Konstruktive Lineare Algebra I

Dozent: Prof. Mohamed Barakat / Mitschrift: Alexander Köster

23. Mai 2018

Eine Sammlung des zusammengefassten Vorlesungs- und Übungsstoffes der linearen Algebra.

Diese Zusammenfassung ersetzt keine Klausurvorbereitung. Sie wurde unabhängig von der Universität erstellt und beinhaltet nur die wichtigsten Sätze und Algorithmen.
Alles aus der Vorlesung, dem zugehörigen Skript und den zugehörigen Übungen, was nicht in dieser Zusammenfassung enthalten ist, ist dennoch wichtig für das Verständnis oder den Beweis der gegebenen Sätze.
Bis auf ein paar Anpassungen, besonders in den ersten und letzten Themenbereichen, unterliegen die Sätze dem Urheberrecht von Prof. Barakat. Ich bin sehr dankbar für die Detailtiefe seiner Vorlesung, die die Veranstaltung deutlich lehrreicher gemacht hat als übliche Vorlesungen der Linearen Algebra.

Besonders wichtige Sätze und Anmerkungen sind in violett geschrieben.
Beispiele sind in pink geschrieben.

Inhaltsverzeichnis

© study.woalk.de Vervielfältigung ohne ausdrückliche Erlaubnis des Autors außerhalb der originalen Website untersagt.

Im gesamten folgenden Dokument sei K ein beliebiger Körper.

0 Mathematische Grundlagen

Definition 0.2.0: Standardmenge

Die „**Standardmenge** n“ für $n \in \mathbb{N}$ ist $\underline{n} := \{m \in \mathbb{N} \mid 1 \leq m \leq n\} = \{1, 2, \ldots, n\} \subset \mathbb{N}$.

0.4 Abbildungen

Bemerkung 0.4.3:

- Eine Abbildung $a : \mathbb{N} \to M$ heißt **Folge** in M, man schreibt oft $(a_i)_{i \in \mathbb{N}}$ mit $a_i := a(i)$.
- Ein n**-Tupel** $x := (x_1, \ldots, x_n)$ mit $n \in \mathbb{N}$ wird als Abbildung $x : \underline{n} \to M,\ i \mapsto x_i$ aufgefasst.

Definition 0.4.7/8/16: Eindeutigkeit/Totalität

Sei $f : X \to Y$ eine Abbildung.

1. f **injektiv**, wenn $\forall x, x' \in X : f(x) = f(x') \Rightarrow x = x'$, bzw. jede Faser *höchstens* einelementig. Genau dann ist f linksinvertierbar. Man schreibt auch $f : X \hookrightarrow Y$.
2. f **surjektiv**, wenn $f(X) = Y$, bzw. jede Faser *mindestens* einelementig.
   Genau dann ist f rechtsinvertierbar. Man schreibt auch $f : X \twoheadrightarrow Y$.
3. f **bijektiv**, wenn injektiv und surjektiv, bzw. jede Faser *genau* einelementig.
   Genau dann ist f invertierbar, und Rechtsinverse = Linksinverse. Man schreibt auch $f : X \xrightarrow{\sim} Y$.

Bemerkung 0.4.10: Endliche Abbildungen

Für eine Abbildung $f : N \to M$ zwischen *endlichen* Mengen N, M gilt:

- $|f(N)| \leq |N|, |M|$
- f injektiv $\Leftrightarrow |f(N)| = |N|$
- f surjektiv $\Leftrightarrow |f(N)| = |M|$
- Ist $|N| = |M|$, gilt: f injektiv $\Leftrightarrow f$ surjektiv $\Leftrightarrow f$ bijektiv

Definition 0.4.11/12: Einschränkung

Sei $f : X \to Y$ eine Abbildung, $X' \subset X$.
Dann heißt $f_{|_{X'}} : X' \to Y, x \mapsto f(x)$ die **Einschränkung** von f auf X'.
Jede Abbildung kann durch Einschränkung injektiv gemacht werden.

Definition 0.4.13: Komposition

Seien $f : N \to M, g : M' \to L$ mit $f(N) \subseteq M' \subseteq M$.
Dann ist $g \circ f : N \to L, \quad (g \circ f)(x) := g(f(x))$ die **Komposition** (Verkettung) von f und g.

Komposition ist assoziativ.

© study.woalk.de

0.5 Relationen

Definition 0.5.1: Relation

Seien N, M Mengen.

1. $R \subseteq M \times N$ heißt **Relation** zwischen M und N. Für $(x, y) \in R$ schreibt man xRy.
2. Ist $R \subseteq M \times M$, so sprechen wir von einer Relation **auf** M. Sie ist:
   (R) **reflexiv** :$\Leftrightarrow \forall x \in M : xRx$
   (R') **antireflexiv** :$\Leftrightarrow \forall x \in M : \neg xRx$
   (S) **symmetrisch** :$\Leftrightarrow \forall x, y \in M : xRy \Rightarrow yRx$
   (S') **antisymmetrisch** :$\Leftrightarrow \forall x, y \in M : (xRy \wedge yRx) \Rightarrow x = y$
   (T) **transitiv** :$\Leftrightarrow \forall x, y, z \in M : (xRy \wedge yRz) \Rightarrow xRz$
3. Eine Relation, die (R), (S') und (T) erfüllt, heißt **(partielle) Ordnung**.
4. Eine Ordnung heißt **Totalordnung**, falls zusätzlich $\forall x, y \in M : xRy \vee yRx$.
5. Eine Relation, die (R), (S) und (T) erfüllt, heißt **Äquivalenzrelation (ÄR)**.

Definition 0.5.7/9: Äquivalenzrelation

Sei $\sim$ eine ÄR auf M. Für $x \in M$ heißt

$$[x] := [x]_{\sim} := \{y \in M \mid x \sim y\}$$

die **Äquivalenzklasse** von $\sim$ zu x (oder von x bezüglich $\sim$).
Die Menge aller Äquivalenzklassen wird mit $M/\sim := \{[x]_{\sim} \mid x \in M\}$ bezeichnet.
Dies ist eine Partition von M.

0.6 Kategorie der Mengen

1 Lineare Gleichungssysteme

Definition 1.1.0: Faser

Für $f : X \to Y$, $y \in Y$ heißt die Menge

$$f^{-1}(\{y\}) := \{x \in X \mid f(x) = y\}$$

Faser von f über y.

Bemerkung 1.1.1: GLS

Die Faser $f(\{b\})$ ist die Lösungsmenge des Gleichungssystems $f(x) = b$ für x.

Definition 1.2.1: (verallgemeinert) Matrix

Seien $m, n \in \mathbb{N}$. Eine $m \times n$**-Matrix** ist eine Abbildung

$$A : \underline{m} \times \underline{n} \to K, \quad (i, j) \mapsto A_{i,j}, \quad A_{i,j} \in K \; \forall i \in \underline{m}, j \in \underline{n}$$

Eine $m \times n$-Matrix A hat m Zeilen und n Spalten. Man sagt $A = (A_{i,j}) \in K^{m \times n}$ mit $i \in \underline{m}$, $j \in \underline{n}$.
Man schreibt in Matrizen manchmal $\cdot$ anstelle von 0, um besser unterscheidbar zu machen, wenn viele Nullen enthalten sind, z.B. in Matrizen über dem $\mathbb{F}_2$-Körper.
Man kann Matrizen addieren und mit Körperelementen multiplizieren (skalieren).

© study.woalk.de

Definition 1.2.2: (VERALLGEMEIENRT) LINEARES GLS

Ein **Lineares Gleichungssystem** mit m Gleichungen und n Unbekannten $x_1, \ldots, x_n$ ist gegeben durch

$$\begin{aligned} A_{1,1}x_1 + A_{1,2}x_2 + \ldots + A_{1,n}x_n &= b_1 \\ A_{2,1}x_1 + A_{2,2}x_2 + \ldots + A_{2,n}x_n &= b_2 \\ \vdots & \quad \vdots \\ A_{m,1}x_1 + A_{m,2}x_2 + \ldots + A_{m,n}x_n &= b_m \end{aligned} \tag{I}$$

wobei $A = (A_{i,j}) \in K^{m\times n}$ und $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^{m\times 1}$.

Ein LGLS heißt **homogen**, wenn von der Form $Ax = 0$.
$\xrightarrow[2.3.15]{}$ $Ax - b$ ist lösbar $\Leftrightarrow b \in \mathrm{Bild}(\tilde{A})$.

Die Lösungsmenge von $Ax = 0$ ist $\mathrm{Kern}(\tilde{A})$ und damit nie leer.

Ist $Y \in K^{n\times 1}$ eine Lösung von $Ax = b$, so durchläuft $X + Y$ mit $X \in \mathrm{Kern}(\tilde{A})$ (Lösung von $Ax = 0$) alle Lösungen von $Ax = b$.

Definition 1.2.5/6: (VERALLGEMEINERT) LINEARE ABBILDUNG

Eine Abbildung $\alpha : K^{n\times 1} \to K^{m\times 1}$ heißt linear, wenn

$$\forall s_1, \ldots, s_k \in K^{n\times 1},\ r_1, \ldots, r_k \in K : \alpha\left(\sum_{i=1}^{k} r_i s_i\right) = \sum_{i=1}^{k} r_i \alpha(s_i)$$

Zu zeigen reicht dazu nur $\alpha(kV + V')$ mit $k \in K;\ V, V' \in K^{n\times 1}$.
Jede lineare Abbildung ist durch die Bilder der Einheitsspalten eindeutig bestimmt.

Definition 1.2.8: (VERALLGEMEINERT) INDUZIERTE LINEARE ABBILDUNG

Die von $A \in K^{m\times n}$ induzierte lineare Abbildung ist

$$\tilde{A} : K^{n\times 1} \to K^{m\times 1}, \quad \xi \mapsto A\xi$$

(Sonderfall des **Matrixproduktes**).

Bemerkung 1.2.10:

Aus Definition 1.2.8 folgt:

$$\tilde{A}(e_j) = Ae_j = A_{-,j}$$

wobei $A_{-,j}$ die j-te Spalte der Matrix A ist.

Bemerkung 1.2.11:

$\tilde{A}(\xi) = A\xi$ ist Linearkombination der Spalten von A mit den Koeffizienten ξ_j mit $j \in \underline{n}$.
$\xrightarrow[1.2.12]{}$ GLS I ist lösbar $\Leftrightarrow$ b aus Spalten von A linearkombinierbar.

Satz 1.2.15:

Zu jeder linearen Abbildung $\alpha : K^{n\times 1} \to K^{m\times 1}$ gibt es genau eine Matrix $A \in K^{m\times n}$ mit $\alpha = \tilde{A}$.

© study.woalk.de

Satz 1.3.1: Komposition linearer Abbildungen

Mit $A \in K^{m\times n}, B \in K^{n\times p}$ ist $\tilde{A} \circ \tilde{B} = \widetilde{AB}$ mit $AB \in K^{m\times p}$.

$\xrightarrow[1.3.4]{}$ Matrixmultiplikation ist assoziativ.

Bemerkung 1.3.6: Lineare Inverse

Das Inverse $(\tilde{A})^{-1}$ einer bijektiven linearen Abbildung $\tilde{A}$ ist wieder linear.
Beweis: *Anwenden der bijektiven linearen Abbildung $\tilde{A}$ auf beiden Seiten der Linearitätsgleichung.*

Übung 2.5:

Aus $A, B \in K^{n\times n}$ invertierbar folgt, dass AB invertierbar mit $(AB)^{-1} = B^{-1}A^{-1}$.

1.4 Gauß- bzw. „Fangcheng"-Algorithmus

Definition 1.4.1: Stufenindex

Sei $M \in K^{m\times n}$. Für $i \in \underline{m}$ ist der i-te Stufenindex

$$\mathrm{St}_i(M) := \begin{cases} \min\{j \in \underline{n} \mid M_{i,j} \neq 0\} & \text{falls } M_{i,-} \text{ keine Nullzeile} \\ n+i & \text{falls } M_{i,-} \text{ Nullzeile} \end{cases}$$

M ist in **Stufenform**, falls die Folge $(\mathrm{St}_i(M))_{i\in\underline{m}}$ streng monoton fallend ist.
Falls zusätzlich für jeden Stufenindex k gilt, dass $M_{-,k} = e_k$, so ist M in **strikter Stufenform**.

Bemerkung 1.4.3:

Für jede injektive Selbstabbildung $g : M \to M$ gilt: $f^{-1}(\{m\}) = (g \circ f)^{-1}(g(\{m\}))$.

Definition 1.4.5/6: Elementare Umformungsmatrizen

Sei $m \in \mathbb{N}$ und e_i die Einheitsspalten, f_j die Einheitszeilen. Sei $M \in K^{m\times n}$.

- Für $1 \leq i, j \leq m$ mit $i \neq j$ und $a \in K$ sei $\mathrm{Add}_m(i,j;a) := I_m + ae_if_j$
  $\Rightarrow \mathrm{Add}_m(i,j;a) \cdot M$ unterscheidet sich nur in der i-ten Zeile von M mit $M_{i,-} + a \cdot M_{j,-}$
  $(\mathrm{Add}_m(i,j;a))^{-1} = \mathrm{Add}_m(i,j;-a)$
- Für $1 \leq i \leq m$ und $a \in K \setminus \{0_K\}$ sei $\mathrm{Mul}_m(i;a) := I_m + (a-1)e_if_i$
  $\Rightarrow \mathrm{Mul}_m(i;a) \cdot M$: Multiplikation der i-ten Zeile von M mit a.
  $(\mathrm{Mul}_m(i;a))^{-1} = \mathrm{Mul}_m(i;a^{-1})$
- Für $1 \leq i < j \leq m$ sei
  $$\mathrm{Ver}_m(i,j) : \underline{m} \times \underline{m} \to K, \quad (p,q) \mapsto \begin{cases} 1 & \text{falls } p = q \notin \{i,j\} \\ 1 & \text{falls } (p,q) \in \{(i,j),(j,i)\} \\ 0 & \text{sonst} \end{cases}$$
  $\Rightarrow \mathrm{Ver}_m(i,j) \cdot M$: Vertauschen der i-ten und j-ten Zeile von M.
  $(\mathrm{Ver}_m(i,j))^{-1} = \mathrm{Ver}_m(i,j)$ (selbstinvers)

© study.woalk.de

Algorithmus 1.4.7: (VERALLGEMEINERT) GAUSS-ALGORITHMUS

GEGEBEN: $M \in K^{m \times n}$
OUTPUT: $M' \in K^{m \times n}$ in (strikter) Stufenform, hervorgegangen durch Linksmultiplikation mit elementaren Umformungsmatrizen aus M.
ALGORITHMUS:

1. Überführe M in Stufenform:
   (a) Finde den kleinsten Spaltenindex j mit $M_{-,j} \neq 0$.
   (b) Finde den kleinsten Zeilenindex i mit $M_{i,-} \neq 0$.
   (c) Falls $i \neq 1$, vertausche die erste und die i-te Zeile.
   (d) Falls $M_{i,j} \neq 1$, ersetze $M \rightsquigarrow \mathrm{Mul}_m\left(1, M_{i,j}^{-1}\right) M$, sodass man mit $M_{1,j} = 1$ weiter arbeitet (normiert).
   (e) Räume die j-te Spalte aus, durch Subtraktion des $M_{i,j}$-Vielfachen der ersten Zeile von der i-ten Zeile, d.h. ersetze $M \rightsquigarrow \mathrm{Add}_m\left(i, 1; -M_{i,j}\right) M$ für $i \in \underline{n} \setminus \{1\}$.
   (f) Wiederhole (1e) mit der Teilmatrix von M, die durch Ignorieren der ersten Zeile und der ersten j Spalten hervorgeht.

   Am Ende hat man eine Matrix in Stufenform.
2. Überführe M in strikte Stufenform, analog (1e).

