I Grundbegriffe

2 Abbildungen

2.1 Überblick
Abbildung Eine Abbildung f von einer Menge X in eine Menge Y ist eine Vorschrift, die jedem $x \in X$ auf eindeutige Weise genau ein $f(x) \in Y$ zuordnet.

Schreibweise: $f : X \to Y, x \mapsto f(x)$ Wichtiges:

- X heißt Definitionsmenge.
- Y heißt Zielmenge
- Zwei Abbildungen sind gleich, wenn
  - Definitionsmenge gleich,
  - Zielmenge gleich,
  - jedem $x \in X$ das gleiche Element $y \in Y$ zugeordnet wird.
- $\mathrm{Abb}(X, Y)$: Menge der Abbildungen von X nach Y.
- Funktionen Abbildungen mit Zielmenge $\mathbb{R}$.

2.3 Beispiel
(a) Identische Abbildung für jede Menge X ist $\mathrm{id}_X : X \to X, x \mapsto x$.

(b) Inklusionsabbildung für jede Teilmenge $A \subseteq X$ ist $\iota_A : A \to X, x \mapsto x$

(c) Konstante Abbildung zu je 2 Mengen X, Y und $y_0 \in Y$ ist $c_{y_0} : X \to Y, x \mapsto y_0$

(d) Charakteristische Funktion zu jeder Menge X und Teilmenge $A \subseteq X$ ist

$$\chi_A : X \to \mathbb{R}, x \mapsto \begin{cases} 1, \text{falls } x \in A \\ 0, \text{falls } x \notin A \end{cases}$$

(e) Kroneckersymbol zu jeder Menge X die Abbildung:

$$X \times X \to \mathbb{R}, (x, y) \mapsto \delta_{x,y} := \begin{cases} 1 \text{ falls } x = y \\ 0 \text{ falls } x \neq y \end{cases}$$

2.4 Definition (Eigenschaften Abbildung)
Mit $f : X \to Y$ Abbildung:

1. f surjektiv, falls $\forall x, x' \in X : f(x) = f(x') \Rightarrow x = x'$
2. f injektiv, falls $\forall y \in Y \, \exists x \in X : f(x) = y$
3. f bijektiv, falls f surjektiv und injektiv

2.6 Definition (Restriktion, Urbild, Bild)
Sei $f : X \to Y$ Abbildung. Dann

- Restriktion / Einschränkung Mit $A \subseteq X$ ist $f|_A : A \to Y, a \mapsto f(a)$
- Bild von $A \subset X$ unter f ist $f(A) := \{f(a) | \forall a \in A\}$
- Urbild von $B \subset Y$ unter f ist $f^{-1}(B) := \{x \in X | f(x) \in B\}$

  Bild von f $\mathrm{Im}(f) := f(X)$

2.9 Definition (Komposition)
Mit Abbildungen $f : X \to Y$ und $g : Y \to Z$ ist Komposition $g \circ f : X \to Z, x \mapsto g(f(x))$.

Abstrakt: $\circ : \mathrm{Abb}(Y, Z) \times \mathrm{Abb}(X, Y) \to \mathrm{Abb}(X, Z)$

2.10 Satz
Die Komposition von Abbildungen $\circ$ ist assoziativ. $h \circ (g \circ f) = (f \circ g) \circ f$ mit entsprechend definierten Abbildungen.

2.11 Definition
Ist $f : X \to Y$ bijektive Abbildung, so existiert zu jedem $y \in Y$ ein $x_y \in X$ mit $f(x_y) = y$, folglich $f^{-1} : Y \to X, y \mapsto x_y$ ist Umkehrabbildung

2.12 Satz
Ist $f : X \to Y$ bijektiv, so ist $\mathrm{id}_X = f^{-1} \circ f = f \circ f^{-1}$

2.14 Definition (Familie)
Mit I, X Mengen heißt Abbildung $x : I \to X, i \mapsto x_i$ Familie von Elementen X mit Indexmenge I bzw. I-Tupel von Elementen von X.

2.15 Beispiel
Folge ist Familie $(x_i)_{i \in \mathbb{N}_0}$ mit Indexmenge $\mathbb{N}_0$

2.16 Definition (Graph)
Graph einer Abbildung $f : X \to Y$ ist $\Gamma_f := \{(x, y) \in X \times Y | y = f(x)\}$

3 Gruppen

3.1 Definition
Sei G Menge. Verknüpfung auf G ist Abbildung $* : G \times G \to G, (x, y) \mapsto x * y$.

- Halbgruppe ist ein Paar $(G, *)$, wenn gilt:

(G1) Assoziativität Für $x, y, z \in G : (x * y) * z = x * (y * z)$

- Monoid ist Halbgruppe, wenn noch gilt:

(G2) Es gibt ein $e \in G$, mit dem für alle $x \in G : x * e = e * x = x$

- Neutrales Element der Verknüpfung $*$: ein $e \in G$ wie in (G2)

3.3 Satz (Eindeutigkeit des neutralen Elements)
Ein Monoid $(G, *)$ besitzt genau ein neutrales Element

3.4 Definition
Gruppe ist ein Monoid $(G, *)$ mit neutralem Element $e \in G$, für den noch gilt

(G3) Für jedes $x \in G$ existiert ein $x' \in G : x * x' = x' * x = e$

Kommutativität Für alle $x, y \in G : x * y = y * x$. Damit

- abelsch Gruppe, welche das Kommutativgesetz einhält
- Inverses Element heißt ein $x' \in G$ wie in (G3).

3.6 Satz (Eindeutigkeit des Inversen)
Ist $(G, *)$ eine Gruppe, so gibt es zu jedem $x \in G$ genau ein inverses Element.

3.7 Beispiel
(a) Triviale Gruppe besteht nur aus dem neutralen Element: $G := \{e\}$

(b) Permutation ist Menge $\mathrm{Sym}(X) := \{f \in \mathrm{Abb}(X, X) \mid f \text{ bijektiv}\}$ auf Menge X, die mit der Komposition Gruppe bildet: $(\mathrm{Sym}(X), \circ)$, genannt symmetrische Gruppe auf X (für $n \in \mathbb{N}$ geschrieben als $S_n := \mathrm{Sym}(\{1, ..., n\})$).

3.10 Satz
Mit $(G, \cdot)$ Gruppe und $x, y \in G$ gilt: $(x^{-1})^{-1} = x, (xy)^{-1} = y^{-1}x^{-1}$.

3.11 Satz
Mit $(G, \cdot)$ und $a, b \in G$ haben die Gleichungen $a \cdot x = b, y \cdot a = b$ eindeutige Lösungen ($x = a^{-1} \cdot b, y = b \cdot a^{-1}$), damit existieren die Kürzungsregeln.

3.12 Bemerkung
- Endlich Eine Gruppe $(G, \cdot)$ ist endlich, falls Menge G endlich
- Ordnung ist die Mächtigkeit von G
- Endliche Gruppen können durch Verknüpungstafeln beschrieben werden.

3.13 Definition
Untergruppe einer Gruppe $(G, \cdot)$ ist nichtleere Teilmenge $H \subseteq G$ mit

(UG1) $x, y \in H : x \cdot y \in H$ (Abgeschlossenheit unter Multiplikation)

(UG2) $x \in H : x^{-1} \in X$ (Abgeschlossenheit Inversem)

3.14 Satz
Sei $(G, \cdot)$ Gruppe und $\emptyset \neq H \subseteq G$. Genau dann ist H Untergruppe von G, wenn sich die Verknüpfung $\cdot$ zu einer Abbildung $\cdot_H : H \times H \to H$ einschränken lässt (d.h. $\cdot|_{H \times H} = \iota_H : H \to G$ die Inklusionsabbildung ist) und $(H, \cdot_H)$ Gruppe ist.

Notation: $H \leq G$

3.16 Beispiel
(a) Jede Gruppe enthält triviale Untergruppe $H = G, H = \{e\}$.

3.17 Lemma
Ist G eine Gruppe, $(H_i)_{i \in I}$ eine Familie von Untergruppen von G, so ist auch $H := \bigcap_{i \in I} H_i$ Untergruppe von G. (Für $I = \emptyset$ setzt man $\bigcap_{i \in I} \in I)H_i = G$).

3.18 Satz
Ist G Gruppe und $X \subseteq G$ Teilmenge, so gibt es eindeutlich bestimmte kleinste Untergruppe H von G, die X enthält, d.h. H enthält X, und ist H' weitere Untergruppe von G, die X enthält, so gilt $H \subseteq H'$.

3.19 Definition
Ist G Gruppe und $X \subseteq G$ Teilmenge, so nennt man die kleinste Untergruppe von G, die X enthält, die von X erzeugte Untergruppe von G. Wird G selbst von endlicher Menge erzeugt, so heißt G endlich erzeugt.

Notation: $\langle X \rangle$ (falls $X = \{x_1, \ldots, x_n\}$ endlich auch $\langle x_1, \ldots, x_n \rangle$).

4 Ringe

4.1 Definition (Ring)
Ein Ring ist ein Tripel $(R, +, \cdot)$ aus Menge R und Verknüpfungen $+ : R \times R \to R$ („Addition“) bzw. $\cdot : R \times R \to R$ („Multiplikation“), das erfüllt:

(R1) $(R, +)$ ist abelsche Gruppe

(R2) $(R, \cdot)$ ist Halbgruppe

(R3) Distributivgesetze gelten für $a, x, y \in R$:

$$a \cdot (x + y) = a \cdot x + a \cdot y \qquad \text{und} \qquad (x + y) \cdot a = (x\dot{a}) + (y \cdot a)$$

Weiterhin:

- kommutativ ist ein Ring $(R, +, \cdot)$, wenn $x \cdot y = y \cdot x \ \forall x, y \in \mathbb{R}$
- Einselement ist das neutrale Element der Multiplikation $e \in R : e \cdot x = x \cdot e = x$.
- Unterring eines Ringes $(R, +, \cdot)$ ist Teilmenge $S \subseteq R$ mit geeigneter Einschränkung von Addition, Multiplikation.
  Aus Übung 31
  Ist R ein Ring und $\emptyset \neq S \subseteqq R$, dann ist S genau dann Unterring von R, wenn folgende Bedingungen gelten:

  (UR1) S ist abgeschlossen bzgl. Addition

  (UR2) S ist abgeschlossen bzgl. Bildung additiver Inverser

  (UR3) S ist abgeschlossen bzgl. Multiplikation

4.3 Beispiel
(a) Nullring ist $R = \{0\}$ mit den einzig möglichen Verknüpfungen $+, \cdot$ und ist kommutativ mit 0 als Einselement.

4.4 Bemerkung
Ist R ein Ring, so gelten für $x, y \in R$:

(a) $0 \cdot x = x \cdot 0 = 0$

(b) $x \cdot (-y) = (-x) \cdot y = -xy$

(c) $(-x) \cdot (-y) = xy$

4.6 Theorem (Division mit Rest in $\mathbb{Z}$)
Für jedes $a \in \mathbb{Z}$ gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$

4.9 Definition (Charakteristik)
Sei R ein Ring mit Einselement 1. Die Charakteristik von R ist das kleinste $n \in \mathbb{N}$ mit $\underbrace{1 + \ldots + 1}_{n \text{ viele}} = 0$, falls so ein n existiert – andernfalls hat R die Charakteristik 0.

