Lineare Algebra 1

Notizen zur Vorlesung

Hans-Bert Rademacher

Wintersemester 2019/20, Universität Leipzig

1. Vorlesung, 14.10.2019

Einleitung

Linearität zwischen skalaren Größen x und $y : y = ax$ für eine Konstante a.
Linearer Zusammenhang zwischen vektorwertigen Größen $x = (x_1, x_2, \ldots, x_m) y = (y_1, y_2, \ldots, y_n)$:
Es gibt Zahlen $a_{ij}, 1 \leq i \leq n, 1 \leq j \leq m$ mit

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m \\ &\cdots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m\,. \end{aligned} \tag{1}$$

Für Werte $x = (x_1, x_2, \ldots, x_m)$ kann man nach den Gleichungen (1) $y = (y_1, y_2, \ldots, y_n)$ berechnen.. Umgekehrt entspricht der Frage, welche $x = (x_1, x_2, \ldots, x_m)$ zu gegebenem $y = (y_1, y_2, \ldots, y_n)$ die Gleichungen (1) erfüllen, die Lösung eines *Linearen Gleichungssystems.* Dies kann keine, genau eine oder unendlich viele Lösungen haben.
Die Sprache der Linearen Algebra ist grundlegend für die Mathematik, Anwendungen gibt es z.B. in in der *Analytischen Geometrie,* der *Optimierung* und der *Theoretischen Physik.*

1 Grundlegende mathematische Begriffe

1.1 Mengen

Menge (von Objekten): Es muss für Objekte feststehen, ob sie zur Menge gehören. Notationen:

$a \in A$	;		a ist Element von A
$b \notin A$	;		b ist nicht Element von A
$A \cap B$	$=$	$\{x; x \in A$ und $x \in B\}$	Durchschnitt
$A \cup B$	$=$	$\{x; x \in A$ oder $x \in B\}$	Vereinigung
$\emptyset$	;		leere Menge
$A - B = A \setminus B$	$=$	$\{x \in A; x \notin B\}$	Differenz
$A \times B$	$=$	$\{(a,b); a \in A, b \in B\}$	Produkt
$\mathcal{P}M$	$=$	$\{T; T \subset M\}$	Potenzmenge
$\mathbb{N}$	$=$	$\{1, 2, 3, \ldots\}$	Natürliche Zahlen

1.2 Begriffe der Aussagenlogik

Eine *Aussage* ist ein schriftlich-sprachliches Gebilde, dem entweder der Wahrheitswert *wahr* oder *falsch* zukommt (*Prinzip der Zweiwertigkeit*). Eine *Aussageform* $A(x)$ geht nach Einsetzen in die Variable x in eine Aussage über. Durch *Verknüpfung* von Aussagen erhält man neue Aussagen, deren Wahrheitswert sich durch die folgenden *Wahrheitstafeln* bestimmt sind:

$\wedge$	:	und	$\vee$	:	oder (einschließendes)
$\neg$	:	non (=nicht)			
$\Rightarrow$	:	folgt (impliziert)	$\Leftrightarrow$	:	äquivalent

Sprachlich gleichwertige Formulierungen für $A \Rightarrow B$ sind die folgenden: Wenn A, dann B; aus A folgt B; A impliziert B; A ist hinreichend für B; B ist notwendig für A.

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

Eine *allgemeingültige* Aussage geht durch jede Einsetzung in eine wahre Aussage über, aus ihnen ergeben sich *Schlussregeln,* nach denen man von wahren Aussagen zu neuen wahren Aussagen gelangt. *Sätze der Aussagenlogik:*

$A \vee \neg A$	;	Satz vom ausgeschlossenen Dritten, tertium non datur
$\neg(A \wedge \neg A)$	;	Satz vom Widerspruch
$\neg(\neg A) \Leftrightarrow A$	;	Satz von der doppelten Verneinung
$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$	;	Sätze von
$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$	;	de Morgan
$(A \Rightarrow B) \Leftrightarrow ((\neg B \Rightarrow \neg A)$	;	Kontrapositionssatz
$(A \Rightarrow B) \wedge A \Rightarrow B$	;	Abtrennungsregel, modus ponens
$(A \Rightarrow B) \wedge \neg B \Rightarrow \neg A$	;	Schlussregel des Aufhebens, modus tollens
$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$	;	Kettenschlussregel
$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	;	Distributiv-
$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$	;	gesetze

Für das Weglassen von Klammern gilt folgende Vereinbarung: Die Verknüpfungen $\wedge, \vee, \Rightarrow, \Leftrightarrow$ binden in dieser Reihenfolge stärker als die folgende.
Der *Allquantor* $\forall x \in M : A(x)$ bzw. $\forall_{x \in M} A(x)$ bedeutet: Für alle $x \in M$ gilt $A(x)$. Der *Existenzquantor* $\exists x \in M : A(x)$ bzw. $\exists_{x \in M} A(x)$ bedeutet: Es gibt ein $x \in M$, für das $A(x)$ gilt. Es gelten folgende Verneinungsregeln:

$$\neg \forall_x A(x) \Leftrightarrow \exists_x \neg A(x) \; ; \; \neg \exists_x A(x) \Leftrightarrow \forall_x \neg A(x) \,.$$

Bei Aussagenformen in zwei Variablen die folgenden Vertauschungsregeln:

$$\forall_x \forall_y A(x,y) \Leftrightarrow \forall_y \forall_x A(x,y) \, ; \; \exists_x \exists_y A(x,y) \Leftrightarrow \exists_y \exists_x A(x,y)$$
$$\exists_y \forall_x A(x,y) \Rightarrow \forall_x \exists_y A(x,y)$$

2. Vorlesung, 16.10.19

1.3 Abbildungen

Eine *Abbildung* $f : D \longrightarrow M$ ordnet jedem Element $x \in D$ aus dem *Definitionsbereich* D genau ein Element $f(x) \in M$ (genannt das *Bild*) zu.
Die Abbildung heißt *injektiv* wenn für alle $x, y \in D$ mit $f(x) = f(y)$ gilt: $x = y$.
Eine Abbildung heißt *surjektiv* wenn es zu jedem $y \in M$ ein $x \in D$ gibt, so dass $y = f(x)$.
Die Menge $f(D) := \{f(d)\,;\, d \in D\}$ heißt das *Bild* von f. f ist surjektiv genau dann, wenn $f(D) = M$.
Eine Abbildung heißt *bijektiv,* wenn sie injektiv und surjektiv ist. Dann ist die *Umkehrabbildung* $f^{-1} : M \longrightarrow D, x = f^{-1}(y) \Leftrightarrow y = f(x)$ erklärt. Die *Identität* einer Menge D ist die Abbildung: $\mathrm{id}_D : D \longrightarrow D, x \mapsto x$.
Zwei Mengen $D; M$ heißen *gleichmächtig,* wenn es eine Bijektion $f : D \longrightarrow M$ gibt.
Für Abbildungen $f : D \longrightarrow M, g : M \longrightarrow N$ ist die *Komposition* die folgende Abbildung: $g \circ f : D \longrightarrow N\,;\, (g \circ f)(x) = g(f(x))$. Dann gilt für die Umkehrabbildung f^{-1} einer bijektiven Abbildung $f : D \longrightarrow M$:

$$f^{-1} \circ f = \mathrm{id}_D\,;\, f \circ f^{-1} = \mathrm{id}_M.$$

1.4 Beweise

Ein *Beweis* ist die Ableitung einer Aussage nach aussagenlogischen Schlussregeln. Zu Grunde gelegt werden als wahr postulierte Aussagen (auch *Axiome* genannt), auf die in Beweisen zurückgegriffen werden darf. An das Axiomensystem stellt man die Anforderung der *logischen Unabhängigkeit* und der *Widerspruchsfreiheit.*
Ein *Beweis* ist die Begründung eines Satzes aus den Axiomen der Theorie mit Hilfe logischer Schlüsse.
Beweismethoden

- **Direkter Beweis:**
  Aus der Gültigkeit der Voraussetzung A (Prämisse) wird mit Hilfe gültiger Schlüsse die Folgerung B (Konklusion) hergeleitet.

  Satz 1.4.1. *Das Quadrat einer ungeraden natürlichen Zahl ist ungerade.*

- **Indirekter Beweis:**
  Um $A \Rightarrow B$ zu zeigen, geht man von der Verneinung der Schlussfolgerung B aus und leitet daraus einen Widerspruch her.

  Satz 1.4.2 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

- **Vollständige Induktion:**
  Sei $A(n)$ eine Aussageform über der Menge $\mathbb{N}$ der natürlichen Zahlen. Wenn gilt

  1. $A(1)$ *Induktionsanfang*
  2. $\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)$ *Induktionsschluss*

  dann gilt $\forall n \in \mathbb{N} : A(n)$.

  Satz 1.4.3. $1 + 2 + \cdots + n = n(n+1)/2$ *für alle* $n \in \mathbb{N}$.

3. VORLESUNG, 21.10.19

Definition 1.4.4. *Für eine natürliche Zahl n definieren wir die Fakultät $n! = \prod_{k=1}^{n} k$.*

Satz 1.4.5. *Die Anzahl A_n der Anordnungen einer n-elementigen Menge ist $n!$.*

1.5 Gruppen

Definition 1.5.1. *Eine* Gruppe *ist ein Paar $(G, \circ)$ bestehend aus einer Menge G und einer Abbildung (die* Verknüpfung *genannt wird)*

$$\circ : G \times G \longrightarrow G; (a, b) \longmapsto a \circ b$$

mit folgenden Eigenschaften (auch Gruppenaxiome *genannt):*

1. Assoziativgesetz: $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$.
2. Existenz des neutralen Elements: $\exists e \in G \forall a \in G : e \circ a = a$.
3. Existenz des inversen Elements: $\forall a \in G \exists b \in G : b \circ a = e$.

Die Gruppe heißt kommutativ *oder* abelsche Gruppe *wenn zusätzlich gilt:* $\forall a, b \in G : a \circ b = b \circ a$.

Beispiel 1.5.2. (1) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe. Die Menge der*rationalen Zahlen* $\mathbb{Q} = \{p/q\,;\, p, q \in \mathbb{Z}, q \neq 0\}$ ist mit der Addition eine abelsche Gruppe.

(2) Sei $\mathbb{Q}^* = \mathbb{Q} - \{0\}$. Dann ist $(\mathbb{Q}^*, \cdot)$ eine abelsche Gruppe.

(3) Sei $M \neq \emptyset$. $S(M) = \{f : M \longrightarrow M; f \text{ ist bijektiv }\}$ heißt die Menge der *Permutationen* von M. Dann ist $(S(M), \circ)$ mit der Komposition von Abbildungen (vgl. Abschnitt 1.3) eine Gruppe, sie wird auch die *symmetrische Gruppe* von M genannt. Für $n \in \mathbb{N}$ setze $S_n = S(\{1, 2, \ldots, n\})$. Dann ist $S_n, n \geq 3$ eine Gruppe mit $n!$ Elementen, die nicht abelsch ist

Lemma 1.5.3. *Sei $(G, \circ)$ eine Gruppe. Dann gilt:*

(a) Für das neutrale Element e gilt: $\forall a \in G : a \circ e = a$.

(b) Es gibt genau ein neutrales Element e.

(c) Wenn b ein (links)inverses Element ist zu a, so ist es auch rechtsinvers, d.h. es gilt: $a \circ b = e$.

(d) Zu jedem $a \in G$ gibt es genau ein inverses Element, das wir dann mit a^{-1} bezeichnen.

4. Vorlesung, 23.10.19

Lemma 1.5.4. *Eine nicht-leere Menge G zusammen mit einer Verknüpfung $\circ : G \times G \longrightarrow G$ ist eine Gruppe genau dann, wenn die Verknüpfung assoziativ ist und wenn es zu je zwei Elementen $a, b \in G$ ein $x \in G$ gibt mit $x \circ a = b$ und ein $y \in G$ mit $a \circ y = b$. Dann sind x, y eindeutig bestimmt.*

Satz 1.5.5. *Es sei $(G, \circ)$ eine Gruppe. Dann gelten folgende Aussagen für $a, b \in G$:*

(a) $\left(a^{-1}\right)^{-1} = a$.

(b) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Definition 1.5.6. *Sei $(G, \circ)$ eine Gruppe, für jedes $g \in G$ wird durch*

$$L_g : G \longrightarrow G, x \mapsto g \circ x$$

die Linkstranslation *und durch*

$$R_g : G \longrightarrow G, x \mapsto x \circ g$$

die Rechtstranslation *mit dem Element $g \in G$ definiert.*

Definition 1.5.7. *Eine Untergruppe H der Gruppe $(G, \circ)$ ist eine Teilmenge $H \subset G$, die mit der Einschränkung der Verknüpfung $\circ$ eine Gruppe bildet.*

Satz 1.5.8 (Untergruppenkriterium)**.** *Eine nicht-leere Teilmenge $H \subset G$ einer Gruppe $(G, \circ)$ besitzt die Struktur einer Untergruppe genau dann, wenn eine der beiden folgenden Aussagen erfüllt ist:*

(a) Für jedes $x, y \in H$ gilt $x \circ y^{-1} \in H$.

(b) Für alle $x, y \in H$ gilt $x^{-1} \in H$ und $x \circ y \in H$.

Beispiel 1.5.9. (1)Für eine natürliche Zahl m ist die Teilmenge $m\mathbb{Z} = \{mx; x \in \mathbb{Z}\}$ eine Untergruppe

(2) Für natürliche Zahlen k, m ist die Teilmenge $mk\mathbb{Z} \subset m\mathbb{Z}$ eine Untergruppe von $m\mathbb{Z}$.

(3) Sei für eine nicht-leere Menge M die Gruppe $S(M)$ der Permutationen gegeben. Für ein $x \in M$ sei $S_x(M)$ die Menge der Permutationen, die das Element x fest lassen, d.h.

$$S_x(M) = \{f \in S(M); f(x) = x\}.$$

Dann ist $S_x(M)$ eine Untergruppe.

Definition 1.5.10. *Es seien $(G, \circ)$ und $(G', \circ')$ Gruppen. Dann heißt eine Abbildung $f : G \longrightarrow G'$ ein* Gruppenhomomorphismus, *bzw.* Homomorphismus *(von Gruppen), falls für alle $x, y \in G$ gilt: $f(x \circ y) = f(x) \circ' f(y)$. (von nun an werden wir beide Gruppenoperationen $\circ$, $\circ'$ mit demselben Symbol bezeichnen.)*

Beispiel 1.5.11. (a) Für $m \in \mathbb{N}$ ist die Abbildung $f_m : \mathbb{Z} \longrightarrow m\mathbb{Z}, f_m(x) = mx$ ein Gruppenhomomorphismus zwischen den Gruppen $(\mathbb{Z}, +)$ und $(m\mathbb{Z}, +)$.

(b) Die Abbildung $e : \mathbb{Z} \longrightarrow \mathbb{Q}^*, e(m) = 2^m$ ist ein Gruppenhomomorphismus zwischen den Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Q}^+, \cdot)$

(c) Für eine Gruppe G und ihre symmetrische Gruppe $S(G)$ (vgl. Beispiel 1.5.2) ist die Abbildung $f : G \longrightarrow S(G), f(g) = L_g$ ein Homomorphismus.

5. Vorlesung, 28.10.19

Satz 1.5.12. *Wenn $G; G'$ Gruppen sind mit neutralem Element e, e' und wenn $f : G \longrightarrow G'$ ein Gruppenhomomorphismus ist, dann gilt $f(e) = e'$ und $f\left(x^{-1}\right) = f(x)^{-1}$ für alle $x \in G$.*

Definition 1.5.13. *Für einen Gruppenhomomorphsimus $f : G \longrightarrow G'$ heißt* $\ker f := f^{-1}(e') = \{x \in G; f(x) = e'\}$ *der* Kern *und* $imf = f(G) = \{f(x); x \in G\}$ *das* Bild *von f.*

Satz 1.5.14. *Sei $f : G \longrightarrow G'$ ein Gruppenhomomorphsimus.*

(a) Wenn $H' \subset G'$ eine Untergruppe ist, dann ist das Urbild $f^{-1}(H') \subset G$ eine Untergruppe von G. Insbesondere ist der Kern $\ker f$ eine Untergruppe von G.

(b) Das Bild imf ist eine Untergruppe von G'.

