Skript zur Vorlesung

Lineare Algebra I

bei Professor Pahlings

Wintersemester 1999/2000

RWTH Aachen

verfaßt von

Sandip Sar-Dessai

Dieses Dokument wurde erstellt mit LyX Version 1.1.6fix1 und enthält die Vorlesungsinhalte der Vorlesung "*Lineare Algebra I*" bei Professor Pahlings im WS 1999/2000 an der RWTH-Aachen.

An dieser Stelle möchte ist ganz besonders Carsten Fuhs danken, der sich die Zeit genommen hat, das Skript komplett durchzusehen und zu korrigieren. Dank seiner Hilfe dürfte die aktuelle Version wesentlich weniger Fehler enthalten als die letzte.

Die aktuelle Version dieses Dokuments läßt sich jederzeit von meiner Homepage runterladen.

Für Kritik, Verbesserungsvorschläge und insbesondere Korrekturen bin ich jederzeit offen.

Sandip Sar-Dessai

Download und Kontakt
Homepage: `http://www.sandip.de`
E-Mail: `mails@sandip.de`

3. Auflage, 1. Oktober 2001

Inhaltsverzeichnis

1 Grundlagen **1**

1.1 Mengen und Abbildungen . . . 1

1.1.1 Mengen . . . 1

1.1.2 Abbildungen . . . 2

1.2 Äquivalenzrelationen . . . 4

1.2.1 Äquivalenzklassen . . . 4

1.2.2 Potenzmengen und Partitionen . . . 5

1.3 Körper und Ringe . . . 5

1.3.1 Die Kongruenzklasse $a \mod m$ . . . 7

1.4 Elementare Umformungen . . . 8

1.4.1 Der Gauß-Algorithmus . . . 8

1.4.2 Matrizen . . . 9

1.5 Matrizenrechnung . . . 11

2 Vektorräume **14**

2.1 Definition und Beispiele . . . 14

2.2 Teilräume . . . 15

2.3 Linearkombinationen und Erzeugendensysteme . . . 17

2.3.1 Linearkombinationen . . . 17

2.3.2 Erzeugendensysteme und Basen . . . 18

2.4 Lineare Abhängigkeit und Basen . . . 19

2.4.1 Lineare Abhängigkeit und Unabhängigkeit . . . 19

2.4.2 Basen und Teilräume sowie Teilmengen . . . 20

2.5 Existenz von Basen . . . 21

2.5.1 Basisergänzungssatz . . . 21

2.5.2 Folgerungen aus dem Basisergänzungssatz . . . 21

2.6 Austauschsatz und Dimension . . . 23

2.6.1 Der Austauschsatz von Steinitz . . . 23

2.6.2 Dimension von Vektor- und Teilräumen . . . 23

3 Lineare Abbildungen **26**
3.1 Lineare Abbildungen 26
3.2 Isomorphismen 28
3.3 Kern und Bild 30
3.4 Homomorphiesatz 32
3.5 Rang einer Matrix 33
3.6 Hauptsatz über lineare Gleichungssysteme 34
3.7 Matrix einer linearen Abbildung 36
3.8 Algebra der linearen Abbildungen 39
3.9 Volle lineare Gruppen 40

4 Determinanten **43**
4.1 Permutationen 43
4.2 Determinanten 45
4.3 Eigenschaften der Determinante 49
4.4 Polynomringe 52
4.5 Polynome über Körpern, Nullstellen 54

5 Eigenwerte und Diagonalisierbarkeit **56**
5.1 Eigenwerte 56
5.2 Das charakteristische Polynom 58
5.3 Minimalpolynom 61
5.4 φ-invariante Teilräume 63
5.5 Die Jordansche Normalform 66

6 Bilinearformen und Skalarprodukte **68**
6.1 Der Dualraum 68
6.2 Bilinearformen 71
6.3 Orthogonalität 73
6.4 Orthogonalisierung 75
6.5 Euklidische Vektorräume 78

Kapitel 1

Grundlagen

1.1 Mengen und Abbildungen

1.1.1 Mengen

Definition 1 (Menge, Element) Eine *Menge* ist eine Zusammenfassung wohlunterschiedener Objekte. Die Objekte heißen dabei *Elemente* der Menge.

Sei M eine Menge. Dann gilt für beliebige x:

- $x \in M$: x ist Element der Menge M.
- $x \notin M$: x ist kein Element von M.

Bemerkung: Es darf nicht gleichzeitig $x \in M$ und $x \notin M$ gelten.

Besondere Zahlmengen

$\mathbb{N}$	Menge der natürlichen Zahlen	$\mathbb{N} = \{1;2;3;\ldots\}$
$\mathbb{Z}$	Menge der ganzen Zahlen	$\mathbb{Z} = \{0;1;-1;2;-2;\ldots\}$
$\mathbb{Q}$	Menge der rationalen Zahlen	$\mathbb{Q} = \left\{\frac{a}{b} \middle| a \in \mathbb{Z} \wedge b \in \mathbb{N}\right\}$
$\mathbb{R}$	Menge der reellen Zahlen	

Darstellung von Mengen

- Aufzählung:
  Beispiel: $M = \{1;2;3;5;7;11\} = \{2;1;3;7;5;11\} = \left\{2;11;\frac{3}{1};\frac{14}{2};5;1\right\}$
- Definition durch ihre Eigenschaft:
  Beispiele: $P = \{x \in \mathbb{N} \,|\, x \text{ ist eine Primzahl}\}$; $M = \{x \in P \,|\, x \leq 11\}$

Operatoren

- $A \subseteq B$: A ist Teilmenge von B; es gilt: wenn $a \in A \Rightarrow a \in B$
- $A = B$: A ist gleich B; es gilt: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

- $A \cap B$: Durchschnitt von A und B; es gilt: $A \cap B = \{x \,|\, x \in A$ und $x \in B\}$
- $A \cup B$: Vereinigung von A und B; es gilt: $A \cup B = \{x \,|\, x \in A$ oder $x \in B\}$
- $A \setminus B$: Differenzmenge von A und B; es gilt: $A \setminus B = \{x \,|\, x \in A$ und $x \notin B\}$
- $A \times B$: Cartesisches Produkt; es gilt: $A \times B = \{(a,b) \,|\, a \in A$ und $b \in B\}$
  Falls $(a,b) = (a',b')$, dann gilt $a = a'$ und $b = b'$.

Bemerkungen:

- $\emptyset$ ist die leere Menge; es gilt: $x \notin \emptyset$ für alle x.
- Für jede Menge A gilt: $\emptyset \subseteq A$.
- Der Durchschnitt zweier Mengen kann leer sein. In diesem Fall heißen A und B disjunkt.
- Ist $A \cup B = \emptyset$, dann gilt sowohl $A = \emptyset$ als auch $B = \emptyset$.

1.1.2 Abbildungen

Definition 2 (Abbildung, Funktion) Sind X und Y Mengen und ist $f \subseteq X \times Y$, so heißt (X,Y,f) *Abbildung* von X nach Y, wenn es zu jedem $x \in X$ genau ein $y \in Y$ gibt mit $(x,y) \in f$. In diesem Falle schreibt man:

$$f: \begin{array}{ccc} X & \longrightarrow & Y \\ x & \longmapsto & y = f(x) \end{array}$$

Zwei Abbildungen $f: X \longrightarrow Y$, $g: A \longrightarrow B$ sind gleich genau dann, wenn:

- $X = A$ (Definitionsbereich ist gleich)
- $Y = B$ (Zielbereich ist gleich)
- für alle $x \in A = X$ gilt: $f(x) = g(x)$

Ein Synonym für "Abbildung" ist "*Funktion*".

Definition 3 (Mächtigkeit einer Menge) $|M|$ ist die *Anzahl der Elemente* (oder *Mächtigkeit*) der Menge M, wenn sie endlich ist, sonst ∞.

Definition 4 (Injektivität, Surjektivität, Bijektivität) Die Funktion $f: X \longrightarrow Y$ heißt...

- ...*injektiv*, wenn aus $f(x) = f(x')$ folgt $x = x'$.
- ...*surjektiv*, wenn es zu jedem $y \in Y$ ein $x \in X$ gibt mit $f(x) = y$.
- ...*bijektiv*, wenn f injektiv und surjektiv ist.

Beispiele:

- Es gilt: $\left|\left\{1, 2, \frac{4}{2}\right\}\right| = |\{1,2\}| = 2$
- Die identische Abbildung $id_X: \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & x \end{array}$ ist bijektiv.

- $f_1 : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array}$ ist weder injektiv noch surjektiv.
- $f_2 : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^{\geq 0} \\ x & \longmapsto & x^2 \end{array}$ ist nicht injektiv, aber surjektiv.
- $f_3 : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{1}{x} \end{array}$ ist keine Fkt., da $(0, y) \notin f_3$ für alle y.
- $f_4 : \begin{array}{ccc} \mathbb{R}^{>0} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array}$ ist injektiv, aber nicht surjektiv.
- $f_5 : \begin{array}{ccc} \mathbb{R}^{\geq 0} & \longrightarrow & \mathbb{R} \\ x^2 & \longmapsto & x \end{array}$ ist keine Funktion, da sie nicht wohldefiniert ist; $x = x' \not\Rightarrow f(x) = f(x')$ gilt nicht, denn $(1, 1) \in f_6$ und $(1, .1) \in f_6$.

Definition 5 (Bild, Urbild, Faser) Sei $f : X \longrightarrow Y$ eine Abbildung und sei $X' \subseteq X$ sowie $Y' \subseteq Y$. Dann ist...

- ...$f(X') = \{ f(x') \,|x' \in X' \}$ das *Bild* von X' unter f, $f(X)$ heißt das Bild von f.
- ... $\overset{-1}{f}(Y') = \{x \in X \,|\, f(x) \in Y'\}$ das *Urbild* von Y' unter f.
- ... $\overset{-1}{f}(y) = \overset{-1}{f}(\{y\}) = \{x \in X \,|\, f(x) = y\}$ die *Faser* von y unter f.

Bemerkungen:

- $f : X \longrightarrow Y$ ist injektiv $\Leftrightarrow \left| \overset{-1}{f}(y) \right| \leq 1, y \in Y$
- $f : X \longrightarrow Y$ ist surjektiv $\Leftrightarrow \left| \overset{-1}{f}(y) \right| \geq 1, y \in Y$
- $f : X \longrightarrow Y$ ist bijektiv $\Leftrightarrow \left| \overset{-1}{f}(y) \right| = 1, y \in Y$

Definition 6 (Verkettung) Sind $f : X \longrightarrow Y$ und $f : Y \longrightarrow Z$ Abbildungen. Dann sei

$$g \circ f : \begin{array}{ccc} X & \longrightarrow & Z \\ x & \longmapsto & g(f(x)) \end{array}$$

die *verkettete Abbildung*.

Satz 1 Sind $f : A \longrightarrow B$, $g : B \longrightarrow C$ sowie $h : C \longrightarrow D$ Abbildungen. Dann gilt:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Beweis: Der Definitionsbereich von $h \circ (g \circ f)$ und $(h \circ g) \circ f$ ist A. Der Zielbereich beider Abbildungen ist D. Es gilt für jedes $x \in A$:

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = ((h \circ g) \circ f)(x)$$

$\square$

1.2 Äquivalenzrelationen

Sei M eine Menge.

Definition 1 (Relation) Eine Teilmenge $R = \{(a,b)\,|\,a,b \in M\} \subseteq M \times M$ heißt auch *Relation* auf M. Dann schreibt man auch aRb statt $(a,b) \in R$.

Definition 2 (Reflexivität, Symmetrie, Transitivität, Äquivalenzrelation) Sei $R = \{(a,b)\,|\,a,b \in M\} \subseteq M \times M$ eine Relation. Dann heißt R...

- ...*reflexiv*, wenn aRa für alle $a \in M$ gilt.
- ...*symmetrisch*, wenn aus aRb folgt bRa für alle $a,b \in M$.
- ...*transitiv*, wenn aus aRb und bRc folgt aRc für alle $a,b,c \in M$.
- ...*Äquivalenzrelation*, wenn R reflexiv, symmetrisch und transitiv ist.

Beispiele:

- $R_= = \{(a,a)\,|\,a \in M\} \subseteq M \times M$ ($aR_=b \Leftrightarrow a = b$) ist Äquivalenzrelation.
- $M = \mathbb{Z}$, $q \in \mathbb{N}$; $R_q = \{(a, a+qx)\,|\,x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$ ist Äquivalenzrelation.

1.2.1 Äquivalenzklassen

Definition 3 (Äquivalenzklasse) Ist $\sim$ eine Äquivalenzrelation auf M, so sei für $a \in M$

$$[a]_\sim = \{b \in M\,|\,a \sim b\}$$

Äquivalenzklasse von a bezüglich $\sim$.

Lemma 1 Sei $\sim$ Äquivalenzrelation auf M

1. $a \sim b \Leftrightarrow [a]_\sim = [b]_\sim$
2. (Zwei) Äquivalenzklassen sind gleich oder disjunkt.
3. Jedes $a \in M$ liegt in einer Äquivalenzklasse.

Beweis:

1. "$\Rightarrow$": Es sei $a \sim b$ in M. Zu zeigen ist: Es gilt $[a]_\sim = [b]_\sim$
   (a) $[a]_\sim \subseteq [b]_\sim$: Es sei $x \in [a]_\sim$ beliebig, zu zeigen ist dann $x \in [b]_\sim$
   Zunächst ist $a \sim x$. Aus $a \sim b$ (Vorr.) folgt $b \sim a$ (Symmetrie). Aus $b \sim a$ und $a \sim x$ folgt $b \sim x$ (Transitivität), was bedeutet, daß $x \in [b]_\sim$.
   (b) $[b]_\sim \subseteq [a]_\sim$: Da auch $b \sim a$ (Symmetrie) folgt aus dem Bewiesenen: $[b]_\sim \subseteq [a]_\sim$.
   (c) Aus (a) und (b) folgt: $[a]_\sim = [b]_\sim$.

   "$\Leftarrow$": Sei $[a]_\sim = [b]_\sim$, zu zeigen ist $a \sim b$.
   Da $b \sim b$ (Reflexivität) ist $b \in [b]_\sim$; da $[b]_\sim = [a]_\sim$ ist auch $b \in [a]_\sim$, d.h. $a \sim b$. $\square$
2. Wir zeigen: $[a]_\sim \cap [b]_\sim \neq \emptyset \Rightarrow [a]_\sim = [b]_\sim$.
   Sei $[a]_\sim \cap [b]_\sim \neq \emptyset$. Es gibt also $x \in [a]_\sim \cap [b]_\sim$, d.h. $a \sim x$ und $b \sim x$. Nach (1) gilt dann $[a]_\sim = [x]_\sim$ und $[b]_\sim = [x]_\sim$, also $[a]_\sim = [b]_\sim$.
3. Nach (1c) gilt $a \in [a]_\sim$. $\square$

1.2.2 Potenzmengen und Partitionen

Definition 4 (Potenzmenge) M sei eine Menge. Dann heißt $P(M) = \{A \mid A \subseteq M\}$ *Potenzmenge* von M.

Bemerkung: Es gilt immer: $\emptyset \in P(M)$.

Definition 5 (Partition) $P \subseteq P(M)$ heißt *Partition* von M, wenn gilt:

1. $M = \bigcup_{A \in P} A$ (d.h. zu jedem $x \in M$ existiert ein $A \in P$ mit $x \in A$).
2. $A \cap A' = \emptyset$ für $A \neq A'$ und $A, A' \in P$

Bemerkung: Aus Lemma 1 folgt: Ist $\sim$ Äquivalenzrelation auf M, so bilden die Äquivalenzklassen bezüglich $\sim$ eine Partition von M: $M/\sim = \{[a]_\sim \mid a \in M\}$. Ist umgekehrt $P \subseteq P(M)$ eine Partition, so kann man die Äquivalenzrelation $\sim$ so definieren: $a \sim b \Leftrightarrow$ es gibt $A \in P$ mit $a, b \in A$.

Beispiel:

Sei $M = \mathbb{Z}$ und $a \equiv_m b$, $m \in \mathbb{N}$ fest, $a \equiv_m b \Leftrightarrow b - a = x \cdot m$ für $x \in \mathbb{Z}$, $b - a \in m \cdot \mathbb{Z}$. Dies ist eine Äquivalenzrelation (meistens schreibt man $a \equiv b \, mod \, m$ statt $a \equiv_m b$). Weiterhin gilt:

- $[0]_m = [0]_{\equiv_m} = \{0; m; 2m; 3m; \ldots; -m; -2m; -3m; \ldots\} = m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$
- Sei $m > 1$. $[1]_m = \{1; 1+m; 1+2m; \ldots; 1-m; \ldots\} = m \cdot \mathbb{Z} + 1 = \{mx + 1 \mid x \in \mathbb{Z}\}$
- $\mathbb{Z}_{/\equiv_m} = \{[0]_m; [1]_m; \ldots; [m-1]_m\}$ Kongruenzklassen von a modulo m

1.3 Körper und Ringe

Definition 1 (Körper) Eine Menge K zusammen mit den Abbildungen

$$+ : \begin{array}{ccc} K \times K & \longrightarrow & K \\ (a,b) & \longmapsto & a+b \end{array} \text{(genannt Addition) und } \cdot : \begin{array}{ccc} K \times K & \longrightarrow & K \\ (a,b) & \longmapsto & a \cdot b \end{array} \text{(genannt Multiplikation)}$$

heißt *Körper*, wenn folgende Regeln für beliebige $a, b, c \in K$ gelten:

1. (K1) Assoziativität der Addition: $(a+b)+c = a+(b+c)$.
2. (K2) Nullelement: es existiert genau ein Nullelement $0 \in K$ mit $0 + a = a + 0 = a$.
3. (K3) Inverses der Addition: Zu jedem $a \in K$ existiert genau ein Element $-a \in K$ mit $a + (-a) = 0$.
4. (K4) Kommutativität der Addition: $a + b = b + a$.
5. (K5) Assoziativität der Multiplikation: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6. (K6) Einselement: Es existiert genau ein Einselement $1 \in K$, $1 \neq 0$, mit $1 \cdot a = a \cdot 1 = a$.
7. (K7) Inverses der Multiplikation: Zu jedem $a \in K \setminus \{0\}$ existiert genau ein $a^{-1} \in K$ mit $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
8. (K8) Kommutativität der Multiplikation: $a \cdot b = b \cdot a$.
9. (K9) Distributivgesetz: $a \cdot (b+c) = a \cdot b + a \cdot c$ und $(a+b) \cdot c = a \cdot c + b \cdot c$.

Beispiele:

- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper
- $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ sind keine Körper

Definition 2 (Ring) Eine Menge R mit Addition und Multiplikation genannten Verknüpfungen $+$ und $\cdot$ (wie beim Körper) und den Eigenschaften (K1) bis (K5) sowie (K9) heißt *Ring*. Ein Ring heißt *kommutativer Ring*, wenn zudem (K8) gilt, und *kommutativer Ring mit Eins*, wenn (K6) und (K8) gelten.

Bemerkungen:

- Jeder Körper ist erst recht ein Ring (kommutativer Ring, kommutativer Ring mit Eins).
- $(\mathbb{Z},+,\cdot)$ ist kommutativer Ring mit Eins.

Folgerung 1 In jedem Körper K gilt:

1. $0\cdot x = x\cdot 0 = 0$ für alle $x\in K$.
2. (a) $-(-x)=x$ sowie (b) $(-x)\cdot y = x\cdot(-y) = -(xy)$
3. Nullteilerfreiheit: $x\cdot y = 0 \Leftrightarrow x=0 \vee y=0$

Bemerkung: (1) und (2) gilt auch in Ringen.

Beweis:

1. $0 = 0\cdot x + (-0\cdot x) = (0+0)\cdot x + (-0\cdot x) = 0\cdot x + 0\cdot x - 0\cdot x = 0\cdot x + (0\cdot x + (-0\cdot x)) = 0\cdot x$.
2. (a) $-(-x)$ ist wegen (K3) das eindeutig bestimmte Element y mit $y+(-x) = (-x)+y = 0$. Nach Definition von $(-x)$ gilt diese Gleichung für $y=x$. Also: $-(-x)=y=x$.
(b) $-(xy)$ ist das eindeutig bestimmte Element $z\in K$ mit $z+(xy) = (xy)+z = 0$. Es gilt $(-x)y+xy = (-x+x)y = 0\cdot y = 0$ (analog $(xy)+(-x)y = 0$). Also ist $(-x)y = z = -xy$.
3. "$\Rightarrow$": wir zeigen $x\neq 0 \Rightarrow y=0$. Da $x\neq 0$, existiert nach (K7) ein $x^{-1}\in K$ mit $x\cdot x^{-1} = x^{-1}\cdot x = 1$.
Dann: $y = 1\cdot y = (x^{-1}\cdot x)\cdot y = x^{-1}\cdot(x\cdot y) = x^{-1}\cdot 0 = 0$.
"$\Leftarrow$": folgt unmittelbar aus (1) □

Beispiel:

Sei $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R} = \{(a,b)\,|a,b\in\mathbb{R}\}$. Dann ist $(\mathbb{R}^2,+,\cdot)$ mit $(a,b)+(a',b') := (a+a',b+b')$ und $(a,b)\cdot(a',b') := (a\cdot a', b\cdot b')$ ein kommutativer Ring mit Eins. Das Nullelement ist $0 := (0,0)$ und das Einselement ist $1 := (1,1)$.

Hinweis: Da $(1,0)\cdot(0,1) = (0,0) = 0$ (verstößt gegen Nullteilerfreiheit) und $(1,0)\cdot(a,b)\neq 1$ für alle $a,b\in\mathbb{R}$ ($(1,0)$ hat kein Inverses), ist K kein Körper.

Bemerkungen:

- In einem Ring $(K,+,\cdot)$ gilt stets $K\neq\emptyset$, weil nach (K2) $0\in K$.
- $K=\{0\}$ mit $+ : (0,0)\longmapsto 0$ und $\cdot : (0,0)\longmapsto 0$ ist ein kommutativer Ring, da (K1)-(K5) und (K8),(K9) erfüllt sind. K ist kein Körper, da (K6) nicht erfüllt ist (dort wird $0\neq 1$ gefordert).
- Ist $K=(K,+,\cdot)$ ein Körper, so gilt $|k|\geq 2$, denn es gibt $0,1\in K$ mit $1\neq 0$. So bildet $(\mathbb{F},0,1)$ mit $\mathbb{F}_2=\{0,1\}$ einen kleinsten Körper (0 ist Nullelement, 1 ist Einselement) mit den wie folgt definierten Verknüpfungen:

$+$	0	1	$\cdot$	0	1
0	0	1	0	0	0
1	1	0	1	0	1

1.3.1 Die Kongruenzklasse $a \bmod m$

Definition 3 (Äquivalenzrelation $\equiv_m$) Auf $\mathbb{Z}$ ist die *Äquivalenzrelation* $\equiv_m$ definiert als $\equiv_m = \{(a,b)\,|\,b-a = m\cdot z,\, m\in\mathbb{Z}\} \subseteq \mathbb{Z}\times\mathbb{Z}$. Die Äquivalenzklasse von a bzgl. $\equiv_m$ ist $[a]_m := [a]_{\equiv_m} = \{b\in\mathbb{Z}\,|\,a\equiv_m b\}$. Die *Kongruenzklasse* von $\equiv_m$ auf $\mathbb{Z}$ ist $\mathbb{Z}/_{(m)} := \mathbb{Z}/\equiv_m = \{[a]_m\,|\,a\in\mathbb{Z}\} = \{[0]_m,[1]_m,\ldots,[m-1]_m\}$.

Lemma 1 $\mathbb{Z}/_{(m)}$ wird für jedes $m\in\mathbb{N}^{>1}$ zusammen mit den wohldefinierten Abbildungen

$$+:\begin{array}{ccc}\mathbb{Z}/_{(m)}\times\mathbb{Z}/_{(m)} & \longrightarrow & \mathbb{Z}/_{(m)}\\ ([a]_m,[b]_m) & \longmapsto & [a+b]_m\end{array}\quad\text{und}\quad\cdot:\begin{array}{ccc}\mathbb{Z}/_{(m)}\times\mathbb{Z}/_{(m)} & \longrightarrow & \mathbb{Z}/_{(m)}\\ ([a]_m,[b]_m) & \longmapsto & [a\cdot b]_m\end{array}$$

zu einem kommutativen Ring mit Eins.

Beweis: Im folgenden Beweis gelte: $[a] := [a]_m$

1. $+,\cdot$ sind “wohldefiniert”
   Sei $[a]=[a']$ sowie $[b]=[b']$. Nach Def. von $\equiv_m$ folgt: $a' = a+xm$ und $b' = b+ym$ $(x,y\in\mathbb{Z})$.
   Zu zeigen ist: (a) $[a+b]=[a'+b']$ sowie (b) $[a\cdot b]=[a'\cdot b']$.
   (a) $[a'+b'] = [a+xm+b+ym] = [a+b+xm+ym] = [(a+b)+m(x+y)] = [a+b]$
   (b) $[a'\cdot b'] = [ab+aym+bxm+xym^2] = [ab+(ay+bx+xym)m] = [a\cdot b]$
2. (K1) und (K5): Assoziativität
   (K1): $([a]+[b])+[c] = \ldots = [(a+b)+c] = [a+(b+c)] = \ldots = [a]+([b]+[c])$, da $a,b,c\in\mathbb{Z}$
   (K5): $([a]\cdot[b])\cdot[c] = \ldots = [(a\cdot b)\cdot c] = [a\cdot(b\cdot c)] = \ldots = [a]\cdot([b]\cdot[c])$, da $a,b,c\in\mathbb{Z}$
3. (K2) Es existiert genau ein $\mathfrak{o} := [0]$ mit $x+\mathfrak{o} = \mathfrak{o}+x = x$ $(x\in K)$:
   $\mathfrak{o}+[a] = [0]+[a] = [0+a] = [a] = [a]+[0] = [a]+\mathfrak{o}$
   Eindeutigkeit: Habe auch $[a']$ die oben genannte Eigenschaft $x+[a'] = x$
   Dann gilt: $[a'] = [0+a'] = [0]+[a'] = [0] = \mathfrak{o}$
4. (K6) Es existiert genau ein $1 := [1]$ mit $x\cdot 1 = x$ $(x\in K)$:
   $1\cdot[a] = [1]\cdot[a] = [1\cdot a] = [a]$. Eindeutigkeit analog zu (3).
5. (K3) Es existiert zu jedem $x\in K$ ein $-x := [-x]\in K$ mit $x+(-x) = \mathfrak{o}$
   $[a]+[-a] = [a+(-a)] = [a-a] = [0] = \mathfrak{o}$
6. (K4) und (K8): Kommutativität
   (K4): $[a]+[b] = [a+b] = [b+a] = [b]+[a]$, da $a,b\in\mathbb{Z}$
   (K8): $[a]\cdot[b] = [a\cdot b] = [b\cdot a] = [b]\cdot[a]$, da $a,b\in\mathbb{Z}$
7. (K9) Distributivität
   $([a]+[b])\cdot[c] = [a+b]\cdot[c] = [(a+b)\cdot c] = [ac+bc] = [ac]+[bc] = [a][c]+[b][c]$, da $a,b,c\in\mathbb{Z}$
8. $0 = [0] \neq [1] = 1$, da $m>1$. □

Satz 1 $(\mathbb{Z}/_{(m)},+,\cdot)$ ist genau dann ein Körper, wenn $m = p$ (für eine Primzahl p).

Beweis: Im folgenden Beweis gelte: $[a] := [a]_m$

1. $\mathbb{Z}/_{(m)}$ ist Körper $\Rightarrow$ m ist Primzahl
   Beweis durch Kontraposition: Ist m keine Primzahl, ist $\mathbb{Z}/_{(m)}$ kein Körper.
   Sei m keine Primzahl $(m>1)$, d.h. $m = ab$ mit $1<a,b<m$. Dann:
   $[a]\cdot[b] = [a\cdot b] = [m] = [0] = \mathfrak{o}$, also gibt es Nullteiler und $\mathbb{Z}/_{(m)}$ ist kein Körper.

2. $m = p$ Primzahl $\Rightarrow \mathbb{Z}/_{(m)}$ ist Körper.
   Nur zu zeigen: Ist $m = p$, dann gilt auch (K7), vgl. Lemma 1.
   Sei $[a] \neq 0$, $a \in \mathbb{Z}$. $\{[a] \cdot [x] \,|\, 0 \leq x < m, x \in \mathbb{Z}\} \subseteq \mathbb{Z}/_{(m)}$.
   Zeige: Linke Seite hat genau $p = m$ Elemente, dann gilt Gleichheit, also ist $[1] \in \mathbb{Z}/_{(p)}$ mit $[1] = [a] \cdot [x]$ für ein $0 \leq x \leq m$. Es reicht zu zeigen $[a] \cdot [x] = [a] \cdot [y] \Rightarrow [x] = [y]$:
   $[ax] = [a][x] = [a][y] = [ay] \Rightarrow ax - ay = a(x-y) = p \cdot z \,(z \in \mathbb{Z})$
   Es gilt: "Teilt eine Primzahl ein Produkt ganzer Zahlen, so teilt sie einen Faktor"
   p teilt nicht a, weil $[a] \neq 0$, also teilt p die Zahl $(x - y)$, d.h. $[x] = [y]$. □

Korollar 1 Sei p eine Primzahl. Dann ist $\mathbb{F}_p := \mathbb{Z}/_{(p)}$ ein Körper mit p Elementen.

Bemerkung: Ist K ein kommutativer Ring mit Eins, dann gilt für $n \in \mathbb{N}$:

$$n \cdot 1 = 1 + 1 + \ldots + 1 = n \in K \;\; (n \,\text{Summanden})$$

1.4 Elementare Umformungen

1.4.1 Der Gauß-Algorithmus

Ein lineares Gleichungssystem über dem Körper K mit m Gleichungen und n Unbekannten $x_1, \ldots, x_n \in K$ $(m, n \in \mathbb{N})$ hat die Form:

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & +\ldots+ & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & +\ldots+ & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & +\ldots+ & a_{mn}x_n & = & b_m \end{array}$$

(im folgenden $(\star)$ genannt).

Gegeben sind $a_{ij}, b_i \in K$ mit $1 \leq i \leq m$ und $1 \leq j \leq n$. Gesucht ist die Lösungsmenge

$$L_{(\star)} = \{(x_1, \ldots, x_n) \,|\, x_i \in K \,\text{erfüllen}\, (\star)\,\}$$

Bemerkung: Die Lösungsmenge eines Gleichungssystems ändert sich nicht, wenn man...

1. ...zwei Gleichungen vertauscht
2. ...das c-fache ($c \in K$) einer Gleichung zu einer anderen addiert
3. ...eine Gleichung mit $c \neq 0 \in K$ multipliziert

Der Gaußsche Algorithmus löst ein lineares Gleichungssystem $(\star)$, in dem die Umformungen (1),(2),(3) aus obiger Bemerkung benutzt werden, um $(\star)$ zu vereinfachen, bis man die Lösungsmenge ablesen kann.

Beweis:

1. trivial
2. Zu Zeigen: $a = b \Leftrightarrow a = b$ (trivial) und $d = e \Leftrightarrow d + ca = e + cb$.
   (a) "$\Rightarrow$": Sei $a = b$ und $d = e$. Dann ist $(c, a) = (c, b)$. Da $\cdot : K \times K \longrightarrow K$ eine Abbildung ist, gilt also $ca = cb$. Weiterhin gilt $d + ca = e + cb$, da auch $+ : K \times K \longrightarrow K$ eine Abbildung ist.
   (b) "$\Leftarrow$": Folgt aus dem Bewiesenen mit $-c$ statt c.
3. $a = b, c \neq 0 \Leftrightarrow ca = cb$ ("$\Leftarrow$" da $c \neq 0$) □

1.4.2 Matrizen

Definition 1 (Matrix) Es sei K ein kommutativer Ring (oder Körper). Eine $m \times n$-*Matrix* A ist ein Schema der Form:

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

$A = [a_{ij}]_{\substack{i=1,\dots,m \\ j=1,\dots,n}} = [a_{ij}]$ mit $a_{ij} \in K$.

formaler: Eine $m \times n$-Matrix über K ist eine Abbildung

$$A: \begin{array}{ccc} \{1,\dots,m\} \times \{1,\dots,n\} & \longrightarrow & K \\ (i,j) & \longmapsto & A(i,j) = a_{ij} \in K \end{array}$$

Zum Gleichungssystem $(\star)$ gehört die “Matrix des Gleichungssystems”

$$[a_{ij}] \in K^{m \times n}$$

und die “erweiterte Matrix”

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{bmatrix} \in K^{m \times (n+1)}$$

Definition 2 (Elementare Umformungen) *Elementare Umformungen*, genauer “Zeilenumformungen” sind Abbildungen der Form:

1. $V_{ij} : K^{m \times n} \longrightarrow K^{m \times n}$ $(1 \le i \le m; 1 \le j \le m)$ vertauscht $i$te und $j$te Zeile
2. $A_{ij}(c) : K^{m \times n} \longrightarrow K^{m \times n}$ $(c \in K; i \neq j)$ addiert das c-fache der $j$ten zur $i$ten Zeile
3. $M_i(c) : K^{m \times n} \longrightarrow K^{m \times n}$ $(c \in K; c \neq 0)$ multipliziert die $i$te Zeile mit c

Definition 3 (Stufenform) Eine Matrix $A = [a_{ij}] \in K^{m \times n}$ hat *Stufenform*, wenn es ein r $(0 \le r \le m)$ gibt und, falls $r > 0$ ist, weiterhin $1 \le j_1 < \dots < j_r \le n$ existieren mit

- $a_{ij_i} = 1$ für $1 \le i \le r$
- $a_{ij} = 0$ für $1 \le i \le r$, $1 \le j \le n$ und $j \neq j_i$
- $a_{ij} = 0$ für $r < i \le m$, $1 \le j \le n$

Satz 1 Ist K ein Körper, so kann man jede Matrix $A \in K^{m \times n}$ $(m, n \in \mathbb{N})$ durch elementare Umformungen auf Stufenform bringen.

Vorbemerkung (Beweis durch vollständige Induktion): Will man eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ beweisen, so kann man das Beweisprinzip der “vollständigen Induktion” benutzen:

1. Induktionsanfang (auch Induktionsverankerung, -voraussetzung): man beweist $A(1)$
2. Induktionsschritt: für $n > 1$ zeigt man, daß aus gültigem $A(n-1)$ die Aussage $A(n)$ folgt

Beweis: Sei $A(m)$ die Aussage, daß jede Matrix $A \in K^{m\times n}$ mit $n \in \mathbb{N}$ sich durch elementare Umformungen auf Stufenform bringen läßt. Beweise $A(m)$ für alle $m \in \mathbb{N}$ durch vollständige Induktion:

1. Induktionsanfang: Sei $m = 1$. Sei weiterhin $A \in K^{1\times n}$, $A = [a_{11},...,a_{1n}]$.
   Sind alle $a_{ij} = 0$ so ist $A = [0,...,0]$ und A hat Stufenform nach Definition $r = 0$. Sonst setze $j_1 = min\{j \,|\, a_{ij} \neq 0\}$
   $$M_1(a_{1j_1}^{-1})(A) = [0,...,0,1,\star,....,\star]$$
   Beachte daß $a_{1j_1} \neq 0$, also existiert $a_{1j_1}^{-1} \in K$.
2. Induktionsschritt: Es sei $m > 1$, $A(m-1)$ gelte, weiterhin sei $A = [a_{ij}] \in K^{m\times n}$.
   Sind alle $a_{ij} = 0$, so hat A bereits Stufenform. Im verbleibenden Falle setze $j_1 := min\left\{ j \,\middle|\, a_{ij} \neq 0 \,\text{für ein}\, i \right\}$, d.h. j_1 ist die erste Spalte, in der ein von Null verschiedenes Element steht. Setze $i = min\left\{ k \,\middle|\, a_{kj_i} \neq 0 \right\}$, also $a_{ij_1} \neq 0$, $a_{ij_1}^{-1} \in K$. Dann:
   $$A_{mi}(-a_{mj_1})...A_{(i+1)i}(-a_{(i+1)j_1})M_i(a_{ij_1}^{-1})$$
   Wende dann V_{1i} an, bis man folgende Form erhält:
   $$B = \begin{bmatrix} 0 & ... & 0 & 1 & ... \\ 0 & ... & 0 & 0 & ... \\ : & : & : & : & \end{bmatrix}$$
   Sei $C \in K^{m\times n}$ die Matrix, die aus B entsteht, wenn man die erste Zeile wegläßt. Nach Induktionsannahme kann man C durch elementare Zeilenumformungen auf Stufenform bringen; wendet man diese Umformungen auf B an, so erhält man:
   $$B' = \begin{bmatrix} 0 & ... & 0 & 1 & b_{1j_2} & b_{1j_3} & ... & b_{ij_r} \\ 0 & ... & 0 & 0 & 1 & 0 & ... & : \\ 0 & ... & 0 & 0 & 0 & 1 & ... & : \\ : & & & \ddots & \ddots & \ddots & \ddots & \end{bmatrix}$$
   Wende auf B' die Umformung $A_{1r}(-b_{1j_r})...A_{13}(-b_{1j_3}) \circ A_{12}(-b_{1j_2})(B') = B''$. Dann hat B'' Stufenform. □

Bemerkung: Der Beweis ergibt einen Algorithmus zum Lösen eines linearen Gleichungssystems (LGS), der Gauß-Algorithmus oder Fang-Cheng-Algorithmus.

