# Lineare Algebra I
# (Lehramt Gymnasium)

**Technische Universität München, WS 2012/13**

Vorlesung: Caroline Lasser

(aktualisiert am 1. Februar 2013)

## Inhaltsverzeichnis

# Literatur


[AZ] Aigner, Martin und Ziegler, Günter, Das BUCH der Beweise, Springer-Verlag, 3. Auflage (2010)

[B] Bosch, Siegfried, Lineare Algebra, Springer-Verlag, 4. Auflage (2008)

[Ded] Dedekind, Richard, Was sind und was sollen die Zahlen? (1888), in Richard Dedekind, Gesammelte mathematische Werke, herausgegeben von Robert Fricke, Emmy Noether, Öystein Ore, Dritter Band, Vieweg (1932)

[Dei] Deiser, Oliver, Grundbegriffe der wissenschaftlichen Mathematik, Springer-Verlag (2010)

[Dy] Dyck, Walther, Gruppentheoretische Studien, Mathematische Annalen 20(1): 1-44 (1882)

[E] Euler, Leonhard, Introductio in analysin infinitorum, Band 1 (E101) von 2 Bänden (1748). Deutsche Übersetzung von Hermann Maser, Springer-Verlag (1885)

[F] Fischer, Gerd, Lineare Algebra, Vieweg, 17. Auflage (2010)

[FL] Fischer, Gerd, Lernbuch Lineare Algebra und Analytische Geometrie, Springer Spektrum, 2. Auflage (2012)

[Fr] Frobenius, Ferdinand Georg, Zur Theorie der linearen Gleichungen, Journal für die reine und angewandte Mathematik 129: 175–180 (1905)

[G] Gauß, Carl Friedrich, Theoria residuorum biquadraticorum, commentatio secunda (1831), Werke Band 2: 93–148

[Gr] Grassmann, Hermann, Die lineare Ausdehnungslehre, Verlag von Otto Wigand, 2. Auflage (1878)

[KM] Karpfinger, Christian und Meyberg, Kurt, Algebra (Gruppen – Ringe – Körper), Spektrum Akademischer Verlag, 2. Auflage (2010)

[N] Noether, Emmy, Idealtheorie in Ringbereichen, Mathematische Annalen 83(1–2): 24–66 (1921)

[W] Weyl, Hermann, Raum Zeit Materie, Springer-Verlag, 5. Auflage (1922)

# 1 Gruppen

## 1.1 Natürliche Zahlen (16.10.)

**Natürliche Zahlen.** Eine Menge $\mathbb{N}$ mit ausgezeichnetem Element $0 \in \mathbb{N}$ und einer Abbildung $s : \mathbb{N} \to \mathbb{N}$ heißt *natürliche Zahlen*, wenn sie die Dedekind-Peano Axiome erfüllen: i) $s$ ist injektiv. ii) $0 \notin s[\mathbb{N}]$. iii) Erfüllt $A \subseteq \mathbb{N}$ sowohl $0 \in A$ als auch $s[A] \subseteq A$, so gilt $A = \mathbb{N}$.

**Injektive Abbildung.** Seien $A$ und $B$ Mengen. Eine Abbildung $f : A \to B$, $x \mapsto f(x)$ heißt *injektiv*, falls für alle $x, y \in A$ aus $f(x) = f(y)$ stets $x = y$ folgt. Die Abbildung $f_1 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$ ist injektiv. Die Abbildung $f_2 : \mathbb{N} \to \mathbb{N}$, $f_2(x) = x - 1$ für $x \geq 1$, $f_2(0) = 0$, ist nicht injektiv.

**Teilmengen.** Seien $M'$ und $M$ Mengen. $M'$ heißt *Teilmenge* von $M$, in Zeichen $M' \subseteq M$, falls für alle $x \in M'$ auch $x \in M$ gilt. Die natürlichen Zahlen sind eine Teilmenge der ganzen Zahlen, die wiederum der rationalen Zahlen, und die der reellen Zahlen: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

**Aussonderung.** Sei $M$ eine Menge. Dann ist $\{x \in M \mid \mathcal{E}(x)\}$ die Teilmenge von $M$, die aus allen $x \in M$ mit $\mathcal{E}(x)$ besteht. $\{x \in \mathbb{N} \mid x \text{ gerade}\} = \{0, 2, 4, \ldots\}$ ist die Menge der geraden natürlichen Zahlen.

**Bild & Urbild.** Ist $f : A \to B$, $A' \subseteq A$ und $B' \subseteq B$, so heißen

$$f[A'] = \{f(x) \mid \ x \in A'\}, \qquad f^{-1}[B'] \ = \ \{x \in M \mid f(x) \in B'\}$$

das *Bild* von $A'$ und das *Urbild* von $B'$ unter $f$. Die Abbildung $f$ heißt *surjektiv*, falls $f[A] = B$. Ist $f$ injektiv und surjektiv, so heißt $f$ *bijektiv*. $f_1$ ist nicht surjektiv, $f_2$ schon. $f_3 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$ für $x$ gerade, $x \mapsto x - 1$ für $x$ ungerade, ist bijektiv.

**Lemma.** Eine Abbildung $f : A \to B$ ist genau dann injektiv, wenn $f^{-1}(\{y\})$ für alle $y \in B$ höchstens ein Element enthält.

**Literatur.** [Ded, §6.71], [Dei, 1.2 & 2.1]

## 1.2 Halbgruppen (19.10.)

**Assoziative Verknüpfung.** Eine Abbildung $* : M \times M \to M$, $(a, b) \mapsto a * b$ auf einer Menge $M$ heißt eine *Verknüpfung* auf $M$. Eine Verknüpfung $*$ auf $M$ heißt *assoziativ*, falls $a * (b * c) = (a * b) * c$ für alle $a, b, c \in M$ gilt.

**Definition Halbgruppe.** Eine Menge $M$ mit einer assoziativen Verknüpfung $* : M \times M \to M$ heißt *Halbgruppe*. Man schreibt oft $(M, *)$.

**Verknüpfungen auf $\mathbb{N}$.** $\mathbb{N}$ mit $m * n = m + n$ oder $m * n = m \cdot n$ ist eine Halbgruppe. $m * n = m - n$ definiert keine Verknüpfung auf $\mathbb{N}$. $m * n = m^n$ ist eine Verknüpfung auf $\mathbb{N}$, aber nicht assoziativ.

**Verknüpfungen auf $\mathbb{Q}$.** $\mathbb{Q}$ mit $a*b = a \cdot b$ ist eine Halbgruppe. $a*b = \frac{1}{2}(a+b)$ ist nicht assoziativ.

**Verknüpfungen auf $\mathbb{R}^n$.** $\mathbb{R}^n$ mit $v * w = v + w = (v_1 + w_1, \ldots, v_n + w_n)$ ist eine Halbgruppe. $\mathbb{R}^2$ mit $v * w = (v_1 + w_2, v_2 + w_1)$ ist nicht assoziativ.

**Komposition.** Sind $f : A \to B$ und $g : B \to C$ Abbildungen, so heißt $g \circ f : A \to C$, $x \mapsto g(f(x))$ die *Komposition* von $g$ nach $f$.

**Lemma.** Die Komposition bijektiver Abbildungen ist bijektiv.

*Beweis.* Aus $g(f(x)) = g(f(y))$ folgt $f(x) = f(y)$ und $x = y$ für alle $x, y$, weil $g$ und $f$ injektiv sind. Also ist $g \circ f$ injektiv. Außerdem gilt $g[f[A]] = g[B] = C$ wegen der Surjektivität von $f$ und $g$. Damit ist $g \circ f$ auch surjektiv. □

**Verknüpfungen auf Abbildungen.** $M = \{f : X \to X\}$ mit $f * g = f \circ g$ ist eine Halbgruppe. Ebenso ist $M = \{f : X \to X \mid f \text{ bijektiv}\}$ mit $f * g = f \circ g$ eine Halbgruppe. Ihre Elemente heißen *Permutationen* von $X$. Für $X = \{1, \ldots, n\}$ wird die Menge der Permutionen mit $S_n$ bezeichnet.

**Kommutative Verknüpfungen.** Ein Verknüpfung $*$ auf $M$ heißt *kommutativ*, wenn $a * b = b * a$ für alle $a, b \in M$ gilt.

**Kommutative Beispiele.** $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}^n, +)$, $(S_1, \circ)$, $(S_2, \circ)$

**Literatur.** [F, 1.2], [FL, 1.2.2].

## 1.3 Gruppen (23.10.)

**Definition.** $G$ mit einer Verknüpfung $* : G \times G \to G$ heißt *Gruppe*, falls gilt: i) $G$ ist eine Halbgruppe. ii) Es gibt $e \in G$ (*neutrales* Element), so dass $e * a = a$ für alle $a \in G$ gilt. iii) Ist $e$ ein neutrales Element, so gibt es für jedes $a \in G$ ein $a' \in G$ mit $a' * a = e$ (*inverses* Element von $a$).

**Links oder rechts?** Sei $(G, *)$ eine Gruppe, $e$ ein neutrales Element, $a \in G$ und $a'$ zu $a$ invers. Dann gilt $a * a' = e$ und $a * e = a$.

*Beweis.* Sei $a''$ zu $a'$ invers. Es gilt: $aa' = (ea)a' = e(aa') = (a''a')(aa') = a''((a'a)a') = a''(ea') = a''a' = e$ und $ae = a(a'a) = (aa')a = ea = a$. □

**Kürzungsregeln.** Sei $(G, *)$ eine Gruppe, und $a, x, y \in G$. Es gilt: i) Aus $a * x = a * y$ folgt $x = y$. ii) Aus $x * a = y * a$ folgt $x = y$.

*Beweis.* Sei $e$ ein neutrales Element und $a'$ zu $a$ invers. zu i) $x = ex = (a'a)x = a'(ax) = a'(ay) = (a'a)y = ey = y$. zu ii) $x = xe = x(aa') = (xa)a' = (ya)a' = y(aa') = ye = y$. □

**Lemma.** i) Das neutrale Element ist eindeutig bestimmt. ii) Das zu $a$ inverse Element ist eindeutig bestimmt (und wird mit $a^{-1}$ bezeichnet).

*Beweis.* zu i) Sind $e, \tilde{e}$ neutrale Elemente, so gilt $e\tilde{e} = e$, $e\tilde{e} = \tilde{e}$ und somit $e = \tilde{e}$. zu ii) Sind $a', \tilde{a}'$ zu $a$ invers, so gilt $\tilde{a}' = \tilde{a}'e = \tilde{a}'(aa') = (\tilde{a}'a)a' = ea' = a'$. □

**Beispiele für Gruppen.** $(\mathbb{Z}, +)$ mit $e = 0$; $(\mathbb{Q} \setminus \{0\}, \cdot)$ mit $e = 1$; $(\mathbb{R}^n, +)$ mit $e = (0, \ldots, 0)$; Permutationen bzgl. $\circ$ mit $\mathrm{id} : X \to X$, $x \mapsto x$ als $e$.

**Inverse.** Sei $G$ eine Gruppe, $a, b \in G$. Es gilt $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$, weil $a^{-1}a = e$ und $(b^{-1}a^{-1})(ab) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$.

**Gruppentafel** für zweielementige Gruppen:

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

**Literatur.** [Dy, I.1], [F, 1.2], [Dei, 3.4]

**Extemporale, 26.10.2012**
Name (anonymisiert):

Bitte bearbeiten Sie ohne Hilfsmittel in 15 Minuten die folgenden Aufgaben.

1. Formulieren Sie die Definition einer Gruppe $(G, *)$.

*Eine Menge $G$ mit einer Verknüpfung $* : G \times G \to G$ heißt Gruppe, falls gilt: i) $(G, *)$ ist eine Halbgruppe. ii) Es gibt ein neutrales Element $e \in G$, so dass $e * a = a$ für alle $a \in G$ gilt. iii) Für jedes $a \in G$ gibt es ein Inverses $a' \in G$ mit $a' * a = e$.*

2. Seien $f : A \to B$, $g : B \to C$ injektiv. Zeigen Sie, dass $g \circ f$ injektiv ist.

*Seien $x, y \in A$ mit $(g \circ f)(x) = (g \circ f)(y)$. Dies bedeutet $g(f(x)) = g(f(y))$. Weil $g$ injektiv ist, folgt $f(x) = f(y)$. Weil $f$ injektiv ist, folgt $x = y$. Also ist $g \circ f$ injektiv.*

3. Seien $f : X \to X$, $g : X \to X$ Abbildungen. Beweisen oder widerlegen Sie: $f \circ g = g \circ f$.

*Sei $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x$ und $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. Dann ist $(f \circ g)(x) = 2x^2$ und $(g \circ f)(x) = 4x^2$ für alle $x \in \mathbb{R}$. Insbesondere gilt $(f \circ g)(1) = 2 \neq (g \circ f)(1) = 4$. Also ist die Komposition von Abbildungen nicht kommutativ.*

**Bewertung:** Maximal 2 Punkte pro Aufgabe, (5 & 6, 4, 3, 2, 1, 0) Punkte entsprechen der Note (1, 2, 3, 4, 5, 6). Bei 41 Teilnehmern gab es 5mal Note 1, 6mal 2, 7mal 3, 10mal 4, 11mal 5, 2mal 6. Durchschnitt: 3,54

## 1.4 Untergruppen (26.10.)

**Links- und Rechtstranslation.** Ist $(G, *)$ eine Gruppe und $a \in G$, so sind $l_a : G \to G$, $x \mapsto a * x$ und $r_a : G \to G$, $x \mapsto x * a$ bijektiv: injektiv wegen Kürzungsregeln, surjektiv wegen $x = r_a(xa') = l_a(a'x)$ für alle $x \in G$.