Algorithmus 1.4.10: GAUSS-ALGORITHMUS ZUM LÖSEN

GEGEBEN: $M = (A \mid b) \in K^{m \times (n+1)}$ erweiterte Matrix eines LGLS $Ax = b$.
GESUCHT: Lösungen des zugehörigen LGLS.
ALGORITHMUS:

1. Wende den Gauß-Algorithmus auf M an, und erhalte eine strikte Stufenform mit derselben Lösungsmenge (wegen 1.4.3).
   Diese ist genau dann leer, wenn $n + n$ ein Stufenindex ist ($0 = 1$).
2. Streiche alle Nullzeilen von M (keine Information) und füge für jeden Nichtstufenindex i_l mit $l \in \underline{d}$ (d Anzahl) der linken Seite eine neue Zeile $\left((I_n)_{i,-} \mid p_l\right)$ zu der erweiterten Matrix hinzu, wobei die p_l paarweise verschiedene Parameter sind. Bringe die resultierende Matrix durch Linksmultiplikation mit Add_m, Ver_m wieder auf strikte Stufenform. Diese ist gegeben durch $(I_n \mid L)$, wobei L eine Spalte ist, die die Lösung abhängig von den Parametern p_l angibt.

Beispiel 1.4.11: (VERALLGEMEINERT) BESTIMMUNG DES BILDES EINER LINEAREN ABBILDUNG

Sei $\tilde{A}$ eine lineare Abbildung mit $A \in K^{m \times n}$.
Löse die erweiterte Matrix $(A \mid x)$ mit $x = (x_1 \quad \cdots \quad x_m)^{\mathrm{tr}}$, bis sich eine Nullzeile ergibt.
Dann ist $x \in \mathrm{Bild}(\tilde{A}) \Leftrightarrow$ Gleichung der rechten Seite in der resultierenden Zeile erfüllt ist.

Definition 1.4.13: TRANSPONIERTE

Ist $A : \underline{m} \times \underline{n} \to K, \quad (i,j) \mapsto A_{i,j}$ eine Matrix, so heißt $A^{\mathrm{tr}} : \underline{n} \times \underline{m} \to K, \quad (i,j) \mapsto A_{j,i}$ die **transponierte Matrix** von A.

Lemma 1.4.14:

Sind $A \in K^{m \times n}, B \in K^{n \times p}$, so ist $(AB)^{\mathrm{tr}} = B^{\mathrm{tr}} A^{\mathrm{tr}} \in K^{p \times m}$.
Ist $\tilde{A}$ surjektiv mit Rechtsinverse $\tilde{B}$, so ist $\widetilde{A^{\mathrm{tr}}}$ injektiv mit Linksinverse $\widetilde{B^{\mathrm{tr}}}$, und umgekehrt.

Man findet Rechtsinverse von $A \in K^{m \times n}$ leicht durch Anwenden des Gauß-Algorithmus auf $(A \mid I_n)$.

© study.woalk.de

Übung 3.2:

Sei $A \in K^{m\times n},\ B \in K^{n\times p},\ C := AB \in K^{m\times p}$.

(i) $C_{ij} = A_{i,-}B_{-,j}$

(ii) $C_{-,j} = AB_{-,j}$

(iii) $C_{i,-} = A_{i,-}B$

(iv) $C = A_{-,1}B_{1,-} + A_{-,2}B_{2,-} + \cdots + A_{-,n}B_{n,-}$

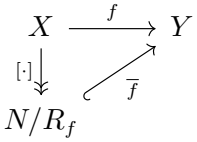
Übung 3.4:

Sei $f : X \to Y$ eine Abbildung. Eine ÄR $R_f \subseteq X \times X$ der Form

$$xR_fx' :\Leftrightarrow f(x) = f(x')$$

heißt **Bildgleichheitsrelation** auf X. Ihre Äquivalenzklassen sind die nicht-leeren Fasern von f.

(Indirekter) **Homomorphiesatz für Mengen**:



kommutiert.

Übung 4.3:

Ist $f : K^{n\times 1} \to K^{m\times 1}$ eine bijektive lineare Abbildung, ist $m = n$.

Übung 4.4:

Sei $A \in K^{m\times n}$ und $\tilde{A}$ surjektiv. A ist bijektiv $\Leftrightarrow$ Rechtsinverse eindeutig. Diese ist dann gleichzeitig Linksinverse und Inverse von A, und damit auch $n = m$.

Übung 5.2:

Sei $A \in K^{n\times n}$. Gibt es eine Matrix $B \in K^{n\times n}$ mit $AB = I_n$, so ist auch $BA = I_n$.

2 Zahlen, Vektoren, Polynome

Definition 2.1.1: Gruppe

Sei G eine *nicht-leere* Menge, $\cdot : G \times G \to G$ eine Verknüpfung auf G. $(G, \cdot)$ heißt **Gruppe**, falls:

(G1) (**Assoziativgesetz**) $\forall x, y, z \in G : x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(G2) (**Neutrales Element**/Einselement) $\exists 1 \in G : \forall g \in G : 1 \cdot g = g \cdot 1 = g$
Dieses Element ist dann eindeutig (Übung 4.2.i).

(G3) (**Inverse Elemente**) $\forall g \in G : \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = 1$
Diese Elemente sind jeweils eindeutig (Übung 4.2.ii).

Falls zusätzlich **kommutativ**, heißt $(G, \cdot)$ **Abelsche Gruppe** und man benutzt auch $+$ als Verknüpftung, mit 0 als Bezeichnung für das Neutralelement und $-g$ als die des Inverses.

Für $a, b \in G$ ist $(ab)^{-1} = b^{-1}a^{-1}$.

Es gilt: Das kartestische Produkt von Gruppen G, H ist wieder eine Gruppe $(G \times H, \cdot)$ mit der komponentenweisen Operation $\cdot$.

© study.woalk.de

Bemerkung 2.1.2: Halbgruppen

- $(G, \cdot)$ heißt **Halbgruppe**, falls (G1) erfüllt ist.
- $(G, \cdot)$ heißt **Monoid** (Halbgruppe mit Eins), falls (G1), (G3) erfüllt sind.

Beispiel 2.1.3.8: (verallgemeinert) Generelle Lineare Gruppe

$\mathrm{GL}_n(K)$, die Menge der invertierbaren Matrizen in $K^{n\times n}$, ist Gruppe mit I_n als Einselement.

Definition 2.1.4: Körper

Sei K eine nicht-leere Menge mit zwei Verknüpfungen $+$ und $\cdot$. Das Tripel $K := (K, +, \cdot)$ heißt **Körper** (*field*), falls gilt:

(K1) $(K, +)$ ist Abelsche Gruppe, das Neutralelement 0 (**Nullelement**).

(K2) $(K, \cdot)$ ist kommutatives Monoid, das Neutralelement 1 (**Einselement**), und es sei $1 \neq 0$.

(K3) $(K^*, \cdot)$ mit $K^* := K \setminus \{0\}$ ist Abelsche Gruppe mit Neutralelement 1.

(K4) **Distributivgesetze**: $a \cdot (b + c) = a \cdot b + a \cdot c$

Gilt nur (K1), (K2) und (K4), heißt $R := (G, +, \cdot)$ **kommutativer Ring mit Eins**.
Ist Multiplikation nicht kommutativ, heißt R nur **Ring mit Eins**.
Gilt in einem Ring R, dass $1 = 0$, dann ist $R = \{0\}$ der einelementige Ring.

Bemerkung 2.1.7.2: Ringhomomorphismus

Sei R ein Ring mit Eins. Für $i \in \mathbb{Z}_{\geq 0}$ und $a \in R$ setze $ia := a + ... + a = \sum_{k=1}^{i} a$.
Es gilt: $\mathbb{Z} \ni 0 \cdot a = 0 \in R$ und $ia = -((-i)\,a)$.
Dadurch definiert ist der **Ringhomomorphismus**

$$\bar{\cdot} : \mathbb{Z} \to R, \quad i \mapsto i1 \text{ mit } 1 \in R$$

Definition 2.1.9: *nomialkoeffizient

Sei $n \in \mathbb{Z}_{\geq 0}$.

- Für $i \in \mathbb{Z}_{\geq 0}$ heißt $\binom{n}{i} := |\mathrm{Pot}_i(\underline{n})|$ **Binomialkoeffizient**, wobei $\mathrm{Pot}_i(M)$ die Menge aller i-elementigen Teilmengen der Menge M.
- Für $i_1, i_2, \ldots, i_k \in \mathbb{Z}_{\geq 0}$ mit $i_1 + i_2 + \cdots + i_k = n$ heißt

$$\binom{n}{i_1, i_2, \ldots, i_k} := \left|\left\{\varphi \in \underline{k}^{\underline{n}} \mid \left|\varphi^{-1}(\{j\})\right| = i_j \; \forall j \in \underline{k}\right\}\right|$$

Multinomialkoeffizient.

Bemerkung 2.1.10: Multinomialsatz

Sei R ein *kommutativer* Ring und $a_1, \ldots, a_n \in R$. Für $m \in \mathbb{N}$ gilt:

$$(a_1 + \cdots + a_n)^m = \sum_{\forall i_1 + \cdots + i_n = m} \binom{m}{i_1, \ldots, i_n} a_1^{i_1} \cdots a_n^{i_n}$$

© study.woalk.de

Satz 2.1.11: Komplexe Zahlen als Matrixkörper

$$\mathbb{C} := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subset \mathbb{R}^{2\times 2}$$

zusammen mit Matrixaddition und Matrixmultiplikation ist der **Körper der komplexen Zahlen**. Man schreibt abkürzend $a + b\mathrm{i}$. Es gilt:

- $(a + b\mathrm{i})\,(c + d\mathrm{i}) = (ac - bd) + \mathrm{i}\,(ab + bc)$
- $(a + b\mathrm{i})^{-1} = \frac{a - \mathrm{i}b}{a^2 + b^2}$

Bemerkung 2.1.12: Teilbarkeit und Rest

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$.

- $|a| := \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$ der **(Absolut-)Betrag**.
- Dann gibt es *eindeutige* Zahlen $q, r \in \mathbb{Z}$ mit $a = q \cdot b + r$ und $0 \leq r < b$.
  r heißt der kleinste, nicht-negative **Rest** von $a \mod b$.
- Falls $r = 0$, sagt man $b \mid a$ sprich „b teilt a“.

Satz 2.1.13: Restklassen

1. Sei $p \in \mathbb{Z}$ fest vorgegeben und $\sim_p := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid p \mid (a - b)\} \subset \mathbb{Z} \times \mathbb{Z}$.
   Dann ist $\sim_p$ eine ÄR auf $\mathbb{Z}$, man schreibt auch $a \equiv b \mod p$.
   Die Äquivalenzklasse $[a] := \{b \in \mathbb{Z} \mid b \sim_p a\}$ für $a \in \mathbb{Z}$ heißt **Restklasse** von $\mathbb{Z}$ modulo p und partitioniert $\mathbb{Z}$ in $|p|$ verschiedene Klassen.
2. Addition und Multiplikation in $\mathbb{Z}$ ist verträglich mit $\sim_p$, d.h. $\mathbb{Z}/\sim_p$ ist ein kommutativer Ring mit Eins und man schreibt $(\mathbb{Z}/\sim_p, +, \cdot) =: \mathbb{Z}/p\mathbb{Z}$ und $[a]_{\sim_p} =: a + p\mathbb{Z}$ oder $\overline{a}$.
3. Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper und heißt $\mathbb{F}_p$ (aber nur für p prim!).

Definition 2.1.14: ggT

Für $a, b \in \mathbb{Z}$ ist der **größte gemeinsame Teiler** von a und b, geschrieben $t := \mathrm{ggT}\,(a, b)$ mit $t \mid a \ \wedge\ t \mid b$ und $d \mid a \ \wedge\ d \mid b \Rightarrow d \mid t \quad \forall d \in \mathbb{Z}$.
Es gilt $\mathrm{ggT}\,(a, 0) = a$. Der ggT ist bis auf Vorzeichen eindeutig.

Algorithmus 2.1.15: Euklidischer Algorithmus für ggT

Gegeben: $a, b \in \mathbb{Z} \setminus \{0\}$
Gesucht: $\mathrm{ggT}\,(a, b)$
Algorithmus:

1. Setze $a_1 := a,\ a_2 := b$.
2. Für $n \geq 3$, setze $a_n := a_{n-2} \mod a_{n-1}$, falls $a_{n-1} \neq 0$.

Nach endlich vielen Schritten ist dann, wenn $a_{k+1} = 0$, der $\mathrm{ggT}\,(a, b) = a_k$.

© study.woalk.de

Bemerkung 2.1.17: (verallgemeinert) Euklidischer Algorithmus als Matrixoperation

Sei R ein Ring und

$$\varepsilon : R^{2\times 1} \to R^{2\times 1}, \quad \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{cases} \begin{pmatrix} b \\ a \mod b \end{pmatrix} & \text{falls } b \neq 0 \\ \begin{pmatrix} a \\ 0 \end{pmatrix} & \text{falls } b = 0 \end{cases}$$

1. **Euklidischer Algorithmus:** Iteriere die Anwendung von ε, so lange der zweite Fall $b = 0$ *nicht* eintritt; d.h. bis zu $k \in \mathbb{N}$ mit $\varepsilon^{k-1}\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = \begin{pmatrix} t \\ 0 \end{pmatrix}$, dann ist $t = \mathrm{ggT}\,(a, b)$.
2. Es gilt im Fall $b \neq 0$: $\varepsilon\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ r \end{pmatrix}$ wobei $a = qb + r$ und $0 \leq r < |b|$.

Algorithmus 2.1.18: Euklidischer Algorithmus mit Bézout-Identität

Gegeben: $a, b \in \mathbb{Z} \setminus \{0\}$
Gesucht: $t = \mathrm{ggT}\,(a, b)$ und $\alpha, \beta \in \mathbb{Z}$ mit $\alpha a + \beta b = t$
Algorithmus:

1. Wie oben $a_1 = a, a_2 = b$.
2. Setze $a_n = q_n a_{n+1} + a_{n+2}$ mit $q_n \in \mathbb{Z}$ für $n \geq 1$.
   Definiere $A_1 = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$ und $A_n = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} A_{n-1}$ für $n \geq 2$.
   Dann liefert die erste Zeile von A_{k-1} das gewünschte (α, β) und es gilt $A_{k-1}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} t \\ 0 \end{pmatrix}$
   Man beachte, dass man wenige Zwischenergebnisse speichern muss und die erste Zeile von A_{k-1} bereits die zweite Zeile von A_{k-2} ist.

Beispiel 2.1.19: Invertieren in Restklassenkörpern

$(25 + 31\mathbb{Z})^{-1}$ in $\mathbb{F}_{31}$. Bestimme dazu die Bézout-Identität vom $\mathrm{ggT}\,(31, 25) = 1$:

$$\begin{aligned} 31 &= 1 \cdot 25 + 6 \\ 25 &= 4 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0 \end{aligned}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}\left(\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ -4 & 5 \end{pmatrix} = \begin{pmatrix} -4 & 5 \\ * & * \end{pmatrix}$$

$\Rightarrow \alpha = -4,\ \beta = 5$ (und zur Erinnerung, $a = 31, b = 25$),
also $-4 \cdot 31 + 5 \cdot 25 = 1$, insbesondere $5 \cdot 25 \equiv 1 \mod 31$ und somit $(25 + 31\mathbb{Z})^{-1} = 5 + 31\mathbb{Z}$.

Definition 2.1.20: Einheitengruppe

Sei R ein Ring mit Eins. Ein Element $u \in R$ heißt **Einheit** (bzw. *multiplikativ invertierbar*), falls $\exists v \in R : uv = vu = 1$.
Die Menge der Einheiten $R^\times := \{u \in R \mid u \text{ Einheit}\}$ wird **Einheitengruppe** genannt.

Man schreibt manchmal auch $R^* := R^\times$ stattdessen, besonders im Fall von Körpern, wo $K^* = K \setminus \{0\}$.

© study.woalk.de

Definition 2.1.22: Nullteiler

Sei R ein kommutativer Ring mit Eins. $r \in R \setminus \{0\}$ heißt **Nullteiler**, falls $\exists s \in R \setminus \{0\} : rs = 0$.

Jeder Körper ist nullteilerfrei (konstruktiv beweisbar).

Übung 5.3.iii:

Falls R ein kommutativer *endlicher* Ring ist, so ist jedes Element $r \in R \setminus \{0\}$ entweder eine Einheit oder ein Nullteiler.