4.10 Definition (Nullteiler)
Sei R ein Ring. Ein $0 \neq x$ heißt Nullteiler von R, wenn es ein $0 \neq y \in R$ gibt mit $xy = 0$ oder $yx = 0$. Ein Ring ohne Nullteiler heißt nullteilerfrei.

4.11 Definition (Einheit)
Sei R ein Ring mit Einselement 1. Ein $x \in R$ heißt invertierbar, oder Einheit von R, wenn es $x' \in R$ mit $xx' = x'x = 1$ gibt.

Notation: $R^\times$ ist Menge der invertierbaren Elemente.

4.13 Satz
Sei R ein Ring mit Einselement 1.

(a) Ist $x \in R$ invertierbar, so ist x kein Nullteiler in R.

(b) Die invertierbaren Elemente $R^\times$ von R bilden mit der Multiplikation eine Gruppe.

5 Körper

5.1 Definition
Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$ mit Einslement $1 \neq 0$, indem jedes $0 \neq x \in K$ invertierbar ist.

5.2 Bemerkung
Ein Körper K ist stets nullteilerfrei, und es gelten

(K1) $(K, +)$ ist abelsche Gruppe mit neutralem Element 0.

(K2) $(K \setminus \{0\}, \cdot)$ ist abelsche Gruppe mit neutralem Element 1.

(K3) Es gelten die Distributivgesetze (R3).

5.4 Definition (Teilkörper)
Ein Teilkörper eines Körpers $(K, +, \cdot)$ ist Teilmenge $L \subseteq K$, die mit geeigneter Einschränkung von $+$ und $\cdot$ wieder Körper ist.

5.6 Beispiel (Komplexe Zahlen)
Komplexe Zahlen ist Menge $\mathbb{C} := \mathbb{R} \times \mathbb{R}$, mit Addition / Multiplikation definiert als $\big((x_1, y_1), (x_2, y_2) \in \mathbb{C}\big)$

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2) \qquad (x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

und sind damit Körper. Die imaginäre Einheit $i := (0, 1)$ erfüllt $i^2 = -1$, und jedes Element $z \in \mathbb{C}$ lässt sich als $z = x + iy$ schreiben, $x, y \in \mathbb{R}$.

5.7 Lemma
Sei $a \in \mathbb{Z}$ eine ganze Zahl und $p \in \mathbb{Z}$ eine Primzahl, die a nicht teilt. Dann gibt es $b, k \in \mathbb{Z}$ mit $ab + kp = 1$.

5.8 Beispiel (Endlicher Primzahlkörper)
Für jede Primzahl $p \in \mathbb{Z}$ ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Ist $\bar{a} \neq \bar{0}$, so gilt $p \nmid a$, und somit gibt es nach 5.7 $b, k \in \mathbb{Z}$ mit

$$\bar{1} = \overline{ab + kp} = \bar{a} + \bar{b}.$$

Zusammen mit 4.12 und 4.13 erhalt man, dass für ein $n \in \mathbb{N}$ die folgenden Aussagen äquivalent sind:

(1) Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper.

(2) Der Ring $\mathbb{Z}/p\mathbb{Z}$ ist nullteilerfrei.

(3) n ist Primzahl.

6 Polynome

Hier ist R kommutativer Ring mit Einslement.

6.2 Definition (Polynomring)
Sei $R[X]$ die Menge der Folgen in R, die fast überall 0 sind, also $R[X] := \{(a_k)_{k \in \mathbb{N}_0} | \forall k : a_k \in R \text{ und } \exists n_0 \, \forall k > n_0 : a_k = 0\}$. Addition und Multiplikation ist gegeben durch

$$(a_k)_{k \in \mathbb{N}_0} + (b_k)_{k \in \mathbb{N}_0} = (a_k + b_k)_{k \in \mathbb{N}_0} \qquad (a_k)_{k \in \mathbb{N}_0} \cdot (b_k)_{k \in \mathbb{N}_0} = (c_k)_{k \in \mathbb{N}_0}, c_k = \sum_{i+j=k} a_i b_j$$

Damit ist $R[X]$ ein kommutativer Ring mit Einselement, der Polynomring (in einer Variablen X) über R.

Weiterhin

- Polynom ist $(a_k)_{k \in \mathbb{N}_0} \in R[X]$ mit Koeffizienten $a_0, a_1, \ldots$.
- Mit $x \in R$ und $(x, 0, 0, \ldots)$ ist R Unterring von $R[X]$
- Mit X als Folge $(0, 1, 0, \ldots)$ lässt sich $X^n = (\delta_{k,n})_{k \in \mathbb{N}_0}$ definieren. Damit schreibt sich auch jedes $(a_k)_{k \in \mathbb{N}_0}$ mit $a_k = 0$ für alle $k > n_0$ als

Notation:

$$f = f(X) = \sum_{k=0}^{n_0} a_k X^k = a_0 + a_1 X + \ldots \qquad f = \sum_{k \geq 0} a_k X^k = \sum_{k \in \mathbb{N}_0} a_k X^k$$

- Der Grad eines Polynoms f ist $\deg(f) := \max\{n \in \mathbb{N}_0 | a_n \neq 0\}$ für $0 \neq f(X) = \sum_{n \geq 0} a_k X^k \in R[X]$.

- $\deg(0) = -\infty$ (Grad des Nullpolynoms)
- Konstanter Term ist a_0
- Leitkoeffizient ist $a_{\deg(f)}$ von f.
- Hat f den Grad $0, 1$ oder 2, so heißt f konstant, linear bzw. quadratisch.

6.4 Satz
Seien $f, g \in R[X]$.

(a) Es ist $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$

(b) Es ist $\deg(fg) \leq \deg(f) + \deg(g)$

(c) Ist R nullteilerfrei, dann ist $\deg(fg) = \deg(f) + \deg(g)$ und $R[X]$ ist nullteilerfrei.

6.5 Theorem (Polynomdivision)
Sei K Körper und sei $0 \neq g \in K[X]$. Für jedes $f \in K[X]$ gibt es eindeutig bestimmte $h, r \in K[X]$ mit $f = gh + r$ und $\deg(r) < \deg(g)$.

6.7 Definition (Polynomauswertung)
Sei $f(X) = \sum_{k \geq 0} a_k X^k \in R[X]$. Für $\lambda \in R$ ist die Auswertung von f in λ als $f(\lambda) = \sum_{k \geq 0} a_k \lambda^k \in R$.

Das Polynom f definiert so eine Abb. $\tilde{f} : R \to R, \lambda \mapsto f(\lambda)$. Ein $\lambda \in R$ mit $f(\lambda) = 0$ heißt Nullstelle von f.

6.8 Lemma
Für $f, g \in R[X]$ und $\lambda \in R$ ist $(f+g)(\lambda) = f(\lambda) + g(\lambda)$ und $(fg)(\lambda) = f(\lambda)g(\lambda)$.

6.9 Satz
Ist K Körper und $\lambda \in K$ Nullstelle von $f \in K[X]$, so gibt es eindeutiges $h \in K[X]$ mit $f(X) = (X - \lambda) \cdot h(x)$.

6.10 Korollar
Sei K ein Körper. Ein Polynom $0 \neq f \in K[X]$ hat höchstens $\deg(f)$ viele Nullstellen in K.

6.11 Korollar
Ist K ein unendlicher Körper, so ist die Abbildung $K[X] \to \mathrm{Abb}(K, K), f \mapsto \tilde{f}$ injektiv.

6.13 Satz
Für einen Körper K sind äquivalent:

(1) Jedes $f \in K[X]$ vom Grad $\deg(f) > 0$ hat eine Nullstelle in K.

(2) Jedes $0 \neq f \in K[X]$ zerfällt über K in Linearfaktoren, also $f(X) = a \cdot \prod_{i=1}^{n} (X - \lambda_n)$ mit $n = \deg(f)$, $a \in K$ und $\lambda_1, \ldots, \lambda_n \in K$.

6.14 Definition
Ein Körper K heißt algebraisch abgeschlossen, wenn er eine Bedingung aus Satz 6.13 erfüllt.

6.15 Theorem (Fundamentalsatz der Algebra, d'Alembert 1746, Gauss 1799)
Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.

II Vektorräume

1 Definition und Beispiele

1.2 Definition (Vektorraum)
Ein K-Vektorraum (oder auch Vektorraum über K) ist ein Tripel $(V, +, \cdot)$ bestehend aus einer Menge V, einer Verknüpfung $+ : V \times V \to V$, genannt Addition, und einer Abbildung $\cdot : K \times V \to V$, genannt Skalarmultiplikation, mit

(V1) $(V, +)$ ist abelsche Gruppe,

(V2) Skalarmultiplikation ist verträglich, d.h. für $\lambda, \mu \in K$, $x, y \in V$:

  (i) $\lambda \cdot (x + y) = \lambda x + \lambda y$

  (ii) $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$

  (iii) $\lambda \cdot (\mu \cdot x) = (\lambda \cdot \mu) \cdot x$

  (iv) $1 \cdot x = x$

Das neutrale Element von $(V, +)$ ist $\mathbf{0}$ und heißt Nullvektor.

1.4 Beispiel (Standardraum)
Standardraum Für $n \in \mathbb{N}$ ist $V = K^n := \prod_{i=1}^{n} K = \{(x_1, \ldots, x_n) | x_i \in K\}$ mit komponentenweiser Addition und komponentenweiser Skalarmultiplikation ein K-Vektorraum.

Nullraum ist der Standardraum für $n = 0$, d.h. $V = \{0\}$.

1.5 Satz
Ist V ein K-Vektorraum, so gelten für $\lambda \in K$ und $x \in V$:

(a) $0 \cdot x = \mathbf{0}$

(b) $\lambda \cdot \mathbf{0} = \mathbf{0}$

(c) $(-\lambda) \cdot x = \lambda \cdot (-x) = -(\lambda \cdot x)$ (insbes. $-1 \cdot x = -x$)

(d) $\lambda \cdot x = \mathbf{0} \Rightarrow \lambda = 0 \vee x = \mathbf{0}$

1.7 Definition (Untervektorraum)
Sei V ein K-Vektorraum. Ein Untervektorraum von V ist nichtleere Teilmenge $W \subseteq V$ mit

(UV1) Für $x, y \in W : x + y \in W$

(UV2) Für $x \in W, \lambda \in K : \lambda x \in W$

1.8 Satz
Sei V ein K-Vektorraum, und $W \subseteq V$ eine Teilmenge. Genau dann ist W ein Untervektorraum von V, wenn W mit geeigneter Einschränkung von Addition und Skalarmultiplikation ein K-Vektorraum ist.

1.9 Beispiel
Triviale Untervektorräume hat jeder K-Vektorraum V, nämlich $W = \{\mathbf{0}\}$ und $W = V$.

1.10 Lemma
Ist V ein K-Vektorraum und $(W_i)_{i \in I}$ eine Familie von Untervektorräumen von V, so ist auch $W := \bigcap_{i \in I} W_i$ ein Untervektorraum von V.

