diese Struktur verallgemeinern.

**Definition 2.1.** Es sei  $K$  ein Körper und  $(V, +)$  eine abelsche Gruppe. Weiters sei eine Abbildung

$$\begin{aligned} K \times V &\rightarrow V \\ (\lambda, v) &\mapsto \lambda v \end{aligned}$$

gegeben, so dass gilt

$$\begin{aligned} \lambda(x + y) &= \lambda x + \lambda y, & (\lambda + \mu)x &= (\lambda x) + (\mu x) \\ \lambda(\mu x) &= (\lambda\mu)x, & 1x &= x \end{aligned}$$

für alle  $x, y \in V, \lambda, \mu \in K$ . Dann heißt  $(V, +)$  zusammen mit der definierten Abbildung  $K$ -Vektorraum.

*Bemerkung.* 1. Die oben definierte Abbildung heißt Skalarmultiplikation, Elemente aus  $K$  heißen Skalare, Elemente aus  $V$  heißen Vektoren,

2. Das neutrale Element  $0 \in V$  heißt Nullvektor,

3. Das inverse Element zu  $x \in V$  wird mit  $-x$  bezeichnet.

4. Ist nur ein Ring  $R$  gegeben, der Rest von Definition 2.1 aber erfüllt, so heißt  $V$  Links- $R$ -Modul (bzw. Rechts- $R$ -Modul bei Skalarmultiplikation von rechts).

**Lemma 2.2.** *Es sei  $V$  ein  $K$ -Vektorraum. Dann gilt*

1.  $0x = 0, \lambda 0 = 0$  für alle  $x \in V, \lambda \in K,$
2.  $\lambda x = 0 \Rightarrow \lambda = 0$  oder  $x = 0,$
3.  $(-1)x = -x$

für alle  $\lambda \in K, x \in V.$

**Definition 2.3.** Es sei  $V$  ein  $K$ -Vektorraum,  $W \subset V$  heißt Untervektorraum, wenn gilt

1.  $W \neq \emptyset,$
2.  $x + y \in W$  für alle  $x, y \in W,$
3.  $\lambda x \in W$  für alle  $\lambda \in K, x \in W.$

**Proposition 2.4.** *Jeder Untervektorraum ist ein Vektorraum (mit der Einschränkung der jeweiligen Abbildungen auf die Teilmenge).*

- Wir betrachten die Frage, welche Vektorräume wir aus einer gegebenen Menge von Vektoren erzeugen können.

*Bemerkung.* Es sei  $I$  eine Menge (eine sogenannte Indexmenge) und  $M_a$  für jedes  $a \in I$  wieder eine Menge. Wir schreiben

1.  $\bigcup_{a \in I} M_a = \{x : x \in M_a \text{ für ein } a \in I\},$
2.  $\bigcap_{a \in I} M_a = \{x : x \in M_a \text{ für alle } a \in I\}$

**Lemma 2.5.** *Es sei  $V$  ein  $K$ -Vektorraum,  $I$  eine Indexmenge, und  $W_a$  sei ein Untervektorraum von  $V$  für jedes  $a \in I.$  Dann gilt*

1.  $W = \bigcap_{a \in I} W_a$  ist ein Untervektorraum von  $V,$
2.  $\tilde{W} = W_a \cup W_b$  ist ein Untervektorraum für  $a, b \in I \Rightarrow W_a \subset W_b$  oder  $W_b \subset W_a.$

**Definition 2.6.** Es sei  $V$  ein  $K$ -Vektorraum,  $E \subset V.$

1. Es sei  $\lambda_e \in K$  für jedes  $e \in E,$  so dass nur für endlich viele  $\lambda_e$  gilt  $\lambda_e \neq 0.$  Dann ist

$$\sum_{e \in E} \lambda_e e = \sum_{e \in E \text{ mit } \lambda_e \neq 0} \lambda_e e \in V$$

eine Linearkombination der  $e \in E.$

2.  $x \in V$  heißt darstellbar als Linearkombination der  $e \in E$  falls  $\lambda_e \in K,$  mit nur endlich vielen  $\lambda_e \neq 0$  existieren mit  $x = \sum_{e \in E} \lambda_e e.$
3. Wir schreiben

$$\text{span}(E) = \{x \in V : x \text{ ist als Linearkombination der } e \in E \text{ darstellbar}\}.$$

Falls  $W = \text{span}(E),$  so heißt  $E$  Erzeugendensystem von  $W.$

4. Eine Menge  $W \subset V$  heißt endlich erzeugt, falls ein Erzeugendensystem von  $W$  mit nur endlich vielen Elementen existiert.

**Lemma 2.7.** *Es sei  $V$  ein  $K$ -Vektorraum und  $E \subset V$ . Dann gilt*

1.  $\text{span}(E)$  ist ein Untervektorraum von  $V$ ,
2. Falls  $W \subset V$  ein Untervektorraum ist und  $E \subset W$ , so gilt  $\text{span}(E) \subset W$ .

## 2.2 Basis und Dimension

- Wir wollen Vektorräume aus möglichst kleinen Mengen von Vektoren erzeugen. In diesem Abschnitt ist immer  $K$  ein Körper  $V$  ein Vektorraum über  $K$ .

**Definition 2.8.**  $X$  und  $I$  seien Mengen, und für  $j \in I$  sei  $e_j \in X$ . Dann wird die Abbildung  $I \rightarrow X, j \mapsto e_j$  als Familie von  $e_j \in X$  bezeichnet. Wir schreiben  $(e_j)_{j \in I} \in X^I = \text{Abb}(I, X)$ .