Satz 2 (Gauß-Algorithmus) Sei $A \in K^{m\times(n+1)}$ die erweiterte Matrix eines LGS. Bringe A durch elementare Zeilenumformungen auf die Stufenform B; das zugehörige Gleichungssystems hat die gleiche Lösungsmenge wie A.

- 1. Fall: es gibt eine Zeile i mit $a_{ij} = 0$ für $j \leq n$ und $a_{in} \neq 0$.
  Diese Zeile steht dann für $0x_1 + ... + 0x_r = b_i$. Diese Gleichung hat keine Lösung, also ist auch das LGS nicht lösbar.
- 2. Fall: es existieren $r \geq 0$ und $1 \leq j_1 < ... < j_r < n+1$, 1. Fall trifft nicht zu.
  Wähle x_k $(1 \leq k \leq n, n \neq j_i)$ beliebig. Jede Wahl bestimmt dann $x_{j_1},...,x_{j_r}$ entsprechend der entsprechenden Zeilengleichung.

1.5 Matrizenrechnung

Definition 1 (Addition, skalare Multiplikation) Es sei K ein Ring oder ein Körper sowie $A,B \in K^{m\times n}$ zwei beliebige Matrizen. Dann ist die *Addition* dieser Matrizen definiert durch:

$$+: \begin{array}{ccc} K^{m\times n} \times K^{m\times n} & \longrightarrow & K^{m\times n} \\ A,B & \longmapsto & (A+B)_{ij} := A_{ij} + B_{ij} \end{array}$$

Die *skalare Multiplikation* ist definiert durch:

$$\cdot: \begin{array}{ccc} K \times K^{m\times n} & \longrightarrow & K^{m\times n} \\ s,A & \longmapsto & (sA)_{ij} := s \cdot A_{ij} \end{array}$$

Beachte: Es können nur Matrizen mit gleicher Zeilen- und Spaltenzahl addiert werden.

Definition 2 (Multiplikation): Es sei K ein Ring. Für $A = [a_{ij}] \in K^{m\times n}$ und $B = [b_{ij}] \in K^{n\times l}$ ist die *Multiplikation* $A \cdot B = AB \in K^{m\times l}$ definiert durch

$$AB = [ab_{ij}] = a_{i1}b_{1k} + \ldots + a_{in}b_{nk}$$

Bemerkung: Um ab_{ij} auszurechnen benötigt man die $i$te Zeile von A und die $k$te Spalte von B.

Beachte: AB existiert nur, wenn die Spaltenzahl von A mit der Zeilenzahl von B übereinstimmt.

Beispiele:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 4 \\ 5 & 5 & 7 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \text{ ist nicht definiert}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \cdot 2 = \begin{bmatrix} 2 & 4 & 6 \\ 8 & 10 & 12 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 6 & 9 & 12 \end{bmatrix}$$

Bemerkung: Ein lineares Gleichungssystem

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & +\ldots+ & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & +\ldots+ & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & +\ldots+ & a_{mn}x_n & = & b_m \end{array}$$

kann man als eine Matrixgleichung $Ax = b$ schreiben mit:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}; x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}; b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Lemma 1 (Assoziativ-, Distributivgesetz) K sei ein Ring, $A \in K^{m\times n}$, $B,B' \in K^{n\times p}$, $C \in K^{p\times q}$. Dann gilt:

1. Assoziativgesetz: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$
2. Distributivgesetz: $A \cdot (B + B') = A \cdot B + A \cdot B'$
3. Distributivgesetz: $(B + B') \cdot C = B \cdot C + B' \cdot C$

Beweis:

1. Assoziativgesetz:

$$\begin{aligned}(A\cdot B)\cdot C &= (AB)_{i1}c_{i1}+...+(AB)_{ip}c_{pj}\\ &= (a_{i1}b_{1i}+...+a_{in}b_{n1})c_{1j}+...+(a_{i1}b_{1p}+...+a_{in}b_{np})c_{pj}\\ &= a_{i1}b_{1i}c_{1j}+...+a_{in}b_{n1}c_{1j}+...+a_{i1}b_{1p}c_{pj}+...+a_{in}b_{np}c_{pj}\\ &= a_{i1}(b_{1i}c_{1j}+...+b_{1p}c_{pj})+...+a_{in}(b_{n1}c_{1j}+...+b_{np}c_{pj})\\ &= a_{i1}(BC)_{1j}+...+a_{in}(BC)_{nj}\\ &= A\cdot(B\cdot C)\end{aligned}$$

   Bemerkung: Der Beweis kann kürzer geführt werden unter Verwendung von Summen. Diese Variante wurde hier jedoch weggelassen.

2. Distributivgesetz:

$$\begin{aligned}A\cdot(B+B') &= \sum_{k=1}^{n} a_{ik}(B+B')_{kj}\\ &= \sum_{k=1}^{n} a_{ik}(b_{kj}+b'_{kj})\\ &= \sum_{k=1}^{n}(a_{ik}b_{kj}+a_{ij}b'_{kj})\\ &= \sum_{k=1}^{n}(a_{ik}b_{kj})+\sum_{k=1}^{n}(a_{ij}b'_{kj})\\ &= (AB)_{ij}+(AB')_{ij}\\ &= (AB+AB')_{ij}\end{aligned}$$

   Bemerkung: Damit $A^2 = A\cdot A$ definiert ist muß $A \in K^{m\times m}$ “quadratisch” sein.

3. Distributivgesetz: Beweisführung analog zu (2). □

Bemerkung: Ist Ξ eine elementare Zeilenoperation (also von der Form V_{ij}, $A_{ij}(c)$, $M_i(c)$ mit $c \neq 0$; siehe Seite 9), dann gilt:

$$\Xi(A)\cdot B = \Xi(A\cdot B)$$

Definition 3 (Einheitsmatrix) Die *Einheitsmatrix* des $K^{m\times m}$ ist die Matrix

$$E_m = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{bmatrix} \in K^{m\times m}$$

Satz 1 Sei $A \in K^{m\times n}$. Dann gilt: $E_m \cdot A = A$.

Folgerung 1 Ist $A \in K^{m\times n}$ und Ξ elementare Zeilenoperation, so entsteht $\Xi(A)$ aus A durch Multiplikation von Links mit einer “elementaren Matrix” (einer E_m-Matrix, mit der elementare Zeilenoperationen durchgeführt wurden), nämlich mit $\Xi(E_m)$, denn $\Xi(A) = \Xi(E_m\cdot A) = \Xi(E_m)\cdot A$.

Satz 2 K sei ein Ring mit Eins, dann ist für $n \in \mathbb{N}$ der $K^{n\times n}$ mit der Matrixaddition und der Matrixmultiplikation

$$+ : K^{n\times n} \times K^{n\times n} \longrightarrow K^{n\times n} \quad \cdot : K^{n\times n} \times K^{n\times n} \longrightarrow K^{n\times n}$$

ein Ring mit Eins. $K^{n\times n}$ ist für $n > 1$ nicht kommutativ (d.h. $AB = BA$ gilt nicht immer).

Beweis: Seien $A, B, C \in K^{n\times n}$. Dann gilt:

1. (K1): $(A+B)+C = \begin{bmatrix} a_{11}+b_{11}+c_{11} & \dots & a_{1n}+b_{1n}+c_{1n} \\ \vdots & & \vdots \\ a_{n1}+b_{n1}+c_{n1} & \dots & a_{nn}+b_{nn}+c_{nn} \end{bmatrix} = A+(B+C)$
2. (K2) Nullelement ist $\mathfrak{o} := \begin{bmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{bmatrix}$. Dann gilt: $A+\mathfrak{o} = A = \mathfrak{o}+A$.
3. (K3) Zu $A = [a_{ij}] \in K^{n\times n}$ setze $-A = \begin{bmatrix} -a_{11} & \dots & -a_{1n} \\ \vdots & & \\ -a_{n1} & \dots & -a_{nn} \end{bmatrix}$. Dann gilt: $A+(-A) = \mathfrak{o}$.
4. (K4) $(A+B)_{ij} = a_{ij}+b_{ij} = b_{ij}+a_{ij} = (B+A)_{ij}$
5. (K5) $(A\cdot B)\cdot C = A\cdot(B\cdot C)$, vergleiche Lemma 1 (Seite 11).
6. (K6) Einselement in $K^{n\times n}$ ist $\mathfrak{1} := E_n$. Dann gilt: $E_n \cdot A = A \cdot E_n = A$.
7. (K9) Distributivgesetze gelten, vergleiche Lemma 1 (Seite 11). $\square$

Kapitel 2

Vektorräume

2.1 Definition und Beispiele

Definition 1 (Vektorraum, K-Modul) Ist K ein Körper, so ist ein K-*Vektorraum* (Vektorraum über K) eine Menge V mit den Abbildungen

$$+ : \begin{array}{ccc} V \times V & \longrightarrow & V \\ (v,w) & \longmapsto & v+w \end{array} \quad \text{und } \cdot : \begin{array}{ccc} K \times V & \longrightarrow & V \\ (s,v) & \longmapsto & s \cdot v \end{array}$$

für die die folgenden Regeln gelten ($u,v,w \in V$, $s,s_1,s_2 \in K$)

1. (V1) Assoziativität der Addition: $(u+v)+w = u+(v+w)$.
2. (V2) Existenz eines Nullelements: Es existiert $0 \in V$ mit $0+v = v = v+0$.
3. (V3) Existenz eines Inversen der Addition: Für jedes $v \in V$ existiert ein $-v \in V$ mit $v+(-v) = (-v)+v = 0$.
4. (V4) Kommutativität der Addition: $v+w = w+v$.
5. (V5) Assoziativität der skalaren Multiplikation: $(s_1 \cdot s_2) \cdot v = s_1 \cdot (s_2 \cdot v)$.
6. (V6) Existenz eines skalaren Einselements: Es existiert $1 \in K$ mit $1 \cdot v = v$[1].
7. (V7) Distributivgesetz: $s \cdot (v+w) = sv+sw$.
8. (V8) Distributivgesetz: $(s_1+s_2) \cdot v = s_1 v + s_2 v$.

Die Elemente aus V heißen Vektoren, die Elemente aus K Skalare. Ist K kein Körper, sondern nur ein Ring mit Eins mit (V1) bis (V8), so heißt V ein K-*Modul*.

Beispiele:

- K Körper, $m,n \in \mathbb{N}$. Dann ist $K^{m \times n}$ ein K-Vektorraum, es gelten die Matrix-Verknüpfungen der Addition und skalaren Multiplikation.
  Speziell ist $K^{n\times 1} = \left\{ \left[\begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \right] \middle| x_i \in K \right\}$ ein Vektorraum (bspw. $\mathbb{R}^{2\times 1} = \left\{ \left[\begin{array}{c} a \\ b \end{array} \right] \middle| a,b \in \mathbb{R} \right\}$).

[1] Dieses Einselement 1 ist das Einselement von K.

- Ist K ein Körper, dann ist K auch K-Vektorraum.
- Sei $M \neq \emptyset$ eine beliebige Menge, K ein Körper. Dann ist

  $$K^M := Abb(M,K) = \{ f : M \longrightarrow K \,|\, f \text{ Abbildung} \}$$

  mit den Verknüpfungen

  $$+ : \begin{array}{ccc} K^M \times K^M & \longrightarrow & K^M \\ (f+g)(x) & \longmapsto & f(x)+g(x) \end{array} \quad \text{und} \cdot : \begin{array}{ccc} K \times K^M & \longrightarrow & K^M \\ (s \cdot f)(x) & \longmapsto & s \cdot f(x) \end{array}$$

  ein Vektorraum. Speziell ist $K^{\mathbb{N}} = \{(a_1, a_2, \ldots) \,|\, a_i \in K\}$ die Menge aller Folgen über K und $K^n = K^{\{1,\ldots,n\}} = \{(a_1, \ldots, a_n) \,|\, a_i \in K\}, n \in \mathbb{N}$ die Menge aller n-Tupel.
- $K^{\emptyset} = \{0\}$ ist K-Vektorraum mit einem Vektor, “Nullvektorraum”.

Lemma 1 (Folgerungen aus den Vektoraxiomen) Ist V ein K-Vektorraum, so gilt:

1. Es gibt genau einen Nullvektor $1 \in V$ mit (V2) und zu jedem $v \in V$ gibt es genau ein $-v \in V$ mit (V3).
2. Sei $s \in K, v \in V$. Dann gilt: $sv = 0 \Leftrightarrow s = 0 \vee v = 0$.
3. $-v = (-1) \cdot v$, $-1 \in K$.

Beweis:

1. Angenommen, es gäbe auch $\widetilde{0} \in V$ mit $\widetilde{0} + v = v$, $v \in V$. Sei $v := 0$. Dann gilt: $\widetilde{0} + v = \widetilde{0} + 0 = 0$. Umgekehrt gilt für $w := \widetilde{0}$: $0 + w = 0 + \widetilde{0} = 0$. Also ist $\widetilde{0} = 0$.
   Angenommen, es gäbe auch $\sim v \in V$ mit $v + \sim v = 0$. Dann gilt:

   $$-v = 0 + (-v) = (v + \sim v) + (-v) = \sim v + v - v = \sim v + (v + (-v)) = \sim v + 0 = \sim v$$

2. “$\Leftarrow$”: zu zeigen: (a) Sei $v \in V$, dann $0 \cdot v = 0$ und (b) sei $s \in K$, dann $s \cdot 0 = 0$.

   (a) $0 = 0v + (-(0v)) = (0+0)v + (-0)v = (0v + 0v) + (-(0v)) = 0v + (0v - (0v)) = 0v + 0 = 0v$

   (b) $0 = s0 + (-(s0)) = s \cdot (0 + 0) + (-(s0)) = s0 + s0 + (-(s0)) = s0$

   “$\Rightarrow$”: Sei $s \in K$, $v \in V$, $s \cdot v = \underline{0}$. Es gilt zu zeigen, daß dann $s = 0 \vee v = 0$ gilt.
   Wir zeigen (logisch äquivalent): Ist $s \neq 0 \Rightarrow v = 0$, wenn $sv = 0$. Ist $s \neq 0$, so existiert $s^{-1} \in K$ mit $s^{-1} \cdot s = 1$. Es gilt: $v = 1v = (s^{-1} \cdot s)v = s^{-1} \cdot (sv) = s^{-1} \cdot 0 = 0$. $v \neq 0$ analog.

3. Nur zu zeigen: $(-1)v + v = 0$.
   $(-1)v + v = (-1)v + 1v = (-1+1)v = 0 \cdot v = 0$. □

2.2 Teilräume

Voraussetzung: V ist ein K-Vektorraum.

Definition 1 (Teilraum) $U \subseteq V$ heißt *Teilraum* von V (i.Z. $U \leq V$), wenn

$$(U, +_{|U \times U} : U \times U \to U, \cdot_{|K \times U} : K \times U \to U)$$

ein K-Vektorraum ist.

Satz 1 $U \subseteq V$ ist ein Teilraum genau dann, wenn...

1. $U \neq \emptyset$
2. $u, u' \in U \Rightarrow u + u' \in U$
3. $s \in K, u \in U \Rightarrow s \cdot u \in U$

Beweis:

- "$\Rightarrow$": U sei Teilraum. Dann gelten per definitionem (1),(2) und (3).
- "$\Leftarrow$": Wegen (2) ist $+_{|U\times U} : U \times U \to U$ eine Abbildung, wegen (3) $\cdot_{|K\times U} : K \times U \to U$.
  Es gelten (V1),(V4),...,(V8) für alle Vektoren aus V, also erst recht für alle aus U.
  (V2) gilt. Das Nullelement liegt in U: nach Lemma 1 (S. 15) $\mathbf{o} = 0 \cdot u \in U$.
  (V3) gilt. Das Inverse liegt in U: Nach Lemma 1 (S. 15) $(-1) \cdot u = -u$, also $-u \in U$. $\square$

Satz 1' (Äquivalent zu Satz 1) U ist Teilraum von V gdw. $\mathbf{o} \in U$ und $s \in K; u, u' \in K \Rightarrow su + u' \in U$.

Beispiele:

- $\{\mathbf{o}\}$ und V sind die "trivialen" Teilräume von V.
- Sei $A \in K^{m\times n}$, K ein Körper. Dann ist die Lösungsmenge des homogenen linearen Gleichungssystems $Ax = \mathbf{o} \in K^{m\times 1}$, $L \neq \emptyset$ ein Teilraum des $K^{n\times 1}$.

Satz 2 Für einen Vektorraum V gilt:

1. Wenn $U_1, U_2 \subseteq V$, dann sind $U_1 \cap U_2$ und $U_1 + U_2$ Teilräume von V.
2. Wenn $U_i \leq V$ für $i \in I$, I Indexmenge. Dann ist $\bigcap_{i\in I} U_i$ ein Teilraum von V.

Beweis:

- U_1, U_2 seien Teilräume. Dann ist $\mathbf{o} \in U_1$ und $\mathbf{o} \in U_2$. Somit ist $\mathbf{o} = \mathbf{o} + \mathbf{o} \in U_1 + U_2$.
  Seien $v_1, v_2 \in U_1 + U_2$ und $s \in K$. Sei weiterhin $v_1 = u_1 + u_2$ ($u_1 \in U_1$, $u_2 \in U_2$) sowie $v_2 = u_1' + u_2'$ ($u_1' \in U_1$ und $u_2' \in U_2$). Dann gilt nach Satz 1':
  $$sv_1 + v_2 = s(u_1 + u_2) + (u_1' + u_2') = (su_1 + u_1') + (su_2 + u_2') \in U_1 + U_2$$
- U sei Teilraum von V für alle $i \in I$. Dann ist $\mathbf{o} \in U_i$ für alle $i \in I$, d.h. $\mathbf{o} \in \bigcap_{i\in I} U_i$,
  Seien $u, u' \in U$. Dann ist (nach Satz 1') $su + u' \in U_i$, $i \in I$, d.h. $su + u' \in \bigcap_{i\in I} U_i$. $\square$

Bemerkung: Wenn U_1, U_2 Teilräume von V sind, ist $U_1 \cup U_2$ im Allgemeinen kein Teilraum von V (Beispiel folgt).

Definition: M sei Menge und K sei Körper. Dann ist

$$K^{(M)} := \{ f : M \to K \mid f(x) \neq 0 \text{ nur für endlich viele } x \in M \}$$

Bemerkung: $K^{(M)}$ ist Teilraum von K^M.

Beweis:

- Die Nullfunktion $f = \underline{0}$ liegt in $K^{(M)}$.
- Seien $f_1, f_2 \in K^{(M)}$, $s \in K$. Sei $f_1(x) \neq 0$ nur für $x \in \{x_1, \dots, x_n\}$, $f_2(x) \neq 0$ nur für $x \in \{y_1, \dots, y_m\}$. Dann ist auch $(sf_1 + f_2)(x) = 0$ für $x \in M \setminus \{x_1, \dots, x_n, y_1, \dots, y_n\}$. □

Beispiel ($U_1 \cup U_2$ ist nicht immer ein Teilraum von V):

Sei $v, w \in \mathbb{R}^2$ mit $v \neq w \neq 0$. Die Gerade $\langle v \rangle = \{s \cdot v | s \in \mathbb{R}\}$ und $\langle w \rangle = \{t \cdot w | t \in \mathbb{R}\}$ durch $\mathfrak{o}$ ist Teilraum des $\mathbb{R}^2$. Obwohl $\langle v \rangle$ und $\langle w \rangle$ Teilräume erzeugen, ist $\langle v \rangle \cup \langle w \rangle$ kein Teilraum.

2.3 Linearkombinationen und Erzeugendensysteme

2.3.1 Linearkombinationen

Sei im folgenden V ein K-Vektorraum.

Definition 1 (Linearkombination) Sind $v_1, \dots, v_n \in V$, so heißt $v \in V$ *Linearkombination* von $v_1, \dots, v_n$ genau dann, wenn es $s_1, \dots, s_n \in K$ gibt mit

$$v = s_1 v_1 + s_2 v_2 + \dots + s_n v_n$$

Wir schreiben für die Menge aller Linearkombinationen von $v_1, \dots, v_n$:

$$\begin{aligned}
\langle v_1, \dots, v_n \rangle &= \langle \{v_1, \dots, v_n\} \rangle \\
&= \{s_1 v_1 + s_2 v_2 + \dots + s_n v_n | s_i \in K,\ 1 \leq i \leq n\} \\
&= \{\textstyle\sum_{i=1}^n s_i y_i | n \in \mathbb{N} \cup \{0\};\ s_i \in K;\ y_i \in Y, Y \subseteq V\} \\
&= \left\{ \textstyle\sum_{v \in Y} f(v) \cdot v \,\middle|\, f \in K^{(Y)} \right\},\ f(v) \neq 0 \text{ für höchstens endlich viele } v \in Y \\
&= \{\text{Linearkombinationen von je endlich vielen Vektoren aus } V\}
\end{aligned}$$

Konventionen:

- Das Erzeugnis der leeren Menge ist der Nullvektor
- Leere Summen sind Null
- Es werden nur Summen $\sum_{i \in I} x_i$ zugelassen, bei der nur endlich viele Summanden ungleich Null sind

Beispiele:

- $n = 0$: $\langle \emptyset \rangle = \{\mathfrak{o}\}$ (per definitionem)
- $n = 1$: $\langle v \rangle = \{sv | s \in K\}$

Definition 1' (Linearkombination) Sind $v_i \in V$, $i \in I$ (I beliebige Indexmenge), so heißt $v \in V$ eine *Linearkombination* von $(v_i)_{i \in I}$, wenn es eine endliche Teilmenge $I' \in I$ gibt und $s_i \in K$ für $i \in I'$ existieren mit

$$v = \sum_{i \in I'} s_i \cdot v_i$$

d.h. wenn v eine Linearkombination von $\{v_i | i \in I'\}$ ist.

Satz 1 Ist $Y \subseteq V$ eine Teilmenge, so ist die Menge $\langle Y \rangle$ ein Teilraum und es ist

$$\langle Y \rangle = \bigcap \{U \,|U \leq V; Y \subseteq U\} = \bigcap_{U \leq V, Y \subseteq U} U$$

der Durchschnitt aller Teilräume von V, die y enthalten.

Beweis:

1. $\langle Y \rangle$ ist ein Teilraum
   (a) Zunächst liegt $\mathfrak{o} \in \langle Y \rangle$ (trivial, falls $Y = \emptyset$, sonst $\exists v \in Y$ mit $\mathfrak{o} = 0 \cdot v \in \langle Y \rangle$)
   (b) Seien $v_1, v_2 \in \langle > \rangle$, $s \in K$ (z.Z. $sv_1 + v_2 \in \langle Y \rangle$). Seien weiterhin $v_1 = \sum_{y \in Y} f_1(y)y$ und $v_2 = \sum_{y \in Y} f_2(y)y$ ($f_1, f_2 \in K^{(Y)}$). Dann:
   $$sv_1 + v_2 = \sum_{y \in Y} s f_1(y)y + \sum_{y \in Y} f_2(y)y = \sum_{y \in Y} (sf_1 + f_2)(y) \cdot y \in \langle Y \rangle$$
2. Ist U Teilraum von V mit $Y \subseteq U$, so gilt $\langle Y \rangle \subseteq U$
   Ein beliebiges Element von $\langle Y \rangle$ ist von der Form $\sum_{i=1}^{n} s_i v_i$ mit $v_1 \in Y$, $s_i \in K$, $n \in \mathbb{N} \cup \{0\}$. Da $Y \subseteq U$, ist $v_i \in U$ für alle i, also auch $s_i v_i \in U$. Mit Induktion nach n läßt sich zeigen, daß dann gilt: $s_1 v_1 + \ldots + s_n v_n \in U$.
3. $Y \subseteq \langle Y \rangle$ ist trivial, da $Y = 1 \cdot Y$.
4. Aus (2) folgt: $\langle Y \rangle \subseteq \bigcap \{U \,|U \text{ Teilraum}, Y \subseteq U\} = \langle Y \rangle \cap \{U \,|U \text{ Teilraum}, Y \subseteq U\} \subseteq \langle Y \rangle$ $\square$

2.3.2 Erzeugendensysteme und Basen

Definition 2 (Erzeugendensystem) Ist $Y \subseteq V$ Teilmenge und $U = \langle Y \rangle$ (ist Teilraum von V) so heißt Y *Erzeugendensystem* von U. U heißt umgekehrt der von Y *erzeugte Teilraum* von V.
V heißt *endlich erzeugter* K-Vektorraum, wenn V ein endliches Erzeugendensystem hat, wenn es also $v_1, \ldots, v_n$ gibt in V mit $V = < v_1, \ldots, v_n >$.

Definition 3 (Basis) Y heißt *Basis* von V, wenn jeder Vektor $v \in V$ sich eindeutig als endliche Linearkombination von paarweise verschiedenen Vektoren aus Y schreiben läßt, d.h. wenn

$$v = \sum_{y \in K^{(Y)}} f(y) \cdot y$$

mit eindeutig bestimmten $f \in K^{(Y)}$.

Beispiele:

- $V = K^{n \times 1} = \left\{(x_1, \ldots, x_n)^T \,|x_i \in K\right\}$, $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)^T$ mit 1 in der i-ten Zeile.
  Dann ist $Y = \{e_1, \ldots, e_n\}$ Basis von V (Standardbasis des $K^{n \times 1}$).
  Begründung: Sei $v = (x_1, \ldots, x_n)^T \in V$ beliebig. Dann ist $v = x_1 e_1 + x_2 e_2 + \ldots + x_n e_n \in \{e_1, \ldots, e_n\}$.
- $L = \left\{x \in \mathbb{R}^5 \,|Ax = \mathfrak{o}\right\}$, $A = \begin{bmatrix} 1 & 3 & 0 & 1 & 3 \\ 2 & 6 & 2 & 3 & 4 \\ 1 & 3 & 2 & 2 & 0 \end{bmatrix}$. Durch elementare Umformungen:
  $$L = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_5 \end{bmatrix} \middle| \begin{array}{c} x_1 + 3x_2 + x_4 = 0 \\ x_3 + \frac{1}{2}x_4 = 0 \\ x_5 = 0 \end{array} \right\} = \left\{ x_2 \begin{bmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -1 \\ 0 \\ -\frac{1}{2} \\ 1 \\ 0 \end{bmatrix} \middle| x_2, x_4 \in \mathbb{R} \right\}$$
  Also besteht eine Basis von L aus den Vektoren $(-3, 1, 0, 0, 0)^T$ und $(-1, 0, -0,5, 1, 0)^T$.

2.4 Lineare Abhängigkeit und Basen

2.4.1 Lineare Abhängigkeit und Unabhängigkeit

Voraussetzung: V ist ein K-Vektorraum.

Definition 1 (Lineare Abhängigkeit) Eine Teilmenge $Y \subseteq V$ heißt *linear abhängig* (l.a.), wenn es $f \neq 0$ (Nullfunktion) in $K^{(Y)}$ gibt mit

$$\sum_{y \in Y} f(y) \cdot y = \mathfrak{o}$$

Y ist linear abhängig genau dann, wenn es $y_1, \ldots, y_n \in Y$ ($y_i \neq y_j$ für $i \neq j$) und $s_1, \ldots, s_n \in K$ ($(s_1, \ldots, s_n) \neq (0, \ldots, 0)$) gibt mit $\mathfrak{o} = \sum_{i=1}^{n} s_i y_i$ und sonst *linear unabhängig* (l.u.).

Korollar 1 Für eine Teilmenge $Y \subseteq V$ gilt:

1. Y linear unabhängig $\Leftrightarrow \sum_{y \in Y} f(y) \cdot y = \mathfrak{o} \Rightarrow f = 0$ für $f \in K^{(Y)}$.
2. Sei $X \subseteq Y \subseteq V$. Dann gilt: Wenn X linear abhängig ist, ist auch Y linear abhängig.
3. Sei $X \subseteq Y \subseteq V$. Dann gilt: Wenn Y linear unabhängig ist, ist auch X linear unabhängig.

Beispiele:

- $\emptyset$ ist linear unabhängig.
- $\{\mathfrak{o}\} \subseteq V$ ist linear abhängig, weil $1 \cdot \mathfrak{o} = \mathfrak{o}$ ($1 \in K \neq 0$)
- $v \neq \mathfrak{o}$. $Y = \{v\}$ ist linear unabhängig ($s \in K$), nach Lemma 1 (Seite 15) gilt $sv = \mathfrak{o} \Rightarrow s = 0$
- $V = \mathbb{R}^{2\times 1}$, $Y = \left\{(1,1)^T, (1,-1)^T, (0,1^T)\right\}$ ist l.a., denn $1v_1 + (-1)v_2 - 2v_3 = (0,0)^T = \mathfrak{o}$.
- $v \neq \mathfrak{o}$. Dann ist $\{v, v\} = \{v\}$ linear unabhängig.

Warnung: Oft wird die lineare (Un-)Abhängigkeit definiert für n-Tupel $(v_1, \ldots, v_n)$ von Vektoren. $(v_1, \ldots, v_n)$ ist linear unabhängig genau dann, wenn aus $\sum_{i=1}^{n} s_i v_i = \mathfrak{o}$ folgt, daß $s_1 = \ldots = s_n = 0$ ist. In diesem Fall ist (v, v) linear abhängig, denn mit $1 \cdot v_1 + (-1) \cdot v_1 = \mathfrak{o}$.

Lemma 1 Sei $Y \subseteq V$ eine Teilmenge von Vektoren. Dann sind äquivalent:

1. Y ist linear abhängig.
2. Es gibt ein $u \in Y$ mit $u \in \langle Y \setminus \{u\} \rangle$ ("d.h. u ist eine Linearkombination der 'anderen' Vektoren aus Y")
3. Es gibt ein $u \in Y$ mit $\langle Y \rangle = \langle Y \setminus \{u\} \rangle$

Beweis:

- (1)⇒(2): Sei Y l.a., d.h. es gibt $f \neq 0$ in $K^{(Y)}$ mit $\sum_{y \in Y} f(y) \cdot y = \mathfrak{o}$. Sei $\emptyset \neq \{y \,|\, f(y) \neq 0\} =: \{y_1, \ldots, y_n\}$ mit disjunkten y_i und $f(y_i) =: s_i \neq 0$. Dann gilt $\sum_{i=1}^{n} s_i y_i = \mathfrak{o}$, $s_1 y_1 + .. + s_n y_n = \mathfrak{o} \Leftrightarrow y_1 = \frac{-s_2}{s_1} y_2 + \ldots + \frac{-s_n}{s_1} y_n$, $s_1 \neq 0$. Setze $u := y_1 \in \langle y_2, \ldots, y_n \rangle = \langle Y \setminus \{u\} \rangle$ ($y_i \neq u$ für $i > 1$).

- (2)⇒(3): Voraussetzung: $u \in Y$ mit $u \in \langle Y \setminus \{u\}\rangle$.
  Offensichtlich gilt: $\langle Y \setminus \{u\}\rangle \subseteq \langle Y\rangle$. Zu zeigen ist also nur noch: $\langle Y\rangle \subseteq \langle Y \setminus \{u\}\rangle$:
  Sei $v \in \langle Y\rangle$, $v = \sum_{y\in Y} f(y)\cdot y$, $f \in K^{(Y)}$. Nach Voraussetzung: $u = \sum_{y\in Y\setminus\{u\}} g'(y)y$, $g' \in K^{(Y\setminus\{u\})}$, also

$$\underline{0} = -u + \sum_{y\in Y\setminus\{u\}} g'(y)y = \sum_{y\in Y} g(y)y,\ g(y) = \begin{cases} -1 & y = u \\ g'(y) & y \in Y\setminus\{u\} \end{cases}$$

  Dann gilt mit $h(y) = (f(y) + f(u)g(y)$:

$$\begin{aligned} v &= v + f(u)\cdot \mathsf{o} = \sum_{y\in Y} f(y)y + \sum_{y\in Y} f(u)g(y)y = \sum_{y\in Y}(f(y) + f(u)g(y))\cdot y \\ &= \sum_{y\in Y\setminus\{u\}} h(y)y \in \langle Y \setminus \{u\}\rangle \end{aligned}$$

- (3)⇒(1): Voraussetzung: $\langle Y\rangle = \langle Y \setminus \{u\}\rangle$ für ein $u \in Y$. Zu zeigen: Y linear abhängig; $u \in Y$, also $u \in \langle Y\rangle = \langle Y \setminus \{u\}\rangle$, $u = \sum_{y\in Y\setminus\{u\}} f'(y)y$, $f' \in K^{(Y\setminus\{u\})}$. $\mathsf{o} = \sum_{y\in Y} f(y)y$ mit $f(y) = \begin{cases} f'(y) & y \neq u \\ -1 & y = u \end{cases}$.
  $f \neq \underline{0}$ weil $f(u) = -1 \neq 0$. □

Beispiel:

$V = \mathbb{R}^{3\times 1}$, $Y = \left\{(1,1,0)^T =: v_1, (-1,-1,0)^T =: v_2, (0,0,1)^T =: v_3\right\}$ ist linear abhängig (denn $v_1 + v_2 = \mathsf{o}$). $v_3 \notin \langle Y \setminus \{v_3\}\rangle = \langle v_1, v_2\rangle$, $v_2 \in \langle Y \setminus \{v_2\}\rangle$.

2.4.2 Basen und Teilräume sowie Teilmengen

Satz 1 Äquivalent sind für eine Teilmenge $B \subseteq V$:

1. B ist eine Basis von V.
2. B ist ein linear unabhängiges Erzeugendensystem von V.
3. B ist ein "minimales" oder "unverkürzbares" Erzeugendensystem von V, d.h. $\langle B\rangle = V$ und für jedes $b \in B$ ist $\langle B \setminus \{b\}\rangle \neq V$.
4. B ist eine "maximale" linear unabhängige Teilmenge, d.h. B ist linear unabhängig, aber $B \cup \{v\}$ ist linear abhängig für jedes $v \in V \setminus B$.

Beweis:

- (1)⇒(2): B sei eine Basis, d.h. zu jedem $v \in V$ existiert genau ein $f \in K^{(B)}$ mit $v \in \sum_{b\in B} f(b)b$ ($\star$), d.h. $\langle B\rangle = V$ und außerdem B l.u., denn wende ($\star$) auf $v = \mathsf{o}$ an, dann:

$$\mathsf{o} = \sum_{b\in B} \underline{0}(b)b = \sum_{b\in B} f_0(b)b \Rightarrow f = \underline{0}$$

- (2)⇒(3): Nach Lemma 1 (Seite 19).
- (3)⇒(4): Voraussetzung: $\langle B\rangle = V$ und für jedes $b \in B$ ist $\langle B \setminus \{b\}\rangle \neq V$, also ist B linear unabhängig nach Lemma 1; zu zeigen: für jedes $v \in V \setminus B$ ist $B \cup \{v\}$ linear abhängig.
  Sei $v \in V \setminus B$. Wir dürfen $v \neq \mathsf{o}$ annehmen, denn $B \cup \{\mathsf{o}\}$ ist l.a. Weil $\langle B\rangle = V$, ist $v = \sum_{i=1}^n s_i v_i$, $s_i \in K, v_i \in B, v_i$ disjunkt. Es gilt: $\mathsf{o} = (-1)v + s_1v_1 + \ldots + s_nv_n$. Dabei ist $v \neq v_i$, weil $v \notin B$. Also ist $\{v, v_1, v_2, \ldots, v_n\}$ linear abhängig, somit ist $B \cup \{v\}$ ebenfalls linear abhängig.

- (4)$\Rightarrow$(1): Voraussetzung: B l.u. und $B \cup \{v\}$ l.a. für jedes $v \in V \setminus B$. Beh.: $\langle B \rangle = V$.
  Sei $v \in V$ beliebig gewählt.
  - 1. Fall: $v \in B$, dann ist $v \in \langle B \rangle$.
  - 2. Fall: $v = \mathit{o}$, dann ist $v \in \langle B \rangle$.
  - 3. Fall: $v \in V \setminus B$ und $v \neq \mathit{o}$. Nach Annahme ist $B \cup \{v\}$ l.a., d.h. $\exists b_1, \ldots, b_n \in B$ paarweise verschieden. Also existieren $s, s_1, \ldots, s_n \in K$ mit $(s, s_1, \ldots, s_n) \neq (0, \ldots, 0)$, so daß $\mathit{o} = sv + s_1 b_1 + \ldots + s_n b_n$. Dabei ist $s \neq 0$, da sonst $\{b_1, \ldots, b_n\}$ l.a. wäre. Also gilt:
  $$v = -\frac{s_1 b_1 + \ldots + s_n b_n}{s} \in \langle b_1, \ldots, b_n \rangle = \langle B \rangle$$
  Also ist v linear abhängig von $b_1, \ldots, b_n$, und somit $B \cup \{v\}$ linear abhängig. $\square$

2.5 Existenz von Basen

2.5.1 Basisergänzungssatz

Satz 1 (Basisergänzungssatz) V sei ein K-Vektorraum. Sei weiterhin $V = \langle X \rangle$, d.h. X sei ein Erzeugendensystem von V, und $L \subseteq V$ linear unabhängig. Dann gibt es $Y \subseteq X$, so daß $L \cup Y$ eine Basis von V ist.