1.11 Satz
Ist V ein K-Vektorraum und $X \subseteq V$ eine Teilmenge, so gibt es einen eindeutig bestimmten kleinsten Untervektorraum W von V, der X enthält.

1.12 Definition
Ist V ein K-Vektorraum und $X \subseteq V$ eine Teilmenge, so nennt man den kleinsten Untervektorraum von V, der X enthält, den von X erzeugten Untervektorraum.

Notation: $\langle X \rangle$

Eine Menge $X \subseteq V$ mit $\langle X \rangle = V$ heißt auch Erzeugendensystem von V. Der Vektorraum V heißt endlich erzeugt, wenn er ein endliches Erzeugendensystem $X \subseteq V$ besitzt.

2 Linearkombination und lineare Abhängigkeit

Sei V ein K-Vektorraum.

2.1 Definition (Linearkombination)

1. Sei $n \in \mathbb{N}_0$. Ein $x \in V$ ist eine (K-)Linearkombination eines n-Tupels $(x_1, \ldots, x_n)$ von Elementen von V, wenn es $\lambda_1, \ldots, \lambda_n \in K$ gibt mit $x = \lambda_1 x_1 + \ldots + \lambda_n x_n$.

   Der Nullvektor ist stets Linearkombination, auch für $n = 0$.

2. Ein $x \in V$ ist eine Linearkombination einer Familie $(x_i)_{i \in I}$ von Elementen von V, wenn es $n \in \mathbb{N}_0$ und $i_1, \ldots, i_n \in I$ gibt, für die x eine Linearkombination von $(x_{i_1}, \ldots, x_{i_n})$ ist.

3. Die Menge $x \in V$, die eine Linearkombination von $\mathcal{F} = (x_i)_{i \in I}$ sind, wird mit $\mathrm{span}_{\mathrm{K}}(\mathcal{F})$ bezeichnet.

2.3 Lemma
Für jede Teilmenge $X \subseteq V$ ist $\mathrm{span}_{\mathrm{K}}(X)$ ein Untervektorraum von V.

2.4 Satz
Für jede Teilmenge $X \subseteq V$ ist $\mathrm{span}_{\mathrm{K}}(X) = \langle X \rangle$ der von X erzeugte Untervektorraum von V.

2.5 Bemerkung
Man nennt $\mathrm{span}_{\mathrm{K}}(X)$ auch den von X aufgespannten Untervektorraum, oder die lineare Hülle von X.

2.6 Beispiel
Sei $V = K^n$ der Standardraum. Für $i = 1, \ldots, n$ sei $e_i = (\delta_{i,1}, \ldots, \delta_{i,n})$. Dann ist $\mathrm{span}_{\mathrm{K}}(e_1, \ldots, e_n) = K^n$, und K^n ist endlich erzeugt. Die $e_1, \ldots, e_n$ heißen Standardbasis.

2.7 Definition (Lineare Abhängigkeit)

1. Sei $n \in \mathbb{N}_0$. Ein n-Tupel $(x_1, \ldots, x_n)$ von Elementen von V sind (K-)linear abhängig, wenn es $\lambda_1, \lambda_n \in K$ gibt, die nicht alle gleich Null sind, und $\lambda_1 x_1 + \ldots + \lambda_n x_n = 0$. Andernfalls heißt $(x_1, \ldots, x_n)$ linear unabhängig

2. Eine Familie $(x_i)_{i \in I}$ von Elementen von V ist linear abhängig, wenn es $n \in \mathbb{N}_0$ und paarweise verschiedene $i_1, \ldots, i_n \in I$ gibt, für welche das n-Tupel $(x_{i_1}, \ldots, x_{i_n})$ linear abhängig ist. Andernfalls heißt $(x_i)_{i \in I}$ linear unabhängig.

2.9 Satz
Genau dann ist eine Familie $(x_i)_{i \in I}$ linear abhängig, wenn es ein $i_0 \in I$ mit $x_{i_0} \in \mathrm{span}_{\mathrm{K}}\left((x_i)_{i \in I \setminus \{i_0\}}\right)$ gibt. In diesem Fall ist $\mathrm{span}_{\mathrm{K}}\left((x_i)_{i \in I}\right) = \mathrm{span}_{\mathrm{K}}\left((x_i)_{i \in I \setminus \{i_0\}}\right)$.

2.10 Satz
Genau dann ist eine Familie $(x_i)_{i \in I}$ linear unabhängig, wenn sich jedes $x \in \mathrm{span}_{\mathrm{K}}\left((x_i)_{i \in I}\right)$ in eindeutiger Weise als Linearkombination der $(x_i)_{i \in I}$ schreiben lässt, d.h. ist $x = \sum_{i \in I} \lambda_i x_i = \sum_{i \in I} \lambda'_i x_i$ mit $\lambda_i, \lambda'_i \in K$, fast alle gleich Null, so ist $\lambda_i = \lambda'_i$ für alle $i \in I$.

3 Basis und Dimension

Sei V ein K-Vektorraum.

3.1 Definition (Basis)
Eine Familie $(x_i)_{i \in I}$ von Elementen von V heißt (K-)Basis von V, wenn gilt:

(B1) Die Familie $(x_i)_{i \in I}$ ist linear unabhängig

(B2) Die Familie $(x_i)_{i \in I}$ erzeugt V, d.h. $\mathrm{span}_{\mathrm{K}}\left((x_i)_{i \in I}\right) = V$.

3.3 Satz
Sei $(x_i)_{i \in I}$ eine Familie von Elementen von V. Genau dann ist $(x_i)_{i \in I}$ eine Basis von V, wenn sich jedes $x \in V$ eindeutig als $x = \sum_{i \in I} \lambda_i x_i$ mit $\lambda_i \in K$, fast alle gleich Null, schreiben lässt.

3.5 Satz
Für eine Familie $\mathcal{B} = (x_i)_{i \in I}$ von Elementen von V sind folgende Aussagen äquivalent:

(1) $\mathcal{B}$ ist eine Basis von V.

(2) $\mathcal{B}$ ist minimales Erzeugendensystem, d.h. $\mathcal{B}$ ist Erzeugendensystem, aber jede Teilmenge $J \subsetneqq I$ ist $(x_i)_{i \in J}$ kein Erzeugendensystem.

(3) $\mathcal{B}$ ist maximal linear unabhängig, d.h. $\mathcal{B}$ ist linear unabhängig, aber jede Familie $(x_i)_{i \in J}$ mit $J \supsetneqq I$ ist linear abhängig.

3.6 Theorem (Basisauswahlsatz)
Jedes endliche Erzeugendensystem von V besitzt eine Basis von V als Teilfamilie: ist $(x_i)_{i \in I}$ ein endliches Erzeugendensystem, so gibt es eine Teilmenge $J \subseteq I$, für die $(x_i)_{i \in J}$ eine Basis ist.

3.7 Korollar
Jeder endlich erzeugte K-Vektorraum besitzt eine endliche Basis.

3.10 Lemma (Austauschlemma)
Sei $\mathcal{B} = (x_1, \ldots, x_n)$ eine Basis von V. Sind $\lambda_1, \ldots, \lambda_n \in K$ und $y = \sum_{i=1}^{n} \lambda_i x_i$, so ist für jedes $j \in \{1, \ldots, n\}$ mit $\lambda_j \neq 0$ auch $\mathcal{B}' = (x_1, \ldots, x_{j-1}, y, x_{j+1}, \ldots, x_n)$ eine Basis von V.

3.11 Theorem (STEINITZ'scher Austauschsatz)
Sei $\mathcal{B} = (x_1, \dots, x_n)$ eine Basis von V und $\mathcal{F} = (y_1, \dots, y_n)$ eine linear unabhängige Familie in V. Dann ist $r \leq n$ und es gibt $i_1, \dots, i_{n-r} \in \{1, \dots, n\}$, für die $\mathcal{B}' = (y_1, \dots, y_r, x_{i_1}, \dots, x_{i_{n-r}})$ eine Basis von V ist.

3.12 Korollar (Basisergänzungssatz)
Ist V endlich erzeugt, so lässt sich jede linear unabhängige Familie zu einer Basis ergänzen: ist $(x_1, \dots, x_n)$ linear unabhängig, so gibt es $m \geq n$ und $x_{n+1}, \dots, x_m \in V$ derart, dass $(x_1, \dots, x_m)$ eine Basis von V ist.

3.13 Korollar
Sind $(x_i)_{i \in I}$ und $(y_j)_{j \in J}$ Basen von V, und ist I endlich, so ist $|I| = |J|$.

3.14 Korollar
Ist V endlich erzeugt, so haben alle Basen von V dieselbe Mächtigkeit.

3.15 Definition (Dimension)
Ist V endlich erzeugt, so ist die Dimension von V die Mächtigkeit $\dim_K(V)$ eine Basis von V. Andernfalls sagt man, dass V unendliche Dimension hat, und schreibt $\dim_K(V) = \infty$.

3.18 Satz
Sei V endlich erzeugt, und $W \subseteq V$ ein Untervektorraum.

(a) Es ist $\dim_K(W) \leq \dim_K(V)$. Insbesondere ist W endlich erzeugt.

(b) Ist $\dim_K(W) = \dim_K(V)$, so ist $V = W$.

4 Summen von Vektorräumen

Sei V ein K-Vektorraum und $(W_i)_{i \in I}$ eine Familie von Untervektorräumen von V.

4.1 Definition (Summe von Untervektorräumen)
Die Summe $(W_i)_{i \in I}$ ist der Untervektorraum $\sum_{i \in I} W_i = \text{span}_K \left(\bigcup_{i \in I} W_i \right)$ von V. Im Fall $I = \{1, \dots, n\}$ schreibt man auch $W_1 + \dots + W_n$ für $\sum_{i \in I} W_i$.

4.2 Lemma
Es ist $\sum_{i \in I} = \left\{ \sum_{i \in I} x_i \middle| \, x_i \in W_i, \text{ fast alle gleich Null} \right\}$

4.4 Satz
Es sind äquivalent:

(1) Jedes $x \in \sum_{i \in I} W_i$ ist eindeutig als $\sum_{i \in I}$ mit $x_i \in W_i$ darstellbar.

(2) Für jedes $i \in I$ ist $W_i \cap \sum_{j \in I \setminus \{i\}} W_j = \{0\}$

4.5 Definition (Direkte Summe von Untervektorräumen)
Ist jedes $x \in \sum_{i \in I} W_i$ eindeutig als $\sum_{i \in I} x_i$ mit $x_i \in W_i$ darstellbar, so sagt man das $\sum_{i \in I} W_i$ die direkte Summe der Untervektorräume $(W_i)_{i \in I}$ ist, und schreibt $\bigoplus_{i \in I} W_i$ für $\sum_{i \in I} W_i$. Im Fall $I = \{1, \dots, n\}$ schreibt man auch $W_i \oplus \dots \oplus W_n$ für $\bigoplus_{i \in I} W_i$.

4.8 Korollar
Seien W_1, W_2 Untervektorräume von V. Es sind äquivalent:

(1) $V = W_1 \oplus W_2$

(2) $V = W_1 + W_2$ und $W_1 \cap W_2 = \{0\}$.