**Definition 2.9.** Es sei  $I$  eine Menge und  $(v_i)_{i \in I}$  eine Familie von Vektoren in  $V$ .

1.  $(v_i)_{i \in I}$  heißt minimales Erzeugendensystem von  $V$ , wenn  $E = \{v_i : i \in I\}$  ein Erzeugendensystem von  $V$  ist und gilt

$$J \subsetneq I \Rightarrow \text{span}\{v_j : j \in J\} \neq V.$$

2.  $(v_i)_{i \in I}$  heißt linear unabhängig, falls gilt: Der Nullvektor ist Linearkombination von Vektoren in  $E = \{v_i : i \in I\}$ , so sind alle Koeffizienten Null.

Nicht linear unabhängige Familien von Vektoren bezeichnen wir als linear abhängig.

*Bemerkung.* Die leere Familie von Vektoren gilt als linear unabhängig.

- Wie in Abschnitt 0 charakterisieren wir linear unabhängige Mengen von Vektoren weiter.

**Lemma 2.10.** *Es sei  $(v_i)_{i \in I}$  eine Familie von Vektoren in  $V$ . Dann gilt:*

1. Falls  $v_j = 0$  für ein  $j \in I$ , so ist  $(v_i)_{i \in I}$  linear abhängig.
2. Falls  $i, j \in I$  existieren mit  $i \neq j, v_i = v_j$ , so ist  $(v_i)_{i \in I}$  linear abhängig.
3. Einelementige Familien von Vektoren sind genau dann linear unabhängig, falls der enthaltene Vektor nicht der Nullvektor ist.
4. Falls  $(v_i)_{i \in I}$  linear unabhängig ist und  $J \subset I$ , so ist  $(v_j)_{j \in J}$  linear unabhängig.
5. Es sei  $I \neq \emptyset$ . Dann gilt  $(v_i)_{i \in I}$  ist linear abhängig genau dann, wenn sich einer der enthaltenen Vektoren als Linearkombination der anderen schreiben lässt.

**Satz 2.11.** *Für eine Familie  $(v_i)_{i \in I}$  von Vektoren in  $V$  sind die folgenden Aussagen äquivalent:*

1.  $(v_i)_{i \in I}$  ist ein minimales Erzeugendensystem von  $V$ .
2.  $(v_i)_{i \in I}$  ist ein linear unabhängiges Erzeugendensystem von  $V$ .



3. Jedes  $v \in V$  hat eine eindeutig bestimmte Darstellung als Linearkombination der Vektoren  $(v_i)_{i \in I}$ .

4.  $(v_i)_{i \in I}$  ist eine maximale linear unabhängige Familie, d.h. für jedes  $w \in V$  gilt  $(w, (v_i)_{i \in I})$  ist linear abhängig.

**Definition 2.12.** Eine Familie  $(v_i)_{i \in I}$  heißt Basis von  $V$ , falls  $(v_i)_{i \in I}$  ein linear unabhängiges Erzeugendensystem von  $V$  ist.

– Wie kann man eine Basis eines Vektorraumes bestimmen?

**Satz 2.13** (Basisauswahlsatz). *Es sei  $N \in \mathbb{N}$ ,  $v_1, \dots, v_N \in V$  und  $V = \text{span}(\{v_1, \dots, v_N\})$ . Dann existieren  $n \in \mathbb{N}$ ,  $i_1, \dots, i_n \in \{1, \dots, N\}$  so dass  $(v_{i_1}, \dots, v_{i_n})$  eine Basis von  $V$  bilden.*

**Lemma 2.14.**  $(v_1, \dots, v_n)$  sei eine Basis von  $V$ , und  $w = \lambda_1 v_1 + \dots + \lambda_n v_n$  mit  $\lambda_a \neq 0$  für ein  $a \in \{1, \dots, n\}$ . Dann ist  $(v_1, \dots, v_{a-1}, w, v_{a+1}, \dots, v_n)$  ebenfalls eine Basis von  $V$ .

**Satz 2.15** (Basisaustauschsatz von Steinitz). *Es sei  $(v_1, \dots, v_n)$  eine Basis von  $V$  und  $(w_1, \dots, w_m)$  eine linear unabhängige Familie von Vektoren in  $V$ . Dann gilt:*

1.  $m \leq n$ .
2. Nach einer geeigneten Umnummerierung von  $(v_1, \dots, v_n)$  ist  $(w_1, \dots, w_m, v_{m+1}, \dots, v_n)$  eine Basis von  $V$ .

**Korollar 2.16.**  $V$  besitze eine Basis aus  $n$  Vektoren. Dann hat jede Basis von  $V$  genau  $n$  Vektoren.

**Definition 2.17.** Wir schreiben

$$\dim_K(V) = \begin{cases} \infty & \text{falls } V \text{ nicht endlich erzeugt ist,} \\ n & \text{falls } V \text{ eine Basis aus } n \text{ Vektoren besitzt.} \end{cases}$$

$\dim_K(V)$  wird als Dimension von  $V$  bezeichnet.

**Satz 2.18** (Basisergänzungssatz von Steinitz).  *$V$  sei ein endlich erzeugter Vektorraum, und  $(w_i)_{i \in I}$  eine Familie linear unabhängiger Vektoren. Dann existiert eine Basis, welche alle Vektoren aus  $(w_i)_{i \in I}$  enthält. Insbesondere besitzt jeder endlich erzeugte Vektorraum eine Basis.*

**Lemma 2.19.** *Es sei  $\dim_K(V) = n < \infty$ . Dann ist jede linear unabhängige Familie von  $n$  Vektoren eine Basis von  $V$ . Weiters gilt, dass die Dimension eines Untervektorraumes von  $V$  nicht größer sein kann, als die Dimension von  $V$  selbst.*

**Satz.** *Jeder Vektorraum besitzt eine Basis.*

## 3 Lineare Abbildungen

### 3.1 Definition und grundlegende Eigenschaften

– Im Folgenden sei  $K$  ein Körper und  $V$  ein Vektorraum über  $K$ .