Satz 1.5.15. *Wenn $f : G \longrightarrow G', f' : G' \longrightarrow G''$ Gruppenhomomorphsimen sind, dann ist auch die Komposition $f' \circ f : G \longrightarrow G''$ ein Gruppenhomomorphismus.*

Satz 1.5.16. *Ein Gruppenhomomorphismus $f : G \longrightarrow G'$ ist injektiv genau dann, wenn der Kern trivial ist, d.h.* $\ker f = \{e\}$, *wobei e das neutrale Element der Gruppe G ist.*

Bemerkung 1.5.17. (a) Ein bijektiver (Gruppen-)Homomorphismus $f : G \longrightarrow G'$ heißt auch *(Gruppen-)Isomorphismus.* Wenn $G = G'$ so wird ein Isomorphismus auch *Automorphismus* genannt. Die Menge $\mathrm{Aut}(G)$ der Automorphismen einer Gruppe bildet ihrerseits wieder eine Gruppe, und zwar eine Untergruppe der Permutationsgruppe $S(G)$.

(b) Für $g \in G$ heißt die Komposition $i_g := L_g \circ R_{g^{-1}} = R_{g^{-1}} \circ L_g$ der durch das Element g bestimmte *innere Automorphismus.* Dann definiert die Abbildung $i : G \longrightarrow \mathrm{Aut}(g), g \longmapsto i_g$ einen Gruppenmorphismus. Das Bild ist dann die *Untergruppe der inneren Automorphismen.* Für eine abelsche Gruppe ist jeder innere Automorphismus die Identität.

1.6 Quotientengruppen

Definition 1.6.1. *Eine* Relation *R bzw. $\sim$ auf einer Menge M ist eine Teilmenge $R \subset M \times M$. Wenn $(x, y) \in R$ so schreiben wir auch $x \sim y$. Diese Relation ist eine* Äquivalenzrelation, *wenn folgende Bedingungen erfüllt sind:*

*(a) Für alle $x \in M$ gilt: $x \sim x$(*Reflexivität*)*

*(b) Für alle $x, y \in M$ gilt: Wenn $x \sim y$, dann gilt auch $y \sim x$. (*Symmetrie*)*

*(c) Für alle $x, y, z \in M$ gilt: Wenn $x \sim y$ und $y \sim z$ dann gilt auch $x \sim z$. (*Transitivität*)*

Beispiel 1.6.2. (a) Die Gleichheitsrelation ist eine Äquivalenzrelation. Dann entspricht der Relation die Teilmenge $\Delta_M = \{(x, x)\,;\, x \in M\}$ die auch die *Diagonale* genannt wird.

(b) Für $m \in \mathbb{N}$ definieren wir $x \sim y$ genau dann, wenn $y - x \in m\mathbb{Z}$, also wenn x und y bei Division durch m den gleichen Rest haben, dafür ist auch die folgende Notation üblich:

$$x \equiv y \pmod m,$$

(x ist *kongruent* y *modulo* m.)

6.Vorlesung 30.10.2019

Definition 1.6.3. *Wenn $\sim$ eineÄquivalenzrelation auf einer Menge M ist, dann ist eine* Äquivalenzklasse *oder* Restklasse *eine Teilmenge $N \subset M$ so dass für alle $x, y \in N$ gilt: $x \sim y$ und für jedes $x \in N$ gilt: Falls $y \sim x$ dann ist $y \in N$.*

Somit bestimmt jedes Element $x \in M$ eine Äquivalenzklasse $[x] = \{y \in M\,;\, y \sim x\}$. Wenn also $x \in [y]$ dann gilt $x \sim y$.

Beispiel 1.6.4. Wir bestimmen die Äquivalenzklassen in den Beispielen 1.6.2:

(a) $[x] = \{x\}$ für jedes $x \in M$.

(b) $[x] = \{x + km\,;\, k \in \mathbb{Z}\}$. Sei z.B. $m = 5$, dann gilt: $[3] = \{\ldots, -7, -2, 3, 8, \ldots\}$. Dann gilt $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$.

Definition 1.6.5. *Eine* Partition *einer nicht-leeren Menge M ist eine Familie $A_i, i \in I$ von nicht-leeren Teilmengen $A_i \subset M$, die paarweise disjunkt sind (also $A_i \cap A_j = \emptyset$ für $i \neq j$.)und $M = \bigcup_{i \in I} A_i$. (*disjunkte Vereinigung*)*

Satz 1.6.6. *(a) Eine Äquivalenzrelation $\sim$ auf M bestimmt eindeutig eine Partition von M durch die Restklassen.*

(b) Umgekhrt bestimmt eine Partition $A_i, i \in I$ eindeutig eine Äquivalenzrelation. Wenn $x \in A_i$, so ist $[x] = A_i$.

Satz 1.6.7. *Sei H eine Untergruppe der Gruppe G. Dann ist die Relation $x \sim_H y$, die durch $x \circ y^{-1} \in H$ erklärt wird, eine Äquivalenzrelation.*

Der Einfachheit halber werden wir im folgenden die Verknüpfung mit einem Punkt $\cdot$ notieren oder das Zeichen ganz weglassen, so wie sie das von der Multiplikation rationaler oder reeller Zahlen gewohnt sind.

Definition 1.6.8. *Eine Untergruppe $H \subset G$ der Gruppe G heißt* invariant *oder* Normalteiler, *wenn für alle $g \in G$ und alle $h \in H$ gilt: $ghg^{-1} \in H$. (Kurz auch als $gHg^{-1} = H$ geschrieben)*

Theorem 1.6.9. *Wenn $H \subset G$ ein Normalteiler ist, dann ist auf der Menge $G/H = \{[x]\,;\, x \in G\}$ der Restklassen durch $[x] \cdot [y] = [x \cdot y]$ eine Gruppenstruktur erklärt (man sagt auch* induziert*).*

Beispiel 1.6.10. Sei $G = \mathbb{Z}, H = m\mathbb{Z}$. Da G abelsch ist $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$ eine Gruppe. Nach Beispiel 1.6.2 können wir die Restklassen in der Form $[0], [1], \ldots, [m-1]$ schreiben, es gilt $[k] + [l] = [k + l]$.

Theorem 1.6.11 (1. Homomorphiesatz für Gruppen)**.** *Wenn $f : G \longrightarrow G'$ ein Homomorphismus zwischen Gruppen ist, dann ist der Kern $\ker f$ von f eine Normalteiler von G und die Quotientengruppe $G/\ker(f)$ ist isomorph zum Bild $\mathrm{im} f$.*

7. Vorlesung, 4.11.19

Beispiel 1.6.12. Wenn G eine Gruppe ist, dann ist die Abbildung $f : G \longrightarrow S(G), f(g) = i_g$ ein Homomorphismus von Gruppen. Hier ist $i_g : G \longrightarrow G\,;\, x \mapsto g \cdot x \cdot g^{-1}$ der durch $g \in G$ definierte innere Automorphismus, vgl. Bemerkung 1.5.17(b). Dann gilt:

$$\ker f = \{x \in G\,;\, g \cdot x \cdot g^{-1} = x\}\,.$$

Diese invariante Untergruppe wird auch *Zentrum* $Z(G)$ der Gruppe genannt. Nach dem 1.Homomorphiesatz sind also die Quotientengruppe $G/Z(G)$ und die Gruppe $f(G)$ der inneren Automorphismen isomorph.

1.7 Ringe und Körper

Definition 1.7.1. *Ein* Ring *ist eine Menge R mit mindestens zwei Elementen und mit zwei Verknüpfungen $+, \cdot$, die folgenden Bedingungen erfüllen:*

(a) $(R, +)$ *ist eine abelsche Gruppe, das neutrale Element wird mit* 0 *bezeichnet.*

(b) die Multiplikation $\cdot$ ist assoziativ, d.h. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ gilt für alle $x, y, z \in R$ und es gibt eine Eins, *d.h. ein mit 1 bezeichnetes Element, so dass $1 \cdot x = x \cdot 1 = x$ für alle $x \in R$.*

*(c) Es gelten die folgenden Beziehungen zwischen Addition und Multipliaktion (*Distributivgesetze*):*

$$x \cdot (y + z) = x \cdot y + x \cdot z\,;\, (x + y) \cdot z = x \cdot z + y \cdot z.$$

Falls zusätzlich die Menge $R^* = R - \{0\}$ bezüglich der Multipliation eine Gruppe bildet mit 1 als neutralem Element, so heißt der Ring auch Körper. *Wenn die Multiplikation kommutativ ist, so heißt der Ring bzw. Körper auch* kommutativ.

Es wird hier nicht verlangt, dass die Multipliation kommutativ ist, obwohl wir meist nur kommutative Körper betrachten werden.

Beispiel 1.7.2.

(a) $(\mathbb{Z}, +, \cdot)$ ist ein Ring, aber kein Körper.

(b) $(\mathbb{Q}, +, \cdot)$ ist ein komutativer Köper.

(c) Die Menge $\mathbb{Z}[t]$ der *Polynome* $p(t) = \sum_{j=0}^{\infty} a_j t^t, a_i \in \mathbb{Z}$, wobei $a_j \neq 0$ für endlich viele j bildet einen kommutativen Ring, aber keinen Körper. Zwei Polynome $\sum_j a_j t^j, \sum_j b_j t^j$ sind gleich genau dann, wenn $a_j = b_j$ für alle $j \geq 0$. Die Addition und Multipliation sind in der naheliegenden Weise definiert:

$$\begin{aligned}(a_0 + a_1 t + a_2 t^2)(b_0 + b_1 t + b_2 t^2) &= (a_0 + b_0) + (a_0 b_1 + a_1 b_0)t \\ &+ (a_0 b_2 + a_1 b_1 + a_2 b_0)t^2 + (a_1 b_2 + a_2 + b_1)t^3 + (a_2 b_2)t^4.\end{aligned}$$

(d) $(\mathbb{R}, +, \cdot)$ ist der kommutative Körper der reellen Zahlen. Reelle Zahlen können durch Dezimaldarstellungen erklärt werden, d.h. durch Folgen rationaler Zahlen.

Satz 1.7.3 (Rechenregeln für einen Ring bzw. Körper)**.** *In einem Ring* $(R, +, \cdot)$ *gilt:*

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

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

(c) $1 \cdot x = 1 \Rightarrow x = 1$.

(d) $0 \neq 1$.

In einem Körper gilt darüber hinaus:

(e) $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$.

(f) $x^2 = x \cdot x = 1 \Leftrightarrow x = \pm 1$.

Beispiel 1.7.4. Wir haben in Beispiel 1.6.2(b) bzw. Beispiel 1.6.4 gesehen, dass $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$ mit der Addition eine abelsche Gruppe ist. Auf $\mathbb{Z}_m$ ist auch die Multiplikation erklärt durch $[x] \cdot [y] = [x \cdot y]$. Dies ist wohldefiniert, sei $[x] = [x'], [y] = [y']$, dann gilt $x = x' + am, y = y' + bm$, somit $x \cdot y = x' \cdot y' + m(ay' + bx' + abm)$. Also $[x \cdot y] = [x' \cdot y']$. Dann ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring, die anderen Bedingungen für einen Ring sind erfüllt, da $(\mathbb{Z}, +, \cdot)$ ein Ring ist.

Bemerkung 1.7.5. Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Form $m\mathbb{Z}$, vgl. Aufgabe 2-4. Wenn dann G die Untergruppe von $\mathbb{Z}$ ist, die von den Untergruppen $p\mathbb{Z}$ und $q\mathbb{Z}$ erzeugt wird, dann gibt es ein $r \in \mathbb{N}$ mit $G = r\mathbb{Z}$. Dabei ist r der größte gemeinsame Teiler von p, q, also $r = \mathrm{ggT}(p, q)$. Wenn p, q *relativ prim* sind, d.h. keinen gemeinsamen Teiler verschieden von 1 besitzen, gibt es ganze Zahlen a, b mit $pa + qb = 1$.

Satz 1.7.6. *Für* $m \in \mathbb{N}$ *ist der Ring* $(\mathbb{Z}_m, +, \cdot)$ *ein Körper genau dann, wenn* m *eine Primzahl ist.*

8. VORLESUNG, 6.11.19

2 Vektorräume und Lineare Abbildungen

2.1 Vektorräume

Definition 2.1.1. *Sei K ein Körper. Dann heißt die Menge V mit der Verknüpfung $+ : (x,y) \in V \times V \longmapsto x + y \in V$ und der Skalarmultipliation $\cdot : (\alpha, x) \in K \times V \longrightarrow \alpha x \cdot = \alpha x \in V$ ein K-*Vektorraum, *wenn $(V,+)$ eine abelsche Gruppe ist und folgendes für alle $\alpha, \beta \in K, x, y \in V$ gilt:*

(a) $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$.

(b) $\alpha(x + y) = \alpha x + \alpha y$.

(c) $\alpha(\beta x)) = (\alpha\beta)x$.

(d) $1x = x$.

Beispiel 2.1.2. (a) $V = K$ ist ein K-Vektorraum.
(b) Für eine natürliche Zahl n ist die Menge der n-Tupel: $V = K^n = K \times \cdots \times K = \{x = (x_1, x_2, \ldots, x_n)\,;\, x_j \in K\}$ ein Vektorraum.
(c) Für eine Menge M sei $\mathrm{Abb}(M,K)$ die Menge aller Abbildungen $f : M \longrightarrow K$ in den Körper K. Dann ist $\mathrm{Abb}(M,K)$ ein K-Vektorraum, dabei wird erklärt: $(f+g)(x) = f(x) + g(x)$ und $(\alpha f)(x) = \alpha f(x)$.
(d) Für einen Körper K ist die Menge $K[t]$ aller Polynome der Form $p(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n$ für ein $n \in \mathbb{N}_0$ ein Vektorraum. Wir setzen dann für dieses Polynom $a_j = 0$ für $j > n$, also können wir das Polynom auch schreiben als

$$p(t) = \sum_{j=0}^{\infty} a_j t^j$$

wobei es eine natürliche Zahl n gibt, so dass $a_j = 0$ für alle $j > n$. Man sagt auch: *Fast alle* Koeffizienten a_j verschwinden, hier bedeutet *fast alle* bis auf eine endliche Ausnahmemenge.
Addition:

$$\sum_{j \geq 0} a_j t^j + \sum_{j \geq 0} b_j t^j = \sum_{j \geq 0} (a_j + b_j)\, t^j.$$

Skalarmultiplikation:

$$\alpha \sum_j a_j t^j = \sum_j (\alpha a_j)\, t^j\,.$$

Satz 2.1.3. *Sei V ein K-Vektorraum. Dann gelten folgende Rechenregeln:*

(a) $0x = 0$ *für alle $x \in V$. (Die erste 0 ist die 0 im Vektorraum, die zweite 0 ist das neutrale Element im Körper)*

(b) $(-1)x = -x$ *für alle $x \in V$.*

(c) $\alpha 0 = 0$ *für alle $\alpha \in K$.*

Definition 2.1.4. *Eine Teilmenge $U \subset V$ eines Vektorraums V über dem Körper K mit deer Vektoraddition $+$ und Skalarmultiplikation $\cdot$ heißt* Unterraum, *falls U mit der Vektoraddition und der Skalarmultiplikation (also der* induzierten Struktur*) ebenfalls ein Vektorraum ist.*

Diese Defintion entspricht der Definition **??** einer Untergruppe. Analog zur Charakterisierung der Untergruppen in Satz 1.5.8 erhalten wir:

Satz 2.1.5 (Unterraumkriterium)**.** *Eine nichtleere Teilmenge $U \subset V$ eines Vektorraums V ist ein Untervektorraum von V genau dann, wenn eine der folgenden Bedingungen erfüllt ist:*

(a) Für alle $x, y \in U$ und $\alpha \in K$ gilt: $x + y \in U$ und $\alpha x \in U$.

(b) Für alle $x, y \in U$ und $\alpha, \beta \in K$ gilt: $\alpha x + \beta y \in U$.

Beispiel 2.1.6. (a) Für $1 \leq m \leq n$ ist

$$K^m \times \{(0, \ldots, 0)\} \in K^{n-m}\} = \{(x_1, \ldots, x_m, 0, \ldots, 0)\,;\, x_i \in K\}$$

ein Untervektorraum von K^n.

(b) Wenn $N \subset M$ dann ist $U := \{f \in \mathrm{Abb}(M, K)\,;\, f(x) = 0 \forall x \in N\}$ ein Untervektorraum von $\mathrm{Abb}(M, K)$.

(c) Der Grad $\deg(p)$ eines Polynoms $p \in K[t]$ mit $p(t) = \sum_j a_j t^j$ ist die größte Zahl $n \geq 0$ mit $a_n \neq 0$, es gilt $\deg p = -1$ für das Nullpolynom. Dann ist für ein $n \in \mathbb{N}$ die Menge $\{p \in K[t]\,;\, \deg(p) \leq n\}$ der Polynome vom Grad höchstens n ein Untervektorraum.

Bemerkung 2.1.7. Folgende Aussagen verifiziert man mit dem Unterraumkriterium 2.1.5.