"Jede linear unabhängige Teilmenge L läßt sich zu einer Basis ergänzen und zwar mit Hilfe von Vektoren aus einem vorgegebenen Erzeugendensystem."

Beweis: Sei $M = \{Z \subseteq X \,|\, L \cup Z \text{ l.u.}\}$; $\emptyset \in M$, denn $L \cup \{\emptyset\} = L$ ist linear unabhängig, $M \neq \emptyset$.

Sei $Y \subseteq M$ maximal[2], d.h. $Y \subseteq X$ und $Y \in M$, aber ist $Y \subset Y' \subseteq X$, dann ist $Y' \notin M$, d.h. $L \cup Y$ ist linear unabhängig, aber $L \cup Y \cup \{v\}$ linear abhängig für jedes $v \in X \wedge v \notin Y \cup L$.

Behauptung: $L \cup Y$ ist Basis. Es ist also noch zu zeigen, daß $\langle L \cup Y \rangle = X$.

Wir zeigen $X \subseteq \langle L \cup Y \rangle$, dann folgt $V = \langle X \rangle \subseteq \langle L \cup Y \rangle$. Sei $v \in X$.

- 1. Fall: $v \in Y$, dann $v \in \langle L \cup Y \rangle$
- 2. Fall: $v \notin Y$, dann ist $L \cup Y \cup \{v\}$ linear abhängig, denn:
  $$\mathit{o} = sv + s_1 v_1 + \ldots + s_n v_n \Leftrightarrow v = -\frac{s_1}{s} v_1 - \ldots - \frac{s_n}{s} v_n \in \langle L \cup Y \rangle$$
  mit v_i disjunkt und $(s, s_1, \ldots, s_n) \neq (0, \ldots, 0)$, $s, s_i \in M$. Insbesondere wichtig ist, daß $s \neq 0$ (gegeben, weil $L \cup Y$ linear unabhängig).

Also ist $L \cup Y$ eine Basis. $\square$

2.5.2 Folgerungen aus dem Basisergänzungssatz

Folgerung 1 Jeder Vektorraum hat eine Basis. Jedes Erzeugendensystem X von V enthält eine Basis.

Beweis: Wende Basisergänzungssatz mit $L = \emptyset$ an. $\square$

[2] Für ein unendliches X ist der Beweis hier nicht vollständig. Warum existiert eine solche maximale Menge? Für $|x| = \infty$ muß man das Lemma von Zorn benutzen (äquivalent zum Auswahlaxiom).

Beispiel:

$V = K^{2\times 2} = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle| a_{ij} \in K \right\}$

$X = \{E_{11}, E_{12}, E_{21}, E_{22}\} \Rightarrow \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22} \Rightarrow \langle X \rangle = V$

$L = \left\{ E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right\}$, L ist linear unabhängig.

L kann man unter Hinzunahme von einer Teilmenge $Y \subseteq X$ zu einer Basis von V ergänzen:

1. $L \cup \{E_{11}\}$ ist linear unabhängig $\Rightarrow E_{11} \in Y$
2. $L \cup \{E_{11}\} \cup \{E_{12}\}$ ist linear abhängig $\Rightarrow E_{12} \notin Y$
3. $L \cup \{E_{11}\} \cup \{E_{21}\}$ ist linear unabhängig $\Rightarrow E_{21} \in Y$
4. $L \cup \{E_{11}\} \cup \{E_{21}\} \cup \{E_{22}\}$ ist linear abhängig $\Rightarrow E_{22} \notin Y$

Also ist $L \cup Y$ Basis von V mit $Y = \{E_{11}, E_{21}\}$

Korollar 2 Ist U ein Teilraum von V, $X \subseteq V$ Teilmenge von V, dann gilt:

$$X \subseteq U \Rightarrow \langle X \rangle \subseteq U$$

Insbesondere gilt: $\langle X \rangle = V \Rightarrow U = V$

Beweis: Klar, denn $\langle X \rangle = \bigcap \{W | X \subseteq W, W \leq V\}$ □

Lemma 1 Seien $v_1, \ldots, v_n \in V$, dann gilt:

$$\begin{aligned} U = \langle v_1, \ldots, v_n \rangle &= \left\langle v_1, \ldots, v_{i-1}, v_i + sv_j, v_{i+1}, \ldots, v_n \right\rangle = U' \text{ für } i \neq j \\ &= \langle v_1, \ldots, v_{i-1}, sv_i, v_{i+1}, \ldots, v_n \rangle \text{ mit } s \neq 0 \\ &= \langle v_1, \ldots, v_n, o \rangle \end{aligned}$$

Beweis: Es ist zu zeigen, daß (1) $U \subseteq U'$ und (2) $U' \subseteq U$:

1. $\langle v_1, \ldots, v_{i-1}, v_i, \ldots, v_n \rangle \in U'$
   $v_i = (v_i + sv_j) - sv_j \in U'$ da $v_i + sv_j \in U'$. Nach Korollar 2 gilt $\langle v_1, \ldots, v_n \rangle \subseteq U'$.
2. $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \in U$, $v_i + sv_j \in U$, also auch $U' \subseteq U$. □

Beispiel:

$V = \mathbb{R}^3, U = \langle (1,1,1), (1,3,5), (1,4,7), (1,5,9) \rangle$

Gesucht: Basis von U. Es gilt:

$U = \langle (1,1,1), (0,2,4), (0,3,6), (0,4,8) \rangle = \langle (1,1,1), (0,1,2), o, o \rangle = \langle w_1 = (1,1,1), w_2 = (0,1,2) \rangle$

$\{w_1, w_2\}$ ist linear unabhängig, denn $rw_1 \neq sw_2$ $(r, s \in \mathbb{R})$, also ist $\{w_1, w_2\}$ Basis von U.

2.6 Austauschsatz und Dimension

2.6.1 Der Austauschsatz von Steinitz

Satz 1 (Austauschsatz von Steinitz) Es seien B und B' Basen des K-Vektorraums V. Dann gibt es zu jedem $v \in B$ ein $v' \in B'$ mit der Eigenschaft, daß $B'' := (B \setminus \{v\}) \cup \{v'\}$ eine Basis von V ist.

Beweis: $B \setminus \{v\}$ ($v \in B$) ist nach Satz 1 (“Eine Basis von V ist unverkürzbares Erzeugendensystem von V”, Seite 20) kein Erzeugendensystem von V. Nach Korollar 2 (Seite 22) gibt es ein $v' \in B'$ mit $v' \notin \langle B \setminus \{v\} \rangle$.
Behauptung: $B'' = (B \setminus \{v\}) \cup \{v'\}$ ist Basis von V.

- Zu zeigen: B'' ist linear unabhängig.
  Sei $\mathit{o} = sv' + s_1 v_1 + ... + s_n v_n$ mit $v_1, ..., v_n \in B \setminus \{v\}$ paarweise verschieden (d.h. $v_i \neq v_j$ für $i \neq j$) und $s, s_1, ..., s_n \in K$.
  Wenn $s = 0$, so folgt dann $s_1 v_1 + ... + s_n v_n = \mathit{o}$ ($v_i \in B \setminus \{v\}$), also auch $s_1 = ... = s_n = 0$, weil $B \setminus \{v\}$ linear unabhängig ist. Ist aber $s \neq 0$, dann ist $v' = -\frac{s_1}{s} v_1 - ... - \frac{s_n}{s} v_n \in \langle B \setminus \{v\} \rangle$, was aber ein Widerspruch zu $v' \notin \langle B \setminus \{v\} \rangle$ ist. Also muß $s = 0$ sein und daher (s.o.) $s_1 = ... = s_n = 0$, d.h. B'' ist linear unabhängig.

- Zu zeigen: B'' ist Erzeugendensystem, d.h. $\langle B'' \rangle = V = \langle B \rangle$.
  Nach Korollar 2 (Seite 22) genügt es zu zeigen, daß $B \subseteq \langle B'' \rangle$ ist. Es gilt bereits $B \setminus \{v\} \subseteq \langle B'' \rangle$. Also nur noch zu zeigen: $v \in \langle B'' \rangle$.
  Wäre $v \notin \langle B'' \rangle$, dann wäre $B'' \cup \{v\}$ linear unabhängig. B ist Basis von V, also $v' \in \langle B \rangle$, $v' = sv + s_1 v_1 + ... + s_n v_n$ mit $v_i \in B \setminus \{v\}$. $v_1, ..., v_n$ sind paarweise verschieden, $s, s_1, ..., s_k \in K$, $s \neq 0$ (weil $v' \notin \langle B \setminus \{v\} \rangle$), also $v = \frac{1}{s} v' - \frac{s_1}{s} v_1 - ... - \frac{s_n}{s} v_n$, und mit $B'' := (B \setminus \{v\}) \cup \{v'\}$ somit $B \subseteq \langle B'' \rangle \Rightarrow V = \langle B'' \rangle$. □

Satz 2 Sind $B = \{v_1, ..., v_n\}$ und $B' = \{u_1, ..., u_m\}$ Basen von V, dann ist $n = |B| = |B'| = m$.

Beweis: Nach dem Austauschsatz (Seite 23) gibt es ein $j_1 \in \{1, ..., m\}$ so, daß $B_1 = \left\{u_{j_1}, v_2, ..., v_n\right\}$ Basis von V ist und $|B_1| = n$. Weiterhin existiert ein $j_2 \in \{1, ..., m\}$ so, daß $B_2 = \left\{u_{j_1}, u_{j_2}, v_3, ..., v_n\right\}$ wieder Basis von V ist und $|B_2| = n$. Schließlich erhält man $j_n \in \{1, .., n\}$ mit $B_n = \left\{u_{j_1}, ..., u_{j_n}\right\}$, $|B_n| = n$. Also ist $m \geq n$.
Analog erhält man $n \geq m$. Aus $m \geq n \wedge n \geq m$ folgt jedoch $m = n$. □

2.6.2 Dimension von Vektor- und Teilräumen

Definition 1 (Dimension) Hat V eine Basis B mit $|B| = n$, $n \in \mathbb{N}_0$, so heißt n die *Dimension* von V, i.Z. $n = dim V$. Nach dem Austauschsatz (Seite 23) gilt $n = dim V \wedge B'$ Basis von $V \Rightarrow |B'| = n$.
Hat V keine endliche Basis, so schreibt man oft auch $dim V = \infty$.

Folgerung 1 Ist V ein endlich erzeugter Vektorraum...

1. ..., so ist $dim V = n \in \mathbb{N}_0$
2. ...und ist U Teilraum von V, so gilt $dim U \leq dim V$ mit $dim U = dim V$ gdw. $U = V$.
3. ...und ist $M \subseteq V$ Teilmenge, so gilt: $|M| < dim V \Rightarrow \langle M \rangle \neq V$
4. ...und ist $M \subseteq V$ Teilmenge, so gilt: $|M| > dim V \Rightarrow M$ linear abhängig
5. ...und ist $M \subseteq V$ Teilmenge, so gilt: $|M| = dim V$, $\langle M \rangle = V \Rightarrow M$ Basis von V
6. ...und ist $M \subseteq V$ Teilmenge, so gilt: $|M| = dim V$, M linear unabhängig $\Rightarrow M$ Basis von V

Beweis:

1. Jedes endl. Erzeugendensystem von V enthält eine endl. Basis von V (Folgerung 1, Seite 21), also $dim V < \infty$.
2. Jede Basis von U kann man zu einer Basis von V ergänzen (Basisergänzungssatz, Seite 21), also $|B'| \leq dim V = n$ sowie $dim U = n \Rightarrow |B'| = n$. Dann ist B' auch Basis von V.
3. $M \subseteq V$, $|M| < dim V = n$. Wäre $\langle M \rangle = V$, so enthielte M eine Basis $B \subseteq M$, $|B| < dim V$, was jedoch ein Widerspruch zu Satz 2 (Seite 23) ist, da B Basis von V ist. Also $\langle M \rangle \neq V$.
4. ... □

Beispiele:

- $dim\ \{\mathfrak{o}\} = 0$, Basis von $\{\mathfrak{o}\}$ ist $\emptyset$.
- $dim K^n = n$, $n \in \mathbb{N}$, denn $B = \{e_1, e_2, ..., e_n\}$ ist Basis von K^n.
- $dim K^{m \times n} = mn$, denn $\left\{ E_{ij} \middle| 1 \leq i \leq m, 1 \leq j \leq n \right\}$ ist Basis.

Satz 3 (Dimensionssatz) Sei V ein K-Vektorraum, $dim V \in \mathbb{N}_0$ und U_1, U_2 seien Teilräume von V. Dann gilt:

$$dim U_1 + dim U_2 = dim(U_1 + U_2) + dim(U_1 \cap U_2)$$

Beweis: Sei $\{u_1, ..., u_d\}$ Basis von $U_1 \cap U_2$, $d = |B| = dim\,(U_1 \cap U_2)$; es gilt: $U_1 \cap U_2 \subseteq U_1 \wedge U_1 \cap U_2 \subseteq U_2$. Nach dem Basisergänzungssatz (Seite 21) kann man B zu einer Basis B_1 von U_1 und zu einer Basis B_2 von U_2 ergänzen. Dann ist $B_1 = \{u_1, ..., u_d, v_1, ..., v_m\}$, $d + m = dim U_1$, sowie $B_2 = \{u_1, ..., u_d, w_1, ..., w_n\}$, $d + n = dim U_2$.

Behauptung: $B' = \{u_1, ..., u_d, v_1, ..., v_m, w_1, ..., w_n\}$ ist Basis von $U_1 + U_2$. Dann sind die Vektoren in B' paarweise verschieden, denn $v_i \in U_1 \setminus U_2 \wedge w_j \in U_2 \setminus U_1$, also $|B'| = d + m + n$. Also:

$$dim\,(U_1 + U_2) = d + m + n \wedge dim\,(U_1 \cap U_2) = d \wedge dim U_1 = d + m \wedge dim U_2 = d + m \Rightarrow \text{Satz 3}$$

Beweis der Behauptung:

- $\langle B' \rangle = U_1 + U_2 = \{\, u + u' | u \in U_1 \wedge u' \in U_2\}$.

  Sei $u + u' \in U_1 + U_2$ beliebig (d.h. $u \in U_1$ und $u' \in U_2$). Da B_1 Basis von U_1 ist, gilt: $u = \sum_{i=1}^{d} s_i u_i + \sum_{j=1}^{m} t_j v_j$ mit $s_i, t_j \in K$. B_2 ist Basis von U_2, also gilt: $u' = \sum_{i=1}^{d} s_i^{,} u_i + \sum_{k=1}^{n} t_k^{,} w_k$ mit $s_i^{,}, t_k^{,} \in K$. Es folgt:

  $$u + u' = \sum_{i=1}^{d} ((s_i + s_i^{,}) \cdot u_i) + \sum_{j=1}^{m} t_j v_j + \sum_{k=1}^{n} t_k^{,} w_k \in \left\langle B' \right\rangle \ (u_i, v_j, w_k \in B')$$

- B' ist linear unabhängig. Sei $\mathfrak{o} = \sum_{i=1}^{d} s_i u_i + \sum_{j=1}^{m} t_j v_j + \sum_{k=1}^{n} t_k^{,} w_k$ mit $\sum_{k=1}^{n} t_k' w_k \in U_2$ und $\sum_{i=1}^{d} s_i u_i + \sum_{j=1}^{m} t_j v_j \in U_1$.

  $$(\star) \quad -\sum_{k=1}^{n} t_k' w_k = \sum_{i=1}^{d} s_i u_i + \sum_{j=1}^{m} t_j v_j = \sum_{i=1}^{d} s_i' u_i \in U_1 \cap U_2$$

  Außerdem gilt:

  $$\mathfrak{o} = \sum_{i=1}^{d} s_i' u_i + \sum_{k=1}^{n} t_k' w_k \ (u_1, w_k \in B_2)$$

Somit ist B_2 linear unabhängig, $s'_1 = ... = t'_1 = ... = t'_n = 0$. Aus $(\star)$ folgt:

$$o = \sum_{i=1}^{d} s_i u_i + \sum_{j=1}^{m} t_j v_j$$

mit $u_i, v_j \in B_1$ l.u.; daraus folgt jedoch B_1 linear unabhängig, also $s_1 = \ldots = s_d = 0$, $t_1 = \ldots = t_m = 0$.
□

Beispiel:

$V = \mathbb{R}^3$, $U_1 = \langle e_1, e_2 \rangle$, $U_2 = \langle e_2, e_3 \rangle$. Dann:

$U_1 \cap U_2 = \langle e_2 \rangle$, $U_1 + U_2 = \mathbb{R}^3$, $dim U_1 = 2$, $dim U_2 = 2$, $dim(U_1 \cap U_2) = 1$, $dim(U_1 + U_2) = 3$.

Kapitel 3

Lineare Abbildungen

3.1 Lineare Abbildungen

Definition 1 (Lineare Abbildung) Eine Abbildung $\varphi : V \longrightarrow W$ heißt *linear* (K-linear), wenn V, W Vektorräume über K sind (genauer: $(V, +, \cdot)$ sowie $(W, +, \cdot)$ Vektorräume) und

1. Additivität: $\varphi(v + v') = \varphi(v) + \varphi(v')$ für alle $v, v' \in V$
2. Homogenität: $\varphi(sv) = s \cdot \varphi(v)$ für alle $s \in K$, $v \in V$

Die Menge aller lin. Abbildungen von V nach W ist $Hom_K(V, W) = \{\varphi : V \longrightarrow W | \varphi \text{ ist } K - \text{linear}\}$.

Lemma 1

1. $\varphi : V \longrightarrow W$ (V, W sind K-Vektorräume) ist linear genau dann, wenn für alle $v, v' \in V$ und $t \in K$ gilt: $\varphi(tv + v') = t \cdot \varphi(v) + \varphi(v')$.
2. Ist $\varphi : V \longrightarrow W$ linear, so gilt $\varphi(\mathit{o}) = \mathit{o}$.

Beweis:

1. "$\Rightarrow$" Aus D1.1 und D1.2 folgt die erste Teilaussage von (1).
"$\Leftarrow$" Aus (1) folgten für $t = 1$ und $v = v'$ bzw. $t = s - 1$ D1.1 und D1.2:
$$s\varphi(v) = (s-1)\varphi(v) + \varphi(v) = t\varphi(v) + \varphi(v) = \varphi(tv + v) = \varphi((s-1)v + v) = \varphi(sv)$$
2. $\varphi(\mathit{o}) = \varphi(0 \cdot \mathit{o}) = 0 \cdot \varphi(\mathit{o}) = \mathit{o}$ □

Beispiele:

- V, W sind K-Vektorräume. Die Nullabbildung $\varphi = \underline{0}$ definiert durch $\varphi : V \longrightarrow W, v \longmapsto \mathit{o}$ ist eine lineare Abbildung.
- $V = W = K$, $a, b, c \in K$. $\varphi_c : K \longrightarrow K, x \longmapsto cx$ ist linear, da
$$\varphi_c(tx + x') = c(tx + x') = ctx + cx' = tcx + cx' = t_c\varphi(x) + \varphi_c(x')$$
Dagegen ist $\psi : K \longrightarrow K, x \longmapsto ax + b$ nur linear für $b = 0$.
- V ist K-Vektorraum, $c \in K$. $\varphi_c : V \longrightarrow V, v \longmapsto cv$ ist lineare Abbildung.

Definition 2 (Basisfolge) $(v_i)_{i \in I}$ (I Indexmenge)[1] heißt eine *Basisfolge* von V, wenn

[1] Dies schließt die Basisfolgen $(v_1, \ldots, v_n)$ ein (wähle $I = \{1, \ldots, n\}$).

1. $v_i \neq v_j$ für $i \neq j$
2. $\{v_i \,|\, i \in I\}$ ist Basis von V

Beispiel:

Sei $V = \mathbb{R}^3$, $e_i := (0,...,0,1,0,...,0) \in V$ mit 1 an der i-ten Stelle. $(e_1,e_2,e_3) \neq (e_2,e_1,e_3)$ sind Basisfolgen, (e_1,e_2,e_1,e_4) ist keine Basisfolge. $\{e_1,e_2,e_3\} = \{e_2,e_1,e_3\} = \{e_1,e_2,e_1,e_3\}$ sind zwar keine Basisfolgen, aber Basen.

Satz 1 Es seien V,W K-Vektorräume. $(v_i)_{i\in I}$ (I Indexmenge) sei eine Basisfolge von V. $w_i \in W$ seien beliebige Vektoren in W ($i \in I$). Dann existiert für $i \in I$ genau eine lineare Abbildung

$$\varphi : \begin{array}{ccc} V & \longrightarrow & W \\ v_i & \longmapsto & \varphi(v_i) = w_i \end{array}$$

“Die Bilder einer Basisfolge $(v_1,...,v_n)$ kann man beliebig vorschreiben, und es gibt dann genau eine lineare Abbildung mit diesen Eigenschaften.”

Stimmen zwei lineare Abbildungen $\varphi,\psi : V \longrightarrow W$ auf einer Basisfolge überein, so sind sie gleich.

Beweis:

- Eindeutigkeit von φ. Sei $v \in V$. damm gibt es eine eindeutige Darstellung von V in der Form $v = \sum_{i\in I} s_i v_i$ mit $s_i \in K, s_i \neq 0$ nur für endlich viele i. Ist $\varphi : V \longrightarrow W$ linear, so folgt, daß

  $$\varphi(v) = \sum_{i\in I} \varphi(s_i v_i) = \sum_{i\in I} s_i \varphi(v_i) = \sum_{i\in I} s_i w_i = \sum_{i\in I} s_i w_i \text{ falls } \varphi(v_i) = w_i$$

  eindeutig bestimmt ist.

- Existenz von φ. Definiere $\varphi : V \longrightarrow W, v = \sum_{i\in I} s_i v_i \longmapsto s_i w_i$. Beachte dabei, daß φ wohldefiniert ist, weil die s_i durch v eindeutig bestimmt sind (Basis-Eigenschaft). Behauptungen:
  - $\varphi(v_i) = w_i$ folgt aus Definition.
  - φ ist linear. Beweis: Sei $v = \sum_{i\in I} s_i v_i$, $v' = \sum_{i\in I} s_i^{,} v_i$, $t \in K$. Dann:

  $$\varphi(tv+v') = \varphi(\sum_{i\in I}(ts_i + s_i^{,})v_i) = \sum_{i\in I}(ts_i + s_i^{,})w_i = t\sum_{i\in I}(s_i w_i) + \sum_{i\in I}(s_i^{,} w_i) = t\varphi(v) + \varphi(v')$$

□

Beispiele:

- $V = W = \mathbb{R}^2$, $B = (e_1,e_2)$. Es gibt genau eine lineare Abbildung $\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ mit $\varphi(e_1) = w_1 \wedge \varphi(e_2) = w_2$.
- $V = \mathbb{K}^{n\times 1}$, $W = \mathbb{K}^{m\times 1}$. Ist $A \in K^{m\times n}$, so ist die Abbildung $\varphi_A : V \longrightarrow W, x \longmapsto Ax$ linear.
  Sei $e_i = (0,...,0,1,0,...,0)^T \in K^{n\times 1}$ mit 1 in der i-ten Zeile. Dann ist $(e_1,e_2,...,e_n)$ Basisfolge von $K^{n\times 1}$. Es gilt:

  $$\varphi_A(e_i) = Ae_i = (a_{1i},...,a_{mi})^T \text{ (die } i - \text{te Spalte von} A)$$

  Nach Satz 1 (Seite 27) ist φ_A die eindeutig bestimmte lineare Abbildung $\varphi : K^{n\times 1} \longrightarrow K^{m\times 1}$ mit $\varphi(e_i) = (a_{1i},...,a_{mi})^T$. Also $Hom_K(K^{n\times 1}, K^{m\times 1}) = \{\varphi_A \,|\, A \in K^{m\times n}\}$.

3.2 Isomorphismen

Erinnerung: Ist $\varphi : X \longrightarrow Y$ Abbildung, so heißt φ injektiv gdw. $\varphi(x) = \varphi(x') \Rightarrow x = x'$, und surjektiv gdw. $Y = Bild\,\varphi := \{\varphi(x)\,|x \in X\}$. φ heißt bijektiv gdw. φ injektiv und surjektiv ist (also $\exists \varphi^{-1} : Y \longrightarrow X$ mit $\varphi \circ \varphi^{-1} = id_Y$ und $\varphi^{-1} \circ \varphi = id_X$, vgl. 1.1.2, Seite 2).

Definition 1 (Mono-, Epi-, Isomorphismus) Eine lineare Abbildung $\varphi : V \longrightarrow W$ heißt *Monomorphismus*, wenn φ injektiv ist, *Epimorphismus*, wenn φ surjektiv ist und *Isomorphismus*, wenn φ bijektiv ist. V, W heißen isomorphe K-Vektorräume (i.Z. $V \cong W$ oder $V \cong_K W$), wenn es (mindestens) einen Isomorphismus $\varphi : V \longrightarrow W$ gibt.

Lemma 1

1. Ist $\varphi : V \longrightarrow W$ ein Isomorphismus, so ist φ^{-1} auch linear, also Isomorphismus.
2. Sind $\varphi : V \longrightarrow W$, $\psi : W \longrightarrow U$ linear (bzw. isomorph), so ist auch $\psi \circ \varphi : V \longrightarrow U$ linear (isomorph).
3. $\cong$ ist Äquivalenzrelation (vgl. S. 4), d.h. reflexiv ($V \cong V$), symmetrisch ($V \cong W \Rightarrow W \cong V$) und transitiv ($V \cong W \wedge W \cong U \Rightarrow V \cong U$).

Beweis:

1. Sei $w, w' \in W$ und $s \in K$. Da φ surjektiv ist, ist $w = \varphi(v)$ für ein $v \in V$ und $w' = \varphi(v')$ für ein $v' \in V$. φ ist außerdem linear, also $\varphi(sv + v') = s\varphi(v) + \varphi(v') = sw + w'$, d.h. $\varphi^{-1}(sw + w') = sv + v' = s\varphi^{-1}(w) + \varphi^{-1}(w')$, also ist φ^{-1} linear (Isomorphismus).
2. Sei $v, v' \in V$ und $s \in K$.
   (a) φ, ψ linear $\Rightarrow \psi \circ \varphi$ ist linear.
   $\psi \circ \varphi(sv + v') = \psi(\varphi(sv + v')) = \psi(s\varphi(v) + \varphi(v')) = s\psi(\varphi(v)) + \psi(\varphi(v')) = s(\psi \circ \varphi)(v) + (\psi \circ \varphi)(v')$.
   (b) φ, ψ injektiv $\Rightarrow \psi \circ \varphi$ ist injektiv.
   Sei $(\psi \circ \varphi)(v) = (\psi \circ \varphi)(v')$, $v, v' \in V$. Dann (da ψ und φ injektiv sind):
   $\psi(\varphi(v)) = \psi(\varphi(v')) \Rightarrow \varphi(v) = \varphi(v') \Rightarrow v = v'$.
   (c) φ, ψ surjektiv $\Rightarrow \psi \circ \varphi$ ist surjektiv.
   Sei $u \in U$. Da ψ surjektiv ist, gibt es ein $w \in W$ mit $u = \psi(w)$, da φ surjektiv ist, existiert ein $v \in V$ mit $w = \varphi(v)$, daher $u = (\psi \circ \varphi)(v)$.
3. Zunächst einmal ist immer die identische Abbildung $id_V : V \longrightarrow V$ ein Isomorphismus, also $V \cong V$, $\cong$ reflexiv. Die Symmetrie folgt aus (1), Transitivität aus (2). □

Satz 1 Es sei $(v_i)_{i \in I}$ eine Basisfolge von V (I Indexmenge) und $\varphi : V \longrightarrow W$ linear. Dann gilt:

1. φ Monomorphismus $\Leftrightarrow (\varphi(v_i))_{i \in I}$ linear unabhängig als n-Tupel (d.h. $\varphi(v_i)$ disjunkt und $\{\varphi(v_i)\}_{i \in I}$ linear unabhängig) bzw. $\sum_{i \in I} s_i \varphi(v_i) = \mathfrak{o} \Rightarrow s_i = 0\,(i \in I)$.
2. φ Epimorphismus $\Leftrightarrow \langle \varphi(v_i) \rangle_{i \in I} = W$
3. φ Isomorphismus $\Leftrightarrow (\varphi(v_1))_{i \in I}$ ist Basisfolge

Beweis:

1. Es gilt:

$$\begin{array}{lll} & \varphi \text{ Monomorphismus} & \\ \Leftrightarrow & \varphi \text{ injektiv} & \\ \Leftrightarrow & \varphi(v) = \varphi(v') \Rightarrow v = v'; v, v' \in V & \\ \Leftrightarrow & \left(\varphi(\sum\limits_i s_i v_i) = \varphi(\sum\limits_i s'_i v_i) \;\Rightarrow\; s_i = s'_i \, \forall i \in I\right) & s_i, s'_i \in K,\ s_i, s'_i \neq 0 \text{ für endl. viele } i \in I \\ \Leftrightarrow & \left(\sum\limits_i s_i \varphi(v_i) = \sum\limits_i s'_i \varphi(v_i) \;\Rightarrow\; s_i - s'_i = 0\right) & \text{für alle } i \in I \\ \Leftrightarrow & \left(0 = \sum\limits_i (s_i - s'_i) \cdot \varphi(v_i) \;\Rightarrow\; s_i - s'_i = 0\right) & \text{für alle } i \in I \\ \Leftrightarrow & (\varphi(v_i))_{i \in I} \text{ ist linear unabhängig} & \end{array}$$

2. Es gilt:

$$\begin{array}{lll} & \varphi \text{ Epimorphismus} & \\ \Leftrightarrow & W = Bild\, \varphi = \{\varphi(v)\,|\, v \in V\} & s_i \neq 0 \text{ nur für endl. viele } i \in I \\ & = \{\varphi(\sum_i s_i v_i)\,|\, s_i \in K\} = \{\sum_i s_i \varphi(v_i)\,|\, s_i \in K\} & \\ & = \langle \varphi(v_i) \rangle_{i \in I} & \end{array}$$

3. Folgt aus (1) und (2). □

Satz 2 Sind V, W K-Vektorräume und endlich erzeugt, so gilt $V \cong W \Leftrightarrow dim V = dim W$. Insbesondere ist $V \cong K^n$, wenn $dim V = n$.

Beweis:

- $V \cong W$, V endlich erzeugt, $(v_1, \ldots, v_n)$ sei Basisfolge von V, $n = dim V$, $\varphi : V \longrightarrow W$ Isomorphismus. Nach Satz 1 (3) (Seite 28) ist $(\varphi(v_1), \ldots, \varphi(v_n))$ Basisfolge von W, also $dim W = n = dim V$.
- Sei $dim V = dim W = n$. V hat Basisfolge $(v_1, \ldots, v_n)$, W hat Basisfolge $(w_1, \ldots, w_n)$. Nach Satz 1 (Seite 27) existiert genau eine lineare Abbildung $\varphi \longrightarrow W$ mit $\varphi(v_i) = w_i$. Nach Satz 1 (3) (Seite 28) ist φ ein Isomorphismus, $V \cong W$. □

Definition 2 (Gleichmächtigkeit): Seien B, B' Mengen, so heißen B und B' *gleichmächtig* (i.Z. $|B| = |B'|$), wenn es eine bijektive Abbildung $\varphi : B \longrightarrow B'$ gibt.

Bemerkung: Ist B Basis von V, B' von W (V, W K-Vektorräume), so gilt $V \cong W \Leftrightarrow |B| = |B'|$

Beispiel:

Ist $dim V = n \in \mathbb{N}$ (V ist K-Vektorraum) und $B = (v_1, \ldots, v_n)$ Basisfolge von V, so ist φ_B ein Isomorphismus mit

$$\varphi_B : \begin{array}{ccc} V & \longrightarrow & K^{n \times 1} \\ v = \sum_{i=1}^n x_i v_i & \longmapsto & \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \varphi_B(v) =_B [v] \end{array}$$

Allgemeiner: Ist B eine Basis von V, so ist

$$\psi_B : \begin{array}{ccc} V & \longrightarrow & K^{(B)} \\ v = \sum_{b \in B} f(b) b & \longmapsto & f \end{array}$$

Isomorphismus.

3.3 Kern und Bild

Definition 1 (Kern, Bild) Ist $\varphi : V \longrightarrow W$ eine K-lineare Abbildung, so ist der *Kern* von φ definiert als $Kern\,\varphi = \{v \in V \,|\, \varphi(v) = \mathit{o}\} = \overset{-1}{\varphi}(\mathit{o})$ und das *Bild* als $Bild\,\varphi = \{\varphi(v) \,|\, v \in V\}$.

Lemma 1 Ist $\varphi : V \longrightarrow W$ linear, so gilt:

1. $Kern\,\varphi$ ist Teilraum von V und es gilt:
   $Kern\,\varphi = \{\mathit{o}\} \Leftrightarrow \varphi$ ist Monomorphismus (injektiv)
2. $Bild\,\varphi$ ist Teilraum von W und es gilt:
   $Bild\,\varphi = W \Leftrightarrow \varphi$ ist Epimorphismus (surjektiv)

Beweis:

1. Sei $v, v' \in Kern\,\varphi$, $s \in K$. Zu zeigen: $sv + v' \in Kern\,\varphi$.
   $\varphi(sv+v') = s\varphi(v) + \varphi(v') = s \cdot \mathit{o} + \mathit{o}$ (weil $v, v' \in Kern\,\varphi$), also $sv + v' \in Kern\,\varphi$.
2. Es gilt:
$$\begin{array}{rcll} \varphi \text{ injektiv} & \Leftrightarrow & \varphi(v) = \varphi(v') \Rightarrow v = v' & v, v' \in V \\ & \Leftrightarrow & \varphi(v-v') = \mathit{o} \Rightarrow v - v' = \mathit{o} & \\ & \Leftrightarrow & \varphi(v'') = \mathit{o} \Rightarrow v'' = \mathit{o} & v'' \in V \\ & \Leftrightarrow & Kern\,\varphi = \{\mathit{o}\} & \end{array}$$
3. Sei $Bild\,\varphi = \{\varphi(v) \,|\, v \in V\}$, zeige, daß $Bild\,\varphi$ Teilraum ist. Seien also $\varphi(v), \varphi(w) \in Bild\,\varphi$, $s \in K$, dann ist $s\varphi(v) + \varphi(v') = \varphi(sv+v') \in Bild\,\varphi$. □

Beispiel:

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

$$\varphi_A : \begin{array}{ccc} K^{n\times 1} & \longrightarrow & K^{m\times 1} \\ (x_1,\ldots,x_n)^T & \longmapsto & A\cdot(x_1,\ldots,x_n)^T \end{array}$$

$Kern\,\varphi_A = \left\{(x_1,\ldots,x_n)^T \,\middle|\, A\cdot(x_1,\ldots,x_n)^T = \mathit{o}\right\}$ ist die Lösung des homogenen Gleichungssystems mit Koeffizientenmatrix A. Weiterhin ist also die Lösungsmenge eines homogenen linearen Gleichungssystems $Kern\,\varphi_A$, also ein Teilraum von $K^{n\times 1}$.

Satz 1 (Dimensionssatz) Ist $dim\,V = n < \infty$ und $\varphi : V \longrightarrow W$ ($dim\,W < \infty$) eine lineare Abbildung, dann gilt:
$$dim\,Kern\,\varphi + dim\,Bild\,\varphi = dim\,V$$

Beweis: Sei $B = (v_1,\ldots,v_d)$ Basisfolge von $Kern\,\varphi$, dann ist $d = dim\,Kern\,\varphi$. Nach dem Basisergänzungssatz (Seite 21) kann man B ergänzen zu einer Basis B' von V:
$$B' = (v_1,\ldots,v_d,v_{d+1},\ldots,v_n),\, n = dim\,V,\, |\{v_{d+1},\ldots,v_n\}| = n-d$$
Zu zeigen: $n - d = dim\,Bild\,\varphi$, also $B'' = (\varphi(v_{d+1}),\ldots,\varphi(v_n))$ ist Basisfolge von $Bild\,\varphi$, oder (1) $\langle B''\rangle = Bild\,\varphi$ sowie (2) B'' linear unabhängig.

1. Sei $w \in Bild\,\varphi$ beliebig, $w = \varphi(v)$ für ein $v \in V$, B Basisfolge von V, also $v = \sum_{i=1}^{n} s_i v_i$, $s_i \in K$. Es gilt:
$$w = \varphi(v) = \varphi\left(\sum_{i=1}^{n} s_i v_i\right) = \sum_{i=1}^{n} s_i\varphi(v_i) = \sum_{i=d+1}^{n} s_i\varphi(v_i)$$
   denn $\varphi(v_1) = \ldots = \varphi(v_d) = \mathit{o}$, $v_i \in Kern\,\varphi$, $1 \le i \le d$, also $w \in \langle B''\rangle$.