–

**Definition 3.1.**  $V$  und  $W$  seien  $K$ -Vektorräume.

1. Eine Abbildung  $F: V \rightarrow W$  heißt ( $K$ )-linear (bzw. Vektorraum-Homomorphismus), falls gilt
  - a)  $F(x + y) = F(x) + F(y)$  für alle  $x, y \in V$ ,
  - b)  $F(\lambda x) = \lambda F(x)$  für alle  $x \in V, \lambda \in K$ .

Wir schreiben in diesem Fall  $F \in \text{Hom}_K(V, W) \subset \text{Abb}(V, W)$ .

2. Falls gilt  $V = W$ , dann heißt  $F$  Vektorraum-Endomorphismus und wir schreiben  $F \in \text{End}_K(V) = \text{Hom}(V, V)$ .
3. Ein bijektiver Vektorraum-Homomorphismus heißt Vektorraum-Isomorphismus. Falls ein solcher von  $V$  nach  $W$  existiert, heißt  $V$  isomorph zu  $W$  und wir schreiben  $V \cong W$ .
4. Falls  $F$  ein bijektiver Vektorraum-Endomorphismus ist, so heißt  $F$  Vektorraum-Automorphismus und wir schreiben  $F \in \text{Aut}_K(V) \subset \text{End}(V)$ .

*Bemerkung.* 1.  $\text{Hom}_K(V, W) \subset \text{Abb}(V, W)$  ist ein Untervektorraum.

2.  $\text{End}_K(V)$  besitzt außerdem die Struktur eines Ringes (mit der Vektoraddition induziert von  $\text{Abb}(V, W)$  und der Nacheinanderausführung als Multiplikation). Weiters gilt die Kompatibilitätsbedingung  $(\lambda F) \circ G = \lambda(F \circ G) = F \circ (\lambda G)$ . Eine solches Objekt heißt  $K$ -Algebra.
3.  $\text{Aut}_K(V)$  ist eine Gruppe (bzgl. der Nacheinanderausführung als Multiplikation), aber kein Vektorraum.

**Lemma 3.2.**  $U, V, W$  seien  $K$ -Vektorräume,  $F \in \text{Hom}_K(V, W), G \in \text{Hom}_K(U, V)$ . Dann gilt

1.  $F(0) = 0$ ,
2.  $F(x - y) = F(x) - F(y)$ ,
3.  $F \circ G \in \text{Hom}_K(U, W)$ ,
4. Falls  $F$  ein Vektorraum-Isomorphismus ist, so gilt  $F^{-1} \in \text{Hom}_K(W, V)$ ,
5. Es sei  $(v_i)_{i \in I}$  eine Familie linear abhängiger Vektoren. Dann ist auch  $(F(v_i))_{i \in I}$  linear abhängig.
6.
  - a) Falls  $\tilde{V} \subset V$  ein Untervektorraum ist, so ist auch  $F(\tilde{V}) \subset W$  ein Untervektorraum, insbesondere ist  $\text{Im}(F) = F(V)$  ein Untervektorraum,
  - b) Falls  $\tilde{W} \subset W$  ein Untervektorraum ist, so ist auch  $F^{-1}(\tilde{W}) \subset V$  ein Untervektorraum, insbesondere ist  $\text{Ker}(F) = F^{-1}(\{0\})$  ein Untervektorraum,
  - c) Falls  $F$  ein Vektorraum-Isomorphismus ist, so gilt  $F(\tilde{V}) \cong \tilde{V}$  für jeden Untervektorraum  $\tilde{V}$  von  $V$ .
7.  $\dim_K(\text{Im}(F)) \leq \dim_K(V)$ .

**Satz 3.3.**  $V, W$  seien  $K$ -Vektorräume,  $I$  eine Indexmenge und  $(v_i)_{i \in I}$  sei eine Basis von  $V$ . Weiters sei  $(w_i)_{i \in I}$  eine Familie von Vektoren in  $W$ . Dann existiert genau eine  $K$ -lineare Abbildung  $F: V \rightarrow W$ , so dass  $F(v_i) = w_i$  für alle  $i \in I$ . Dieses  $F$  erfüllt weiters

1.  $\text{Im}(F) = \text{span}\{w_i : i \in I\}$ ,
2.  $F$  injektiv  $\Leftrightarrow (w_i)_{i \in I}$  linear unabhängig.

**Proposition 3.4.** *Es gilt  $G \in \text{Hom}_K(V, W)$  injektiv  $\Leftrightarrow \ker(G) = \{0\}$ .*

**Korollar 3.5.** *Es sei  $V$  ein  $K$ -Vektorraum mit  $\dim_K(V) = n < \infty$ . Dann gilt:  $V \cong K^n$ . Weiters gilt für jeden  $K$ -Vektorraum  $W$  mit  $\dim_K(W) = n$ , dass  $V \cong W$ .*

– Die Vektorräume  $\text{Im}(F)$  und  $\ker(F)$  sind eine weitere Betrachtung wert.

**Definition 3.6.** Zu  $F \in \text{Hom}_K(V, W)$  heißt  $\text{rg}(F) = \dim_K(F(V))$  der Rang von  $F$ .

**Satz 3.7** (Dimensionsformel). *Es sei  $F \in \text{Hom}_K(V, W)$ ,  $\dim_K(V) < \infty$ . Dann gilt*

$$\dim_K(V) = \dim_K(\ker(F)) + \text{rg}(F).$$

**Definition 3.8.**  $V$  sei ein  $K$ -Vektorraum,  $V_1, V_2$  Untervektorräume.

1.  $V_1 + V_2 = \text{span}(V_1 \cup V_2)$
2. Wir schreiben  $W = V_1 \oplus V_2$ , falls  $W = V_1 + V_2$  und  $V_1 \cap V_2 = \emptyset$ . In diesem Fall heißt  $W$  direkte Summe von  $V_1$  und  $V_2$ .  $V_1$  und  $V_2$  heißen dann komplementäre Untervektorräume von  $V$ .