2.2 Gruppenoperationen

Definition 2.2.1: Gruppenoperation

Sei G eine Gruppe und M eine beliebite Menge, $m \in M$ ein beliebiges Element.

1. G **operiert** auf M (von links), falls eine Abbildung $\omega : G \times M \to M$ (**Operation**) existiert mit
   (Op1) $1 \cdot m = \omega(1, m) = m$ für $1 \in G$
   (Op2) $g(hm) = (gh)m \quad \forall g, h \in G$
2. G operiere auf M. Dann heißt $Gm := \{gm \mid g \in G\} \subseteq M$ die **Bahn** von m unter G.

Sei im folgenden Rest des Kapitels G eine Gruppe, die auf der Menge M operiert.

Satz 2.2.4:

Definiere die ÄR $\sim_G$ auf M durch $m \sim_G m' :\Leftrightarrow \exists g \in G : gm = m'$
Dann sind ihre Äquivalenzklassen die Bahnen von M unter G: $M/\sim_G = \{Gm \mid m \in M\}$

Definition 2.2.5: Invarianten

Eine Abbildung $f : M \to N$ in eine beliebige Menge N heißt eine **Invariante der Operation**, falls f konstant auf den Bahnen ist, sprich falls $f(gm) = f(m) \ \forall g \in G \forall m \in M$. Anders ausgedrückt: $\sim_f \supseteq \sim_G$
Die Invariante heißt **trennend**, falls verschiedenen Bahnen verschiedene Werte von f zugeordnet werden, sprich falls $f(m) = f(m') \Rightarrow Gm = Gm'$. Anders ausgedrückt: $\sim_f = \sim_G$

Übung 6.1:

$\mathrm{GL}_2(\mathbb{Z})$ operiert auf $\mathbb{Z}^{2\times 1}$ und $\binom{a}{b} \mapsto |\mathrm{ggT}(a, b)|$ ist trennende Invariante.

Beispiel 2.2.8: Bildgleichheits-Operation

Sei $A \in K^{m\times n}$. $\mathrm{Kern}(\tilde{A})$ operiert durch Addition auf $K^{n\times 1}$, wobei $\tilde{A}$ eine trennende Invariante ist. Die Bildgleichheitsäquivalenzklassen sind also genau die Bahnen, sprich $\sim_{\tilde{A}} = \sim_{\mathrm{Kern}\,\tilde{A}}$.

© study.woalk.de

2.3 Vektorräume

Definition 2.3.2: Vektorraum

Eine Abelsche Gruppe $(\mathcal{V}, +)$ zusammen mit einer äußeren Verknüpfung

$$K \times \mathcal{V} \to \mathcal{V}, \quad (a, X) \mapsto aX$$

heißt **Vektorraum** über K oder (kürzer) K-Vektorraum, falls gilt:

(V1) $a(X+Y) = aX + aY \quad \forall a \in K,\ X, Y \in \mathcal{V}$

(V2) $(a+b)X = aX + bY \quad \forall a, b \in K,\ X \in \mathcal{V}$

(V3) $(ab)X = a(bX) \quad \forall a, b \in K,\ X \in \mathcal{V}$

(V4) $1X = X \quad \forall X \in \mathcal{V}$

Die Elemente von $\mathcal{V}$ heißen **Vektoren**.

$0X = 0 \in \mathcal{V}$, $(-1)X = -X \in \mathcal{V}$.
Seien im folgenden Rest des Kapitels $\mathcal{V}$ und $\mathcal{W}$ beliebige K-Vektorräume („VRe“).

Beispiel 2.3.4: Raum der Abbildungen

Sei M eine nicht-leere Menge.
Dann ist K^M ein K-VR mit werteweiser Addition und werteweiser äußeren Multiplikation.

Damit kann man ableiten, dass K selbst, K^n, $K^{n\times 1}$, $K^{m\times n}$, K^K, $K^{\mathbb{N}}$ allesamt K-VRe sind.

Definition 2.3.5: VR-Homomorphismus

$\varphi : \mathcal{V} \to \mathcal{W}$ heißt K-linear oder K**-Homomorphismus**, falls $\forall X, Y \in \mathcal{V},\ a \in K : \varphi(aX + Y) = a\varphi(X) + \varphi(Y)$.

- Ist φ injektiv: **Monomorphismus**
- Ist φ surjektiv: **Epimorphismus**
- Ist φ bijektiv: **Isomorphismus**
- Ist $\mathcal{V} = \mathcal{W}$: **Endomorphismus** (siehe **??**)
- Ist φ Endomorphismus und bijektiv: **Automorphismus**

VRe heißen **isomorph**, fals ein Isomorphismus zwischen diesen existiert, man schreibt $\mathcal{V} \cong \mathcal{W}$.

Ist $\varphi : \mathcal{V} \to \mathcal{W}$ Iso., ist $\varphi^{-1} : \mathcal{W} \to \mathcal{V}$ auch Iso.

Beispiel 2.3.6: Einige Morphismen

- $\cdot^{\mathrm{tr}} : K^{m\times n} \to Kn \times m$ ist Isomorphismus.
- Jede Abbildung $f : M \to N$ liefert $f^* : K^N \to K^M, \quad g \mapsto g \circ f$. f^* ist genau dann Iso., wenn f bijektiv. Dann ist $(f^*)^{-1} = (f^{-1})^*$
- Für $V \in \mathcal{V}^n$ ist $\lambda_V : K^n \to \mathcal{V}, \quad a \mapsto a_1V_1 + \cdots + a_nV_n$ der **Linearkombinationshomomorphismus**.

Bemerkung 2.3.7: Endomorphismenring

$\mathrm{End}(\mathcal{V}) := \{\alpha : \mathcal{V} \to \mathcal{V} \mid \alpha \text{ linear}\}$ ist ein Ring mit werteweiser Addition und Komposition $\circ$ als Multiplikation, genannt der **Endomorphismenring** des VRs $\mathcal{V}$.
Seine Einheitengruppe ist $\mathrm{End}(\mathcal{V})^\times =: \mathrm{GL}(\mathcal{V}) := \{\alpha \in \mathrm{End}(\mathcal{V}) \mid \alpha \text{ bijektiv}\}$, genannt die **generelle Lineare Gruppe** über $\mathcal{V}$.

© study.woalk.de

Definition 2.3.8: Teilräume

Eine Teilmenge $\mathcal{T} \subseteq \mathcal{V}$ heißt **Teilvektorraum** oder Untervektorraum von $\mathcal{V}$, falls
(T1) $\mathcal{T} \neq \emptyset$
(T2) $\forall X, Y \in \mathcal{T},\ a \in K : aX + Y \in \mathcal{T}$
Man schreibt dann $\mathcal{T} \leq \mathcal{V}$.

Übung 6.2:

Ist $\mathcal{T} \leq \mathcal{V}$, so ist $\mathcal{T}$ auch ein K-VR.

Übung 6.4:

- $\mathrm{Hom}(\mathcal{V}, \mathcal{W}) := \{f \in \mathcal{W}^{\mathcal{V}} \mid f \text{ ist linear}\}$
- $\mathrm{Hom}(\mathcal{V}, \mathcal{W})$ ist auch abgeschlossen unter werteweiser Addition und Komposition $\circ$.
- $\mathrm{Hom}(K^{n\times 1}, K^{m\times 1}) \cong K^{m\times n}$.
- $\left|\mathrm{Hom}\left(\mathbb{F}_p^{n\times 1}, \mathbb{F}_p^{m\times 1}\right)\right| = \left|\mathbb{F}_p^{m\times n}\right| = p^{m\cdot n}$

Satz 2.3.10:

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ Homomorphismus. Es gilt:
1. $\mathrm{Kern}(\varphi) := \varphi^{-1}(\{0\}) \leq \mathcal{V}$
2. $\mathrm{Bild}(\varphi) := \{\varphi(V) \mid V \in \mathcal{V}\} \leq \mathcal{W}$
3. Ist $\mathcal{S} \leq \mathcal{W}$, so ist $\varphi^{-1}(\mathcal{S}) := \{X \in \mathcal{V} \mid \varphi(X) \in \mathcal{S}\} \leq \mathcal{V}$.
4. Ist $\mathcal{T} \leq \mathcal{V}$, so ist $\varphi(\mathcal{T}) \leq \mathcal{W}$.

Definition 2.3.11: Direkte Summe

1. Auf dem kartesischen Produkt $\mathcal{V} \times \mathcal{W}$ definiere
$$+ : (\mathcal{V} \times \mathcal{W}) \times (\mathcal{V} \times \mathcal{W}) \to \mathcal{V} \times \mathcal{W}, \quad ((V, W), (V', W')) \mapsto (V + V', W + W')$$
als komponentenweise Addition und
$$\cdot : K \to (\mathcal{V} \times \mathcal{W}) \to \mathcal{V} \times \mathcal{W}, \quad (a, (V, W)) \mapsto (aV, aW)$$
als komponentenweise Multiplikation mit Körperelement (Skalarmultiplikation).
$\Rightarrow (\mathcal{V} \times \mathcal{W}, +, \cdot) =: \mathcal{V} \oplus_{\mathrm{a}} \mathcal{W}$ wieder K-VR, die **äußere direkte Summe**.
2. Seiem $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$. Falls sich jedes $V \in \mathcal{V}$ *eindeutig* als $V = T_1 + T_2$ mit $T_i \in \mathcal{T}_i$ schreiben lässt, so heißt $\mathcal{V} = \mathcal{T}_1 \oplus_{\mathrm{i}} \mathcal{T}_2$ die **innere direkte Summe**.

Beispiel 2.3.13: Projektionen

Sei $\mathcal{V} = \mathcal{T}_1 \oplus_{\mathrm{i}} \mathcal{T}_2$.
1. $\pi_i : \mathcal{T}_1 \oplus \mathcal{T}_2 \to \mathcal{T}_i, \quad T_1 + T_2 \mapsto T_i$ für $i \in \underline{2}$ ist eine surjektive lineare Abbildung (Epi.), welche man **Projektion** auf $\mathcal{T}_i$ bezüglich der Zerlegung $\mathcal{V} = \mathcal{T}_1 \oplus \mathcal{T}_2$ nennt.
Es gilt: $\mathrm{Kern}\,\pi_1 = \mathcal{T}_2$ und $\mathrm{Kern}\,\pi_2 = \mathcal{T}_1$
2. $\iota_i : T_i \to \mathcal{V}, \quad T_i \mapsto T_i$ ist eine injektive lineare Abbildung.
Es gilt: $\mathrm{Bild}\,\iota_i = \mathcal{T}_i$ für $i \in \underline{2}$

Man beachte: $\pi_2 \circ \iota_1 : \mathcal{T}_1 \to \mathcal{T}_2$ und $\iota_2 \circ \pi_1 : \mathcal{T}_2 \to \mathcal{T}_1$ sind *Nullabbildungen*.

© study.woalk.de

Übung 7.1:

(i) $\mathcal{T}_1 \oplus_\mathrm{a} \mathcal{T}_2 \cong \mathcal{T}_1 \oplus_\mathrm{i} \mathcal{T}_2$

(ii) $\mathcal{V} = \mathrm{Bild}(\iota_1) \oplus_\mathrm{i} \mathrm{Bild}(\iota_2)$ und $\mathrm{Bild}(\iota_i) \cong \mathcal{T}_i$

wenn $\iota_i : \mathcal{T}_i \to \mathcal{T}_1 \oplus_\mathrm{a} \mathcal{T}_2,\ t \mapsto \begin{cases}(t,0) & \text{für } i=1\\(0,t) & \text{für } i=2\end{cases}$ die **Einbettung** von $\mathcal{T}_i$ in $\mathcal{T}_1 \oplus_\mathrm{a} \mathcal{T}_2$.

(iii) $(\mathcal{T}_1 \oplus \mathcal{T}_2)/\mathcal{T}_2 \cong \mathcal{T}_1$

Satz 2.3.14: KERNOPERATION

(Verallgemeinerung von Beispiel 2.2.8)
Sei $\varphi : \mathcal{V} \to \mathcal{W}$ Homomorphismus. Die nicht-leeren Fasern von φ sind gleichzeitig die Bahnen der Operation von $\mathrm{Kern}\,\varphi$ auf $\mathcal{V}$ per Addition

$$\mathrm{Kern}(\varphi) \to \mathcal{V}, \quad (X, Y) \mapsto X + V$$

Definition 2.3.16: KONGRUENZ

Eine ÄR $\sim$ auf $\mathcal{V}$ heißt **verträglich** mit der VR-Struktur oder einfach **linear** oder **Kongruenz**, falls $\forall X, X', Y, Y' \in \mathcal{V},\ a \in K : X \sim X' \wedge Y \sim Y' \Rightarrow aX + Y \sim aX' + Y'$

Übung 7.2:

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ Homomorphismus.

(i) φ injektiv $\Leftrightarrow \mathrm{Kern}\,\varphi = \{0\}$

(ii) $\sim_\varphi$, die Bildgleichheit, ist eine Kongruenz.

(iii) Ist $\mathcal{U} \leq \mathcal{V}$ ein TR von $\mathcal{V}$, so ist $\sim^\mathcal{U}$ auf $\mathcal{V}$ mit $X \sim^\mathcal{U} Y :\Leftrightarrow X - Y \in \mathcal{U}$ eine Kongruenz.

Lemma 2.3.18: KONGRUENZKLASSEN

Ist $\sim$ eine Kongruenz auf $\mathcal{V}$, so gilt:

1. Die Kongruenzklasse $[0]$ des Nullelements ist ein TR $[0] := \mathcal{U} \leq \mathcal{V}$
2. $\sim = \sim^\mathcal{U}$
3. $\sim^\mathcal{U} = \sim_\mathcal{U}$ ($\leftarrow$ die Gruppenoperation) d.h. die Kongruenz nach $\mathcal{U}$ stimmt mit der ÄR $\sim_\mathcal{U}$ überein, die durch die Operation von $\mathcal{U}$ auf $\mathcal{V}$ durch Addition induziert wird.
4. Die Kongruenzklasse $[X]$ mit $X \in \mathcal{V}$ ist gegeben durch

$$\mathcal{U} + X = \{U + X \mid U \in \mathcal{U}\} = \{X + U \mid U \in \mathcal{U}\} = X + \mathcal{U}$$

also durch die Bahn von X unter der obigen Operation von $\mathcal{U}$ auf $\mathcal{V}$!

$\xrightarrow[2.3.19]{}$ Ist $\varphi : \mathcal{V} \to \mathcal{W}$ linear, ist $\sim_\varphi = \sim_{\mathrm{Kern}\,\varphi} = \sim^{\mathrm{Kern}\,\varphi}$

© study.woalk.de

Satz 2.3.20: Faktorräume

Sei $\mathcal{U} \leq \mathcal{V}$ und $\sim^{\mathcal{U}}$ die zugehörige Kongruenz.
Die Menge $\mathcal{V}/\sim^{\mathcal{U}} = \mathcal{V}/\sim_{\mathcal{U}}$ der Kongruenzklassen (bzw. der Bahnen von $\mathcal{U}$) wird mit $V/\mathcal{U}$ „$\mathcal{V}$ modulo $\mathcal{U}$“ bezeichnet. Die Elemente von $\mathcal{V}/\mathcal{U}$ heißen (auch) **Restklassen** nach $\mathcal{U}$. Es gilt:

1. $\mathcal{V}/\mathcal{U}$ mit wohldef. Addition $(X+\mathcal{U})+(Y+\mathcal{U}) := (X+Y)+\mathcal{U} \quad \forall X, Y \in \mathcal{V}$ und Multiplikation $a(X+\mathcal{U}) := aX+\mathcal{U} \quad \forall X \in \mathcal{V},\ a \in K$ ist ein K-VR, genannt **Faktorraum**, **Quotientenraum** oder **Restklassenraum**.
2. Die Abbildung $\nu : \mathcal{V} \to \mathcal{V}/\mathcal{U}, \quad X \mapsto X+\mathcal{U}$ ist der **natürliche Epimorphismus** von $\mathcal{V}$ auf $\mathcal{V}/\mathcal{U}$. Es gilt: $\operatorname{Kern}\nu = \mathcal{U}$
   Jeder Teilraum eines Vektorraums ist Kern eines geeigneten Homomorphismus.