2. Sei $s_{d+1}\varphi(v_{d+1}) + \ldots + s_n\varphi(v_n) = \mathfrak{o}$ mit $s_i \in K$, zu zeigen: $s_{d+1} = \ldots = s_n = 0$.
   Es gilt $\varphi\left(\sum\limits_{i=d+1}^{n} s_i v_i\right) = \mathfrak{o}$, weil φ linear ist. Da $B = (v_1, \ldots, v_d)$ Basisfolge von $Kern\,\varphi$ ist, gilt $\sum_{i=d+1}^{n} s_i v_i = \sum_{j=1}^{d} s_j v_j$ mit $s_1, \ldots, s_d \in K$. Demnach gilt also:
   $$\mathfrak{o} = -\sum_{i=d+1}^{n} s_i v_i + \sum_{j=1}^{d} s_j v_j, \text{ also } s_1 = \ldots = s_d = -s_{d+1} = \ldots = -s_n = 0$$
   Die Linearkombination der Vektoren $(\varphi(v_1), \ldots, \varphi(v_n)) = B''$ ist also linear unabhängig. □

Definition 2 (Rang einer Abbildung) Ist $\varphi : V \longrightarrow W$ lineare Abbildung, so ist der *Rang* von φ definiert als
$$Rg\,\varphi := dim\,Bild\,\varphi$$

Folgerung 1 Ist $\varphi : V \longrightarrow W$ linear, $dim V, dim W < \infty$, so ist $dim\,Kern\,\varphi = dim V - Rg\, f$.

Beispiel:

$A \in K^{m\times n}$, $\varphi = \varphi_A$, $\varphi_A : K^{n\times 1} \longrightarrow K^{m\times 1}, x \longmapsto Ax$. $Kern\,\varphi$ ist die Lösungsmenge des Gleichungssystems $Ax = \mathfrak{o}$, also ist die Lösungsmenge Vektorraum der Dimension $n - Rg\,\varphi_A$.

Definition 3 (Rang einer Matrix) Ist $A \in K^{m\times n}$ (K Körper), so ist der *Rang* der Matrix A definiert als
$$Rg\,A := Rg\,\varphi_A = dim\,Bild\,\varphi_A$$
wobei $\varphi_A : K^{n\times 1} \longrightarrow K^{m\times 1}, x \longmapsto Ax$.

Beispiel:

$Rg\,A := Rg\,\varphi_A := dim\,Bild\,\varphi_A$, e_i Einheitsvektoren, $\{e_1, \ldots, e_n\}$ Standardbasis von $K^{n\times 1}$.

$Bild\,\varphi_A = \langle \varphi_A(e_1), \ldots, \varphi_A(e_n)\rangle = \langle Ae_1, \ldots, Ae_n\rangle = \left\langle (a_{11}, \ldots, a_{m1})^T, \ldots, (a_{1n}, \ldots, a_{mn})^T \right\rangle$

Dabei heißt $\left\{(a_{11}, \ldots, a_{m1})^T, \ldots, (a_{1n}, \ldots, a_{mn})^T\right\}$ der Spaltenraum von A.

Folgerung 2 Sei $dim V < \infty$ und $\varphi : V \longrightarrow W$ linear. Dann gilt:

1. φ ist Monomorphismus (injektiv) genau dann, wenn $Rg\,\varphi = dim V$
2. φ ist Epimorphismus (surjektiv) genau dann, wenn $Rg\,\varphi = dim W$
3. Ist $dim V = dim W$, so gilt: φ Monomorphis $\Leftrightarrow$ φ Epimorphismus $\Leftrightarrow$ φ Isomorphismus
4. φ ist Monomorphismus genau dann, wenn $Kern\,\varphi = \{\mathfrak{o}\}$, also wenn $dim\,Kern = 0$

Bemerkung: Sei $f : X \longrightarrow Y$ eine Abbildung und seien X und Y endliche Mengen. f ist genau dann injektiv (surjektiv), wenn $|X| = |Bild\, f|$ ($|Y| = |Bild\, f|$).

Beispiel:

Es sei die V die Menge der Polynomfunktionen von $\mathbb{R}$ nach $\mathbb{R}$, also
$$V = \mathbb{P}(\mathbb{R}) = \left\{ f : \mathbb{R} \longrightarrow \mathbb{R} \,\middle|\, \exists n \in \mathbb{N}_0; a_0, \ldots, a_n \in \mathbb{R} : \; f(x) = \sum_{i=0}^{n} a_i x^i, x \in \mathbb{R} \right\}$$

Sei weiterhin $\varphi : V \longrightarrow V, f \longmapsto f'$ (f' Ableitung von f) linear. Dann gilt $(cf_1 + f_2)' = cf_1' + f_2', c \in \mathbb{R}, f_1, f_2 \in V$. $Kern\,\varphi = \langle p_0\rangle$ (wobei $p_0(x) = 1 = x^0$), $dim\,Kern\,\varphi = 1$, φ nicht injektiv, aber surjektiv.

3.4 Homomorphiesatz

Frage: Sei $\varphi : V \to W$. Es ist bekannt, daß $\overset{-1}{\varphi}(o) = Kern\,\varphi$. Was ist $\overset{-1}{\varphi}(w)$ für $w \in W$?

Beispiel:

$V = \mathbb{R}^2$

$\varphi : V \longrightarrow V, (x,y) \longmapsto (x-y, y-x)$

$Kern\,\varphi = \{(x,y) \in V \,|x = y\}$, $Bild\,\varphi = \{(z,-z) \in V \,|z \in \mathbb{R}\}$

$v_0 = (z,0)$, $w = \varphi(v_0) = (z,-z) \in Bild\,\varphi$

$$\begin{aligned} \overset{-1}{\varphi}(w) &= \{(x,y)\,|\varphi(x,y) = w\} = \{(x,y)\,|x-y = z\} \\ &= \left\{v_0 + x \,\middle|\, x \in \mathbb{R}^2\right\} = \{v_0 + u\,|u \in Kern\,\varphi\} \end{aligned}$$

Satz 1 Ist $\varphi : V \longrightarrow W$ eine lineare Abbildung, $w \in W$ mit $\varphi(v_o) = w$ für ein $v_0 \in V$, d.h. $w \in Bild\,\varphi$. Dann ist

$$\overset{-1}{\varphi}(w) = \{v\,|\varphi(v) = w\} = \{v_0 + u\,|u \in Kern\,\varphi\}$$

Definition 1 (Restklasse, Restklassenraum) Ist U Teilraum von V so ist für $v \in V$

$$v + U := \{v + u\,|u \in U\}$$

die *Nebenklasse* (*Restklasse*) von V nach U. Die Menge der Restklassen $V/U := \{v + U\,|v \in V\}$ heißt *Restklassenraum* (*Faktorraum*).

vergleiche hierzu auch $\mathbb{Z}/_{(m)} = \{[x]_m\,|x \in \mathbb{Z}, m \in \mathbb{N}\}$; $[x]_m = \{x + zm\,|z \in \mathbb{Z}\}$, Seite 5.

Bemerkung: Ist U Teilraum von V, so sei für $v, v' \in V$ definiert: $v \sim_U v' \Leftrightarrow v - v' \in U$. Dann ist $\sim_U$ Äquivalenzrelation und

$$[v]_{\sim_U} = \left\{v' \in V \,\middle|\, v - v' \in U\right\} = \{v + u\,|u \in U\} = v + U$$

Satz 2 Ist U Teilraum von V (V ist K-Vektorraum), so wird $V/U = \{v + U\,|v \in V\}$ zu einem K-Vektorraum mit $(v+U) + (v'+U) := (v+v') + U$ und $s \cdot (v+U) := sv + U$ ($v, v' \in U, s \in K$). Die Abbildung $\pi_U : V \longrightarrow V/U, v \longmapsto v + U$ ist dann ein Epimorphismus mit $Kern\,\pi_U = U$.

Satz 3 (Homomorphiesatz) Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung.

1. Dann ist $Kern\,\varphi$ Teilraum von V, $Bild\,\varphi$ Teilraum von W.
2. Ist $\pi = \pi_{Kern\,\varphi} : V \longrightarrow V/Kern\,\varphi, v \longmapsto v + Kern\,\varphi$, so gilt $\Phi : V/Kern\,\varphi \longrightarrow Bild\,\varphi, v + Kern\,\varphi \longmapsto \varphi(v)$ ist Isomorphismus und $\varphi = \Phi \circ \pi$.

Beweis:

1. Bereits erledigt, vgl. Lemma 1, Seite 30

2. Wohldefiniertheit von Φ:

$$v + Kern\,\varphi = v' + Kern\,\varphi \Leftrightarrow v - v' \in Kern\,\varphi \Leftrightarrow \varphi(v - v') = \underline{0} \Leftrightarrow \varphi(v) = \varphi(v')$$

"$\Rightarrow$" bedeutet: Φ ist wohldefiniert, "$\Leftarrow$" bedeutet: Φ ist injektiv. Offensichtlich ist Φ surjektiv, also bijektiv. Überprüfung der Linearität ($v, v' \in V, s \in K$):

$$\begin{aligned}\Phi(s(v + Kern\,\varphi) + (v' + Kern\,\varphi)) &= \Phi(sv + v' + Kern\,\varphi)\\ &= \varphi(sv + v') = s\varphi(v) + \varphi(v')\\ &= s\Phi(v + Kern\,\varphi) + \Phi(v' + Kern\,\varphi)\end{aligned}$$

□

Folgerung 1

1. Ist U Teilraum von V, $dim V < \infty$, dann gilt: $dim V/U = dim V - dim U$.
2. Jeder Teilraum eines Vektorraums ist Kern einer linearen Abbildung.

Beweis:

1. Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Nach Dimensionssatz gilt dann: $dim\,Kern\,\varphi + dim\,Bild\,\varphi = dim V$. Wende dies an mit $\varphi = \pi_U : V \longrightarrow V/U, v \longmapsto v + U$. Dann ist $Bild\,\pi_U = V/U$ und $Kern\,\pi_U = \{v \in V \,|\, v + U = \underline{0} + U\} = U$.
2. U ist Kern von $\pi_U : V \longrightarrow V/U$ □

3.5 Rang einer Matrix

Definition 1 (Zeilenraum, Spaltenraum) Sei $A = [a_{ij}] \in K^{m\times n}$. Dann ist der *Zeilenraum* $ZR(A)$ (*Spaltenraum* $SR(A)$) definiert als:

$$ZR(A) := \langle (a_{11}, a_{12}, \ldots, a_{1n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn}) \rangle \leq K^{1\times n}$$

$$SR(A) := \left\langle \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \ldots, \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} \right\rangle \leq K^{m\times 1}$$

Satz 1 Ist $A = [a_{ij}] \in K^{m\times n}$, so gilt:

1. $Rg A = dim\,SR(A) = dim \left\langle (a_{11}, a_{21}, \ldots, a_{m1})^T, \ldots, (a_{1n}, a_{2n}, \ldots, a_{mn})^T \right\rangle$
2. Der Rang von A ändert sich nicht bei elementaren Spaltenoperationen.
3. Der Rang von A ändert sich nicht bei elementaren Zeilenoperationen.

Beweis:

1. Sei $\varphi_A : K^{n\times 1} \longrightarrow K^{m\times 1}, x \longmapsto Ax$. Dann:

$$Rg A = dim\,Bild\,\varphi_A = dim \langle \varphi_A(e_1), \ldots, \varphi_A(e_n) \rangle = dim \langle Ae_1, \ldots, Ae_n \rangle = dim\,SR(A)$$

2. Gilt nach Lemma 2, Seite 22.

3. Betrachte das Gleichungssystem $Ax = \mathfrak{o}$. Das Gleichungssystem hat die Lösungsmenge $L = Kern\,\varphi_A$. L ändert sich nicht bei elementaren Zeilenoperationen, daher gilt, sofern A' auf A durch elementare Zeilenoperationen entsteht: $Kern\,\varphi_{A'} = Kern\,\varphi_A$.
Nach dem Dimensionssatz ist $dim\,Kern\,\varphi_{A'} = n - Rg\,A'$ und $dim\,Kern\,\varphi_A = n - Rg\,A$, also $Rg\,A' = Rg\,A$. □

Beispiel:

$$
\begin{aligned}
Rg\begin{bmatrix} 17 & \frac{1}{3} & \sqrt{3} & \pi & 1+i & e \\ 1 & i & \sqrt{2} & 0 & 3 & 17 \\ i & e & \sqrt{3} & 0 & 5 & 16 \end{bmatrix}
&= Rg\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & i & \sqrt{2} & 0 & 3 & 17 \\ i & e & \sqrt{3} & 0 & 5 & 16 \end{bmatrix} \\
&= Rg\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & i & \sqrt{2} & 0 & 3 & 17 \\ 0 & e+1 & \sqrt{3}-\sqrt{2}i & 0 & 5-3i & 16-17i \end{bmatrix} \\
&= Rg\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \\
&= dim\,\langle e_2, e_3, e_1\rangle = 3
\end{aligned}
$$

Satz 2

1. Jede $m \times n$-Matrix $A \in K^{m\times n}$, K Körper, kann man mittels elementarer Zeilen- und Spaltenoperationen auf die Form
$$\begin{bmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ 0 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & & 1 & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{bmatrix}$$
bringen, wobei in der "Hauptdiagonalen" $r = Rg\,A$ Einsen sind.

2. Ist $ZR(A) = \langle [a_{11},\dots,a_{1n}],\dots,[a_{m1},\dots,a_{mn}]\rangle$ der Zeilenraum von A, so ist $dim\,ZR(A) = dim\,SR(A) = Rg\,A$ (Zeilenrang=Spaltenrang).

Beweis: In Kapitel 1 wurde bereits bewiesen, daß man durch elementare Zeilenoperationen die Matrix A auf Stufenform bringen kann (vgl. Seite 9). Diese Matrix in Stufenform heiße A'; r sei die Anzahl der "Stufen", beachte: die ersten r Zeilen von A' sind linear unabhängig, $dim\,ZR(A') = r$.
Durch Anwendung von elementaren Spaltenoperationen entsteht A'' in der in Satz 2 (1) gegebenen Form. Es gilt dann:
$$Rg\,A = Rg\,A'' = r$$
□

3.6 Hauptsatz über lineare Gleichungssysteme

Satz 1 (Hauptsatz über lineare Gleichungssysteme)

1. Ein homogenes lineares Gleichungssystem $Ax = \mathfrak{o}$ mit $A \in K^{m\times n}$ hat eine Lösungsmenge L_0, die ein Teilraum von $K^{n\times 1}$ ist mit $dim\,L_0 = n - Rg\,A$.
Insbesondere hat $Ax = \mathfrak{o}$ nur die triviale Lösung $x = \mathfrak{o}$ gdw. $n = Rg\,A$.

2. Das Gleichungssystem $Ax = b$ mit $A \in K^{m\times n}$, $b \in K^{m\times 1}$ ist genau dann lösbar, wenn $Rg\,A = Rg\,[A,b]$, wobei $[A,b]$ die erweiterte Matrix ist.
3. Ist $v_1 \in K^{n\times 1}$ Lösung von $Ax = b$ (d.h. $Av_1 = b$), so ist die gesamte Lösungsmenge von $Ax = b$ die Restklasse $v_1 + L_0 = \{v_1 + v \,|\, v \in L_0\}$.
   Insbesondere gilt: Ist $Ax = b$ eindeutig lösbar, so muß $rang\,A = n$ sein.
4. Ist $m \leq n$, so gilt: Ist $Rg\,A = n$, dann ist $Ax = b$ eindeutig lösbar.

Beweis:

1. L_0 ist der Kern von $\varphi_A : K^{n\times 1} \longrightarrow K^{m\times 1}, x \longmapsto Ax$. Also ist L_0 als Kern einer linearen Abbildung ein Teilraum von $K^{n\times 1}$. Dann gilt (1) nach dem Dimensionssatz $dim\,L_0 + dim\,Bild\,\varphi_A = dim\,K^{n\times 1} = n$ mit $dim\,Bild\,\varphi_A = Rg\,A$.
2. Es gilt:
$$\begin{aligned} & Ax = b \text{ ist lösbar } \Leftrightarrow b \in Bild\,\varphi_A = SR(A) \\ \Leftrightarrow\ & SR(A) = \langle SR(A), b\rangle \Leftrightarrow Rg\,A = dim\,SR(A) = dim\,\langle SR(A), b\rangle = Rg\,[A,b] \end{aligned}$$
3. Die Lösungsmenge L_b ist $\overset{-1}{\varphi_A}(b)$, also die Restklasse $v_1 + L_0$ (Satz 1, Seite 32).
4. $Rg\,A \leq Rg[A,b] \leq m$, da $Rg(A,b) = dim\,SR\,[A,b] \leq K^{m\times 1}$. Ist $Rg\,A = n$, $m \leq n$, dann:
$$n = Rg\,A \leq Rg\,[A,b] \leq m \leq n \Rightarrow n = Rg\,A = Rg\,[A,b] = m = n$$
   Weiterhin folgt aus $Rg\,A = Rg\,[A,b]$, daß $Ax = b$ lösbar ist. □

Beispiel (van-der-Monde-Gleichungssystem):

Sei K Körper, $x_0,\ldots,x_n \in K$, $A = A_{x_0,\ldots,x_n} = \begin{bmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{bmatrix} \in K^{n\times n}$ (van-der-Monde-Matrix).

Voraussetzung: $x_0,\ldots,x_n$ paarweise verschieden. Dann:

$$\begin{aligned} Rg\,A &= Rg \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & x_1 - x_0 & x_1^2 - x_0x_1 & \ldots & x_1^n - x_0x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n - x_0 & x_n^2 - x_0x_n & \ldots & x_n^n - x_0x_n^{n-1} \end{bmatrix} \\ &= Rg \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & (x_1 - x_0) & x_1(x_1 - x_0) & \ldots & x_1^{n-1}(x_1 - x_0) \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & (x_n - x_0) & x_n(x_n - x_0) & \ldots & x_n^{n-1}(x_n - x_0) \end{bmatrix} \\ &= Rg \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & x_1 & \ldots & x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & x_n & \ldots & x_n^{n-1} \end{bmatrix} \end{aligned}$$

Der rechte untere Teil der Matrix ist nun wieder eine van-der-Monde-Matrix, also:

$$= \ldots = Rg \begin{bmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{bmatrix} = n + 1$$

Folgerung: Das Gleichungssystem $A_{x_0,\dots,x_n}\begin{bmatrix} a_0 \\ \vdots \\ a_n \end{bmatrix} = o$ ist nur trivial lösbar. Also:

$$\begin{array}{ccccccccc} a_0 & + & x_0 a_1 & + & \dots & + & x_0^n a_n & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_0 & + & x_n a_1 & + & \dots & + & x_n^n a_n & = & 0 \end{array} \Rightarrow a_1 = \dots = a_n = 0$$

Satz 2 Ist $f : K \longrightarrow K$ eine Polynomfunktion höchstens n-ten Grades, d.h. gibt es $a_0, a_1, \dots, a_n \in K$ mit $f(x) = \sum_{i=0}^n x^i a_i$, so hat f höchstens n Nullstellen oder $f(x) = \underline{0}$ ist die Nullfunktion.

Beweis: Angenommen, f hätte die paarweise verschiedenen Nullstellen $x_0, \dots, x_n \in K$, also $f(x_j) = \sum_{i=0}^n a_i x_j^i = 0$ für $j = 0, \dots, n$. Dann folgt (nach der van-der-Monde-Matrix) $a_0 = \dots = a_n = 0$, d.h. $f(x) = \underline{0}$. □

Satz 3 Ist K Körper mit $|K| > n$, so sind die Polynomfunktionen $p_i : K \longrightarrow K, x \longmapsto x^i$ $(0 \le i \le n)$ linear unabhängig, genauer: $\{p_i | 0 \le i \le n\}$ ist linear unabhängig.

Beweis: Angenommen, $\sum\limits_{i=0}^n a_i p_i = 0$, $a_i \in K$. Wähle in K paarweise verschiedene Elemente $x_0, \dots, x_n \in K$ (Beachte: n verschiedene Elemente nur, weil $|K| > n$!). Setze nacheinander in $\sum\limits_{i=0}^n a_i x_j^i = 0$ $x_0, x_1, \dots, x_n$ ein. Dann $(j = 0, \dots, n)$:

$$\sum_{i=0}^n a_i x_j^i = 0 \Rightarrow a_0 = \dots = a_n = 0$$

□

3.7 Matrix einer linearen Abbildung

Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung. Sei $B = (v_1, \dots, v_n)$ Basisfolge von V und $B' = (w_1, \dots, w_m)$ Basisfolge von W. Nach Satz 1 (Seite 27) ist φ vollständig bestimmt durch $\varphi(v_j)$ für $j = 1, \dots, n$. Da B' Basisfolge von W ist, gibt es ein $a_{ij} \in K$ mit $\varphi(v_j) = \sum_{i=1}^m a_{ij} w_i$ $(j = 1, \dots, n)$ eindeutig bestimmt.

Definition 1 (Matrix einer linearen Abbildung): Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, V, W K-Vektorräume, $B = (v_1, \dots, v_n)$ eine Basisfolge von V und $B' = (w_1, \dots, w_m)$ eine Basisfolge von W. Seien $a_{ij} \in K$ so gewählt, daß $\varphi(v_j) = \sum_{i=1}^m a_{ij} w_i$ $(j = 1, \dots, n)$. Dann heißt die Matrix

$$_{B'}\varphi_B = {}_{B'}[\varphi]_B = [a_{ij}] \in K^{m \times n}$$

Matrix der linearen Abbildung φ bezüglich der Basenfolgen B und B'.

Merke: In den Spalten von $_{B'}[\varphi]_B$ stehen die Koeffizienten der Bilder der Basisvektoren von B bezüglich der Basis B'.

$$\begin{array}{ccc} & \kappa_B & \\ V & \longrightarrow & K^{n\times 1} \\ \varphi\downarrow & & \downarrow \varphi_A \\ W & \longrightarrow & K^{m\times 1} \\ & \kappa_{B'} & \end{array}$$

Abbildung 3.1: Beziehungen unter den linearen Abbildungen.

Beispiele:

- $A \in K^{m\times n}$, $\varphi_A : K^{n\times 1} \longrightarrow K^{m\times 1}, x \longmapsto Ax$; $B = (e_1, \ldots, e_n)$ Standardbasis von $K^{n\times 1}$, $B' = (f_1, \ldots, f_m)$ Standardbasis von $K^{m\times 1}$. $\varphi_A(e_j) = A \cdot e_j = (a_{1j}, \ldots, a_{mj})^T = \sum_{i=1}^m a_{ij} f_i$ für $j = 1, \ldots, n$, also:

$$_{B'}[\varphi]_B = \left[\begin{array}{ccc} & a_{1j} & \\ \leftarrow & : & \rightarrow \\ & a_{mj} & \end{array} \right] = A$$

- $V = \langle sin, cos \rangle \leq \mathbb{R}^{\mathbb{R}}$, $\varphi : V \longrightarrow V, f \longmapsto f'$ Ableitung.
  $B = B' = (sin, cos)$ Basisfolge von V, $\varphi(sin) = 0sin + 1cos = cos$, $\varphi(cos) = -1sin + 0cos = -sin$,

$$_{B'}[\varphi]_B = \left[\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \right]$$

- $\varphi : \mathbb{R} \longrightarrow \mathbb{R}^{2\times 1}, x \longmapsto \left(\begin{array}{c} x \\ -x \end{array} \right)$,
  $B = (1)$ Basisfolge von $\mathbb{R}$, $B' = (w_1 = (1, -1)^T, w_2 = (1, 0)^T)$ Basisfolge von $\mathbb{R}^{2\times 1}$,

$$_{B'}[\varphi]_B = \left[\begin{array}{c} 1 \\ 0 \end{array} \right]$$

Bezeichnung: Ist $B = (v_1, \ldots, v_n)$ Basisfolge von V. Dann ist

$$\kappa_B : \begin{array}{ccc} V & \longrightarrow & K^{n\times 1} \\ v = \sum_{j=1}^n a_j v_j & \longmapsto & \left[\begin{array}{c} a_1 \\ : \\ a_n \end{array} \right] = \kappa_B(v) = {_B v} = {_B[v]} \end{array}$$

κ_B ist Isomorphismus.

Satz 1 Ist $\varphi : V \longrightarrow W$ eine K-lineare Abbildung und sind $B = (v_1, \ldots, v_n)$ und $B' = (w_1, \ldots, w_m)$ Basisfolgen von V bzw. W, so gilt für beliebige $v \in V$:

$$_{B'}[\varphi(v)] = {_{B'}[\varphi]_B} \cdot {_B v}$$

d.h. für $A = {_{B'}[\varphi]_B} \in K^{m\times n}$ gilt $\kappa_{B'} \circ \varphi = \varphi_A \circ \kappa_B$, vgl. Abb. 3.1.

Beweis: $_{B'}[\varphi]_B = [a_{ij}] \in K^{m\times n}$ bedeutet $\varphi(v_j) = \sum_{i=1}^m a_{ij} w_i$, $v = \sum_{j=1}^n x_j v_j$, d.h.

$$_B v = \left[\begin{array}{c} x_1 \\ : \\ x_n \end{array} \right] = \kappa_B(v)$$

Also:

$$\begin{aligned}\varphi(v) &= \varphi\left(\sum_{j=1}^{n} x_j v_j\right) = \sum_{j=1}^{n} x_j \varphi(v_j) = \sum_{j=1}^{n} x_j \cdot \sum_{i=1}^{m} a_{ij} w_i = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{ij} x_j\right) w_i \\ &= {}_{B'}[\varphi(V)] = Ax\end{aligned}$$

□

Folgerung 1 $Rg\,\varphi = Rg\,{}_{B'}[\varphi]_B$, denn $\kappa_{B'}(Bild\,\varphi) = Bild\,\varphi_A$, also:

$$Rg\,\varphi = dim\,Bild\,\varphi = dim\,\kappa_{B'}(Bild\,\varphi) = dim\,Bild\,\varphi_A = Rg\,A$$

Satz 2 Seien $\psi : U \longrightarrow V$ und $\varphi : V \longrightarrow W$ lineare Abbildungen, $B = (u_1, ..., u_m)$ Basisfolge von U, $B' = (v_1, ..., v_n)$ von V und $B'' = (w_1, ..., w_p)$ von W. Dann:

$${}_{B''}[\varphi \circ \psi]_B = {}_{B''}[\varphi]_{B'} \cdot {}_{B'}[\psi]_B$$

Beweis: ${}_{B'}[\psi]_B = [a_{ij}] = A \in K^{n\times m}$, ${}_{B''}[\varphi]_{B'} = [c_{ij}] = C \in K^{p\times n}$, ${}_{B''}[\varphi\circ\psi]_B = [d_{ij}] = D \in K^{p\times m}$, $\psi(u_j) = \sum_{i=1}^{n} a_{ij} v_i$, $\varphi(v_k) = \sum_{l=1}^{p} c_{lk} w_l$. Dann:

$$\begin{aligned}(\varphi\circ\psi)(u_j) &= \varphi(\psi(u_j)) = \varphi\left(\sum_{i=1}^{n} a_{ij} v_i\right) = \sum_{i=1}^{n} a_{ij}\varphi(v_i) \\ &= \sum_{i=1}^{n} a_{ij} \cdot \sum_{l=1}^{p} c_{li} w_l = \sum_{l=1}^{p}\left(\sum_{i=1}^{n} a_{ij} c_{li}\right) w_l \\ &= \sum_{l=1}^{p}\sum_{i=1}^{n}(c_{li} a_{ij}) w_l = \sum_{l=1}^{p}[CA]_{lj}\cdot w_l = \sum_{l=1}^{p} d_{lj}\cdot w_l\end{aligned}$$

also $D = CA$. □

Folgerung 2 $B = (v_1, ..., v_n)$ Basisfolge von V, $B' = (w_1, ..., w_n)$ Basisfolge von V. Dann gilt mit $P := {}_{B'}[id_V]_B$, $Q := {}_B[id_V]_{B'}$:

$${}_B[id_V]_B = E_n = P\cdot Q = Q\cdot P = {}_{B'}[id_V\}_{B'}$$

Satz 3 Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung, B und B' Basisfolgen von V, C und C' Basisfolgen von W. Dann:

$${}_{C'}[\varphi]_{B'} = {}_{C'}[id_W]_C \cdot {}_C[\varphi]_B \cdot {}_B[id_V]_{B'}$$

Beweis: zweimalige Anwendung von Satz 2. □

Beispiel:

$V = \mathbb{R}^2$, $\varphi : V \longrightarrow V, (x,y) \longmapsto (-\frac{1}{3} + \frac{2}{3}y, \frac{4}{3}x + \frac{1}{3}y)$ linear

$B = (e_1, e_2)$

$$\begin{aligned}\varphi(e_1) &= \varphi((1,0)) = -\tfrac{1}{3}e_1 + \tfrac{4}{3}e_2 \\ \varphi(e_2) &= \varphi((0,1)) = \tfrac{2}{3}e_1 + \tfrac{1}{3}e_2\end{aligned} \quad \Rightarrow \; {}_B[\varphi]_B = \begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \\ \frac{4}{3} & \frac{1}{3}\end{bmatrix}$$

$B' = (v_1 = (1,2), v_2 = (1,-1))$

$$\begin{aligned}\varphi(v_1) &= \varphi((1,2)) = e_1 \\ \varphi(v_2) &= \varphi((1,-1)) = -e_2\end{aligned} \quad \Rightarrow \; {}_{B'}[\varphi]_{B'} = \begin{bmatrix} 1 & 0 \\ 0 & -1\end{bmatrix}$$

3.8 Algebra der linearen Abbildungen

Satz 1 Sind V,W Vektorräume über K, so ist $Hom(V,W) = \{\varphi : V \longrightarrow W \,|\, \varphi \text{ linear}\}$ ein Teilraum von $Abb(V,W) = W^V$ (Vektorraum aller Abbildungen von $V \longrightarrow W$).

Ist $B = (v_1,\ldots,v_n)$ Basisfolge von V, $B' = (w_1,\ldots,w_m)$ Basisfolge von W, so ist

$$\mu = {}_{B'}\mu_B : \begin{array}{ccc} Hom(V,W) & \longrightarrow & K^{m\times n} \\ \varphi & \longmapsto & {}_{B'}[\varphi]_B \end{array}$$

ein Isomorphismus von K-Vektorräumen. Insbesondere ist $\dim Hom(V,W) = mn$.

Beweis:

- Zu zeigen: $Hom(V,W)$ ist Teilraum
  1. $Hom(V,W)$ enthält trivialerweise $\underline{0} : V \longrightarrow W, v \longmapsto o$.
  2. Seien $\varphi,\psi \in Hom(V,W)$ und $s \in K$. Zu zeigen: $s\varphi+\psi \in Hom(V,W)$, $s\varphi+\psi : V \longrightarrow W$ linear.
  $$\begin{aligned}(s\varphi+\psi)(tv_1+v_2) &= s\varphi(tv_1+v_2)+\psi(tv_1+v_2)\\ &= s(t\varphi(v_1))+\varphi(v_2))+t\psi(v_1)+\psi(v_2)\\ &= t(s\varphi(v_1)+\psi(v_1))+s\varphi(v_2)+\psi(v_2)\\ &= t((s\varphi+\psi)(v_1))+(s\varphi+\psi)(v_2)\end{aligned}$$

- Zu zeigen: μ ist Isomorphismus (B,B',μ wie in Satz 1), also μ (1) ist linear, (2) injektiv, (3) surjektiv:
  1. Seien $\varphi,\psi \in Hom(V,W)$, $s \in K$. Zu zeigen: $\mu(s\varphi+\psi) = s\mu(\varphi)+\mu(\psi)$
  Sei $\mu(\varphi) = {}_{B'}\varphi_B = [a_{ij}] \in K^{m\times n}$ (d.h. $\varphi(v_j) = \sum_{i=1}^m a_{ij}w_i$) und $\mu(\psi) = {}_{B'}\psi_B = [c_{ij}] \in K^{m\times n}$, d.h. $\psi(v_j) = \sum_{i=1}^m c_{ij}w_i$.
  $$\begin{aligned}(s\varphi+\psi)(v_j) &= s\varphi(v_j)+\psi(v_j) = s\sum_{i=1}^m a_{ij}w_i + \sum_{i=1}^m c_{ij}w_i\\ &= \textstyle\sum_{i=1}^m (sa_{ij}+c_{ij})w_i = {}_B[s\varphi+\psi]_B\\ &= s[a_{ij}]+[c_{ij}] = s\mu(\varphi)+\mu(\psi), \text{ also } \mu \text{ linear}\end{aligned}$$
  2. $\varphi \in Kern\,\mu$ bedeutet: $o = \mu(\varphi) = {}_{B'}[\varphi]_B$. d.h. $\varphi(v_j) = o \in W$, also $\varphi = \underline{0}$. Demnach $\dim Kern\,\mu = 0$, μ injektiv.
  3. Sei $A = [a_{ij}] \in K^{m\times n}$ beliebig gegeben. Nach Satz 1 (Seite 27) gibt es (genau) eine lineare Abbildung $\varphi : V \longrightarrow W, \varphi(v_j) \longmapsto \sum_{i=1}^m a_{ij}w_i$, $j = 1,\ldots,n$.
  Dann ist nach Definition $\mu(\varphi) = {}_{B'}[\varphi]_B = A$, d.h. μ ist surjektiv. □

Definition 1 (Endomorphismus) Ist V ein K-Vektorraum, so ist $End(V) = Hom(V,V)$ und die Abbildungen in $End(V)$ heißen *Endomorphismen*.

Satz 2 Ist V ein K-Vektorraum, so ist $(End(V),+,\circ)$ mit $v \in V$ und

$$+ : (\varphi+\psi)(v) = \varphi(v)+\psi(v),\ \circ : (\varphi\circ\psi)(v) = \varphi(\psi(v))$$

ein Ring mit Eins ($1 = id_v$).

Ist $B = (v_1,\ldots,v_n)$ Basisfolge von V sowie $\mu_B = {}_B\mu_B : End(V) \longrightarrow K^{n\times n}, \varphi \longmapsto {}_B[\varphi]_B$ ein Ring-Isomorphismus, d.h. μ_B ist bijektiv und für $\lambda,\lambda' \in End(V)$ gilt:

1. $\mu(\lambda+\lambda') = \mu(\lambda)+\mu(\lambda')$
2. $\mu(\lambda\circ\lambda') = \mu(\lambda)\cdot\mu(\lambda')$
3. $\mu(id_V) = E_n$

Definition 2 (assoziative Algebra) Ist K Körper, so ist eine *assoziative K-Algebra A* ein K-Vektorraum $(A,+,\cdot)$ mit $+ : A \times A \longrightarrow A$, $\cdot : K \times A \longrightarrow A$ und mit zusätzlicher Multiplikation

$$\cdot : A \times A \longrightarrow A, (a,a') \longmapsto a \cdot a'$$

so daß $(A,+,\cdot)$ ein Ring ist und für alle $s \in K$, $a,a' \in A$ gilt:

$$s \cdot a \cdot a' = (s \cdot a) \cdot a' = a \cdot (s \cdot a')$$

Beispiel:

- V sei K-Vektorraum, dann ist $End(V)$ eine K-Algebra.
- Ist K Körper, so ist $K^{n\times n}$ für $n \in \mathbb{N}$ eine K-Algebra.
- $\mathbb{C}$ ist eine $\mathbb{R}$-Algebra, ein $\mathbb{R}$-Vektorraum, ein Körper.

3.9 Volle lineare Gruppen

Definition 1 (Gruppe) Eine *Gruppe G* ist eine Menge zusammen mit einer Verknüpfung $\circ : G \times G \longrightarrow G, (a,b) \longmapsto a \circ b$ mit

1. (G1) Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c)$, $a,b,c \in G$
2. (G2) Neutrales Element: Es gibt ein $e \in G$ mit $a \circ e = e \circ a = a$ für alle $a \in G$.
3. (G3) Inverses Element: Für alle $a \in G$ gibt es ein $a' \in G$ mit $a \circ a' = a' \circ a = e$.

Definition 2 (Monoid) Erfüllt eine Menge G nur die Eigenschaften (G1) und (G2) einer Gruppe, d.h. besitzt sie nicht unbedingt ein Inverses der Multiplikation, so heißt $(G,\circ)$ *Monoid*.