**Satz 3.9.** *Es gilt*

$$\dim_K(V_1 + V_2) = \dim_K(V_1) + \dim_K(V_2) - \dim_K(V_1 \cap V_2).$$

**Satz 3.10.** *Es sei  $V$  ein  $K$ -Vektorraum,  $W \subset V$  ein Untervektorraum. Wir schreiben für  $x, y \in V$ , dass  $x \sim y$  wenn  $x - y \in W$ . Dann gilt*

1.  $\sim$  ist eine Äquivalenzrelation,
2. Auf  $\bar{V} = V / \sim$  existiert eine eindeutige Vektorraumstruktur, so dass die Quotientenabbildung  $p: V \rightarrow \bar{V}$ ,  $p: x \mapsto [x]$  ein Homomorphismus ist.

**Definition 3.11.**  $\bar{V}$  mit der Vektorraumstruktur aus dem obigen Satz heißt Quotientenvektorraum  $V/W$ .

**Satz 3.12** (Homomorphiesatz).  *$V$  und  $W$  seien  $K$ -Vektorräume,  $F \in \text{Hom}_K(V, W)$ . Dann existiert genau eine lineare Abbildung*

$$\bar{F}: V / \ker(F) \rightarrow \text{im}(F)$$

mit  $F(x) = (\bar{F} \circ p)(x)$  für alle  $x \in V$ , wobei  $p$  die Quotientenabbildung  $V \rightarrow V / \ker(F)$  darstellt. Die Abbildung  $\bar{F}$  ist ein Isomorphismus.

**Satz 3.13** (Isomorphiesätze). *Es seien  $V$  ein  $K$ -Vektorraum,  $V_1, V_2 \subset V$  Untervektorräume. Dann gilt*

$$(V_1 + V_2) / V_1 \cong V_2 / (V_1 \cap V_2)$$

und, falls  $V_1 \subset V_2 \subset V$ ,

$$(V / V_1) / (V_2 / V_1) \cong V / V_2$$

## 4 Matrizen

- Wir kennen lineare Gleichungssysteme und Matrizen im Reellen bereits aus Kapitel 0. Hier werden wir diese Aussagen verallgemeinern.

**Definition 4.1.** 1. Es sei  $X$  eine Menge,  $m, n \in \mathbb{N}$ . Dann heißt ein rechteckiges Schema

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

mit  $a_{ij} \in X$  eine  $(m \times n)$ -Matrix. Wir schreiben  $A = (a_{ij})$ .

2. Die  $a_{ij}$  heißen Einträge (oder Komponenten) von  $A$ .

3.  $(a_{i1} \ a_{i2} \ \dots \ a_{in})$  heißt  $i$ -te Zeile von  $A$ ,  $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$  heißt  $j$ -te Spalte von  $A$ .

4. Die Menge aller  $(m \times n)$ -Matrizen mit Einträgen aus  $X$  bezeichnen wir mit  $\text{Mat}_X(m \times n)$ .

- Matrizen mit Einträgen aus einem Körper  $K$  sind natürlich besonders wichtig.

**Satz 4.2.**  $\text{Mat}_K(m \times n)$  besitzt die Struktur eines  $K$ -Vektorraumes und es gilt

$$K^{mn} \cong \text{Mat}_K(m \times n) \cong \text{Hom}_K(K^n, K^m).$$

*Bemerkung.* Die Spaltenvektoren von  $A$  sind die Bilder der Standardbasisvektoren der  $K^n$ .

*Bemerkung.* Mit Matrizen über einem Körper  $K$  lässt sich nun genauso rechnen, wie im Kapitel 0 bereits im Reellen besprochen. Die bekannte Matrixmultiplikation entspricht einer Hintereinanderausführung von linearen Abbildungen. Ebenso lassen sich nun lineare Gleichungssysteme  $Ax = b$  in  $K^n$  ebenso wie in Kapitel 0 lösen. Dank der Isomorphie aus Satz 4.2 übertragen sich auch sämtliche Dimensionsformeln auf das Rechnen mit Matrizen.

**Definition 4.3.** 1. Es sei  $A = (a_{ij}) \in \text{Mat}_K(m \times n)$ . Mit  $A^\top \in \text{Mat}_K(n \times m)$  bezeichnen wir die transponierte Matrix mit Einträgen  $(a_{ij}^\top) = (a_{ji})$ .

2. Die zur Identitätsabbildung  $\text{Id}: K^n \rightarrow K^n$  gehörige Matrix

$$E_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \text{ heißt Einheitsmatrix.}$$

3.  $A \in \text{Mat}_K(n \times n)$  heißt invertierbar, falls eine Matrix  $A^{-1} \in \text{Mat}_K(n \times n)$  existiert mit  $A^{-1}A = E_n$ .

*Bemerkung.* Die Zeilenoperationen  $Z_j^\lambda$  und  $Z_{ij}^\lambda$  aus Kapitel 0 lassen sich durch Matrizen darstellen (welche von links an eine Matrix  $A$  multipliziert werden).

- Nachdem alle  $n$ -dimensionalen  $K$ -Vektorräume isomorph zu  $K^n$  sind, lassen sich (nach Wahl einer Basis) beliebige lineare Abbildungen zwischen endlichdimensionalen Vektorräumen als Matrizen darstellen.