4.9 Satz
Seien W_1, W_2 Untervektorräume von V mit den Basen $(x_i)_{i \in I_1}$ bzw. $(x_i)_{i \in I_2}$, wobei $I_1 \cap I_2 = \emptyset$. Es sind äquivalent:

(1) $V = W_1 \oplus W_2$

(2) $(x_i)_{i \in I_1 \cup I_2}$ ist eine Basis von V.

4.10 Korollar
Ist V endlichdimensional, so ist jeder Untervektorraum eine direkte Summe, d.h. ist W ein Untervektorraum von V, so gibt es (i.A. nicht eindeutig bestimmten) Untervektorraum W' von V (genannt lineares Komplement zu W) mit $V = W \oplus W'$. Es ist $\dim_K(W') = \dim_K(V) - \dim_K(W)$.

4.12 Theorem (Dimensionsformel)
Ist V endlichdimensional und sind W_1, W_2 Untervektorräume von V, so ist $\dim_K(W_1 + W_2) + \dim_K(W_1 \cap W_2) = \dim_K(W_1) + \dim_K(W_2)$.

4.13 Definition (Externes Produkt von Vektorräumen)
Das (externe) Produkt einer Familie $(V_i)_{i \in I}$ von K-Vektorräumen ist der K-Vektorraum $\prod_{i \in I} V_i$ bestehend aus dem kartesischen Produkt der V_i mit komponentenweiser Addition und Skalarmultiplikation.

4.14 Definition (Externe direkte Summe von Vektorräumen)
Die (externe) direkte Summe einer Familie $(V_i)_{i\in I}$ von K-Vektorräumen ist der Untervektorraum $\bigoplus_{i\in I} V_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} V_i \,\middle|\, x_i = 0 \text{ für fast alle } i \right\}$ des Produktes $\prod_{i\in I} V_i$.

4.16 Lemma
Sei $(V_i)_{i\in I}$ eine Familie von K-Vektorräumen und $V := \bigoplus_{i\in I} V_i$. Für jedes $j \in I$ ist $\tilde{V}_j = V_j \times \prod_{i\in I\setminus\{j\}} \{0\}$ ein Untervektorraum von V, und $V = \bigoplus_{i\in I} \tilde{V}_i$.

III Lineare Abbildungen

In diesem Kapitel sei K ein Körper.

1 Matrizen

1.1 Definition (Matrix)
Seien $m, n \in \mathbb{N}_0$. Eine $m \times n$-Matrix über K ist en rechteckiges Schema

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

mit $a_{ij} \in K$ für $i = 1, \dots, m; j = 1, \dots, n$. Man schreibt dies auch als

$$A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$$

, oder einfach $A = (a_{ij})_{i,j}$, wenn m und n aus dem Kontext hervorgehen.

- Die $a_{i,j}$ heißen Koeffizienten der Matrix, und wir definieren $(A)_{ij} := a_{ij}$.
- Die Menge der $m \times n$-Matrizen wird mit $\mathrm{Mat}_{m\times n}(K)$ oder $K^{m\times n}$ bezeichnet.
- Man nennt das Paar (m, n) auch den Typ (manchmal auch Dimension) der Matrix

  Ist $m = n$, so spricht man von quadratischen Matrix, und schreibt $\mathrm{Mat}_n(K) := \mathrm{Mat}_{n\times n}(K)$.
- Zu einer Matrix $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{m\times n}(K)$ definiert man die transponierte Matrix $A^t := (a_{ij})_{j,i} \in \mathrm{Mat}_{n\times m}(K)$.

1.2 Beispiel
Seien $m, n \in \mathbb{N}$ fest.

(a) Die Nullmatrix ist $0 = (0)_{i,j} \in \mathrm{Mat}_{m\times n}(K)$.

(b) Für $k \in \{1, \dots, m\}$ und $l \in \{1, \dots, n\}$ ist die $(k, l)-$Basismatrix gegeben durch $E_{kl} = (\delta_{ik}\delta_{jl})_{i,j} \in \mathrm{Mat}_{m\times n}(K)$.

(c) Die Einheitsmatrix ist $\mathbb{1}_n = (\delta_{i,i})_{i,j} \in \mathrm{Mat}_n(K)$. Insbesondere ist $\mathbb{1}_n = \mathrm{diag}(1, \dots, 1)$

(d) Für die Permutation $\sigma \in S_n$ definiert man die Permutationsmatrix $P_\sigma = (\delta_{i,1}\sigma(i), j)_{i,j} \in \mathrm{Mat}_n(K)$

(e) Für $a_1, \dots, a_n \in K$ hat man den Zeilenvektor $(a_1, \dots, a_n) := (a_1 \ \dots \ a_n) \in \mathrm{Mat}_{1\times n}(K)$, sowie

den Spaltenvektor $(a_1, \dots, a_n)^t = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathrm{Mat}_{n\times 1}(K)$.

1.3 Definition
Seien $A = (a_{ij})_{i,j}, B = (b_{ij})_{i,j} \in \mathrm{Mat}_{m\times n}(K)$ und $\lambda \in K$. Man definiert auf $\mathrm{Mat}_{m\times n}(K)$ koeffizientenweise Addition und Skalarmultiplikation.

1.4 Satz
$(\mathrm{Mat}_{m\times n}(K), +, \cdot\,)$ ist ein K-Vektorraum der Dimension $\dim_K(\mathrm{Mat}_{m\times n}(K)) = mn$ mit Basis $\mathcal{B} = (E_{ij})_{(i,j)\in\{1,\dots,m\}\times\{1,\dots,n\}}$.

1.5 Definition (Matrizenmultiplikation)
Seien $m, n, r \in \mathbb{N}_0$. Sind

$$A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in \mathrm{Mat}_{m\times n}(K) \quad \text{und} \quad B = (b_{jk})_{\substack{j=1,\dots,n \\ k=1,\dots,r}} \in \mathrm{Mat}_{m\times r}(K)$$

, so definieren wir $C = A \cdot B$ als die Matrix $C = (c_{ik})_{\substack{i=1,\dots,m \\ k=1,\dots,r}} \in \mathrm{Mat}_{m\times r}(K)$ mit $c_{ik} = \sum_{j=1}^n a_{ij}b_{jk}$

1.7 Lemma
Für $m, n, r \in \mathbb{N}_0, A \in \mathrm{Mat}_{m\times n}(K), \mathcal{B} \in \mathrm{Mat}_{n\times r}(K)$ und $\lambda \in K$ gilt $A(\lambda \cdot B) = (\lambda \cdot A)B = \lambda \cdot AB$.

1.8 Lemma
Matrizenmultiplikation ist assoziativ: für $m, n, r, s \in \mathbb{N}_0, A \in \mathrm{Mat}_{m\times n}(K), B \in \mathrm{Mat}_{n\times r}, C \in \mathrm{Mat}_{r\times s}$ ist $A(BC) = (AB)C$.

1.9 Lemma
Für $m, n, r \in \mathbb{N}_0, A, A' \in \mathrm{Mat}_{m\times n}(K)$ und $B, B' \in \mathrm{Mat}_{n\times r}(K)$ ist $(A + A')B = AB + A'B$ und $A(B + B') = AB + AB'$.

1.10 Satz
Mit der Matrizenmultiplikation wird $\mathrm{Mat}_n(K)$ zu einem Ring mit Einselement $\mathbb{1}_n$.

1.12 Definition
Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt invertierbar oder regulär, wenn sie im Ring $\mathrm{Mat}_n(K)$ invertierbar ist, sonst singulär.

die Gruppe $\mathrm{GL}_n(K) = \mathrm{Mat}_n(K)^\times$ der invertierbaren Matrizen heißt die allgemeine lineare Gruppe.

1.14 Lemma
Für $A, A_1, A_2 \in \mathrm{Mat}_{m\times n}(K)$ und $B \in \mathrm{Mat}_{n\times r}(K)$ ist $(A_1 + A_2)^t = A_1^t + A_2^t, (A^t)^t = A$ und $(AB)^t = B^t A^t$.

1.15 Satz
Für $A \in \mathrm{GL}_n(K)$ ist $A^t \in \mathrm{GL}_n(K)$ und $(A^t)^{-1} = (A^{-1})^t$.

2 Homomorphismen von Gruppen

Seien G und H zwei multiplikativ geschriebene Gruppen.
2.1 Definition
Eine Abbildung $f : G \to H$ heißt Gruppenhomomorphismus (oder ein Homomorphismus von Gruppen), wenn für alle $x, y \in G$ gilt:

(GH) $f(xy) = f(x)f(y)$

Die Menge der Homomorphismen $f : G \to H$ bezeichnet man mit $\hom(G, H)$.

2.4 Satz
Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

(a) $f(1) = 1$

(b) Für $x \in G$ ist $f(x^{-1}) = f(x)^{-1}$

(c) Für $x_1, \dots, x_n \in G$ ist $f(x1 \dots x_n) = f(x_1) \dots f(x_n)$

(d) Ist $G_0 \le G$ eine Untergruppe, so ist $f(G_0) \le H$.

(e) Ist $H_0 \le H$ eine Untergruppe, ist ist $f^{-1}(H_0) \le G$.

2.5 Satz
Seien G_1, G_2 und G_3 Gruppen. Sind $f_1 : G_1 \to G_2$ und $f_2 : G_2 \to G_3$ Gruppenhomomorhpismen, so ist auch $f_2 \circ f_1 : G_1 \to G_3$ ein Gruppenhomomorphimus.

2.6 Definition
Ein Homomorphismus $f : G \to H$ ist ein Monomorphismus, wenn f injektiv ist, ein Epimorphismus, wenn f surjektiv ist, und ein Isomorphismus, wenn f bijektiv ist.

Die Gruppen G und H heißen isomorph, wenn es einen Isomorphismus $f : G \to H$ gibt.
Notation: $G \cong H$.

2.7 Lemma
Ist $f : G \to H$ ein Isomorphismus, so ist auch $f^{-1} : H \to G$ ein Isomorphismus.

2.8 Satz
Sei $f : G \to H$ ein Homomorphismus. Genau dann ist f ein Isomorphismus, wenn es einen Homomorphismus $f' : H \to G$ mit $f' \circ f = \mathrm{id}_G$ und $f \circ f' = \mathrm{id}_H$ gibt.

2.9 Korollar
Isomorphie von Gruppen ist eine Äquivalenzrelation: Sind G, G_1, G_2, G_3 Gruppen, so gilt:

(i) $G \cong G$ (Reflexivität)

(ii) Ist $G_1 \cong G_2$, so auch $G_2 \cong G_1$ (Symmetrie)

(iii) Ist $G_1 \cong G_2$ und $G_2 \cong G_3$, so auch $G_1 \cong G_3$. (Transitivität)

2.12 Definition
Der Kern eines Gruppenhomomorphismus $f : G \to H$ ist $\mathrm{Ker}(f) := f^{-1}(\{1\}) = \{x \in G \mid f(x) = 1\}$

2.13 Lemma
Ist $f : G \to H$ ein Homomorphismus, so ist $N := \mathrm{Ker}(f)$ eine Untergruppe von G mit $x^{-1}yx \in N$ für alle $x \in G, y \in N$.