Beispiele:

- Ist $(K,+,\cdot)$ ein Ring, so ist $(K,+)$ eine Gruppe
- Ist $(K,+,\cdot)$ ein Ring mit Eins, so ist $(K,\cdot)$ ein Monoid
- Ist $(K,+,\cdot)$ ein Körper, so ist $(K \setminus \{0\},\cdot)$ eine Gruppe

Lemma 1 Es sei $(G,\circ)$ ein Monoid. Dann gilt:

1. Es gibt in G nur ein Element e mit der Eigenschaft (G2)
2. Gibt es zu $a \in G$ Elemente $x,y \in G$ mit $ax = e = ya$, so ist $x = y =: a'$. a heißt dann invertierbar. Insbesondere ist in $(G3)$, falls G eine Gruppe ist, a' eindeutig durch a bestimmt.
3. Sind $a,b \in G$ invertierbar, so gilt: $a \circ b$ ist invertierbar und $(a \circ b)' = b' \circ a'$

Beweis:

1. Habe $e' \in G$ hat auch die Eigenschaft $a \circ e' = e' \circ a = a$ für $a \in G$. Dann: $e' = e \circ e' = e$.
2. $a \circ x = e$ und $y \circ a = e$. Dann gilt: $x = e \circ x = (y \circ a) \circ x = y \circ (a \circ x) = y \circ e = y$
3. Es seien $a,a' \in G$ invertierbar und $a \circ a' = e$ sowie $b \circ b' = e$. Dann:

   $$(a \circ b)' = (a \circ b) \circ (b' \circ a) = a \circ (b \circ b') \circ a' = a \circ a' = e = b' \circ b = b' \circ (a' \circ a) \circ b = (b' \circ a') \circ (a \circ b)$$

$\square$

Bezeichnung: In einem Monoid $(G,\cdot)$ schreibt man a^{-1} statt a' und in einem Monoid $(G,+)$ schreibt man $-a$ statt a', falls $a \in G$ invertierbar ist.

Folgerung 1 Ist $(G,\circ)$ ein Monoid, so ist $G^\star = \{a \in G \,|\, a \, \text{invertierbar}\}$ eine Gruppe.

Definition 3 (Volle Lineare Gruppe) Für einen beliebigen Vektorraum V seien $GL(V)$ und $GL(n,K)$ mit K Körper, $n \in \mathbb{N}$ definiert als

$$GL(V) = \{\varphi \in End(V) \,|\, \varphi \, \text{ist bijektiv}\} \text{ bzw. } GL(n,K) = \{A \in K^{n\times n} \,|\, Rg A = n\}.$$

Satz 1

1. $(GL(V),\circ)$ ist Gruppe ("volle lineare Gruppe auf V", engl. "general linear group").
2. $GL(n,K)$ ist Gruppe ("volle lin. Gruppe vom Grad n über K") mit Matrixmultiplikation.
3. Ist $dim V = n$ und $B = (v_1,...,v_n)$ Basisfolge von V, so ist

$$\mu : \begin{array}{ccc} GL(V) & \longrightarrow & GL(n,K) \\ \varphi & \longmapsto & {}_B[\varphi]_B \end{array}$$

ein Isomorphismus von Gruppen, d.h. μ ist bijektiv und $\mu(\varphi \circ \varphi') = \mu(\varphi) \circ \mu(\varphi')$.

Lemma 2 Ist $A \in K^{m\times n}$, $C \in K^{n\times p}$, dann gilt: $Rg\,(A\cdot C) \le Rg A$ und $Rg\,(A\cdot C) \le Rg C$.

Beweis:

$$\begin{aligned} Rg\,(AC) &= dim Bild\, \varphi_{AC} = dim \left\{\varphi_{AC}(x) \,\middle|\, x \in K^{p\times 1}\right\} \\ &= dim \left\{\varphi_A(\varphi_C(x)) \,\middle|\, x \in K^{p\times 1}\right\} \le dim Bild\, \varphi_A = Rg A \end{aligned}$$

Analog mit $Rg\,(AC) \le Rg C$. □

Satz 2 Äquivalent sind für eine Matrix $A \in K^{n\times n}$

1. $Rg A = n$ (d.h. $A \in GL(n,K)$)
2. A ist in $K^{n\times n}$ "invertierbar", d.h. es existiert $A^{-1} \in K^{n\times n}$ mit $A\cdot A^{-1} = A^{-1}\cdot A = E_n$
3. Es gibt ein $X \in K^{n\times n}$ mit $A\cdot X = E_n$ (aus Lemma 1 folgt: $X = A^{-1}$)
4. Es gib $Y \in K^{n\times n}$ mit $Y\cdot A = E_n$ (aus Lemma 1 folgt: $Y = A^{-1}$)

Beweis: folgt aus Lemma 2. □

Frage: Wie findet man zu $A \in GL(n,K)$ das A^{-1} bzw. wie findet man zu A ein X mit $AX = E_n$?

Die j-te Spalte von $X = [x_{ij}]$ ist Lösung von $Ax = e_j$ (e_j ist j-te Spalte von E_n). Also sind die folgenden Gleichungssysteme zu lösen:

$$Ax = e_1 \text{ ergibt } \begin{bmatrix} x_{11} \\ : \\ x_{n1} \end{bmatrix}, ..., Ax = e_n \text{ ergibt } \begin{bmatrix} x_{1n} \\ : \\ x_{nn} \end{bmatrix}.$$

Das heißt, mit elementaren Zeilenoperationen ist die erweiterte Matrix $[A\, e_n]$ auf Stufenform zu bringen. Um nun A^{-1} zu berechnen, bringt man die Matrix $[A\,|\,E_n] \in K^{n\times 2n}$ auf die Form $[E_n\,|\,X]$. Dann ist $X = A^{-1}$.

Eine elementare Zeilenoperation erhält man auch durch Linksmultiplikation mit elementaren Matrizen der folgenden Formen:

1. $U_{ij}(s)$ ensteht, wenn man in E_n ein Element u_{xy} $(x \neq y)$ in ein s ändert.
2. P_{ij} ensteht, wenn man in E_n die Zeilen i und j vertauscht.
3. $D_i(s)$ ensteht, wenn man in E_n ein Element d_{ii} durch s ersetzt $(1 \leq i \leq n)$.

Ist $RgA = n$ (d.h. $A \in GL(n,K)$), so gibt es elementare Matrizen $M_1, \ldots, M_r$ mit

$$M_r \cdot \ldots \cdot M_2 \cdot M_1 \cdot A = E_n \Leftrightarrow A^{-1} = M_r \cdot \ldots \cdot M_2 \cdot M_1$$

Folgerung 2 Jede Matrix $A \in GL(n,K)$ ist ein Produkt von elementaren Matrizen.

Es folgt weiterhin: $A^{-1} = M_1^{-1} \cdot \ldots \cdot M_r^{-1}$.

Beachte: Die Inverse einer elementaren Matrix ist eine elementare Matrix:

$$U_{ij}(s)^{-1} = U_{ij}(-s); P_{ij}^{-1} = P_{ij}; D_i(s)^{-1} = D_i(s^{-1}), s \neq 0$$

Kapitel 4

Determinanten

Ziel: Wir wollen eine Abbildung $det : K^{n\times n} \longrightarrow K$ einführen mit

$$det(A\cdot B) = det(A)\cdot det(B), det(E_n) = 1, Rg A < n \Rightarrow det(A) = 0$$

Dabei soll K ein kommutativer Ring sein.

4.1 Permutationen

Definition 1 (Permutation) Ist Ω eine Menge, so heißt eine bijektive Abbildung $\sigma : \Omega \longrightarrow \Omega$ eine *Permutation*.

$$\begin{aligned} Sym(\Omega) &:= \{\sigma : \Omega \longrightarrow \Omega \,|\, \sigma \,\text{bijektiv}\} \\ S_n &:= Sym(\{1,\ldots,n\}) \end{aligned}$$

Ein $\sigma \in S_n$ kann man durch eine Wertetabelle angeben:

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ j_1 & \ldots & j_n \end{pmatrix}, \sigma(i) = j_i$$

Beachte: $j_1,\ldots,j_n$ müssen paarweise verschieden sein.

Bemerkung: $(Sym(\Omega),\circ)$ ist eine Gruppe, $(S_n,\circ)$ ist die *symmetrische Gruppe* auf Ω vom Grade n. Es gilt: $|S_n| = n! = 1\cdot 2\cdot\ldots\cdot n$.

Definition 2 (Zyklus) Ein $\sigma \in S_n$ heißt ein *k-Zyklus*, wenn es $i_1,i_2,\ldots,i_k \in \{1,\ldots,n\}$ paarweise verschieden gibt mit

$$\sigma(i_1) = i_2; \sigma(i_2) = i_3; \sigma(i_3) = i_4; \ldots; \sigma(i_k) = i_1$$

und $\sigma(i) = i$ für $i \notin \{i_1,\ldots,i_k\}$.

Definition 3 (Transposition) Ein 2-Zyklus heißt *Transposition*.

Beispiel:

Sei $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 3 & 4 & 9 & 7 & 2 & 6 \end{pmatrix}$. Es gilt: $\sigma(1) = 8, \sigma(8) = 2, \sigma(2) = 1$; $\sigma(3) = 5, \sigma(5) = 4, \sigma(4) = 3, \sigma(3) = 5$ sowie $\sigma(7) = 7$ und $\sigma(6) = 9, \sigma(9) = 6$. Somit läßt sich σ schreiben als $\sigma = \sigma_1\circ\sigma_2\circ\sigma_3\circ\sigma_4 = \sigma_1\circ\sigma_2\circ\sigma_3$ mit $\sigma_1 = (1,8,2)$, $\sigma_2 = (3,5,4)$, $\sigma_3 = (6,9)$, $\sigma_4 = (7)$.

Bezeichnung: Die Schreibweise $\sigma = (i_1, i_2, ..., i_k)$ bedeutet: $\sigma(i_1) = i_2; \sigma(i_2) = i_3; ...; \sigma(i_k) = i_1$ und $\sigma(i) = i$ für $i \notin \{i_1, ..., i_k\}$.

Definition 4 (Ziffernfremdheit) Zwei Zyklen $(j_1, ..., j_k)$ und $(i_1, ..., i_l)$ heißen *ziffernfremd*, wenn $\{j_1, ..., j_k\} \cap \{i_1, ..., i_l\} = \emptyset$.

Satz 1 Jedes $\sigma \in S_n$...

1. ...ist ein Produkt aus ziffernfremden Zyklen.
2. ...kann man als Produkt von Transpositionen schreiben.
3. ...kann man als Produkt von Transpositionen aus $\{(1,2), (2,3), ..., (n-1, n)\}$ schreiben.

Beweis:

1. Induktion nach der Anzahl k der Nichtfixpunkte von σ.
   (a) $k = 0$: Dann ist $\sigma = id = (1)$ ein 1-Zyklus.
   (b) $k > 0$: Es gibt $j \in \{1, ..., n\}$ mit $\sigma(j) \neq j$. Setze $j_1 := j$, $j_2 := \sigma(j)$, $j_3 = \sigma^2(j) = \sigma(\sigma(j))$ u.s.w., $r = min\left\{i \,\middle|\, \sigma^i(j) \in \{j_1, ..., j_i\}\right\}$. Behauptung: $\sigma^r(j) = j_1$.
   Beweis: sonst wäre $\sigma^r(j) = j_l$ mit $2 \leq l \leq r$. Dann: $\sigma^{r-1}(j) = j_{l-1} \in \{j_1, ..., j_r\}$. Dies ist jedoch ein Widerspruch zur Minimalität von r.
   Setze $\sigma_1 = (j_1, j_2, ..., j_r)$. $\sigma_1^{-1} \circ \sigma$ hat r Fixpunkte mehr als σ. Nach Induktionsannahme ist $\sigma_1^{-1} \circ \sigma = \sigma_2 \circ ... \circ \sigma_m$ mit ziffernfremden Zyklen $\sigma_2, ..., \sigma_m$. Also:
$$\sigma = \sigma_1 \circ ... \circ \sigma_m$$
2. Nach (1) genügt es zu zeigen: jeder k-Zyklus läßt sich als Produkt von Transpositionen schreiben:
$$(j_1, ..., j_k) = (j_1, j_2) \circ (j_2, j_3) \circ ... \circ (j_{k-1}, j_k)$$
3. Nach (2) genügt es zu zeigen ($i < j$):
$$(i, j) = (i, i+1) \circ (i+1, i+2) \circ ... \circ (j-1, j) \circ (j-2, j-1) \circ ... \circ (i, i+1)$$

□

Definition 5 (Signum einer Permutation) Ist $\sigma \in S_n$, so ist $sgn\,\sigma$ definiert als:
$$sgn\,\sigma = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \mathbb{Q}$$

Beispiele:

- $sgn\,id = 1$
- $\sigma = (1, 2)$. Dann:
- Es gilt:

$$\begin{aligned} sgn\,\sigma &= \prod_{j=2}^n \tfrac{\sigma(1)-\sigma(j)}{1-j} \cdot \prod_{j=3}^n \tfrac{\sigma(2)-\sigma(j)}{2-j} \cdot \prod_{3 \leq i < j \leq n} \overbrace{\frac{\sigma(i) - \sigma(j)}{i - j}}^{=1} \\ &= \tfrac{2-1}{1-2} \cdot \overbrace{\prod_{j=3}^n \left(\frac{2-j}{1-j} \frac{1-j}{2-j} \right)}^{=1} = -1 \end{aligned}$$

Satz 2

1. Es gilt: $sgn(\sigma_1 \circ \sigma_2) = sgn\,\sigma_1 \cdot sgn\,\sigma_2$
2. $sgn\,\tau = -1$ falls τ Transposition
3. $sgn\,\sigma = (-1)^{k-1}$ falls σ ein k-Zyklus
4. $sgn\,\sigma \in \{1; -1\}$

Beweis:

1. $sgn(\sigma_1 \circ \sigma_2) = \prod_{1 \le i < j \le n} \frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma(i) - \sigma(j)} \cdot \prod_{1 \le i < j \le n} \frac{\sigma_2(i) - \sigma_2(j)}{i-j}$. Durchläuft $\{i, j\}$ alle 2-elementigen Teilmengen von $\{1, ..., n\}$, so auch $\{\sigma_2(i), \sigma_2(j)\}$. Beachte:
$$\frac{\sigma(i) - \sigma(j)}{i-j} = \frac{\sigma(j) - \sigma(i)}{j-i}, \text{ also } sgn\,\sigma = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i-j} = sgn(\sigma_1 \circ \sigma_2) = sgn\,\sigma_1 \circ sgn\,\sigma_2$$
2. Es sei $\tau = (i, j)$, $i \neq j$. Wähle $\sigma \in S_n$ mit $\sigma(i) = 1$, $\sigma(j) = 2$. Der Zyklus $\sigma^{-1} \circ (1,2) \circ \sigma = (i, j)$ überführt i in j (und umgekehrt) sowie alle anderen Ziffern in sich selbst. Nach (1) gilt, daß
$$sgn(i, j) = sgn\,\sigma^{-1} \cdot sgn(1,2) \cdot sgn\,\sigma = (-1) \cdot sgn(\sigma^{-1} \circ \sigma) = (-1) \cdot sgn\,id = -1$$
3. Ist $\sigma = (j_1, ..., j_k)$ ein k-Zyklus, dann ist $\sigma = (j_1, j_2) \circ ... \circ (j_{k-1}, j_k)$.
Also gilt nach (1): $sgn\,\sigma = sgn(j_1, j_2) \cdot ... \cdot sgn(j_{k-1}, j_k) = (-1)^{k-1}$
4. Folgt aus (1), (2), Satz 1 (Seite 44). $\square$

Definition 6 (gerade Permutation) $\sigma \in S_n$ heißt eine *gerade Permutation*, wenn $sgn\,\sigma = 1$. Die Menge aller geraden Permutationen $A_n = \{\sigma \in S_n \,|\, sgn\,\sigma = 1\}$ heißt *alternierende Gruppe*.

Folgerung 1 A_n ist eine Gruppe. Für $n \ge 2$: $S_n = A_n \cup (\tau \circ A_n)$, τ Transposition.

Beweis: $\sigma_1, \sigma_2 \in A_n \Rightarrow sgn(\sigma_1 \circ \sigma_2) = 1$, also $(\sigma_1 \circ \sigma_2) \in A_n$. $\sigma_1 \circ \sigma_1^{-1} = id \Rightarrow sgn(\sigma_1^{-1}) = 1, \sigma_1^{-1} \in A_n$, $id \in A_n$. Ist $\sigma \in S_n \setminus A_n$, dann $sgn\,\sigma = -1$. τ Transposition, $sgn\,\tau = -1$, also $sgn(\tau \circ \sigma) = (-1)(-1) = 1$. $\square$

Folgerung 2 $|A_n| = \frac{n!}{2}$, weil $|A_n| = |\tau \circ A_n|$

4.2 Determinanten

Geometrische Motivation in $\mathbb{R}^2$ Für $v, w \in \mathbb{R}^2$ sei $\Delta(v, w)$ der orientierte Flächeninhalt des von v, w aufgespannten Parallelogramms. Eigenschaften ($u, v, w \in \mathbb{R}^2$, $s \in \mathbb{R}$):

1. $\Delta(sv, w) = s\Delta(v, w)$ sowie $\Delta(v, sw) = s\Delta(v, w)$
2. $\Delta(u + v, w) = \Delta(u, w) + \Delta(v, w)$ sowie $\Delta(u, v + w) = \Delta(u, v) + \Delta(u, w)$
3. $\Delta(v, v) = 0$ und $\Delta(e_1, e_2) = 1$
4. $\Delta(v, w) = -\Delta(w, v)$ da
$$0 = \Delta(v + w, v + w) = \Delta(v, v) + \Delta(v, w) + \Delta(w, v) + \Delta(w, w) \Leftrightarrow \Delta(v, w) = -\Delta(w, v)$$

Hierdurch ist $\Delta : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}$ eindeutig bestimmt.

$$\begin{aligned}\Delta((a,b)^T,(c,d)^T) &= \Delta(ae_1+be_2, ce_1+de_2)\\ &= \Delta(ae_1,ce_1)+\Delta(ae_1,de_2)+\Delta(be_2,ce_1)+\Delta(be_2,de_2)\\ &= ac\Delta(e_1,e_1)+ad\Delta(e_1,e_2)+bc\Delta(e_2,e_1)+bd\Delta(e_2,e_2)\\ &= ad-bc\end{aligned}$$

Definition 1 (Determinantenform) Sei K ein kommutativer Ring mit Eins, $n \in \mathbb{N}$, $V = K^{n\times 1}$. Eine Abbildung

$$D : V \times ... \times V \longrightarrow K$$

(wobei V n-mal verknüpft wird) heißt *Determinantenform*, wenn

1. $D(v_1,...,sv_i+v_i',...,v_n) = sD(v_1,...,v_i,...,v_n)+D(v_1,...,v_i',...,v_n)$ ($i = 1,...,n$, $v_i, v_i' \in V$), d.h. D soll als Funktion des i-ten Arguments linear sein
2. $D(v_1,...,v_n) = 0$ falls es ein $i \neq j$ gibt mit $v_i = v_j$
3. $D(e_1,...,e_n) = 1$ wobei $e_i = (0,...,0,1,0,...,0)^T \in V$ mit der Eins in der i-ten Zeile.

$D : V \times ... \times V \longrightarrow K$ mit (1) und (2) heißt auch “alternierende Multilinearform”.

Lemma 1 Ist $D : V \times ... \times V \longrightarrow K$ (V n-mal verknüpft) eine Determinantenform, so gilt:

1. $D(v_1,...,v_i,...,v_j,...,v_n) = -D(v_1,...,v_j,...,v_i,...,v_n)$
2. $D(v_{\sigma(1)},...,v_{\sigma(n)}) = \varepsilon(\sigma)\cdot D(v_1,...,v_n)$ für $\sigma \in S_n$ und $\varepsilon(\sigma) = \begin{cases} 1 \in K & falls \quad sgn\,\sigma = 1 \in \mathbb{Q} \\ -1 \in K & falls \quad sgn\,\sigma = -1 \in \mathbb{Q}\end{cases}$
3. $D(v_1,...,v_i+\sum_{j\neq i} s_j v_j,...,v_n) = D(v_1,...,v_i,...,v_n)$

Beweis:

1. Es gilt:

$$\begin{aligned} 0 &= D(v_1,.,v_i+v_j,.,v_i+v_j,.,v_n)\\ &= D(v_1,.,v_i,.,v_i,.,v_n)+D(v_1,.,v_i,.,v_j,.,v_n)\\ &\quad +D(v_1,.,v_j,.,v_i,.,v_n)+D(v_1,.,v_j,.,v_j,.,v_n)\\ \text{also} \quad & 0 = D(v_1,...,v_i,...,v_j,...,v_n)+D(v_1,...,v_j,...,v_i,...,v_n)\\ \Leftrightarrow \quad & D(v_1,...,v_i,...,v_j,...,v_n) = -D(v_1,...,v_j,...,v_i,...,v_n)\end{aligned}$$

2. In (1) gezeigt: Ist $\tau = (i,j)$ Transposition, so ist $D(v_{\tau(1)},...,v_{\tau(n)}) = -D(v_1,...,v_n)$.
   Ist $\sigma \in S_n$, so kann man nach Satz 1, Seite 44, schreiben: $\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_m$.
   Induktion nach m:
   (a) $m = 1$: siehe Teil (1)
   (b) $m > 1$: $\tau_2 = ... = \tau_m = \sigma'$. Dann: $D(v_{\sigma(1)},...,v_{\sigma(n)}) = D(v_{\tau_1(\sigma'(1))},...,v_{\tau_n(\sigma'(n))})$
   Nach (1) gilt: $... = -D(v_{\sigma'(1)},...,v_{\sigma'(n)})$, nach Induktionsannahme: $... = -\varepsilon(\sigma')\cdot D(v_1,...,v_n)$.
   Weiterhin: $sgn\,\sigma = sgn\,\tau_1 \cdot sgn\,\sigma' = -sgn\,\sigma'$, $\varepsilon(\sigma) = -\varepsilon(\sigma')$, also insgesamt:
   $$D(v_{\tau(1)},...,v_{\tau(n)}) = ... = \varepsilon(\sigma)\cdot D(v_1,...,v_n)$$
   (c) $D(v_1,...,v_i+\sum_{j\neq i} s_j v_j,...,v_n) = D(v_1,...,v_i,...,v_n)+\sum_{j\neq i} s_j D(v_1,...,v_j,...,v_j,...,v_n)$
   Die Summe $\sum_{j\neq i}...$ ist aber Null, da in D zwei Argumente gleich v_j sind. □

Satz 1 (Existenz und Eindeutigkeit der Determinanten) Es sei K ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Dann gibt es genau eine Determinantenform

$$D : K^{n\times 1} \times \ldots \times K^{n\times 1} \longrightarrow K$$

und es gilt für $v_j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{bmatrix} \in K^{n\times 1}$, $j = 1, \ldots, n$: $D(v_1, \ldots, v_n) = \sum_{\sigma\in S_n} \varepsilon(\sigma) \cdot a_{\sigma(1)1} \cdot \ldots \cdot a_{\sigma(n)n}$ wobei $\varepsilon(\sigma) = \begin{cases} 1 \in K & \text{falls} \quad sgn\,\sigma = 1 \in \mathbb{Q} \\ -1 \in K & \text{falls} \quad sgn\,\sigma = -1 \in \mathbb{Q} \end{cases}$

Beweis:

1. Eindeutigkeit:
   Sei $v_j = \sum\limits_{i=1}^{n} a_{ij} e_i$, $j = 1, \ldots, n$. Voraussetzung: D ist Determinantenform. Dann gilt:

$$\begin{aligned} D(v_1, \ldots, v_n) &= D(\sum_{i=1}^{n} a_{i1} e_i, v_2, \ldots, v_n) = \sum_{i_1=1}^{n} a_{i_1 1} \cdot D(e_{i_1}, v_2, v_3, \ldots, v_n) \\ &= \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} a_{i_1 1} \cdot a_{i_2 2} \cdot D(e_{i_1}, e_{i_2}, v_3, \ldots, v_n) \\ &= \sum_{i_1=1}^{n} \ldots \sum_{i_n=1}^{n} [a_{i_1 1} \cdot \ldots \cdot a_{i_n n} \cdot D(e_{i_1}, \ldots, e_{i_n})] \end{aligned}$$

   $D(e_{i_1}, \ldots, e_{i_n})$ ist jedoch Null, falls $\{i_1, \ldots, i_n\} \neq \{1, \ldots, n\}$. Ist dagegen $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$, so ist $\sigma = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix} \in S_n$ und es gilt:

$$D(e_{i_1}, \ldots, e_{i_n}) = D(e_{\sigma(1)}, \ldots, e_{\sigma(n)}) = \varepsilon(\sigma) \cdot D(e_1, \ldots, e_n) = \varepsilon(\sigma)$$

2. Existenz:
   Wir definieren $D : K^{n\times 1} \times \ldots \times K^{n\times 1} \longrightarrow K$ durch

$$D(v_1, \ldots, v_n) = \sum_{\sigma\in S_n} \varepsilon(\sigma) \cdot a_{\sigma(1)1} \cdot \ldots \cdot a_{\sigma(n)n}$$

   Zu zeigen: Dann gilt (1),(2),(3) (Definition 1, Seite 46).

   (a) $D(v_1, \ldots, sv_i + v'_i, \ldots, v_n) = \sum\limits_{\sigma\in S_n} [\varepsilon(\sigma) \cdot a_{\sigma(1)1} \cdot \ldots \cdot (sa_{\sigma(i)i} + a'_{\sigma(i)i}) \cdot \ldots \cdot a_{\sigma(n)n}]$
   $= sD(v_1, \ldots, v_i, \ldots, v_n) + D(v_1, \ldots, v'_i, \ldots, v_n)$

   (b) Sei $v_i = v_j$ für $i \neq j$. Da $S_n = A_n \cup (A_n \circ \tau)$ gilt:

$$\begin{aligned} & D(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) \\ = & \sum_{\rho\in A_n} a_{\rho(1)1} \cdot \ldots \cdot a_{\rho(n)n} \\ & + \sum_{\rho\in A_n} (-1) \cdot a_{\rho(\tau(1))1} \cdot \ldots \cdot a_{\rho(\tau(i))i} \cdot \ldots \cdot a_{\rho(\tau(j))j} \cdot \ldots \cdot a_{\rho(\tau(n))n} \\ = & \sum_{\rho\in A_n} a_{\rho(1)1} \cdot \ldots \cdot a_{\rho(n)n} - \sum_{\rho\in A_n} a_{\rho(\tau(1))1} \cdot \ldots \cdot a_{\rho(\tau(n))n} \\ = & \ 0 \end{aligned}$$

   (c) $D(e_1, \ldots, e_n) = 1$ □

Folgerung 1 Aus (1) und (2) folgt:

1. $D(v_{\sigma(1)},...,v_{\sigma(n)}) = \varepsilon(\sigma)\cdot D(v_1,...,v_n)$ mit $\sigma \in S_n$
2. $D(v_1,...,v_i + \sum_{i\neq j} s_i v_j,...,v_n) = D(v_1,...,v_n)$

Definition 2 (transponierte Matrix) Ist $A \in K^{m\times n}$, so sei $A^T \in K^{n\times m}$ definiert durch $(A^T)_{ij} := (A)_{ji}$. A^T heißt die zu A *transponierte Matrix*.

Beispiel:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}, A^T = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$$

Satz 2 Es gilt für $A \in K^{n\times n}$: $det\,A^T = det\,A$.

Beweis: $A = [a_{ij}] \in K^{n\times n}$. Dann:

$$det\,A^T = \sum_{\sigma\in S_n} \varepsilon(\sigma)\cdot a_{1\sigma(1)}\cdot ...\cdot a_{n\sigma(n)} = \sum_{\sigma^{-1}\in S_n} \varepsilon(\sigma^{-1})\cdot a_{\sigma^{-1}(1)1}\cdot ...\cdot a_{\sigma^{-1}(n)n} = det\,A$$

□

Satz 3 (Cramersche Regel) Ist $A = [a_{ij}] \in K^{n\times n}$ und $det\,A$ in K invertierbar, so hat das Gleichungssystem $Ax = b$ für $b \in K^{n\times 1}$ genau eine Lösung $(x_1,...,x_n)^T$ und es gilt:

$$x_i = \frac{det\,[a_1,...,a_{i-1},b,a_{i+1},...,a_n]}{det\,A}$$

Folgerung 2 $A \in \mathbb{Z}^{n\times n}$, $det\,A = \pm 1$. Dann hat $ax = b$ eine eindeutige ganzzahlige Lösung.

Korollar zu Satz 1 Ist $\Phi : K^{n\times 1}\times ...\times K^{n\times 1} \longrightarrow K$ "alternierende Multilinearform", d.h. es gelten (1) und (2) aus der Definition 1, Seite 46. Dann ist

$$\Phi = c\cdot D$$

mit $c = \Phi(e_1,...,e_n)$.

Beweis:

$$\begin{array}{lll} & \Phi(v_1,...,v_n) & \text{Anwendung Satz 1} \\ = & \sum\limits_{i_1=1}^{n} ... \sum\limits_{i_n=1}^{n} a_{i_1 1}\cdot ...\cdot a_{i_n n}\cdot \Phi(e_{i_1},...,e_{i_n}) & \Phi(e_{i_j}) = 0 \text{ falls } \sigma = \begin{pmatrix} 1 & ... & n \\ i_1 & ... & i_n \end{pmatrix} \notin S_n \\ = & \sum\limits_{\sigma\in S_n} a_{i_1}\cdot ...\cdot a_{i_n}\cdot \Phi(e_{\sigma(i_1)}\cdot ...\cdot e_{\sigma(i_n)})\cdot \varepsilon(\sigma) & \\ = & \Phi(e_1,...,e_n)\cdot \sum\limits_{\sigma\in S_n} \varepsilon(\sigma)\cdot a_{i_1}\cdot ...\cdot a_{i_n} & \\ = & \Phi(e_1,...,e_n)\cdot D(v_1,...,v_n) & \end{array}$$

□

4.3 Eigenschaften der Determinante

Satz 1 Sind $A, B \in K^{n\times n}$, so gilt
$$det\,(A\cdot B) = det\,A\cdot det\,B$$

Beweis: $\Phi : K^{n\times 1}\times \ldots \times K^{n\times 1} \longrightarrow K$ (n-mal $\times$) sei definiert durch $\Phi(v_1,\ldots,v_n) := D(Av_1,\ldots,Av_n) = det(AB)$ falls $v_1,\ldots,v_n$ Spalten von B sind und $Ae_1,\ldots,Ae_n$ Spalten von A.

Φ ist alternierende Multilinearform (d.h. es gelten (1) und (2) aus Definition 1, Seite 46), denn:

- (1) gilt:

$$\begin{aligned}
\Phi(v_1,\ldots,sv_i+v_i^{'},\ldots,v_n) &= D(Av_1,\ldots,A(sv_i+v_i^{'}),\ldots,Av_n)\\
&= sD(Av_1,\ldots,Av_i,\ldots,Av_n)+D(Av_1,\ldots,Av_i^{'},\ldots,Av_n)\\
&= s\Phi(v_1,\ldots,v_i,\ldots,v_n)+\Phi(v_1,\ldots,v_i^{'},\ldots,v_n)
\end{aligned}$$

- (2) gilt: $v_i = v_j$ für $i \neq j$, dann ist $Av_i = Av_j$, also $\Phi(v_1,\ldots,v_n) = D(Av_1,\ldots,Av_n) = 0$

Nach Korollar zu Satz 1 (Seite 48) ist $\Phi = c\cdot D$ mit $c = \Phi(e_1,\ldots,e_n) = D(Ae_1,\ldots,Ae_n) = det\,A$. Sind $v_1,\ldots,v_n$ Spaltenvektoren von B, so ist also:

$$\Phi(v_1,\ldots,v_n) = det(AB) = det\,A\cdot D(v_1,\ldots,v_n) = det\,A\cdot det\,B$$

□

Folgerung 1 Ist $A\in K^{n\times n}$ invertierbar (d.h. gibt es $A^{-1}\in K^{n\times n}$ mit $A\cdot A^{-1} = A^{-1}\cdot A = E_n$) so ist $det\,A$ in K invertierbar und es gilt:
$$det\,A^{-1} = (det\,A)^{-1}\in K$$

Beweis: Aus Satz 1 folgt: $1 = det\,E_n = det\,(A\cdot A^{-1}) = det\,A\cdot det\,A^{-1}$. □

Beispiele:

- Genau dann ist $A\in\mathbb{Z}^{n\times n}$ invertierbar in $\mathbb{Z}^{n\times n}$, wenn gilt: $det\,A\in\{1;-1\}$
- K Körper, $A\in K^{n\times n}$. Genau dann ist A invertierbar, wenn gilt: $det\,A\neq 0$.

Satz 2 Ist V ein K-Vektorraum, $B = (v_1,\ldots,v_n)$ Basisfolge und $\varphi\in End\,V$. Dann ist $det\,\varphi := det\,({}_B\varphi_B)$ unabhängig von der Wahl der Basisfolge B.

Beweis: Ist $B' = (w_1,\ldots,w_n)$ auch Basisfolge von V. Dann gilt:

$$\begin{aligned}
{}_{B'}\varphi_{B'} &= {}_{B'}id_B\cdot{}_B\varphi_B\cdot{}_Bid_{B'}\\
\Rightarrow det\,{}_{B'}\varphi_{B'} &= det\,{}_{B'}id_B\cdot det\,{}_B\varphi_B\cdot det\,{}_Bid_{B'}\\
&= (det\,{}_Bid_{B'})^{-1}\cdot det\,{}_B\varphi_B\cdot det\,{}_Bid_B\\
&= det\,{}_B\varphi_B
\end{aligned}$$

□

Satz 3 Seien $A \in K^{m\times m}$, $B \in K^{p\times p}$ und $C \in K^{m\times p}$. Dann gilt:

$$det \begin{bmatrix} A & C \\ 0 & B \end{bmatrix} = det\,A \cdot det\,B$$

Beweis: Es gilt $X = X_1 \cdot X_2$ mit $X := \begin{bmatrix} A & C \\ 0 & B \end{bmatrix}$, $X_1 := \begin{bmatrix} E_m & 0 \\ 0 & B \end{bmatrix}$ und $X_2 := \begin{bmatrix} A & C \\ 0 & E_p \end{bmatrix}$. Nach Satz 1 gilt dann $det\,X = det\,X_1 \cdot det\,X_2$. Zu zeigen:

1. $det\,X_1 = det\,B$ offensichtlich.
2. $det\,X_2 = det\,A$. Sei $\Phi : K^{m\times 1} \times ... \times K^{m\times 1} \longrightarrow K$ (m-mal $\times$) definiert durch

$$\Phi(v_1,...,v_m) = det \begin{bmatrix} v_1...v_m & C \\ 0 & E_p \end{bmatrix}$$

dann ist Φ alt. Multilinearform. Nach Korollar zu Satz 1, Seite 48, ist $\Phi = c \cdot D$ mit

$$c = \Phi(e_1,...,e_n) = det \begin{bmatrix} 1 & \dots & 0 & & & \\ \vdots & \ddots & \vdots & & C & \\ 0 & \dots & 1 & & & \\ 0 & \dots & 0 & 1 & \dots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 1 \end{bmatrix} = det\,E_{m+p} = 1$$

nach Lemma 1, Seite 46. Sind $v_1,...,v_n$ Spaltenvektoren von A, dann gilt:

$$\Phi(v_1,...,v_n) = det \begin{bmatrix} A & C \\ 0 & E_p \end{bmatrix} = D(v_1,...,v_n) = det\,A$$

□

Definition 1 (Kronecker-Symbol) Das *Kroneckersymbol* δ_{ij} ist definiert als:

$$\delta_{ij} := \begin{cases} 1 & \text{fuer} \quad i = j \\ 0 & \text{fuer} \quad i \neq j \end{cases}$$

Satz 4 (Laplace'scher Entwicklungssatz) Ist $A = [a_{ij}] \in K^{n\times n}$, so sei $A_{ij} \in K^{(n-1)\times(n-1)}$ die Matrix, die man aus A durch Weglassen der i-ten Zeile und j-ten Spalte erhält. Dann gilt:

$$\sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ik} \cdot A_{ij} = \begin{cases} det\,A & \text{fuer} \quad j = k \\ 0 & \text{fuer} \quad j \neq k \end{cases} = \delta_{jk} \cdot det\,A \text{ für } 1 \leq j,k \leq n$$

Beweis: $v_1,...,v_n$ seien die Spalten von A. Dann gilt:

$\delta_{jk} \cdot det\,A$

$= D(v_1,...,v_{j-1},v_k,v_{j+1},...,v_n)$ nach L1 (2), Seite 4.2.

$= (-1)^{j-1} D(v_k,v_1,...,v_{j-1},v_{j+1},...,v_n)$ $v_k = \sum_{i=1}^{n} a_{ik} e_i$

$= \sum_{i=1}^{n} (-1)^{j-1} \cdot a_{ik} \cdot D(e_i,v_1,...,v_{j-1},v_{j+1},...,v_n)$

$$= \sum_{i=1}^{n} (-1)^{j-1} \cdot a_{ik} \cdot det \begin{bmatrix} 0 & a_{11} & \dots & a_{1\,j-1} & a_{1\,j+1} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & a_{i1} & \dots & a_{i\,j-1} & a_{i\,j-1} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{n1} & \dots & a_{n\,j-1} & a_{n\,j+1} & \dots & a_{nn} \end{bmatrix}$$

$$= \sum_{i=1}^{n} (-1)^{j-1} \cdot (-1)^{i-1} \cdot a_{ik} \cdot det \begin{bmatrix} 1 & a_{i1} & \dots & a_{i\,j-1} & a_{i\,j+1} & \dots & a_{in} \\ 0 & & & & & & \\ \vdots & & & A_{ij} & & & \\ 0 & & & & & & \end{bmatrix}$$

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

Bemerkung: Der Laplace'sche Entwicklungssatz läßt sich nur gut einsetzen, wenn die Matrix viele Nullen hat.