**Lemma.** Ist $(G, *)$ eine Halbgruppe und $l_a, r_a$ für alle $a \in G$ bijektiv, so ist $(G, *)$ eine Gruppe.

*Beweis.* Für $a, b \in G$ gibt es $x, y \in G$ mit $r_a(x) = a$, $l_a(y) = b$ und $x * b = x * (a * y) = (x * a) * y = a * y = b$. Das $z \in G$ mit $r_a(z) = x$ ist invers zu $a$. □

**Gruppentafel** für dreielementige Gruppen:

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

**Untergruppe.** Sei $(G, *)$ eine Gruppe. $U \subseteq G$ heißt eine *Untergruppe* von $G$, falls $U \neq \emptyset$ sowie $a * b \in U$ und $a^{-1} \in U$ für alle $a, b \in U$ gilt.

**Gruppe.** Eine Untergruppe ist eine Gruppe.

*Beweis.* $* : G \times G \to G$ erfüllt $*[U \times U] \subseteq U$ und ist auch auf $U$ assoziativ. Wegen $U \neq \emptyset$ gibt es $a \in U$ und es gilt $a^{-1} \in U$ und $e = a * a^{-1} \in U$. □

**Untergruppen von $\mathbb{Z}$.** Ist $U$ eine Untergruppe von $(\mathbb{Z}, +)$, so gibt es genau ein $m \in \mathbb{N}$ mit $U = m\mathbb{Z} := \{m \cdot x \mid x \in \mathbb{Z}\}$.

*Beweis.* $U = \{0\} = 0 \cdot \mathbb{Z}$. Andernfalls gibt es positive ganze Zahlen in $U$. Sei $m$ die kleinste von ihnen. Dann gilt $m\mathbb{Z} \subseteq U$. Sei $n \in U$. Wir schreiben $n = qm + r$ mit $q \in \mathbb{Z}$, $0 \leq r < m$. Dann ist $r \in U$ und somit $r = 0$ und $U \subseteq m\mathbb{Z}$. □

**Äquivalenzrelation.** Sei $M$ eine Menge. $R \subseteq \{(x, y) \mid x, y \in M\}$ heißt *Äquivalenzrelation* auf $M$ falls für alle $x, y, z \in M$ gilt: i) $(x, x) \in R$. ii) Aus $(x, y) \in R$ folgt $(y, x) \in R$. iii) Aus $(x, y) \in R$ und $(y, z) \in R$ folgt $(x, z) \in R$. D.h. eine Äquivalenzrelation ist reflexiv, symmetrisch und transitiv.

**Lemma.** Sei $U$ eine Untergruppe von $G$. Dann definieren $x \sim_U y$, falls $xy^{-1} \in U$, und $x \sim^U y$, falls $x^{-1}y \in U$, zwei Äquivalenzrelationen auf $G$.

*Beweis.* für $\sim_U$: i) $xx^{-1} = e \in U$. ii) Aus $xy^{-1} \in U$ folgt $yx^{-1} = (xy^{-1})^{-1} \in U$. iii) Aus $xy^{-1} \in U$ und $yz^{-1} \in U$ folgt $xz^{-1} = (xy^{-1})(yz^{-1}) \in U$. □

**Teilen mit Rest.** Für $U = m\mathbb{Z}$ sind $\sim_U$ und $\sim^U$ gleich. Für $m > 0$ gilt $x \sim_{m\mathbb{Z}} y$ genau dann, wenn $x = q_x m + r$, $y = q_y m + r$ mit $q_x, q_y \in \mathbb{Z}$, $0 \leq r < m$.

**Literatur.** [F, 1.2], [FL, 1.1.5, 1.2.5], [Dei, 1.3, 3.1 & 3.4]

## 1.5 Faktorgruppen (30.10.)

**Nebenklassen.** Sei $U$ eine Untergruppe von $G$. Für $a \in G$ gilt

$$\{g \in G \mid a \sim_U g\} = \{g \in G \mid \exists u \in U : ag^{-1} = u\} = \{ua \mid u \in U\} = Ua,$$
$$\{g \in G \mid a \sim^U g\} = \{g \in G \mid \exists u \in U : a^{-1}g = u\} = \{au \mid u \in U\} = aU.$$

Diese Äquivalenzklassen heißen die *Rechts- und Linksnebenklassen* von $a$.

**Zerlegung.** Es gilt $G = \bigcup_{a \in G} aU$, wobei die Vereinigung disjunkt ist. Gleiches gilt für die Rechtsnebenklassen.

*Beweis.* Ist $aU \cap bU \neq \emptyset$, so gibt es $g \in G$ mit $a \sim^U g$, $b \sim^U g$. Wegen Symmetrie und Transitivität gilt $a \sim^U b$ und $aU = bU$. Also ist entweder $aU \cap bU = \emptyset$ oder $aU = bU$. Für $a \in G$ ist $a = ae \in aU$ und somit $G = \bigcup_{a \in G} aU$. □

**Restklassen.** Für $G = \mathbb{Z}$, $U = m\mathbb{Z}$, $m > 0$ und $a \in \mathbb{Z}$ ist $aU = Ua = a + m\mathbb{Z}$ und enthält alle ganzen Zahlen, die nach Division durch $m$ den gleichen Rest wie $a$ haben. $a + m\mathbb{Z}$ heißt *Restklasse* von $a$ modulo $m$. Es ist $\mathbb{Z} = (0 + m\mathbb{Z}) \cup \cdots \cup (m - 1 + m\mathbb{Z})$, und die Vereinigung ist disjunkt.

**Normalteiler.** Sei $U$ eine Untergruppe von $G$. Gilt $aU = Ua$ für alle $a \in G$, so ist $\sim_U$ gleich $\sim^U$, und $U$ heißt *Normalteiler* von $G$.

**Lemma.** Ist $U$ eine Untergruppe von $G$, so sind äquivalent: i) $U$ ist Normalteiler von $G$. ii) $aU * bU = (ab)U$ für alle $a, b \in G$. iii) $aUa^{-1} = U$ für alle $a \in G$.

*Beweis.* i)⇒ii): $aU * bU = \{aubv \mid u, v \in U\} = \{abwv \mid v, w \in U\} = (ab)U$. ii)⇒iii): $aU = U * aU = \{uav \mid u, v \in U\} \supseteq Ua$ und $a^{-1}U \supseteq Ua^{-1}$, woraus $aUa^{-1} \supseteq U$ und $U \supseteq aUa^{-1}$ folgt. iii)⇒i): $aU = a(a^{-1}Ua) = Ua$. □

**Faktorgruppe.** Ist $U$ ein Normalteiler von $G$, so definiert

$$G/U = \{aU \mid a \in G\}, \qquad aU * bU = (ab)U$$

eine Gruppe, die sogenannte *Faktorgruppe* von $G$ bezüglich $U$. Das neutrale Element ist $U$, und das zu $aU$ Inverse ist $a^{-1}U$.

**Zyklische Gruppen.** Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z}$, $m > 0$, heißt die *zyklische Gruppe* der Ordnung $m$. Sie ist abelsch und enthält $m$ Elemente.

**Literatur.** [F, 1.2], [Dei, 1.3 & 3.4], [KM, 3.2]

# 2 Ringe und Körper

## 2.1 Ringe (02.11.)

**Definition.** Eine Menge $R$ mit zwei Verknüpfungen $+ : R \times R$, $(a, b) \mapsto a + b$ und $\cdot : R \times R$, $(a, b) \mapsto a \cdot b$ heißt *Ring*, falls gilt: i) $(R, +)$ ist abelsche Gruppe. ii) $(R, \cdot)$ ist eine Halbgruppe. iii) Es gelten die Distributivgesetze $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in R$.

**Beispiele.** $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sind mit der üblichen Addition und Multiplikation Ringe. Die Menge der Funktionen $\{f : \mathbb{R} \to \mathbb{R}\}$ sind mit $(f+g)(x) = f(x)+g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$ ein Ring. $\mathbb{Z}/m\mathbb{Z} = \{[0], \ldots, [m-1]\}$ ist mit $[a]+[b] = [a+b]$, $[a] \cdot [b] = [a \cdot b]$ ein Ring.

**Multiplikationstafeln.** $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, $\mathbb{Z}/\mathbb{Z} = \{0\}$. Für $\mathbb{Z}/m\mathbb{Z}$, $m = 2, 3, 4$ gilt:

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

| $\cdot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Wegen $2 \cdot 2 = 0$ ist $((\mathbb{Z}/4\mathbb{Z}) \setminus \{0\}, \cdot)$ keine Gruppe.

**Restklassenringe.** Ein Ring $R$ heißt *nullteilerfrei*, wenn für alle $a, b \in R$ aus $a \cdot b = 0$ stets $a = 0$ oder $b = 0$ folgt. $\mathbb{Z}/m\mathbb{Z}$ ist genau dann nullteilterfrei, wenn $m$ eine Primzahl ist.

*Beweis.* Ist $m$ eine Primzahl und $[k] \cdot [l] = 0$, so gilt $k \cdot l = m \cdot r$ für ein $r \in \mathbb{Z}$, und $k$ oder $l$ hat $m$ als Primfaktor, was $[k] = 0$ oder $[l] = 0$ bedeutet. Also ist $\mathbb{Z}/m\mathbb{Z}$ nullteilerfrei. Ist $m$ keine Primzahl, so gibt es $1 < k, l < m$ mit $m = k \cdot l$. Es ist $[k] \neq 0$, $[l] \neq 0$, aber $[m] = 0$. Also ist $\mathbb{Z}/m\mathbb{Z}$ nicht nullteilerfrei. □

**Nullteilerfreie Ringe.** In einem nullteilerfreien Ring $R$ ist $R^* := R \setminus \{0\}$ bezüglich $\cdot$ ein Halbgruppe, aber nicht immer eine Gruppe: In $\mathbb{Z}$ fehlen multiplikative Inverse, in $2\mathbb{Z}$ sogar das Einselement.

**Literatur.** [N, §1], [F, 1.3], [FL, 1.3.1]

## 2.2 Komplexe Zahlen (06.11.)

**Definition.** Ein Ring $R$ heißt *Körper*, falls $(R^*, \cdot)$ ein abelsche Gruppe ist.

**Beispiele.** $\mathbb{Q}$, $\mathbb{R}$ sind Körper. Endliche, kommutative, nullteilerfreie Ringe sind Körper. Insbesondere ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper, wenn $m$ eine Primzahl ist.

*Beweis.* Wir zeigen, dass $r_a : R^* \to R^*$, $x \mapsto a \cdot x$ für alle $a \in R^*$ injektiv ist. Aus $r_a(x) = r_a(y)$ folgt $a \cdot (x - y) = 0$ und $x - y = 0$ und $x = y$. Wegen $R^*$ endlich ist $r_a$ auch surjektiv (Schubfachprinzip). □

**Definition** $\mathbb{C} = \{(x, y) \mid x, y \in \mathbb{R}\}$ mit den Verknüpfungen

$$\begin{aligned} + &: \mathbb{C} \times \mathbb{C} \to \mathbb{C},\ ((x_1, y_1), (x_2, y_2)) \mapsto (x_1 + x_2, y_1 + y_2) \\ \cdot &: \mathbb{C} \times \mathbb{C} \to \mathbb{C},\ ((x_1, y_1), (x_2, y_2)) \mapsto (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) \end{aligned}$$

ist ein kommutativer Körper mit Nullelement $(0, 0)$ und Einselement $(1, 0)$.

*Beweis.* Sei $w = x^2 + y^2$. Wir überprüfen nur, dass $(x/w, -y/w)$ zu $(x, y)$ invers ist: $(x/w, -y/w) \cdot (x, y) = (x^2/w + y^2/w, xy/w - yx/w) = (1, 0)$. □

**Polarkoordinaten.** Wir beschreiben $z = (x, y) \in \mathbb{C}$ durch den Betrag $|z| = \sqrt{x^2 + y^2}$ und den Winkel $\alpha$ zwischen $(x, y)$ und $(1, 0)$ gegen den Uhrzeigersinn gemessen: $z = |z|\mathrm{e}^{i\varphi} = |z|(\cos\varphi + i \sin\varphi)$. Die Multiplikation ist

$$\begin{aligned} & z_1 \cdot z_2 \\ &= |z_1|\,|z_2|(\cos\varphi_1 \cos\varphi_2 - \sin\varphi_1 \sin\varphi_2 + i(\cos\varphi_1 \sin\varphi_2 + \sin\varphi_1 \cos\varphi_2)) \\ &= |z_1| \cdot |z_2| \cdot \mathrm{e}^{i\varphi_1}\mathrm{e}^{i\varphi_2} = |z_1| \cdot |z_2| \cdot \mathrm{e}^{i(\varphi_1 + \varphi_2)}. \end{aligned}$$

Insbesondere gilt $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ für alle $z_1, z_2 \in \mathbb{C}$.