2.14 Satz
Sei $f : G \to H$ ein Homomorphismus. Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = \{1\}$.

2.15 Definition
Ist N eine Untergruppe von G mit $x^{-1}yx \in N$ für alle $x \in G, y \in N$, so nennt man N einen Normalteiler von G.
Notation: $N \trianglelefteq G$.

3 Homomorphismus von Ringen

Seien R, S, T Ringe.

3.1 Definition
Eine Abbildung $f : R \to S$ heißt Ringhomomorphismus (oder ein Homomorphismus von Ringen), wenn für $x, y \in R$ gilt:

(RH1) $f(x + y) = f(x) + f(y)$

(RH2) $f(xy) = f(x)f(y)$

- Die Menge der Homomorphismen $f : R \to S$ wird mit $\hom(R, S)$ bezeichnet.
- Ein Homomorphismus $f : R \to S$ ist ein Monomorphismus, Epimorphismus oder Isomorphismus, wenn f injektiv, surjektiv oder bijektiv ist.
- Gibt es einen Isomorphismus $f : R \to S$, so nennt man S und R isomorph.
  Notation: $S \cong R$
- Ein Element aus $\mathrm{End}(R) := \mathrm{Hom}(R, R)$ nennt man Endomorphismus von R.
- Der Kern eines Ringhomomorphismus $f : R \to S$ ist $\mathrm{Ker}(f) := f^{-1}(\{0\})$

3.4 Satz
Sind $f : R \to S$ und $g : S \to T$ Ringisomorphismen, so ist auch $g \circ f : R \to T$ ein Ringisomorphismus.

3.5 Lemma
Ist $f : R \to S$ ein Ringisomorphismus, so auch $f^{-1} : S \to S$.

3.6 Satz
Sei $f : R \to S$ ein Ringhomomorphismus. Genau dann ist f ein Ringisomorphismus, wenn es einen Ringhomomorphismus $f' : S \to R$ mit $f' \circ f = \mathrm{id}_R$ und $f \circ f' = \mathrm{id}_S$ gibt.

3.7 Lemma
Der Kern $I := \mathrm{Ker}(f)$ eines Ringhomomorphismus $f : R \to S$ ist eine Untergruppe von $(R, +)$ und $xa \in I$ und $ax \in I$ für alle $x \in R, a \in I$.

3.8 Satz
Sei $f : R \to S$ ein Ringhomomorphismus. Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = \{0\}$.

3.9 Definition
Ist I eine Untergruppe von $(R, +)$ mit $xa \in I$ und $ax \in I$ für alle $x \in R$ und $a \in I$, so nennt man I Ideal von R und schreibt $I \trianglelefteq R$.

4 Homomorphismen von Vektorräumen

Seien V, W und U drei K-Vektorräume.

4.1 Definition (Lineare Abbildung)
Eine Abbildung $f : V \to W$ heißt (K-)linear (oder auch ein Homomorphismus von K-Vektorräumen), wenn für alle $x, y \in V$ und $\lambda \in K$ gilt:

(L1) $f(x + y) = f(x) + f(y)$ (Additivität)

(L2) $f(\lambda x) = \lambda f(x)$ (Homogenität)

- Die Menge der K-linearen Abbildungen $f \in \mathrm{Abb}(V, W)$ wird mit $\mathrm{Hom}_K(V, W)$ bezeichnet.
- Die Elemente $\mathrm{End}_K(V) := \mathrm{Hom}(V, V)$ nennt man Endomorphismus von V.
- Eine lineare Abbildung $f : V \to W$ ist ein Monomorphismus, Epimorphismus bzw. Isomorphismus, falls f injektiv, surjektiv oder bijektiv ist.
- Einen Endomorphismus $f : V \to V$, der auch Isomorphismus ist, nennt man Automorphismus von V.
  Notation: $\mathrm{Aut}_K(V)$ (Menge der Automorphismen)
- Der Kern einer linearen Abbildung $f : V \to W$ ist $\mathrm{Ker}(f) := f^{-1}(\{0\})$

4.3 Satz
Eine Abbildung $f : V \to W$ ist genau dann K-linear, wenn für alle $x, y \in V$ und $\lambda, \mu \in K$ gilt:

(L) $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$

4.5 Beispiel
Sei $V = K^n$ und $W = K^m$. Wir fassen die Elemente von V und W als Spaltenvektoren auf. Zu einer Matrix $A \in \mathrm{Mat}_{m \times n}(K)$ definieren wir eine Abbildung $f_A : V \to W$ durch $f_a(x) = Ax$.

4.6 Satz
Sei $f : V \to W$ eine K-lineare Abbildung. Dann gilt:

(a) $f(0) = 0$

(b) Für $x, y \in V$ ist $f(x - y) = f(x) - f(y)$

(c) Sind $(x_i)_{i\in I}$ aus V und $(\lambda_i)_{i\in I}$ aus K, fast alle gleich Null, so ist $f(\sum_{i\in I} \lambda_i x_i) = \sum_{i\in I} \lambda_i f(x_i)$.

(d) Ist $(x_i)_{i\in I}$ linear abhängig in V, so ist $f\big((x_i)_{i\in I}\big)$ linear abhängig in W.

(e) Ist $V_0 \subseteq V$ ein Untervektorraum, so auch $f(V_0) \subseteq W$ von W.

(f) Ist $W_0 \subseteq W$ ein Untervektorraum, so auch $f^{-1}(W) \subseteq V$ von V.

4.7 Satz
Die Komposition K-linearer Abbildungen ist wieder K-linear: sind $f : V \to W$ und $g : W \to U$ zwei K-lineare Abbildungen, so auch $g \circ f : V \to U$.

4.8 Lemma
Ist $f : V \to W$ ein Isomorphismus, so ist auch $f^{-1} : W \to V$.

4.9 Satz
Sei $f : V \to W$ linear. Genau dann ist f ein Isomorphismus, wenn eine lineare Abbildung $f' : W \to V$ existiert mit $f' \circ f = \mathrm{id}_V, f \circ f' = \mathrm{id}_W$.

4.11 Satz
Ist $f : V \to W$ eine lineare Abbildung, so ist $\mathrm{Ker}(f)$ ein Untervektorraum von V. Genau dann ist f ein Monomorphismus, wenn $\mathrm{Ker}(f) = \{0\}$.

5 Der Vektorraum der linearen Abbildungen

Seien V, W zwei K-Vektorräume.

5.1 Satz
Sei $(x_i)_{i\in I}$ eine Basis von V und $(y_i)_{i\in I}$ eine Familie in W. Dann gibt es genau eine lineare Abbildung $f : V \to W$ mit $f(x_i) = y_i$. für alle i. Diese ist durch $f(\sum_{i\in I} \lambda_i x_i) = \sum_{i\in I} \lambda_i f(x_i)$ gegeben und erfüllt

(a) $\mathrm{Im}(f) = \mathrm{span}_K \big((y_i)_{i\in I}\big)$,

(b) genau dann ist f injektiv, wenn $(y_i)_{i\in I}$ linear unabhängig ist.

5.2 Korollar
Ist V endlich dimensional, $(x_1, \dots, x_n)$ eine linear unabhängige Familie in V und $(y_1, \dots, y_n)$ eine Familie in W, so gibt es eine lineare Abbildung $f : V \to W$ mit $f(x_i) = y_i$ für alle i.

5.3 Korollar
Ist $(x_i)_{i\in I}$ eine Basis von V und $(y_i)_{i\in I}$ eine Basis von W, so gibt es genau einen Isomorphismus $f : V \to W$ mit $f(x_i) = y_i$ für alle i.

5.4 Korollar
Zwei endlichdimensionale K-Vektorräume sind genau dann zueinander isomorph, wenn sie dieselbe Dimension haben.

5.5 Korollar
Ist $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V, so gibt es genau einen Isomorphismus $\Phi_{\mathcal{B}} : K^n \to V$ mit $f(e_i) = v_i$ für $i = 1, \dots, n$. Insbesondere ist jeder endlich dimensionale K-Vektorraum V isomorph zu einem Standardvektorraum K^n, nämlich für $n = \dim(V)$.

5.6 Definition
Die Abbildung ΦB heißt Koordinatensystem zu $\mathcal{B}$. Für $v \in V$ ist $(x_1, \dots, x_n)^t = \Phi B^{-1}(v) \in K^n$ der Koordinatenvektor zu v bezüglich $\mathcal{B}$, und $x_1, \dots, x_n$ sind die Koordinaten von v bezüglich $\mathcal{B}$.

5.7 Satz
Die Menge $\mathrm{Hom}_K(V, W)$ ist ein Untervektorraum von $\mathrm{Abb}(V, W)$.

5.8 Lemma
Sei U ein weiterer K-Vektorraum. Sind $f, f_1, f_2 \in \mathrm{Hom}_K(V, W)$ und $g, g_1, g_2 \in \mathrm{Hom}_K(U, W)$, so ist $f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$ und $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$.

5.9 Korollar
Mit der Komposition wird $\mathrm{End}_K(V)$ zu einem Ring mit Einselement id_V, und $\mathrm{End}_K(V)^\times = \mathrm{Aut}_K(V)$.

5.11 Lemma
Seien $m, n, r \in \mathbb{N}$ und $A \in \mathrm{Mat}_{m\times n}(K), B \in \mathrm{Mat}_{n\times r}(K)$. Für die linearen Abbildungen $f_A \in \mathrm{Hom}_K(K^n, K^m), f_B \in \mathrm{Hom}_K(K^n, K^r), f_{AB} \in \mathrm{Mat}_K(K^r, K^m)$ gilt dann $f_{AB} = f_A \circ f_B$.

5.12 Satz
Die Abbildung $A \mapsto f_A$ liefert einen Isomorphismus von K-Vektorräumen $F_{m\times n} : \mathrm{Mat}_{m\times n}(K) \xrightarrow{\cong} \mathrm{Hom}_K(K^n, K^m)$ sowie einen Ringisomorphismus $F_{n\times n} : \mathrm{Mat}_n(K) \xrightarrow{\cong} \mathrm{End}_K(K^n)$, der GL_n auf $\mathrm{Aut}_K(K^n)$ abbildet.

6 Koordinationdarstellung lineare Abbildungen

Seinen V und W zwei endlichdimensionale K-Vektorräume mit Basen $\mathcal{B} = (x_1, \ldots, x_n)$ und $\mathcal{C} = (y_1, \ldots, y_m)$
6.1 Definition (Darstellende Matrix)
Sei $f \in \mathrm{Hom}_K(V, W)$. Für $j = 1, \ldots, n$ schreiben wir

$$f(x_j) = \sum_{i=1}^{m} a_{ij} y_i$$

mit eindeutig bestimmten $a_{ij} \in K$. Die Matrix

$$M_{\mathcal{C}}^{\mathcal{B}}(f) = (a_{ij})_{i,j} \in \mathrm{Mat}_{m\times n}(K)$$

heißt die darstellende Matrix von f bezüglich der Basen $\mathcal{B}$ und $\mathcal{C}$.