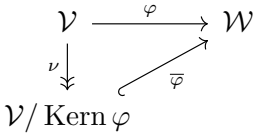
VR	$\mathcal{V}$	$\varphi : \mathcal{V} \to \mathcal{W}$	$\mathcal{T} \leq \mathcal{W}$	$\mathcal{V} \oplus \mathcal{W}$	$\operatorname{Hom}(\mathcal{V}, \mathcal{W})$	$\mathcal{V}/\sim$
Menge	M	$f : M \to N$	$S \subseteq M$	$M \times N$ *und* $M \cup N$	N^M	$M/\sim$

Satz 2.3.21: Homomorphiesatz („Lieblingssatz“)

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ ein Homomorphismus.
Dann faktorisiert φ in die Komposition des natürlichen Epimorphismus $\nu = \nu_\varphi : \mathcal{V} \to \mathcal{V}/\operatorname{Kern}\varphi$ und des Monomorphismus

$$\overline{\varphi} : \mathcal{V}/\operatorname{Kern}\varphi \to \mathcal{W}, \quad X + \operatorname{Kern}\varphi \mapsto \varphi(X)$$

also $\varphi = \overline{\varphi} \circ \nu$, d.h. das Diagramm

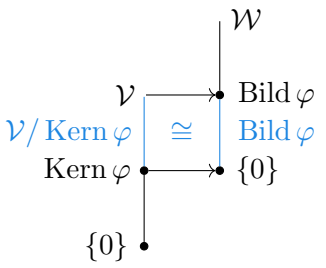


kommutiert.

Folgerung aus Homomorphiesatz:

Der Monomorphismus $\overline{\varphi}$ induziert einen Isomorphismus $\overline{\varphi} : \mathcal{V}/\operatorname{Kern}\varphi \xrightarrow{\sim} \operatorname{Bild}\varphi$. Also:

$$\varphi : \mathcal{V} \to \mathcal{W} \text{ linear} \Rightarrow \mathcal{V}/\operatorname{Kern}\varphi \cong \operatorname{Bild}\varphi$$



„je größer der Kern, desto kleiner das Bild“

Beispiel 2.3.22: Homomorphiesatz im LGls

Sei $A \in K^{m\times n}$ mit $\varphi := \tilde{A}$.
Dann sagt der Homomorphiesatz:

1. Diejenigen $b \in K^{m\times 1}$, für die $\varphi(x) = Ax = b$ lösbar, bilden TR $\operatorname{Bild}\varphi \leq K^{n\times 1}$.
2. $\operatorname{Bild}\varphi \cong K^{n\times 1}/\operatorname{Kern}\varphi$
3. Die Lösungsmenge von $Ax = b$ für ein $b \in \operatorname{Bild}\varphi$ ist eine Restklasse nach $\operatorname{Kern}\varphi$ und wird unter Isomorphismus $\overline{\varphi}$ auf b abgebildet. Insbesondere bildet die Gesamtheit aller nicht-leeren Fasern für variierendes $b \in \operatorname{Bild}\varphi$ einen Vektorraum, den Faktorraum nach $\operatorname{Kern}\varphi$.
4. Je größer der Kern von φ, desto weniger rechte Seiten b gibt es, für die das GLS lösbar ist.

© study.woalk.de

Beispiel 2.3.23: Homomorphiesatz in direkten Summen

(siehe Übung 7.1.iii)
Insbesondere ist $\mathcal{T}_1$ eine **Transversale** von $\pi_1 : \mathcal{T}_1 \oplus \mathcal{T}_2 \twoheadrightarrow \mathcal{T}_1$, d.h. ein Vertretersystem der Restklassen von $\mathcal{T}_1 \oplus \mathcal{T}_2$ nach $\mathcal{T}_2$.

Satz 2.3.24: Faktorisierung von Homomorphismen über Spalten

Sei $A \in K^{m\times n}$. $\tilde{A}$ kann in eine surjektive lineare Abbildung $\tilde{G}$ mit $G \in K^{r\times n}$ mit $r \in \mathbb{Z}_{\geq 0}$ und eine injektive lineare Abbildung $\tilde{B}$ mit $B \in K^{m\times r}$ faktorisiert werden: $\tilde{A} = \tilde{B} \circ \tilde{G}$ oder $A = BG$

$$\begin{array}{ccc} K^{n\times 1} & \xrightarrow{\tilde{A}} & K^{m\times 1} \\ {\scriptstyle\tilde{G}}\downarrow & \nearrow_{\tilde{B}} & \\ K^{r\times 1} & & \end{array}$$

→ **Algorithmus dazu:** Wähle G als die Matrix, die aus der strikten Stufenform ohne Nullzeilen (streichen!) aus A hervorgeht. Die Zeilenzahl von G sei also r. Seien $S(i) := \mathrm{St}_i(G)$ die Stufenindizes von G.
Definiere $B \in K^{m\times r}$ dadurch, dass die j-te Spalte von B gleich der $S(j)$-ten Spalte von A ist ($B_{-,j} = A_{-,S(j)}$).

Beispiel 2.3.25: Faktorisierung von Homomorphismen über Spalten

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \\ 6 & 6 & 6 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 5 & 4 \\ 6 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 & -2 & -3 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

↓

strikte Stufenform von A: 1. Spalte, 2. Spalte haben die Stufen. Nimm also 1. und 2. von A für B.

$\begin{pmatrix} 1 & \cdot & -1 & -2 & -3 \\ \cdot & 1 & 2 & 3 & 4 \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$ → Nullzeilen löschen → G

Hilfreich, da $\mathrm{Kern}\,\tilde{A} = \mathrm{Kern}\,\tilde{G}$ (leichter bestimmbar).

© study.woalk.de

2.4 Polynomringe

Definition 2.4.1: Potenzreihenring

1. Auf dem K-VR $K^{\mathbb{Z}_{\geq 0}}$ definieren wir eine *kommutative* Multiplikation:

$$(a_0, a_1, a_2, a_3, \dots) \cdot (b_0, b_1, b_2, b_3, \dots) = (c_0, c_1, c_2, c_3, \dots)$$

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\ &\vdots \\ c_n &:= a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 \end{aligned}$$

   $\Rightarrow (K^{\mathbb{N}_0}, +, \cdot)$ (wobei $\cdot$ die gerade definierte Multiplikation, $\mathbb{N}_0 := \mathbb{Z}_{\geq 0}$) zusammen mit der K-VR-Struktur von $K^{\mathbb{N}_0}$ wird mit $K[[x]]$ bezeichnet, dem **(formalen) Potenzreihenring** über K in der Unbestimmten $x := (0, 1, 0, 0, \dots)$.

   Statt $(a_0, a_1, a_2, a_3, \dots)$ schreibt man auch $\sum_{i=0}^{\infty} a_i x^i$.

2. Eine Potenzreihe $a = (a_0, a_1, a_2, \dots) \in K[[x]]$ heißt **Polynom**, falls ein $n \in \mathbb{Z}_{\geq 0}$ existiert mit $a_i = 0 \quad \forall i > n$. Für $a \neq 0$ heißt das kleinste derartige n dann der **Grad** von a. Wir setzen für die Nullfolge $\operatorname{Grad}(0) := -\infty$.

   Die Menge aller Polynome ist ein Teilraum von $K[[x]]$ mit in sich abgeschlossener Multiplikation, man nennt dies den **Polynomring** $K[x]$.

Bemerkung 2.4.2: Multiplikation mit Unbestimmten

Es gilt: $x \cdot (a_0, a_1, a_2, \dots) = (0, a_0, a_1, a_2, \dots)$.
Multiplikation mit x ist linear und injektiv.

Übung 8.1:

(i) Für $a \in K[[x]]$ ist $\mu_a : K[[x]] \to K[[x]], \quad b \mapsto ab$ linear.
μ_a ist injektiv $\Leftrightarrow a \neq 0$.
Insbesondere gilt damit das Distributivgesetz in $K[[x]]$.

(ii) Für $a, b \in K[[x]]$ gilt die **Gradformel**: $\operatorname{Grad}(ab) = \operatorname{Grad} a + \operatorname{Grad} b$

Beispiel 2.4.3: Schriftliche Multiplikation ohne Übertrag

In $\mathbb{Q}[x]$ berechnen wir ab mit $a := (1, 2, 0, 1, 0, 0, \dots)$ und $b := (4, 3, 2, 1, 0, 0, \dots)$:

$1 \cdot b$	4	3	2	1	0	0	
$+2x \cdot b$		8	6	4	2	0	0
$+0x^2 \cdot b$			0	0	0	0	0
$+1x^3 \cdot b$				4	3	2	1
$ab =$	4	11	8	9	5	2	1

© study.woalk.de

Bemerkung 2.4.4:

1. $1 := (1, 0, 0, \dots) \in K[x] \subset K[[x]]$ ist das multiplikative Neutralelement.
3. Es gilt $x^i x^j = x^{i+j}$
4. Sei $a \in K[x]$ ein Polynom vom Grad n, dann gilt $a = a_0 + a_1 x + a_2 x^2 + \dots a_n x^n$. Insbesondere liefert dies eine Identifikation von K mit
   $K[x]_{\mathrm{Grad} \leq 0} = \{a \in K[x] \mid \mathrm{Grad}\, a \leq 0\} = \{0\} \cup \{a \in K[x] \mid \mathrm{Grad}\, a = 0\}$
5. $K[x]_{\mathrm{Grad} < n} := \{a \in K[x] \mid \mathrm{Grad}\, a < n\}$ ist ein TR von $K[x]$.

Definition 2.4.5: Algebra über einem Körper

1. Sei R ein Ring mit eins, der gleichzeitig ein K-VR ist. Man nennt R dann eine assoziative K-Algebra mit Eins, oder kürzer **K-Algebra**, falls gilt:
   $$k(ab) = (ka)b = a(kb) \quad \forall k \in K,\ a, b \in R$$
2. Ist S eine weitere K-Algebra mit Eins, so heißt die Abbildung $\varphi : R \to S$ **K-Algebren-Homomorphismus**, falls
   - φ ist K-linear.
   - $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in R$
   - $\varphi(1_R) = 1_S$

Zwei K-Algebren R, S sind **Algebra-isomorph**, falls es K-Algebren-Homomorphismen $f : R \to S,\ g : S \to R$ gibt mit $g \circ f = \mathrm{id}_R$ und $f \circ g = \mathrm{id}_S$.

Satz 2.4.6: Polynom-Algebra

1. $K[x]$ ist eine kommutative K-Algebra.
2. Seien $a, b \in K[x] \setminus \{0\}$ Polynome. Dann existieren eindeutig bestimmte Polynome
   $q, r \in K[x]$ mit $\xrightarrow{\text{Div. mit Rest}} a = qb + r$ mit $\mathrm{Grad}\, r < \mathrm{Grad}\, b$ (**Polynomdivision**).

Folgerung 2.4.9: Polynomrestklassen

Sei $p \in K[x] \setminus \{0\}$ vom Grad n.
Dann gilt: Die Vielfachen p bilden einen TR $pK[x] \leq K[x]$ und $K[x] = K[x]_{\mathrm{Grad}<n} \oplus_{\mathrm{i}} pK[x]$.
Insbesondere hat der Faktorraum $K[x]/pK[x]$ den TR $K[x]_{Grad<n}$ als Vertretersystem der Restklassen = Kongruenzklassen = Bahnen (nach Homomorphiesatz ist $K[x]/pK[x] \cong K[x]_{\mathrm{Grad}<n}$ und Vertreter durch Polynomdivision).
Für die Kongruenz $a \sim^{pK[x]} b$ schreibt man oft $a \equiv b \mod p$.

Analog $\mathbb{Z}$, es gibt auch Analogon zu Primzahlen:
irreduzible Polynome, die nicht als Produkt von *zwei* Polynomen *echt kleineren* Grades geschrieben werden können, d.h. $n := \mathrm{Grad}(p) > 0$ und p hat keine Teiler in $K[x]$ vom Grad g mit $0 < g < n$.
ggT, Euklidischer Algorithmus inklusive der Bézout-Identität existieren analog in $K[x]$.
Es gibt auch analog $\mathbb{Q}$ einen Quotientenkörper $K(x)$, den **Körper der rationalen Funktionen**,
wobei $K(x) := (K[x] \times (K[x] \setminus \{0\}))/\sim$ mit $(p, q) \sim (r, t) :\Leftrightarrow pt = qr$.

Bemerkung 2.4.10:

Die Multiplikation mit x induziert einen Endomorphismus von $K[x]/pK[x]$:

$$x^i + pK[x] \overset{\cdot x}{\mapsto} x^{i+1} + pK[x]$$
$$x^{n-1} + pK[x] \overset{\cdot x}{\mapsto} x^n + pK[x] = \left(-a_0 - a_1 x - \dots - a_{n-1} x^{n-1}\right) + pK[x]$$

© study.woalk.de

Satz 2.4.11:

Sei $p \in K[x]$.

1. Durch vertreterweise Addition und Multiplikation ist $K[x]$ eine K-Algebra mit $\overline{1} := 1 + pK[x]$.
2. Ist $p \in K[x]$ irreduzibel, ist $K[x]/pK[x]$ ein Körper.

Beispiel 2.4.12: Einige Polynomrestklassenkörper

1. Neue Konstruktion von $\mathbb{C}$: In $\mathbb{R}[x]$ ist $p := x^2 + 1$ irreduzibel. Bezeichne die Restklasse von x mit $\overline{x} := x + (x^2+1)\mathbb{R}[x]$. Dann gilt, dass $\overline{x}^2 = -\overline{1}$.
   Die Elemente von $\mathbb{R}/(x^2+1)\mathbb{R}[x]$ sind gegeben durch $a + b\overline{x}$ mit $a, b \in \mathbb{R}$.
2. $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2+x+1)\mathbb{F}_2[x]$ ist der 4-elementige Körper.
3. $\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}[x]/(x^3-2)\mathbb{Q}[x]$ ist Körper, $\overline{x} =: \sqrt[3]{2}$.

Bemerkung 2.4.13:

Sei A eine assoziative K-Algebra, z.B. $A = K$ oder $A = K^{n\times n}$.

1. Für $a \in A$ ist $x^i \mapsto a^i$ der **Einsetzungshomomorphismus** $\varepsilon_a : K[x] \to A, \quad p(x) \mapsto p(a)$ ein K-Algebren-Homomorphismus.
2. Ein Element $a \in A$ heißt **Wurzel** („Nullstelle“) von p, falls $p(a) = 0$, also $\varepsilon_a(p) = 0$.
3. Für $a \in K$ ist $p(a)$ der Rest der Division von $p \mod (x-a)$.
4. Für $a \in K$ ist $\mathrm{Kern}(\varepsilon_a) = (x-a)K[x]$.
5. Ein Polynom vom Grad n hat höchstens n verschiedene Wurzeln.
6. Eine Abbildung $f \in K^K$ heißt **Polynomfunktion**, falls $\exists p \in K[x] : \forall a \in K : f(a) = p(a)$
   In diesem Fall schreibt man $f := f_p$. Es ist $\varepsilon : K[x] \to K^K, \quad p \mapsto f_p : K \to K,\ a \mapsto p(a)$ ein K-Algebren-Homomorphismus. Sein Bild bezeichnet man mit $\mathrm{PolFu}(K)$.
   ε ist injektiv $\Leftrightarrow |K| = \infty$. Dann ist ihre Korestriktion $\varepsilon' : K[x] \to \mathrm{PolFu}(K)$ ein Iso.
   ε ist surjektiv $\Leftrightarrow |K| < \infty$ (es ist $|K^K| = |K|^{|K|}$, $|K[x]| = \infty$).

$t^4 + t^2 + t + 6 = ? \mod (t^2 - 3)$ **Einfache Lösung:** Man kann jetzt annehmen, dass $t^2 = 3$, einsetzen.

Übung 8.2:

Sei $p \in K[x]$.

(i) siehe 2.4.13.3.

(ii) Für $\mathrm{Grad}\, p \in \{2, 3\}$ ist p irreduzibel $\Leftrightarrow$ p hat keine Wurzeln in K.