**Literatur.** [E, 1.3 & 8.133], [G, §30], [Dei, 2.3], [FL, 1.3.6]

## 2.3 Angeordnete Körper (09.11.)

**Konventionen.** Sei $K$ ein Körper. Das additiv Neutrale wird mit 0, das multiplikativ Neutrale mit 1 bezeichnet. Für $a \in K$, $b \in K^*$ ist $-a$ das additiv Inverse zu $a$ und $b^{-1}$ das multiplikativ Inverse zu $b$, sowie $a/b := a \cdot b^{-1}$.

**Rechenregeln.** Für alle $x, y, a, b \in K$ gilt: i) $0 \cdot x = x \cdot 0 = 0$. ii) $x(-y) = -(xy)$ und $(-x)(-y) = xy$. Insbesondere $(-1)x = -x$. iii) $a/b + x/y = (ay + bx)/(by)$ für $b, y \neq 0$.

*Beweis.* zu i) $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$, also $0 \cdot x = 0$. zu ii) $xy + x(-y) = x(y-y) = x \cdot 0 = 0$ und $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$. zu iii) $(by)(a/b + x/y) = b(y(a/b + x/y)) = b(ya/b + x) = ya + bx$. □

**Charakteristik.** Sei $R$ ein Ring mit 1. Dann ist die *Charakteristik* $\mathrm{char}(R)$ von $R$ die kleinste natürliche Zahl $n \in \mathbb{N}^*$ mit $n \cdot 1 := (1 + \cdots + 1) = 0$. Gilt $n \cdot 1 \neq 0$ für alle $n \in \mathbb{N}^*$, so ist $\mathrm{char}(R) = 0$.

**Lemma.** Die Charakteristik eines nullteilerfreien Rings $R$ ist 0 oder prim.

*Beweis.* Ist $\mathrm{char}(R) = m = kl$ mit $1 < k, l < m$, so gilt $0 = m \cdot 1 = (k \cdot 1) \cdot (l \cdot 1)$ und wegen Nullteilerfreiheit $k \cdot 1 = 0$ oder $l \cdot 1 = 0$. Widerspruch. □

**Lineare Ordnung.** Sei $M$ eine Menge. $R \subseteq M \times M$ heißt *lineare Ordnung*, falls für alle $x, y, z \in M$ gilt: i) $(x, x) \in R$. ii) Aus $(x, y), (y, x) \in R$ folgt $x = y$. iii) Aus $(x, y), (y, z) \in R$ folgt $(x, z) \in R$. iv) $(x, y) \in R$ oder $(y, x) \in R$. Eine lineare Ordung ist also reflexiv, antisymmetrisch, transitiv und kann je zwei Elemente aus $M$ vergleichen. Man schreibt $x \leq y$ für $(x, y) \in R$.

**Angeordneter Körper.** Sei $K$ ein Körper und $\leq$ eine lineare Ordnung auf $K$. In einem *angeordnetem Körper* $K$ gilt für alle $x, y, z \in K$: i) Aus $x \leq y$ folgt $x + z \leq y + z$. ii) Aus $0 \leq x, y$ folgt $0 \leq x \cdot y$.

**Lemma.** In einem angeordneten Körper $K$ gilt $0 \leq x^2$ für alle $x \in K$. Insbesondere ist $0 \leq 1$.

*Beweis.* Für $0 \leq x$ gilt $0 \leq x \cdot x = x^2$. Für $x \leq 0$ gilt $0 \leq -x$ und $0 \leq (-x) \cdot (-x) = x^2$. □

**Beispiele.** $\mathbb{Q}$ und $\mathbb{R}$ sind angeordnet, $\mathbb{C}$ wegen $i^2 = -1$ nicht.

**Lemma.** Ein angeordneter Körper $K$ hat Charakteristik Null.

*Beweis.* Ist $\mathrm{char}(K) > 0$, so gilt $0 \leq 1 \leq \ldots \leq \mathrm{char}(K) \cdot 1 = 0$, also $1 = 0$. □

**Literatur.** [F, 1.3.3], [Dei, 2.3], [FL, 1.3.6]

## 2.4 Polynome (13.11.)

**Definition.** Sei $K$ ein Körper, $a_0, \ldots, a_n \in K$. Dann heißt $f = a_0 + a_1 t + \cdots + a_n t^n$ ein *Polynom* über $K$ in der Unbestimmten $t$, und $K[t]$ bezeichnet die Menge solcher Polynome. Der *Grad* von $f$ ist $\deg(f) = \max\{n \in \mathbb{N} \mid a_n \neq 0\}$. Für das Nullpolynom setzt man $\deg(0) = -\infty$.

**Ring der Polynome.** Seien $f = a_0 + \cdots + a_n t^n$, $g = b_0 + \cdots + b_m t^m$ mit $m \leq n$. Wir definieren

$$f + g = c_0 + \cdots + c_n t^n, \qquad f \cdot g = d_0 + \cdots + d_{n+m} t^{n+m}$$

mit $c_k = a_k + b_k$ für $k \leq m$ und $c_k = a_k$ für $k > m$ sowie $d_k = \sum_{i+j=k} a_i b_j$. Dann ist $(K[t], +, \cdot)$ ein kommutativer, nullteilerfreier Ring, und es gilt $\deg(f+g) \leq \max(\deg(f), \deg(g))$ sowie $\deg(f \cdot g) = \deg(f) + \deg(g)$.

*Beweis.* Wir überprüfen, dass $K[t]$ nullteilerfrei ist: Sei $f \cdot g = 0$. Dann ist $\deg(f) + \deg(g) = -\infty$, woraus $\deg(f) = -\infty$ oder $\deg(g) = -\infty$ folgt. Also ist $f = 0$ oder $g = 0$. □

**Polynomdivsion.** Seien $f, g \in K[t]$ und $g \neq 0$. Dann gibt es eindeutig bestimmte $q, r \in K[t]$ mit $f = q \cdot g + r$ und $\deg(r) < \deg(g)$.

*Beweis.* Zur Eindeutigkeit: Seien $q, \tilde{q}, r, \tilde{r} \in K[t]$ mit $f = qg + r = \tilde{q}g + \tilde{r}$ und $\deg(r), \deg(\tilde{r}) < \deg(g)$. Dann ist $(q - \tilde{q})g = \tilde{r} - r$ und $\deg(q - \tilde{q}) + \deg(g) = \deg(\tilde{r} - r) < \deg(g)$. Also gilt $\deg(q - \tilde{q}) = -\infty$ und somit $q = \tilde{q}$, $r = \tilde{r}$. Zur Existenz: Sei $f = a_n t^n + \cdots + a_0$, $g = b_m t^m + \cdots + b_0$ mit $a_n, b_m \neq 0$. Falls $n < m$, setze $f = 0 \cdot g + f$. Falls $n \geq m$, setze $q_1 = a_n / b_m t^{n-m}$, $f_1 = f - q_1 g$. Dann ist $\deg(f_1) < \deg(f)$. Wir sind fertig, falls $\deg(f_1) < m$. Andernfalls wiederholt man die Konstruktion mit $f_1$ anstelle von $f$, etc. Nach $k$ Schritten erfüllt $f_k = f_{k-1} - q_k g$ dann $\deg(f_k) < m$ und $f = q_1 g + f_1 = \ldots = (q_1 + \cdots + q_k)g + f_k$. □

**Nullstellen.** $f = t^2 + 1 \in \mathbb{R}[t]$ hat keine Nullstelle in $\mathbb{R}$. Ist $K = \{a_0, \ldots, a_n\}$ ein endlicher Körper, so hat $f = (t - a_0) \cdots (t - a_n) + 1 \in K[t]$ keine Nullstelle in $K$.

**Anzahl von Nullstellen.** Sei $K$ ein Körper, $f \in K[t]$, $f \neq 0$ und $k$ die Anzahl der Nullstellen von $f$ in $K$. Dann gilt $k \leq \deg(f)$.

*Beweis.* mit Induktion über $\deg(f) = n$. Induktionsanfang $n = 0$: $f = a_0 \neq 0$ hat keine Nullstelle. Induktionsschritt von $n$ nach $n+1$: Sei $\deg(f) = n+1$. Hat $f$ keine Nullstelle, so sind wir fertig. Hat $f$ ein Nullstelle $\lambda \in K$, so gibt es eindeutig bestimmtes $q, r$ mit $f = q(t - \lambda) + r$, $\deg(r) < 1$. Also ist $r = b_0 = f(\lambda) = 0$ und $f = q(t - \lambda)$ und $\deg(q) = n$. Nach Induktionsvoraussetzung hat $q$ höchstens $n$ Nullstellen, und es gilt $k \leq n + 1$. □

**Literatur.** [F, 1.3], [FL, 1.4]

# 3 Vektorräume

## 3.1 Der $n$-dimensionale reelle Raum (16.11.)

**Definition.** $\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}$ ist die Menge der geordneten $n$-*Tupel* reeller Zahlen. Wir nennen die Elemente des $\mathbb{R}^n$ *Vektoren* und definieren die *Addition* und die *skalare Multiplikation* folgendermaßen:

$$\begin{aligned} + &: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n,\ (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n), \\ \cdot &: \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n,\ \lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n). \end{aligned}$$

**Punkt oder Pfeil?** Im $\mathbb{R}^2$ können wir einen Vektor als Punkt der Ebene ansehen oder als Pfeil, der den Ursprung $0 = (0, 0)$ mit dem Punkt verbindet. Manchmal zeichnet man einen vom Ursprung weg verschobenen Pfeil.

**Geraden in $\mathbb{R}^2$.** Seien $v, v' \in \mathbb{R}^2$, $v \neq v'$ und $g : \mathbb{R} \to \mathbb{R}^2$, $\lambda \mapsto v + \lambda(v' - v)$. Dann heißt $g[\mathbb{R}]$ die durch $v$ und $v'$ laufende *Gerade*. Es gilt $g(0) = v$, $g(1) = v'$. $G \subseteq \mathbb{R}^2$ ist genau dann eine Gerade, wenn es $(a_1, a_2) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ und $b \in \mathbb{R}$ mit $G = \{x \in \mathbb{R}^2 \mid a_1 x_1 + a_2 x_2 = b\}$ gibt.

*Beweis.* $x \in g[\mathbb{R}] \Leftrightarrow x - v = \lambda(v' - v)$ für ein $\lambda \in \mathbb{R} \Leftrightarrow (x_2 - v_2)/(x_1 - v_1) = (v_2' - v_2)/(v_1' - v_1)$ oder $(x_1 - v_1)/(x_2 - v_2) = (v_1' - v_1)/(v_2' - v_2) \Leftrightarrow (x_2 - v_2)(v_1' - v_1) = (x_1 - v_1)(v_2' - v_2) \Leftrightarrow a_1 x_2 + a_2 x_2 = b$ mit $a_1 = v_2 - v_2'$, $a_2 = v_1' - v_1$, $b = v_2 v_1' - v_1 v_2'$. □

**Der Schnitt** zweier verschiedener Geraden im $\mathbb{R}^2$ besteht entweder aus einem Punkt oder ist leer.

*Beweis.* Sei $x \in G_1 \cap G_2 = \{x \in \mathbb{R}^2 \mid a_{11} x_1 + a_{12} x_2 = b_1, a_{21} x_1 + a_{22} x_2 = b_2\}$. Ist $(a_{11}, a_{21}) = (0, 0)$, so ist $b_1/a_{12} \neq b_2/a_{22}$. Also $G_1 \cap G_2 = \emptyset$. Ist $a_{11} \neq 0$, so gilt $a_{11} x_1 + a_{12} x_2 = b_1$, $(a_{22} - a_{12} a_{21}/a_{11}) x_2 = b_2$. Ist $a_{22} - a_{12} a_{21}/a_{11} = 0$, so ist der Schnitt leer. Andernfalls gilt $x_2 = b_2/(a_{22} - a_{12} a_{21}/a_{11})$ und $x_1 = (b_1 - a_{12} x_2)/a_{11}$. Analog für $a_{11} = 0$, $a_{21} \neq 0$. □

**Lineares Gleichungssystem.** Wir haben eben ein lineares Gleichungssystem $Ax = b$ mit einer reellen $2 \times 2$ Matrix $A \in \mathbb{R}^{2\times 2}$ gelöst:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}.$$

**Literatur.** [W, §2–3], [F, 0.1–0.3]

## 3.2 Vektorräume (20.11.)

**Definition.** Sei $K$ ein Körper. Eine Menge $V$ zusammen mit einer Addition und einer skalaren Multiplikation

$$+ : V \times V \to V, (v, w) \mapsto v + w, \qquad \cdot : K \times V \to V, (\lambda, v) \mapsto \lambda \cdot v$$

heißt *Vektorraum* bezüglich $K$, falls für alle $\lambda, \mu \in K$, $v, w \in V$ gilt: i) $(V, +)$ ist eine abelsche Gruppe. ii) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ und $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$. iii) $\lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$. iv) $1 \cdot v = v$.