Definition 2 (Adjunkte) Ist $A = [a_{ij}] \in K^{n \times n}$, so sei die *Adjunkte* zu A

$$adj A := \left[(-1)^{i+j} \cdot det A_{ji}\right]_{\substack{i=1..n \\ j=1..n}}$$

die zu A komplementäre Matrix.

Korollar 1 $adj A \cdot A = det A \cdot E_n$

Folgerung 2 $A \in K^{n \times n}$ ist in $K^{n \times n}$ invertierbar genau dann, wenn $det A$ in K invertierbar ist und dann ist:

$$A^{-1} = \frac{1}{det A} \cdot adj A$$

Folgerung 3 Sei K Körper, dann ist für $A \in K^{n \times n}$ äquivalent:

1. $Rg A = n$ (d.h. $A \in GL(n,K)$)
2. A ist in $K^{n \times n}$ invertierbar
3. $det A \neq 0$

Beweis: (1)⇔(2) folgt aus Satz 2, 41; (2)⇒(3) folgt aus Satz 1; (2)⇐(3) folgt aus Korollar 1. □

Definition 3 (invertierbar) Ist $det A \neq 0$, $A \in K^{n \times n}$, so heißt A *invertierbar* (oder "*regulär*", "*nicht singulär*").

Beispiel:

- Sei $A_n = \begin{bmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & \ddots & \vdots \\ 0 & -1 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 2 & -1 \\ 0 & \dots & 0 & -1 & 2 \end{bmatrix} = [a_{ij}]$, also $a_{ij} = \begin{cases} 0 & \text{fuer} & |i-j| > 1 \\ -1 & \text{fuer} & |i-j| = 1 \\ 2 & \text{fuer} & i = j \end{cases}$. Entwicklung nach erster Spalte, Anwendung von Satz 4 für $j = k = 1$:

$$\begin{aligned} det A_n &= a_{11} \cdot det\,(A_n)_{11} - a_{21} \cdot det\,(A_n)_{21} + 0 \\ &= 2 \cdot det \begin{bmatrix} 2 & -1 & 0 & \dots \\ -1 & 2 & \ddots & \ddots \\ 0 & \ddots & \ddots & -1 \\ \vdots & \ddots & -1 & 2 \end{bmatrix} + 1 \cdot det \begin{bmatrix} -1 & 0 & 0 & \dots \\ -1 & 2 & -1 & \ddots \\ 0 & \ddots & \ddots & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{bmatrix} \\ &= 2 \cdot det A_{n-1} + ((-1) \cdot (det A_{n-2})) \\ &= 2 \cdot det A_{n-1} - det A_{n-2} \end{aligned}$$

- van-der-Monde-Determinante: Sei $A \in K^{(n+1)\times(n+1)}$ eine van-der-Monde-Matrix (vgl. S. 35), $x_i \in K$.
  Berechnen der Determinante:
  Sei v_j die j-te Spalte von A. Dann gilt (Entwicklung nach erster Zeile):

$$
\begin{aligned}
det A &= det \begin{bmatrix} 1 & x_0 & \dots & x_0^n \\ : & x_1 & \dots & x_1^n \\ : & : & & : \\ 1 & x_n & \dots & x_n^n \end{bmatrix} (i\,\text{te Spalte}) - (1.\,\text{Spalte} \cdot x_\star^{i-1})\ i > 1 \\
&= det \begin{bmatrix} 1 & x_0 - x_0 & \dots & x_0^n - x_0 x_0^{n-1} \\ : & x_1 - x_0 & \dots & x_1^n - x_0 x_1^{n-1} \\ : & : & & : \\ 1 & x_n - x_0 & \dots & x_n^n - x_0 x_n^{n-1} \end{bmatrix} \\
&= det \begin{bmatrix} 1 & 0 & \dots & 0 \\ : & x_1 - x_0 & \dots & (x_1 - x_0) x_1^{n-1} \\ : & : & & : \\ 1 & x_n - x_0 & \dots & (x_1 - x_0) x_n^{n-1} \end{bmatrix} \text{Entwicklung nach 1. Zeile} \\
&= 1 \cdot det \begin{bmatrix} (x_1 - x_0) & \dots & (x_n - x_0) x_1^{n-1} \\ : & & : \\ (x_n - x_0) & \dots & (x_n - x_0) x_n^{n-1} \end{bmatrix} \\
&= (x_1 - x_0) \cdot \ldots \cdot (x_n - x_0) \cdot det \begin{bmatrix} 1 & \dots & x_1^{n-1} \\ : & & : \\ 1 & \dots & x_n^{n-1} \end{bmatrix} \text{vdM} - \text{Matrix} \\
&= \dots \\
&= \prod_{j>i} (x_j - x_i)
\end{aligned}
$$

  Insbesondere folgt hieraus: $det A = 0 \Leftrightarrow \exists i \neq j \,\text{mit}\, x_i = x_j$.

4.4 Polynomringe

Sei K ein Körper oder kommutativer Ring mit Eins.

Definition 4 (Polynomring) Eine K-Algebra R heißt *Polynomring* über K in der Unbestimmten X, i.Z. $R = K[X]$, wenn jedes $f \in R$ mit $f \neq \underline{0}$ eine eindeutige Darstellung

$$f = a_0 1 + a_1 X + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i$$

existiert mit $a_i \in K$, $a_n \neq 0$; $1 = X^0$ ist Einselement von R. In diesem Fall heißt n der *Grad* von f (*Grad* f).

Bemerkung: $K[X]$ hat immer ∞ viele Elemente. Ist K ein Körper, so ist $\left\{X^i \,|\, i \in \mathbb{N}_0\right\}$ eine K-Basis von $K[X]$, also $dim K[X] = \infty$.

Bemerkung: Polynome sind von Polynomfunktionen zu unterscheiden!

$$\mathbb{P}(K) = \left\{ f : K \longrightarrow K \,\middle|\, \exists n \in \mathbb{N}, a_0, \ldots, a_n \in K : \ f(x) = \sum_{i=0}^{n} a_i x^i \,\forall x \in K \right\}$$

Ist $f \in \mathbb{P}(K)$, so heißt f “Polynomfunktion”. Ist bspw. K ein endlicher Körper, $|K| = q$, so ist $|Abb(K,K)| = q^q$, also $|P(K)| = q^q < \infty$, denn $dim \mathbb{P}(K) = q$.

Satz 1 Ist A eine beliebige K-Algebra, $\alpha \in A$ und ist $K[X]$ Polynomring über K in der Unbestimmten X, so gibt es genau einen K-Algebra-Homomorphismus

$$\varphi_\alpha : \begin{array}{ccc} K[X] & \longrightarrow & A \\ \varphi_\alpha[X] & \longmapsto & \alpha \end{array}$$

φ heißt "Einsetzungshomomorphismus" zu α und man schreibt für $f \in K[X]$: $f(\alpha) := \varphi_\alpha(f)$

Beweis:

1. Eindeutigkeit: Sei $\varphi : K[X] \longrightarrow A$ ein K-Algebra-Hom. Dann (falls $\varphi(X) = \alpha$):

$$\varphi\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} a_i \varphi(X^i) = \sum_{i=0}^{n} a_i \varphi(X)^i = \sum_{i=0}^{n} a_i \alpha^i$$

2. Existenz: Wir definieren $\varphi_\alpha : K[X] \longrightarrow A$ so ($a_i \in K$, $a_n \neq 0$):

$$\varphi_\alpha\left(\sum_{i=0}^{n} a_i X^i\right) := \sum_{i=0}^{n} a_i \alpha^i \text{ sowie } \varphi(\underline{0}) := 0$$

Dann ist φ_α wohldefiniert, weil jedes $f \neq \underline{0}$ eindeutig als $\sum_{i=0}^{n} a_i X^i$ ($a_n \neq 0$) darstellbar. Ein K-Algebra-Homomorphismus ist eine K-lineare Abbildung φ mit $\varphi(fg) = \varphi(f) \cdot \varphi(g)$ und $\varphi(\underline{1}) = 1$:

(a) Linearität:

$$\begin{aligned} & \varphi_\alpha\left(\sum_{i=0}^{n} a_i X^i + c \cdot \sum_{j=0}^{m} b_j X^j\right) && \begin{array}{l} a_i = 0 \,\text{fuer}\, i > n \\ b_i = 0 \,\text{fuer}\, i > m \end{array} \\ = \; & \varphi_\alpha\left(\sum_{i=0}^{max(n,m)} (a_i + c b_i) X^i\right) \\ = \; & \sum_{i=0}^{max(n,m)} (a_i + c b_i)\alpha^i \\ = \; & \sum_{i=0}^{max(n,m)} a_i \alpha^i + c \cdot \sum_{i=0}^{max(n,m)} b_i \alpha^i \\ = \; & \varphi_\alpha\left(\sum_{i=0}^{max(n,m)} a_i X^i\right) + c \cdot \varphi\left(\sum_{i=0}^{max(n,m)} b_i X^i\right) \end{aligned}$$

(b) $\varphi(fg) = \varphi(f) \cdot \varphi(g)$:

$$\begin{aligned} & \varphi_\alpha\left(\sum_{i=0}^{n} a_i X^i \cdot \sum_{j=0}^{m} b_j X^j\right) \\ = \; & \varphi_\alpha\left(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i \cdot b_j \cdot X^{i+j}\right) = \varphi_\alpha\left(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i \cdot b_j \cdot X^{k}\right), k := i+j \\ = \; & \varphi_\alpha\left(\sum_{k=0}^{m+n}\left(\sum_{i,j;\, i+j=k} a_i \cdot b_j\right) \cdot X^k\right) = \varphi_\alpha\left(\sum_{k=0}^{m+n}\left(\sum_{i=0}^{k} a_i \cdot b_{k-i}\right) \cdot X^k\right) \\ = \; & \sum_{k=0}^{m+n}\left(\sum_{i=0}^{k} a_i \cdot b_{k-i}\right) \cdot \alpha^k = \sum_{i=0}^{n} a_i \alpha^i \cdot \sum_{j=1}^{m} b_j \alpha^j \end{aligned}$$

(c) $\varphi(\underline{1}) = 1$: $\varphi_\alpha(\underline{1}) = \varphi_\alpha(X^0) = \alpha^0 = 1$ □

Folgerung 1 Sind $K[X]$ und $K[Y]$ Polynomringe über K, so existiert genau ein K-Algebra-Isomorphismus $\varphi : K[X] \longrightarrow K[Y]$ mit $\varphi[X] = Y$ (Begründung: φ_Y wie in Satz 1 mit $A = K[Y]$ ist Isomorphismus).

Satz 2 Zu jedem kommutativen Ring mit Eins K gibt es einen Polynomring in einer Unbestimmten X.

Beweis: Sei $R = K^{(\mathbb{N}_0)} = \left\{ (a_i)_{i=0}^{\infty} | a_i \neq 0 \text{ nur fuer endlich viele } i \in \mathbb{N}_0, a_i \in K \right\}$ eine K-Algebra mit K-Basis $(e_i)_{i=0}^{\infty}$ mit $e_i = (\delta_{ij})_{j=0}^{\infty} = (0, \ldots, 1, \ldots, 0)$ (1 in der i-ten Spalte). Setze $X := e_1$.

1. Addition, Multiplikation mit Skalaren (wie in Vektoraxiomen, Seite 14):
$$(a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty} = (a_i + b_i)_{i=0}^{\infty} \text{ sowie } c \cdot (a_i)_{i=0}^{\infty} = (c \cdot a_i)_{i=0}^{\infty}$$
2. Multiplikation in R wird so definiert:
$$(a_i)_{i=0}^{\infty} \cdot (b_j)_{j=0}^{\infty} = (c_k)_{k=0}^{\infty} \text{ mit } c_k = \sum_{i=0}^{k} a_i \cdot b_{k-i} \in R$$

Damit wird R Ring, also K-Algebra. Einselement ist $e_0 = (\delta_{j0})_{j=0}^{\infty}$, denn $e_0 \cdot (b_j)_{j=0}^{\infty} = (c_k)_{k=0}^{\infty}$ mit $c_k = \sum_{i=0}^{k} \delta_{i0} \cdot b_{k-i} = b_k$. Es gilt: $e_1 \cdot e_1 = e_2 = X^2$, allgemein: $e_n = X^n$; $\left\{ X^i | 0 \leq i \in \mathbb{N}_0 \right\}$ ist K-Basis von R. $\square$

Beispiel:

$f = (X-1)(X-2) = X^2 - 3X + 2 \in \mathbb{Q}[X]$, $\varphi_\alpha : K[X] \longrightarrow K^{2\times 2}, f \longmapsto f(\alpha)$, $\mathbb{Q}^{2\times 2}$ ist $\mathbb{Q}$-Algebra.
$A = \begin{bmatrix} 3 & -1 \\ 2 & 0 \end{bmatrix} \in \mathbb{Q}^{2\times 2}$, $f(A) = (A - E_2)(A - 2E_2) = A^2 - 3A + 2E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.
Beachte: Aus $(X-1)$ wird (weil über 2×2-Matrizen) $(X - E_2)$!

4.5 Polynome über Körpern, Nullstellen

K sei ein Körper.

Lemma 1 $f, g \in K[X] \setminus \{\underline{0}\}$. Es gilt: $Grad\,(fg) = Grad\, f + Grad\, g$. Insbesondere folgt:
$$f \neq \underline{0} \wedge g \neq \underline{0} \Rightarrow fg \neq \underline{0}$$

Beweis: $Grad\, f = n$, $Grad\, g = m$. $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{j=0}^{m} b_j X^j$. Dann:
$$f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

Insbesondere gilt mit $c_k := \left(\sum_{i=0}^{k} a_i b_{k-i} \right)$: $c_{n+m} = a_n b_m \neq 0$, da $a_n \neq 0$ und $b_m \neq 0$. $\square$

Satz 1 (Polynomdivision) Sei $f \in K[X]$, $f \neq \underline{0}$, dann gibt es zu jedem $g \in K[X]$ Polynome $q, r \in K[X]$ mit $g = q \cdot f + r$ mit $Grad\, r < Grad\, f$ oder $r = 0$.

Beweis: Sei $Grad\, f = n$, $Grad\, g = m$. Ist $m < n$, so setze $q = 0$, $r = g = \underline{0} \cdot f + g$. O.B.d.A. sei $g \neq \underline{0}$ (denn sonst $g = \underline{0} \cdot f + \underline{0}$ und $m \geq n$), $g = \sum_{i=1}^{m} b_i X^i$ ($b_m \neq 0$) und $f = \sum_{i=0}^{n} a_i X^i$ ($a_n \neq 0$). Induktion nach m:

- $m = 0$: $g = b_0 X^0 = b_0$, $f = a_0 X^0 = a_0$. Setze $q = \frac{b_0}{a_0} X^0 = \frac{b_0}{a_0}$ und $r = \underline{0}$.
- $m > 0$: $g_1 = g - \frac{b_m}{a_n} X^{m-n} f$. Dann ist $Grad\, g_1 < m$.
  nach Induktionsannahme gibt es $q_1, r \in K[X]$ mit
  $$g_1 = fq + r \,\text{mit}\, Grad\, r < Grad\, f \,\text{oder}\, r = 0$$
  daraus folgt
  $$g = f_q + r + \frac{b_m}{a_n} X^{m-n} f = (q_1 + \frac{b_m}{a_n} X^{m-n}) f + r$$
  Setze also $q = q_1 + \frac{b_m}{a_n} X^{m-n} \Rightarrow$ Satz 1. $\square$

Beispiel:

$f = X^2 - 3X + 2$, $g = X^5 - 3X^4 + 2X^3 + X^2 - 1$,
$g = X^5 - 3X^4 + 2X^3 + X^2 - 1 = (X^2 - 3X + 2) \cdot (X^3 + 1) + (3X - 3) = f \cdot (X^3 + 1) + (3X - 3)$

Definition 1 (Nullstelle) Ist $f \in K[X]$ und $c \in K$, so heißt c *Nullstelle* von f, wenn $f(c) = 0$.

Lemma 2 $c \in K$ ist Nullstelle von $f \in K[X]$ genau dann, wenn $f = (X - c) \cdot q$ mit $q \in K[X]$.

Beweis: Nach Satz 1 gibt es $q \in K[X]$ und $r \in K[X]$ mit

$$f = (X - c)q + r \text{ wobei } Grad\, r < 1 \text{ oder } r = \underline{0}$$

Setze $r = aX^0 = a \cdot 1$. Wende Einsetzungshomomorphismus φ_c an:

$$\varphi_c(f) = f(c) = (c - c) \cdot q(c) + a = a \;\text{ also, da } c - c = 0: \quad f(c) = 0 \Leftrightarrow a = 0 \Leftrightarrow r = 0$$

□

Definition 2 (Vielfachheit) $c \in K$ heißt Nullstelle von $f \in K[X]$ mit *Vielfachheit* k, wenn

$$f = (X - c)^k \cdot q \text{ mit } q(c) \neq 0$$

Bemerkung: In dieser Definition ist k (und auch q) eindeutig durch f und c bestimmt.

Angenommen $|K| = \infty$ und $f \in Kern\,\varphi$ also $f = \sum_{i=0}^{n} a_i X^i$ und $\varphi(f) = 0$ Nullfunktion. Das bedeutet: $f = \sum_{i=0}^{n} a_i X^i = 0$ für jedes $X \in K$. Demnach hat f ∞ viele Nullstellen. Nach Folgerung 1 muß dann $f = \underline{0}$ sein. Somit ist $Kern\,\varphi = \{\underline{0}\}$, φ ist bijektiv also ein Isomorphismus.

Bemerkung: Ist $|K| = q$ so ist $dim\,K[X] = \infty$ aber $dim\,\mathbb{P}(K) = q$. In Polynome $f \in K[X]$ darf man Elemente einer beliebigen K-Algebra einsetzen, in eine Polynomfunktion $f \in \mathbb{P}(K)$ darf man nur Elemente aus K einsetzen.

Beispiel:

$K = \mathbb{F}_2 = \{0; 1\}$.
In K gilt $x^2 = x$ für alle $x \in K$ also $p_1 : K \longrightarrow K, x \longmapsto x$ und $p_2 : K \longrightarrow K, x \longmapsto x^2$ sind gleich.
Für $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in K^{2\times 2}$ gilt aber $A^2 \neq A$.

Kapitel 5

Eigenwerte und Diagonalisierbarkeit

5.1 Eigenwerte

Sei V ein K-Vektorraum, $dim V = n < \infty$. $B = (v_1,\dots,v_n)$ sei Basisfolge von V. $\varphi \in End V$ d.h. $\varphi : V \longrightarrow V$, ${}_B[\varphi]_B = {}_B\varphi_B = [a_{ij}] \in K^{n\times n}$, $\varphi(v_j) = \sum_{i=1}^{n} a_{ij}\cdot v_i$.

Ziel: Zu gegebenem $\varphi \in End V$ suche Basisfolge B' so, daß ${}_{B'}\varphi_{B'}$ "möglichst einfach" ist, d.h. die Art der Abbildung offenlegt.

In Satz 2 (siehe Seite 49) hatten wir gesehen:

$$ {}_{B'}\varphi_{B'} = P^{-1}\cdot {}_B\varphi_B \cdot P \text{ mit } P = {}_B id_{B'} $$

Definition 1 (Diagonalisierbarkeit) $\varphi \in End V$ (bzw. $A \in K^{n\times n}$) heißt *diagonalisierbar*, wenn es eine Basisfolge B' von V gibt (bzw. $P \in GL(n,K)$ gibt) mit

$$ {}_{B'}\varphi_{B'} = \begin{bmatrix} t_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & t_n \end{bmatrix} \text{ bzw. } P^{-1}\cdot A\cdot P = \begin{bmatrix} t_1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & t_n \end{bmatrix} $$

Definition 2 (Eigenvektor, Eigenwert) $v \in V$ heißt *Eigenvektor* von $\varphi \in End V$, wenn $v \neq o$ und $\varphi(v) = tv$ für ein $t \in K$ (d.h. $\varphi(v) \in \langle v\rangle$). t heißt dann *Eigenwert* von φ. $v \in K^{n\times 1}\setminus\{0\}$ heißt *Eigenvektor* von $A \in K^{n\times n}$, wenn $Av = tv$ für $t \in K$; t heißt dann *Eigenwert* von A.

Beachte: Für jedes $t \in K$ gilt $\varphi(0) = 0 = t\cdot 0$.

Folgerung 1 $\varphi \in End V$, $dim V = n < \infty$, ist genau dann diagonalisierbar, wenn es eine Basis von V gibt, die aus Eigenvektoren von φ besteht.

Definition 3 (Menge der Eigenvektoren) Die *Menge der Eigenvektoren* $E_\varphi(t)$ von $\varphi \in End V$ ist definiert als

$$ E_\varphi(t) = \{v \in V \mid \varphi(v) = tv \wedge t \in K \text{ beliebig und } \varphi \in End(V)\} $$

Bemerkung: Für $\varphi \in End V$ und $t \in K$ beliebig ist $E_\varphi(t) = Kern(\varphi - t\cdot id_V)$, also ein Teilraum von V. t ist genau dann Eigenwert von φ, wenn gilt $E_\varphi(t) \neq \{o\}$.

Beweis:

$$v \in E_\varphi(t) \Leftrightarrow \varphi - tv = \mathfrak{o} \Leftrightarrow (\varphi - t \cdot id_V)(v) = \mathfrak{o} \Leftrightarrow v \in Kern(\varphi - t \cdot id_V)$$

□

Definition 4 (Eigenraum) Gilt $E_\varphi(t) \neq \{\mathfrak{o}\}$, dann heißt $E_\varphi(t)$ *Eigenraum* von φ zum Eigenwert t mit $t = \{\mathfrak{o}\} \cup \{v | v \text{ Eigenvektor von } \varphi \text{ zum Eigenwert } t\}$.

Lemma 1 $\varphi \in End\,V$, $dim\,V = n < \infty$. Dann sind folgende Aussagen äquivalent:

1. $t \in K$ ist Eigenwert von φ
2. $Rg(\varphi - t \cdot id_V) < n$
3. $det(\varphi - t \cdot id_V) = 0$
4. $det({}_B\varphi_B - t \cdot E_n) = 0$.

Beweis:

$$t \text{ Eigenwert von } \varphi \Leftrightarrow Kern(\varphi - t \cdot id_V) \neq \{\mathfrak{o}\} \Leftrightarrow Rg(\varphi - t \cdot id_V) < n$$

(folgt aus dem Dimensionssatz, Seite 30), weiterhin gilt:

$$Rg\,\psi < n \Leftrightarrow det\,\psi = 0 \text{ für } \varphi \in End\,V, dim\,V = n$$

□

Beispiel:

$\varphi \in End\left(\mathbb{R}^{2\times 1}\right)$, $B = (e_1, e_2)$

Betrachte die Abbildung mit der Matrix ${}_B\varphi_B = \frac{1}{3}\begin{bmatrix} -1 & 2 \\ 4 & 1 \end{bmatrix}$. Was macht diese Matrix?

1. Berechnung der Eigenwerte t:

$$\begin{aligned} t \text{ Eigenwert} &\Leftrightarrow det\left(\begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \\ \frac{4}{3} & \frac{1}{3} \end{bmatrix} - t\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \mathfrak{o} \\ &\Leftrightarrow det\begin{bmatrix} -\frac{1}{3} - t & \frac{2}{3} \\ \frac{4}{3} & \frac{1}{3} - t \end{bmatrix} = \mathfrak{o} \\ &\Leftrightarrow t^2 - \frac{1}{9} - \frac{8}{9} = t^2 - 1 = (t+1)(t-1) = \mathfrak{o} \\ &\Leftrightarrow t = 1 \vee t = -1 \end{aligned}$$

2. Berechnung der Eigenvektoren für $t = 1$ und $t = -1$:

   (a) $v \in E_\varphi(1) \Leftrightarrow \varphi(v) = 1v \Leftrightarrow (\varphi - 1 \cdot id)(v) = \mathfrak{o}$

   $$\begin{bmatrix} -\frac{4}{3} & \frac{2}{3} \\ \frac{4}{3} & -\frac{2}{3} \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \mathfrak{o} \Rightarrow E_\varphi(1) = \left\langle \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\rangle$$

   (b) $v \in E_\varphi(-1) \Leftrightarrow \varphi(v) = -v \Leftrightarrow (\varphi + 1 \cdot id)(v) = \mathfrak{o}$

   $$\begin{bmatrix} \frac{2}{3} & \frac{2}{3} \\ \frac{4}{3} & \frac{4}{3} \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \mathfrak{o} \Rightarrow E_\varphi(-1) = \left\langle \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\rangle$$

3. $B' = (v_1, v_2)$, $v_1 = (1,2)^T$, $v_2 = (1,-1)^T$

   $${}_{B'}[\varphi]_{B'} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

   Also ist φ Schrägspiegelung (Spiegelung an der Ursprungsgerade).

Satz 1 Sind $t_1,\ldots,t_m$ paarweise verschiedene Eigenwerte von φ ($t_i \neq t_j$ für $i \neq j$) und ist v_i Eigenvektor von φ zum Eigenwert t_i, so ist $(v_1,\ldots,v_m)$ linear unabhängig. “Eigenvektoren zu verschiedenen Eigenwerten sind linear unabhängig.”

Beweis: Induktion nach m

- Induktionsanfang: $m = 1$: Ein Eigenvektor v_1 zu t_1 ist ungleich dem Nullvektor, also ist (v_1) linear unabhängig.
- Induktionsannahme: $A(m)$ gilt.
- Induktionsschluß: $a_1v_1 + \ldots + a_mv_m = \mathfrak{o}$ $(\star)$ mit $a_i \in K$.
  Wende auf $(\star)$ φ an. Man erhält: $a_1t_1v_1 + \ldots + a_mt_mv_m = \mathfrak{o}$
  Multipliziere $(\star)$ mit t_m. Dadurch erhält man: $a_1t_mv_1 + \ldots + a_1t_mv_m = \mathfrak{o}$
  Subtrahiere nun: $a_1(t_1 - t_m)v_1 + \ldots + a_{m-1}(t_{m-1} - t_m)v_{m-1} = \mathfrak{o}$. Nach Induktionsannahme ist $a_1(t_1 - t_m) = \ldots = a_{m-1}(t_{m-1} - t_m)v_{m-1} = \mathfrak{o}$. Also ist $a_i(t_i - t_m) = \mathfrak{o}$ $(t_i - t_m \neq 0)$ für $(i = 1,\ldots,m-1)$. Daher ist also $a_1 = \ldots = a_{m-1} = 0$, und aus $(\star)$ bleibt: $a_mv_m = \mathfrak{o}$ mit $v_m \neq \mathfrak{o}$. Es folgt: $a_m = 0$. □

5.2 Das charakteristische Polynom

Definition 1 (charakteristische Matrix, ch. Polynom): Ist $A \in K^{n\times n}$ (K Körper), so heißt

$$\tilde{A} = [XE_n - A] = \begin{bmatrix} X-a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & -a_{n-1\,n} \\ -a_{n1} & \ldots & -a_{n\,n-1} & X-a_{nn} \end{bmatrix} \in K[X]^{n\times n}$$

($K[X]$ ist Polynomring über K in X) *charakteristische Matrix* von A.

$$\chi_A = det\,\widetilde{A} = det\,[XE_n - A] \in K[X]$$

heißt *charakteristisches Polynom* von A.

Folgerung 1 Aus Lemma 1 (Seite 57) läßt sich folgern:

$$\begin{aligned} t \in K \text{ ist Eigenwert von } \varphi \quad &\Leftrightarrow \quad det\,(A - tE_n) = 0 \\ &\Leftrightarrow \quad det\,(tE_n - A) = 0 \\ &\Leftrightarrow \quad \chi_A(t) = 0 \\ &\Leftrightarrow \quad t \text{ Nullstelle des char. Polynoms} \end{aligned}$$

Satz 1 Ist $A \in K^{n\times n}$ (K Körper), so ist

$$\chi_A = det(XE_n - A) = X^n - c_1X^{n-1} + c_2X^{n-2} + \ldots + (-1)^n c_n$$

mit $c_1 = Spur\,A := a_{11} + a_{22} + \ldots + a_{nn}$ und $c_n = det\,A$.

Beweis: $\chi_A = det\,\widetilde{A}$, $\widetilde{A} = [\widetilde{a}_{ij}]$ mit

$$K[X] \ni \widetilde{a}_{ij} = \begin{cases} X - a_{ij} & i = j \\ -a_{ij} & i \neq j \end{cases} \quad \text{und } Grad\,\widetilde{a}_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

$$\begin{aligned}\chi_a = det\widetilde{A} &= \sum_{\sigma\in S_n} \varepsilon(\sigma)\cdot \widetilde{a}_{\sigma(1)1}\cdot\ldots\cdot\widetilde{a}_{\sigma(n)n} \\ &= (X-a_{11})\cdot\ldots\cdot(X-a_{nn}) + \sum_{\sigma\in S_n,\sigma\neq id} \varepsilon(\sigma)\cdot \widetilde{a}_{\sigma(1)1}\cdot\ldots\cdot\widetilde{a}_{\sigma(n)n}\end{aligned}$$

Es ist $\widetilde{a}_{\sigma(1)1}\cdot\ldots\cdot\widetilde{a}_{\sigma(n)n} = 0$ oder $grad\,(\widetilde{a}_{\sigma(1)1}\cdot\ldots\cdot\widetilde{a}_{\sigma(n)n}) \leq n-2$. Ist $\sigma \neq id$, so gibt es mindestens 2 Ziffern i_1, i_2 mit $\sigma(i_1)\neq i_1$ und $\sigma(i_2) = i_2$. Also:

$$\chi_A = (X-a_{11})\cdot\ldots\cdot(X-a_{nn}) + \begin{cases} 0 & \text{oder} \\ g & \text{mit}\, Grad\, g \leq n-2 \end{cases}$$

Daher ist

$$\text{Koeffizient von}\, X^n \text{ in } \chi_A = \text{Koeffizient von } X^n \text{ in} \,(X-a_{11})\cdot\ldots\cdot(X-a_{nn}) = 1$$

Also:

$$\ldots. X^{n-1}\ldots = -a_{11} - \ldots - a_{nn} = -spur\, A$$

$\square$

Satz 2

1. Sind $A, A' \in K^{n\times n}$ ähnlich, d.h. gibt es $P \in GL(n,K)$ und $A' = P^{-1}AP$, so ist $\chi_A = \chi_{A'}$, insbesondere ist $Spur\,A = Spur\,A'$ und $det\,A = det\,A'$.
2. t ist Eigenwert von $\varphi \in End\,V$ gdw. für $A = {}_B\varphi_B$ gilt: t ist Nullstelle von χ_A.

Beweis:

1. $\chi_{A'} = det(XE_n - P^{-1}AP) = det(P^{-1}(XE_n - A)P) = det(P^{-1})\cdot det(XE_n - A)\cdot det(P) = det(XE_n - A) = \chi_A$
   Benutze nun Satz 1.
2. (vgl. Lemma 1, Seite 57): t ist Eigenwert von $\varphi \Leftrightarrow det(A - tE_n) = 0 \Leftrightarrow det(tE_n - A) = 0$.
   Setze: $\widetilde{A} = XE_n - A = [\widetilde{a_{ij}}]$. Dann:

$$\begin{aligned}\chi_A(t) &= det(XE_n - A)(t) \\ &= \sum_{\sigma\in S_n} \varepsilon(\sigma)\cdot\widetilde{a}_{\sigma(1)1}(t)\cdot\ldots\cdot\widetilde{a}_{\sigma(n)n}(t) \\ &= det\begin{bmatrix} t-a_{11} & \ldots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \ldots & t-a_{nn}\end{bmatrix} = det(tE_n - A) = 0\end{aligned}$$

$\square$

Definition 2 (Vielfachheit) Sei t Eigenwert von φ, $A = {}_B\varphi_B \in K^{n\times n}$. t hat die *algebraische Vielfachheit k*, wenn t k-fache Nullstelle von χ_A ist, also wenn $\chi_A = (X-t)^k \cdot g$ mit $g(t) \in K[X] \neq 0$. t hat die *geometrische Vielfachheit* $dim\,E_\varphi(t) = dim\,Kern(\varphi - t\cdot id_V)$.

Satz 3 Ist t Eigenwert von $\varphi \in End V$, $dim V = n < \infty$, dann gilt:

$$\text{geometrische Vielfachheit von } t \leq \text{algebraische Vielfachheit von } t$$

Beweis: Sei $(v_1, ..., v_r)$ Basisfolge von $Kern(\varphi - t \cdot id_V) = E_\varphi(t)$, wobei r geometrische Vielfachheit von t ist. Ergänze diese Basisfolge zur Basisfolge $V = (v_1, ..., v_r, ..., v_n)$ von V. Dann gilt:

$$A = {}_B\varphi_B = \begin{bmatrix} t & & & & \\ & \ddots & & A_2 & \\ & & t & & \\ 0 & \cdot\cdot & 0 & & n \\ \vdots & \ddots & \vdots & A_1 & \\ 0 & \cdot\cdot & 0 & & \end{bmatrix}$$

mit $A_1 \in K^{(n-r)\times(n-r)}$ (r ist Anzahl diagonaler t's) und $A_2 \in K^{n\times(n-r)}$. Weiterhin gilt:

$$\chi = det(XE_n - A) = det \begin{bmatrix} X-t & & & \\ & \ddots & & -A_2 \\ & & X-t & \\ & 0 & & XE_{n-r} - A_1 \end{bmatrix} = (X-t)^r \cdot \chi_{A_1}$$

also ist t Nullstelle von χ_A mit Vielfachheit r. □

Beispiele:

- ${}_B\varphi_B = A = \begin{bmatrix} t & 1 & 0 \\ 0 & t & 1 \\ 0 & 0 & t \end{bmatrix}$, $\varphi = \varphi_A$, $\chi_A = det \begin{bmatrix} X-t & -1 & 0 \\ 0 & X-t & -1 \\ 0 & 0 & X-t \end{bmatrix} = (X-t)^3$, $V = K^{3\times 1}$.

  Dann:

$$\begin{aligned} E_\varphi(1) &= Kern(\varphi - t \cdot id) \\ &= \{v \in K^{3\times1} \mid (A - tE_3)v = 0\} \\ &= \left\{ v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \middle| \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 0 \right\} \quad \text{also } dim E_\varphi(t) = 1 \end{aligned}$$

  geometrische Vielfachheit von t ist 1, algebraische Vielfachheit ist 3.

- $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $\varphi = \varphi_A : \begin{array}{ccc} \mathbb{R}^{2\times1} & \longrightarrow & \mathbb{R}^{2\times1} \\ x & \longmapsto & Ax \end{array}$

  $\chi_A = X^2 + 1$ hat in $\mathbb{R}$ keine Nullstellen, φ bzw. A hat keinen Eigenwert in $\mathbb{R}$.

  $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$; $\chi_A(A) = A^2 + E_n = 0$

Satz 4 (Cayley, Hamilton) Sei $A \in K^{n\times n}$, K Körper. Dann ist $\chi_A(A) = 0$.

Beweis (zwei Möglichkeiten):

1. $\widetilde{A} = (XE_n - A) = [\widetilde{a_{ij}}] = [\delta_{ij}X - a_{ij}]$. $D = [d_{ij}] = adj \widetilde{A}^t$ sei die Adjunkte.

$$D \cdot \widetilde{A}^T = det \widetilde{A}^T \cdot E_n = \sum_{j=1}^{n} d_{ij} \cdot \widetilde{a}_{kj} = \delta_{ik} \cdot \chi_A \quad \text{setze } A \text{ ein...}$$

$$\sum_{j=1}^{n} d_{ij}(A) \cdot \widetilde{a}_{kj}(A) = \delta_{ik} \cdot \chi_A(A)$$

Wir zeigen: $\chi_A(A)\cdot e_i = 0$ für $i = 1,\dots,n$. Linke Seite ist i-te Spalte von $\chi_A(A)$.

$$\begin{aligned}
\chi_A(A)\cdot e_i &= \sum_{k=1}^{n} \chi_A(A)\cdot \delta_{ik}\cdot e_k = \sum_{k=1}^{n}\sum_{j=1}^{n} d_{ij}(A)\cdot \widetilde{a}_{kj}(A)\cdot e_k \\
&= \sum_{j=1}^{n} d_{ij}(A)\cdot \sum_{k=1}^{n}\left(\delta_{kj}A - a_{kj}E_n\right)\cdot e_k \\
&= \sum_{j=1}^{n} d_{ij}(A)\left(Ae_j - \sum_{k=1}^{n} a_{kj}\cdot e_k\right) = 0
\end{aligned}$$

denn $Ae_j = [a_{1j},\dots,a_{nj}]^T = \sum_{k=1}^{n} a_{kj}e_k$. □

2. “Beweis” nach Cayley
   $n = 2$, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $\chi_A = X^2 - (a_{12}+a_{12})X + a_{11}a_{22} - a_{12}a_{21}$
   $B = A^2 - (a_{11}+a_{22})A + (a_{11}a_{22} - a_{12}a_{21})E_2 = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$
   $b_{11} = a_{11}^2 + a_{12}a_{21} - (a_{11}+a_{22})a_{11} + a_{11}a_{22} - a_{12}a_{21} = 0$ etc. □

Folgerung 2 Ist $A \in K^{n\times n}$ beliebig, K ein Körper, dann gibt es $f \in K[X]$ mit $f(A) = 0$. *Grad* $f \le n$, f normiert, d.h. $f = \sum_{i=0}^{m} a_iX^i$, $a_m = 1$, $m \le n$.