Übung 8.4: Lagrange-Interpolation

Seien $a_1, \ldots, a_n \in K$ beliebige Elemente und $s_1, \ldots, s_n \in K$ paarweise verschieden.
Dann $\exists$ eindeutig $p \in K[x]_{\mathrm{Grad}<n} : \forall i \in \underline{n} : p(s_i) = a_i$, nämlich $p(x) := \sum_{i=1}^{n} \prod_{j \in \underline{n}\setminus\{i\}} \frac{x - s_j}{s_i - s_j}$

Definition 2.4.14: Algebraische Abgeschlossenheit

Ein Körper K heißt **algebraisch abgeschlossen**, falls jedes nicht-konstante Polynom über K eine Wurzel in K hat, d.h. falls jedes Polynom in Linearfaktoren zerfällt.

© study.woalk.de

Satz 2.4.15: *sogenannter* „Fundamentalsatz" der Algebra

$\mathbb{C}$ ist algebraisch abgeschlossen.

3 Struktur endlich erzeugter VRe

Ist $\mathcal{V}$ ein K-VR mit $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$, gilt: $\mathcal{T}_1 \cup \mathcal{T}_2 \leq \mathcal{V} \Leftrightarrow \mathcal{T}_1 = \mathcal{T}_2$.
Sei M eine Menge von Teilräumen $\mathcal{W} \leq \mathcal{V}$. Dann gilt: $\bigcap_{\mathcal{W} \in M} \mathcal{W} \leq \mathcal{V}$.

Definition 3.1.4: Erzeugnis

Sei $\mathcal{V}$ ein K-VR mit $M \subset \mathcal{V}$ eine Teil*menge*.

1. Das **Erzeugnis** (Vekrorraumerzeugnis) $\langle M \rangle$ von M ist der Durchschnitt aller Teilräume von $\mathcal{V}$, die M enthalten. $\langle M \rangle := \bigcap_{M \subset \mathcal{W} \leq \mathcal{V}}$ und somit der kleinste TR von $\mathcal{V}$, der M enthält.
2. Eine **Linearkombination** von Elementen aus M ist ein Vektor $V \in \mathcal{V}$, für den ein $n \in \mathbb{N}$ mit $a \in K^n,\ X \in M^n$ existiert mit $V = a_1 X_1 + \cdots + a_n X_n$.
   Ist $M = \emptyset$, so ist der Nullvektor $0 \in \mathcal{V}$ die einzige Linearkombination aus Vektoren in M.
   Die Menge aller Linearkombinationen von M bezeichnen wir mit
   $\mathcal{LK}(M) := \{\sum_{i=1}^{n} a_i X_i \mid n \in \mathbb{Z}_{\geq 0},\ X \in M^n,\ a \in K^n\}$

Satz 3.1.5:

Sei $\mathcal{V}$ ein K-Vektorraum und $M \subset \mathcal{V}$, dann gilt: $\langle M \rangle = \mathcal{LK}(M)$

Definition 3.1.7: Vektorraum-Summe

Seien $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$. Dann definiert man (als Ersatz für Vereinigung) die **Summe der beiden TRe**:
$\mathcal{T}_1 + \mathcal{T}_2 := \langle \mathcal{T}_1 \cup \mathcal{T}_2 \rangle =: \langle \mathcal{T}_1, \mathcal{T}_2 \rangle$

Bemerkung 3.1.8: Vektorraum-Summe und ihre Verwandschaft

Seien $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$.

1. $\mathcal{T}_1 + \mathcal{T}_2 = \{X_1 + X_2 \mid X_1 \in \mathcal{T}_1,\ X_2 \in \mathcal{T}_2\}$
2. $\varphi : \mathcal{T}_1 \oplus_{\mathrm{a}} \mathcal{T}_2 \to \mathcal{V}, \quad (X_1, X_2) \mapsto X_1 + X_2$ ist eine lineare Abbildung mit $\mathrm{Bild}\,\varphi = \mathcal{T}_1 + \mathcal{T}_2$ und $\mathrm{Kern}\,\varphi = \{(T, -T) \mid \mathcal{T} \in \mathcal{T}_1 \cap \mathcal{T}_2\}$.
   Insbesondere gilt $\mathcal{T}_1 + \mathcal{T}_2 = \mathcal{T}_1 \oplus_{\mathrm{i}} \mathcal{T}_2 \Leftrightarrow \mathcal{T}_1 \cap \mathcal{T}_2 = \{0\}$.
3. Ist $M = \{X\} \subset \mathcal{V}$, dann ist $\langle X \rangle := \langle M \rangle = \{aX \mid a \in K\}$.

Es gilt: $\{(T, -T) \mid T \in \mathcal{T}_1 \cap \mathcal{T}_2\} \underset{\text{abstrakt}}{\cong} \mathcal{T}_1 \cap \mathcal{T}_2$

$\mathcal{T}_1 \cap \mathcal{T}_2 \hookrightarrow \mathcal{T}_1 \oplus_{\mathrm{a}} \mathcal{T}_2 \twoheadrightarrow \mathcal{T}_1 + \mathcal{T}_2$
vgl.: $N_1 \cap N_2 \hookrightarrow N_1 \sqcup N_2 \twoheadrightarrow N_1 \cup N_2$

$\mathcal{T}_1 \oplus_{\mathrm{a}} \mathcal{T}_2$ —— $\mathcal{T}_1 + \mathcal{T}_2$ —— $\mathcal{T}_1 \cap \mathcal{T}_2 \cong$ „wenn $\mathcal{T}_1 \cap \mathcal{T}_2 = \{0\}$, ist $\mathcal{T}_1 + \mathcal{T}_2 = \mathcal{T}_1 \oplus_{\mathrm{a}} \mathcal{T}_2$"

Definition 3.1.10: Erzeugendensystem

K-VR $\mathcal{V}$ heißt **endlich erzeugt** (e.e.), falls eine *endliche* Teilmenge $M \subseteq \mathcal{V}$ mit $\langle M \rangle = \mathcal{V}$ existiert.
Jedes solche M heißt **Erzeugendensystem** (EZS) von $\mathcal{V}$.

© study.woalk.de

Bemerkung 3.1.11: Endliches Erzeugen mit Beispielen

1. $\mathcal{V} := K^{n\times 1}$ ist endlich erzeugt, denn die Spalten $e_i = (I_n)_{-,i}$ bilden ein Erzeugendensystem.
2. $K[x]$ ist *nicht* endlich erzeugt, denn $\forall$ endliche Teilmenge ist Grad der Polynome beschränkt.
3. Ist $\varphi : \mathcal{V} \to \mathcal{W}$ ein Homomorphismus und M ein Erzeugendensystem, von $\mathcal{V}$, dann ist $\varphi(M) = \{\varphi(m) \mid m \in M\}$ ein Erzeugendensystem von $\operatorname{Bild}\varphi \subseteq \mathcal{W}$.
   D.h. EZSe bilden unter Epimorphismen wieder auf EZSe ab.
4. Ist $\mathcal{V}$ e.e. und $\varphi : \mathcal{V} \to \mathcal{W}$ Epimorphismus $\Rightarrow \mathcal{W}$ e.e.
5. Sind $\mathcal{V}, \mathcal{W}$ e.e. $\Rightarrow \mathcal{V} \oplus_a \mathcal{W}$ e.e.

Definition 3.1.12: Minimales Erzeugendensystem

Sei $\mathcal{V}$ ein K-VR, dann heißt $M \subseteq \mathcal{V}$ **minimales Erzeugendensystem**, falls
$\langle M\rangle = \mathcal{V}$ und $\langle M \setminus \{X\}\rangle \neq \mathcal{V} \quad \forall X \in M$ (man darf keinen weglassen).

Definition 3.2.2: Lineare Unabhängigkeit

Sei $\mathcal{V}$ ein K-VR und $X \in \mathcal{V}^n$. Folgende Aussagen sind äquivalent:

0. X heißt **linear unabhängig**.
1. $a_1X_1 + \ldots a_nX_n = 0 \Rightarrow a_1 = \cdots = a_n = 0$ für $a \in K^n$.
2. Der Linearkombinationshomomorphismus λ_X ist ein *Monomorphismus*, also $\operatorname{Kern}\lambda_X = \{0\}$.
3. $\forall Y \in \langle X\rangle : \exists$ eindeutiges $a \in K^n : Y = a_1X_1 + a_2X_2 + \cdots + a_nX_n$.

Eine endliche Menge heißt linear unabhängig, wenn das Tupel aus allen Mengenelementen linear unabhängig ist. Eine unendliche Menge heißt linear unabhängig, falls jede endliche Teilmenge linear unabhängig ist.

Bemerkung 3.2.3:

Sei $X \in \mathcal{V}^n$, $\varphi : \mathcal{V} \to \mathcal{W}$ linear und $\varphi \circ X = (\varphi(X_1), \ldots, \varphi(X_n)) \in \mathcal{W}^n$ linear unabhängig $\Rightarrow X$ linear unabhängig.

Übung 9.1:

Sei $\mathcal{V}$ ein K-VR und $M \subseteq N \subseteq \mathcal{V}$.

(i) M Erzeugendensystem von $\mathcal{V} \Rightarrow N$ Erzeugendensystem von $\mathcal{V}$

(ii) N linear unabhängig $\Rightarrow M$ linear unabhängig

Satz 3.2.6: Basis

Sei $\mathcal{V}$ ein K-VR und $X \in \mathcal{V}^n$. Dann sind folgende Aussagen äquivalent:

1. X ist ein *minimales EZS* von $\mathcal{V}$.
2. X ist *maximal linear unabhängig* in $\mathcal{V}$.
3. X ist ein linear unabhängiges EZS.
4. $\lambda_X : K^n \to \mathcal{V}$ ist der Linearkombinations**isomorphismus**.
5. X heißt **Basis** von $\mathcal{V}$ (Definition).

$\xrightarrow[3.2.7]{}$ Sei X eine Basis von $\mathcal{V}$.
$\lambda_X^{-1} = \kappa_X^{\mathrm{tr}} : \mathcal{V} \to K^n, \quad a_1X_1 + \cdots + a_nX_n \mapsto (a_1, \ldots, a_n)$ heißt **Zeilenkoordinatenabbildung** bezüglich der Basis X. Analog: $\kappa_X(V) \in K^{n\times 1}$ ist die **Koordinatenspalte** von $V \in \mathcal{V}$.
Damit ist $\mathcal{V} \cong K^{n\times 1}$!

© study.woalk.de

Merke :

$B \in \mathcal{V}^n$ ist eine Basis von $\mathcal{V} \Leftrightarrow V \in \mathcal{V}$ ist eine *eindeutige* Linearkombination der Vektoren von B.

- *Existenz* von Linearkombinationen: B ist EZS.
- *Eindeutigkeit* von Linearkombinationen: B ist linear unabhängig.

Satz 3.3.1: Steinitz'scher Austauschsatz

Sei $\mathcal{V}$ ein K-VR und $X \in \mathcal{V}^n$ ein EZS von $\mathcal{V}$, und sei $Y \in \mathcal{V}^s$ linear unabhängig.
Dann gilt: $s \leq n$ und nach geeigneter Umordnung der X_is ist $(Y_1, \ldots, Y_s, X_{s+1}, \ldots, X_n)$ ein EZS von $\mathcal{V}$.

$\xrightarrow[3.3.2]{}$ Sei $\mathcal{V}$ ein e.e. K-VR.
Dann $\exists$ eindeutiges $n \in \mathbb{Z}_{\geq 0}$, sodass jede Basis von $\mathcal{V}$ aus genau n Vektoren besteht. Nenne $n =: \operatorname{Dim} \mathcal{V}$ die **Dimension** von $\mathcal{V}$. Ist $\mathcal{V}$ nicht e.e., so setzen wir $\operatorname{Dim} \mathcal{V} = \infty$. $\operatorname{Dim} K^M = |M|$ für bel. Mengen M.

Bemerkung 3.3.4:

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ ein K-VR-Homomorphismus.

2. Ist $\langle Y_1, \ldots, Y_m \rangle = \mathcal{V}$, so ist $\langle \varphi(Y_1), \ldots, \varphi(Y_m) \rangle = \operatorname{Bild} \varphi \leq \mathcal{W}$.
3. Ist φ Isomorphismus, so bildet φ Basen von $\mathcal{V}$ auf Basen von $\mathcal{W}$ ab.
   Insbesondere gilt $\operatorname{Dim} \mathcal{V} = \operatorname{Dim} \mathcal{W}$.

$\to$ **Folgerung 3.3.5:**

Sei $\mathcal{V}$ ein e.e. K-VR.

1. **Basisergänzungssatz**: Ist $X \in \mathcal{V}^s$ linear unabhängig, kann man X zu einer Basis von $\mathcal{V}$ ergänzen, denn $s \leq \operatorname{Dim} \mathcal{V}$.
2. Ist $\mathcal{T} \leq \mathcal{V}$, so ist $\operatorname{Dim} \mathcal{T} \leq \operatorname{Dim} \mathcal{V}$, und $\operatorname{Dim} T = \operatorname{Dim} \mathcal{V} \Leftrightarrow \mathcal{T} = \mathcal{V}$.
3. Ist $\mathcal{T} \leq \mathcal{V}$ mit $X \in \mathcal{T}^m$ Basis von $\mathcal{T}$ und $(X_1, \ldots, X_m, Y_1, \ldots, Y_k)$ Basis von $\mathcal{V}$, so ist $(Y_1 + \mathcal{T}, \ldots, Y_k + \mathcal{T})$ eine Basis von $\mathcal{V}/\mathcal{T}$. Insbesondere ist $\operatorname{Dim}(\mathcal{V}/\mathcal{T}) = \operatorname{Dim} \mathcal{V} - \operatorname{Dim} \mathcal{T}$.

Also **Dimensionssatz für Unterräume**: $\operatorname{Dim} \mathcal{V} = \operatorname{Dim} \mathcal{T} + \operatorname{Dim}(\mathcal{V}/\mathcal{T})$

Übung 10.2:

Sei $\mathcal{V}$ ein K-VR, $\mathcal{U} \leq \mathcal{V}$ mit Basis $\mathcal{B}$ bestehend aus den Elementen von $B \subseteq \mathcal{U}$, und sei $C \subseteq \mathcal{V}$.
Dann bilden die Elemente von $\{c + \mathcal{U} \mid c \in C\}$ eine Basis von $\mathcal{V}/\mathcal{U}$
$\Leftrightarrow B \cap C = \emptyset$ und die Elemente von $B \cup C$ bilden Basis von $\mathcal{V}$.

$\to$ **Folgerung 3.3.6/7/8: Dimensionssätze**

Sei $\mathcal{V}$ e.e., $\alpha : \mathcal{V} \to \mathcal{W}$ ein Homomorphismus. Dann gilt: $\operatorname{Dim}(\operatorname{Bild} \alpha) + \operatorname{Dim}(\operatorname{Kern} \alpha) = \operatorname{Dim} \mathcal{V}$
Seien $\mathcal{V}_1, \mathcal{V}_2$ e.e. K-VRe. Nach Übung 10.1 gilt: $\operatorname{Dim}(\mathcal{V}_1 \oplus_a V_2) = \operatorname{Dim} \mathcal{V}_1 + \operatorname{Dim} \mathcal{V}_2$
Seien $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$ (e.e.). Dann gilt: $\operatorname{Dim}(\mathcal{T}_1 + \mathcal{T}_2) + \operatorname{Dim}(\mathcal{T}_1 \cap \mathcal{T}_2) = \operatorname{Dim} \mathcal{T}_1 + \operatorname{Dim} \mathcal{T}_2$.

Satz 3.3.11: Unendliche Basen

Sei $\mathcal{V}$ ein K-VR, $X \subseteq \mathcal{V}$.

(a) X heißt EZS von $\mathcal{V}$, falls $\forall V \in \mathcal{V}$ endliche Linearkombination der Elemente von X ist.

(b) X heißt linear unabhängig, falls alle endlichen Teilmengen von X linear unabhängig sind.

© study.woalk.de

4 Konstruktive Aspekte

Satz 4.1.1:

Seien $\mathcal{V}, \mathcal{W}$ zwei K-VRe und $X \in \mathcal{V}^n,\ Y \in \mathcal{W}^n$.