**Standardraum.** $K^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in K\}$ mit

$$\begin{aligned} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n), \\ \lambda \cdot (x_1, \ldots, x_n) &= (\lambda x_1, \ldots, \lambda x_n) \end{aligned}$$

ist ein $K$-Vektorraum.

**Matrizen.** Die Menge $K^{m \times n}$ der $m \times n$ Matrizen mit $m$ Zeilen, $n$ Spalten und Einträgen aus $K$ ist ein $K$-Vektorraum bezüglich $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$, $\lambda \cdot (a_{ij}) = (\lambda a_{ij})$. Man kann $K^{m \times n}$ mit $K^{mn}$ identifizieren.

**Zahlen.** $\mathbb{C}$ ist bezüglich der üblichen Addition auf $\mathbb{C}$ und der skalaren Multiplikation $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$, $(\lambda, v) \mapsto \lambda v$ ein $\mathbb{R}$-Vektorraum.

**Polynome.** $K[t]$ ist bezüglich der üblichen Addition und der skalaren Multiplikation $\lambda \cdot (a_0 + \cdots + a_n t^n) = \lambda a_0 + \cdots + (\lambda a_n) t^n$ ein $K$-Vektorraum.

**Abbildungen.** Sei $M$ eine Menge. Die Abbildungen $\{f : M \to K\}$ sind bezüglich $(f + g)(x) = f(x) + g(x)$ und $(\lambda \cdot f)(x) = \lambda f(x)$ ein $K$-Vektorraum. $f : \{1, \ldots, n\} \to K$ können wir mit dem „Vektor“ $(f(1), \ldots, f(n)) \in K^n$ identifizieren. $f : \mathbb{N} \to K$ können wir mit der Zahlenfolge $(f_n)_{n \in \mathbb{N}}$ identifizieren.

**Rechenregeln.** In einem $K$-Vektorraum gilt für alle $\lambda \in K$, $v \in V$: i) $0 \cdot v = 0$. ii) $\lambda \cdot 0 = 0$. iii) Aus $\lambda \cdot v = 0$ folgt $\lambda = 0$ oder $v = 0$. iv) $(-1) \cdot v = -v$.

**Literatur.** [F, 1.4], [FL, 2.1.1], [B, 1.4]

## 3.3 Unterräume (23.11.)

**Definition.** Sei $V$ ein $K$-Vektorraum. Eine Teilmenge $U \subseteq V$ heißt *Unterraum* von $V$, falls gilt: i) $U \neq \emptyset$. ii) Aus $v, w \in U$ folgt $v + w \in U$. iii) Aus $v \in U$, $\lambda \in K$ folgt $\lambda v \in U$.

**Satz.** Ein Unterraum $U \subseteq V$ ist mit der von $V$ induzierten Addition und skalaren Multiplikation ein Vektorraum.

*Beweis.* Für alle $v, w \in U$ gilt $v + w, -v \in U$. Also ist $(U, +)$ eine Untergruppe von $(V, +)$ und zudem eine abelsche Gruppe. Aus iii) folgt $\cdot[K \times U] \subseteq U$. Die Distributivgesetze und die Assoziativität der skalaren Multiplikation vererbt $V$. Ebenso gilt $1 \cdot v = v$ für alle $v \in U$. □

**Beispiele.** i) $\{0\}$ ist immer ein Unterrraum. ii) $\{x \in \mathbb{R}^2 \mid a_1 x_1 + a_2 x_2 = b\}$ ist für $b \neq 0$ kein Unterraum von $\mathbb{R}^2$. iii) Für $A \in K^{n \times n}$, $x \in K^n$ ist $Ax \in K^n$,

$$(Ax)_i = \sum_{j=1}^{n} a_{ij} x_j, \qquad i = 1, \ldots, n.$$

$\{x \in K^n \mid Ax = 0\}$ ist ein Unterraum des $K^n$.

**Literatur.** [F, 1.4], [FL, 2.1.2 & 2.1.3], [B, 1.4.]

## 3.4 Linearkombinationen, lineare Unabhängigkeit (27.11.)

**Linearkombination.** Seien $V$ ein $K$-Vektorraum und $v_1, \ldots, v_n \in V$. Ein Vektor $v \in V$ heißt *Linearkombiation* von $v_1, \ldots, v_n$, wenn es $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ gibt.

**Aufgespannter Raum.** Sei $M \subseteq V$. Die Menge aller $v \in V$, die eine Linearkombination von Vektoren in $M$ sind, heißt von $M$ *aufgespannter Raum* und wird mit $\operatorname{span}(M)$ bezeichnet: Für $v \in \operatorname{span}(M)$ gibt es $v_1, \ldots, v_n \in M$, $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Man setzt $\operatorname{span}(\emptyset) = \{0\}$. $\operatorname{span}(M)$ ist der kleinste Unterraum von $V$, der $M$ enthält.

*Beweis.* $\{0\} \subseteq \operatorname{span}(M) \subseteq V$. Wegen $v + w, \lambda v \in \operatorname{span}(M)$ für alle $v, w \in \operatorname{span}(M)$, $\lambda \in K$ ist $\operatorname{span}(M)$ ein Unterraum. Ist $U \supseteq M$ ein Unterraum von $V$, so gilt $\operatorname{span}(M) \subseteq U$. □

**Beispiele.** i) Ist $v \in \mathbb{R}^2 \setminus \{0\}$, so ist $\operatorname{span}(v) = \{\lambda v \mid \lambda \in \mathbb{R}\}$ die durch $v$ und 0 laufende Gerade. ii) Das *Kronecker-Symbol* $\delta_{ij}$ erfüllt $\delta_{ij} = 1$ für $i = j$ und $\delta_{ij} = 0$ sonst. Der $i$-te Einheitsvektor

$$e_i = (\delta_{1i}, \ldots, \delta_{ni}) \in K^n$$

ist an der $i$-ten Stelle 1 und sonst 0. Es gilt $\operatorname{span}(e_1, \ldots, e_n) = K^n$. iii) $\operatorname{span}(t^n \mid n \in \mathbb{N}) = K[t]$.

**Definition.** Eine Teilmenge $M \subseteq V$ eines $K$-Vektorraums $V$ heißt *linear unabhängig*, falls für alle paarweise verschiedenen $v_1, \ldots, v_n \in M$ und alle $\lambda_1, \ldots, \lambda_n \in K$ gilt: Aus $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ folgt $\lambda_1 = \ldots = \lambda_n = 0$.

**Literatur.** [F, 1.4], [FL, 2.1.2 & 2.1.3], [B, 1.4.]

**Extemporale, 27.11.2012**
Name (letzte Anonymisierung und VTTMM):

Bitte bearbeiten Sie ohne Hilfsmittel in 15 Minuten die folgenden Aufgaben.

1. Sei $K$ ein Körper, $f \in K[t]$ und $\lambda \in K$ mit $f(\lambda) = 0$. Zeigen Sie, dass es genau ein $q \in K[t]$ mit $f = q(t - \lambda)$ gibt.

*Es gibt eindeutig bestimmte* $q, r \in K[t]$ *mit* $f = q(t - \lambda) + r$ *und* $\deg(r) < \deg(t - \lambda)$ *(Polynomdivision). Wir zeigen, dass* $r$ *das Nullpolynom ist. Wegen* $\deg(r) < \deg(t - \lambda) = 1$ *gilt* $\deg(r) = -\infty$ *oder* $\deg(r) = 0$. *Wegen* $0 = f(\lambda) = q(\lambda) \cdot 0 + r(\lambda)$ *gilt* $r(\lambda) = 0$ *und* $r = 0$.

2. Sei $K$ ein Körper. Formulieren Sie die Definition eines $K$-Vektorraums $(V, +, \cdot)$.

$V$ *zusammen mit einer Addition* $+ : V \times V \to V$, $(v, w) \mapsto v + w$ *und einer skalaren Multiplikation* $\cdot : K \times V \to V, (\lambda, v) \mapsto \lambda \cdot v$ *heißt* $K$*-Vektorraum, falls für alle* $\lambda, \mu \in K$, $v, w \in V$ *gilt: i)* $(V, +)$ *ist abelsche Gruppe. ii)* $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$, $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$. *iii)* $\lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$. *iv)* $1 \cdot v = v$.

3. Beweisen oder widerlegen Sie: $U = \left\{(x, y) \in \mathbb{R}^2 \mid y = x^2\right\}$ ist ein Unterraum von $\mathbb{R}^2$.

$U$ *ist kein Unterrraum, da* $U$ *nicht additiv abgeschlossen ist:* $(1, 1) \in U$ *und* $(2, 4) \in U$, *aber* $(1, 1) + (2, 4) = (3, 5) \notin U$, *weil* $5 \neq 3^2$.

**Bewertung:** Maximal 2 Punkte pro Aufgabe, (5 & 6, 4, 3, 2, 1, 0) Punkte entsprechen der Note (1, 2, 3, 4, 5, 6). Bei 36 Teilnehmern gab es 1mal Note 1, 6mal 2, 3mal 3, 8mal 4, 9mal 5, 9mal 6. Durchschnitt: 4,25

**Befragung zum Zeitaufwand, 30.11.2012**
Name (letzte Anonymisierung und VTTMM):

Bitte geben Sie Ihre durchschnittliche wöchentliche Arbeitszeit an.

| | Analysis I | Lin. Algebra I |
|---|---|---|
| Nachbereiten der Vorlesung | 1.6h | 1.3h |
| Studium von Lehrbüchern ergänzender Literatur & Internetquellen | 1.3h | 0.6h |
| Selbstständiges Bearbeiten von Übungaufgaben | 2.2h | 2.3h |
| Gruppenarbeit an Übungsaufgaben | 2.4h | 2.4h |
| Vor- und Nachbereiten der Ergänzungen | 0.3h | 0.2h |
| Summe | 7.8h | 6.8h |

In blau ist der Mittelwert eingetragen, den die Befragung von 27 StudentInnen ergeben hat. Es empfiehlt sich mehr Zeit auf die selbstständige Bearbeitung von Übungsaufgaben zu verwenden, insbesondere eine Reinschrift der Lösung.

## 3.5 Lineare Unabhängigkeit (30.11.)

**Beispiele im $\mathbb{R}^3$.** i) $v_1 = (1,2,3)$, $v_2 = (4,5,6)$ sind linear unabhängig, denn aus $\lambda_1 v_1 + \lambda_2 v_2 = 0$ folgt $\lambda_1 + 4\lambda_2 = 0$, $2\lambda_1 + 5\lambda_2 = 0$ und $\lambda_1 = -4\lambda_2$, $3\lambda_2 = 0$, also $0 = \lambda_2 = \lambda_1$. ii) $v_1$, $v_2$ und $v_3 = (7,8,9)$ sind linear abhängig: $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0$ bedeutet

$$\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ bzw. } \begin{pmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Hiervon ist jedes $(\lambda_3, -2\lambda_3, \lambda_3)$ eine Lösung.

**Beispiele im $K^n$.** i) $\{e_1, \ldots, e_n\} \subseteq K^n$ ist linear unabhängig. ii) Sei $A \in K^{n\times n}$ eine unipotente obere Dreiecksmatrix: $a_{ii} = 1$ für alle $i$ und $a_{ij} = 0$ für $i > j$. Die Zeilenvektoren $\{v_1, \ldots, v_n\}$ von $A$ sind linear unabhängig, denn $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ bedeutet $\lambda_n = 0, \ldots, \lambda_1 = 0$ (Rückwärtssubstitution).

**Polynome.** Die Monome $\{t^n \mid n \in \mathbb{N}\} \subseteq K[t]$ sind linear unabhängig, denn $\lambda_0 + \lambda_1 t^{k_1} + \cdots + \lambda_n t^{k_n} = 0$ gilt nur für das Nullpolynom.

**Funktionen.** $1, \cos(x), \sin(x) \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ sind linear unabhängig: Aus $\lambda_1 \cdot 1 + \lambda_2 \cdot \cos + \lambda_3 \cdot \sin = 0$ folgt $\lambda_1 + \lambda_2 = 0$ $(x = 0)$, $\lambda_1 + \lambda_3 = 0$ $(x = \frac{\pi}{2})$, $\lambda_1 - \lambda_2 = 0$ $(x = \pi)$. Dieses lineare Gleichungssystem hat $(\lambda_1, \lambda_2, \lambda_3) = (0,0,0)$ als einzige Lösung.

**Satz.** Für $M \subseteq V$ sind äquivalent: i) $M$ ist linear unabhängig. ii) $0 \notin M$ und für jedes $v \in \mathrm{span}(M) \setminus \{0\}$ gibt es eindeutig bestimmte, paarweise verschiedene $v_1, \ldots, v_n \in M$ und eindeutig bestimmte $\lambda_1, \ldots, \lambda_n \in K^*$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$.