(a) Wenn $U_1, \ldots, U_m$ Untervektorräume sind des Vektorraums V, dann ist der Durchschnitt $\cap_{j=1,2,\ldots,m} U_j = U_1 \cap \ldots \cap U_m$ ebenfalls ein Untervektorraum.
Diese Aussage gilt auch für eine unendliche Menge von Untervektorräumen $U_i, i \in I$, d.h. dann ist auch $\cap_{i \in I} U_i$ ein Untervektorraum.

(b) Wenn $U_1, \ldots, U_m$ Untervektorräume sind eines Vektorraums V dann ist die *Summe* $U_1 + \ldots + U_m = \{v_1 + \ldots + v_m\,;\, v_j \in U_j\}$ ebenfalls ein Untervektorraum.
Dies gilt auch für eine unendliche Indexmenge I, wenn man die Summe $\sum_i U_i$ folgendermaßen definiert: $v \in \sum_{i \in I} U_i \Leftrightarrow v = \sum_{i \in I} v_i$ wobei fast alle (bis auf eine endliche Ausnahme) $v_i = 0$ sind, also $\#\{i \in I\,;\, v_i \neq 0\} < \infty$.

9. VORLESUNG, 11.11.19

2.2 Lineare Abbildung

Wir führen nun die strukturerhaltenden Abbildungen zwischen Vektorräumen ein. Dies wird ermöglichen zu präzisieren, wann Vektorräume die gleiche Struktur haben (wir werden dies später auch *isomorph* nennen).

Definition 2.2.1. *Eine Abbildung* $f : V \longrightarrow W$ *zwischen* K*-Vektorräumen* V, W *heißt* linear, *wenn für alle* $x, y \in V$ *und* $\alpha, \beta \in K$ *gilt:*

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y). \tag{2}$$

Beispiel 2.2.2. (a) Die O-Abbildung $V \longrightarrow K, x \mapsto =$ ist linear, ebenso die Identität $\mathbb{1}_V : x \in V \longrightarrow x \in V$.

(b) Wenn $V = K^n$, so heißt für $k \in \{1, 2, \ldots, n\}\}$ die Abbildung

$$\mathrm{pr}_k : (x_1, \ldots, x_n) \in K^n \mapsto x_k \in K$$

die Projektion des Vektors x auf seine k-te Komponente.

(c) Wenn $V = K[t]$ so ist die Abbildung

$$D : \sum_{j \geq 0} a_j t^j \longmapsto \sum_{j \geq 1} j a_j t^{j-1}$$

linear. Für $K = \mathbb{R}$ entspricht das der Ableitung des Polynoms (vgl. Analysis).

(d) Für eine Menge M und ein Element $a \in M$ heißt die Abbildung

$$E_s : \mathrm{Abb}(M, K) \longrightarrow K \,;\, E_a(f) = f(a)$$

die *Auswertungsabbildung* in a, sie ist linear.

Eine lineare Abbildung kann man auch als Vektorraum-Homomorphismus bezeichnen, in Analogie zur entsprechenden Aussage bei Gruppen erhalten wir:

Satz 2.2.3. *Sei* $f : V \longrightarrow W$ *eine lineare Abbildung zwischen Vektorräumen. Dann gilt:*

(a) Wenn $U \subset W$ *ein Unterraum ist, dann ist das Urbild* $f^{-1}(U) \subset V$ *ein Unterraum von* V*. Insbesondere ist der* Kern $\ker f := \{x \in V \,;\, f(x) = 0\}$ *von* f *ein Untervektorraum von* V*.*

(b) Das Bild $imf := f(V) = \{f(x) \,;\, x \in V\}$ *ist ein Untervektorraum von* W*.*

Beispiel 2.2.4. Vgl. Beispiel 2.2.2: (a) Für die Nullabbildung gilt: $\ker 0 = V, \mathrm{im} 0 = 0$. Für die Identität $\mathbb{1}_V : \ker \mathbb{1}_V = 0; \mathrm{im} \mathbb{1}_V = V$.
(b) Für die Projektion $\mathrm{pr}_k : K^n \longrightarrow K$ auf die k-te Komponente gilt: $\ker \mathrm{pr}_k = \{x \in K^n; x_k = 0\}; \mathrm{impr}_k = K$.
(c) Sei $V = \mathbb{Q}[t]$ oder $V = \mathbb{R}[t]$. Dann ist $\ker D = \{\sum_j a_j t^j \,;\, a_j = 0$ für alle $j > 0\}$, d.h. die konstanten Polynome. Die Abbildung ist surjektiv, d.h. $\mathrm{im} D = \mathbb{Q}[t]$, da $D\left(\sum_j b_j t^j\right) = \sum_j a_j t^j$ mit $b_j = a_{j+1}/(j+1)$ falls $a_{j+1} \neq 0$, und $b_j = 0$ falls $a_{j+1} = 0$.

(d) Sei $V = \mathbb{Q}[t]$ oder $V = \mathbb{R}[t]$, d.h. $K = \mathbb{Q}$ oder $K = \mathbb{R}$. Wähle $s \in K$. Dann betrachten wir die Auswertungsabbildung

$$ev_s : K[t] \longrightarrow K\,;\, ev_s(p) = ev_s\left(\sum_j a_j t^j\right) = p(s) = \sum_j a_j s^j.$$

Dann besteht der Kern aus den Polynomen, für die s eine Nullstelle ist, also

$$\ker ev_s = \{p \in K[t]\,;\, p(s) = 0\} = \left\{\sum_j a_j t^j \in K[t]\,;\, \sum_j a_j s^j = 0\right\}.$$

Für $s = 0$ gilt insbesondere

$$\ker ev_0 = \{p \in K[t]\,;\, p(0) = 0\} = \left\{\sum_j a_j t^j \in K[t]\,;\, a_0 = 0\right\} = \{tp\,;\, p \in K[t]\} = tK[t].$$

Da lineare Abbildungen die Vektorraumhomomorphismen sind, erhalten wir für lineare Abbildungen analoge Aussagen zu den Ergebnissen für Gruppenhomomorphismen:

Satz 2.2.5. *(a) Wenn $f : U \longrightarrow V, g : V \longrightarrow W$ lineare Abbildungen zwischen Vektorräumen sind, dann ist auch die Komposiition $g \circ f : U \longrightarrow W$ linear.*

(b) Wenn die lineare Abbildung $f : V \longrightarrow W$ bijektiv ist (auch linearer Isomorphismus *genannt), dann ist auch die Umkehrabbildung $f^{-1} : W \longrightarrow V$ linear (und damit eine linearer Isomorphismus).*

Bemerkung 2.2.6. (a) Ein linearer Isomorphismus $f : V \longrightarrow V$ heißt auch *linearer Automorphismus*. Die linearen Automorphismen bilden eine Untergruppe $\mathrm{Aut}(V) = \{f : V \longrightarrow V, f \text{ linearer Isomorphismus}\}$ der symmetrischen Gruppen $S(V) = \{f : V \longrightarrow V\,;\, f \text{ bijektiv }\}$. Diese Untergruppe $\mathrm{Aut}(V)$ heißt auch *Allgemeine lineare Gruppe $Gl(V)$*, im Englischen *general linear group*.

(b) Sei $U \subset V$ ein Unterraum, dann wird durch $x \sim y \Leftrightarrow x - y \in U$ eine Äquivalenzrelation auf V erklärt, vgl. Satz **??**. Dann ist V/U die Menge der Restklassen, auf der dann die Addition und Skalarmultiplikation wohldefiniert ist.

Satz 2.2.7. *Sei $f : V \longrightarrow W$ linear. Dann ist der induzierte Homomorphismus*

$$\overline{f} : V/\ker f \longrightarrow imf, \overline{f}([x]) = f(x)$$

ein Isomorphismus.

Beispiel 2.2.8. Wir setzen die Beispiele fort, vgl. Beispiel 2.2.2 und Beispiel 2.2.4: (b) $K^n/\ker(\mathrm{pr}_k) \cong K$.

(c) $\mathbb{R}[t]/\ker D \cong \mathrm{im}D \cong \mathbb{R}[t]$ und $\mathbb{R}[t]/\ker ev_0 \cong \mathbb{R}$.

10. Vorlesung, 13.11.19

2.3 Lineare Unabhängigkeit und Erzeugendensysteme

Definition 2.3.1. *(a) Für eine Indexmenge I und eine Menge X wird durch eine Abbildung $i \in I \mapsto x_i \in X$ eine* Familie *von Elementen in X definiert. Hier wird auch die Notation $[(x_i)_{i\in I}]$ eingeführt.*

(b) Für eine Familie von Vektoren $(v_i)_{i\in I}$ ist die lineare Hülle *definiert durch:*

$$[(v_i)_{i\in I}] = \left\{ \sum_{i\in I} \alpha_i v_i \,;\, \alpha_i \in K \,,\, \#\{i \in I; \alpha_i \neq 0\} < \infty \right\}$$

Für eine endliche Familie $v_1, v_2, \ldots, v_r \in V$ gilt also

$$[v_1, v_2, \ldots, v_r] = \left\{ \sum_{i=1}^{r} \alpha_i v_i \,;\, \alpha_i \in K \right\}.$$

Beispiel 2.3.2. (a) In K^3 seien die Vektoren $e_1 = (1,0,0), e_2 = (0,1,0)$ gegeben. Dann gilt:

$$[e_1, e_2] = \{(\alpha_1, \alpha_2, \alpha_3) \in K^3 \,,\, \alpha_3 = 0\}.$$

(b) Sei $V = K[t]$ der Vektorraum der Polynome. Wenn $E = \{1, t, t^2, t^3, \ldots\}$ so ist die lineare Hülle $[E] = V$.

Satz 2.3.3. *Die lineare Hülle $[(v_i)_{i\in I}]$ einer Familie $(v_i)_{i\in I}$ von Vektoren eines Vektorraums V ist ein Unterraum.*

Definition 2.3.4. *Eine Familie $(v_i)_{i\in I}$ von Vektoren eines Vektorraums V heißt* Erzeugendensystem, *falls die lineare Hülle der Vektorraum ist, also $[(v_i)_{i\in I}] = V$.*

Satz 2.3.5. *Sei $f : V \longrightarrow W$ eine lineare Abbildung zwischen Vektorräumen.*

(a) Wenn $(v_i)_{i\in I}$ eine Familie von Vektoren von V ist, dann gilt $\left[f\,(v_i)_{i\in I}\right] = f\,([(v_i)_{i\in I}])$. Also ist das Bild unter f der linearen Hülle einer Familie von Vektoren gleich der linearen Hülle der Bildvektoren der Familie unter der linearen Abbildung.

(b) Wenn die Familie $(v_i)_{i\in I}$ ein Erzeugendensystem von V ist, dann ist die Abbildung f eindeutig durch die Werte $f(v_i), i \in I$ festgelegt.

Nun suchen wir ein Erzeugendensystem mit möglichst wenigen Elementen:

Definition 2.3.6. *Eine Familie $(v_i)_{i\in I}$ von Vektoren in dem Vektorraum V heißt* linear unabhängig *(oder* frei*), wenn aus $\sum_{i\in I} \alpha_i v_i = 0$ für Elemente $\alpha_i \in K$, (die für nur endlich viele i nicht = sind), folgt, dass $\alpha_i = 0$ für alle $i \in I$ gilt. Andernfalls ist die Familie von Vektoren* linear abhängig.

Es gibt also nur eine Möglichkeit, den Nullvektor als Linearkombination der Vektoren v_i darzustellen.

Beispiel 2.3.7. (a) v (als Familie aus einem Vektor) ist linear unabhängig genau dann, wenn $v \neq 0$.

(b) Die Vektoren $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$ sind linear unabhängig im Vektorraum K^n.

(c) Im Vektorraum $K[t]$ der Polynome sind die Elemente $1, t, t^2, \ldots$ linear unabhängig.

Satz 2.3.8. *Wenn $(v_i)_{i\in I}$ eine Familie von Vektoren im Vektorraum V ist, dann ist diese Familie linear unabhängig genau dann, wenn jeder Vektor $v \in [(v_i)_{i\in I}]$ in der linearen Hülle genau eine Darstellung $v = \sum_i \alpha_i v_i$ besitzt.*

Beispiel 2.3.9. (a) Wenn $(v_i)_{i\in I}$ eine Familie von Vektoren in V ist und $j \in I$, dann gilt: Wenn $(v_i)_{i\in I-\{j\}}$ nicht linear unabhängig ist, dann auch $(v_i)_{i\in I}$. Wenn $(v_i)_{i\in I}$ linear unabhängig ist, dann auch $(v_i)_{i\in I-\{j\}}$.

(b) Gegeben sind zwei Vektoren $x = (x_1, x_2), y = (y_1, y_2) \in K^2$. Diese Vektoren sind linear unabhängig genau dann, wenn

$$d = x_2 y_1 - x_1 y_2 \neq 0\,.$$

Satz 2.3.10. *Sei $F = (v_i)_{i\in I}$ eine Familie von Vektoren im Vektorraum V. Für jede Teilmenge $J \subset I$ ist dann $F_J = (v_i)_{i\in J}$ die entsprechende Teilfamilie. Dann ist die Familie F linear unabhängig genau dann, wenn für jede echte Teilmenge $J \subset I$ und $J \neq I$ gilt: $[F_J] \neq [F]$, d.h. $[v_i; i \in J] \neq [v_i; i \in I]$.*

11. Vorlesung, 19.11.19

Satz 2.3.11. *Wenn $(v_i)_{i \in I}$ eine linear unabhängige Familie von Vektoren im Vektorraum V ist und $f : V \longrightarrow W$ eine injektive, lineare Abbildung von Vektorräumen ist, dann ist die Familie $(f(v_i))_{i \in I}$ linear unabhängig.*

2.4 Basis und Dimension

Definition 2.4.1. *Eine Familie $(v_i)_{i \in I}$ von Vektoren in einem Vektorraum V heißt eine* Basis, *wenn sie ein linear unabhängiges Erzeugendensystem ist.*

Beispiel 2.4.2. (a) Die Vektoren $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$ sind eine Basis von $V = K^n$.
(b) Die Polynome $1, t, t^2, \ldots$ bilden eine Basis des Vektorraums $K[t]$.

Lemma 2.4.3. *Wenn $B = (v_i)_{i \in I}$ eine Basis des Vektorraums V ist und $f : V \longrightarrow W$ eine injektive, lineare Abbildung von Vektorräumen ist, dann ist $f(v_i)_{i \in I}$ eine Basis des Unterraums $\operatorname{im} f$.*

Satz 2.4.4. *Seien $V; W$ Vektorräume und $B = (v_i)_{i \in I}$ eine Basis von V. Dann gilt: Zu jeder Familie $(w_i)_{i \in I}$ von Vektoren in W gibt es genau eine lineare Abbildung $f : V \longrightarrow W$ mit $f(v_i) = w_i$ für alle $i \in I$.*

Eine lineare Abbildung $f : V \longrightarrow W$ ist also eindeutig durch ihre Werte auf einer Basis bestimmt.

Lemma 2.4.5. *Wenn $B = (v_i)_{i \in I}$ eine Familie von Vektoren im Vektorraum V ist, so dass für $j \in I$ gilt, dass $B' = (v_i)_{i \in I - \{j\}}$ linear unabhängig ist und $v_j \in V - [B']$, dann ist B auch linear unabhängig.*

Theorem 2.4.6. *Sei $B = (v_i)_{i \in I}$ eine Familie von Vektoren im Vektorraum V. Dann sind folgende Aussagen äquivalent:*

(a) B ist eine Basis.

(b) B ist ein minimales Erzeugendensystem, d.h. für jedes $J \subset I, J \neq I$ ist $(v_i)_{i \in J}$ kein Erzeugendensystem.

(c) B ist eine maximale Familie linear unabhängiger Vektoren, d.h. für jede Familie $(v_i)_{i \in K}$ von Vektoren in V mit $I \subset K, I \neq K$ ist $(v_i)_{i \in K}$ linear abhängig.

Nun wollen wir untersuchen, wie man eine Basis erhält, bzw. zeigen, dass jeder Vektorraum eine Basis besitzt:

Satz 2.4.7 (Basisauswahlsatz)**.** *Aus einem endlichen Erzeugendensystem $(v_1, \ldots, v_r)$ eines Vektorraums V kann man eine Basis auswählen, d.h. es gibt Indices $i_1, \ldots, i_n \in \{1, 2, \ldots, r\}$, so dass $(v_{i_1}, \ldots, v_{i_n})$ eine Basis ist.*

Lemma 2.4.8 (Austauschlemma von Steinitz)**.** *Sei V ein Vektorraum mit Basis $(v_1, \ldots, v_r)$ und*

$$w = \alpha_1 v_1 + \ldots + \alpha_r v_r \in V.$$

Falls $\alpha_k \neq 0$ für ein $k \in \{1, \ldots, r\}$, so ist

$$(v_1, \ldots, v_{k-1}, w, v_{k+1}, \ldots, v_r)$$

ebenfalls eine Basis.