1. Ist X ein EZS von $\mathcal{V}$, so gibt es *höchstens* eine lineare Abbildung $\varphi : \mathcal{V} \to \mathcal{W}$ mit $\varphi \circ X = Y$.
2. Ist X linear unabhängig und $\mathcal{V}$ e.e., so gibt es *mindestens* eine lineare Abbildung φ.
3. Ist X Basis von $\mathcal{V}$, gibt es *genau eine* lineare Abbildung φ.

Bemerkung 4.1.4: Induzierter Homomorphismus

$\tilde{\cdot} : K^{m\times n} \to \mathrm{Hom}\left(K^{n\times 1}, K^{m\times 1}\right), \quad A \mapsto \tilde{A}$ ist ein Isomorphismus.

Definition 4.1.5: Koordinatenabbildung

Sei $\mathcal{V}$ ein n-dimensionaler K-VR mit Basis $B \in \mathcal{V}^n$. Dann heißt der Isomorphismus

$$\kappa_B : \mathcal{V} \to K^{n\times 1}, \quad X = a_1 B_1 + \cdots + a_n B_n \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

die **Spalten-Koordinatenabbildung**.

Satz 4.1.7: Abbildungsmatrix

Sei $\mathcal{V}$ ein K-VR mit Basis $B \in \mathcal{V}^n$ und $\mathcal{W}$ ein K-VR mit Basis $C \in \mathcal{W}^m$. Dann gilt:

1. Die Abbildung ${}_C\Lambda_B : K^{m\times n} \to \mathrm{Hom}\left(\mathcal{V}, \mathcal{W}\right), \quad A \mapsto \kappa_C^{-1} \circ \tilde{A} \circ \kappa_B$ ist ein Isomorphismus.
2. Sei die Umkehrabbildung ${}_C\Lambda_B{}^{-1} : \mathrm{Hom}\left(\mathcal{V}, \mathcal{W}\right) \to K^{m\times n}, \quad \varphi \mapsto {}^C\varphi^B$ Man nennt ${}^B\varphi_C$ die Matrix von φ bezüglich der Basen B und C.
   Per Definition gilt $\varphi = \kappa_C^{-1} \circ \widetilde{{}^C\varphi^B} \circ \kappa_B$.
   Damit kommutiert das Diagramm:
   $$\begin{array}{ccc} \mathcal{V} & \xrightarrow{\varphi} & \mathcal{W} \\ {\scriptstyle \kappa_B}\downarrow & & \downarrow{\scriptstyle \kappa_C} \\ K^{n\times 1} & \xrightarrow{\widetilde{{}^C\varphi^B}} & K^{m\times 1} \end{array}$$
3. Insbesondere gilt für $V \in \mathcal{V}$: ${}^C\left(\varphi\right) = {}^C\varphi^B \cdot {}^BV$
   In der i-ten Spalte von ${}^C\varphi^B$ steht die Koordinatenspalte von $\varphi\left(B_i\right)$ bezüglich der Basis C.

Satz 4.1.9: Verkettung von Abbildungsmatrizen

Seien $\varphi : \mathcal{V} \to \mathcal{W}$ und $\psi : \mathcal{W} \to \mathcal{U}$ K-lineare Abbildungen,
die VRe haben die Basen $B \in \mathcal{V}^n,\ C \in \mathcal{W}^m,\ D \in \mathcal{U}^p$.
Dann gilt: ${}^D\left(\psi \circ \varphi\right){}^B = {}^D\psi^C \cdot {}^C\varphi^B$

Folgerung 4.1.10: Basiswechsel

1. Sind B und B' Basen von $\mathcal{V}$, so heißt ${}^B\mathrm{id}_{\mathcal{V}}{}^{B'}$ die **Basiswechselmatrix** bzw. die Matrix der Basistransformation, und es gilt ${}^{B'}\mathrm{id}_{\mathcal{V}}{}^B = \left({}^B\mathrm{id}_{\mathcal{V}}{}^{B'}\right)^{-1}$.
2. Sind $C, C' \in \mathcal{W}^n$ Basen von $\mathcal{W}$ und ist $\varphi : \mathcal{V} \to \mathcal{W}$ linear, so gilt ${}^{C'}\varphi^{B'} = {}^{C'}\mathrm{id}_{\mathcal{V}}{}^C\,{}^C\varphi^B\,{}^B\mathrm{id}_{\mathcal{V}}{}^{B'}$

© study.woalk.de

Definition 4.2.1: Zeilen- und Spaltenräume

Sei $A \in K^{m\times n}$, $\mathcal{V}$ ein K-VR.

1. Es bezeichnet $\mathrm{TR}(\mathcal{V}) := \{\mathcal{T} \mid \mathcal{T} \leq \mathcal{V}\}$ die Menge aller Teilräume von $\mathcal{V}$.
2. $\mathrm{Z}(A) := \langle A_{1,-}, A_{2,-}, \ldots, A_{m,-}\rangle \leq K^{1\times n}$ heißt **Zeilenraum** von A und seine Dimension ist der **Zeilenrang** von A.
3. $\mathrm{S}(A) := \langle A_{-,1}, A_{-,2}, \ldots, A_{-,n}\rangle \leq K^{m\times 1}$ heißt **Spaltenraum** von A und seine Dimension ist der **Spaltenrang** von A. Es ist $\mathrm{S}(A) = \mathrm{Bild}\,\tilde{A}$.

Bemerkung 4.2.2/3: Rang

Sei $A \in K^{m\times n}$, $g \in \mathrm{GL}_m(K), h \in \mathrm{GL}_n(K)$.

1. Dann haben A und gA denselben Zeilenraum und somit auch den selben Zeilenrang. Insbesondere produziert der Gauß'sche Algorithmus eine Basis des Zeilenraums.
3. A und Ah haben denselben Spaltenraum und somit denselben Spaltenrang.

$\Rightarrow$ Zeilanrang = Spaltenrang $=: \mathrm{Rang}(A)$.
$\mathrm{Rang}\,A =$ Anzahl nicht-Nullzeilen in der strikten Stufenform von A (Gauß).

$\xrightarrow[4.2.5]{}$ Für $A \in K^{m\times n}$ ist $\mathrm{Kern}\,\tilde{A} = \mathcal{L}(Ax = b)$ mit $\mathrm{Dim}\,\mathcal{L} = n - \mathrm{Rang}\,A$. Es ist $\mathrm{Rang}\,A = \mathrm{Dim}\left(\mathrm{Bild}\,\tilde{A}\right)$.

Satz 4.2.6: Zeilenraum und GL

1. $\mathrm{GL}_m(K)$ operiert auf $K^{m\times n}$ durch Linksmultiplikation.
2. Der Zeilenraum $\mathrm{Z} : K^{m\times n} \to \mathrm{TR}(K^{1\times n})$ ist eine trennende Invariante dieser Operation.
3. Jede Bahn enthält genau eine Matrix in Stufengestalt.

$\xrightarrow[4.2.7]{}$ Jeder k-dimensionale TR von $K^{1\times n}$ mit $k > 0$ hat eine eindeutige Standardbasis $(Z_1, \ldots, Z_k)$, die dadurch ausgezeichnet ist, dass die Matrix $Z \in K^{k\times n}$ mit $Z_{i,-} = Z_i$ in strikter Stufenform ist.

Definition 4.2.9: Rang von Homomorphismen

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ ein K-VR-Homomorphismus. Definiere $\mathrm{Rang}(\varphi) := \mathrm{Dim}(\mathrm{Bild}\,\varphi)$.

$\xrightarrow[4.2.10]{}$ Seien $\varphi : \mathcal{V} \to \mathcal{W}$, B Basis von $\mathcal{V}$, C Basis von $\mathcal{W}$.

$$\Rightarrow \mathrm{Rang}(\varphi) = \mathrm{Rang}({}^{C}\varphi^{B}) \underset{\text{Übung 11.3}}{=} \mathrm{Rang}_{B,C}(\varphi) := \mathrm{Rang}(\kappa_C \circ \varphi \circ \lambda_B) = \mathrm{Dim}(\mathrm{Bild}\,\varphi)$$

© study.woalk.de

→ **Folgerung 4.2.11: „Offenbarung“**

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ eine lineare Abbildung von endlich-dimensionalen K-VRen. Dann existiert eine Basis B von $\mathcal{V}$ und eine Basis C von $\mathcal{W}$ derart, dass die Abbildungsmatrix ${}^{C}\varphi^{B}$ folgende einfache Gestalt annimmt:

$$ {}^{C}\varphi^{B} = \begin{pmatrix} 1 & 0 & & \cdots & & 0 \\ 0 & \ddots & 0 & \cdots & & \\ \vdots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ 0 & & \cdots & & 0 & 0 \\ \vdots & & & & & \vdots \end{pmatrix} $$

mit genau $\operatorname{Rang}\varphi$ Einsen auf der Diagonalen.
Dann ist $\varphi(B_i) = C_i$ für $i \in \underline{\operatorname{Rang}\varphi}$ und $\varphi(B_i) = 0$ für $\operatorname{Rang}\varphi < i < \operatorname{Dim}\mathcal{V}$.

Starte mit zwei beliebigen Basen $B' \in \mathcal{V}^n$, $C' \in \mathcal{W}^m$. Berechne ${}^{C'}\varphi^{B'}$ und bringe sie mit Hilfe des (Zeilen-)Gauß-Algorithmus auf strikte Stufenform und mit Hilfe des völlig analogen Spalten-Gauß schließlich auf die gewünschte Form, wir nennen sie A.
Durch die Buchführung bei den Gauß-Algorithmen bestimmen wir also Matrizen $g \in \mathrm{GL}_n(K)$ und $h \in \mathrm{GL}_m(K)$ mit $g\left({}^{C'}\varphi^{B'}\right)h = A$. Nun interpretiere h als ${}^{B}\mathrm{id}_{\mathcal{V}}^{B'}$ und g als ${}^{C'}\mathrm{id}_{\mathcal{W}}^{C}$ und leite daraus B und C ab.

→ **Folgerung 4.2.12: Rang und GL**

Die Gruppe $\mathrm{GL}_m(K) \times \mathrm{GL}_n(K)$ operiert auf $K^{m\times n}$ durch

$$(\mathrm{GL}_m(K) \times \mathrm{GL}_n(K)) \times K^{m\times n} \to K^{m\times n}, \quad ((g,h),M) \mapsto gMh^{-1}$$

Matrizen in der gleichen Bahn heißen **äquivalent**. (Nach Folgerung 4.2.11:)
Der Rang $\operatorname{Rang} : K^{m\times 1} \to \mathbb{Z}_{\geq 0}, \quad M \mapsto \operatorname{Rang} M$ ist eine trennende Invariante dieser Operation.

5 Endomorphismen

Definition 5.1.1: Endomorphismenring

Sei $\mathcal{V}$ ein K-VR. Dann heißt $\operatorname{End}(\mathcal{V}) := \operatorname{Hom}(\mathcal{V},\mathcal{V})$ zusammen mit der Addition und Komposition von linearen Abbildungen der **Endomorphismenring** von $\mathcal{V}$. Dieser ist eine K-Algebra, die für $\operatorname{Dim}\mathcal{V} > 1$ *nicht* kommutativ ist. Es bildet $\operatorname{End}(\mathcal{V})^{\times} =: \mathrm{GL}(\mathcal{V})$.

Bemerkung 5.1.2: Endo-Abbildungsmatrix

Sei $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$. Dann ist $\operatorname{End}(\mathcal{V}) \to K^{n\times n}, \quad \varphi \mapsto {}^{B}\varphi^{B}$
ein Isomorphismus und K-Algebren-Homomorphismus.

Bemerkung 5.1.3: Ähnlichkeit

1. $\alpha \in \operatorname{End}(\mathcal{V})$, $B, B' \in \mathcal{V}^n$ Basen.
   ${}^{B'}\alpha^{B'} = \left({}^{B}\mathrm{id}_{\mathcal{V}}^{B'}\right)^{-1} \cdot {}^{B}\alpha^{B} \cdot {}^{B}\mathrm{id}_{\mathcal{V}}^{B'} = {}^{B'}\mathrm{id}_{\mathcal{V}}^{B} \cdot {}^{B}\alpha^{B} \cdot \left({}^{B'}\mathrm{id}_{\mathcal{V}}^{B}\right)^{-1}$
2. $\mathrm{GL}_n(K)$ operiert auf $K^{n\times n}$ durch $\mathrm{GL}_n(K) \times K^{n\times n} \to K^{n\times n}, \quad (g,A) \mapsto gAg^{-1}$.
   Matrizen in der gleichen Bahn heißen **ähnlich**.

© study.woalk.de

Definition 5.1.4: Spur

Für $A \in K^{n\times n}$ heißt $\mathrm{Spur}(A) := \sum_{i=1}^{n} A_{i,i}$ die **Spur** der Matrix A (Summe der Diagonaleinträge).

Sei $\mathcal{V}$ endlich-dimensionaler K-VR. Für $\alpha \in \mathrm{End}(\mathcal{V})$ definiert man die Spur von α durch $\mathrm{Spur}(\alpha) := \mathrm{Spur}({}^{B}\alpha^{B})$ für eine beliebige Basis B (wohldefiniert unabhängig der Basis).

Bemerkung 5.1.5: Spur-Identitäten

1. Für $A \in K^{m\times n}$ und $B \in K^{n\times m}$ gilt: $\mathrm{Spur}(AB) = \mathrm{Spur}(BA) = \sum_{i,j} A_{i,j}B_{j,i}$
2. Für $A \in K^{n\times n}$ und $g \in \mathrm{GL}_n(K)$ gilt: $\mathrm{Spur}(gAg^{-1}) = \mathrm{Spur}(A)$ (folgt aus 1.)

5.2 Das Minimalpolynom

Beispiel 5.2.1: Einsetzungshomomorphismen

1. Für $A \in K^{n\times n}$, $p = p(x) = a_0x^0 + a_1x + \cdots + a_dx^d \in K[x]$ sei:
   $p(A) := a_0I_n + a_1A + \cdots + a_dA^d \in K^{n\times n}$.
   Es heißt $\varepsilon_A : K[x] \to K^{n\times n}, \quad p \mapsto p(A)$ der Einsetzungshomomorphismus der Matrix A.
2. Für $\alpha \in \mathrm{End}(\mathcal{V})$ und $p \in K[x]$ sei: $p(\alpha) := a_0\mathrm{id}_{\mathcal{V}} + a_1\alpha + \cdots + a_d\alpha^d \in \mathrm{End}(\mathcal{V})$.
   Es heißt $\varepsilon_\alpha : K[x] \to \mathrm{End}(\mathcal{V}), p \mapsto p(\alpha)$ der Einsetungshomomorphismus des Endo. α.

Übung 12.1.i: Für $g \in \mathrm{GL}_n(K)$, $p \in K[x]$ gilt: $p(g^{-1}Ag) = g^{-1}p(A)g$

Lemma 5.2.2: Minimalpolynome

1. Sei $A \in K^{n\times n}$, so gibt es ein *normiertes* Polynom $\mu_A \in K[x]$ mit $\mathrm{Kern}(\varepsilon_A) = \mu_A K[X]$. Dieses Polynom heißt das **Minimalpolynom** („MinPoly“) von A.
2. Ist $\mathcal{V}$ ein endlich-dimensionaler K-VR und $\alpha \in \mathrm{End}(\mathcal{V})$, so gibt es genau ein normiertes Polynom $\mu_\alpha \in K[x]$ mit $\mathrm{Kern}(\varepsilon_\alpha) = \mu_\alpha K[x]$. Dieses heißt das **Minimalpolynom** von α.

Das Minimalpolynom ist **invariant unter Transponieren**, d.h. $\mu_A = \mu_{A^{\mathrm{tr}}}$.

Bemerkung 5.2.3:

1. Der Grad des MinPolys von A ist das kleinste $s \in \mathbb{N}$ mit $(I_n, A, \ldots, A^s)$ linear abhängig. Insbesondere ist μ_A wohldefiniert.
2. Das MinPoly, genauer $\mu : K^{n\times n} \to K[x], \quad A \mapsto \mu_A$, ist eine Invariante der Ähnlichkeitsklassen von $K^{n\times n}$, also ähnliche Matrizen haben das gleiche MinPoly (nach Übung 12.1.ii).
3. Sei $\alpha \in \mathrm{End}(\mathcal{V})$, $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$ und $A := {}^{B}\alpha^{B} \in K^{n\times n}$. Dann gilt $\mu_\alpha = \mu_A$.