*Beweis.* ii)⇒i): Ist $\lambda_1 v_1 = 0$, $v_1 \in M$, so folgt $\lambda_1 = 0$. Ist $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ und ein $\lambda_i \neq 0$, so sei o.E. $\lambda_1 \neq 0$. Dann ist $v_1 = -\lambda_2/\lambda_1 v_2 - \cdots - \lambda_n/\lambda_1 v_n$, was der Eindeutigkeit widerspricht. i)⇒ii): Ist $v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 w_1 + \cdots + \mu_m w_m$ mit $v_i, w_i \in M$, $\lambda_i, \mu_i \in K^*$, so folgt $0 = \lambda_1 v_1 + \cdots + \lambda_n v_n - \mu_1 w_1 - \cdots - \mu_m w_m$. Wegen der linearen Unabhängigkeit gilt $m = n$ und (nach Umnummerierung) $v_i = w_i$ für alle $i$. Es folgt aus $0 = (\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_n - \mu_n)v_n$ auch $\lambda_i = \mu_i$ für alle $i$. □

**Literatur.** [F, 1.4], [FL, 2.1.4], [B, 1.5]

## 3.6 Basen (04.12.)

**Lemma.** $M$ ist genau dann linear unabhängig, wenn $v \notin \operatorname{span}(M \setminus \{v\})$ für alle $v \in M$ gilt.

*Beweis.* Es gibt ein $v \in M$ mit $v \in \operatorname{span}(M \setminus \{v\})$ genau dann, wenn es ein $v \in M$, $\lambda_1, \ldots, \lambda_n \in K$ und $v_1, \ldots, v_n \in M \setminus \{v\}$ mit $\lambda_1 v_1 + \cdots + \lambda_n v_n - v = 0$ gibt. Dies ist äquivalent zur linearen Abhängigkeit von $M$. □

**Definition.** Eine Teilmenge $M \subseteq V$ heißt *Erzeugendensystem* eines Vektorraums $V$, falls $\operatorname{span}(M) = V$. Ein linear unabhängiges Erzeugendensystem heißt *Basis*.

**Beispiele.** i) $\emptyset$ von $\{0\}$. ii) $\{e_1, \ldots, e_n\}$ von $K^n$. iii) $\{1, i\}$ ist eine Basis des $\mathbb{R}$-Vektorraums $\mathbb{C}$. iv) $\{t^n \mid n \in \mathbb{N}\}$ von $K[t]$.

**Satz.** Sei $V \neq \{0\}$ eine $K$-Vektorraum. Für $B \subseteq V$ sind äquivalent:

i) $B$ ist eine Basis von $V$.

ii) Für jedes $v \in V \setminus \{0\}$ gibt es eindeutig bestimmte, paarweise verschiedene $v_1, \ldots, v_n \in B$ und eindeutige $\lambda_1, \ldots, \lambda_n \in K^*$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$.

iii) $\operatorname{span}(B) = V$ und $\operatorname{span}(B \setminus \{v\}) \neq V$ für alle $v \in B$.

iv) $B$ ist linear unabhängig und $B \cup \{v\}$ ist für jedes $v \in V \setminus B$ linear abhängig.

*Beweis.* Bereits bewiesen ist i)⇔ii) und i)⇒iii). Außerdem ist i) äquivalent zu $B$ linear unabhängig und für jedes $v \in V$ gibt es $v_1, \ldots, v_n \in B$ und $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Dies ist äquivalent zu iv). Aus iii) folgt $\operatorname{span}(B) = V$, und für alle $v \in B$ gibt es $w \in V$ mit $w \notin \operatorname{span}(B \setminus \{v\})$ und so ein $w$ läßt sich nur mit $v$ über $B$ linear kombinieren. Dann gilt $v \notin \operatorname{span}(B \setminus \{v\})$ und i). □

**Charakterisierungen.** Eine Basis von $V$ ist ein mimimales Erzeugendensystem von $V$ sowie eine maximal linear unabhängige Teilmenge von $V$.

**Literatur.** [Gr, §20], [F, 1.5], [FL, 2.2]

## 3.7 Dimension (07.12.)

**Basisauswahlsatz.** Ist $V = \operatorname{span}(M)$ und $M$ endlich, so kann man aus $M$ eine Basis von $V$ auswählen, da $M$ sich in endlich vielen Schritten zu einem minimalen Erzeugendensystem verkürzen läßt. Dies beweist die Existenz einer Basis für endliche erzeugte Vektorräume.

**Austauschlemma.** Sei $V$ ein $K$-Vektorraum und $B$ eine Basis von $V$. Sei $v \in V$ und $v_1, \dots, v_n \in B$, $\lambda_1, \dots, \lambda_n \in K^*$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Dann ist $B_i = B \setminus \{v_i\} \cup \{v\}$ für alle $i = 1, \dots, n$ eine Basis von $V$.

*Beweis.* Wir betrachten $B_1$. Für $w \in V$ gibt es $w_1, \dots, w_m \in B$, $\mu_1, \dots, \mu_m \in K$ mit $w = \mu_1 w_1 + \cdots + \mu_m w_m$. Ist ein $w_j = v_1$, so gilt $w_j = 1/\lambda_1 v - \lambda_2/\lambda_1 v_2 - \cdots - \lambda_n/\lambda_1 v_n$ und $w \in \operatorname{span}(B_1)$, d.h. $V = \operatorname{span}(B_1)$. Seien $z_1, \dots, z_l \in B_1$, $\kappa_1, \cdots, \kappa_l \in K$ mit $0 = \kappa_1 z_1 + \cdots + \kappa_l z_l$. Schlimmstenfalls ist ein $z_j = v$, o.E. $z_1 = v$, und es gilt $0 = \kappa_1(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n) + \kappa_2 z_2 + \cdots + \kappa_l z_l$. Da $B$ linear unabhängig ist und $\lambda_i \in K^*$, folgt $\kappa_i = 0$ für alle $i$. □

**Austauschsatz.** Sei $V$ ein $K$-Vektorraum und $B = \{v_1, \dots, v_n\}$ eine Basis von $V$. Ist $\{w_1, \dots, w_m\} \subseteq V$ linear unabhängig, so gilt $m \leq n$, und es gibt $n-m$ Vektoren in $B$, so dass (nach Umnummerierung) $\{w_1, \dots, w_m, v_{m+1}, \dots, v_n\}$ eine Basis von $V$ ist.

*Beweis.* Induktion nach $m$. Induktionsanfang $m = 0$: klar. Induktionsschritt $m-1 \to m$: Nach Induktionsannahme gilt $m-1 \leq n$, $\{w_1, \dots, w_{m-1}, v_m, \dots, v_n\}$ ist eine Basis von $V$. Wäre $m - 1 = n$, so wäre $\{w_1, \dots, w_{m-1}\}$ eine Basis von $V$, was der linearen Unabhängigkeit von $\{w_1, \dots, w_m\}$ widerspricht. Also gilt $m - 1 \neq n$ und $m \leq n$. Außerdem ist $w_m = \lambda_1 w_1 + \cdots + \lambda_{m-1} w_{m-1} + \lambda_m v_m + \cdots + \lambda_n v_n$ und $\lambda_i \neq 0$ für mindestens ein $i \geq m$. Tauschen wir das zugehörige $v_i$ mit $w_m$ aus, so erhalten wir eine Basis von $V$. □

**Korollar.** Hat ein Vektorraum $V$ eine endliche Basis, so sind alle Basen von $V$ endlich und haben die gleiche Länge.

**Definition.** Besitzt ein Vektorraum $V$ eine endliche Basis, so heißt die Länge der Basis die *Dimension* $\dim V$ von $V$. Besitzt $V$ keine endliche Basis, so definieren wir $\dim V = \infty$. Wir vereinbaren $\infty + \infty = \infty$, $\infty + n = \infty$ für $n \in \mathbb{N}$.

**Unterräume.** Ist $U$ Unterraum eines Vektorraums $V$, so gilt $\dim U \leq \dim V$. Aus $\dim U = \dim V < \infty$ folgt $U = V$.

**Beispiele.** i) $\dim\{0\} = 0$. ii) $\dim K^n = n$. iii) Für $(a_1, a_2) \neq (0, 0)$ ist $\{x \in \mathbb{R}^n \mid a_1 x_1 + a_2 x_2 = 0\}$ ein $(n-1)$-dimensionaler Unterraum des $\mathbb{R}^n$. iv) $\dim K[t] = \infty$. v) $\dim_{\mathbb{R}} \mathbb{C} = 2$, $\dim_{\mathbb{C}} \mathbb{C} = 1$.

**Literatur.** [F, 1.5], [FL, 2.2], [B, 1.5]

## 3.8 Summen von Vektorräumen (11.12.)

**Definition.** Sei $V$ ein Vektorraum, und $U_1, \ldots, U_m$ Unterräume von $V$. Dann ist

$$U_1 + \cdots + U_m := \{u_1 + \cdots + u_m \mid u_j \in U_j, j = 1, \ldots, m\}$$

die *Summe* von $U_1, \ldots, U_m$. Es gilt $U_1 + \cdots + U_m = \operatorname{span}(U_1 \cup \cdots \cup U_m)$ und $\dim(U_1 + \cdots + U_m) \leq \dim(U_1) + \cdots + \dim(U_m)$.

**Dimensionsformel.** Für Unterräume $U_1, U_2 \subseteq V$ eines Vektorraumes $V$ gilt $\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim U_1 + \dim U_2$.

*Beweis.* Ist $\dim U_1 = \infty$ oder $\dim U_2 = \infty$, so ist nichts zu beweisen. Andernfalls ergänzen wir eine Basis $\{u_1, \ldots, u_m\}$ von $U_1 \cap U_2$ zu einer Basis $B_1 = \{u_1, \ldots, u_m, v_1, \ldots, v_k\}$ von $U_1$ und zu einer Basis $B_2 = \{u_1, \ldots, u_m, w_1, \ldots, w_l\}$ von $U_2$. Es gilt $U_1 + U_2 = \operatorname{span}(B_1 \cup B_2)$. Aus $\lambda_1 u_1 + \cdots + \lambda_m u_m + \mu_1 v_1 + \cdots + \mu_k v_k + \kappa_1 w_1 + \cdots + \kappa_l w_l = 0$ folgt $\lambda_1 u_1 + \cdots + \lambda_m u_m + \mu_1 v_1 + \cdots + \mu_k v_k \in U_1 \cap U_2$ und $\mu_1 = \ldots = \mu_k = 0$. Dann folgt auch $\lambda_1 = \ldots = \lambda_m = \kappa_1 = \ldots = \kappa_l = 0$. □

**Direkte Summe.** Ein Vektorraum $V$ heißt die *direkte Summe* von zwei Unterräumen $U_1, U_2 \subseteq V$, wenn $V = U_1 + U_2$ und $U_1 \cap U_2 = \{0\}$. Man schreibt dann $V = U_1 \oplus U_2$.

**Lemma.** Gilt $V = U_1 + U_2$ mit $U_1, U_2 \neq \{0\}$, so sind äquivalent: i) $V = U_1 \oplus U_2$. ii) Jedes $v \in V$ ist eindeutig darstellbar als $v = u_1 + u_2$ mit $u_1 \in U_1$, $u_2 \in U_2$. iii) Je zwei Vektoren $u_1 \in U_1^*$, $u_2 \in U_2^*$ sind linear unabhängig.

*Beweis.* i)⇒ii) Ist $V \ni v = u_1 + u_2 = u_1' + u_2'$ mit $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$, so gilt $u_1 - u_1', u_2 - u_2' \in U_1 \cap U_2$ und $u_1 = u_1'$, $u_2 = u_2'$. ii)⇒iii) Für $u_1 \in U_1^*$, $u_2 \in U_2^*$ folgt aus $\lambda_1 u_1 + \lambda_2 u_2 = 0$ wegen eindeutiger Darstellung der Null $\lambda_1 = \lambda_2 = 0$. iii)⇒i) Ist $0 \neq v \in U_1 \cap U_2$, so sind $v$ und $-v$ linear unabhängig. Widerspruch. □

**Komplement.** Ist $V$ ein Vektorraum und $U \subseteq V$ Unterraum, so gibt es einen Unterraum $U' \subseteq V$ mit $V = U \oplus U'$. $U'$ heißt das *Komplement* zu $U$ in $V$.

*Beweis.* Ist $\dim V < \infty$, so ergänzen wir eine Basis $\{u_1, \ldots, u_m\}$ von $U$ zu einer Basis $\{u_1, \ldots, u_m, v_1, \ldots, v_k\}$ von $V$ und setzen $U' = \operatorname{span}\{v_1, \ldots, v_k\}$. Für $\dim V = \infty$ geht man ähnlich vor. □

**Beispiel.** Für $V = \mathbb{R}^2$ und $U = \{(0, y) \mid y \in \mathbb{R}\}$ ist jeder Unterraum $U_a = \{(x, ax) \mid x \in \mathbb{R}\}$, $a \in \mathbb{R}$, ein Komplement zu $U$, $\mathbb{R}^2 = U \oplus U_a$.

**Literatur.** [F, 1.6], [B, 1.6]

# 4 Lineare Abbildungen

## 4.1 Homomorphismen (14.12.)

**Definition.** Seien $(G, *)$ und $(H, *')$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt *Homomorphismus*, falls $\varphi(a * b) = \varphi(a) *' \varphi(b)$ für alle $a, b \in G$ gilt. Ein bijektiver Homomorphismus heißt *Isomorphismus*.

**Lemma.** Sei $\varphi : G \to H$ eine Homomorphismus, $e_G, e_H$ die neutralen Elemente und $a \in G$. Es gilt: i) $\varphi(e_G) = e_H$. ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$. iii) Ist $\varphi$ ein Isomorphismus, so auch die Umkehrabbildung $\varphi^{-1} : H \to G$.