6.2 Satz
Sei $f \in \mathrm{Hom}_K(V, W)$. Die darstellende Matrix $M_{\mathcal{C}}^{\mathcal{B}}(f)$ ist die eindeutige Matrix $A \in \mathrm{Mat}_{m\times n}(K)$, für das Diagramm

$$\begin{tikzcd}
K^n \arrow[r, "f_A"] \arrow[d, "\Phi_{\mathcal{B}}"'] & K^m \arrow[d, "\Phi_{\mathcal{C}}"] \\
V \arrow[r, "f"] & W
\end{tikzcd}$$

kommutiert, d.h. für die $\Phi_{\mathcal{C}} \circ f_A = f \circ \Phi_{\mathcal{B}}$ gilt.
6.3 Korollar
Die Abbildung

$$M_{\mathcal{C}}^{\mathcal{B}} \colon \mathrm{Hom}_K(V, W) \longrightarrow \mathrm{Mat}_{m\times n}(K)$$

ist ein Isomorphismus von K-Vektorräumen.

6.4 Lemma
Sei U ein weiterer endlichdimensionaler K-Vektorraum mit Basis $\mathcal{A}$. Sind $f \in \mathrm{Hom}_K(V, W)$ und $g \in \mathrm{Hom}_K(U, V)$, so ist

$$M_{\mathcal{C}}^{\mathcal{B}}(f) \cdot M_{\mathcal{B}}^{\mathcal{A}}(g) = M_{\mathcal{C}}^{\mathcal{B}\mathcal{A}}(f \circ g).$$

6.5 Korollar
Sei $f \in \mathrm{Hom}_K(V, W)$. Genau dann ist f ein Isomorphismus, wenn $m = n$ und $M_{\mathcal{C}}^{\mathcal{B}}(f) \in \mathrm{GL}_n(K)$. In diesem Fall ist $M_{\mathcal{C}}^{\mathcal{B}}(f))^{-1} = M_{\mathcal{B}}^{\mathcal{C}}(f^{-1})$.

6.6 Korollar
Die Abbildung

$$M_{\mathcal{B}} \colon = M_{\mathcal{B}}^{\mathcal{B}} \colon \mathrm{End}_K(V) \longrightarrow \mathrm{Mat}_n(K)$$

ist ein Ringhomomorphismus, der $\mathrm{Aut}_K(V)$ auf $\mathrm{GL}_n(K)$ abbildet.

6.7 Definition (Transformationsmatrix)
Sind $\mathcal{B}$ und $\mathcal{B}'$ Basen von V, so nennt man

$$T_{\mathcal{B}'}^{\mathcal{B}} \colon = M_{\mathcal{B}'}^{\mathcal{B}}(\mathrm{id}_V) \in \mathrm{GL}_n(K)$$

die Transformationsmatrix des Basiswechsels von $\mathcal{B}$ nach $\mathcal{B}'$.

6.9 Satz (Transformationsformel)
Seien $\mathcal{B}$ und $\mathcal{B}'$ Basen von V sowie $\mathcal{C}$ und $\mathcal{C}'$ Basen von W, und sei $f \in \mathrm{Hom}_K(V, W)$. Dann ist

$$M_{\mathcal{C}'}^{\mathcal{B}'}(f) = T_{\mathcal{C}'}^{\mathcal{C}} \cdot M_{\mathcal{C}}^{\mathcal{B}}(f) \cdot \left(T_{\mathcal{B}'}^{\mathcal{B}}\right)^{-1}.$$

6.10 Korollar
Sind $\mathcal{B}$ und $\mathcal{B}'$ Basen von V und $f \in \mathrm{End}_K(V)$, so gilt

$$M_{\mathcal{B}'} = T_{\mathcal{B}'}^{\mathcal{B}} \cdot M_{\mathcal{B}}^{\mathcal{B}}(f) \cdot \left(T_{\mathcal{B}'}^{\mathcal{B}}\right)^{-1}.$$

7 Quotienträume

Seien V und W zwei K-Vektorräume und U ein Untervektorraum von V.
7.1 Definition
Ein <u>affiner Unterraum</u> von V ist eine Teilmenge der Form

$$x + U := \{x + u \colon u \in U\} \subseteq V,$$

wobei U ein beliebiger Untervektorraum von V ist und $x \in V$.

7.2 Lemma
für $x, x' \in V$ sind äquivalent:

(1) $x + U = x' + U$

(2) $x' \in x + U$

(3) $x' - x \in U$

7.3 Lemma
Sei $f \in \operatorname{Hom}_K(V, W)$ und $U \operatorname{Ker}(f)$. Für $y \in f(V)$ ist die <u>Faser</u> $f^{-1}(y) \colon = f^{-1}(\{y\})$ von f der affine Unterraum $x + U$ für ein beliebiges $x\,\mathrm{in}f^{-1}(y)$.

7.4 Beispiel
Sind $V = \mathbb{R}^2$ und $W = \mathbb{R}$ und $f(x_1, x_2) = 2x_1 - x_2$, so sind die Fasern von f genau die Geraden $L \subseteq \mathbb{R}^2$ der Steigung 2.

7.5 Lemma
Seien $x_1, x_1', x_2, x_2' \in V$ und $\lambda \in K$. Ist $x_1 + U = x_1' + U$ und $x_2 + U = x_2' + U$, so ist $(x_1 + x_2) + U = (x_1' + x_2') + U$ und $\lambda x_1 + U = \lambda x_1' + U$.

7.6 Definition (Quotientvektorraum)
Der <u>Quotientenvrktorraum</u> von V modulo U ist Menge der affinen Unterräume:

1) $V/U := \{x + U \colon x \in V\}$

2) zusammen mit Addition: $(x_1 + U) + (x_2 + U) := (x_1 + x_2) + U$

3) und der Skalarmultiplikation $\lambda \cdot (x + U) := \lambda x + U$

Definiere Abbildung $\pi_U : V \to V/U$ durch $\pi_U(x) = x + U$.

7.7 Satz
Der Quotientenraum V/U ist ein K-Vektorraum und π_U ist ein Epimorphismus mit Kern U.

7.8 Theorem (Homomorphiesatz)
Sei $f \in \operatorname{Hom}_K(V, W)$ mit $U \subseteq \operatorname{Ker}(f)$. Dann gibt es genau eine lineare Abbildung $\bar{f} : V/U \to W$ mit $f = \bar{f} \circ \pi_U$.

$$\begin{tikzcd}
V \arrow[rr, "f"] \arrow[dr, "\pi_U"'] & & W \arrow[dl, dashed, "\bar{f}"] \\
& V/U &
\end{tikzcd}$$

Diese erfüllt $\operatorname{Ker}(\bar{f}) = \operatorname{Ker}(f)/U = \{x + U \colon x \in \operatorname{Ker}(f)\}$.

7.9 Korollar
Für $f \in \operatorname{Hom}_K(V, W)$ ist $\operatorname{Im}(f) \cong V/\operatorname{Ker}(f)$. Insbesondere gilt: Ist f ein Epimorphismus, so ist $W \cong V/\operatorname{Ker}(f)$.

7.10 Satz
Seien U und U' Unterräume von V. Genau dann ist $V = U \oplus U'$, wenn $\pi_{U|U'} : U' :\to V/U$ ein Isomorphismus ist.

7.11 Korollar
Ist V endlichdimensional, so ist $\dim_K(V/U) = \dim_K(V) - \dim_K(U)$.

7.12 Korollar
Ist V endlichdimensional und $f \in \operatorname{Hom}_K(V, W)$, so ist $\dim_K(V) = \dim_K(\operatorname{Ker}(f)) + \dim_K(\operatorname{Im}(f))$.

7.13 Korollar
Ist V endlichdimensional und $f \in \operatorname{End}_K(V)$, so sind äquivalent:

(1) $f \in \operatorname{Aut}_K(V)$

(2) f ist injektiv

(3) f ist surjektiv

8 Rang

V und W endlichdimensional K-Vektorräume, $F \in \mathrm{Hom}_K(V, W)$.

8.1 Definition
Der Rang einer Abbildung f ist $\mathrm{rank}(f) := \dim_K(\mathrm{Im}(f))$.

8.3 Lemma
Sei U ein weiterer K-Vektorraum und $g \in \mathrm{Hom}_K(U, V)$.

(a) Ist g surjektiv, so ist $\mathrm{rank}(f \circ g) = \mathrm{rank}(f)$

(b) Ist f surjektiv, so ist $\mathrm{rank}(f \circ g) = \mathrm{rank}(g)$

8.4 Satz
Sei $r \in \mathbb{N}_0$. Genau dann ist $\mathrm{rank}(f) = r$, wenn es Basen $\mathcal{B}$ von V und $\mathcal{C}$ von W gibt, für die $M_{\mathcal{B}}^{\mathcal{C}} = E_r := \sum_{i=1}^{r} E_{ii}$.

8.5 Definition
Der Rang einer Matrix $A \in \mathrm{Mat}_{m\times n}$ ist $\mathrm{rank}(A) := \mathrm{rank}(f_A)$, wobei $f_A : K^n \to K^m$ die durch A beschriebene lineare Abbildung ist.

8.6 Bemerkung
Sei $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{m\times n}(K)$.

- fasst Spalten $a_j = (a_{1j}, \dots, a_{mj})^t$ als Elemente des K^m auf und definiert den Spaltenraum $\mathrm{SR}(A) = \mathrm{span}_{\mathrm{K}}(a_1, \dots, a_n) \subseteq K^m$.
- entsprechend definieren die Zeilen $\tilde{a}_i = (a_{i1}, \dots, a_{in})$ und definiert den Zeilenraum $\mathrm{ZR}(A) = \mathrm{span}_{\mathrm{K}}(a_1, \dots, a_m^t) \subseteq K^n$

Dann gelten noch:

- $\mathrm{Im}(f_A) = \mathrm{SR}(A)$ und damit $\mathrm{rank}(A) = \dim_K(\mathrm{SR}(A))$.
- $\mathrm{SR}(A^t) = \mathrm{ZR}(A)$, deshalb $\mathrm{rank}(A^t) = \dim_K(\mathrm{ZR}(A))$

8.7 Lemma
Ist $A \in \mathrm{Mat}_{m\times n}(K), S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ mit $SAT = E_r$, wobei $r = \mathrm{rank}(A)$.

8.8 Satz
Für jedes $A \in \mathrm{Mat}_{m\times n}(K)$ gibt es $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n(K)$ mit $SAT = E_r$, wobei $r = \mathrm{rank}(A)$.

8.9 Korollar
Seien $A, B \in \mathrm{Mat}_{m\times n}(K)$. Genau dann gibt es $S \in \mathrm{GL}_m(K)$ und $T \in \mathrm{GL}_n$ mit $B = SAT$, wenn $\mathrm{rank}(A) = \mathrm{rank}(B)$.

8.10 Satz
Für $A \in \mathrm{Mat}_{m\times n}(K)$ ist $\mathrm{rank}(A) = \mathrm{rank}(A^t)$.

8.11 Korollar
Für $A \in \mathrm{Mat}_n(K)$ sind äquivalent:

(1) $A \in \mathrm{GL}_n(K)$, d.h. A sind linear unabhängig

(2) $\mathrm{rank}(A) = n$

(3) Die Zeilen von A sind linear unabhängig.