**Definition 4.4.** Es sei  $W$  ein  $K$ -Vektorraum und  $m, n \in \mathbb{N}$ . Dann schreiben wir

$$W^{\{1, \dots, m\}} \times \text{Mat}_K(m \times n) \rightarrow W^{\{1, \dots, n\}}$$

$$(w_1, \dots, w_m) \times (a_{ij}) \mapsto \left( \sum_{i=1}^n a_{i1} w_1, \dots, \sum_{i=1}^n a_{im} w_m \right)$$

oder kurz

$$(\mathcal{B}, A) \mapsto \mathcal{B} \cdot A,$$

mit  $\mathcal{B} = (w_1, \dots, w_m) \in W^{\{1, \dots, m\}}$ ,  $A = (a_{ij}) \in \text{Mat}(m \times n)$ .

**Definition 4.5.** Es seien  $V, W$   $K$ -Vektorräume mit jeweiligen Basen  $\mathcal{A} = (v_1, \dots, v_n)$  beziehungsweise  $\mathcal{B} = (w_1, \dots, w_m)$ .

1. Für  $F \in \text{Hom}_K(V, W)$  mit  $F(v_j) = \sum_{i=1}^m a_{ij} w_i$ ,  $j = 1, \dots, n$ ,  $(a_{ij}) \in K$  bezeichnet  $M(\mathcal{B}, F, \mathcal{A}) = (a_{ij}) \in \text{Mat}_K(m \times n)$  die darstellende Matrix von  $F$  bezüglich  $\mathcal{B}$  und  $\mathcal{A}$ . Wir schreiben

$$F(\mathcal{A}) = \mathcal{B} \cdot M(\mathcal{B}, F, \mathcal{A}).$$

2. Im Falle  $V = W$ ,  $F = \text{Id} \in \text{End}_K(W)$  heißt  $M(\mathcal{B}, \mathcal{A}) = M(\mathcal{B}, \text{Id}, \mathcal{A})$  Basiswechselmatrix von  $\mathcal{A}$  nach  $\mathcal{B}$ .

*Bemerkung.* 1. Wieder sind die Spalten von  $M(\mathcal{B}, F, \mathcal{A})$  die Bilder der Basisvektoren von  $V$ , kodiert durch die Koeffizienten wenn diese Bilder in der Basis  $\mathcal{B}$  ausgedrückt werden.

2. Wir kennen die bei gegebenen Basen  $\mathcal{A}$  und  $\mathcal{B}$  festgelegten kanonischen Isomorphismen  $I_{\mathcal{A}}: V \rightarrow K^n$  bzw.  $I_{\mathcal{B}}: W \rightarrow K^m$ . Es gilt nun der wichtige Zusammenhang

$$I_{\mathcal{B}} \circ F \circ I_{\mathcal{A}}^{-1} = F_{M(\mathcal{B}, F, \mathcal{A})}.$$

3. Damit folgt auch, dass gilt

$$M(\mathcal{E}^{(m)}, F_{\mathcal{A}}, \mathcal{E}^{(n)}) = A,$$

wobei  $\mathcal{E}^{(m)}$  und  $\mathcal{E}^{(n)}$  die Standardbasen des  $K^m$  bzw.  $K^n$  bezeichnen. Unsere Notation ist also konsistent: Die darstellende Matrix einer durch eine Matrix  $A$  beschriebenen Abbildung  $F_A: K^n \rightarrow K^m$  ist wieder  $A$ .

**Satz 4.6.** Es seien  $V, W$   $K$ -Vektorräume mit jeweiligen Basen  $\mathcal{A} = (v_1, \dots, v_n)$  beziehungsweise  $\mathcal{B} = (w_1, \dots, w_m)$  und es sei  $F \in \text{Hom}_K(V, W)$ . Dann gilt für  $x \in K^n = \text{Mat}_K(n \times 1)$ , dass

$$F(\mathcal{A} \cdot x) = \mathcal{B} \cdot M(\mathcal{B}, F, \mathcal{A}) \cdot x.$$

**Korollar 4.7.** *Es seien  $V$  ein  $K$ -Vektorräume mit Basen  $\mathcal{A} = (v_1, \dots, v_n)$  und  $\tilde{\mathcal{A}} = (\tilde{v}_1, \dots, \tilde{v}_n)$ ,  $W$  ein  $K$ -Vektorräume mit Basen  $\mathcal{B} = (w_1, \dots, w_m)$  und  $\tilde{\mathcal{B}} = (\tilde{w}_1, \dots, \tilde{w}_m)$ ,  $F \in \text{Hom}_K(V, W)$ . Dann gilt*

$$M(\tilde{\mathcal{B}}, F, \tilde{\mathcal{A}}) = M(\tilde{\mathcal{B}}, \mathcal{B}) \cdot M(\mathcal{B}, F, \mathcal{A}) \cdot M(\mathcal{A}, \tilde{\mathcal{A}})$$

*Bemerkung.* 1. Basiswechselmatrizen sind immer invertierbar.

2. Sämtliche Ergebnisse für das Rechnen mit Matrizen lassen sich nun auf  $\text{Hom}_K(V, W)$  übertragen (solange  $V$  und  $W$  endlichdimensional sind).
3. Insbesondere lassen sich für gegebenes  $F \in \text{Hom}_K(V, W)$  immer Basen  $\mathcal{A}$  und  $\mathcal{B}$  von  $V$  und  $W$  finden, so dass gilt

$$M(\mathcal{B}, F, \mathcal{A}) = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & & & & & \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$

wobei die Einheitsmatrix in der oberen linken Ecke die Größe  $r \times r$  besitzt mit  $r = \text{rg}(F)$ .

## 5 Dualräume

- In diesem Abschnitt betrachten wir die linearen Abbildungen von einem  $K$ -Vektorraum  $V$  in dessen Grundkörper  $K$ .