*Beweis.* i) $e_H\varphi(e_G) = \varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ und damit $e_H = \varphi(e_G)$. ii) $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_H$. iii) $\varphi^{-1}$ ist bijektiv. Seien $a, b \in G$, $c = \varphi(a)$, $d = \varphi(b)$. Dann ist $\varphi^{-1}(cd) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(c)\varphi^{-1}(d)$. □

**Isomorphismen.** Für $m \in \mathbb{N}^*$ ist $\varphi : (\mathbb{Z}, +) \to (m\mathbb{Z}, +)$, $x \mapsto m \cdot x$ ein Isomorphismus. $\varphi : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$, $x \mapsto \mathrm{e}^x$ ist ebenfalls Isomorphismus.

**Kern.** Seien $G, H$ Gruppen und $\varphi : G \to H$ eine Abbildung. Dann heißt $\ker(\varphi) = \{a \in G \mid \varphi(a) = e_H\}$ der *Kern* von $\varphi$. Ist $\varphi$ ein Homomorphismus, so ist $\ker(\varphi)$ ein Normalteiler von $G$ und $\varphi[G]$ eine Untergruppe von $H$.

*Beweis.* Sei $U = \ker(\varphi)$. Es gilt $e_G \in U$, $\varphi(ab) = \varphi(a)\varphi(b) = e_H$, $\varphi(a^{-1}) = \varphi(a)^{-1} = e_H$ für alle $a, b \in U$. Also ist $U$ Untergruppe von $G$. Sind $a, b \in G$, so bedeutet $a \sim_U b$ dass $ab^{-1} \in U$ bzw. $\varphi(ab^{-1}) = e_H$ bzw. $\varphi(a) = \varphi(b)$ gilt, und $\sim_U$, $\sim^U$ fallen zusammen. Außerdem gilt $e_H \in \varphi[G]$, $\varphi(a)\varphi(b) = \varphi(ab)$, $\varphi(a)^{-1} = \varphi(a^{-1})$ für alle $a, b \in G$. Also ist $\varphi[G]$ Untergruppe von $H$. □

**Lemma.** Ein Homomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn $\ker(\varphi) = \{e_G\}$ gilt.

*Beweis.* Ist $\varphi$ injektiv, so gilt $\ker(\varphi) = \{e_G\}$. Gilt $\ker(\varphi) = \{e_G\}$, so folgt aus $\varphi(a) = \varphi(b)$ auch $\varphi(ab^{-1}) = e_H$ und $ab^{-1} = e_G$ und $a = b$. □

**Homomorphiesatz.** Ist $\varphi : G \to H$ ein Homomorphismus und $U = \ker(\varphi)$, so definiert $\widetilde{\varphi} : G/U \to \varphi[G]$, $aU \mapsto \varphi(a)$ einen Isomorphismus.

*Beweis.* Wegen $\varphi(a) = \varphi(b)$ für $a \sim_U b$ ist $\widetilde{\varphi}$ wohldefiniert. Für $a, b \in G$ ist $\widetilde{\varphi}(abU) = \varphi(ab) = \varphi(a)\varphi(b) = \widetilde{\varphi}(aU)\widetilde{\varphi}(bU)$. Also ist $\widetilde{\varphi}$ Homomorphismus. Wegen $\ker(\widetilde{\varphi}) = \{aU \mid \widetilde{\varphi}(aU) = e_H\} = \{aU \mid \varphi(a) = e_H\} = \{U\}$ ist $\widetilde{\varphi}$ injektiv. Nach Definition ist $\widetilde{\varphi}$ auch surjektiv. □

**Literatur.** [F, 1.2], [KM, 4.4]

## 4.2 Lineare Abbildungen (18.12.)

**Definition.** Seien $V, W$ Vektorräume über $K$. Eine Abbildung $F : V \to W$ heißt *linear* oder *Homomorphismus*, falls $F(u+v) = F(u) + F(v)$, $F(\lambda u) = \lambda F(u)$ für alle $u, v \in V$, $\lambda \in K$ gilt. Ein bijektiver Homomorphismus heißt *Isomorphismus*.

**Eigenschaften.** Sei $F : V \to W$ linear. Dann gilt: i) $F(0) = 0$. ii) Ist $M \subseteq V$ linear abhängig, so auch $F[M]$. iii) Sind $V' \subseteq V$ und $W' \subseteq W$ Unterräume, so auch $F[V']$ und $F^{-1}[W']$. iv) Ist $F$ ein Isomorphismus, so auch $F^{-1} : W \to V$.

*Beweis.* i) $F(0) = F(0 \cdot 0) = 0 \cdot F(0) = 0$. ii) Gibt es $m_1, \ldots, m_n \in M$ paarweise verschieden und $(\lambda_1, \ldots, \lambda_n) \neq 0$ mit $0 = \lambda_1 m_1 + \cdots + \lambda_n m_n$, so gilt auch $0 = \lambda_1 F(m_1) + \cdots + \lambda_n F(m_n)$. iii) $0 \in F[V']$, $F(u)+F(v) = F(u+v)$, $\lambda F(v) = F(\lambda v)$ für alle $u, v \in V'$, $\lambda \in K$. Außerdem ist $0 \in F^{-1}[W']$ und $u + v, \lambda u \in F^{-1}[W']$ für $u, v \in F^{-1}[W']$, $\lambda \in K$. iv) Nachrechnen. □

**Matrizen.** Sei $K$ ein Körper. Eine $m \times n$-Matrix $A \in K^{m \times n}$ ist ein Rechteckschema mit $m$ Zeilen und $n$ Spalten, und für $x \in K^n$ ist das Matrix-Vektor-Produkt $Ax \in K^m$ definiert durch

$$Ax = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix},$$

das heißt $(Ax)_i = \sum_{j=1}^{n} a_{ij} x_j$ für $i = 1, \ldots, m$. Die Abbildung $F : K^n \to K^m$, $x \mapsto Ax$ ist linear.

**Raum der Homomorphismen.** $\mathrm{Hom}(V, W) := \{F : V \to W \mid F \text{ linear}\}$ ist mit $(F+G)(v) := F(v) + G(v)$ und $(\lambda F)(v) := \lambda F(v)$ ein Vektorraum über $K$.

**Literatur.** [F, 2.1], [FL, 2.3.1–2.3.3], [B, 2.1]

## 4.3 Bild und Kern (21.12.)

**Definition.** Ist $F : V \to W$ eine lineare Abbildung, so heißen $F[V] = \{f(x) \mid x \in V\}$ das *Bild* und $\ker(F) = \{x \in V \mid F(x) = 0\}$ der *Kern* von $F$. Das Bild ist ein Unterraum von $W$, der Kern ein Unterraum von $V$.

**Eigenschaften.** Sei $F : V \to W$ linear. i) $F : V \to W$ ist genau dann injektiv, wenn $\ker(F) = \{0\}$ gilt. ii) Sind $v_1, \ldots, v_n \in V$ derart, dass $F(v_1), \ldots, F(v_n)$ paarweise verschieden sind und $\{F(v_1), \ldots, F(v_n)\}$ linear unabhängig ist, so ist $\{v_1, \ldots, v_n\}$ linear unabhängig. Insbesondere gilt $\dim F[V] \leq \dim V$.

*Beweis.* zu ii) Aus $\lambda_1 v_1 + \cdots + v_n \lambda_n = 0$ folgt $\lambda_1 F(v_1) + \cdots + \lambda_n F(v_n) = 0$ und $\lambda_1 = \ldots = \lambda_n = 0$. □

**Dimensionsformel.** Ist $F : V \to W$ linear, so gilt $\dim V = \dim \ker(F) + \dim F[V]$. Insbesondere fallen für lineare Abbildungen zwischen endlich-dimensionalen Vektorräumen Injektivität, Surjektivität und Bijektivität zusammen.

*Beweis.* Aus $\dim \ker(F) = \infty$ oder $\dim F[V] = \infty$ folgt $\dim V = \infty$. Betrachten wir $\dim F[V], \dim \ker(F) < \infty$. Seien $\{F(v_1), \ldots, F(v_m)\}$ und $\{v_{m+1}, \ldots, v_n\}$ eine Basis von $F[V]$ und $\ker(F)$. Zeige, dass $\{v_1, \ldots, v_n\}$ eine Basis von $V$ ist. Sei $v \in V$. Dann gilt $F(v) = \lambda_1 F(v_1) + \cdots + \lambda_m F(v_m)$ und $\ker(F) \ni v - \lambda_1 v_1 - \cdots - \lambda_m v_m = \lambda_{m+1} v_{m+1} + \cdots + \lambda_n v_n$. Also ist $v \in \operatorname{span}\{v_1, \ldots, v_n\}$. Sei $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$. Dann gilt $\lambda_1 F(v_1) + \cdots + \lambda_m F(v_m) = 0$ und $\lambda_1 = \ldots = \lambda_m = 0$. Dann ist $\lambda_{m+1} v_{m+1} + \cdots + \lambda_n v_n = 0$ und $\lambda_{m+1} = \ldots = \lambda_n = 0$. Also ist $\{v_1, \ldots, v_n\}$ linear unabhängig. □

**Beispiel.** Für

$$F : \mathbb{R}^2 \to \mathbb{R}^2, \qquad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -2x + 2y \\ -x + y \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

ist $F[\mathbb{R}^2] = \operatorname{span}(2, 1)$ und $\ker(F) = \operatorname{span}(1, 1)$. Für $w = (2\lambda, \lambda) \in F[\mathbb{R}^2]$ ist $F^{-1}[\{w\}] = (0, \lambda) + \ker(F)$.

**Affiner Unterraum.** $X \subseteq V$ heißt *affiner Unterraum* eines Vektorraums $V$, falls es ein $v \in V$ und einen Unterraum $U \subseteq V$ mit $X = v + U$ gibt.

**Lemma.** Ist $F : V \to W$ linear, $w \in F[V]$ und $v \in F^{-1}[\{w\}]$, so gilt $F^{-1}[\{w\}] = v + \ker(F)$. Also ist die Lösungsmenge der linearen Gleichung $F(x) = w$ der affine Unterraum, der $\ker(F)$ um eine spezielle Lösung verschiebt.

*Beweis.* Ist $x \in F^{-1}[\{w\}]$, so gilt $F(x) = w = F(v)$ und $x - v \in \ker(F)$. Ist $x \in v + \ker(F)$, so gilt $F(x) = F(v) + 0 = w$ und $x \in F^{-1}[\{w\}]$. □

**Literatur.** [F, 2.2.1–2.2.5], [FL, 2.3.2–2.3.4], [B, 2.1]

## 4.4 Quotientenräume (08.01.)

**Äquivalenz modulo eines Unterraums.** Sei $V$ ein Vektorraum und $U$ ein Unterraum von $V$. Dann ist $x \sim y :\Leftrightarrow x - y \in U$ eine Äquivalenzrelation auf $V$.

*Beweis.* Seien $x, y, z \in V$. Es gilt $x - x = 0 \in U$. Aus $x - y \in U$ folgt $y - x = -(x-y) \in U$. Aus $x-y \in U$ und $y-z \in U$ folgt $x-z = (x-y)-(y-z) \in U$. □

**Quotientenraum.** Für $v \in V$ ist der affine Unterraum $v+U$ die Äquivalenzklasse von $v$ modulo $U$. Die Menge der Äquivalenzklassen $\{v + U \mid v \in V\} =: V/U$ wird durch $(v + U) + (w + U) = (v + w) + U$, $v, w \in V$ und $\lambda \cdot (v + U) = \lambda v + U$, $\lambda \in K$, $v \in V$ zum $K$-Vektorraum, und heißt der *Quotientenraum* von $V$ modulo $U$.

*Beweis.* Für $v \in V$ ist $\{w \in V \mid w \sim v\} = \{w \in V \mid w - v \in U\} = v + U$. Für $v, v', w, w' \in V$ mit $v \sim v'$ und $w \sim w'$ folgt aus $x \sim (v' + w')$ stets $x \sim (v + w)$ und aus $x \sim \lambda v$ stets $x \sim \lambda v'$. Also sind $+$ und $\cdot$ wohldefiniert. $U$ ist der Nullvektor in $V/U$, $-v + U$ das Inverse zu $v + U$ für alle $v \in V$. □

**Lemma.** Es gilt $\dim V = \dim U + \dim V/U$.

*Beweis.* $\rho : V \to V/U$, $v \mapsto v + U$ ist linear, surjektiv mit $\ker(\rho) = U$. Also ist $\dim V = \dim \ker(\rho) + \dim \rho[V] = \dim U + \dim V/U$. □

**Satz.** Ist $F : V \to W$ linear und $U \subseteq \ker(F)$. So gibt es genau eine lineare Abbildung $\widetilde{F} : V/U \to W$ mit $F = \widetilde{F} \circ \rho$. Insbesondere ist $\ker(\widetilde{F}) = \ker(F)/U$.