(4) Die Spalten von A sind linear unabhängig.

(5) Es gibt $S \in \mathrm{GL}_n(K)$ mit $SA = \mathbb{1}_n$

(6) Es gibt $T \in \mathrm{GL}_n(K)$ mit $AT = \mathbb{1}_n$

9 Lineare Gleichungssysteme

Sei $A \in \mathrm{Mat}_{m\times n}(K)$ und $b \in K^m$.

9.1 Definition
Unter einem lineare Gleichungssystem verstehen wir eine Gleichung der Form

$$Ax = b.$$

Dieses heißt homogen, wenn $b = 0$, sonst inhomogen, und

$$L(A, b) = \{x \in K^n \colon Ax = b\}$$

ist sein Lösungsraum.

9.3 Bemerkung

- homogene System $Ax = 0$ hat als Lösungsraum den <u>Untervektorraum</u> $L(A,0) = \mathrm{Ker}(f_A)$ der Dimension $\dim_K(L(A,0)) = n - rk(A)$.
- inhomogene System $Ax = b$ hat entweder $L(A,b) = \emptyset$, oder <u>affine Unterraum</u> $L(A,b) = f_A^{-1}(b) = x_0 + L(A,0)$, $x_0 \in L(A,b)$ bel.
- erhält alle Lösungen des inhomogenen Systems, wenn eine Lösung des inhomogenen Systems und alle Lösungen des homogenen Systems
- Im Klartext! Wie sieht der Lösungsraum aus?
  Die Anzahl der Lösungen lässt sich dann an den b_i ablesen.
  - Ist mindestens eines der $b_{k+1}, \ldots, b_m$ ungleich null, so gibt es keine Lösung.
  - Sind alle $b_{k+1}, \ldots, b_m$ gleich null (oder $k = m$) so gilt:
    * Ist $k = n$, so ist das Gleichungssystem eindeutig lösbar.
    * Ist $k < n$, gibt es unendlich viele Lösungen. Der Lösungsraum hat die Dimension $n - k$.

9.4 Definition
Die Matrix $A = (a_{ij})_{i,j}$ hat <u>Zeilenstufenform</u>, wenn es $0 \leq r \leq m$ und $1 \leq k_1 < k_2 < \cdots < k_r \leq n$ gibt mit:

(i) für $1 \leq i \leq r$ und $1 \leq j < k_i$ ist $a_{ij} = 0$

(ii) für $1 \leq i \leq r$ ist $a_{ik_i} \neq 0$ (sogenanntes <u>Pivotelement</u>)

(iii) für $1 < i \leq m$ und $1 \leq j < n$ ist $a_{ij} = 0$

$$\begin{pmatrix} 0 & \ldots & 0 & a_{1k_1} & * & \ldots & \ldots & * \\ 0 & \ldots & \ldots & 0 & a_{2k_2} & * & \ldots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & a_{rk_r} \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix}$$

9.5 Lemma
Sei A in Zeilenstufenform wie in 9.4. Dann ist $f = rk(A)$.

9.6 Satz
Sei A in Zeilenstufenform wie in 9.4.

(a) Ist $b_i \neq 0$ für ein $r < i \leq m$, so ist $L(A,b) = \emptyset$.

(b) Ist $b_i = 0$ für alle $r < i \leq m$, so erhält man alle $x \in L(A,b)$, indem erst $x_j \in K$ für $j \in \{1, \ldots, n\} \setminus \{k_1, \ldots, k_r\}$ beliebig wählt unf für $i = r, \ldots, 1$ rekursiv

$$x_{k_i} = a_{ik_i}^{-1} \cdot \left(b_i - \sum_{j=k_i+1}^{n} a_{ij} x_j \right)$$

setzt.

9.7 Definition (Elementarmatrizen)
Für $i,j \in \{1, \ldots, m\}$ mit $i \neq j, \lambda \in K^\times$ und $\mu \in K$ definiere $m \times m$-Matrizen

$$\begin{aligned} S_i(\lambda) &:= \mathbb{1}_m + (\lambda - 1) \cdot E_{ii} = \mathrm{diag}(1, \ldots, 1, \lambda, 1, \ldots, 1), \\ Q_{i,j}(\mu) &:= \mathbb{1}_m + \mu E_{ii}, \\ P_{i,j} &:= \mathbb{1}_m + E_{ij} + E_{ji} - E_{ii} - E_{jj}. \end{aligned}$$

9.8 Lemma
Es sind $S_i(\lambda), Q_{ij}(\mu), P_{i,j} \in \mathrm{GL}_m(K)$: Es ist $S_i(\lambda^{-1}) = S_1(\lambda^{-1}), Q_{i,j}(\mu)^{-1} = Q_{i,j}(-\mu), P_{i,j}^{-1} = p_{i,j}$. Insbesondere gilt: Ist E eine der Elementarmatrizen $S_i(\lambda), Q_{i,j}(\lambda), P_{i,j}$, so ist $\mathrm{ZR}(A)$ und $L(EA,0) = L(A,0)$, insbesondere $\mathrm{rank}(EA) = \mathrm{rank}(A)$.

9.9 Theorem (Eliminationsverfahren von Gauß)
Zu jeder Matrix $A \in \mathrm{Mat}_{m \times n}(K)$ gibt es $l \in \mathbb{N}_0$ und Elementarmatrizen $E_1, \ldots, E_l$ vom Typ II, III, für die $E_l \cdots E_1 A$ in Zeilenstufenform.

9.11 Korollar
Zu jeder Matrix $A \in \mathrm{Mat}_{m \times n}(K)$ gibt es eine invertierbare Matrix $S \in \mathrm{GL}_m(K)$, für die SA in Zeilenstufenform ist.

9.13 Korollar
Jedes $A \in \mathrm{GL}_n(K)$ ist ein Produkt von Elementarmatrizen.

IV Determinanten

Sei $n \in \mathbb{N}$.

1.1 Beispiel
Für $i, j \in \{1, \dots, n\}$ mit $i \neq j$ bezeichne $\tau_{ij} \in S_n$ die Transposition $\tau_{ij}(k) = \begin{cases} j & k = i \\ i & k = j \\ k & \text{sonst} \end{cases}$

Offenbar gilt $\tau_{ij}^2 = \tau_{ij}^{-1} = \tau_{ij} = \tau_{ji}$.

1.2 Satz
Für jedes $\sigma \in S_n$ gibt es $r \in \mathbb{N}_0$ und Transposition $\tau_1, \dots, \tau_r \in S_n$ mit $\sigma = \tau_1 \cdots \tau_r$.

1.3 Definition
Sei $\sigma \in S_n$, dann

(1) Ein Fehlstand von σ ist ein Paar (i, j) mit $1 \leq i \leq j \leq n$ und $\sigma(i) > \sigma(j)$

(2) Das Vorzeichen (oder Signum) von σ ist $\operatorname{sgn}(\sigma) = (-1)^{f(\sigma)} \in \{+1, -1\} = \mu_2$, wobei $f(\sigma)$ die Anzahl der Fehlstände von σ ist

(3) Man nennt σ gerade, wenn $\operatorname{sgn}(\sigma) = +1$, sonst ungerade

1.4 Beispiel
(a) Genau dann hat σ keine Fehlstände, wenn $\sigma = \mathrm{id}$ und insbesondere gilt $\operatorname{sgn}(\mathrm{id}) = +1$.

(b) die Permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_n$ hat Fehlstände $(1, 3)$ und $(2, 3)$, sonst $\operatorname{sgn}(\sigma) = (-1)^2 = 1$

(c) Die Transposition $\tau_{1,3} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, hat Fehlstände $(1, 2), (2, 3)$ und $(1, 3)$, somit $\operatorname{sgn}(\tau_{1,3}) = (-1)^3 = -1$

(d) Eine Transposition $\tau_{ij} \in S_n$ ist ungerade. Ist $i < j$, so sind die Fehlstände $(i, i+1), \dots, (i, j)$ und $(i+1, j), \dots, (j-1, j)$ also $j - (i+1) + i + (j-1) + 1 - (i+1) = 2(j-i) - 1$ viele

1.5 Lemma
Für $\sigma \in S_n$ ist $\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{Q}$

1.6 Satz
Die Abbildung $\operatorname{sgn} : S_n \to \mathbb{Z}^\times = \mu_2$ ist ein Gruppenhomomosphismus.

1.7 Korollar
Für $\sigma \in S_n$ ist $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.

1.8 Korollar
Sei $\sigma \in S_n$. Sind $\tau_1, \dots, \tau_r$ Transpositionen mit $\sigma = \tau_1 \cdots \tau_r$, so ist $\operatorname{sgn}(\sigma) = (-1)^r$

1.9 Korollar
Die geraden Permutationen

$$A_n := \{\sigma \in S_n \colon \operatorname{sgn}(\sigma) = +1\}$$

bilden einen Normalteiler der S_n, genannt die alternierende Gruppe A_n. Ist $\tau \in S_n$ mit $\operatorname{sgn}(\tau) = -1$, so gilt für $A_n\tau := \{\sigma\tau \colon \sigma \in A_n\}$:

- $A_n \cup A_n\tau = S_n$ und
- $A_n \cap A_n\tau = \emptyset$

2 Determinanten

Sei $n \in \mathbb{N}$.

2.1 Bemerkung
Wir werden nun auch Matrizen mit Koeffzienten im Ring R anstatt K betrachten. Mit der gewohnten Additon und Multiplikation bilden die $n \times n$-Matrizen einen Ring $\mathrm{Mat}_n(R)$ und wir definieren wieder $\mathrm{GL}_n(R) = \mathrm{Mat}_n(R)^\times$.

2.2 Bemerkung
- $(a_1, \dots, a_n) \in R^m$ Spaltenvektoren, so bezeichnen wir mit $A = (a_1, \dots, a_n) \in \mathrm{Mat}_{m \times n}(R)$ die Matrix mit Spalten $(a_1, \dots, a_n)$
- $(\tilde{a}_1, \dots, \tilde{a}_m) \in R^n$ Spaltenvektoren, so bezeichnen wir mit $\tilde{A} = (\tilde{a}_1, \dots, \tilde{a}_m) \in \mathrm{Mat}_{m \times n}(R)$ die Matrix mit Zeilen $(\tilde{a}_1, \dots, \tilde{a}_m)$

2.3 Bemerkung
Wir hatten in III.2.15 definiert:

$$\det A = ad - bc, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(K)$$

und festgestellt: $\det A \neq 0 \Leftrightarrow A \in \mathrm{GL}_2(K)$.
Interpretation in $\mathbb{R}^2$ (Determinante von A, ist die Fläche, welche aufgespannt wird von $x_1 = (a,b)$ und $x_2 = (c,d)$, siehe Bild)

Bemerkung

(i) Für $\lambda \in R$ ist $\det(\lambda x_1, x_2) = \det(x_1, \lambda x_2) = \lambda \det(x_1, x_2)$
und für $x_i = \tilde{x}_1 + \tilde{x}_2$ ist

a) $\det(x_1, x_2) = \det(\tilde{x}_1, x_2) + \det(\tilde{x}_2, x_2)$

b) $\det(x_1, x_2) = \det(x_1, \tilde{x}_1) + \det(\tilde{x}_1, x_2)$.