© study.woalk.de

Beispiel 5.2.4: Einige MinPoly

1. $\mu_0 = x \in K[x]$ für $0 \in K^{n\times n}$ sowie $0 \in \mathrm{End}(\mathcal{V})$.
2. $\mu_{I_n} = \mu_{\mathrm{id}_\mathcal{V}} = x - 1$
4. Sei $\mathcal{V} := \langle \sin, \cos \rangle \leq \mathbb{R}^\mathbb{R}$ und $\partial \in \mathrm{End}(\mathcal{V})$ der Ableitungsoperator.

   $$\partial(\sin) = \sin' = \cos, \quad \partial(\cos) = \cos' = -\sin$$

   Also ist $\mu_\partial = x^2 + 1 \Rightarrow \langle 1, \partial \rangle \leq \mathrm{End}(\mathbb{R}^\mathbb{R})$ ist eine neue Darstellung von $\mathbb{C}$.
5. Im Allgemeinen gilt für $A \in K^{n\times n}$:

   $$K^{n\times n} \geq K[A] := \langle I_n, A, \ldots, A^{s-1} \rangle = \mathrm{Bild}\, \varepsilon_A = K[x] / \mathrm{Kern}(\varepsilon_A) = K[x] / \mu_A K[x]$$

   als K-Algebra.

Für $\alpha \in \mathrm{End}(\mathcal{V})$ heißt $\mathcal{U} \leq \mathcal{V}$ **α-invarianter TR** von $\mathcal{V}$, wenn $\alpha(\mathcal{U}) \subseteq \mathcal{U}$ (Einschränkung auf $\mathcal{U}$ abgeschlossen).

Lemma 5.2.5: Teiler des MinPoly

Sei $\alpha \in \mathrm{End}(\mathcal{V})$ und $\mathcal{U} \leq \mathcal{V}$ ein α-invarianter TR von $\mathcal{V}$. Dann definiert α zwei Abbildungen
$\beta := \alpha_{|\mathcal{U}} \in \mathrm{End}(\mathcal{U})$ und
$\gamma \in \mathrm{End}(\mathcal{V}/\mathcal{U}), \quad \gamma(X + \mathcal{U}) = \alpha(X) + \mathcal{U}$.
Es gilt: $\mathrm{kgV}(\mu_\beta, \mu_\gamma) \mid \mu_\alpha \mid \mu_\beta \mu_\gamma$

Bemerkung 5.2.6: 5.2.5 für Matrizen

$A = \begin{pmatrix} B & * \\ 0 & C \end{pmatrix} \in K^{n\times n}$ mit quadratischen Matrizen B, C.

Dann gilt: $\mathrm{kgV}(\mu_B, \mu_C) \mid \mu_A \mid \mu_B \mu_C$ und ${}^D\alpha^D = \begin{pmatrix} B & * \\ 0 & C \end{pmatrix}$ bildet auf Faktorraum ab.

Wegen der Invarianz unter Transponieren gilt dies auch für $\begin{pmatrix} B & 0 \\ * & C \end{pmatrix}$.

Bemerkung 5.2.8: MinPoly bezüglich eines Vektors

Sei $\mathcal{V}$ ein e.e. K-VR, $\alpha \in \mathrm{End}(\mathcal{V})$, $V \in \mathcal{V} \setminus \{0\}$.
Dann gibt es ein kleinstes $k \leq \mathrm{Dim}\, \mathcal{V}$, dass

$$\left(V, \alpha(V), \alpha^2(V), \ldots, \alpha^k(V)\right) \in \mathcal{V}^{k+1}$$

linear abhängig ist und eine eindeutige Abhängigkeit $(a_0, a_1, \ldots, a_{k-1}, 1) \in K^{n+1}$ mit

$$a_0 V + a_1 \alpha(V) + \cdots + a_{k-1} \alpha^{k-1}(V) + \alpha^k(V) = 0$$

existiert.
Dann heißt $\mu_{\alpha,V}(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + x^k$ das Minimalpolynom von α bzgl. V.
Der k-dimensionale TR $\mathcal{W} := K[\alpha] V := \{p(\alpha)(V) \mid p \in K[x]\} = \langle V, \alpha(V), \ldots, \alpha^{k-1}(V) \rangle$ (Basis) ist invariant unter α, sprich $\alpha(\mathcal{W}) \leq \mathcal{W}$ und $\mu_{\alpha,V}(x)$ ist das MinPoly der Einschränkung $\beta := \alpha_{|\mathcal{W}} : \mathcal{W} \to \mathcal{W}, \quad W \mapsto \alpha(\mathcal{W})$. Mit Lemma 5.2.5 gilt: $\mu_{\alpha,V} \mid \mu_\alpha$

© study.woalk.de

Bemerkung 5.2.9: Begleitmatrix

Sei $p = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$ ein normiertes Polynom vom Grad d. Die Multiplikation mit x (bzw. $\overline{x}$) induziert eine lineare Abbildung m_p auf $K[x]/pK[x]$, die bzgl. der Standardbasis $B := \left(\overline{1}, \overline{x}, \ldots, \overline{x}^{d-1}\right) \in (K[x]/pK[x])^d$ mit $\overline{x} := x + pK[x]$ (Restklasse von x) die Matrix

$$ {}^B m_p^B = \begin{pmatrix} 0 & 0 & & \cdots & 0 & -a_0 \\ 1 & 0 & & & & -a_1 \\ 0 & 1 & & & \vdots & \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & 0 & \\ 0 & 0 & \cdots & 0 & 1 & -a_{d-1} \end{pmatrix} := M_p \in K^{d \times d} $$

hat. Diese heißt **Begleitmatrix** von p. Nach Bem. 5.2.8: $\mu_{M_p} = \mu_{m_p} = p$

Algorithmus 5.2.10: Berechnung des MinPoly

Gegeben: $\alpha \in \mathrm{End}(\mathcal{V})$ eines e.e. K-VRes $\mathcal{V}$
Gesucht: Das MinPoly μ_α
Algorithmus:

1. Wähle $V' \in \mathcal{V} \setminus \{0\}$ (beliebig, oft z.B. erste Spalte von A wenn $\tilde{A} = \alpha$ oder $e_i,\ i \in \underline{\mathrm{Dim}\,\mathcal{V}}$).
2. Bestimme das Minimalpolynom $\mu_{\alpha,V'}(x)$ (aus Übung 12.3) folgendermaßen:
   (a) Bestimme ${}^B\alpha(V'),\ {}^B\alpha^2(V'), \ldots$ bis $(V', \alpha(V'), \ldots, \alpha^s(V'))$ linear abhängig.
   (b) Bestimme die lineare Abhängigkeit $0 = \alpha^s(V') + a_{s-1}\alpha^{s-1}(V') + \cdots + a_1\alpha(V') + a_0\mathrm{id}_\mathcal{V}$.
   (c) Das MinPoly des Teilraums ist $\mu_{\alpha,V'} = x^s + a_{s-1}x^{s-1} + \cdots + a_1 x + a_0$.
   Setze $\mathcal{W} := K[\alpha]V' = \langle V', \alpha(V'), \ldots, \alpha^{s-1}(V')\rangle$ und $\mu := \mu_{\alpha,V'}$.
3. Solange $\mathcal{W} \neq \mathcal{V}$, wähle $V \in \mathcal{V} \setminus \mathcal{W}$ und bestimme $\mu_{\alpha,V}$ wie oben.
   Ersetze μ durch $\mathrm{kgV}(\mu,\ \mu_{\alpha,V}) = \frac{\mu \cdot \mu_{\alpha,V}}{\mathrm{ggT}(\mu,\ \mu_{\alpha,V})}$
   und $\mathcal{W}$ durch $\mathcal{W} + K[\alpha]V = \langle \mathcal{W}, K[\alpha]V\rangle$.
   Falls $\mathcal{W} \neq \mathcal{V}$, wiederhole Schritt 3.
4. Sobald $\mathcal{W} = \mathcal{V}$, gilt $\mu_\alpha = \mu$.

In $\mathbb{F}_2$ findet man leicht lineare Unabhängigkeit $\to$ Abhängigkeit, da jeder Vektor seine „private 1“ haben muss.
Es gilt, dass $\mathrm{Grad}\,\mu_\alpha \leq \mathrm{Dim}\,\mathcal{V}$.

5.3 Eigenwerte, Eigenvektoren, Diagonalisierbarkeit

Definition 5.3.1: Eigenwerte & Eigenvektoren

Sei $\mathcal{V}$ ein K-VR und $\alpha \in \mathrm{End}(\mathcal{V})$.

1. $a \in K$ heißt **Eigenwert** (EW) von α, falls ein $V \in \mathcal{V} \setminus \{0\}$ existiert mit $\alpha(V) = aV$.
   Dann ist V **Eigenvektor** (EV) von α zum Eigenwert a.
   Allgemein ist $E_\alpha(a) = E(a) := \mathrm{Kern}(\alpha - a \cdot \mathrm{id}_\mathcal{V})$ der **Eigenraum** (ER) von α zum EW a.
   Eine Zahl $a \in K$ ist EW $\Leftrightarrow E_\alpha(a) \neq \{0\}$, also genau wenn a einen EV hat.
2. Eine Basis E von $\mathcal{V}$ aus Eigenvektoren von α heißt **Eigenvektorbasis**.
3. α ist **diagonalisierbar** (siehe später), falls eine Eigenvektorbasis von $\mathcal{V}$ bzgl. α existiert.
4. Für $A \in K^{n\times n}$ heißt ein Vektor $X \in K^{n\times 1} \setminus \{0\}$ EV zum EW $a \in K$, falls $AX = aX$ gilt und $E_A(a) = \{X \in K^{n\times 1} \mid AX = aX\}$ der ER von A bzgl. a.

© study.woalk.de

Es gilt:

Sei $A \in K^{n\times n}$.

1. Für $g \in \mathrm{GL}_n(K)$ ist $g^{-1}Ag$ Diagonalmatrix $\Leftrightarrow$ Spalten von g Eigenvektorbasis von A bilden.
2. $\tilde{A}$ ist genau dann diagonalisierbar, wenn $\exists g \in \mathrm{GL}_n(K) : g^{-1}Ag$ Diagonalmatrix.
3. Die Diagonalmatrix besteht aus den EWen auf der Diagonale, in der Reihenfolge, wie die EVen in der Basis vorkommen.

Satz 5.3.3: Eigenwerte und MinPoly

Sei $\alpha \in \mathrm{End}(\mathcal{V})$ des e.e. K-VRes $\mathcal{V}$.
$a \in K$ ist EW von $\alpha \Leftrightarrow \mu_\alpha(a) = 0$, also a eine Wurzel des MinPolys μ_α ist.

Beispiel 5.3.5/6: Projektionen

Eine **Projektion** ist eine Abbildung $\pi \in \mathrm{End}(\mathcal{V})$ mit $\pi^2 = \pi$.
Sieht man von den Grenzfällen $\pi = 0 \in \mathrm{End}(\mathcal{V})$ und $\pi = \mathrm{id}_\mathcal{V}$ ab, ist $\mu_\pi = x^2 - x = x(x-1)$.
Somit sind $0, 1$ die EWe von π und $\mathcal{V} = E_\pi(1) \oplus E_\pi(0)$ mit $E_\pi(0) := \mathrm{Kern}(\pi) = \mathrm{Bild}(\mathrm{id}_\mathcal{V} - \pi)$ und $E_\pi(0) := \mathrm{Kern}(\pi - \mathrm{id}_\mathcal{V}) = \mathrm{Bild}(\pi)$

Insbesondere hat man eine Eigenvektorbasis E für π mit ${}^E\pi^E = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \in K^{\mathrm{Dim}\,\mathcal{V}\times \mathrm{Dim}\,\mathcal{V}}$

mit $\mathrm{Dim}\, E_\pi(1)$ Einsen und $\mathrm{Dim}\, E_\pi(0)$ Nullen.

Bemerkung 5.3.7:

Sei $\mathcal{V}$ ein e.e. K-VR und $\alpha \in \mathrm{End}(\mathcal{V})$.

1. Sei $V \in \mathcal{V}$ und μ_α das MinPoly von α bzgl. V. Sei B eine Ergänzung von $(V, \alpha(V), \ldots, \alpha^{d-1}(V))$ zu einer Basis von $\mathcal{V}$. Dann gilt: ${}^B\alpha^B = \begin{pmatrix} M_{\mu_{\alpha,V}} & * \\ 0 & * \end{pmatrix}$
3. Es gibt immer ein V, sodass $\mu_{\alpha,V} = \mu_\alpha$.

Satz 5.3.8: MinPoly und Summenzerlegung

Sei $\mathcal{V}$ ein e.e. K-VR, $\alpha \in \mathrm{End}(\mathcal{V})$ mit MinPoly μ_α.

1. Ist $\mu_\alpha = p_1(x)\,p_2(x)$ mit $p_1, p_2 \in K[x]$ teilerfremd, von positivem Grad und normiert, also $\mathrm{ggT}(p_1, p_2) = 1$, dann gibt es eine α-invariante direkte Summenzerlegung $\mathcal{V} = \mathcal{T}_1 \oplus_\mathrm{i} \mathcal{T}_2$, sodass $\alpha_i : \mathcal{T}_i \to \mathcal{T}_i, \quad T \mapsto \alpha(T)$ Minimalpolynom p_i für $i \in \underline{2}$ hat. Insbesondere hat ${}^B\alpha^B$ Blockdiagonalgestalt für *angepasste* Basen von $\mathcal{V}$ (s.u.).
2. Ist $\mu_\alpha = \prod p_i$ mit $p_i \in K[x]$ paarweise teilerfremd, so gibt es eine α-invariante direkte Summenzerlegung $\mathcal{V} = \bigoplus_{i=1}^d \mathcal{T}_i$, sodass $\alpha_i : \mathcal{T}_i \to \mathcal{T}_i, T \mapsto \alpha(T)$ MinPoly p_i hat.

© study.woalk.de

Bemerkung 5.3.9:

$\mathcal{V} = \bigoplus_{i=1}^{d} \mathcal{T}_i$ bedeutet, dass $\forall X \in \mathcal{V}$ eindeutig schreiben lässt als $X = \sum_{i=1}^{d} X_i$ mit $X_i \in \mathcal{T}_i$.
Folgende Aussagen sind äquivalent (aus Übung 9.5):

1. $V = \bigoplus_{i=1}^{d} \mathcal{T}_i$
2. Sind B_i Basen von $\mathcal{T}_i$ mit $i \in \underline{d}$, so ist $\bigcup_{i=1}^{d} B_i$ eine Basis von $\mathcal{V}$ (eine solche Basis heißt eine **angepasste Basis** bzgl. der Zerlegung).
3. $\mathcal{V} = \langle \mathcal{T}_1, \ldots, \mathcal{T}_d \rangle = \mathcal{T}_1 + \cdots + \mathcal{T}_d =: \sum_{i=1}^{d} \mathcal{T}_i$, d.h. $\mathcal{V}$ wird durch alle $\mathcal{T}_i$ erzeugt (und es sind auch alle notwendig), und für jedes $j \in \underline{d}$ gilt: $\mathcal{T}_j \cap \left(\sum_{i \neq j} \mathcal{T}_i \right) = \{0\}$

Folgerung 5.3.12: Wurzeln und Diagonalisierbarkeit

Sei $\mathcal{V}$ ein e.e. K-VR und $\alpha \in \operatorname{End}(\mathcal{V})$ mit MinPoly vom Grad d. $\exists$ Eigenvektorbasis von α (also α diagonalisierbar), wenn das MinPoly genau d verschiedene Wurzeln hat: $s_1, \ldots, s_d$, also muss $\mu_\alpha = \prod_{i=1}^{d} (x - s_i)$ die Gestalt vom MinPoly sein.

Beispiel 5.3.13: MinPoly für Dreiecksmatrizen

Für $A = \begin{pmatrix} a_1 & & * \\ & a_2 & \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$ (obere Dreiecksmatrix) mit $a_1, a_2, \ldots, a_n$ *paarweise verschieden* ist $\mu_A = \prod_{i=1}^{n} (x - a_i)$ und A ist diagonalisierbar, also ähnlich zu $\operatorname{Diag}(a_1, \ldots, a_n)$.