5.3 Minimalpolynom

Definition 1 (Minimalpolynom) Ist $\varphi \in End\,V$ oder $A \in K^{n\times n}$, K Körper, so heißt μ $(= \mu_\varphi = \mu_A) \in K[X]$ *Minimalpolynom* von φ bzw. von A, wenn

1. $\mu(\varphi) = 0$ bzw. $\mu(A) = 0$
2. Ist $0 \ne f \in K[X]$, $f(\varphi) = 0$ bzw. $f(A) = 0$, so ist $Grad\,\mu \le Grad\,f$.
3. μ ist “normiert”, d.h. von der Form $\mu = X^m + a_{m-1}X^{m-1} + \dots + a_1X^0 + a_0$.

Lemma 1 Ist $P \in K[X]$, $f(\varphi) = 0$ ($f(A) = 0$), so “teilt” μ_φ (μ_A) f ($\mu_\varphi | f$ bzw. $\mu_A | f$), d.h.

$$f = \mu_\varphi \cdot g \text{ bzw. } f = \mu_A \cdot g \text{ mit } g \in K[X]$$

Beweis: Division mit Rest ergibt $f = g\mu + r$ mit $Grad\,r < Grad\,\mu$ oder $r = 0$. Setze φ (bzw. A) ein. Dann:

$$f(\varphi) = g(\varphi)\circ\mu(\varphi) + r(\varphi)$$

Da $f(\varphi) = 0$ und $\mu(\varphi) = 0$, ist $r(\varphi) = 0$, denn wäre $r(\varphi) \ne 0$, dann wäre nach (2) $Grad\,r \ge Grad\,\mu$, was jedoch ein Widerspruch ist. □

Folgerung 1

1. μ_φ bzw. μ_A (Minimalpolynom) ist eindeutig bestimmt.
2. μ_A teilt das charakteristische Polynom χ_A.

Beweis:

1. Wären μ und g Minimalpolynome von A (bzw. φ), so würde $\mu|g$ und $g|\mu$ gelten, also
$$g = c\mu$$
mit $Grad\, g = Grad\, \mu$. Weiterhin ist $c = 1$, weil g und μ normiert sind.

2. Nach Cayley-Hamilton (Satz 4, Seite 5.2) ist $\chi_A(A) = 0$. Wende dann Lemma 1 an. □

Wie findet man μ_A?
1. Möglichkeit: χ_A bekannt. Betrachte Teiler f von χ_A und setze A ein. $f(A) \overset{?}{=} 0$.
2. Möglichkeit: Finde kleinstes $m \in \mathbb{N}$ mit $(A \in K^{n\times n})$ $A^m \in \langle E_n = A^0, A, A^2, \ldots, A^{m-1}\rangle$. Dann ist $A^m = a_0E_n + a_1A + \ldots + a_{m-1}A^{m-1}$ und $\mu_A = X^m - a_{m-1}X^{m-1} - \ldots - a_1X - a_0$

Beispiel:

$A = [a_{ij}] \in K^{2n\times 2n}$, $a_{ij} = 1$ für $i + j$ gerade, $a_{ij} = 0$ für $i + j$ ungerade.

$$A = \begin{bmatrix} 0 & 1 & 0 & \ldots \\ 1 & 0 & 1 & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{bmatrix} \qquad (E_n, A) \text{ linear unabhängig}$$

$$A^2 = \begin{bmatrix} n & 0 & n & \ldots \\ 0 & n & 0 & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{bmatrix} \qquad (E_n, A, A^2) \text{ linear unabhängig}$$

$$A^3 = \begin{bmatrix} 0 & n^2 & 0 & \ldots \\ n^2 & 0 & n^2 & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{bmatrix} \qquad A^3 = n^2A$$

Also ist $\mu_A = X^3 - n^2X = X(X - n)(X + n)$.

Satz 1 $t \in K$ ist Eigenwert von $\varphi \in End\,V$ $(dim\,V < \infty)$ bzw. von A genau dann, wenn $\mu_\varphi(t) = 0$ bzw. $\mu_A(t) = 0$. "Die Eigenwerte sind genau die Nullstellen des Minimalpolynoms".

Beweis:

1. Nach Folgerung 1, Seite 58, gilt "t ist Eigenwert genau dann, wenn $\chi_A(t) = 0$". Es folgt: $\chi_A = \mu_A \cdot q$ mit $q \in K[X]$, $\chi_A = \mu_A(t) \cdot q(t)$. $\mu_A(t) = 0 \Rightarrow \chi_A(t) = 0$, d.h. t ist Eigenwert.

2. Sei umgekehrt t Eigenwert von A. Dann ist $f(t)$ Eigenwert von $f(A)$ für $f \in K[X]$. Setze $f = \mu_A$. Also ist $\mu_A(t) = 0$. □

Folgerung 2 μ_A und χ_A haben die gleichen Nullstellen, wenn auch evtl. (meistens) mit verschiedenen Vielfachheiten.

Beispiel (Fortsetzung):

A hat Eigenwerte $0, -n, n$.

Geometrische Vielfachheit vom Eigenwert 0 ist $dim\,E_{\varphi_A}(0) = 2n - Rg\,A = 2n - 2$, geo. Vfh. von n ist $dim\,E_{\varphi_A}(n) = 2n - Rg(A - nE_{2n}) = 1$. Entsprechend ergibt sich für die geo.Vfh. von $-n$ ebenfalls 1.

Algebraische Vielfachheit vom Eigenwert 0 von A ist größer oder gleich $2n-2$. Entsprechend für n größer oder gleich 1 und für $-n$ ebenfalls ≥ 1. Also ist $\chi_A = X^{2n-2}(X - n)(X + n)$, $Grad\,\chi_A = 2n$.

Es gibt Basisfolge $B = (v_1, \dots, v_{2n})$ (d.h. $P \in GL(2n, K)$) mit

$$_B[\varphi_A]_B = P^{-1}AP = \begin{bmatrix} n & 0 & \dots & 0 \\ 0 & -n & & : \\ : & & 0 & : \\ 0 & \dots & \dots & 0 \end{bmatrix}$$

A ist diagonalisierbar.

Satz 2 Sei $\varphi \in End V$ ($dim V = n < \infty$). φ ist genau dann diagonalisierbar, wenn

$$\mu_\varphi = (X - t_1) \cdot \dots \cdot (X - t_r) \text{ mit } t_i \neq t_j \text{ für } i \neq j$$

Beweis:

- "$\Rightarrow$": Sei $B = (v_1, \dots, v_n)$ Basisfolge mit

$$\begin{aligned} _B\varphi_B &= diag(t_1, \dots, t_1, t_2, \dots, t_2, \dots, t_r, \dots, t_r) \\ &= diag(t_1 - t_2, \dots, t_1 - t_2, 0, \dots, 0, \dots, t_n - t_2, \dots, t_n - t_2) \\ &= \dots = 0 \end{aligned}$$

  $\mu = (X - t_1) \cdot \dots \cdot (X - t_n)$, $\mu(A) = 0$, $t_i \neq t_j$.

- "$\Leftarrow$": Siehe Kapitel 4. □

5.4 φ-invariante Teilräume

Voraussetzung: $\varphi \in End(V)$.

Definition 1 (invarianter Teilraum) Ein Teilraum U von V heißt φ-*invariant*, wenn aus $u \in U$ folgt $\varphi(u) \in U$ (d.h. $\varphi(U) \leq U$).

Beispiele:

- $\{o\}$ und V sind φ-invariant
- Ist t Eigenwert, so ist $E_\varphi(t) = \{v \in V \mid \varphi(v) = tv\}$ φ-invariant: $\varphi(V) \in \langle v \rangle$. Es ist sogar jeder Teilraum von $E_\varphi(t)$ φ-invariant.
- Sind U_1, U_2 φ-invariante Teilräume, so sind $U_1 \cap U_2$ und $U_1 + U_2$ φ-invariant.
- Ist $f \in K[X]$ so sind $U_1 = Kern\, f(\varphi)$ und $U_2 = Bild\, f(\varphi)$ φ-invariant.
  Beweis: $X \cdot f = f \cdot X$ in $K[X]$, also $\varphi \cdot f(\varphi) = f(\varphi) \cdot \varphi$.
  (a) $u \in U_1 \Leftrightarrow f(\varphi)(u) = \underline{0} \Rightarrow f(\varphi)(\varphi(u)) = 0$ $[\varphi(u) \in U_1]$
  (b) $u \in U_2 \Leftrightarrow u = f(\varphi)(w)$ für ein $w \in V$ denn $\varphi(u) = f(\varphi)(\varphi(w)) \in Bild\, f(\varphi) = U_2$ □

Lemma 1 Sei U ein φ-invarianter Teilraum, dann...

1. ... ist $\varphi|_U \in End(U)$ (Restriktion von φ auf U) φ-invariant. Durch

$$\varphi' : \begin{array}{ccc} V/U & \longrightarrow & V/U \\ v + U & \longmapsto & \varphi(v) + U \end{array}, \ \varphi' \in End(V \setminus U)$$

   wird auch der Faktorraum V/U φ-invariant.

2. Ist $B_1 = (v_1, ..., v_r)$ Basisfolge von U und $B = (v_1, ..., v_r, v_{r+1}, ..., v_n)$ Basisfolge von V, so ist ${}_B\varphi_B = \begin{bmatrix} A_1 & A_3 \\ 0 & A_2 \end{bmatrix}$, $A_1 \in K^{r \times n}$, $A_2 \in K^{(n-r)\times(n-r)}$, mit $A_1 = {}_{B_1}[\varphi|_U]_{B_1} \in K^{r\times r}$ und $A_2 = {}_{B'_2}[\varphi']_{B'_2}$ wobei $B'_2 = (v_{r+1} + U, ..., v_n + U)$.

3. $\chi_\varphi = \chi_A = \chi_{A_1} \cdot \chi_{A_2} = \chi_{\varphi|_U} \cdot \chi_{\varphi'}$, weiterhin: $\mu_{\varphi|_U} | \mu_\varphi$ und $\mu_{\varphi'} | \mu_\varphi$ ("|": "teilt"). Weiterhin gilt:
$$\mu_{A_1}|\mu_A,\ \mu_{A_2}|\mu_A \text{ und } 0 = \mu_A(A) = \begin{bmatrix} \mu_A(A_1) & \star \\ 0 & \mu_A(A_2) \end{bmatrix}$$

Definition 2 (direkte Summe) Seien U_1, U_2 Teilräume von V und ist $V = U_1 + U_2$ und $U_1 \cap U_2 = \{0\}$. Dann ist V *direkte Summe* von U_1 und U_2, in Zeichen: $V = U_1 \oplus U_2$.

Bemerkung: Ist $V = U_1 \oplus U_2$ mit φ-invarianten Teilräumen U_1 und U_2, $B_1 = (v_1, ..., v_r)$ Basisfolge von U_1 und $B_2 = (v_{r+1}, ..., v_n)$ Basisfolge von U_2, so ist:
$${}_B\varphi_B = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$
mit $A_1 = {}_{B_1}[\varphi|_{U_1}]_{B_1}$ und $A_2 = {}_{B_2}[\varphi|_{U_2}]_{B_2}$.

Lemma 2 Ist $\varphi \in End\,V$ mit $\mu_\varphi = (X-t)^m$, so gibt es eine Basis $B = (v_1, ..., v_n)$ mit
$${}_B[\varphi]_B = \begin{bmatrix} t & & \star \\ & \ddots & \\ 0 & & t \end{bmatrix}$$
Insbesondere ist $\chi_\varphi = (X-t)^n$ mit $n = dim V$.

Beweis: Benutze Lemma 1 mit $U = \langle v_1 \rangle$, wobei v_1 Eigenvektor von φ zum Eigenwert t.
$${}_B[\varphi]_B = \begin{bmatrix} t & A_3 \\ 0 & A_2 \end{bmatrix}$$
mit $\mu_{A_2} = (X-t)^{m_1}$, $m_1 \leq m$, φ' wie in Lemma 1. Nach Induktion existiert eine Basis $B'_2 = (v'_2, ..., v'_n)$, $v'_i = v_i + U$.
$${}_{B'_2}[\varphi]_{B'_2} = \begin{bmatrix} t & & \star \\ & \ddots & \\ 0 & & t \end{bmatrix}$$
$B = (v_2, ..., v_n)$, dann hat ${}_B[\varphi]_B$ *die* gewünschte Gestalt. □

Lemma 3 Ist $f \in K[X]$, K Körper, mit $f(t) \neq 0$, $t \in K$, dann gibt es zu beliebigem $m \in \mathbb{N}$ Polynome $g, h \in K[X]$ mit
$$1 = g \cdot f + h \cdot (X-t)^m$$

Beweis: Induktion nach m:

- $m = 1$: Division mit Rest ergibt:
$$f = (X-t)q + c \quad c \in K, c = f(t) \neq 0, q \in K[X]$$
Daraus folgt: $1 = \frac{1}{c} \cdot f + (-q) \cdot (X-t) \cdot \frac{1}{c}$.

- $m > 1$: $1 = g_1 \cdot f + h_1(X-t)^{m-1}$ nach Induktionsannahme. Multipliziere mit $\frac{1}{c}(-q)(X-t) = 1 - \frac{1}{c} f$, man erhält $1 - \frac{1}{c} f = (1 - \frac{1}{c}) \cdot f \cdot g_1 \cdot f + \frac{1}{c} h_1(-q)(X-t)^m$, also $1 = (...) \cdot f + (\frac{1}{c} \cdot g \cdot h_1)(X-t)^m$, was der gesuchten Form entspricht. □

Satz 1 Sei $f \in K[X]$ mit $f(\varphi) = 0$ und $f = (X-t)^m \cdot f_1$ mit $f_1(t) \neq 0$ (z.B. $f = \mu_\varphi$ oder $f = \chi_\varphi$), t Eigenwert von φ. Dann ist

$$V = Kern(\varphi - t \cdot id)^m \oplus Bild(\varphi - t \cdot id)^m$$

(der erste Summand sei U_1, der zweite U_2) mit φ-invarianten Teilräumen U_1 und U_2. Es gibt also eine Basisfolge B von V mit

$$_B[\varphi]_B = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$

mit $\chi_{A_1} = (X-t)^r$ und $\chi_{A_2}(t) \neq 0$. Ist speziell $f = \chi_\varphi$, so ist $\chi_{A_1} = (X-t)^m$ und $\chi_{A_2} = f_1$, ist $r = \mu_\varphi$, so ist $\mu_{A_1} = (X-t)^m$ und $\mu_{A_2} = f_1$.

Beweis: Wende Lemma 3 auf f_1 und t an: $1 = gf_1 + h(X-t)^m$. Setze nun φ an: $id_V = g(\varphi)f_1(\varphi) + h(\varphi)(\varphi - t \cdot id_V)^m$ und wende dies schließlich auf $v \in V$ an: $(\star)$ $v = g(\varphi)f_1(\varphi)(v) + h(\varphi)(\varphi - t \cdot id_V)^m(v)$. Der erste Summand von $(\star)$ sei v_1, der zweite v_2. Es gilt:

1. $v_2 = (\varphi - t \cdot id)^m(h(\varphi)(v)) \in Bild\,(\varphi - t \cdot id_V)^m = U_2$
2. $v_1 \in U_1 = Kern(\varphi - t \cdot id)^m$ denn $(\varphi - t \cdot id_V)^m(v_1) = g(\varphi)(\varphi - t \cdot id)^m f_1(\varphi)(v) = 0$ (denn $f(\varphi) = \underline{0}$)

Also $V = U_1 + U_2$. Behauptung: $U_1 \cap U_2 = U_2 \cap U_1 = \{0\}$. Sei $v \in U_1 \cap U_2$, also $v = (\varphi - t \cdot id)^m w \in U_1 = Kern(\varphi - t \cdot id)^m$, d.h. $0 = (\varphi - t \cdot id)^{2m} w$. Setze v in $(\star)$ ein:

$$v = g(\varphi) \cdot f_1(\varphi)(v) + h(\varphi)(\varphi - t \cdot id)^m(v) = g(\varphi) \cdot f_1(\varphi)(\varphi - t \cdot id)^m(w) = 0$$

Demnach ist $V = U_1 \oplus U_2$, also bei angepaßter Basis $_B[\varphi]_B = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$. t ist nicht Eigenwert von A_2 weil alle Eigenvektoren von φ zum Eigenwert t in U_1 liegen. Es gilt weiterhin $\mu_{A_1} = \mu_A = \mu_\varphi$. Für ein beliebiges Polynom $g \in K[X]$ ist

$$0 = g(A) \Leftrightarrow g(A_1) = 0 \wedge g(A_2) = 0$$

□

Folgerung 1 Ist $\mu_\varphi = (X-t_1) \cdot \ldots \cdot (X-t_r)$ mit $t_i \neq t_j$ für $i \neq j$, so ist φ diagonalisierbar.

Beweis: Wende Satz 1 an mit $t = t_1$, $f = \mu_\varphi$, $f_1 = (X-t_2) \cdot \ldots \cdot (X-t_r)$. Es gibt danach eine Basis B mit

$$A = {}_B[\varphi]_B = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$

mit $\mu_{A_1} = X - t_1$ und $\mu_{A_2} = f_1 = (X-t_2) \cdot \ldots \cdot (X-t_r)$ also $A_1 = t_1 E_{r_1} = \begin{bmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_r \end{bmatrix}$. Mittels Induktion folgt die Behauptung. □

Satz 2 (Fahnensatz) Ist $\chi_\varphi = \prod_{i=1}^r (X-t_i)^{k_i}$, $t_i \neq t_j$ für $i \neq j$, so gibt es eine Basis B von V mit

$$_B[\varphi]_B = \begin{bmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{bmatrix} = diag(A_1, \ldots, A_r)\,\mathrm{mit} A_i = \begin{bmatrix} t_i & & \star \\ & \ddots & \\ 0 & & t_i \end{bmatrix}$$

Beweis: Wende Induktion, Satz 1 und Lemma 2 an. □

Bemerkung: Als “Fahne” wird hier eine Folge von Teilräumen $U_0 \subset U_1 \subset U_2 \ldots$ mit $dim U_i = i$ bezeichnet, vgl. Abb. 5.1.

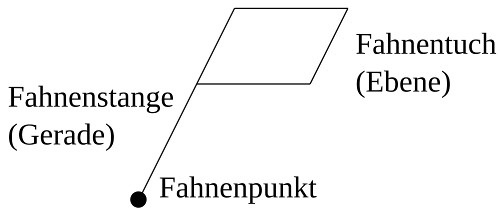

Abbildung 5.1: Zur Veranschaulichung des Fahnensatzes.

5.5 Die Jordansche Normalform

Satz 1 Ist $\varphi \in End\,V$ mit dem charakteristischen Polynom $\chi_\varphi = \prod_{i=1}^r (X-t_i)^{k_i}$, $t_i \neq t_j$ für $i \neq j$, dann gibt es eine Basisfolge B, so daß:

$$_B\varphi_B = A = diag(A_1,\ldots,A_r)$$

$A_i \in K^{k_i \times k_i}$ mit $A_i = diag(J_{m_1}(t_i),\ldots,J_{m_{d(i)}}(t_i))$ und $J_m(t) = \begin{bmatrix} t & 0 & \ldots & 0 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 1 & t \end{bmatrix} \in K^{m\times m}$.

Bei anderer Ordnung der Basisvektoren erhält man A^T statt A.

Beweis: Nach Satz 1, Seite 65, ist

$$V = Kern(\varphi - t_1 \cdot id)^{k_1} \oplus Kern(\varphi - t_2 \cdot id)^{k_2} \oplus \ldots \oplus Kern(\varphi - t_r \cdot id)^{k_r}$$

O.B.d.A. sei $r=1$, $\chi = (X-t)^n$. Setze $\psi = \varphi - t\cdot id_V$, $\chi_\psi = X^n$ und $\mu_\psi = X^m$ mit $m \leq n$. $U_i := Kern\,\psi$.
Dann ist zunächst einmal $\{o\} = U_0 \leq U_1 \leq \ldots \leq U_m = V$ und $d_i = dim\,U_i - dim\,U_{i-1}$.
Behauptung: $U_i = \langle u_1,\ldots,u_{d_i}\rangle \oplus U_{i-1}$ ($(u_1,\ldots,u_{d_i})$ linear unabhängig) und $i>1$. Dann ist $(\psi(u_1),\ldots,\psi(u_{d_i}))$ linear unabhängig, sogar in U_{i-1} und $(\psi(u_1)+U_{i-2},\ldots,\psi(u_{d_i})+U_{i-2})$ linear unabhängig in U_{i-1}/U_{i-2}.

Beweis der Behauptung: $\sum_{i=1}^{d_i} a_i\psi(u_i) \in U_{i-2}$. Zu zeigen $a_1 = \ldots = a_{d_i} = 0$. Es gilt:

$$0 = \psi^{i-2}\left(\sum_{i=1}^{d_i} a_i\psi(u_i)\right) = \psi^{i-1}\left(\sum_{i=1}^{d_i} a_i u_i\right) \in U_{i-1} \cap \langle u_1,\ldots.,u_{d_i}\rangle$$

also $a_1 = \ldots = a_{d_r} = 0$.
Daher können wir Vektoren $v_1,\ldots,v_{d_i} \in V$ finden mit

$$\begin{aligned} V = U_m &= \langle v_1,\ldots,v_{d_m}\rangle \oplus U_{m-1} \\ U_{m-1} &= \left\langle \psi(v_1),\ldots,\psi(v_{d_m}),v_{d_m+1},\ldots,v_{d_{m-1}}\right\rangle \oplus U_{m-2} \\ &\ldots \\ U_1 &= \left\langle \psi^{m-1}(v_1),\ldots,\psi^{m-1}(v_{d_m}),\psi^{m-2}(v_{d_m+1}),\ldots,\psi^{m-2}(v_{d_{m-1}}),\ldots,v_{d_2+1},\ldots,v_{d_1}\right\rangle \end{aligned}$$

Die aufgelisteten Vektoren bilden ein Erzeugendensystem von V bestehend aus Vektoren

$$d_m + d_{m-1} + \ldots + d_2 + d_1 = n = dim\,V$$

also eine Basis. Ordne dieser Basis “spaltenweise”, d.h.

$$\begin{aligned} B = &(v_1,\psi(v_1),\ldots,\psi^{m-1}(v_1),\ldots,v_{d_m},\ldots,\psi^{m-1}(v_{d_m}), \\ &v_{d_m+1},\ldots,\psi^{m-2}(v_{d_m+1}),\ldots,v_{d_m-1},\ldots,\psi^{m-2}(v_{d_{m-1}}),\ldots,v_{d_2+1},\ldots,v_{d_1}) \end{aligned}$$

Dann ist

$$
\begin{aligned}
{}_B\Psi_B &= diag(\underbrace{J_m(0),\ldots,J_m(0),}_{d_m}\ \underbrace{J_{m-1}(0),\ldots,J_{m-1}(0)}_{d_{m-1}-d_m}\ ,\ldots,\ \underbrace{J_1(0),\ldots,J_1(0)}_{d_1-d_2}\ ) \\
&= {}_B\Psi_B + t\cdot E_n
\end{aligned}
$$

$\square$

Bemerkung: Um die Transponierte A^T zu bekommen muß man B “spaltenweise von unten nach oben” anordnen. Die Voraussetzung von Satz 1 ist stets erfüllt, falls $K=\mathbb{C}$ oder K ein algebraisch abgeschlossener Körper ist.

Beispiel:

$\chi_\varphi = (X-t)^4$. Mögliche Variationen:

Jordan-Form	Minimalpolynom	$dim\,Kern(\varphi - t\cdot id)$
$\begin{bmatrix} t&0&0&0\\1&t&0&0\\0&1&t&0\\0&0&1&t\end{bmatrix}$	$(X-t)^4$	1
$\begin{bmatrix} t&0&0&0\\1&t&0&0\\0&1&t&0\\0&0&0&t\end{bmatrix}$	$(X-t)^3$	2
$\begin{bmatrix} t&0&0&0\\1&t&0&0\\0&0&t&0\\0&0&1&t\end{bmatrix}$	$(X-t)^2$	2
$\begin{bmatrix} t&0&0&0\\1&t&0&0\\0&0&t&0\\0&0&0&t\end{bmatrix}$	$(X-t)^2$	3
$\begin{bmatrix} t&0&0&0\\0&t&0&0\\0&0&t&0\\0&0&0&t\end{bmatrix}$	$(X-t)$	4

Minimalpolynom: *Exponent ist Größe des größten Jordanblocks*
$dim\,Kern(\varphi - t\cdot id)$: *Anzahl der Jordanblöcke*

Kapitel 6

Bilinearformen und Skalarprodukte

6.1 Der Dualraum

Voraussetzung: V ist ein K-Vektorraum.

Definition 1 (Dualraum, Linearform) $V^\star = Hom(V,K)$ heißt *Dualraum* von V. Jedes $\lambda \in V^\star$ heißt eine *Linearform* (*lineares Funktional*) auf V: $\lambda : V \longrightarrow K$.

Bemerkung: Ist $dim V = n < \infty$ und $B = (v_1, \ldots, v_n)$ Basisfolge, so ist $dim V^\star = n$ und $B^\star = (v_1^\star, \ldots, v_n^\star)$ ist eine Basis von $V^\star$ mit $v_i^\star(v_j) = \delta_{ij}$, die die zu B duale Basis heißt.

$$v_i^\star\left(\sum_{j=1}^{n} x_j v_j\right) = x_i$$

Ist $\lambda \in V^\star$, dann $\lambda = \sum a_i v_i^\star$ mit $a_i = \lambda(v_i)$.

Warnung: Ist $dim V = \infty$ dann ist i.allg. $V \ncong V^\star$.

Beispiel:

$K = \mathbb{F}_2$, $V = \mathbb{F}_2^{(\mathbb{N})} = \{\, (a_i)_{i=1}^\infty | a_i \neq 0$ nur für endlich viele $i\}$ (abzählbare Menge). Dann:

$$\begin{array}{ccll} V & \longrightarrow & \mathbb{N} & \text{(Bijektion)} \\ (a_i)_{i=1}^\infty & \longmapsto & \sum_{i=1}^{\infty}(a_i 2^i) + 1 & \end{array}$$

$$\begin{array}{ccll} V^\star & \longrightarrow & \mathbb{F}_2^{\mathbb{N}} & \text{(Bijektion)} \\ \lambda & \longmapsto & \lambda(e_i) & \end{array}$$

$\mathbb{F}_2^{\mathbb{N}}$ ist nicht abzählbar, d.h. es gibt keine Bijektion

$$\mathbb{F}_2^{\mathbb{N}} \longrightarrow \mathbb{N}$$

denn wäre $\mathbb{F}_2^{\mathbb{N}} = \left\{ f^{(i)} \middle| i \in \mathbb{N} \right\}$, so setze $g \in \mathbb{F}_2^{\mathbb{N}}$ mit $g = f_i^{(i)} + 1 \in \mathbb{F}_2$, dann ist $g \neq f^{(i)}$ für alle $i \in \mathbb{N}$, also $V \ncong V^\star$.

$B = (v_1, \ldots, v_n)$ Basisfolge, $B^\star = (v_1^\star, \ldots, v_n^\star)$ dazu duale Basis, $\lambda \in V^\star$, $\lambda = \sum_{i=1}^n a_i v_i^\star$ und $v = \sum_{i=1}^n x_i v_i$. Dann ist $\lambda(v) = \sum_{i=1}^n a_i x_i$ und $Kern\,\lambda = \{\, v = \sum_{i=1}^n x_i v_i \,|\, a_1 x_1 + \ldots + a_n x_n = 0\}$

Duale Aufgabentypen:

1. Gegeben ist homogenes lineares Gleichungssystem mit

$$\begin{array}{cccc} a_{11}x_1 & +\ldots+ & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & +\ldots+ & a_{mn}x_n & = & 0 \end{array}$$

   Suche Lösungsraum, d.h. gegeben $\lambda_1, \ldots, \lambda_m$, suche $Kern\,\lambda_1 \cap \ldots \cap Kern\,\lambda_m$.

2. Gegeben ist Teilraum U, gesucht homogenes lineares Gleichungssystem, das gerade U als Lösungsmenge hat ("Stelle U durch LGS dar"), d.h. suche $\lambda_n, \ldots, \lambda_m \in V^\star$ mit

$$\{\, v \in V \,|\, \lambda_i(v) = 0 \,\text{mit}\; 1 \leq i \leq m\} = U = \langle \lambda_n, \ldots, \lambda_m \rangle =: U^\circ$$

Definition 2 (Annihilator) Ist $U \leq V$ so heißt $U^\circ = \{\lambda \in V^\star \,|\lambda(u) = 0\, \forall u \in U\,\}$ *Annihilator* von U.

Lemma 1 Ist $U \leq V$ so gilt:

1. $U^\circ \leq V^\star$
2. $U_1 \leq U_2 \Rightarrow U_2^\circ \leq U_1^\circ$
3. $(U_1 + U_2)^\circ = U_1^\circ \cap U_2^\circ$
4. $(U_1 \cap U_2)^\circ \supseteq U_1^\circ + U_2^\circ$

Beweis:

1. klar
2. klar
3. $U_1, U_2 \subseteq U_1 + U_2$, also nach (2) $(U_1+U_2)^\circ \subseteq U_1^\circ, U_2^\circ \subseteq U_1^\circ \cap U_2^\circ$. Umgekehrt sei $\lambda \in U_1^\circ \cap U_2^\circ$, dann gilt für $u_i \in U_i$: $\lambda(u_1 + u_2) = \lambda(u_1) + \lambda(u_2) = 0 + 0 = 0$, also $\lambda \in (U_1 + U_2)^\circ$
4. $U_1 \cap U_2 \subseteq U_1, U_2$, $U_1^\circ, U_2^\circ \subseteq (U_1 \cap U_2)^\circ$ Teilraum, also $U_1^\circ + U_2^\circ \subseteq (U_1 \cap U_2)^\circ$. □

Satz 1 Ist $dim V = n < \infty$ und $U, U_1, U_2 \leq V$, so gilt:

1. $dim U + dim U^\circ = dim V = n$
2. $(U_1 \cap U_2)^\circ = U_1^\circ + U_2^\circ$

Beweis:

1. $(v_1, \ldots, v_d)$ sei Basisfolge von U, $B = (v_1, \ldots, v_d, \ldots, v_n)$ von V und $B^\star = (v_1^\star, \ldots, v_n^\star)$ duale Basis von $V^\star$. Es gilt:

$$\lambda = \sum_{i=1}^{n} a_i v_i^\star \in U^\circ \Leftrightarrow a_i = \lambda(v_i) = 0\,(i = 1, \ldots, d) \Leftrightarrow \lambda \in \left\langle v_{d+1}^\star, \ldots, v_n^\star \right\rangle$$

   Also: $U^0 = \left\langle v_{d+1}^\star, \ldots, v_n^\star \right\rangle \Rightarrow dim U^\circ = n - dim U$.

2. Es gilt (vgl. hierzu Kapitel 2: $dim U_1 + dim U_2 = dim(U_1 \cap U_2) + dim(U_1 + U_2)$):

$$\begin{aligned} dim(U_1 \cap U_2)^\circ &= n - dim(U_1 \cap U_2) \\ &= n - (dim U_1 + dim U_2 - dim(U_1 + U_2)) \\ &= n - dim U_1 + n - dim U_2 - (n - dim(U_1 + U_2)) \\ &= dim U_1^\circ + dim U_2^\circ - dim(U_1 + U_2)^\circ \quad (\star) \\ &= dim(U_1^\circ + U_2^\circ) \end{aligned}$$

$(\star)$: Aus Lemma 1 (3) folgt $(U_1 + U_2)^\circ = U_1^\circ \cap U_2^\circ$. Aus Lemma 1 (4) folgt umgekehrt $U_1^\circ + U_2^\circ = (U_1 \cap U_2)^\circ$. □

Satz 2 Ist V ein K-Vektorraum, so ist

$$\alpha : \begin{array}{ccc} V & \longrightarrow & V^{\star} = (V^{\star})^{\star} \\ v & \longmapsto & \alpha_v(\lambda) = \lambda(v) \in K \end{array} \quad \text{mit } \lambda \in V^{\star}$$

eine injektive lineare Abbildung, sogar ein Isomorphismus, falls $dim V = n < \infty$. Weiterhin heißt $V^{\star\star}$ Bidualraum, α_v Auswertung an V; α ist “natürlich”, d.h. unabhängig von jeder Basiswahl.

Beweis:

- für $v \in V$ ist α_v linear, d.h. in $(V^{\star})^{\star}$.
- $\alpha : v \longmapsto \alpha_v$ ist linear.
- α ist injektiv:

$$\begin{aligned} Kern\,\alpha &= \{v \in V \,|\, \alpha_v = \underline{0}\} = \{v \in V \,|\, \alpha_v(\lambda) = \underline{0}\ \forall \lambda \in V^{\star}\} \\ &= \{v \in V \,|\, \langle v \rangle^\circ = V^{\star}\} = \{v \in V \,|\, dim\,\langle v \rangle = 0\} = \{0\} \end{aligned}$$

da $dim V < \infty$ ist $dim V = dim V^{\star\star}$, also folgt aus α injektiv auch α surjektiv. □

Satz 3 (Dualitätssatz) Ist $dim V = n < \infty$, so ist

$$\Delta : \begin{array}{ccc} \{U \,|\, U \le V\} & \longrightarrow & \{L \,|\, L \in V^{\star}\} \\ U & \longmapsto & U^\circ \end{array}$$

eine bijektive Abbildung mit

1. $dim U^\circ = n - dim U$
2. $U_1 \le U_2 \Rightarrow U_2^\circ \le U_1^\circ$
3. $(U_1 + U_2)^\circ = U_1^\circ \cap U_2^\circ$ und $(U_1 \cap U_2)^\circ = U_1^\circ + U_2^\circ$

Beweis: Δ surjektiv. Sei $L \le V^{\star}$ gesucht, $U \le V$ mit $L = U^\circ$.

$$L^\circ = \{\alpha_v \in V^{\star\star} \,|\, \lambda(v) = \alpha_v(\lambda) = 0 \forall \lambda \in L\} = \left\{ \alpha_v \,\middle|\, v \in \bigcap_{\lambda \in L} Kern\,\lambda\,(=: U) \right\} = \alpha(U)$$

Behauptung: $L = U^\circ$. Beachte, daß $dim L = n - dim L^\circ = n - dim\,\alpha(U) = n - dim U_2 = dim U^\circ$ (α ist Isomorphismus). $L \le U^\circ$ da $U = \bigcap_{\lambda \in L} Kern\,\lambda$ also $L = U^\circ$. Da Δ injektiv: $U_1, U_2 \le V$, $U_1^\circ = U_2^\circ \Rightarrow \alpha(U_1) = U_1^{\circ\circ} = U_2^{\circ\circ} = \alpha(U_2) \Rightarrow U_1 = U_2$, weil α Isomorphismus. □

Folgerung 1 Ist $U \leq V$ und $U^\circ = \langle \lambda_1, ..., \lambda_r \rangle$, so ist $U = \bigcap_{i=1}^n Kern\, \lambda_i$. Ist $|K| = q < \infty$, $dim V = n < \infty$, V K-Vektorraum, so gilt:

$$|\{U \leq V \,|dim U = i\}| = |\{U \leq V \,|dim U = n - i\}|$$

Beispiel:

$V = \mathbb{F}_2^{101}$, $U \leq V$, $dim U = 99$. Es gilt:

$$|\{W \leq V \,|U \leq W\}| = \left|\left\{W^\circ \leq V^\star \,\middle|U^0 \geq W^\circ\right\}\right| = 5, \text{ also } dim U^\circ = 101 - 99 = 2$$

6.2 Bilinearformen

Definition 1 (Bilinearform) Eine Abbildung $\Phi : V \times V \longrightarrow K$ heißt *Bilinearform*, wenn

1. $\Phi(sv_1 + v_2, w) = s\Phi(v_1, w) + \Phi(v_2, w)$
2. $\Phi(v, sw_1 + w_2) = s\Phi(v, w_1) + \Phi(v, w_2)$

Φ heißt symmetrisch, wenn $\Phi(v, w) = \Phi(w, v)$ für alle $v, w \in V$ ist. Ist $B = (v_1, ..., v_n)$ Basisfolge von V so heißt $\Phi_B = [\Phi]_B = [\Phi(v_i, v_j)]$ (Gram-)Matrix von Φ bezüglich B.