(ii) Ist $x_1 = x_2$, so ist $\det A = 0$.

(iii) $\det \mathbb{1}_2 = 1$.

Sei R kommutativer Ring mit Einselement, K Körper und $n \in \mathbb{N}$.

2.5 Definition
Eine Abbildung $\delta : \mathrm{Mat}_n(R) \to R$ heißt Determinantenabbildung, wenn gilt:

(D1) δ ist linear in jeder Zeile:
Sind $a_1, \ldots, a_n$ die Zeilen von $A \in \mathrm{Mat}_n(R)$ und ist $i \in \{1, \ldots, n\}$ und $a_i = \lambda^{'} a^{'} + \lambda^{''} a^{''}$ mit $\lambda^{'}, \lambda^{''} \in R$ und Zeilenvektoren $a_i^{'}, a_i^{''}$, so ist

$$\delta(A) = \lambda^{'} (a_1^{'}, \ldots, a_i^{'}, \ldots, a_n^{'}) + \lambda^{''} (a_1^{''}, \ldots, a_i^{''}, \ldots, a_n^{''})$$

(D2) δ ist alternierend. Sind $a_1, \ldots, a_n$ die Zeilen von $A \in \mathrm{Mat}_R$ und $i, j \in \{1, \ldots, n\}, i \neq j$, mit $a_i = a_j$, so ist $\delta(A) = 0$

(D3) δ ist normiert $\delta(\mathbb{1}_n)$

2.6 Beispiel
Sei $\delta : \mathrm{Mat}_n(K) \to K$ eine Determinantenabbildung. Ist $A \in \mathrm{Mat}_n(K)$ nicht invertierbar so ist die Zeile $a_1, \ldots, a_n$ von A linear abhängig, es gibt also i mit $a_i = \sum_{j=1} \lambda_j a_j$ mit $(\lambda_i \in K)$. Es folgt

$$\begin{aligned}\delta(A) = \delta(a_1, \ldots, a_n) &\overset{(D1)}{=} \sum_{j=1} \lambda_j \delta(a_1, \ldots, a_j, \ldots, a_n) \\ &\overset{(D2)}{=} \sum_{j=1} \lambda_j \cdot 0 = 0\end{aligned}$$

2.7 Lemma
Erfüllt die Abbildung $\delta : \mathrm{Mat}_n(R) \to R$ die Axiome (D1) und somit für jedes $\sigma \in S_n$ und Zeilenvektoren $a_1, \ldots, a_n$:

$$\delta(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) = \mathrm{sgn}(\sigma) \cdot \delta(a_1, \ldots, a_n).$$

2.8 Lemma
Erfüllt die Abbildung $\delta : \mathrm{Mat}_n(R) \to R$ die Axiome (D1) und (D2), so gilt für $A = ({a_{ij}}_{i,j}) \in \mathrm{Mat}_n(R)$

$$\delta(A) = \delta(\mathbb{1}_n) \cdot \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

2.9 Theorem
Es gibt genau eine Determinantenabbildung

$$\det \mathrm{Mat}_n(R) \to R$$

und diese ist gegeben durch die LEIBNIZ-Formel.

2.10 Beispiel
(a) $n = 2$, damit $S_2 = \{\mathrm{id}, \tau_{12}\}$

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \sum_{\sigma \in S_2} a_{1\sigma(1)} a_{2\sigma(2)} = a_{11}a_{22} - a_{12}a_{21}$$

(b) $n = 3$, damit $s_3 = \{\mathrm{id}, \tau_{12}, \tau_{13}, \tau_{23}, \sigma_1, \sigma_2\}$ mit $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
$A_3 = \{\mathrm{id}, \sigma_1, \sigma_2\}$ und $S_3 \setminus A_3 = \{\tau_{12}, \tau_{13}, \tau_{23}\}$

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= \sum_{\sigma \in S_3} a_{1\sigma(1)} a_{2\sigma(2)} a_{2\sigma(3)} a_{2\sigma(2)} \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12} \end{aligned}$$

die sogenannte Regel von Sarrus.

(c) Ist $A = (a_{ij})_{i,j}$ eine obere Dreiecksmatrix (siehe A108), also $a_{ij} = 0$ für $i = j$, so ist

$$\det A = \det \begin{pmatrix} a_{ii} & \cdots \\ 0 & \ddots \; a_{nn} \end{pmatrix} = \prod_{i=1}^{n} a_{ii}$$

(d) Für $i \neq j, \lambda \in K^\times, \mu \in K$ ist $\det(S_i(\lambda)) = \lambda, \det(Q_{ij}(\mu)) = 1, \det(P_{ij}) = -1$
(gibt nur eine Permutation $\sigma_{ij} = -1$ und $\mathrm{sgn}(\sigma_{ij}) = -1$)

(e) Ist A Blockmatrix[Matrix] der Gestalt

$$A = \begin{bmatrix} A_1 & C \\ 0 & A_2 \end{bmatrix} \text{ mit } A_1, A_2, C \in \mathrm{Mat}_n(R)$$

So ist $\det(A) = \det(A_1) \cdot \det(A_2) + 0$.

2.11 Korollar
Für $A \in \mathrm{Mat}_n(R)$ ist $\det(A) = \det(A^t)$. Insbesondere erfüllt det die Axiome (D1) und (D2) auch für Spalten statt Zeilen.

2.12 Theorem (Determinantenmultiplikationssatz)
Für $A, B \in \mathrm{Mat}_n(R)$ ist $\det(AB) = \det(A) \cdot \det(B)$.

2.13 Korollar
Die Abbildung $\det : \mathrm{Mat}_n(R) \to R$ schränkt sich zu einem Gruppenhomomorphismus $\mathrm{GL}_n(R) \to R^\times$. Ist $R = K$ ein Körper, so ist $A \in \mathrm{Mat}_n(K)$ also genau dann invertierbar, wenn $\det(A) \neq 0$, und in diesem Fall ist $\det(A^{-1}) = (\det(A))^{-1}$.

2.14 Korollar
Die Matrizen von Determinanten 1 bilden einen Normalteiler $\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) \colon \det(A)\}$ der allgemeinen linearen Gruppe, die sog. spezielle lineare Gruppe.

2.15 Korollar
Elementare Zeilenumformungen von Typ II ändern die Determinante der Matrix A nicht. Elementare Zeilenumformungen von Typ III ändern nur das Vorzeichen.

V Minoren

Sei $m, n \in \mathbb{N}$.

1.1 Definition
Sei $A = (a_{ij})_{i,j} \in \mathrm{Mat}_n(R)$. Für $i, j \in \{1, \dots, n\}$ definiere die $n \times n$-Matrix

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1j-1} & 0 & a_{1j+1} & \dots & a_{1n} \\ \vdots & & & \vdots & & & \vdots \\ a_{i-11} & \dots & a_{i-1j-1} & 0 & a_{i-1j+1} & \dots & a_{i-1n} \\ 0 & \dots & 0 & 1 & a_{i-1j+1} & \dots & 0 \\ a_{i+11} & \dots & a_{i+1j-1} & 0 & a_{i+1j+1} & \dots & a_{i+1n} \\ \vdots & & & \vdots & & & \vdots \\ a_{n1} & \dots & a_{nj-1} & 0 & a_{nj+1} & \dots & a_{mn} \end{pmatrix}$$

die durch Ersetzen der i-ten Zeile durch e_j und j-ten Spalte durch e_i aus A hervorgeht,

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j+1} & \dots & a_{i-1n} \\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j+1} & \dots & a_{i+1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{nj-1} & a_{nj+1} & \dots & a_{mn} \end{pmatrix}$$

die durch Streichen der i-ten Zeile und der j-ten Spalte entsteht. Weiter definiere die zu A adjungierte Matrix als $A^{\#} = (a_{ij}^{\#})_{i,j}\,\mathrm{Mat}_n(R)$, wobei $a_{ij}^{\#} = \det(A_{ij})$.

1.2 Lemma
Sei $A \in \mathrm{Mat}_n(R)$ mit Spalten $a_1, \dots, a_n$. Für $i, j \in \{1, \dots, n\}$ gilt:

(a) $\det(A_{ij}) = (-1)^{+j} \det(A_{ij}^{'})$

(b) $\det(A_{ij}) = \det(a_1, \dots, a_{j-1}, e_i, a_{j+1}, \dots, a_n)$

1.3 Satz
Für $A \in \mathrm{Mat}_n(R)$ ist $A^{\#}A = A \cdot A^{\#} = \det(A)\mathbb{1}_n$.

1.4 Korollar
Es ist $\mathrm{GL}_n(R) = \{A \in \mathrm{Mat}_n(R) \colon \det(A) \in R^{\times}\}$ und für $\mathrm{GL}_n(R)$ ist

$$A^{-1} = \frac{1}{\det(A)} A^{\#}.$$

1.5 Korollar
Sei $A = (a_{ij})_{i,j} \in \mathrm{Mat}_n(R)$. Für jedes $i \in \{1, \dots, n\}$ gilt dir Formel für die Entwicklung nach der i-ten Zeile

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

für jedes $j \in \{1, \dots, n\}$ gilt die Formel für die Entwicklung nach der j-ten Spalte

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

1.6 Korollar (Cramersche Regel)
Sei $A \in \mathrm{GL}_n(R)$ mit Spalten $a_1, \dots, a_n$ und sei $b \in R^n$. Weiter sei $x = (x_1, \dots, x_n)^t \in R^n$die (eindeutige) Lösung des Linearen Gleichungssystems $Ax = b$. Dann ist für $i \in \{1, \dots, n\}$:

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

1.7 Definition (Minoren)
Sei $A(a_{ij})_{i,j} \in \mathrm{Mat}_n(R)$ und $1 \leq r \leq m, 1 \leq s \leq n$. Eine $r \times s$- Teilmatrix von A ist eine Matrix der Form $(a_{i\mu, j\nu})_{\mu,\nu} \in \mathrm{Mat}_{r \times s}(R)$ mit $1 \leq i_1, \dots, i_r \leq m$ und $1 \leq j_1, \dots, j_r \leq n$. Ist $A^{'}$ eine $r \times s$ -Teilmatrix A, so bezeichnet man $\det(A^{'})$ als einen r-Minor von A.

1.8 Beispiel
Ist $A \in \mathrm{Mat}_n(R)$ und $i, j \in \{1, \ldots, n\}$, so ist A'_{ij} eine Teilmatrix von A und $\det(A'_{i,j}) = (-1)^{i+j} a^{\#}_{ji}$ ein $(n-1)$-Minor von A.

1.9 Satz
Sei $A \in \mathrm{Mat}_{m \times n}(K)$ und $r \in \mathbb{N}$. Genau dann is $\mathrm{rank}(A) \geq r$, wenn es eine $r \times r$ Teilmatrix A' von A mit $\det(A') \neq 0$ gibt.

1.10 Korollar
Sei $A \in \mathrm{Mat}_{m \times n}(K)$. Der Rang von A ist das größte $r \in \mathbb{N}$, für das A eine von Null verschiedenen r-Minor hat.

Index