12. Vorlesung, 25.11.19

Satz 2.4.9 (Austauschsatz). *In einem Vektorraum V sei eine Basis $(v_1, \ldots, v_r)$ und eine linear unabhängige Familie $(w_1, \ldots, w_n)$ gegeben. Dann ist $n \leq r$, und es gibt Indices $I_1, \ldots, i_n \in \{1, \ldots, r\}$, so dass man durch Austausch von v_{i_1} durch $w_1, \ldots, v_{i_n}$ durch w_n wieder eine Basis erhält. Durch Umnummerierung $(i_1 = 1, \ldots, i_n = n)$ ist dann also*

$$(w_1, \ldots, w_n, v_{n+1}, \ldots, v_r)$$

auch eine Basis.

Korollar 2.4.10. *Wenn ein Vektorraum V eine endliche Basis besitzt, dann ist jede Basis endlich.*

Korollar 2.4.11. *Zwei Basen $(v_1, \ldots, v_r)$ und $(w_1, \ldots, w_k)$ haben die gleiche Länge, d.h. $r = k$.*

Definition 2.4.12. *Für einen Vektorraum V über dem Körper K definieren wir die* Dimension $\dim_K V \in \mathbb{N}_0 \cup \{\infty\}$:

$$\dim_K V = \begin{cases} r & ; \quad \textit{es gibt eine Basis der Länge } r \\ \infty & ; \quad \textit{es gibt keine endliche Basis} \end{cases}$$

Satz 2.4.13 (Basisergänzungssatz). *Sei $(v_i)_{i \in I}$ eine linear unabhängige Familie von Vektoren im Vektorraum V. Dann kann diese Familie zu einer Basis ergänzt werden, d.h. es gibt eine Basis $(v_i)_{i \in J}$ mit $I \subset J$.*

Im Fall unendlicher Dimension gilt die Aussage des Satzes auch, dann benötigt der Beweis aber tiefliegende mengentheoretische Hilfsmittel, so das *Zornsche Lemma.*

Theorem 2.4.14. *Jeder Vektorraum V besitzt eine Basis.*

Beispiel 2.4.15. (a) $\dim K^n = n$, denn $(e_1, \ldots, e_n)$ ist eine Basis. Hier ist $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$. Und damit hat jede Basis die Länge n.

(b) $\dim_{\mathbb{R}} \mathbb{R}[t] = \infty$, da $1, t, t^2, \ldots$ eine Basis ist.

(c) $\dim_{\mathbb{Q}} \mathbb{R} = \infty$. Denn wäre die Dimension von $\mathbb{R}$ über $\mathbb{Q}$ endlich, so wären die reellen Zahlen *abzählbar.*

(d) $\dim_{\mathbb{C}} \mathbb{C} = 1, \dim_{\mathbb{R}} \mathbb{C} = 2$. Eine Basis über $\mathbb{C}$ ist z.B. 1, eine Basis über $\mathbb{R}$ ist z.B. $1, i$.

Definition 2.4.16. *Sei $U \subset V$ ein Unterraum von des Vektorraums V. Ein Unterraum U' heißt dann* Komplement, *von U, wenn $U \cap U' = \{0\}$ und $V = U + U'$.*

Beispiel 2.4.17. (a) In K^3 ist $U = \{(x, y, 0); x, y \in K\}$ ein Unterraum. Dann ist für jeden Vektor $v \notin U$, also $v = (x_1, y_1, z_1), z_1 \neq 0$ der von v erzeugte Unterraum $U' = K\dot{v} = \{\alpha v; \alpha \in K\}$ ein Komplement von U.

(b) Für $U = V$ ist $\{0\}$ ein Komplement und umgekehrt ist für $U = \{0\}$ der Vektorraum V selbst ein Komplement.

Satz 2.4.18. *Zu jedem Unterraum U von V existiert ein Komplement.*

Wir stellen jetzt eine Beziehung eines Komplements U' zu einem Unterraum U von V zu dem Restklassenraum V/U her, den wir in Bemerkung **??** eingeführt haben:

Satz 2.4.19. *Sei U ein Unterraum des Vektorraums V. Dann ist jedes Komplement isomorph zum Restklassenraum V/U, dann heißt die Dimension eines Komplements auch* Kodimension *des Unterraums U.*

Wir erhalten als

Korollar 2.4.20. *Wenn also $f : V \longrightarrow W$ eine lineare Abbildung ist und U' ein Komplement zum Unterraum $U = \ker f$, dann ist die Einschränkung $f|U' : U' \longrightarrow imf$ ein Isomorphismus.*

Lemma 2.4.21. *Wenn V endlich-dimensional ist und U ein Unterraum mit Komplement U', dann gilt*

$$\dim V = \dim U + \dim U'.$$

13. Vorlesung, 27.11.19

Aus Korollar 2.4.20 und Lemma 2.4.21 erhalten wir direkt:

Satz 2.4.22. *Wenn $f : V \longrightarrow W$ eine lineare Abbildung ist und V endlich-dimensional ist, dann gilt:*

$$\dim V = \dim \ker f + \dim imf .$$

Korollar 2.4.23. *Sei V ein endlich-dimensionaler Vektorraum und $f : V \longrightarrow W$ linear.*

(a) Wenn f injektiv ist, so gilt: $\dim V \leq \dim W$.

(b) Wenn f surjektiv ist, so gilt: $\dim V \geq \dim W$.

(c) Wenn $\dim V = \dim W$ und wenn f injektiv oder surjektiv ist, dann ist f auch bijektiv, also ein Isomorphismus.

Theorem 2.4.24 (Dimensionsformel für Unterräume)**.** *Wenn U, W endlich-dimensionale Unterräume des Vektorraums V sind, dann gilt:*

$$\dim(U \cap W) + \dim(U + W) = \dim U + \dim W.$$

Beispiel 2.4.25. Sei $V = K^3$, und U, W Unterräume der Dimension $\dim U = 1, \dim W = 2$. Falls $U \cap W = \{0\}$, so gilt $\dim(U + W) = \dim U + \dim W = 3$ dann ist W ein Komplement zu U, bzw. U ein Komplement zu W. Falls $U \cap W \neq 0$, so folgt, dass U ein Unterraum von W ist. Dann gilt also $\dim(U \cap W) + \dim(U + W) = 1 + 2 = \dim U + \dim W$.

Satz 2.4.26. *Wenn V ein endlich-dimensionaler Vektorraum ist, dann bestimmt jede Basis $(b_1, \ldots, b_n)$ ein* Koordinatensystem, *d.h. einen linearen Isomorphismus*

$$\Phi_B : V \longrightarrow K^n ; \Phi_B(b_j) = e_j.$$

Dabei ist $e_i = (\delta_{i1}, \ldots, \delta_{in})$ die kanonische Basis von K^n.

3 Matrizen und Lineare Abbildungen

3.1 Der Vektorraum der linearen Abbildungen

Von nun an betrachten wir nur noch Vektorräume über kommutativen Körpern K.

Satz 3.1.1. *Wenn V, W Vektorräume über K sind, bezeichnen wir mit $Hom(V, W)$ die Menge der linearen Abbildungen. Dieser Raum ist ein Vektorraum über K.*

Wenn $V = W$ besitzt $\mathrm{Hom}(V, W)$ noch eine zusätzliche Struktur, dann benutzt man auch die Notation $\mathrm{End}(V) = \mathrm{Hom}(V, V)$.

Satz 3.1.2. *Der Vektorraum $End(V) = Hom(V, V)$ eines Vektorraums V mit der Komposition von Abbildungen als Multiplikation hat die Struktur eines Rings mit Einselement Id_V, wir setzen $fg = g \circ f$.*

14.Vorlesung, 4.12.19

Bemerkung 3.1.3. (a) $A = \mathrm{End}(V)$ ist sogar eine K-*Algebra*. D.h. A ist ein Vektorraum, der zugleich mit der Vektorraumaddition als Addition ein Ring ist. Außerdem gilt für die Skalare Multiplikation das folgende *gemischte Assoziativgesetz:*

$$\alpha(xy) = (\alpha x)y$$

für alle $x, y \in A, \alpha \in K$.

(b) Wenn $\dim V = 1$ so ist eine lineare Abbildung $V \longrightarrow V$ nach Wahl eines Vektors $e \neq 0$ als Basisvektor eindeutig durch ein Element $\alpha \in K$ bestimmt: $f(e) = \alpha e$. Dann kann man $\mathrm{End}(V)$ mit dem Körper K identifizieren.

(c) Falls $\dim V \geq 2$, so ist $\mathrm{End}(V)$ ein Ring, der weder kommutativ, noch ein Körper ist.

(c) In einem Ring R bilden die multiplikativ invertierbaren Elemente eine Gruppe R^* bezüglich der Multiplikation. Die multiplikativ invertierbaren linearen Endomorphismen sind gerade die Automorphismen. Also ist die Menge $\mathrm{Aut}(V) = \{f \in \mathrm{End}(V)\,;\, f \text{ invertierbar }\}$ eine Gruppe bezüglich der Komposition, sie ist die *allgemeine lineare Gruppe* $\mathrm{Gl}(V)$, vgl. Bemerkung **??**.

3.2 Dualräume und transponierte Abbildungen

Es wird später darum gehen, einen Vektor $v \in V$ in einer Basis $B = \{b_1, \ldots, b_r\}$ darzustellen, also die Elemente $(v_1, \ldots, v_r) \in K^r$ zu bestimmen, so dass $v = \sum_i v_i b_i$ gilt. Dies kann man übersichtlich mit Linearformen, also linearen Abbildungen $V \longrightarrow K$ beschreiben:

Definition 3.2.1. *Für einen Vektorraum V über dem Körper K bezeichnet $V^* = Hom(V, K)$ den* Dualraum. *Die Elemente $\omega \in V^*$ heißen* Linearformen.

Beispiel 3.2.2. (a) Die Projektion $\mathrm{pr}_k : K^n \longrightarrow K, x = (x_1, \ldots, x_k) \longmapsto x_k \in K$ ist eine Linearform auf K^n.

(b) Sei $B = \{b_1, \ldots, b_n\}$ eine Basis des Vektorraums V. Dann definieren wir eine lineare Abbildung $\mathrm{pr}_k : V \longrightarrow K, x = \sum_{i=1}^n x_i b_i \longmapsto x_k$. Diese Abbildung ist eine Linearform.

(c) Die Abbildung $f : \sum_i a_i t^i \in \mathbb{R}[t] \longmapsto \sum_i a_i$ ist eine Linearform, also ein Element aus dem Dualraum $\mathbb{R}[t]^*$.

Bemerkung 3.2.3. (a) Für eine Linearform $\omega \in V^*, \omega \neq 0$ hat der Kern $\ker \omega$ die Kodimension 1. Dies folgt aus Satz 2.4.22, da die Abbildung surjektiv ist, also $\dim \mathrm{im}\omega = 1$. Wenn also V endlich-dimensional ist, gilt $\dim \ker \omega = \dim V - 1$.

Definition 3.2.4. *Für einen Vektorraum V über dem Körper K und seinem Dualraum V^* wird die* natürliche Paarung

$$\langle ., . \rangle : V^* \times V \longrightarrow K; \;\; (\omega, x) \longmapsto \omega(x)$$

definiert.

Satz 3.2.5. *Die natürliche Paarung $\langle ., . \rangle : V^* \times V \longrightarrow K$ ist* bilinear, *d.h. linear in jedem Argument.*

Lemma 3.2.6. *Für eine Basis $B = (b_i)_{i \in I}$ eines Vektorraums V definieren wir die lineare Abbildung $f_B : V \longmapsto V^*$ durch $\langle f_B(b_i), b_j \rangle = \delta_{ij}$. Dann ist die Abbildung f_B injektiv und die Familie $f_B(b_i)_{i \in I}$ ist linear unabhängig. Diese Familie ist eine Basis genau dann, wenn der Vektorraum V endlich-dimensional ist. Zur Vereinfachung der Notation schreiben wir auch kurz $b^* = f_B(b)$.*

Korollar 3.2.7. *Wenn V ein endlich-dimensionaler Vektorraum ist, dann sind der Dualraum V^* und der Vektorraum isomorph, es gilt also* $\dim V^* = \dim V$.

Lemma 3.2.8. *Für einen Vektorraum V betrachten wir den Dualraum V^* und den Dualraum $V^{**} = (V^*)^*$ des Dualraums V^*. Wir definieren eine Abbildung*

$$\Phi : V \longrightarrow V^{**} \, ; \, \Phi(x)(\omega) = \omega(x) = \langle \omega, x \rangle \tag{3}$$

für alle $\omega \in V^*$. Die Abbildung Φ ist linear und injektiv. Die Abbildung Φ ist ein Isomorphismus genau dann, wenn V endlich-dimensional ist.

Bemerkung 3.2.9. (a) Die Abbildung Φ ist *kanonisch,* bei ihre Definition ist nicht von einer Wahl abhängig. Dagegen ist die Abbildung f_B eine nicht-kanonische lineare Abbildung zwischen Vektorraum und Dualraum, sie hängt offensichtlich von der Wahl der Basis ab.

(b) Wenn $B = \{b_1, \ldots, b_r\}$ eine Basis des Vektorraums V und $B^* = \{b_1^*, \ldots, b_r^*\}$ die duale Basis ist, dann gelten folgende Beziehungen für jeden Vektor $v \in V$ und jede Linearform $\omega \in V^*$:

$$v = \sum_{i=1}^{r} \langle b_i^*, v \rangle b_i \, ; \; \omega = \sum_{j=1}^{r} \langle \omega, b_j \rangle b_j^*. \tag{4}$$

Wir zeigen, dass eine lineare Abbildung $f : V \longrightarrow W$ eine kanonische lineare Abbildung $f^T : W^* \longrightarrow V^*$ zwischen den Dualräumen induziert:

Satz 3.2.10. *Wenn $f : V \longrightarrow W$ eine lineare Abbildung zwischen Vektorräumen ist, dann wird durch $f^T : W^* \longrightarrow V^*$ mit $f^T(\omega)(v) = \omega(f(v))$ bzw. $\langle f^T(\omega), v \rangle = \langle \omega, f(v) \rangle$ für alle $\omega \in W^*, v \in V$ eine lineare Abbildung definiert, sie wird als* transponierte Abbildung *von f bezeichnet.*

15.Vorlesung, 9.12.19

Beispiel 3.2.11. (a)

$$\frac{d}{dt} : \sum_{i \geq 0} a_i t^i \in \mathbb{R}[t] \longmapsto \sum_{i \geq 0} (i+1) a_{i+1} t^i \in \mathbb{R}[t]$$

ist eine lineare Abbildung, die Auswertungsabbildung $ev_x : \mathbb{R}[t] \longrightarrow \mathbb{R}$ ist eine Linearform. Wir bestimmen die transponierte Abbildung $(d/dt)^T \in \mathrm{End}\,(\mathbb{R}[t]^*)$ angewendet auf die Linearform ev_x, die wir anwenden auf $p \in \mathbb{R}[t]^*$:

$$\frac{d}{dt}\,(ev_x)\,(p) = ev_x \frac{d}{dt} p = \frac{dp}{dt}(x)\,.$$

Satz 3.2.12. *Die Abbildung*

$$\Psi : Hom(V;W) \longrightarrow Hom(V^*;W^*);\;\; f \longmapsto f^T$$

ist linear und injektiv. Falls V und W endlich-dimensional sind, ist die Abbildung Ψ ein Isomorphismus.

Lemma 3.2.13. *Wenn $f : V \longrightarrow W$ und $g : W \longrightarrow U$ linear sind, dann gilt*

$$(g \circ f)^T = f^T \circ g^T.$$

Bemerkung 3.2.14. Die Vektorräume $\mathrm{End}(V)$ sowie $\mathrm{End}(V^*)$ sind auch Ringe, vgl. Bemerkung 3.1.3. Dann folgt aus Satz 3.2.10 und Lemma 3.2.13, dass die Abbildung

$$\Psi : f \in \mathrm{End}(V) \longmapsto f^T \in \mathrm{End}(V^*)$$

ein *Ring-Antihomomorphismus* ist, d.h. eine lineare Abbildung bezüglich der Addition und bezüglich der Multiplikation gilt:

$$(f \circ g)^T = g^t \circ f^T\,;\; (1_V)^T = 1_{V^*}\,.$$

Hier ist $1_V = \mathbb{1}_V, 1_{V^*} = \mathbb{1}_{V^*}$. Daraus folgt dann für $f \in \mathrm{Gl}(V) : f^T \in \mathrm{Gl}(V^*)$ mit $\left(f^T\right)^{-1} = \left(f^{-1}\right)^T$.