**Definition 5.1.** 1.  $V^* = \text{Hom}_K(V, K)$  heißt Dualraum von  $V$ . Die Elemente von  $V^*$  heißen Linearformen.

2. Falls  $\mathcal{A} = (v_1, \dots, v_n)$  eine Basis von  $V$  ist, so heißt  $(v_1^*, \dots, v_n^*)$  mit  $v_j^* \in V^*$ , so dass

$$v_j^*(v_i) = \delta_{ji} = \begin{cases} 1 & \text{falls } j = i, \\ 0 & \text{sonst,} \end{cases}$$

die zu  $\mathcal{A}$  duale Basis.

**Satz 5.2.** *Es sei  $V$  ein endlichdimensionaler Vektorraum über  $K$ . Dann gilt*

1. *Zu jeder Basis von  $V$  gibt es eine eindeutig bestimmte duale Basis, welche eine Basis von  $V^*$  bildet.*
2.  *$V$  und  $V^*$  sind isomorph, insbesondere gilt also  $\dim_K(V) = \dim_K(V^*)$ .*

**Korollar 5.3.**  *$V$  sei ein  $K$ -Vektorraum. Dann existiert zu jedem  $x \neq 0 \in V$  ein  $\alpha \in V^*$  mit  $\alpha(x) \neq 0$ .*

- Wir betrachten nun, welche linearen Abbildungen auf Dualräumen von linearen Abbildungen auf Vektorräumen induziert werden

**Satz 5.4.** *Es seien  $V, W$   $K$ -Vektorräume,  $F \in \text{Hom}_K(V, W)$ ,  $\alpha \in W^*$ . Wir schreiben  $F^\top(\alpha) = \alpha \circ F$ . Dann gilt*

1.  $F^\top(\alpha) \in V^*$ ,  $F^\top \in \text{Hom}_K(W^*, V^*)$ ,
2.  $F \mapsto F^\top$  ist ein injektiver Homomorphismus  $\text{Hom}_K(V, W) \rightarrow \text{Hom}_K(W^*, V^*)$ ,
3. Falls  $V$  und  $W$  endlichdimensional sind, ist  $F \mapsto F^\top$  ein Vektorraum-Isomorphismus.

**Definition 5.5.** Die in Satz 5.4. eingeführte Abbildung  $F^\top$  heißt die zu  $F$  transponierte (oder duale) Abbildung.

*Bemerkung.* Wir erinnern uns an die transponierte Matrix.

**Satz 5.6.** *Es sei  $V$  ein  $K$ -Vektorraum mit Basis  $\mathcal{A}$ ,  $W$  ein  $K$ -Vektorraum mit Basis  $\mathcal{B}$  und  $F \in \text{Hom}_K(V, W)$ . Dann gilt*

$$M(\mathcal{B}, F, \mathcal{A})^\top = M(\mathcal{A}^*, F^\top, \mathcal{B}^*).$$

*Bemerkung.* Mit  $\mathcal{A}^*$  bezeichnen wir die zu  $\mathcal{A}$  duale Basis.

- Es bleibt noch die Frage zu beantworten, was eine zweimalige Transposition bewirkt.

**Satz 5.7.**  *$V$  und  $W$  seien  $K$ -Vektorräume. Dann gilt*

1. Die Abbildung  $V \rightarrow (V^*)^*$ ,  $x \mapsto x^{\top\top}$  mit  $x^{\top\top}(\alpha) = \alpha(x)$  für  $x \in V$ ,  $\alpha \in V^*$  ist ein injektiver Homomorphismus. Man nennt diesen die kanonische Injektion in den Bidualraum.
2. Im Fall  $\dim_K(V) < \infty$  ist der Homomorphismus aus 1. ein Isomorphismus.
3. Es sei  $F \in \text{Hom}_K(V, W)$ . Wir schreiben  $F^{\top\top} = (F^\top)^\top$  und es gilt

$$(F(x))^{\top\top} = F^{\top\top}(x^{\top\top}).$$

## 6 Determinanten

### 6.1 Permutationen und deren Signatur

- Wir betrachten in diesem Unterabschnitt Permutationen, das sind bijektive Selbstabbildungen endlicher Mengen.

**Definition 6.1.** Die Gruppe der bijektiven Selbstabbildungen einer endlichen Menge  $X$  bezeichnen wir mit  $\text{Sym}(X)$ .

**Definition 6.2.** Es sei  $X$  eine endliche Menge,  $s: X^2 \rightarrow \{-1, 0, 1\}$  eine Orientierung, d.h.  $s(x, y) = 0$  falls  $x = y$  und  $s(x, y) \in \{-1, 1\}$  für  $x \neq y$  mit  $s(x, y) = -s(y, x)$ .

Es sei nun  $\pi \in \text{Sym}(X)$ . Wir schreiben

$$\text{sign}(\pi) = \prod \frac{s(\pi x, \pi y)}{s(x, y)},$$

wobei das Produkt über alle ungeordneten Paare in  $X$  genommen wird, d.h. alle möglichen zweielementigen Teilmengen  $\{x, y\}$  von  $X$  mit  $x \neq y$ .

*Bemerkung.* Die Signatur einer Permutation ist unabhängig von der ursprünglichen Wahl der Orientierungsabbildung. Man sieht, dass nur die Anzahl der ungeordneten Paaren entscheidend ist, deren Orientierung von  $\pi$  geändert wird. Solche Paare nennt man Fehlstände von  $\pi$ .