*Beweis.* Es gilt $\widetilde{F}(v + U) = F(v)$ für alle $v \in V$. Für $v, v' \in V$ mit $v \sim v'$ gilt $\widetilde{F}(v' + U) = F(v') = F(v') + F(v - v') = F(v) = \widetilde{F}(v + U)$. Also ist $\widetilde{F}$ wohldefiniert. Die Linearität vererbt sich von $F$. Es gilt $v + U \in \ker(\widetilde{F})$ gdw. $v \in \ker F$ gdw. $v + U \in \ker(F)/U$. □

**Korollar.** Ist $F : V \to W$ linear und $U = \ker(F)$, so ist $\widetilde{F} : V/U \to F[V]$, $\widetilde{F}(v + U) = F(v)$ ein Isomorphismus.

**Geraden im $\mathbb{R}^2$.** Ist $V = \mathbb{R}^2$ und $U = \{(x, ax) \mid x \in \mathbb{R}\}$, so besteht $V/U$ aus Verschiebungen von $U$. Für $v \sim v'$ ist das Lot auf $U$ gleich lang.

**Literatur.** [F, 2.2.6–2.2.9]

# 5 Matrizen

## 5.1 Lineare Gleichungssysteme (11.01.)

**Lineares Gleichungssystem.** Eine Matrix $A = (a_{ij}) \in K^{m\times n}$ und ein Spaltenvektor $b \in K^m$ definieren ein lineares Gleichungssystem $Ax = b$. Ein Lösungsvektor $x \in K^n$ erfüllt $\sum_{j=1}^{n} a_{ij}x_j = b_i$ für alle $i = 1, \ldots, m$.

**Lösungsräume.** Ist $F : K^n \to K^m$, $x \mapsto Ax$, so gilt $\text{Lös}(A, b) := \{x \in K^n \mid Ax = b\} = F^{-1}[\{b\}]$ und $\text{Lös}(A, 0) = \ker(F)$. Ist $b \in F[K^n]$ und $v \in K^n$ eine Lösung von $Ax = b$, so gilt $\text{Lös}(A, b) = v + \text{Lös}(A, 0)$.

**Affine Unterräume.** Seien $V$ ein Vektorraum und $U, U'$ Unterräume von $V$, so dass $v + U = v' + U'$ für $v, v' \in V$. Dann gilt $U = U'$ und $v - v' \in U$. Man definiert deshalb $\dim(v + U) := \dim U$.

*Beweis.* Es gilt $U = \{x - y \mid x, y \in v + U\} = \{x - y \mid x, y \in v' + U'\} = U'$. Aus $v + U = v' + U$ folgt dann $v - v' \in U$. □

**Rang.** Ist $A \in K^{m\times n}$ und $F : K^n \to K^m$, $x \mapsto Ax$, so definieren $\ker A := \ker F$, $\text{Im}A := F[K^n]$ und $\text{rang}A := \dim \text{Im}A$ den *Kern*, das *Bild* und den *Rang* der Matrix $A$. Der Rang einer Matrix ist die Dimension des von den Spaltenvektoren erzeugten Unterraums, und es gilt $1 \leq \text{rang}A \leq \min(m, n)$.

*Beweis.* $\text{rang}A = \dim F[K^n] \leq m$ und $F[K^n] = \text{span}\{F(e_1), \ldots, F(e_n)\}$. $F(e_k) = Ae_k$ ist der $k$-te Spaltenvektor von $A$, weil $(Ae_k)_i = \sum_{j=1}^{n} a_{ij}(e_k)_j = a_{ik}$. Insbesondere gilt $\text{rang}A \leq n$. □

**Satz.** Sei $A \in K^{m\times n}$ und $b \in K^m$. Dann gilt: i) $\text{Lös}(A, 0)$ ist ein Unterraum von $K^n$ mit $\dim \text{Lös}(A, 0) = n - \text{rang}A$. ii) $\text{Lös}(A, b)$ ist entweder leer oder ein affiner Unterraum von $K^n$ der Dimension $n - \text{rang}A$.

**Erweiterte Matrix.** Für $A \in K^{m\times n}$ und $b \in K^n$ heißt die Matrix $(A, b) \in K^{m\times(n+1)}$, deren letzte Spalte $b$ ist, die *erweiterte* Matrix. Es gilt: $\text{Lös}(A, b) \neq \emptyset$ genau dann, wenn $\text{rang}A = \text{rang}(A, b)$.

*Beweis.* Es gilt $\text{Im}A \subseteq \text{Im}(a, b)$. Also ist $\text{rang}A = \text{rang}(A, b)$ äquivalent zu $\text{Im}A = \text{Im}(A, b)$. Dies ist äquivalent zu $b \in \text{Im}A$, was $\text{Lös}(A, b) \neq \emptyset$ bedeutet. □

**Korollar.** Sei $A \in K^{m\times n}$ und $b \in K^m$. Es gilt: $Ax = b$ besitzt genau dann eine eindeutige Lösung $x \in K^n$, wenn $\text{rang}A = \text{rang}(A, b) = n$.

*Beweis.* Wir zeigen, dass die Lösung genau dann eindeutig ist, wenn $\text{rang}A = n$. Dies gilt wegen $\dim \text{Lös}(A, b) = \dim \text{Lös}(A, 0) = n - \text{rang}A$. □

**Literatur.** [Fr], [F, 2.3], [FL, 2.3.5]

## 5.2 Lineare Abbildungen und Matrizen (15.01.)

**Satz.** Seien $V$ und $W$ Vektorräume über $K$, $B \subseteq V$ eine Basis von $V$ und $F : V \to W$ linear. Ist $G : V \to W$ linear mit $G(v) = F(v)$ für alle $v \in B$, so gilt $G = F$.

*Beweis.* Für jedes $v \in V$ gibt es $v_1, \ldots, v_n \in B$, $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Also ist $G(v) = \lambda_1 G(v_1) + \cdots + \lambda_n G(v_n) = F(v)$. □

**Geordnete Basen.** Sei $\dim V = n < \infty$. Ist die Reihenfolge der Vektoren einer Basis $B$ von $V$ wichtig, so notieren wir $B = (v_1, \ldots, v_n)$ als Tupel.

**Korollar.** Ist $(v_1, \ldots, v_n)$ eine Basis von $V$ und $w_1, \ldots, w_n \in W$, so gibt es genau ein lineares $F : V \to W$ mit $F(v_j) = w_j$ für alle $j = 1, \ldots, n$. Insbesondere gibt es einen Isomorphismus von $\mathrm{Hom}(V, W)$ nach $W^n$, und es gilt $\dim \mathrm{Hom}(V, W) = \dim W^n$.

**Matrizen.** Zu jedem linearen $F : K^n \to K^m$ gibt es genau ein $A \in K^{m \times n}$ mit $F(x) = Ax$ für alle $x \in K^n$.

*Beweis.* $F(e_j)$ ist der $j$-te Spaltenvektor von $A$. □

**Darstellende Matrizen.** Sei $(v_1, \ldots, v_n)$ eine Basis von $V$ und $(w_1, \ldots, w_m)$ eine Basis von $W$. Dann gibt es zu jedem linearen $F : V \to W$ genau ein $A \in K^{m \times n}$ mit $F(v_j) = a_{1j} w_1 + \cdots + a_{mj} w_m$ für alle $j = 1, \ldots, n$. Die so definierte Abbildung $\mathrm{Hom}(V, W) \to K^{m \times n}$, $F \mapsto A$ ist ein Isomorphimus.

*Beweis.* Für jedes $j = 1, \ldots, n$ gibt es eindeutige $a_{1j}, \ldots, a_{mj} \in K$ mit $F(v_j) = a_{1j} w_1 + \cdots + a_{mj} w_m$. Bijektivität wegen $\dim \mathrm{Hom}(V, W) = mn = \dim K^{m \times n}$. □

**Korollar.** Seien $\dim V, \dim W < \infty$, und $F : V \to W$ linear mit $\dim F[V] = r$. Dann gibt es Basen von $V$ und $W$, so dass die $F$ darstellende Matrix $A = (\mathrm{Id}_r, 0; 0, 0)$ ist.

*Beweis.* Ist $(F(v_1), \ldots, F(v_r)) = (w_1, \ldots, w_r)$ eine Basis von $F[V]$, so ergänzen wir beliebig zu einer Basis $(w_1, \ldots, w_m)$ von $W$ und mit $v_{r+1}, \ldots, v_n \in \ker F$ zu einer Basis $(v_1, \ldots, v_n)$ von $V$. Dann ist $F(v_j) = w_j$ für $j = 1, \ldots, r$ und $F(v_j) = 0$ für $j = r + 1, \ldots, n$. □

**Literatur.** [F, 2.4], [B, 2.1]

## 5.3 Multiplikation von Matrizen (18.01.)

**Lemma.** Sind $G : U \to V$, $F : V \to W$ linear, so ist $F \circ G : U \to W$ linear.

*Beweis.* Für $u, u' \in U$ und $\lambda \in K$ ist $(F \circ G)(u + u') = F(G(u) + G(u')) = (F \circ G)(u) + (F \circ G)(u')$ und $(F \circ G)(\lambda u) = F(\lambda G(u)) = \lambda(F \circ G)(u)$. □

**Herleitung.** Seien $A \in K^{m \times n}$ und $B \in K^{n \times r}$ sowie $F : K^n \to K^m$, $x \mapsto Ax$ und $G : K^r \to K^n$, $x \mapsto Bx$. Dann ist $F \circ G : K^r \to K^m$ linear und es gibt genau ein $C \in K^{m \times r}$ mit

$$(F \circ G)(x) = Cx$$

für alle $x \in K^r$. Für die $j$-te Spalte von $C =: AB$ gilt $c_j = (F \circ G)(e_j) = Ab_j$. Also ist

$$c_{ij} = (c_j)_i = \sum_{k=1}^{n} a_{ik}(b_j)_k = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

**Literatur.** [F, 2.5], [FL, 2.4.3–5]

## 5.4 Invertierbare Matrizen (22.01.)

**Matrizenring.** $K^{n\times n}$ ist ein nicht-nullteilerfreier, nicht-kommutativer Ring:

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\neq\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}.$$

*Beweis.* Die Assoziativität der Komposition von Abbildungen vererbt sich auf die Matrizenmultiplikation. □

**Rang.** Für $A\in K^{m\times n}$, $B\in K^{n\times r}$ gilt

$$\mathrm{rang}A+\mathrm{rang}B-n\leq\mathrm{rang}(AB)\leq\min\{\mathrm{rang}A,\mathrm{rang}B\}.$$

*Beweis.* Mit $F:\mathrm{Im}B\to K^m$, $x\mapsto Ax$ gilt $\mathrm{rang}(AB)=\dim F[\mathrm{Im}B]=\dim(\mathrm{Im}B)-\dim\ker F=\mathrm{rang}B-\dim\ker F$ und $\mathrm{rang}(AB)\leq\mathrm{rang}B$. Wegen $\mathrm{Im}(AB)\subseteq\mathrm{Im}A$ gilt $\mathrm{rang}(AB)\leq\mathrm{rang}A$. Außerdem folgt aus $\ker F\subseteq\ker A$ auch $\mathrm{rang}(AB)\geq\mathrm{rang}B-\dim\ker A=\mathrm{rang}B+\mathrm{rang}A-n$. □

**General linear group.** Eine Matrix $A\in K^{n\times n}$ heißt *invertierbar*, wenn es $A'\in K^{n\times n}$ mit $A'\cdot A=\mathrm{Id}$ gibt. $A'$ ist eindeutig bestimmt, heißt die zu $A$ inverse Matrix und wird mit $A^{-1}$ bezeichnet.

$$\mathrm{GL}(n,K)=\{A\in K^{n\times n}\mid A\text{ invertierbar}\}$$

ist bezüglich der Matrizenmultiplikation eine Gruppe, die nur für $n=1$ abelsch ist. Für $A\in\mathrm{GL}(n,K)$ gilt $AA^{-1}=\mathrm{Id}=A^{-1}A$, $\ker A=\{0\}$ und $\mathrm{rang}A=n$.

**Korollar.** Für $A\in\mathrm{GL}(n,K)$ und $B\in K^{n\times r}$ gilt $\mathrm{rang}(AB)=\mathrm{rang}B$. Für $A\in K^{m\times n}$ und $B\in\mathrm{GL}(n,K)$ gilt $\mathrm{Im}(AB)=\mathrm{Im}A$ und $\mathrm{rang}(AB)=\mathrm{rang}A$.

**Transponierte Matrix.** Für $A\in K^{m\times n}$ definiert $A^T\in K^{n\times m}$ mit $(A^T)_{ij}=A_{ji}$ die zu $A$ *transponierte Matrix*. Es gilt

$$(A+B)^T=A^T+B^T,\quad(AC)^T=C^TA^T,\quad(\lambda A)^T=\lambda A^T,\quad(A^T)^T=A$$

für $A,B\in K^{m\times n}$, $C\in K^{n\times r}$ und $\lambda\in K$.

**Transponiert und invertiert.** Für $A\in\mathrm{GL}(n,K)$ gilt $A^T\in\mathrm{GL}(n,K)$ mit $(A^T)^{-1}=(A^{-1})^T=:A^{-T}$.

**Literatur.** [F, 2.5], [FL, 2.4.3–5]

**Extemporale, 25.01.2013**
Name (anonymisiert als VTTMM):

Bitte bearbeiten Sie ohne Hilfsmittel in 15 Minuten die folgenden Aufgaben.