Lemma 3.2.15. *Sei $D = \{d_1, \ldots, d_n\}$ eine Basis von V mit dualer Basis $D^* = \{d_1, \ldots, d_n^*\}$, sei $\Phi_D : V \longrightarrow K^n$ das dadurch bestimmte Koordinatensystem, vgl. Satz 2.4.26: Dann gilt für das Koordinatensystem $\Phi_D^* : V^* \longrightarrow K^n$ von V^* in Bezug auf die Basis D^* :*

$$f_E \circ \Phi_{D^*} = \left(\Phi_D^T\right)^{-1}. \tag{5}$$

Hierbei ist $f_E : K^n \longrightarrow (K^n)^*$ die durch die kanonische Basis $\{e_1, \ldots, e_n\}$ bestimmte lineare Abbildung mit $f_E(e_j) = e_j^*$.

16.Vorlesung, 11.12.19

3.3 Matrizen

Das Rechnen mit Matrizen stand am Anfang der Linearen Algebra:

Definition 3.3.1. *Eine* (m,n)-Matrix A *über einem Körper* K *ist eine Familie* $(a_{ij})_{(i,j)\in I}$ *von Elementen in* K *mit der Indexmenge* $I = \{(i,j)\,;\,1 \le i \le m, 1 \le j \le n\}$*. Man kann die Matrix also auch mit dem Schema*

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

identifizieren. Die i*-te Zeile* A^i *ist die* $(1,n)$ *Matrix*

$$(a_{i1}, \dots, a_{in})$$

und die j*-te Spalte* A_j *ist die* $(m,1)$*-Matrix*

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

Wir bezeichnen mit $M_K(m,n)$ *die Menge der* (m,n)*-Matrizen über* K*.*

Lemma 3.3.2. *Für eine* (m,n)*-Matrix* A *wird durch* $f_A : K^n \longrightarrow K^m, f_A(x_1,\dots,x_n) = \left(\sum_{j=1}^n a_{1j}x_j, \dots, \sum_{j=1}^n a_{mj}x_j\right)$ *eine lineare Abbildung definiert. Umgekehrt ist jede lineare Abbildung* $f : K^n \longrightarrow K^m$ *von dieser Form.*

Die j-te Spalte A_j der Matrix enthält also gerade die Koeffizienten des Vektors $f(d_j)$ in Bezug auf die Basis E. Man unterscheidet nicht zwischen der Matrix A und der dadurch definierten linearen Abbildung f_A, also verwenden wir auch die Notation A an Stelle von f_A.

Bemerkung 3.3.3. Die Menge $M_K(m,n)$ ist ein K-Vektorraum, die Addition und die skalare Multiplikation sind definiert durch:

$$(a_{ij})_{i,j} + (b_{ij})_{i,j} = (a_{ij} + b_{ij})_{i,j}\ ;\ \alpha\,(a_{ij})_{i,j} = (\alpha(a_{ij}))_{i,j}\ .$$

Wir bezeichnen mit E_{kl} für $1 \le k \le m, 1 \le l \le n$ die Matrix mit den Koeffizienten $a_{ij} = \delta_{ik}\delta_{jl}$ wobei $\delta_{ij} \in \{0,1\}$ das *Kronecker-Symbol* ist mit

$$\delta_{ij} = \begin{cases} 1 & ;\ i = j \\ 0 & ;\ i \neq j \end{cases}$$

Die Matrix hat also in der k-ten Zeile und l-ten Spalte eine 1, alle anderen Einträge sind 0. Dann gilt also für eine Matrix $A = (a_{ij}) : A = \sum_{i,j} a_{ij}E_{ij}$. Dies zeigt, dass E_{kl} eine Basis bilden, d.h. $\dim M_K(m,n) = mn$.

Eine linearen Abbildung $f : V \longrightarrow W$ zwischen endlich-dimensionalen Vektorräumen kann man nach Wahl von Basen D, E von V, W durch eine Matrix darstellen.

Definition 3.3.4. *Wenn* $f : V \longrightarrow W$ *eine lineare Abbildung ist und* $D = \{d_1, \ldots, d_n\}$ *eine Basis von* V *bzw.* $E = \{e_1, \ldots, e_m\}$ *eine Basis ist von* W *und seien* $\Phi_D : V \longrightarrow K^n$ *bzw.* $\Phi_E : W \longrightarrow K^m$ *die zugehörigen Koordinatensysteme nach Satz 2.4.26, dann ist die* Darstellung der linearen Abbildung f *in Bezug auf die Basen* D *und* E *die lineare Abbildung*

$$\Phi_E \circ f \circ \Phi_D^{-1} : K^n \longrightarrow K^m \,. \tag{6}$$

die wir dann auch mit der Matrixdarstellung dieser linearen Abbildung identifizieren.

17.Vorlesung 16.12.19

Mit Hilfe der dualen Basen erhalten wir folgende Beschreibung:

Satz 3.3.5. *Sei $f : V \longrightarrow W$ eine lineare Abbildung zwischen den Vektorräumen V, W und seien D, E Basen von V, W und sei E^* die duale Basis von E. Dann gilt für die Matrixdarstellung von f bezüglich D, E :*

$$\Phi_E \circ f \circ \Phi_D^{-1} = (\langle e_i^*, f(d_j)\rangle)_{i,j} \ . \tag{7}$$

Definition 3.3.6. *Wenn $D = \{d_1, \ldots, d_n\}$ und $D' = \{d'_1, \ldots, d'_n\}$ Basen sind des Vektorraums V, dann heißt der Isomorphismus*

$$T^D_{D'} = \Phi_{D'} \circ \Phi_D^{-1} : K^n \longrightarrow K^n \tag{8}$$

die durch die Basen D und D' bestimmte Koordinatentransformation.

Dann können wir die Koordinatendarstellung einer Matrix in Bezug auf verschiedene Basen folgendermaßen ineinander umrechnen:

Satz 3.3.7. *Gegeben ist eine lineare Abbildung $f : V \longrightarrow W$ zwischen den Vektorräumen V und W. Es seien D, D' Basen des Vektorraums V und E, E' Basen des Vektorraums W, sowie $T^D_{D'} = \Phi_{D'} \circ \Phi_D^{-1}$ und $S^E_{E'} = \Phi_{E'} \circ \Phi_E^{-1}$ die in Definition 3.3.6 eingeführten Koordinatentransformationen, dann gilt für die Matrixdarstellungen $\Phi_E \circ f \circ \Phi_D^{-1}$ bzw. $\Phi_{E'} \circ f \circ \Phi_{D'}^{-1}$ von f in Bezug auf die Basen D, E bzw. D', E' :*

$$\Phi_{E'} \circ f \circ \Phi_{D'}^{-1} = S^E_{E'} \circ \left(\Phi_E \circ f \circ \Phi_D^{-1}\right) \circ \left(T^D_{D'}\right)^{-1} \ . \tag{9}$$

Beispiel 3.3.8. $V = K^3, W = K^2$. Sei $D = \{d_1, d_2, d_3\}$ die kanonische Basis und $D' = \{d'_1 = d_1, d'_2 = d_1 + d_2, d'_3 = d_1 + d_2 + d_3\}$. Dann ist $\Phi_D = \mathrm{Id}, \Phi_{D'}(d'_i) = d_i, i = 1, 2, 3$, also $\Phi_{D'}(d'_1) = \Phi_{D'}(d_1) = d_1, d_2 = \Phi_{D'}(d'_2) = \Phi_{D'}(d_1 + d_2)$, somit $\Phi_{D'}(d_2) = d_2 - \Phi_{D'}(d_1) = d_2 - d_1$. Schließlich $d_3 = \Phi_{D'}(d'_3) = \Phi_{D'}(d_1 + d_2 + d_3)$, also $\Phi_{D'}(d_3) = d_3 - \Phi_{D'}(d_1) - \Phi_{D'}(d_2) = d_3 - d_1 - (d_2 - d_1) = d_3 - d_2$. Also ist die Matrixdarstellung von $\Phi_{D'}$:

$$\Phi_{D'} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} .$$

Somit gilt dann

$$T^D_{D'} = \Phi_{D'} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} ; T^{D'}_D = \Phi_{D'}^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Sei $E = \{e_1, e_2\}$ die kanonische Basis von $W = K^2$, und $E' = \{e'_1 = -e_2, e'_2 = e_1\}$, somit $\Phi_{E'} \circ \Phi_E^{-1} = \Phi_{E'}$. Dann gilt $\Phi_{E'}(e'_1) = \Phi_{E'}(-e_2) = e_1$, also $\Phi_{E'}(e_2) = -e_1$. Und $e_2 = \Phi_{E'}(e'_2); \Phi_{E'}(e_1) = e_2$. Also ist die Matrixdarstellung:

$$\Phi_{E'} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} .$$

Dann betrachte die lineare Abbildung

$$A = \begin{pmatrix} 1 & 3 & 2 \\ 0 & 1 & 2 \end{pmatrix} : V = K^3 \longrightarrow W = K^2 .$$

Dann ist die Koordinatendarstellung A' der Matrix A bezüglich der Basen D', E' :

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

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

Bei den letzten Umformungen benutzt man das *Matrizenprodukt*, das wir erst im nächsten Abschnitt einführen.

3.4 Das Produkt von Matrizen

Die Addition in dem Vektorraum $\mathrm{Hom}(V; W)$ entspricht der Addition von Matrizen, wie wir im vorigen Abschnitt gesehen haben. Der Komposition von linearen Abbildungen entspricht das Produkt von Matrizen:

Definition 3.4.1. *Für die (l, m)-Matrix $B = (b_{ij})_{i,j} \in M_K(l, m)$ und die (m, n)-Matrix $A = (a_{jk})_{j,k} \in M_K(m, n)$ ist das Produkt $BA = C = (c_{ik})_{i,k} \in M_K(l, n)$ als (l, n)-Matrix mit den Koeffizienten*

$$c_{ik} = \sum_{j=1}^{m} b_{ij} a_{jk}$$

definiert.

Bemerkung 3.4.2.

$$\begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & & . \\ b_{l1} & \dots & b_{lm} \end{pmatrix} \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & . \\ a_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} \sum_j b_{1j} a_{j1} & \dots & \sum_j b_{1j} a_{jn} \\ \vdots & & . \\ \sum_j b_{lj} a_{j1} & \dots & \sum_j b_{lj} a_{jn} \end{pmatrix} .$$

Beispiel 3.4.3.

$$\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 2 \\ -1 & 0 & 0 & -1 \\ 0 & 0 & 3 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 2 \\ -2 & 0 & -1 & -3 \end{pmatrix} .$$

Satz 3.4.4. *Eine (m, n)-Matrix $A = (a_{jk})_{j,k}$ kann mit einer linearen Abbildung $A : K^n \longrightarrow K^m$ identifiziert werden, ebenso eine (l, m)-Matrix $B = (b_{jk})_{j,k}$ mit einer linearen Abbildung $B : K^m \longrightarrow K^l$. Dann entspricht dem Matrizenprodukt BA die lineare Abbildung $B \circ A : K^n \longrightarrow K^l$, also die Komposition der linearen Abbildungen.*

Beispiel 3.4.5. (a) Die lineare Abbildung $A : x \in K^n \longmapsto A(x) \in K^m$ kann man auch als Matrizenprodukt Ax^T interpretieren, wobei x^T die $(n, 1)$-Matrix mit den Elementen $x_j, j = 1, \dots, n$ ist, also

$$Ax^T = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ . & & . \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ . \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_i a_{1i} x_i \\ \dots \\ \sum_i a_{mi} x_i \end{pmatrix}$$

(b) Einer Linearform $\omega \in (K^n)^* = \mathrm{Hom}(V;K)$ entspricht die $(1,n)$-Matrix mit den Einträgen: $\langle e_1^*, \omega(d_j)\rangle$, vgl. Satz 3.3.5. Hier ist $\{d_1,\ldots,d_n\}$ die kanonische Basis von K^n, e_1^* ist die kanonische Basis von K^*, d.h. $e_1^*(y) = y$. Also $\langle e_1^*, \omega(d_j)\rangle = \omega(d_j) = \omega_j$, wobei $\omega = \sum_i \omega_i d_i^*$. Also $\omega(x) = \sum_i \omega_i x_i$ bzw. in Matrixschreibweise:

$$(\omega_1,\ldots,\omega_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_i \omega_i x_i \,.$$

Nach Bemerkung 3.1.3 ist $\mathrm{End}(V)$ ein Ring. Dies überträgt sich auf $M_K(n,n)$:

18.Vorlesung 18.12.19

Satz 3.4.6. *Der Raum $M_K(n,n)$ der (n,n)-Matrizen über dem Körper K mit der Matrizenaddition und der Matrizenmultiplikation trägt die Struktur eines Rings. Das Einselement ist die* Einheitsmatrix $\mathbb{1} = \mathbb{1}_n = E = E_n$ *mit der Matrixdarstellung* $(\delta_{ij})_{i,j}$. *Das Nullelement ist die Nullmatrix.*

Nach Bemerkung 3.1.3(c) erhalten wir folgende

Definition 3.4.7. *Die Menge der multiplikativen invertierbaren Matrizen im Ring $M_K(n,n) = End(K^n)$ bildet eine Gruppe unter dem Matrizenprodukt. Diese Gruppe heißt* allgemeine lineare Gruppe in n Variablen. *Die Bezeichnung ist $Gl(K^n) = Gl(n;K)$.*

Bemerkung 3.4.8. (a) Für $a \in K$ ist die Matrix der Form $a\mathbb{1}$ eine *sklalare Matrix,* sie ist bestimmt durch den Skalar a. Es gilt also für die Matrixdarstellung $a\mathbb{1} = (a_{ij})_{i,j}$: $a_{ij} = a\delta_{ij}$ bzw.:

$$a\mathbb{1} = a\mathbb{1}_n = aE_n = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix}$$

Diese Matrix ist invertierbar genau dann, wenn $a \neq 0$.

(b) Eine *Diagonalmatrix* $A = (a_{ij})_{i,j}$ hat von Null verschiedene Einträge nur in der Diagonale, es gibt also $a_1, \dots, a_n \in K$ mit $a_{ij} = a_i\delta_{ij}$, bzw.

$$A = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{pmatrix}$$

(c) Eine *obere Dreiecksmatrix* $A = (a_{ij})_{i,j}$ hat unterhalb der Diagonale nur Nullen, also $a_{ij} = 0$ für $i > j$, also

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

Man kann zeigen, dass eine obere Dreiecksmatrix genau dann invertierbar ist, wenn alle Diagonalelemente $a_{jj} \neq 0$ sind.

(d) Die symmetrische Gruppe S_n der Permutationen der Menge $\{1, 2, \dots, n\}$ haben wir in Beispiel 1.5.2 eingeführt. Für $\sigma \in S_n$ definieren wir die *Permutationsmatrix* mit Hilfe der kanonischen Basis $\{e_1, \dots, e_n\}$ durch: $A_\sigma(e_k) = e_{\sigma(k)}$. Es handelt sich also um eine Matrix, die in jeder Zeile und in jeder Spalte genau eine 1 hat, alle anderen Einträge sind 0.

$$A = \left(e^T_{\sigma(1)}, e^T_{\sigma(2)}, \dots, e^T_{\sigma(n)}\right)$$

Beispielsweise gilt:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \in S_4\,;\, A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Da $A_{\sigma\circ\tau} = A_\sigma A_\tau$ sind die Permutationsmatrizen invertierbar: $A_\sigma^{-1} = A_{\sigma^{-1}}$. somit ist die Abbildung:

$$\sigma \in S_n \longmapsto A_\sigma \in \mathrm{Gl}(n,K)$$

ein Gruppenhomomorphismus. Diese Abbildung ist injektiv, da $A_\sigma = \mathbb{1}$ impliziert $\sigma = \mathrm{Id}$.

3.5 Der Rang

Definition 3.5.1. *Der Rang rgf einer linearen Abbildung $f \in Hom(V;W)$ ist die Dimension des Bildes, also $rgf = \dim imf$.*

Eine Matrix $A \in M_K(m,n)$ ist gleichzeitig eine lineare Abbildung in $\mathrm{Hom}(K^m, K^n)$ somit ist auch der Rang $\mathrm{rg}A$ definiert. Damit folgt für $f \in \mathrm{Hom}(V,W) : \mathrm{rg}f \leq \dim V, \mathrm{rg}f \leq \dim W$. Also gilt z.B. $\mathrm{rg}A \leq \min\{m,n\}$.