**Definition** (Alternative Variante von Definition 6.2).

$$\text{sign}(\pi) = (-1)^{\text{Anzahl Fehlstände von } \pi}.$$

**Satz 6.3.** *Die Signaturabbildung*

$$\text{sign}: \text{Sym}(X) \rightarrow \{-1, 1\}$$

*ist ein Gruppenhomomorphismus.*

*Bemerkung.* Es sei  $(x_1, \dots, x_k) \in X^{\{1, \dots, k\}}$  eine Familie paarweise verschiedener Elemente aus  $X$ . Die Abbildung  $\pi \in \text{Sym}(X)$ , welche  $x_i$  auf  $x_{i+1}$  für  $1 \leq i < k$ ,  $x_k$  auf  $x_1$  und alle anderen Elemente auf sich selbst abbildet wird als Zyklus von  $(x_1, \dots, x_k)$  bezeichnet. Man berechnet leicht, dass ein solcher Zyklus die Signatur  $(-1)^{k-1}$  besitzt.

**Satz 6.4.** *Jede Permutation lässt sich (bis auf die Reihenfolge) eindeutig als Produkt von disjunkten Zyklen schreiben.*

**Korollar 6.5.** *Jede Permutation ist Produkt von Transpositionen, das sind Zyklen der Länge 2.*

**Satz 6.6.** *sign ist der einzige nicht-triviale Homomorphismus  $\text{Sym}(X) \rightarrow \{-1, 1\}$ .*

## 6.2 $k$ -Formen

**Definition 6.7.** Es sei  $V$  ein  $K$ -Vektorraum. Eine Abbildung  $\mu: V^k \rightarrow K$  heißt  $k$ -stellige multilineare Abbildung (oder Multilinearform), falls  $\mu$  linear in jedem Argument ist, d.h.

$$\mu(x_1, \dots, \lambda x_j + y_j, \dots, x_k) = \lambda \mu(x_1, \dots, x_j, \dots, x_k) + \mu(x_1, \dots, y_j, \dots, x_k).$$

für  $x_i \in V$ ,  $i = 1, \dots, k$ ,  $y_j \in V$ ,  $\lambda \in K$ .

**Definition 6.8.** Eine  $k$ -stellige multilineare Abbildung  $\mu: V^k \rightarrow K$  heißt alternierend oder  $k$ -Form, wenn sie die zwei folgenden (äquivalenten) Bedingungen erfüllt:

1.  $\mu(x_1, \dots, x_k) = 0$ , falls ein Vektor zweimal vorkommt.
2.  $\mu(x_1, \dots, x_j + \lambda x_i, \dots, x_k) = \mu(x_1, \dots, x_j, \dots, x_k)$  für  $1 \leq i \neq j \leq k$ .

**Lemma 6.9.** *Eine Multilinearform  $\mu$  ist genau dann alternierend, wenn  $\mu(x_1, \dots, x_k) = 0$  für alle linear abhängigen Familien von Vektoren  $(x_j)$ .*

**Lemma 6.10.** *Seien  $U$  und  $V$   $K$ -Vektorräume. Dann gilt*

1. *Jede Linearkombination von  $k$ -Formen auf  $V$  ist wieder eine  $k$ -Form.*



2. Sei  $F : V \rightarrow U$  eine lineare Abbildung und  $\mu$  eine  $k$ -Form auf  $U$ . Dann ist  $\mu^F$ , definiert durch

$$\mu^F(a_1, \dots, a_k) = \mu(F(a_1), \dots, F(a_k))$$

eine  $k$ -Form auf  $V$ .

**Lemma 6.11.** Sei  $\mu$  eine  $k$ -Form auf  $V$ . Dann ist für alle  $x_1, \dots, x_k \in V$  und alle  $1 \leq i < j \leq k$

$$\mu(x_1, \dots, x_i, \dots, x_j, \dots, x_k) = -\mu(x_1, \dots, x_j, \dots, x_i, \dots, x_k)$$

*Bemerkung.* Falls  $K$  ein Körper mit Charakteristik ungleich 2 ist, so ist jede Multilinearform mit der Eigenschaft aus dem vorangegangenen Lemma automatisch auch eine  $k$ -Form. Im Fall  $\chi(K) = 2$  gilt aber  $1 + 1 = 0$ , somit  $1 = -1$  und es folgt aus der Eigenschaft  $\mu(x_1, \dots, x_i, \dots, x_i, \dots, x_k) = -\mu(x_1, \dots, x_i, \dots, x_i, \dots, x_k)$  nicht, dass  $\mu(x_1, \dots, x_i, \dots, x_i, \dots, x_k) = 0$ .

**Lemma 6.12.** Sei  $\mu : V^k \rightarrow K$  eine  $k$ -Form,  $x_1, \dots, x_k \in V$  und  $\tau \in \text{Abb}(\{1, 2, \dots, k\})$ . Dann gilt

$$\mu(\tau(x_1), \dots, \tau(x_k)) = \text{sign}(\tau)\mu(x_1, \dots, x_k),$$

wobei wir  $\text{sign}(\tau) = 0$  für  $\tau \in \text{Abb}(X) \setminus \text{Sym}(X)$  gesetzt haben.

**Korollar 6.13.** Sei  $v_1, \dots, v_n$  eine Basis von  $V$ ,  $\mu$  eine  $k$ -Form. Dann ist  $\mu$  eindeutig festgelegt durch die Werte

$$\mu(v_{i_1}, v_{i_2}, \dots, v_{i_k}) \text{ mit } 1 \leq i_1 < i_2 < \dots < i_k \leq n.$$

**Korollar 6.14.** Falls  $\dim_K(V) < k$ , so ist 0 die einzige  $k$ -Form auf  $V$ .

### 6.3 Determinanten

- Wir betrachten nun die (bis auf einen Faktor) eindeutige  $n$ -Form auf  $V$  mit  $\dim_K(V) = n$ .