1. Sei $A \in K^{m\times n}$ und $B \in GL(n, K)$. Zeigen Sie $\operatorname{rang}(AB^{-1}) = \operatorname{rang}(A)$.

*Wegen* $B^{-1} \in GL(n, K)$ *ist* $B^{-1} : K^n \to K^n$, $x \mapsto B^{-1}$ *bijektiv, und es gilt* $\operatorname{Im}(AB^{-1}) = \operatorname{Im}(A)$ *und damit* $\operatorname{rang}(AB^{-1}) = \dim \operatorname{Im}(AB^{-1}) = \dim \operatorname{Im}(A) = \operatorname{rang}(A)$.

2. Seien $V$ und $W$ Vektorräume über einem Körper $K$, $\mathcal{A} = (v_1, \ldots, v_n)$ eine Basis von $V$, $\mathcal{B} = (w_1, \ldots, w_m)$ eine Basis von $W$ und $F : V \to W$ eine lineare Abbildung. Formulieren Sie die Definition der darstellenden Matrix von $F$ bezüglich $\mathcal{A}$ und $\mathcal{B}$.

*Die darstellende Matrix von* $F$ *bezüglich* $\mathcal{A}$ *und* $\mathcal{B}$ *ist die durch*

$$F(v_j) = \sum_{i=1}^{m} a_{ij} w_i, \qquad j = 1, \ldots, n,$$

*definierte Matrix* $A = (a_{ij}) \in K^{m\times n}$.

3. Beweisen oder widerlegen Sie:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 12 \\ 0 & 2 & 7 \\ 0 & 1 & 3 \end{pmatrix}.$$

*Die Gleichung ist nicht richtig, da das Produkt zweier oberer Dreiecksmatrizen eine obere Dreiecksmatrix ist, und die Matrix auf der rechten Seite der Gleichung in der dritten Zeile, zweiten Spalte einen Nichtnull-Eintrag hat.*

*Bewertung:* Maximal 2 Punkte pro Aufgabe, (5 & 6, 4, 3, 2, 1, 0) Punkte entsprechen der Note (1, 2, 3, 4, 5, 6). Bei 32 Teilnehmern gab es 2mal Note 1, 5mal 2, 8mal 3, 16mal 4, 1mal 5, 0mal 6. Durchschnitt: 3,28

## 5.5 Koordinatentransformationen (25.01.)

**Koordinatensystem.** Sei $V$ ein Vektorraum über $K$ und $B = (v_1, \ldots, v_n)$ ein Basis von $V$. Dann gibt es genau einen Isomorphismus $\Phi_B : K^n \to V$ mit $\Phi_B(e_j) = v_j$ für alle $j = 1, \ldots, n$. Man nennt $\Phi_B$ das durch $B$ bestimmte *Koordinatensystem* von $V$ und $x = \Phi_B^{-1}(v)$ die Koordinaten von $v \in V$.

**Transformationsmatrix.** Seien $A = (v_1, \ldots, v_n)$ und $B = (w_1, \ldots, w_n)$ Basen von $V$. Dann definiert $\Phi_B^{-1} \circ \Phi_A$ einen Isomorphismus $T_B^A : K^n \to K^n$, den wir mit der *Transformationsmatrix* $T_B^A \in \mathrm{GL}(n, K)$ identifizieren. Ist $V \ni v = x_1 v_1 + \cdots + x_n v_n = y_1 w_1 + \cdots + y_n w_n$, so gilt $y = T_B^A x$. Außerdem ist $(T_B^A)^{-1} = T_A^B$.

**Darstellende Matrizen I.** Sei $\dim V = n$, $\dim W = m$, $A$ eine Basis von $V$ und $B$ eine Basis von $W$ sowie $F : V \to W$ linear. Dann gilt für die $F$ darstellende Matrix $D = \Phi_B^{-1} \circ F \circ \Phi_A \in K^{m \times n}$. Insbesondere ist $T_B^A$ die darstellende Matrix von $\mathrm{Id} : V \to V$.

*Beweis.* Seien $A = (v_1, \ldots, v_n)$ und $B = (w_1, \ldots, w_m)$. Wir bezeichnen mit $e_j$ die kanonischen Basisvektoren des $K^n$ und $K^m$. Es gilt $\Phi_B(De_j) = \Phi_B(d_j) = \Phi_B(d_{1j}e_1 + \cdots + d_{mj}e_m) = d_{1j}w_1 + \cdots + d_{mj}w_m = F(v_j) = F(\Phi_A(e_j))$. □

**Darstellende Matrizen II.** Seien $U, V, W$ endlich-dimensionale Vektorräume mit Basen $A, B, C$ und $G : U \to V$, $F : V \to W$ linear. Für die darstellenden Matrizen gilt $D_{F \circ G} = D_F \cdot D_G$.

*Beweis.* $D_{F \circ G} = \Phi_C^{-1} \circ F \circ G \circ \Phi_A = (\Phi_C^{-1} \circ F \circ \Phi_B) \cdot (\Phi_B^{-1} \circ G \circ \Phi_A) = D_F \cdot D_G$. □

**Transformationsformel.** Seien $V, W$ endlich-dimensional, $A, A'$ Basen von $V$ und $B, B'$ Basen von $W$ sowie $F : V \to W$ linear. Dann gilt für die darstellenden Matrizen $D' = T_{B'}^B \cdot D \cdot (T_{A'}^A)^{-1}$.

*Beweis.* $D' = \Phi_{B'}^{-1} \circ F \circ \Phi_{A'} = (\Phi_{B'}^{-1} \circ \Phi_B) \cdot (\Phi_B^{-1} \circ F \circ \Phi_A) \cdot (\Phi_A^{-1} \circ \Phi_{A'}) = T_{B'}^B \cdot D \cdot (T_{A'}^A)^{-1}$. □

**Spalten- und Zeilenrang.** Sei $A \in K^{m \times n}$ und $a_1, \ldots, a_m \in K^n$ die Zeilen von $A$. Es gilt $\mathrm{rang} A = \dim \mathrm{span}\{a_1, \ldots, a_m\}$.

*Beweis.* Wir zeigen $\mathrm{rang} A^T = \mathrm{rang} A =: r$. Es gibt Basen von $K^n$ und $K^m$, so dass $A : K^n \to K^m$, $x \mapsto Ax$ durch $B = (\mathrm{Id}_r, 0; 0, 0)$ dargestellt wird. Und es gibt invertierbare Matrizen $S, T$ mit $B = SAT^{-1}$. Es gilt $A^T = T^T B^T S^{-T}$ und $\mathrm{rang} A^T = \mathrm{rang}(T^T B^T S^{-T}) = \mathrm{rang} B^T = r$. □

**Literatur.** [F, 2.6], [FL, 2.5], [B, 3.1–3.2]

## 5.6 Gaußsche Elimination I (29.01.)

**Zeilenstufenform.** Sei $A \in K^{m\times n}$ und $a_1, \dots, a_m \in K^n$ die Zeilen von $A$. Die Matrix $A$ ist in *Zeilenstufenform*, falls gilt:

1. Es gibt $0 \le r \le \min(m,n)$, so dass $a_1, \dots, a_r \neq 0$ und $a_{r+1}, \dots, a_m = 0$.
2. Für $j_i := \min\{j \mid a_{ij} \neq 0\}$ gilt $j_1 < \dots < j_r$.

In diesem Fall sind $a_1, \dots, a_r$ linear unabhängig, und $\operatorname{rang} A = r$.

**Elementare Zeilenumformungen.** Sei $P_i^j \in K^{m\times m}$ mit $(P_i^j)_{kl} = 1$ falls $k = l \notin \{i,j\}$ oder $(k,l) \in \{(i,j),(j,i)\}$, $(P_i^j)_{kl} = 0$ sonst. Dann vertauscht $x \mapsto P_i^j x$ die $i$-te und $j$-te Komponente. Sei $\lambda \in K$ und $Q_i^j(\lambda) \in K^{m\times m}$ mit $(Q_i^j(\lambda))_{kl} = 1$ falls $k = l$, $(Q_i^j(\lambda))_{ij} = \lambda$, $(Q_i^j(\lambda))_{kl} = 0$ sonst. Dann addiert $x \mapsto Q_i^j(\lambda)x$ das $\lambda$-fache der $j$-ten zur $i$-ten Komponente. Insbesondere $P_i^j, Q_i^j(\lambda) \in \mathrm{GL}(m,K)$.

*Beweis.* $(P_i^j x)_i = \sum_{l=1}^m (P_i^j)_{il} x_l = x_j$, $(P_i^j x)_j = x_i$ und $(P_i^j x)_k = x_k$ sonst. $(Q_i^j(\lambda)x)_i = \sum_{l=1}^m (Q_i^j(\lambda))_{il} x_l = x_i + \lambda x_j$ und $(Q_i^j(\lambda)x)_k = x_k$ sonst. □

**Satz.** Für jedes $A \in K^{m\times n}$ gibt es endlich viele elementare Zeilenumformungen $S_1, \dots, S_k \in \mathrm{GL}(m,K)$, so dass $S_k \cdots S_1 A$ Zeilenstufenform hat.

*Beweis.* Seien $a_1, \dots, a_n$ die Spalten von $A$.

Fall 1: Ist $a_{11} \neq 0$, so ist die erste Spalte von $B = Q_m^1(-\frac{a_{m1}}{a_{11}}) \cdots Q_2^1(-\frac{a_{21}}{a_{11}})A$ nur in der ersten Zeile nicht Null, und wir arbeiten mit $A_1 = (b_2, \dots, b_n)$ weiter.

Fall 2: Ist $a_1 = 0$, so setzen wir $A_1 = (a_2, \dots, a_n)$.

Fall 3: Ist $a_1 \neq 0$, aber $a_{11} = 0$, so gibt es $i$ mit $(P_i^1 A)_{11} \neq 0$. Wir bearbeiten $P_i^1 A$ wie in Fall 1.

In allen Fällen wird die Zahl der Spalten um Eins reduziert. Nach endlich vielen Schritten ist die Matrix in Zeilenstufenform. □

**Literatur.** [F, 0.4 & 2.7], [FL, 2.5], [B, 3.2]

## 5.7 Gaußsche Elimination II (01.02.)

**Lösbarkeit.** Seien $A \in K^{m\times n}$ und $b \in K^m$. Sei $S \in \mathrm{GL}(m,K)$ so gewählt, dass $SA$ Zeilenstufenform hat. Es gilt $\mathrm{Lös}(A,b) = \mathrm{Lös}(SA,Sb)$. Insbesondere gilt $\mathrm{Lös}(A,b) \neq \emptyset$ genau dann, wenn $(Sb)_j = 0$ für alle $j > \mathrm{rang}A$.

*Beweis.* Die Lösbarkeit ist äquivalent zu zu $\mathrm{rang}(SA) = \mathrm{rang}(SA,Sb)$. Dies ist äquivalent zu $(Sb)_j = 0$ für $j > \mathrm{rang}A$. □

**Spaltenvertauschung.** Für die Spalten $p_1,\dots,p_n$ von $P_i^j \in K^{n\times n}$ gilt $p_i = e_j$, $p_j = e_i$ und $p_k = e_k$ sonst. Also sind für $A \in K^{m\times n}$ in $AP_i^j = (Ap_1,\dots,Ap_n)$ die $i$-te und $j$-te Spalte vertauscht, und es gibt $S \in \mathrm{GL}(m,K)$ und $P \in \mathrm{GL}(n,K)$, so dass $SAP$ Zeilenstufenform mit $j_1 = 1,\dots,j_r = r$ hat.

**Lösungsraum.** $\mathrm{Lös}(SAP,Sb)$ lässt sich durch Rückwärtssubstitution parametrisieren: Seien $x_{r+1},\dots,x_n$ fest aber beliebig, $\tilde{A} = SAP$, $\tilde{b} = Sb$. Dann sind die Komponenten $x_1,\dots,x_r$ von $x \in \mathrm{Lös}(SAP,Sb)$ durch

$$x_k = (\tilde{b}_k - \tilde{a}_{k,k+1}x_{k+1} - \cdots - \tilde{a}_{k,n}x_n)/\tilde{a}_{kk}$$

für $k = r,\dots,1$ bestimmt. Und es gilt $P^{-1}x \in \mathrm{Lös}(A,b)$.

**Permutationsmatrizen.** $P \in \mathrm{GL}(n,K)$ heißt *Permutationsmatrix*, falls es eine Permutation $\pi \in S_n$ gibt, so dass $p_i = e_{\pi(i)}$ für $i = 1,\dots,n$ gilt, wobei $p_1,\dots,p_n$ die Zeilen von $P$ sind. Es gilt $P_\sigma P_\pi = P_{\pi\circ\sigma}$, so dass die Permutationsmatrizen die Gruppenstruktur von $S_n$ erben.

*Beweis.* $P_\sigma P_\pi x = P_\sigma(x_{\pi(1)},\dots,x_{\pi(n)})^T = (x_{\pi(\sigma(1))},\dots,x_{\pi(\sigma(n))})^T$. □

**Literatur.** [F, 0.4 & 2.7], [FL, 2.5], [B, 3.2]