Lemma 3.5.2. *Wenn D bzw. E eine Basis ist von V bzw. W, und $f \in Hom(V,W)$, und wenn $\Phi_D : V \longrightarrow K^n$ bzw. $\Phi_E : W \longrightarrow K^m$ die Koordinatensysteme von V bzw. W bezüglich D bzw. E sind, dann gilt:*

$$rgf = rg\left(\Phi_E \circ f \circ \Phi_D^{-1}\right) .$$

Satz 3.5.3. *Wenn $r = rgf$ für $f \in Hom(V,W)$ dann gibt es eine Basis D von V bzw. F von W, so dass*

$$\Phi_f \circ f \circ \Phi_D^{-1}(e_j) = \begin{cases} e_j & ; \quad 1 \leq j \leq r \\ 0 & ; \quad j > r \end{cases}$$

Also

$$\Phi_f \circ f \circ \Phi_D^{-1}(e_j) = \left(\begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

Korollar 3.5.4. *Sei $A \in M_K(m,n), rgA = r$. Dann existieren $S \in Gl(m,K), T \in Gl(n,K)$, so dass*

$$SAT^{-1} = \left(\begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array}\right) .$$

Satz 3.5.5. *$A, B \in M_K(n,n)$ heißen* ähnlich, *(Notation: $A \sim B$) genau dann, wenn es $S \in gl(m,K), T \in Gl(n,K)$ gibt mit $B = SAT^{-1}$. Dies ist eine Äquivalenzrelation.*

Satz 3.5.6. *Für $A, B \in M_K(n,n)$ gilt: $A \sim B \Leftrightarrow rgA = rgB$.*

Bemerkung 3.5.7. Diese Aussage ist ein *Klassifikationsresultat.* Für jede Restklasse wird ein Element, nämlich

$$\left(\begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array}\right), \tag{10}$$

ausgezeichnet.
Es folgt, dass es $1 + \min\{m,n\}$ Äquivalenzklassen gibt.

Zu $f \in \text{Hom}(V, W)$ haben wir die transponierte Abbildung $f^T \in \text{Hom}(W^*, V^*)$ eingeführt. Also ist auch insbesondere zu $A \in M_K(m, n)$ die transponierte Matrix $A^T \in M_K(n, m)$ definiert.

Satz 3.5.8. *Sei $A = (a_{ij})_{i,j} \in M_K(m, n)$. Dann sind die Elemente $(b_{ji})_{j,i} \in M_K(n, m)$ erklärt durch: $B_{ji} = a_{ij}$.*

Das Transponieren entspricht der Spiegelung an der Hauptdiagonalen:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}^T = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{nn} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 5 \end{pmatrix}^T = \begin{pmatrix} 1 & 1 \\ 2 & -1 \\ 3 & 5 \end{pmatrix}.$$

Korollar 3.5.9. *Sei $A \in M_K(m, n); B \in M_K(l, m)$. Dann gilt:*

$$(BA)^T = A^T B^T.$$

Bemerkung 3.5.10. In Satz 3.3.5 haben wir die Matrixdarstellung $\Phi_E f \Phi_D^{-1}$ einer linearen Abbildung $f : V \longrightarrow W$ bezüglich der Basis D bzw. E von V bzw. W erklärt. Wir vergleichen diese Darstellung mit der Matrixdarstellung von $f^T : W^* \longrightarrow V^*$ bezüglich $\Phi_E^* : W^* \longrightarrow K^m, \Phi_D^* : V^* \longrightarrow K^n$: Dann gilt:

$$\left(\Phi_E f \Phi_{D^*}^{-1}\right)^T = \Phi_{D^*} f^T \Phi_{E^*}^{-1}.$$

Nach Lemma **??** gilt: $\Phi_{D^*} = \left(\Phi_D^T\right)^{-1}; \Phi_{E^*} = \left(\Phi_E^T\right)^{-1}$ (wobei wir die kanonische Identifikation $K^n \cong (K^n)^*, K^m \cong (K^m)^*$ benutzen. Dann gilt:

$$\left(\Phi_E f \Phi_{D^{-1}}^{-1}\right)^T = \left(\Phi_{D^{-1}}^{-1}\right)^T f^T \Phi_E^T = \Phi_{D^*} \circ f^T \circ \Phi_{E^*}^{-1}.$$

Satz 3.5.11. *$rgA = rgA^t$, d.h. der Spaltenrang stimmt mit dem Zeilenrang überein.*

19.Vorlesung 6.1.2020

4 Lineare Gleichungssysteme

4.1 Lösbarkeit Linearer Gleichungssysteme

Lineare Gleichungssysteme treten in vielen Anwendungen auf, die Lösbarkeitsfrage dieser Gleichungen war ein entscheidender Motor für die Entwicklung der Linearen Algebra:

Definition 4.1.1. *(a) Ein* Lineares Gleichungssystem *mit n Unbekannten und m Gleichungen hat die Form*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_1 \\ &\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_1 \end{aligned}$$

bzw.

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \,;\, i = 1, 2, \ldots, m\,.$$

Hierbei sind $a_{ij}, b_i \in K$. Die Elemente a_{ij} bzw. b_i definieren eine (m,n)-Matrix $A = (a_{ij})_{1 \le i \le m, 1 \le j \le n} \in M_K(m,n)$ bzw. einen Vektor $b = (b_i)_{1 \le i \le m} \in K^m$. Also können wir für ein (m,n)-Lineares Gleichungssystem auch schreiben:

$$A(x) = b$$

mit $A \in M_K(m,n), b \in K^m$.

(b) Ein Element $x_1 \in K^n$ heißt Lösung *des Linearen Gleichungssystems $A(x) = b$, wenn $A(x_1) = b$.*

Bemerkung 4.1.2. In der Schreibweise $A(x) = b$ haben wir zunächst x nicht als Vektor in K^n spezifiziert, im allgemeinen könnte es nämlich keine Lösung geben. Wir suchen also die Menge der Lösungen des Linearen Gleichungssystems, also die Menge

$$\{y \in K^n \,;\, A(y) = b\} = A^{-1}(\{b\}) = A^{-1}(b).$$

Wir werden in Zukunft nicht mehr zwischen dem Symbol x und einem (gesuchten) $x \in K^n$ unterscheiden.

Beispiel 4.1.3. Das $(2,3)$-Lineare Gleichungssystem

$$\begin{aligned} 2x_1 + 3x_2 - 2x_3 &= 5 \\ 5x_1 + 7x_2 &= -2 \end{aligned}$$

entspricht also in Matrixform dem Linearen Gleichungssystem $A(x) = b$ mit

$$A = \begin{pmatrix} 2 & 3 & -2 \\ 5 & 7 & 0 \end{pmatrix} \,;\, b = (5, -2).$$

In Matrixnotation bzw. der Notation mit Hilfe des Matrizenprodukts kann man auch schreiben $A \cdot x^T = b^T$, also

$$\begin{pmatrix} 2 & 3 & -2 \\ 5 & 7 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 5 \\ -2 \end{pmatrix}.$$

Eine Lösung ist in diesem Fall $x_1 = (1, -1, -3)$. Also gilt in diesem Fall:

$$\begin{pmatrix} 2 \\ 5 \end{pmatrix} \cdot 1 + \begin{pmatrix} 3 \\ 7 \end{pmatrix} \cdot (-1) + \begin{pmatrix} -2 \\ 0 \end{pmatrix} \cdot (-3) = \begin{pmatrix} 5 \\ -2 \end{pmatrix}$$

Eine Lösung des Linearen Gleichungssystems liefert also auch eine Darstellung des Vektors b als Linearkombination der Spaltenvektoren der Matrix A.

Als Kriterium für die Existenz bzw. Eindeutigkeit der Lösung erhalten wir:

Theorem 4.1.4 (Fundamentalsatz für Lineare Gleichungssysteme)**.** *Gegeben ist ein (m, n) Lineares Gleichungssystem $A(x) = b$.*

(a) Das Lineare Gleichungssystem besitzt eine Lösung genau dann, wenn der Rang rg$A$ der Koeffizientenmatrix A übereinstimmt mit dem Rang rg(A, b^T) der um den Spaltenvektor b^T erweiterten *Matrix (A, b^T).*

(b) Das Lineare Gleichungssystem besitzt höchstens eine Lösung genau dann, wenn rg$A = n$. (d.h. wenn es eine Lösung gibt, so ist sie eindeutig)

Beispiel 4.1.5. (a)

$$A = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 1 & 7 \end{pmatrix} ;\ b^T = \begin{pmatrix} 4 \\ -1 \end{pmatrix}$$

Dann gilt rg$A = 2$, da die ersten beiden Spaltenvektoren offensichtlich linear unabhängig sind und eine $(2, 3)$-Matrix höchstens den Rang 2 haben kann. Somit ist auch rg$(A, b^T) = 2$, also ist das Lineare Gleichungssystem $A(x)0b$ lösbar.
Da rg$A = 2 \leq 3 = n$ gilt, ist das Lineare Gleichungssystem nicht eindeutig lösbar.

(b) Wir betrachten das Lineare Gleichungssystem $2x_1 + x_2 = 1; 4x_1 + 2x_2 = 0$. Wegen

$$\text{rg} \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} = 1 ;\ \text{rg} \begin{pmatrix} 2 & 1 & 1 \\ 4 & 2 & 0 \end{pmatrix} = 2$$

besitzt dieses Lineare Gleichungssystem keine Lösung.

Insbesondere erhalten wir:

Satz 4.1.6. *Gegeben ist ein (m, n) Lineares Gleichungssystem $A(x) = b$.*

(a) Es gibt für jedes $b \in K^m$ eine Lösung $x \in K^n$ genau dann, wenn rg$A = m$.

(b) Sei $m = n$. Es gibt für jedes $b \in K^n$ genau eine Lösung $x \in K^n$ genau dann, wenn rg$A = n$.

Definition 4.1.7. *Ein Lineares Gleichungssystem $A(x) = 0$ heißt* homogen, *für ein Lineares Gleichungssystem $A(x) = b$ heißt das Lineare Gleichungssystem $A(x) = 0$ das* zugehörige homogene Lineare Gleichungssystem.

Dann erhalten wir folgende Aussage über die Lösungen homogener Linearer Gleichungssysteme bzw. über den Zusammenhang von Lösungen eines Linearen Gleichungssystems und seines zugehörigen homogenen Linearen Gleichungssystems:

Theorem 4.1.8. *(a) Ein homogenes Lineares Gleichungssystem $A(x) = 0$ besitzt stets eine, und zwar die triviale Lösung $x = 0$. Die Menge der Lösung ist der Unterraum* $\ker A$. *Es gibt also nur eine Lösung, wenn* $\ker A = 0$.

(b) Wenn $x_1 \in K^n$ eine Lösung des Linearen Gleichungssystems $A(x) = b$ ist, dann ist jede Lösung x dieses Linearen Gleichungssystems von der Form $x = x_1 + y$, wobei $y \in \ker A$.

Bemerkung 4.1.9. In Teil (b) nennt man x_1 eine *partikuläre* oder *spezielle* Lösung, dann läßt sich jede Lösung, bzw. jede *allgemeine* Lösung x als Summe $x_1 + y$ der partikulären Lösung x_1 und einer allgemeinen Lösung y des zugehörigen homogenen Linearen Gleichungssystems schreiben. Die Lšoungsmenge $L = \{x \in K^n\,;\, A(x) = b\} = \{x_1 + y\,;\, y \in \ker A\}$ ist i.a kein Vektor(unter)raum, aber ein *affiner Unterraum.* In einem Vektorraum V heißt eine Teilmenge $U \subset V$ ein *affiner Unterraum* genau dann, wenn für jeden Vektor $u_1 \in U$ die Menge $\{u - u_1\,;\, u \in U\}$ ein Untervektorraum ist. Dessen Dimension heißt dann die *Dimension* des affinen Raums U. Somit ist die Dimension des Lösungsraums in Teil (b) gegeben durch $\dim \ker A = n - \mathrm{rg}(A)$.

Beispiel 4.1.10.

$$x_1 + 2x_2 + x_3 = 5 \tag{11}$$
$$x_2 - x_3 = -1 \tag{12}$$

Für das zugehörige homogene Lineare Gleichungssystem erhält man als allgemeine Lösung: $y = (-3\alpha, \alpha, \alpha)$ für $\alpha \in K$. Der Lösungsraum des homogenen Linearen Gleichungssystems hat die Dimension 1. Eine spezielle Lösung von Gleichung (11) ist $(1, 1, 2)$. Also ist die allgemeine Lšoung von Gleichung (11) gegeben durch: $x = (1 - 3\alpha, 1 + \alpha, 2 + \alpha)\,, \alpha \in K$.

20.Vorlesung 8.1.2020

4.2 Das Gaußsche Eliminationsverfahren

In diesem Abschnitt lernen wir ein Verfahren kennen, das explizit die Lösungen eines Linearen Gleichungssystems bestimmt.

Satz 4.2.1. *Wir nennen zwei Lineare Gleichungssysteme $A(x) = b$ und $\overline{A}(x) = \overline{b}$* äquivalent, *wenn es eine invertierbare quadratische Matrix $S \in Gl(n, K)$ gibt mit $\overline{A} = SA, \overline{b} = S(b)$. Dies ist eine Äquivalenzrelation. Außerdem stimmen die Lösungsmengen äquivalenter Systeme überein.*

Bemerkung 4.2.2. In Bemerkung **??** haben wir die Matrizen $E_{ij} = (\delta_{ik}\delta_{lj})_{k,l}$ als Basis des Raums $M_K(n, n)$ eingeführt, diese Matrizen haben nur an einer Stelle einen von $=$ verschiedenen Eintrag. Und zwar eine 1 in der i-ten Zeile und der j-ten Spalte. Wir erklaren für $\alpha, \beta \in K, \alpha \neq 0$ die Matrix $S_{ij}(\alpha, \beta) = \alpha\mathbb{1} + \beta E_{ij}$. Dann ist $S_{ij}(\alpha, \beta) \in \mathrm{Gl}(n, K)$, d.h. die Matrix ist invertierbar. Es gilt

$$\begin{aligned} S_{ij}(\alpha,\beta)A &= \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & \dots & \alpha & \dots & \beta & \dots & 0 \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ \alpha a_{i1} + \beta a_{j1} & \dots & \alpha a_{in} + \beta a_{jn} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \end{aligned}$$

Also entspricht die Multiplikation mit der Matrix $S_{ij}(\alpha, \beta)$ der folgenden *elementaren Zeilenumformung:* Addiere zu dem α-fachen der i-ten Zeile der Matrix A das α-fache der j-ten Zeile.

Also gilt insbesondere $S_{ij}(1/\alpha, -\beta/\alpha)S_{ij}(\alpha, \beta) = \mathbb{1}$, d.h. $S_{ij}(\alpha, \beta)$ ist invertierbar, falls $\alpha \neq 0$.