**Satz 6.15.** Es sei  $v_1, \dots, v_n$  eine Basis von  $V$  und  $\beta \in K$ . Dann existiert genau eine  $n$ -Form  $\mu$  auf  $V$  mit  $\mu(v_1, \dots, v_n) = \beta$ .

**Korollar 6.16.** Es sei  $\dim_K(V) = n$  und  $\mu$  eine nicht-triviale (d.h.  $\mu$  nicht identisch Null)  $n$ -Form auf  $V$ . Weiters sei  $\nu$  eine  $n$ -Form auf  $V$ . Dann existiert  $\beta \in K$  mit  $\nu = \beta\mu$ .

- Es sei  $e_1, \dots, e_n$  die Standardbasis des  $K^n$  und  $\mu_0$  sei die eindeutig bestimmte  $n$ -Form mit  $\mu_0(e_1, \dots, e_n) = 1$ . Wir nennen  $\mu_0$  die Standard- $n$ -Form des  $K^n$ . Die Determinante einer Matrix  $A \in \text{Mat}_K(n \times n)$  mit Spaltenvektoren  $a_1, \dots, a_n$  ist nun gegeben durch

$$\det(A) = \mu_0(a_1, \dots, a_n).$$

Alternativ schreiben wir

**Definition 6.17.** Die Determinante  $\det(A)$  ist eine alternierende Form in den Spalten einer Matrix  $A$  mit  $\det(E_n) = 1$ .

**Lemma 6.18.** Mit  $A = (a_{ij})_{i,j=1,\dots,n}$  gilt

$$\det(A) = \sum_{\pi \in \text{Sym}(\{1,\dots,n\})} \text{sign}(\pi) \prod_{j=1}^n a_{\pi(j),j}.$$

**Satz 6.19.** Es gilt

1.  $\det(A \cdot B) = \det(A) \cdot \det(B)$
2.  $\det(A) = 0 \Leftrightarrow A$  nicht invertierbar.

**Satz 6.20.** Es gilt

1.  $\det(A^\top) = \det(A)$
2. Die Determinante ist eine alternierende Form in den Spalten einer Matrix.

## 6.4 Der Laplacesche Entwicklungssatz

- Wir lernen nun eine weitere Methode kennen, um die Determinante einer Matrix zu berechnen.

**Satz 6.21** (Cramersche Regel, Variante I). Es sei  $A = (a_1, \dots, a_n) \in \text{Mat}_K(n \times n)$  invertierbar, und  $Ax = b$ . Dann gilt für  $x = (x_1, \dots, x_n)$

$$x_j = \frac{\det(a_1, \dots, a_{j-1}, b, a_{j+1}, \dots, a_n)}{\det(A)}.$$

- Für  $A \in \text{Mat}_K(n \times n)$  bezeichnen wir mit  $A_{ij} \in \text{Mat}_K((n-1) \times (n-1))$  die Matrix, die entsteht, wenn aus  $A$  die  $i$ -te Zeile und die  $j$ -te Spalte entfernt werden.

**Satz 6.22** (Laplacescher Entwicklungssatz). Es sei  $A = (a_{ij})_{i,j=1,\dots,n} \in \text{Mat}_K(n \times n)$  und  $j_0 \in \{1, \dots, n\}$ . Dann gilt

$$\det(A) = \sum_{i=1}^n (-1)^{i+j_0} a_{i,j_0} \det(A_{i,j_0})$$

**Definition 6.23.** Es sei  $A \in \text{Mat}_K n \times n$ . Die zu  $A$  adjunkte Matrix  $\text{adj}(A) = (g_{ij}) \in \text{Mat}_K(n \times n)$  ist die Matrix mit den Einträgen

$$g_{ij} = (-1)^{i+j} \det(A_{ji}).$$

**Satz 6.24.** Es gilt  $\text{adj}(A) \cdot A = \det(A)E_n$ .

*Bemerkung.* 1. Es gilt auch  $A \cdot \text{adj}(A) = \det(A)E_n$

2. Falls  $A$  invertierbar ist, so folgt  $A^{-1} = \frac{\text{adj}(A)}{\det(A)}$ .

## 6.5 Die Determinante als Volumen

- Die geometrische Interpretation einer Determinante ist die eines vorzeichenbehafteten Volumens. Mit  $\text{vol}(a_1, \dots, a_n)$  für  $a_j \in \mathbb{R}^n$ ,  $j = 1, \dots, n$ , sei das Volumen der

Menge

$$PE(a_1, \dots, a_n) = \left\{ \sum_{j=1}^n \lambda_j a_j : 0 \leq \lambda_j \leq 1 \text{ für } j = 1, \dots, n \right\} \subset \mathbb{R}^n,$$

also des Spats (oder Parallelepipeds), bezeichnet.

**Satz 6.25.** *Es gilt  $\text{vol}(a_1, \dots, a_n) = |\det(a_1, \dots, a_n)|$ .*

**Definition 6.26.** Eine Volumenform auf  $V$  mit  $\dim_K(V) = n$  ist eine nicht-triviale  $n$ -Form.

**Definition 6.27.** Für  $F \in \text{Hom}_K(V, V)$  definieren wir  $\det(F)$  durch

$$\mu^F = \det(F)\mu$$

für eine beliebige Volumenform  $\mu$  auf  $V$ .

**Satz 6.28.** *Es sei  $V$  ein  $n$ -dimensionaler Vektorraum mit Basis  $\mathcal{A}$  und  $F \in \text{End}_K(V)$ . Dann gilt*

$$\det(F) = \det(M(\mathcal{A}, F, \mathcal{A})).$$

**Korollar 6.29.** *Es gilt*

1. *Die Determinante einer Matrix ist invariant unter einem Basiswechsel,*
2.  $\det(F \circ G) = \det(F) \circ \det(G)$ .