Wegen der Invarianz unter Transponieren gilt dies auch für $A = \begin{pmatrix} a_1 & & 0 \\ & a_2 & \\ & \ddots & \\ * & & a_n \end{pmatrix}$ (untere Dreiecksmatrix).

5.4 Determinanten

Sei im Rest dieses Kapitels $\mathcal{V}$ ein K-VR der Dimension n und $B \in \mathcal{V}^n$ eine Basis von $\mathcal{V}$.

Definition 5.4.1: „Wunschliste“

Die (bzgl. B normierte) **Determinante** von $\mathcal{V}$ ist eine Abbildung

$$\det_B : \mathcal{V}^n \to K, \quad (V_1, \ldots, V_n) \mapsto \det_B(V_1, \ldots, V_n)$$

mit folgenden Eigenschaften:

1. $\det_B$ ist **multilinear** (linear in jeder Komponente), d.h.

$$\begin{aligned} &\det_B(X_1, \ldots, X_{i-1}, aX_i + bX_i', X_{i+1}, \ldots, X_n) \\ &= a \det_B(X_1, \ldots, X_i, \ldots, X_n) + b \det_B(X_1, \ldots, X_i', X_n) \quad \forall X \in \mathcal{V}^n,\ i \in \underline{n},\ X' \in \mathcal{V}^n \end{aligned}$$

2. $\det_B$ ist **alternierend**, d.h. $\det_B(X) = 0\ \forall X \in \mathcal{V}^n$ mit $\exists i, j \in \underline{n},\ i \neq j : X_i = X_j$.
3. $\det_B$ ist **normiert**, d.h. $\det_B(B) = 1$.

Lemma 5.4.7:

Ist $X \in \mathcal{V}^n$ und $\pi \in \mathrm{S}_n$, so gilt: $\det_B(X \circ \pi) = \det_B(X) \cdot \operatorname{sign} \pi$

© study.woalk.de

Satz 5.4.8: Eindeutigkeit der Determinante

Falls eine Determinante auf $\mathcal{V}$ mit Normierung bzgl. Basis B existiert, ist sie eindeutig bestimmt.
Beweis: Sie ist definiert für $X \in \mathcal{V}^n$ durch $\det_B(X) = \sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} {}^B(X_i)_{\pi(i)}$

Satz 5.4.9: Existenz der Determinante

Die angegebene Formel ist eine alternierende Multilinearform, die bzgl. Basis B normiert ist.

Satz 5.4.10: Basiswechsel der Determinante

Sind $B, B' \in \mathcal{V}^n$ Basen von $\mathcal{V}$, gilt: $\det_{B'} = (\det_B(B'))^{-1} \det_B$

Satz 5.4.11: Linearitäten der Determinante

1. Sei $X \in \mathcal{V}^n, 1 \leq k \leq n$ und das Tupel $Y : \underline{n} \to \mathcal{V}, \quad i \mapsto \begin{cases} X_i & i \neq 0 \\ X_k + Z & i = k \end{cases}$
   für $Z \in \langle X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n \rangle$. Dann ist $\det_B(X) = \det_B(Y)$.
   In Worten: Man kann andere Vektoren aus X zu einem Vektor aus X addieren, ohne die Determinante zu ändern. (folgt aus Linearität)
2. $X \in \mathcal{V}^n$ ist genau dann linear abhängig, wenn $\det_B(X) = 0$.

Definition 5.4.12/13: Determinante einer Matrix

Sei $A \in K^{n \times n}$. Dann setzt man $\det(A) := \det_E(A_{-,1}, \ldots, A_{-,n})$ mit $E = (e_1, \ldots, e_n)$.
Es ist $\det(A) = \sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} A_{\pi(i),i}$

Beispiel 5.4.13: Einfache Determinanten

2. $\det\left(\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}\right) = a_1 b_2 - a_2 b_1$
3. $\det\left(\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}\right) = a_1 b_2 c_3 + a_3 b_1 c_2 + a_2 b_3 c_1 - a_1 b_3 c_2 - a_3 b_2 c_1 - a_2 b_1 c_3$

Satz 5.4.15: Eigenschaften von Matrixdeterminanten

1. Für $A \in K^{n \times n}$ gilt $\det(A) = \det(A^{\mathrm{tr}})$.
2. Für $A \in K^{n \times n}$ gilt: A invertierbar $\Leftrightarrow \det(A) \neq 0$.
3. Für $A_1, A_2 \in K^{n \times n}$ gilt: $\det(A_1 \cdot A_2) = \det(A_1) \det(A_2)$
4. Für $A \in K^{n \times n}$ und $g \in \mathrm{GL}_n(K)$ ist $\det(g^{-1} A g) = \det(A)$.
5. Sei $\alpha \in \operatorname{End}(\mathcal{V})$, $\mathcal{V}$ e.e. mit B Basis von $\mathcal{V}$. Dann setze $\det(\alpha) := \det({}^B\alpha^B)$, $\operatorname{Spur}(\alpha) := \operatorname{Spur}({}^B\alpha^B)$.

$\xrightarrow[5.4.16]{}$ Die Einschränkung von $\det$ auf $\mathrm{GL}_n(K)$ bildet auf K^* ab und ist ein Gruppenhomomorphismus mit $\operatorname{Kern}(\det) =: \mathrm{SL}_n(K)$, die **speziellen linearen Abbildungen** mit Determinante 1 („Volumenerhaltend“).

© study.woalk.de

Bemerkung 5.4.17: Rechenregeln für Matrixdeterminanten

Sei $A \in K^{n\times n}$.

1. $\det A$ ändert sich *nicht*, wenn man ein *Vielfaches* einer Spalte (Satz 5.4.11.1) oder Zeile (Satz 5.4.15.1) zu einer anderen hinzuaddiert.
2. Es gilt: $\det\begin{pmatrix} a_1 & * & \cdots & * \\ 0 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & a_n \end{pmatrix} = a_1 \cdot a_2 \cdots a_n$
3. $detA$ multipliziert sich mit (-1), wenn man zwei Spalten oder zwei Zeilen vertauscht, *jedes Mal* (alternierend).
4. Entsteht A' aus A durch Multiplikation einer Spalte oder Zeile mit $a \in K$, ist $\det A' = a \cdot \det A$. Insbesondere ist $\det(aA) = a^n \det A$.
5. Zur Berechnung der Determinante bringt man sie mit Hilfe des **Gauß-Algorithmus** (Zeilen- oder Spalten-Gauß) unter Beachtung von (3) und (4) in (einfache) Stufenform, dann benutze (2).

Für $k+l=n$, $A_1 \in K^{k\times k}$, $A_2 \in K^{l\times l}$, $A_3 \in K^{l\times k}$ ist $\det\begin{pmatrix} A_1 & 0 \\ A_3 & A_2 \end{pmatrix} = \det(A_1)\det(A_2)$.

Satz 5.4.19: Laplace'scher Entwicklungssatz *nach einer Spalte*

Für $A \in K^{n\times n}$, $i,j \in \underline{n}$ sei $A^{(i,j)} \in K^{(n-1)\times(n-1)}$ die Matrix, die aus A durch Streichen der i-ten Zeile und j-ten Spalte entsteht, die **gestürzte Matrix**.
Dann gilt für $k \in \underline{n}$: $\det A = \sum_{i=1}^{n} A_{i,k} \cdot (-1)^{i+k} \det\left(A^{(i,k)}\right)$.
Entwicklung nach einer Zeile ist analog.

Laplace + Gauß hat eine gute Laufzeit!

Satz 5.4.21: Cramer'sche Regel *(mehr theoretischer Nutzen)*

Ist $A \in K^{n\times n}$ vom Höchstrang, also $\det A \neq 0$, und $b \in K^{n\times 1}$ beliebige Spalte, dann ist die eindeutige Lösung des LGS $Ax=b$ für $x \in K^{n\times 1}$ gegeben durch $X_{i,1} = \frac{\det\left(A^{i,b}\right)}{\det A}$ mit $i \in \underline{n}$, wobei $A^{i,b}$ dieselben Spalten wie A hat, außer in der i-ten Spalte, dort steht b.

Folgerung 5.4.22: Inverse durch Determinante

Für $A \in \mathrm{GL}_n(K)$ ist $(A^{-1})_{i,j} = \frac{(-1)^{i+j}\det\left(A^{(i,j)}\right)}{\det A}$.
Die Matrix $\left((-1)^{i+j}\det\left(A^{(i,j)}\right)\right)_{i,j}$ heißt **Matrix der Kofaktoren** von A.
Ist B die Matrix der Kofaktoren, ist $AB = \det(A)\cdot I_n$ („fast die Inverse").

© study.woalk.de

5.5 Charakteristisches Polynom

Für das Behandeln allgemeinerer Fälle, wo $\operatorname{Grad}\mu_A < \operatorname{Grad}\mathcal{V}$ ist und daher μ_A nicht als Invariante ausreicht, um einfache Blockdiagonalgestalt zu erhalten.

Definition 5.5.1: Charakteristisches Polynom

1. Sei $A \in K^{n\times n}$. Das **charakteristische Polynom** von A ist $\chi_A(x) = \det(xI_n - A) \in K[x]$.
   $xI_n - A \in K[x]^{n\times n} \subset K(x)^{n\times n}$, damit wieder in einem Körper, daher darf man $\det$ benutzen.
2. Sei $\mathcal{V}$ ein e.e. K-VR und $\alpha \in \operatorname{End}(\mathcal{V})$. Dann heißt $\chi_\alpha(x) := \det(xI_n - {}^B\alpha^B)$ das **charakteristische Polynom** von α, wobei B eine beliebige Basis von $\mathcal{V}$ ist (nach Lemma 5.5.2 ist χ_α unabhängig von B und wohldefiniert).

Bemerkung 5.5.3: Rechenregeln für das charakteristische Polynom

1. Ist $A = \operatorname{Diag}(a_1, \ldots, a_n)$ mit $a \in K^n$, so ist $\chi_A = \prod_{i=1}^n (x - a_i)$.
   Sind die a_i paarweise verschieden, so ist $\chi_A = \mu_A$.
2. Ist $A = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}$ mit A_i quadratischen Matrizen (Blockdreiecksm.), so ist $\chi_A = \chi_{A_1}\chi_{A_2}$.
3. Ähnliche Matrizen haben das gleiche charakteristische Polynom. Damit haben wir *noch eine* Invariante der Ähnlichkeitsklassen!
4. Ist A diagonalisierbar, so ist $\chi_A = \prod_{a\in\mathrm{EW}(A)} (x-a)^{\dim E_A(a)}$, wobei $\mathrm{EW}(A)$ die Menge der Eigenwerte von A ist.

Übung „letzte“:

Ist $A = aI_n + bJ_n$ mit $b \neq 0$ und $J_n \in K^{n\times n}$, $(J_n)_{i,j} = 1\ \forall i,j \in \underline{n}$, so gilt:
J_n und A sind diagonalisierbar wenn $n1_K \neq 0$.
In diesem Fall ist $\mathrm{EW}(A) = \{a+nb,\ a\}$ und die Dimension der ERe ist 1 bzw. $n-1$.
Also ist $\chi_A = (x-(a+nb))(x-a)^{n-1}$ und $\mu_A = (x-(a+nb))(x-a)$.

Satz 5.5.4: Wichtigste Eigenschaften des charakteristischen Polynoms

Sei $\mathcal{V}$ ein e.e. K-VR und $\operatorname{End}(\mathcal{V})$. Dann gilt:

1. $\chi_\alpha(x) \in K[x]$ ist normiert vom Grad $n = \dim\mathcal{V}$. Der Koeffizient von x^{n-1} ist gleich $-\mathrm{Spur}(\alpha)$ und der Koeffizient von x^0 ist $(-1)^n \det(\alpha)$.
2. $a \in K$ ist EW von $\alpha \Leftrightarrow \chi_\alpha(a) = 0$, d.h. falls $a \in K$ eine Wurzel von $\chi_\alpha(x)$ ist. Also haben μ_α und χ_α die gleichem Wurzeln.
3. **Cayley-Hamilton:** $\chi_\alpha(\alpha) = 0$, d.h. $\mu_\alpha \mid \chi_\alpha$
   $\xrightarrow[5.5.5]{}$ Ist $p \in K[x]$ normiert von Grad $n = \dim\mathcal{V}$ und $A = M_p$, dann gilt: $\chi_A = \mu_A = p$.
   Allgemeiner: Wegen $\mu_A \mid \chi_A \Rightarrow \chi_A = \mu_A \Leftrightarrow \operatorname{Grad}\mu_A = \dim\mathcal{V}$

© study.woalk.de

Umformulierung von Satz 5.3.8:

Bemerkung 5.5.6: Zerlegung in Haupträume

Sei $\mathcal{V}$ ein e.e. K-VR und $\alpha \in \operatorname{End}(\mathcal{V})$.
Schreibe das MinPoly $\mu_\alpha = \prod_{i=1}^{l} p_i^{m_i}$ mit p_i irreduzibel, normiert und paarweise verschieden (vgl. Primfaktorzerlegung!).
Setzt man $q_i := \prod_{j \neq i} p_j^{m_j}$ so ist $\operatorname{ggT}(q_1, \ldots, q_l) = 1$.
Schreibt man die 1 als $1 = a_1 q_1 + \cdots + a_l q_l \in K[x]$ (Bézout), so sind die $\pi_i = a_i(\alpha)\, q_i(\alpha)$ mit α vertauschbare Projektionen, die folgendes erfüllen:

$$\pi_i \circ \pi_j = \delta_{ij} \pi_i, \ \mathrm{id}_{\mathcal{V}} = \pi_1 + \cdots + \pi_l$$

Die Teilräume $\mathcal{U}_i := \operatorname{Bild} \pi_i$ sind α-invariante TRe von $\mathcal{V}$, die wir auch **Haupträume** nennen wollen.
Genauer: $\mathcal{U}_i$ ist Hauptraum zum Faktor p_i.
Es gilt: $\mathcal{V} = \bigoplus_i \mathcal{U}_i$ und für $\alpha_i = \alpha_{||\mathcal{U}}$ (sowohl im Def.-, als auch im Wertebereich eingeschränkt auf $\mathcal{U}$) ist $\mu_{\alpha_i} = p_i^{m_i}$.
Das MinPoly μ_α teilt sicherlich $p_i^{m_i}$, da $\left(p_i^{m_i}\right)(\alpha)_{|\mathcal{U}_i} = 0$. Andererseits teilt μ_α das Produkt $\prod_{i=1}^{l} \mu_{\alpha_i}$ und somit muss $\mu_{\alpha_i} = p_i^{m_i}$.
Daher gilt: $\mathcal{U}_i = \operatorname{Kern}\left(p_i^{m_i}(\alpha)\right) = \operatorname{Bild}\left(q_i(\alpha)\right)$
$\Rightarrow$ Bézout überflüssig.
Ist B_i eine Basis von $\mathcal{U}_i$ ($1 \leq i \leq l$), so ist $B = (B_1, \ldots, B_l)$ eine Basis von $\mathcal{V}$ und

$${}^{B}\alpha^{B} = \begin{pmatrix} {}^{B_1}\alpha_1{}^{B_1} & & 0 \\ & \ddots & \\ 0 & & {}^{B_l}\alpha_l{}^{B_l} \end{pmatrix}$$

Satz 5.5.7:

Sei $\alpha \in \operatorname{End}(\mathcal{V})$ mit $\mu_\alpha = p^m$ für ein irreduzibles, normiertes $p \in K[x]$. Dann gibt es Zahlen $1 \leq m_1, m_2, \ldots, m_s \leq m$ und eine Basis B von $\mathcal{V}$, sodass

$${}^{B}\alpha^{B} = \begin{pmatrix} M_{p^{m_1}} & & * \\ & \ddots & \\ 0 & & M_{p^{m_s}} \end{pmatrix}$$

mit einem $m_i = m$.
Insbesondere gilt: $d := \operatorname{Grad} p \mid \operatorname{Dim} \mathcal{V} =: n$ und $\chi_A = p^c$ mit $c = m_1 + \cdots + m_s = \frac{n}{d} \geq m$

© study.woalk.de