Bezeichne mit a_i die i-te Zeile der Matrix A, dann ist also die Matrix A gegeben durch:

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix}$$

Also ist für $i < j$:

$$S_{ij}(\alpha)A = \begin{pmatrix} a_1 \\ \vdots \\ a_i + \alpha a_j \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix}.$$

Es ist dann leicht einzusehen, dass die Vertauschung von zwei Zeilen ebenfalls die Hintereinanderausführung elementarer Zeilenumformungen ist:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} \to \begin{pmatrix} a_1 \\ \vdots \\ a_i - a_j \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} \to \begin{pmatrix} a_1 \\ \vdots \\ a_i - a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} \to \begin{pmatrix} a_1 \\ \vdots \\ -a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} \to \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix}$$

Elementare Zeilenumformungen sind also Hintereinanderausführungen von

1. Multiplikation einer Zeile mit $\alpha \in K^*$
2. Addition einer Zeile zu einer anderen Zeile
3. Vertauschung von Zeilen

Satz 4.2.3. *Ein (m, n) Lineares Gleichungssystem $A(x) = b$ ist äquivalent zu einem Linearen Gleichungssystem $A^*(x) = b^*$ in* Zeilenstufenform, *d.h. für die Koeffizienten $A = \left(a^*_{ij}\right)_{i,j}$ gilt: Es gibt r Zahlen $1 \leq j_1 < j_2 < \ldots < j_r \leq n, r = rgA$, so dass $a^*_{ij} = 0$ für alle $j < j_1$ oder $j_k \leq j < j_{k+1}, j_k < i$ oder $j_r \leq j \leq n, j_r < i$. Darüberhinaus gilt $a_{1j_1}a_{2j_2}\cdots a_{rj_r} \neq 0$. Durch wiederholte elementare Zeilenumformungen (bzw. Multiplikation mit Matrizen der Form $S_{ij}(\alpha, \beta)$) kann die Zeilenstufenform erreicht werden.*

Bemerkung 4.2.4. Die Zeilenstufenform von A^* :

$$\begin{pmatrix} 0 & \ldots & a^*_{1j_1} & \ldots & . & \ldots & \ldots & . & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 & a^*_{2j_2} & \ldots & . & . & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 & a^*_{rj_r} & \ldots \\ 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & 0 \end{pmatrix} \tag{13}$$

Die Lösungen eines Linearen Gleichungssystems in Zeilenstufenform sind leicht anzugeben:

Theorem 4.2.5. *Sei $A(x) = b$ ein (m, n) Lineares Gleichungssystem. Sei $A^*(x) = b^*$ ein hierzu äquivalentes Lineares Gleichungssystem in Zeilenstufenform. Das Lineare Gleichungssystem $A(x) = b$ besitzt eine Lösung genau dann, wenn $b_i^* = 0$ für alle $i > r$. Dann wähle $x_j, j \notin J := \{j_1, j_2, \ldots, j_r\}$ beliebig, daraus ergeben sich rekursiv für $r, r-1, \ldots$:*

$$\begin{aligned} x_{j_r} &= \frac{1}{a^*_{rj_r}} \left(b^*_r - \sum_{j > j_r} a^*_{rj} x_j \right) \\ x_{j_{r-1}} &= \frac{1}{a^*_{r-1,j_{r-1}}} \left(b^*_{r-1} - \sum_{j > j_{r-1}} a^*_{r-1,j} x_j \right) \\ &= \frac{1}{a^*_{r-1,j_{r-1}}} \left(b^*_{r-1} - \sum_{j > j_{r-1}, j \neq j_r} a^*_{r-1,j} x_j - a_{r-1,j_r} x_{j_r} \right) \end{aligned}$$

und für $k = r-2, r-3, \ldots$:

$$x_{j_k} = \frac{1}{a^*_{k,j_k}} \left(b^*_k - \sum_{j > j_k, j \notin J} a^*_{kj} x_j - \sum_{j > j_k, j \in J} a^*_{kj} x_j \right)$$

So erhält man rekursiv Gleichungen für $x_{j_r}, x_{j_{r-1}}, x_{j_{r-2}}, \ldots$ in Abhängigkeit von $x_j, j \notin J$. Der Lösungsraum ist also ein affiner Unterraum der Dimension $n - r$.

Bemerkung 4.2.6. Tatsächlich könnte man durch weitere elementare Zeilenumformungen auch erreichen, dass man folgende *spezielle Zeilenstufenform* erreicht:

$$\begin{pmatrix} 0 & \ldots & 1 & a_{1,j_1+1} & \ldots & . & \ldots & \ldots & . & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 & 1 & a^*_{2,j_2+1} & \ldots & . & . & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 & 1 & a^*_{r,j_r+1} & \ldots \\ 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & 0 & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & \ldots & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & 0 & \end{pmatrix} \tag{14}$$

Wenn man dann noch Vertauschungen der Variablen zuläßt, was in Rechnungen meist zu Konfusion führt..., erreicht man die Form

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a_{1,r+1} & \ldots \\ 0 & 1 & 0 & \ldots & 0 & a_{2,r+1} & \ldots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 & 1 & a_{r,r+1} & \ldots \\ 0 & \ldots & 0 & 0 & 0 & 0 & \ldots \\ \vdots & & \vdots & & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 & 0 & 0 & \ldots \end{pmatrix} \tag{15}$$

or

$$\left(\begin{array}{c|c} \mathbb{1}_r & * \\ \hline 0 & 0 \end{array} \right)$$

Dann vereinfachen sich die Formeln für die Lösungen aus Theorem 4.2.5 entsprechend.

Beispiel 4.2.7.

$$\left[\begin{array}{cccc|c|c} 1 & 3 & -1 & 2 & 2 & \\ 2 & 1 & -1 & 0 & 1 & \\ 0 & 2 & 1 & 3 & 4 & \\ 2 & 4 & -1 & 3 & 4 & \end{array}\right] \to \left[\begin{array}{cccc|c|c} 1 & 3 & -1 & 2 & 2 & \\ 0 & -5 & 1 & -4 & -3 & Z_2 - 2Z_1 \\ 0 & 2 & 1 & 3 & 4 & \\ 0 & -2 & 1 & -1 & 0 & Z_4 - 2Z_1 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c|c} 1 & 3 & -1 & 2 & 2 & \\ 0 & -10 & 2 & -8 & -6 & 2Z_2 \\ 0 & 10 & 5 & 15 & 20 & 5Z_3 \\ 0 & 0 & 2 & 2 & 4 & Z_4 + Z_3 \end{array}\right] \to \left[\begin{array}{cccc|c|c} 1 & 3 & -1 & 2 & 2 & \\ 0 & -5 & 1 & -4 & -3 & \\ 0 & 0 & 7 & 7 & 14 & Z_3 + Z_2 \\ 0 & 0 & 1 & 1 & 2 & Z_4/2 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c|c} 1 & 3 & -1 & 2 & 2 & \\ 0 & -5 & 1 & -4 & -3 & \\ 0 & 0 & 1 & 1 & 2 & \\ 0 & 0 & 0 & 0 & & \end{array}\right]$$

Aus dieser Zeilenstufenform lesen wir die Lösungen ab:

$$\begin{aligned} x_3 &= 2 - x_4 \\ -5x_2 &= -3 - x_3 + 4x_4 = -3 - (2 - x_4) + 4x_4 = -5 + 5x_4 \\ x_2 &= 1 - x_4 \\ x_1 &= 2 - 3x_2 + x_3 - 2x_4 = 2 - 3(1 - x_4) + (2 - x_4) \\ &= 1 \end{aligned}$$

Also ist die allgemeine Lösung von der Form

$$(x_1, x_2, x_3, x_4) = (1, 1 - x_4, 2 - x_4, x_4) = (1, 1, 2, 0) - x_4(0, -1, -1, 1)$$

für $x_4 \in K$. Also ist $(1, 1, 2, 0)$ eine spezielle Lösung und der Kern der Abbildung A wird erzeugt vom Vektor $(0, -1, -1, 1)$. Aus der Zeilenstufenform liest man ab. $\mathrm{rg}A = 3$, somit ist die Dimension des Lösungsraums $n - \mathrm{rg}A = 4 - 3 = 1$.

21.Vorlesung 13.1.2020

4.3 Die symmetrische Gruppe

wir untersuchen die symmetrische Gruppe S_n, die wir als Gruppe der Permutationen einer n-elementigen Menge $\{1, 2, \ldots, n\}$ eingeführt haben.

Definition 4.3.1. *Ein $\sigma \in S_n$ heißt* Tansposition *der Elemente $i, j \in \{1, 2, \ldots, n\}$ wenn $i \not{0} j$ und $\sigma(i) = j, \sigma(j) = i$ und $\sigma(k) = k$ für alle $k \neq i, j$. Für diese Transposition schreiben wir auch (i, j).*

Satz 4.3.2. *(a) Die* Ordnung *von S_n, also die Anzahl der Elemente, ist $n!$.*

(b) Für $n \geq 3$ ist S_n nicht abelsch.

(c) $(i, j) \cdot (j, i) = \mathbb{1}$.

(d) Jede Transposition (i, j) ist konjugiert zu der Transposition $(1, 2)$, d.h. es gibt ein $\sigma \imath n S_n$ mit $(i, j) = \sigma(1, 2)\sigma^{-1}$.

Lemma 4.3.3. *Zu jeder Permutation $\sigma \in S_n, n \geq 2$ gibt es (nicht eindeutig bestimmte) Transpositionen $(i_1, j_1), \ldots, (i_k, j_k)$ mit $k \leq n$ und $\sigma = (i_1, j_1) \circ \cdots \circ (i_k, j_k)$ ist das Produkt von höchstens n Transpositionen.*

Definition 4.3.4. *Eine Transposition $(i, j); 1 \leq i < j \leq n$ heißt* Verstellung *oder* Fehlstellung, *wenn $\sigma(i) > \sigma(j)$. Das* Vorzeichen *der Permutation ist erklärt durch*

$$\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} \in \{\pm 1\}\,.$$

Die Permutation σ heißt gerade *bzw.* ungerade, *wenn $\epsilon\sigma = 1$ bzw. $= -1$.*

Bemerkung 4.3.5. $\epsilon(\sigma) = \pm 1$ da mit $(j - i)$ im Nenner auch $(j - i)$ bzw. $-(j - i)$ im Zähler auftritt, je nachdem ob (i, j) eine Verstellung ist, oder nicht. Insbesondere ist die Permutation σ also gerade bzw. ungerade genau denn, wenn die Anzahl der Paare, die eine Verstellung von σ sind, gerade bzw. ungerade ist.

Satz 4.3.6. *Sei $n \geq 2$.*

(a) Die Abbildung

$$\epsilon : \sigma \in S_n \longmapsto \epsilon(\sigma) \in \{\pm 1\} \cong \mathbb{Z}_2$$

ist ein Gruppenhomomorphismus.

(b) Wenn $\sigma = (i_1, j_1) \circ \cdot \circ (i_k, j_k)$ dann gilt $\epsilon(\sigma) = (-1)^k$.

Beispiel 4.3.7.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Dann können wir σ als Produkt von Transpositionen darstellen:

$$\begin{aligned} \sigma_1 &= (1, 2) \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\ \sigma_2 &= (2, 4) \circ \sigma_1 = \mathrm{Id}\,. \end{aligned}$$

Also $\sigma = (2, 4) \circ (1, 2)$. Somit $\epsilon(\sigma) = (-1)(-1) = 1$.

Definition 4.3.8. *Für $n \geq 2$ ist die* alternierende Gruppe *die Untergruppe $\{\sigma \in S_n\,;\, \epsilon(\sigma) = 1\}$ der geraden Permutationen.*

Satz 4.3.9. *Die alternierende Gruppe A_n ist eine invariante Untergruppe von S_n und $S_n/A_n \cong \mathbb{Z}_2$. Jede $\sigma \in S_n - A_n$ läßt sich darstellen als Produkt $\sigma = \tau \circ \sigma'$ einer Transposition und einer geraden Permuatation $\sigma' \in A_n$. Die alternierende Gruppe hat die Ordnung $n!/2$.*

4.4 Determinante

Von nun an betrachten wir kommutative Körper K.

Definition 4.4.1. *Eine Abbildung*

$$\det : M_K(n,n) \longrightarrow K$$

heißt Determinante *bzw.* Determinantenabbildung, *wenn folgende Eigenschaften erfüllt sind:*

(a) det *ist* multilinear, *d.h. linear in jeder Zeile. Wenn*

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

mit den Zeilen $a_1, \ldots, a_n$ dann gilt

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i + b_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ b_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}$$

und

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \alpha a_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \alpha \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}.$$

(b) det *ist* alternierend, *d.h.*

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} = -\det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix}.$$

(c) $\det(\mathbb{1}) = 1$.

Bemerkung 4.4.2. Aus der Multilinearität folgt, dass $\det A = 0$ wenn eine Zeile $a_i = 0$. Ebenso folgt, dass $\det A = 0$ falls $a_i = a_j, i \neq j$.

Satz 4.4.3. *Eine Determinante besitzt auch die folgende Eigenschaft: Sei* $\alpha, \beta \in K, i \neq j$

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \alpha a_i + \beta a_j \\ a_{i+1} \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} = \alpha \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ a_i \\ a_{i+1} \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix}.$$

22.Vorlesung 15.1.2020

Bemerkung 4.4.4. (a) Man kann durch mehrfache Addition des Vielfachens einer j-ten Zeile zur i-ten Zeile, d.h. Multiplikation mit einer Matrix $S_{ij}(1, \alpha)$ eine Zeilenstufenform einer Matrix A erreichen. Nach Satz 4.4.3 stimmt die Determinante dieser Matrix in Zeilenstufenform mit $\det A$ überein.

(b) Wenn $\mathrm{rg}A = r < n$ dann ist $\det A = 0$. Nach (a) erreicht man die Zeilenstufenform, wenn $r < n$ dann ist ein Zeilenvektor 0, somit gilt $\det A = 0$.

(c) Für eine Diagonalmatrix

$$D = \begin{pmatrix} d_1 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ 0 & 0 & d_3 & \dots & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & d_n \end{pmatrix}$$

also $D = (d_{ij})$ mit $d_{ij} = d_i \delta_{ij}$ gilt:

$$\det A = d_1 d_2 \cdots d_n \,.$$

Denn nach Bemerkung 4.4.4 gilt $\det A = d_1 d_2 \cdots d_n \cdot \mathbb{1} = d_1 d_2 \cdots d_n$ nach Definition 4.4.1 (c).

(d) Falls $\mathrm{rg}A = n$ und falls A durch Zeilenumformungen der Form $S_{ij}(a, \beta)$, also Addition des Vielfachen einer anderen Zeile zu einer gegebenen Zeile, auf die Zeilenstufenform A^* mit Hauptdiagonalelementen $a_{11}^*, \dots, a_{nn}^* \neq 0$ gebracht werden kann, dann gilt $\det A = \det A^* = a_{11}^* \cdots a_{nn}^*$: Denn durch weitere elementare Zeilenumformungen der Art $S_{ij}(1, \beta)$ erreicht man die Diagonalmatrix D mit den Einträgen $d_i = a_{ii}^*$.

Theorem 4.4.5. *Es existiert genau eine Determinante, es gilt:*

$$\det A = \sum_{\sigma \in S_n} a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \,. \tag{16}$$

Beispiel 4.4.6. (a) $n = 2 : S_2 = \{\mathrm{Id}, (1,2)\}$, also

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

(b)

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

woraus wegen $S_3 = A_3 \cup \{\tau \circ \sigma; \sigma \in A_3\}, \tau = (1,2)$ folgt:

$$\det A = \sum_{\sigma \in A_3} a_{1\sigma(1)} a_{2\sigma(2)} a_{3\sigma(3)} - \sum_{\sigma \in A_3} a_{1\tau\sigma(1)} a_{2\tau\sigma(2)} a_{3\tau\sigma(3)}.$$

Dies wird auch als *Regel von Sarrus* bezeichnet:

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

Man bildet das Produkt aus den Einträgen in den drei Diagonalen von oben links nach unten rechts und subtrahiert die Produkte aus den Einträgen in den drei Diagonalen von unten links nach oben rechts.

Theorem 4.4.7. *$A, B \in M_K(n,n)$. Dann gilt*

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

Insbesondere ist dann

$$\det : Gl(n,K) \longrightarrow K^*$$

ein Gruppenhomomorphismus.

Bemerkung 4.4.8. (a) Falls A invertierbar ist, so gilt $\det(A^{-1}) = \det(A)-1$. Dies folgt aus $AA^{-1} = \mathbb{1}$.

(b) Für eine Matrix $A \in M_K(n,n)$ gilt: A ist invertierbar genau dann, wenn $\det(A) \neq 0$. Im Beweis von Theorem 4.4.5 wurde gezeigt, dass $\det A = n$ äquivalent ist dazu, dass A invertierbar ist..

(c) Die *spezielle lineare Gruppe* $\mathrm{SL}(n,K)$ ist der Kern des Gruppenhomomorphismus $\det : \mathrm{Gl}(n,K) \longrightarrow K^*$. Obere Dreiecksmatrizen $A = (a_{ij})$ mit $\det A = a_{11}a_{22} \cdot a_{nn} = 1$ liegen also in $\mathrm{SL}(n,K)$.

23.Vorlesung 22.01.2020

Definition 4.4.9. *Sei V ein Vektorraum über dem Körper K und $f : V \longrightarrow V$ eine linearer Endomorphismus.*

(a) Das Element $\lambda \in K$ heißt Eigenwert *, wenn es einen Vektor $x \in V, x \neq 0$ gibt mit $f(x) = \lambda x$. Der Vektor x ist dann ein* Eigenvektor *zum Eigenwert λ.*

(b) Die Menge der Eigenvektoren zum Eigenwert λ heißt Eigenraum *zum Eigenwert λ, er kann mit $\ker(f - \lambda Id)$ identifiziert werden.*

(c) Da eine Matrix $A \in M_K(n, n)$ auch als lineare Abbildung $A : K^n \longrightarrow K^n$ aufgefaßt werden kann, sind auch Eigenwerte, Eigenvektoren und Eigenräume für die Matrix A erklärt.

Bemerkung 4.4.10. Wenn $\lambda \in K$ ein Eigenwert ist, besitzt also das lineare Gleichungssystem $(A - \lambda \mathbb{1})(x) = 0$ eine nicht-triviale Lsöung $x \neq 0$. Dann muss also $A - \lambda \mathbb{1}$ nicht invertierbar sein, die Dimension des Lösungsraums stimmt also überein mit $n - \operatorname{rg}(A - \lambda \mathbb{1})$. Insbesondere gilt $\det(A - \lambda \mathbb{1}) = 0$. Dann ist also 0 ein Eigenwert, wenn $\det A = 0$, wenn also A nicht invertierbar ist.

Beispiel 4.4.11. Wir betrachten die $(2, 2)$-Matrix

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Geometrisch beschreibt diese Abbildung eine *Drehung* um den Winkel α. Abhängig davon, ob wir diese Matrix für $K = \mathbb{R}$ oder $K = \mathbb{C}$ betrachten, untersuchen wir ihre Eigenwerte. Nach Bemerkung 4.4.10 ist λ ein Eigenwert, wenn für λ gilt:$\det(A - \lambda \mathbb{1}) = 0$. Wir bilden

$$\begin{aligned} \det\left\{\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} - \lambda \mathbb{1}\right\} &= \det\begin{pmatrix} \cos\alpha - \lambda & -\sin\alpha \\ \sin\alpha & \cos\alpha - \lambda \end{pmatrix} \\ &= \lambda^2 - 2\lambda\cos\alpha + 1 = (\lambda - \cos\alpha)^2 + \sin^2\alpha = 0\,. \end{aligned}$$

Diese quadratische Gleichung hat über $\mathbb{R}$ nur eine Lösung, falls $\sin\alpha = 0$, also $\alpha = k\pi, k \in \mathbb{Z}$. Dann gilt $A = \pm\mathbb{1}$. Andernfalls hat A über $\mathbb{R}$ keinen Eigenwert. Über $\mathbb{C}$ gibt es immer die beiden Lösungen: $\lambda_{1,2} = \cos\alpha \pm i \sin\alpha$ mit der imaginären Einheit i mit $i^2 = -1$.

Definition 4.4.12. *Für eine Matrix $A \in M_K(n, n)$ heißt*

$$\chi_A(t) = \det(t\mathbb{1} - A)$$

das charakteristische Polynom.

Bemerkung 4.4.13. Wenn $p(t) = \sum_j^n a_j t^j$ ein Polynom ist, dann heißt $n = \operatorname{grad}(p)$ der *Grad* von p, sofern $a_n \neq 0$. Wegen

$$\begin{aligned} \chi_A(t) = \sum_{\sigma \in S_n} \epsilon(\sigma) \left(t\delta_{1\sigma(1)} - a_{1\sigma(1)}\right) \cdots \left(t\delta_{n\sigma(n)} - a_{n\sigma(n)}\right) \\ = \sum_{i=0}^{n} \alpha_i t^t \end{aligned}$$

folgt $\alpha_n = 1$ $\alpha_{n-1} = -\sum_{i=1}^n a_{ii} = -\mathrm{Spur}(A)$ und $\alpha_0 = (-1)^n \det A$. Dies sieht man so ein. In obiger Formel ist der Term, der $\sigma = \mathrm{Id}$ entspricht:

$$(t - a_{11}) \cdots (t - a_{nn}) = t^n - t^{n-1} \sum_i a_{ii} + R(t)\,,$$

wobei $R(t)$ ein Polynom vom Grad $\leq (n-2)$ ist. Für $t = 0$ erhalten wir $\chi_A(0) = \det(-A) = (-1)^n \det A$.

Beispiel 4.4.14.

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

$$\chi_A(t) = \det \begin{pmatrix} t-1 & 0 & -2 \\ 0 & t & -1 \\ 0 & 1 & t \end{pmatrix} = (t-1)\det \begin{pmatrix} t & -1 \\ 1 & t \end{pmatrix} = (t-1)(t^2+1) = t^3 - t^2 + t - 1\,.$$

Also $\det A = 1, \mathrm{Spur} A = 1$. Für $K = \mathbb{R}$ gibt es nur einen Eigenwert, nämlich 1. Für $K = \mathbb{C}$ sind darüber hinaus auch $i, -i$ Eigenwerte.

Bemerkung 4.4.15. Wenn $A, B \in M_K(n,n)$ konjugiert zueinander sind, d.h. wenn es eine invertierbare Matrix $T \in \mathrm{Gl}(n,K)$ gibt mit $B = TAT^{-1}$, dann gilt

$$\begin{aligned} \chi_B(t) &= \det(t\mathbb{1} - B) = \det\left(t\mathbb{1} - TAT^{-1}\right) \\ &= \det\left(T\,(t\mathbb{1} - A)\,T^{-1}\right) = \det(t\mathbb{1} - A) = \chi_A(t)\,. \end{aligned}$$

Damit kann man also einsehen, dass das charakteristische Polynom $\chi_f(t)$ einer linearen Abbildung eines endlich-dimensionalen Vektorraums V der Dimension n wohldefiniert ist. Sei $\Phi_B : V \longrightarrow K^n$ ein Isomorphismus, dann definiere $\chi_f(t) = \chi_A(t)$ für $A = \Phi_B \circ f \circ \Phi_B^{-1}$. Damit sind dann auch die Determinante $\det f = \det A$, die Spur $\mathrm{Spur} f = \mathrm{Spur} A$ wohldefiniert (also unabhängig von der Wahl des Koordinatensystems).

Zusammenfassend erhalten wir also das

Theorem 4.4.16. *Die Nullstellen des charakteristischen Polynoms $\chi_A(t)$ einer Matrix $A \in M_K(n,n)$ bzw. des charakteristischen Polynoms $\chi_f(t)$ eines linearen Endomorphismus $f \in End(V)$ stimmen überein mit den Eigenwerten der Matrix A bzw. des linearen Endomorphismus f.*

Theorem 4.4.17. *(a) Eine Matrix $A \in M_K(n,n)$ ist konjugiert zu einer Diagonalmatrix (d.h. ist* digaonalisierbar*) genau dann, wenn es in K^n eine Basis $B = \{b_1, \ldots, b_n\}$ aus Eigenvektoren von A gibt.*

(b) eine lineare Abbildung $f : V \longrightarrow V$ besitzt eine Koordinatendarstellung $\Phi_B \circ f \circ \Phi_B^{-1}$ als Diagonalmatrix genau dann, wenn die zugehörige Basis B aus Eigenvektoren von A besteht.

Beispiel 4.4.18. Die Matrix

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

ist nicht diagonalisierbar. Das charakteristische Polynom ist gegeben durch:

$$\chi_A(t) = \det \begin{pmatrix} t-1 & -1 \\ 0 & t-1 \end{pmatrix} = (t-1)^2$$

also ist $\lambda = 1$ der einzige Eigenwert. Der Eigenraum hat die Dimension

$$\mathrm{rg}(\mathbb{1} - A) = \mathrm{rg} \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} = 1.$$

Also gibt es keine Basis aus Eigenvektoren.

Satz 4.4.19. *Wenn $b_1, \ldots, b_r$ von = verschiedene Eigenvektoren eines linearen Endomorphismus $f : V \longrightarrow V$ mit r paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_r$ sind, dann sind die Vektoren $b_1, \ldots, b_r$ linear unabhängig.*

<u>24.Vorlesung 27.01.2020</u>

4.5 Zerlegung von Polynomen

Da die Nullstellen des charakteristischen Polynoms die Eigenwerte der linearen Abbildung sind, notieren wir einige Eigenschaften von Polynomen in Bezug auf die Darstellung mit Hilfe von Linearfaktoren: Zur Gültigkeit des *Euklidischen Algorithmus:*

Theorem 4.5.1 (Polynomdivision)**.** *Seien $p(t), q(t)$ Polynome mit Koeffizienten in K, $gradp = n \geq 0, gradq = m \geq 0$. Dann gibt es eindeutig bestimmte Polynome $d(t), r(t)$ mit $gradr(t) < m$, so dass:*

$$p(t) = d(t)q(t) + r(t)\,.$$

Falls $n < m$ so ist $d(t) = 0, r(t) = p(t)$. Falls Falls $n \geq m$, so gilt $gradd(t) = n{-}m$, $gradr(t) < m$, (einschließlich $r(t) = 0$, dann ist $gradr(t) = -\infty$.)

Durch Polynomdivision erhält man z.B.:

$$(t^5 + t^4 + 2t + 1) = (t^2 -^{)}\,(t^3 + t^2 + 2t + 2) + 6t + 5\,.$$

Korollar 4.5.2. *Sei $p(t) \in K[t]$ ein Polynom vom Grad $n \geq 1$. Dann ist $\lambda \in K$ eine Nullstelle von $p(t)$, d.h. $p(\lambda)=0$, genau dann, wenn es ein Polynom $d(t)$ vom Grad $(n-1)$ gibt, so das*

$$p(t) = d(t)(t - \lambda)\,.$$

Bemerkung 4.5.3. (a) Ein Polynom $p(t)$ *zerfällt vollständig in Linearfaktoren* wenn es Elemente $\lambda_1, \ldots, \lambda_r \in K$ gibt, mit

$$p(t) = a_n(t - \lambda_1) \cdots (t - \lambda_r)\,.$$

Die λ_i sind dann die Nullstellen von $p(t)$. Wir können zusätzlich fordern, dass diese Zahlen paarweise verschieden sind, dann

$$p(t) = a_N(t - \lambda_1)^{m_1} \cdots (t - \lambda_s)^{m_s}\,,$$

d.h. hier sind die Zahlen $\lambda_1, \cdots, \lambda_s$ paarweise verschieden und den *Vielfachheiten* oder *Multiplizitäten* $m_1, \ldots, m_s \in \mathbb{N}$. Dann gilt $m_1 + \cdots + m_s = n$.

(b) Es ist eine Frage der Algebra, in welchen Körpern K jedes Polynom in Linearfaktoren zerfällt. Wir zitieren (ohne Beweis)den folgenden Satz

Theorem 4.5.4 (Fundamentalsatz der Algebra)**.** *Jedes Polynom $p(t) \in \mathbb{C}[t]$ zerfällt in Linearfaktoren.*

Daraus ergibt sich leicht:

Satz 4.5.5. *Jedes Polynom $p(t) \in \mathbb{R}[t]$ zerfällt in ein Produkt von Linearfaktoren und quadratischen Polynomen.*

Damit erhalten wir das

Theorem 4.5.6. *Wenn das charakteristische Polynom χ_f eines Endomorphisms $f : V \longrightarrow V$ vollständig in Linearfaktoren zerfällt mit paarweise verschiedenen Nullstellen, dann ist f diagonalisierbar, d.h. bezüglich einer Basis aus Eigenvektoren hat f die Darstellung $(\lambda_i \delta_{ij})_{i,j}$. Dann ist der Vektorraum $V = V_f(\lambda_1) \oplus \cdots \oplus V_f(\lambda_n)$ die direkte Summe der ein-dimensionalen Eigenräume $V_f(\lambda_j)$.*
Insbesondere: Falls das charakteristische Polynom $\chi_A(t)$ einer Matrix $A \in M_K(n,n)$ vollständig in Linearfaktoren zerfällt mit paarweise verschiedenen Nullstellen, dann ist A konjugiert zu einer Diagonalmatrix.

25.Vorlesung 29.01.2020

4.6 Satz von Cayley-Hamilton

Bemerkung 4.6.1. Für eine Matrix $A \in M_K(n,n)$ betrachte die Potenzen $A^0 = \mathbb{1}, A^1 = A, A^2, \dots$. Da $\dim M_K(n,n) = n^2$ gilt: $\mathbb{1}, A, A^2, \dots, A^{n^2}$ sind linear abhängig. Es gibt also eine Relation der Form

$$a_0\mathbb{1} + a_1 A + a_2 A^2 + \ldots + a_{n^2} A^{n^2} = 0$$

für $a_i \in K$. Der Satz von Cayley-Hamilton zeigt, dass schon die Potenzen $\mathbb{1}, A, a^2, \dots, A^n$ linear abhängig sind, d.h. es gibt $a_0, a_1, \dots, a_n \in K$, so dass

$$a_0\mathbb{1} + a_1 A + a_2 A^2 + \ldots + a_n A^n = 0$$

diese Aussage schreibt man auch so: Für das Polynom

$$p(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n$$

gilt:

$$p(A) = a_0\mathbb{1} + a_1 A + a_2 A^2 + \ldots + a_n A^n = 0\,.$$

Wir untersuchen den Spezialfall $n = 2$ und A ist eine Diagonalmatrix mit den Einträgen λ, μ in der Hauptdiagonalen. Dann ergibt sich aus der Gleichung

$$a_0\mathbb{1} + a_1 A + a_2 A^2 = 0$$

für $a_2 = 1$ ein lineares Gleichungssystem für a_1, a_0 mit der Lösung $a_1 = -(\lambda + \mu) = -\mathrm{Spur}A, a_0 = \lambda\mu = \det A$. Diese Gleichung gilt dann also auch für alle diagonalisierbaren Matrizen. Das Polynom

$$p(t) = t^2 - (\mathrm{Spur}A)\, t + \det A$$

ist das *charakteristische Polynom* χ_A der Matrix A, für eine diagonalisierbare Matrix $A \in M_K(2,2)$ haben wir also gezeigt: $\chi_A(A) = 0$.

Definition 4.6.2. $A \in M_K(n,n)$: *Dann definieren wir die Abbildung*

$$\Psi_A : K[t] \longrightarrow M_K(n,n)\,;$$
$$\Psi_A(p(t)) = \Psi_A\left(\sum_{i=0}^n a_i t^i\right) = \sum_{i=0}^n a_i A^i\,.$$

Lemma 4.6.3. Ψ_A *ist ein Ringhomomorphismus, d.h.*

$$\Psi_A\left(\alpha p(t) + \beta q(t)\right) = \alpha\Psi_A(p(t)) + \beta\Psi_A(q(t))$$
$$\Psi_A(p(t)q(t)) = \Psi_A(p(t))\Psi_A q(t))\,.$$

wir benutzen die folgende Notation: $\mathrm{im}\Psi_A = K[A]$.

Theorem 4.6.4 (Cayley-Hamilton)**.** *Für eine Matrix $A \in M_K(n,n)$ sei χ_A das charakteristische Polynom. Dann gilt:*

$$\Psi_A\left(\chi_A(A)\right) = \chi_A(A) = 0 \in M_K(n,n)\,.$$

Satz 4.6.5. *Sei $A \in M_K(n,n)$. Dann gibt es genau ein Polynom $\mu_A(t)$ mit höchstem Koeffizienten 1, so dass jedes Polynom $p(t)$ mit $p(A) = 0$ Vielfaches ist von $\mu_A(t)$. Insbesondere teilt $\mu_A(t)$ das charakteristische Polynom $\chi_A(t)$; d.h. $\mu_A(t)|\chi_A(t)$. Das Polynom $\mu_A(t)$ heißt* Minimalpolynom *von A.*

26.Vorlesung 03.02.2020

Beispiel 4.6.6. (a)

$$A = \lambda \mathbb{1} = \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} \Rightarrow \chi_A(t) = \det \begin{pmatrix} t-\lambda & & \\ & \ddots & \\ & & t-\lambda \end{pmatrix} = (t-\lambda)^n$$

Das Minimalpolynom hat also die Form $\mu_a(t) = (t-\lambda)^k, k \leq n$. Da $A - lambdaid = 0$ gilt $\mu_A(t) = t - \lambda$.

(b)

$$A = J_k(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \in M_K(k,k)$$

Dann gilt

$$\chi_A = \det \begin{pmatrix} t-\lambda & -1 & & \\ & \ddots & \ddots & \\ & & \ddots & -1 \\ & & & t-\lambda \end{pmatrix} = (t-\lambda)^k .$$

Wegen

$$B = A - \lambda \mathbb{1} = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

und $B(e_1) = 0, B(e_i) = e_{i-1}, i = 2, \ldots, k$ gilt $B^l(e_i) = 0, i \leq l, B^l(e_i) = e_{i-l}, i \geq l+1$. Somit ist $B^{k-1} \neq 0, B^k = 0$. Die Matrix B ist *nilpotent*. Deshalb stimmen das Minimalpolynom und das charakteristische Polynom überein:

$$\mu_A(t) = \chi_A(t) = (t-\lambda)^k.$$

Satz 4.6.7. *$f \in End(V)$ bzw. $A \in M_K(n,n)$ besitzt eine Darstellung als (obere)Dreiecksmatrix genau dann, wenn $\chi_f(t)$ (bz.w $\chi_A(t)$) vollständig in Linearfaktoren zerfällt, d.h. es gibt $\lambda_1, \ldots, \lambda_n \in K$ mit*

$$\chi_f(t) = (t-\lambda_1)\ldots(t-\lambda_n).$$

Folgerung 4.6.8 (Cayley-Hamilton für Dreiecksmatrizen)**.** Wenn $f \in \mathrm{End}(V)$ und wenn $\chi_f(t)$ vollständig in Linearfaktoren zerfällt, dann gilt $\chi_f(f) = 0$.