Beispiel:

- $V = K^{n\times 1}$, $B = (e_1, ..., e_n)$

  $$\Phi_1\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}\right) = \sum_{i=1}^n x_i y_i \qquad \Phi_{1B} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$$

  $$\Phi_2\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}\right) = \sum_{i=1}^{n-1} x_i y_i - x_n y_n \qquad \Phi_{2B} = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -1 \end{bmatrix}$$

- $V = \mathbb{P}_n(\mathbb{R}) = \{\text{Polynomfunktionen vom Grad } \leq n,\ \mathbb{R} \longrightarrow \mathbb{R}\}$
  $B = (p_0, ..., p_n)$, $p_i = (x) = x^i$ $(x \in \mathbb{R})$
  $\Phi(f, g) = \int_0^1 f(x)g(x)\,dx$ und $\Phi(p_i, p_j) = \int_0^1 x^{i+j}\,dx = \frac{1}{i+j+1}$

  $$\Phi_B = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots \\ \frac{1}{2} & \frac{1}{3} & \ddots & \ddots \\ \frac{1}{3} & \ddots & \ddots & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{bmatrix}$$

Lemma 1

1. Ist $B = (v_1, ..., v_n)$ Basisfolge von V und $\Phi_B = [a_{ij}]$, Φ Bilinearform, dann (wobei K mit $K^{1\times 1}$ identifiziert wird):
   $$\Phi(v, w) = {}_B(v)^T \cdot [a_{ij}] \cdot {}_B(w)$$
2. Umgekehrt gibt es zu jeder Matrix $A = [a_{ij}]$ genau eine Bilinearform Φ mit
   $$\Phi_B = [\Phi_B] = A$$

3. Ist auch $B' = (v'_1, ..., v'_n)$ Basisfolge von V, so ist
$$\Phi_{B'} = P^T \cdot \Phi_B \cdot P$$
mit der Basiswechselmatrix $P = {}_B[id]_{B'}$, und wenn $P = [p_{ij}]$ ist, ist $v'_j = \sum_{i=1}^n p_{ij} v_i$.

Beweis:

1. bereits erledigt.
2. Zu $[a_{ij}] \in K^{n\times n}$, $B = (v_1, ..., v_n)$ definiere $\Phi(v,w) := {}_B v^T \cdot [a_{ij}] = [w]$, dann ist Φ Bilinearform.
3. $\Phi(v'_i, v'_j) = \sum_{k=1}^n \sum_{l=1}^n p_{ki} p_{lj} \Phi(v_k, v_l) = \sum_{k=1}^n p_{ki} \sum_{l=1}^n a_{kl} p_{lj}$ mit $a_{kl} := \Phi(v_k, v_l)$. Ist $A = [a_{kl}] = \Phi_B$, dann gilt: $\Phi(v'_i, v'_j) = ... = \left[P^T AP\right]_{ij}$ mit $[AP]_{kj} := \sum_{l=1}^n a_{kl} p_{lj}$. □

Definition 2 (Kongruenz) $A, A' \in K^{n\times n}$ heißt *kongruent*, wenn es $P \in GL(n,K)$ gibt mit
$$A' = P^T \cdot A \cdot P$$
(zum Vergleich: A, A' sind genau dann *ähnlich*, wenn $A' = P^{-1}AP$)

Bemerkungen:

- Kongruenz ist eine Äquivalenzrelation
- $A, A' \in K^{n\times n}$ kongruent $\Rightarrow det\,A' = (det\,P)^2 det\,A$
- A, A' kongruent, A symmetrisch. Dann ist auch A' symmetrisch, d.h. $A'^T = A'$
denn beachte $(A_1 \cdot A_2)^T = A_2^T \cdot A_1^T$, $A' = P^T AP \Rightarrow A'^T = (P^T AP)^T = P^T A^T P^{TT} = P^T A^T P = A'$ falls $A^T = A$

Beispiel:

- $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A' = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \in \mathbb{R}^{2\times 2}$ sind kongruent (mit $P = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$; A, A' sind aber nicht ähnlich)
- $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, $A' = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ sind ähnlich, aber nicht kongruent.

Bemerkung: $Bifo(V) = \{\Phi : V \times V \longrightarrow K \,|\, \Phi \text{ Bilinearform}\}$ ist K-Vektorraum. Ist $\Phi \in Bifo(V)$, so ist für jedes $w \in V$ die Abbildung $\Phi_w : v \longrightarrow \Phi(v,w)$ linear, d.h. $\Phi_w \in V^\star$ und die Abbildung $V \longrightarrow V^\star, w \longmapsto \Phi_w$ ist linear.

Lemma 2 Die Abbildung
$$\Lambda : \begin{array}{ccc} Bifo(V) & \longrightarrow & Hom(V, V^\star) \\ \Phi & \longmapsto & (\varphi : w \longrightarrow \Phi_w) \end{array}$$
ist ein Isomorphismus. Ist $B = (v_1, ..., v_n)$ Basisfolge von V so ist ${}_{B^\star}[\varphi]_B = \Phi_B$ wobei $B^\star$ die zu B duale Basis von $V^\star$ ist und $\varphi = \Lambda(\Phi)$.

Beweis: ${}_{B^\star}[\varphi]_B = [a_{ij}] \in K^{n\times n}$ bedeutet $\varphi(v_j) = \sum_{i=1}^n a_{ij} v_i^\star$, d.h. $\varphi(v_j)(v_i) = a_{ij}$ und $\Phi(v_i, w_j) = \Phi_{w_j}(v_i)$ also $[a_{ij}] = \Phi_B$. □

Definition 3 (Radikal, Ausartung) Ist $\Phi : V \times V \longrightarrow K$ Bilinearform, so heißt $Rad\,\Phi = \{w \in V \,|\Phi(v,w) = 0\,\text{für alle } v \in V\}$ *Radikal*. Φ heißt *nicht ausgeartet*, wenn $Rad\,\Phi = \{o\}$.

Lemma 3 Ist $B = (v_1, \ldots, v_n)$ Basis von V, so ist $\Phi \in Bifo(V)$ nicht ausgeartet genau dann, wenn $Rg\,\Phi_B = n$.

Beweis:

$$\begin{aligned} \Phi\,\text{ist nicht ausgeartet} \quad &\Leftrightarrow \quad Rad\,\Phi = \{o\} \Leftrightarrow \Phi_w = 0\,\text{nur fuer}\, w = o \\ &\Leftrightarrow \quad \varphi : w \longmapsto \Phi_w\,\text{ist injektiv} \\ &\Leftrightarrow \quad Rg_{B^\star}\,\varphi_{B'} = n = Rg\,\Phi_B\,\text{nach Lemma 2} \end{aligned}$$

□

6.3 Orthogonalität

Φ sei symmetrische Bilinearform auf V.

Definition 1 (Orthogonalität, Isotrop) $v, w \in V$ heißen *orthogonal* (bzgl. Φ), wenn $\Phi(v,w) = 0$ (i.Z. $v \perp w$). Ist $M \leq V$, so sei $M^\perp = \{v \in V \,|v \perp x\,\text{fuer alle } x \in M\}$. $v \in V$ heißt *isotrop*, wenn $v \perp v$.

Beispiel:

- $V = \mathbb{R}^n$, $\Phi\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}\right) = \sum_{i=1}^n x_i y_i$

  $v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \Rightarrow x_1 = \ldots = x_n = 0$, $v = o$ einziges Isotrop

- $V = \mathbb{R}^n$, $\Phi\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}\right) = \sum\limits_{i=1}^{n-1} x_i y_i - x_n y_n$

  $v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \Rightarrow v \perp v \Leftrightarrow x_n^2 = \sum\limits_{i=1}^{n-1} x_i^2$

  Beachte: Φ ist nicht ausgeartet, denn $Rg\,\Phi_B = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -1 \end{bmatrix} = n$

Satz 1 Sei Φ symmetrische Bilinearform auf V und $U \leq V$ Teilraum, dann ist $U^\perp$ auch ein Teilraum und es gilt (falls $dim V = n < \infty$):

1. $dim\,U + dim\,U^\perp = dim\,V + dim(U \cap Rad(\Phi))$
2. Ist Φ nicht ausgeartet, so ist $dim\,U + dim\,U^\perp = dim\,V$

Beweis: Sei $\Lambda' = U \longrightarrow V^\star$, $u \longmapsto \Phi_u$ mit $\Phi_u(v) = \Phi(v,u)$. Nach dem Dimensionssatz gilt dann $dim\,Bild\,\Lambda' + dim\,Kern\,\Lambda' = dim\,U$. Es gilt weiterhin:

1. $Kern\,\Lambda' = \{u \in U \,|\Phi_u = 0\} = \{u \in U \,|\Phi(v,u) = 0 \forall v \in V\} = U \cap Rad\,\Phi$
2. $Bild\,\Lambda' = \{\Phi_u \,|u \in U\} = (U^\perp)^\circ,\ \Phi_u(u') = \Phi(u',u)$.

Benutze $dim\,(U^\perp)^\circ = n - dim U^\perp$, daraus folgt die Behauptung. □

Folgerung 1 Gibt es in V keine isotropen Vektoren (d.h. $v \in V$ mit $v \perp v$) außer $v = \mathfrak{o}$ so ist:

$$U \oplus U^\perp = V \quad \text{falls } dim V < \infty$$

Beweis: $v \in U \cap U^\perp \Rightarrow v \perp v$ also $v = \mathfrak{o}$ nach Voraussetzung. Weiterhin $U \cap U^\perp = \{\mathfrak{o}\}$. Es gilt:

$$dim U + dim U^\perp = dim(U + U^\perp) + dim(U \cap U^\perp) = dim V$$

(da $dim\,(U \cap U^\perp) = 0$), also $U + U^\perp = V$. □

Beispiel:

$V = \mathbb{R}^3, B = (e_1, e_2, e_3), \Phi_B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$, d.h.

$$\Phi\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \right) = x_1y_1 + x_2y_2 - x_3y_3$$

Sei $v_1 := e_2 + e_3, U = \langle v_1 \rangle$. $\Phi(e_1 + e_3, e_2 + e_3) = 0$.

$$U^\perp = \langle v_1, e_1 \rangle, dim U^\perp = 3 - dim U = 2, U \subseteq U^\perp$$

Definition 2 (Orthogonalbasis) $B = (v'_1, \dots, v'_n)$ heißt *Orthogonalbasis* (bzgl. Φ) wenn $v'_1 \perp v'_j$ für $i \neq j$, d.h. $\Phi_{B'}$ ist Diagonalmatrix. Für Matrizen gilt: $\Phi_B = A$, dann ist $\Phi_{B'} = P^T AP$ mit $P = {}_B[id]_{B'} \in GL(n,K)$.

Frage: Gegeben $A \in K^{n \times n}$. Gibt es $P \in GL(n,K)$ mit $P^T AP = diag(t_1, \dots, t_n)$, $t_i \in K$?
Offensichtlich gilt dies nicht, wenn $A \neq A^T$ gilt, also ist die Frage nur sinnvoll bei symmetrischen Matrizen.

Beispiel:

Sei K Körper mit $char\,K = 2$[1], z.B. $\mathbb{F}_2$, $dim V = 2$, Basis $B = (v_1, v_2)$. Sei $\Phi_B = A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $v_1 \perp v_1$ und $v_2 \perp v_2$. Es gilt:

$v \in V \Leftrightarrow v = x_1v_1 + x_2v_2 \in V$ mit $x_i \in K$.
$\Phi(v,v) = x_1x_2\Phi(v_1,v_2) + x_1x_2\Phi(v_2,v_1) = x_1x_2(1+1) = 0$ also $v \perp v$.

Gäbe es eine Basis $B'(v'_1, v'_2)$ mit $\Phi_{B'} = \begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix}$ so wäre $t_i = \Phi(v'_i, v'_i) = 0$, also $\Phi_{B'} = 0$ und somit $\Phi(v,w) = 0$ für alle $v, w \in V$, was ein Widerspruch ist, denn wir wissen $\Phi(v_1, v_2) = 1$.

Satz 2 Ist $char\,K \neq 2$ und ist $\Phi : V \times V \longrightarrow K$ eine symmetrische Bilinearform, $dim V = n < \infty$, so existiert zu Φ eine Orthogonalbasis $B = (v_1, \dots, v_n)$ d.h. $\Phi_B = (t_1, \dots, t_n)$, $t_i \in K$.

Beweis: Induktion nach $n = dim V$: Der Induktionsanfang $n = 1$ ist trivial. Für $n > 1$ erhält man:

[1] $char\,K = n \Leftrightarrow 1 + \dots + 1 = 0$ (n Einsen) und es gibt kein $n' < n$ mit dieser Eigenschaft.

- 1. Fall: Angenommen, alle $v \in V$ seien isotrop, d.h. $\Phi(v,v) = 0 \; \forall v \in V$. Seien $v,w \in V$ beliebig. Es gilt:
$$0 = \Phi(v+w, v+w) = \Phi(v,v) + \Phi(w,v) + \Phi(v,w) + \Phi(w,w) = (1+1)\Phi(v,w) \neq 0$$
also muß $\Phi(v,w) = 0$ sein für alle $v,w \in V$, und Φ ist die Nullabbildung, jede Basis ist Orthogonalbasis.

- 2. Fall: Es gibt $v_1 \in V$ mit $\Phi(v_1,v_1) \neq 0$. Sei $U = \langle v_1 \rangle$. Nach Satz 1 (Seite 73) folgt dann $U \cap U^\perp = \{0\}$ also $0 \cdot v_1 \in U \cap U^\perp = \{0\}$ und somit $c \cdot \Phi(v_1,v_1) = 0 \Rightarrow c = 0$. Also $V = U \oplus U^\perp$mit $dim U^\perp = n-1$. Setze $\Phi' = \Phi\big|_{U^\perp \times U^\perp} : U^\perp \times U^\perp \longrightarrow K$ symmetrische Bilinearform. Nach Induktionsannahme gibt es eine Orthogonalbasis $B' = (v_2, ..., v_n)$ von $U^\perp$ bzgl. Φ mit $\Phi(v_i,v_j) = 0$, $i \neq j$, $i,j \geq 2$. Dann gilt jedoch $B = (v_1, v_2, ..., v_n) \Rightarrow \Phi(v_i,v_j) = 0 \; \forall i,j \geq 1$. $\square$

6.4 Orthogonalisierung

Sei $\Phi : V \times V \longrightarrow K$ eine symmetrische Bilinearform, $dim V = n < \infty$.

Frage: Wie findet man eine Orthogonalbasis zu Φ (falls es eine gibt), bzw.: wie findet man zu $A \in K^{n \times n}$ mit $A^T = A$ ein $P \in GL(n,K)$ mit $P^T A P = diag(t_1, ..., t_n)$, $t_i \in K$?

1. Verfahren: Elementare Operationen

Gibt es $P \in GL(n,K)$ mit $P^T A P = diag(t_1,...,t_n)$ so muß (Kapitel 3.9, Seite 41) $P = P_1 \cdot ... \cdot P_r$ sein, wobei P_i Elementarmatrizen sind, und entsprechend $P^T = P_r^T \cdot ... \cdot P_1^T$. Dann gilt: $P^T A P = P_r^T ... P_2^T (P_1^T A P_1) P_2 ... P_r$.

Elementare Matrizenoperationen sind:

1. $P_1 = D_i(t) = \begin{bmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & t & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \dots & \dots & 0 & \ddots \end{bmatrix}$ ($t \neq 0$ in Spalte i, Zeile i)

   $A \to AP_1$ bedeutet: Multiplikation der i-ten Spalte von A mit t. $A \to P_1^T A P_1$ bedeutet: "Multipliziere i-te Spalte von A mit t und danach i-te Zeile mit t

2. $P_1 = P_{ij} = \begin{bmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 0 & 1 & & \vdots \\ \vdots & & 1 & 0 & 0 & \vdots \\ \vdots & & & 0 & 1 & 0 \\ 0 & \dots & \dots & \dots & 0 & \ddots \end{bmatrix}$ (i-te und j-te Spalte vertauscht)

   $A \to AP_1$ bedeutet: Vertauschung der i-ten mit der j-ten Spalte. $A \to P_1^T A P_1$ bedeutet: "Vertausche i-te und j-te Spalte von A und danach i-te und j-te Zeile von AP_1.

3. $P_1 = U_{ij}(t) = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & t & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{bmatrix}$ (t in der i-ten Zeile und j-ten Spalte)

   $A \to AP_1$ bedeutet Addiere t-faches der i-ten Spalte zur j-ten Spalte. $A \to P_1^T A P_1$ bedeutet: "Addiere

t-faches der i-ten Spalte zur j-ten von A und danach t-faches der i-ten Zeile von AP_1 zur j-ten Spalte von AP_1.

Verfahren: Man bringe A durch gekoppelte elementare Spalten- und Zeilenoperationen auf Diagonalgestalt. Dabei erhält man $P = E_n P_1 P_2 ... P_r$ indem man nur elementare Spaltenoperationen auf E_n anwendet.

Beispiel:

$$\begin{array}{cccc}
A_i & \rightarrow A_iP_i \rightarrow P_i^T A_i P_i = A_{i+1} & & \\
\begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 4 \\ 2 & 4 & 4 \end{bmatrix} & \rightarrow \begin{bmatrix} 1 & 0 & 2 \\ 1 & 1 & 4 \\ 2 & 2 & 4 \end{bmatrix} \rightarrow & \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 2 & 4 \end{bmatrix} & P_1 = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
& \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 2 & 2 & 0 \end{bmatrix} \rightarrow & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} & P_1P_2 = \begin{bmatrix} 1 & -1 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\
& \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & -4 \end{bmatrix} \rightarrow & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -4 \end{bmatrix} & P_1P_2P_3 = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \\
& \rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{bmatrix} \rightarrow & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} & P = P_1P_2P_3P_4 = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & \frac{1}{2} \end{bmatrix}
\end{array}$$

Anwendung:

$A = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 2 & 4 \\ 2 & 4 & 4 \end{bmatrix} = \Phi_B$, $B = (e_1, e_2, e_3)$ Basis von $V = \mathbb{R}^3$.

$Q = \{v = \sum x_i e_i \,|\Phi(v,v) = 1\} = \left\{v = \sum_{i=1}^{3} x_i e_i \,\middle|x_1^2 + 2x_2^2 + 4x_3^2 + 2x_1x_2 + 4x_1x_3 + 8x_2x_3 = 1\right\}$

$\Phi_{B'} = diag(1,1,-1) = P^TAP$, $B' = (v_1, v_2, v_3)$ mit $v_1 = e_1, v_2 = e_2 - e_1, v_3 = -e_2 + \frac{1}{2}e_3$, $Q = \left\{v = \sum_{i=1}^{3} y_i v_i \,|\Phi(v,v) = 1\right\} =$ $\left\{v = \sum y_i v_i \,\middle|y_1^2 + y_2^2 - y_3^2 = 1\right\}$

Also beschreibt Φ einen Hyberboloiden

Definition 1 (quadratische Form) Ist $\Phi : V \times V \longrightarrow K$ Bilinearform, so heißt die Abbildung $V \longrightarrow K, v \longmapsto \Phi(v,v)$ die zu Φ gehörige *quadratische Form*.

2. Verfahren: Gram-Schmidtsches Orthogonalisierungsverfahren

Satz 1 (Gram-Schmidtsches Orthogonalisierungsverfahren) $\Phi : V \times V \longrightarrow K$ sei symmetrische Bilinearform ohne isotrope Vektoren außer 0 (d.h. $\Phi(v,v) = 0 \Rightarrow v = 0$). $B = (v_1, ..., v_n)$ sei Basisfolge von V. Dann erhält man eine Orthogonalbasis $B' = (v'_1, ..., v'_n)$ von V wie folgt:
Setze $v'_1 := v_1$, und definiere danach rekursiv

$$v'_k = v_k - \sum_{j=1}^{k-1} \frac{\Phi(v'_j, v_k)}{\Phi(v'_j, v'_j)} v'_j$$

Dabei ist $\langle v_1, ..., v_k \rangle = \langle v'_1, ..., v'_k \rangle$. Ist $B'' = (v''_1, ..., v''_n)$ auch Orthogonalbasis von V mit $\langle v_1, ..., v_k \rangle = \langle v''_1, ..., v''_k \rangle$ für $k \leq n$, so ist $v''_j = c_j v'_j$ mit $c_j \in K^{\neq 0}$.

Beweis: zu zeigen $\Phi(v'_k, v'_i) = 0$ für $1 \leq i < k \leq n$ und $\langle v_1, ..., v_k \rangle = \langle v'_1, ..., v'_k \rangle$. Induktion nach k:

1. $k = 1$: trivial.

2. $k > 1$:
$$\Phi(v'_k, v'_i) = \Phi(v_k, v'_i) = \sum_{j=1}^{k-1} \frac{\Phi(v'_j, v_k)}{\Phi(v'_j, v'_j)} \Phi(v'_j, v'_j)$$
Da $\Phi(v'_i, v'_j) = 0$ für $i = j$ nach Induktionsannahme gilt weiterhin:
$$... = \Phi(v_k, v'_i) - \Phi(v'_i, v_k) = 0$$
und somit $\langle v'_1, ..., v'_k \rangle = \langle v'_1, ..., v'_{k-1} \rangle + \langle v_k \rangle = \langle v_1, ..., v_{k-1} \rangle + \langle v_k \rangle = \langle v_1, ..., v_k \rangle$.

Eindeutigkeit: $\Phi(v''_i, v''_j) = 0$ für $i \neq j$. $\langle v_1, ..., v_k \rangle = \langle v''_1, ..., v''_k \rangle$; Sei $U = \langle v_1, ..., v_k \rangle \cap \langle v_1, ..., v_{k-1} \rangle^{\perp}$, $v'_k, v''_k \in U$, $dim(U) = 1$, also $v''_k = v'_k \cdot c_k$ mit $c_k \neq 0$. □

Bemerkung: Ist $\Phi : V \times V \longrightarrow K$ symmetrische Bilinearform, $dim V$ beliebig und sind v_i ($i \in I$, I Indexmenge mit $I \subseteq \{1, ..., dim V\}$), in V vorgegeben mit $\Phi(v_i, v_j) = \delta_{ij} c_i$ mit $c_i \in K \neq 0$. Dann:

1. $(v_i)_{i \in I}$ ist linear unabhängig.
2. Ist $v \in \langle v_i | i \in I \rangle$, dann ist $\Phi(v, v_i) \neq 0$ nur für endlich viele i und
$$v = \sum_{i \in I} \frac{\Phi(v, v_i)}{\Phi(v_i, v_i)} v_i$$
v heißt Fourierkoeffizient von v bezüglich v_i.

Beweis:

1. Ist $0 = \sum_{i \in I} s_i v_i$, $s_i \neq 0$ nur für endlich viele $i \in I$.
$$0 = \Phi(v_j, 0) = \sum_{i \in I} s_i \cdot \Phi(v_j, v_i) = s_j \cdot \Phi(v_j, v_j)$$
mit $\Phi(v_i, v_j) = 0$ für $i \neq j$ und $\Phi(v_j, v_j) = c_j \neq 0$, also $s_j = 0$ für alle j.
2. $v = \sum_{i \in I} s_i v_i$ mit $s_i \neq 0$ nur für endlich viele i.
$$\Phi(v, v_j) = \sum_{i \in I} s_i \cdot \Phi(v_i, v_j) = s_j \cdot \Phi(v_j, v_j)$$
mit $\Phi(v_i, v_j) = 0$ für $i \neq j$ und $\Phi(v_j, v_j) = c_j \neq 0$ □

Beispiel:

$V = \{ f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f \text{ stetig}, \ f(x) = f(x + 2\pi) \, \forall x \in \mathbb{R} \}$, $f_{2n}(x) = cos(nx)$, $f_{2n-1}(x) = sin(nx)$, $n \in \mathbb{N}_0$.
$$\Phi(f, g) = \int_{-\pi}^{\pi} f(x) g(x) \, dx$$
$(f, g \in V)$. Dann ist $\Phi(f_i, f_j) = \delta_{ij} c_i$ mit $0 \neq c_i \in \mathbb{R}$,
$$c_0 = \int_{-\pi}^{\pi} 1 \, dx = 2\pi \, \text{und} \, c_{2n} = \int_{-\pi}^{\pi} cos^2(x) \, dx = \pi = c_{2n-1}$$
$f \in \langle f_n \rangle_{n \in \mathbb{N}_0} \Rightarrow f = \sum_{i \in \mathbb{N}_0} a_i f_i$ mit $a_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x) \, dx$, $a_{2n} = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) cos(nx) \, dx$, $a_{2n-1} = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) sin(nx) \, dx$.

6.5 Euklidische Vektorräume

Definition 1 (positive Definitheit, Skalarprodukt, eukl. Vektorraum) Ist V ein $\mathbb{R}$-Vektorraum und $\Phi : V \times V \longrightarrow K = \mathbb{R}$ symmetrische Bilinearform, so heißt Φ *positiv definit*, wenn

$$\Phi(v,v) > 0 \,\forall v \in V \setminus \{0\}$$

Φ heißt *Skalarprodukt* genau dann, wenn Φ eine positiv definite symmetrische Bilinearform . Ein *euklidischer Vektorraum* ist ein $\mathbb{R}$-Vektorraum zusammen mit einem Skalarprodukt.

Beispiel:

- $(\mathbb{R}^{n\times 1}, \Phi)$ mit $\Phi(x,y) = x^T y = \sum x_i y_i$ ist euklidischer Vektorraum.
- $V = \mathbb{P}(\mathbb{R}) = \{\text{Polynomfkt.}\, \mathbb{R} \longrightarrow \mathbb{R}\}$ oder $V = \{\, f : [-1;1] \longrightarrow \mathbb{R} \,|\, f \text{ stetig} \,\}$ mit $\Phi(f,g) = \int_{-1}^{1} f(x)g(x)\,dx$. Dann ist (V,Φ) euklidischer Raum.

Definition 2 (Norm) Ist (V,Φ) euklidischer Raum, so heißt für $v \in V$ $\|v\| = \sqrt{\Phi(v,v)} \in \mathbb{R}^{\geq 0}$ *Norm* von v.

Definition 3 (Euklidischer Abstand) Seien $v,w \in V$, V euklidischer Vektorraum, dann heißt $d(v,w) = \|v-w\|$ *euklidischer Abstand* von v,w.

Satz 1 (Cauchy-Schwarzsche Ungleichung) Ist (V,Φ) euklidischer Raum, so gilt:

$$\Phi(v,w)^2 \leq \|v\|^2 \cdot \|w\|^2,\ \ v,w \in V$$

mit Gleichheit genau dann, wenn v,w linear abhängig sind.

Beweis: Trivial für $w = 0$; also sei o.B.d.A. $w \neq 0$;
v,w linear abhängig genau dann, wenn $v = sw$ mit $s = \frac{\Phi(v,w)}{\|w\|^2} \Leftrightarrow \Phi(v-sw, v-sw) = 0$. Für beliebiges v und s ist $\Phi(v-sw, v-sw) = \|v\|^2 + s^2\|w\|^2 - 2s\Phi(v,w)$ $(\star)$. Setze in $(\star)$ $s = \frac{\Phi(v,w)}{\|w\|^2}$ ein.

$$\begin{aligned} 0 &\leq \|v\|^2 + \frac{\Phi(v,w)^2}{\|w\|^2} - 2\frac{\Phi(v,w)^2}{\|w\|^2} = \|v\|^2 - \frac{\Phi(v,w)^2}{\|w\|^2} \\ \Leftrightarrow \quad \|\Phi(v,w)\|^2 &\leq \|v\|^2 \|w\|^2 \end{aligned}$$

wobei Gleichheit genau dann gilt, wenn $0 = \Phi(v-sw, v-sw)$, d.h. wenn $v = sw$. $\square$

Folgerung 1 Ist (v,Φ) euklidischer Raum, so gilt:

1. $\|v\| \geq 0$ und $\|v\| = 0 \Leftrightarrow v = 0$
2. $\|sv\| = |s| \cdot \|v\|$ für $s \in \mathbb{R}$
3. Dreiecksungleichung: $\|v+w\| \leq \|v\| + \|w\|$ für alle $v,w \in V$

Beweis:

1. klar
2. klar
3. $\|v+w\|^2 = \Phi(v+w, v+w) = \|v\|^2 + \|w\|^2 + 2\Phi(v,w) \leq \|v\|^2 + \|w\|^2 + 2\|v\|\,\|w\| \leq (\|v\| + \|w\|)^2$ nach Satz 1 $\square$

Satz 2 Ist (V,Φ) ein euklidischer Raum. $U \leq V$, U sei endlich dimensional und $v \in V$. Dann gibt es genau einen Vektor $u_0 \in U$ mit
$$\|v-u_0\| = \min_{u\in U}\|v-u\|$$

Beweis: Sei $(u_1,\dots,u_n)$ Basisfolge von U. Ist $v \in U$, so setze $u_0 = v$. Sei also $v \notin U$, dann setze $W = \langle u_1,\dots,u_n,v\rangle$, $dim W = n+1$.

$$\begin{aligned} dim(U^\perp \cap W) &= dim W - dim U = 1 \\ U^\perp \cap W &= \langle v_0\rangle \end{aligned}$$

$(v_0,u_1,\dots,v_n)$ Basis von W, $W = U \oplus \langle v_0\rangle$ $(\langle v_0\rangle = U^\perp \cap W$, $v = \sum_{i=1}^n s_i u_i + s_o v_o \in W$, $s_i \in K = \mathbb{R}$.
Setze $u_0 = \sum_{i=1}^n s_i u_i$. Dann folgt für $u \in U$ beliebig:

$$\|v-u\|^2 = \|v-u_0+u_0-u\|^2 = \|v-u_0\|^2 + \|u_0-u\|^2 + 2\Phi(v-u_0,u_0-u) \geq 0$$

mit Gleichheit genau dann, wenn $\|u_0-u\| = 0$, d.h. wenn $u = u_0$. □

Definition 4 (Orthonormalsystem) Ist (V,Φ) euklidischer Vektorraum und $(v_i)_{i\in I}$ Orthogonalsystem, d.h.
$$\Phi(v_i,v_j) = \delta_{ij}c_i,\ 0 \neq c_i \in \mathbb{R}, \text{ also } c_i > 0$$
dann ist $(w_i)_{i\in I}$ mit $w_i := \frac{1}{\sqrt{e_i}}v_i = \frac{v_i}{\|v_i\|}$ ein *Orthonormalsystem*, d.h. $\Phi(w_i,w_j) = \delta_{ij}$.

Satz 3 Ist (V,Φ) euklidischer Raum und $(v_i)_{i\in\mathbb{N}}$ ein Orthonormalsystem und $U_n = \langle v_1,\dots,v_n\rangle$, $n = 1,2,\dots$. Dann gibt es zu jedem n (bei gegebenem $v \in V$) genau ein $u_n \in U_n$ mit

$$\|v-u_n\| = \min_{u\in U_n}\|v-u\|$$

Es ist $u_n = \sum_{i=1}^n \Phi(v,v_i)v_i$ und es gilt $\sum_{j=1}^\infty \left(\Phi(v,v_j)^2\right) \leq \|v\|$.

Beweis: siehe Satz 2. $W_n = U_n + \langle v\rangle = U_n \oplus (U_n^\perp \cap W_n)$, $v - \sum_{i=1}^n a_i v_i \in \langle w\rangle \in U_n^\perp$;
$v = u_n + cw$, $\Phi(v,v_j) = \Phi(u_n,v_j) + \Phi(cw,v_j) = a_j$

$$\begin{aligned} 0 &\leq \|v-u_n\|^2 = \Phi(v-u_n,v-u_n) \\ \Leftrightarrow 0 &\leq \|v\|^2 - 2\Phi(v,u_n) + \|u_n\|^2 \\ \Leftrightarrow 0 &\leq \|v\|^2 - 2\sum_{i=1}^n \Phi(v,v_i)\Phi(v,v_i) + \sum \Phi(v,v_i) \\ \Leftrightarrow 0 &\leq \|v\|^2 - \sum_{i=1}^n \Phi(v,v_i)^2 \\ \Leftrightarrow \sum_{i=1}^n \Phi(v,v_i)^2 &\leq \|v\|^2 \end{aligned}$$

□

Beispiele:

- $V = \{f : [-\pi,\pi] \longrightarrow \mathbb{R} \,|\, f \text{ stetig}\}$, $\Phi(f,g) = \int_{-\pi}^{\pi} f(x)g(x)\,dx$, (V,Φ) eukl. Raum.

$$\left.\begin{aligned} f_{2n}(x) &= \tfrac{1}{\sqrt{\pi}}cos(nx) \\ f_{2n-1}(x) &= \tfrac{1}{\sqrt{x}}sin(nx) \\ f_0(x) &= \tfrac{1}{\sqrt{2\pi}} \end{aligned}\right\} (f_i)_{i=0}^\infty \text{ Orthonormalsystem}$$

  $f \in V$, $a_i = \Phi(f,f_i) = \int_{-\pi}^{\pi} f_i(x)f(x)\,dx$ (Fourierkoeffizient). $\sum_{i=0}^n a_i f_i$ ist die beste Approximation von f in $U_n = \langle f_0,\dots,f_n\rangle$.
  Warnung: $\sum_{i=1}^\infty a_i f_i(x) = f(x)$ gilt nicht allgemein; $\sum_{i=0}^n a_i^2 \leq \int_{-\pi}^{\pi} f(x)^2\,dx$

- Gegeben seien $(x_0, y_0), \dots, (x_n, y_n)$ im $\mathbb{R}^2$, $x_0 < x_1 < \dots < x_n$, $U \leq P_n(\mathbb{R})$. Gesucht wird $g \in U$ mit $\Delta_g = \sum_{k=0}^n (y_k - g(x_k))^2$ minimal, $\Phi(f, g) := \sum_{k=0}^n f(x_k) g(x_k)$,

$$0 = \|f\|^2 = \Phi(f, f) = \sum_{k=0}^n f(x_k)^2 \Rightarrow f(x_0) = f(x_1) = \dots = f(x_n) = 0$$

Daraus folgt: f hat $n+1$ Nullstellen, *Grad* $f \leq n$, also $f = 0$. Es gibt ein $f_0 \in V$ mit $f_0(x_i) = y_i$ für $i = 0, \dots, n$ $(\star)$

$$f_0(x) = \sum_{i=0}^n a_i x^i$$

$(\star)$ kann man in Matrixform schreiben, vgl. von-der-Monde-Matrix (Seite 35). Diese Matrix ist invertierbar, weil $x_i \neq x_j$ für $i \neq j$. Dann ist $\Delta_g = \sum_{k=0}^n (f_0(x_k) - g(x_k))^2 = \|f_0 - g\|$,
Finde $g \in U_n$ mit $\|f_0 - g\| = \min_{u \in U} \|f_0 - u\|$, $U = \langle u_1, \dots, u_r \rangle$

  - 1. Möglichkeit: $(u_1, \dots, u_r)$ ist Basis von U. Orthonormalisiere (mit Gram-Schmidt) und erhalte ON-Basis $(w_1, \dots, w_r)$ von U. Dann ist $g = \sum_{i=1}^r \Phi(f_0, w_i) w_i$ mit $\sum_{k=0}^n y_k w_i(x_k)$ nach Satz 3.
    Berechnung: $U = \langle p_2 \rangle = \left\{ x \longmapsto cx^2 \,|\, x \in \mathbb{R} \right\}$
    $\|p_2\|^2 = \Phi(p_2, p_2) = \sum_{k=0}^n x_k^n$, $\quad w = \left(\sum_{k=0}^n x_k^n\right)^{-\frac{1}{2}} p_2$, $g = \Phi(f_0, w) w = \sum_{k=0}^n y_k w(x_k) w$,
    $g(x) = \sum_{k=0}^n y_k x_k^2 \cdot \left(\sum_{k=1}^n x_k^n\right)^{-\frac{1}{2}} \cdot \left(\sum_{k=0}^n x_k^n\right)^{-\frac{1}{2}} \cdot x^2$.

$$\frac{\sum y_k x_k^2}{\sum x_k^n} = c$$

  - 2. Möglichkeit: $g = \sum_{i=1}^r c_i u_i$ wobei die c_i bestimmt sind durch $\Phi(f_0 - \sum_{i=1}^r c_i u_i, u_j) = 0$ für $j = 1, 2, \dots, r$;

$$\sum_{k=0}^r \left(y_k - \sum_{i=1}^r c_i u_i(x_k) \right) \cdot u_j(x_k) = 0$$

    Berechnung: $U = \langle p_0, p_1 \rangle = \{ x \longmapsto c_0 + c_1 x \,|\, c_0, c_1 \in \mathbb{R} \}$
    $\sum_{k=0}^n \left(y_k - \sum_{i=0}^1 c_i p_i(x_k)\right) \cdot p_i(x_k) = 0$; $j = 0, 1$
    $\sum_{k=0}^n (y_k - (c_0 + c_1 x_k)) = 0$, $(n+1) c_0 + \sum_{k=0}^n x_k c_1 = \sum_{k=0}^k y_k$
    $\sum_{k=0}^n (y_k - (c_0 + c_1 x_k)) x_k = 0$, $\sum_{k=0}^n x_k c_0 + \sum_{k=0}^n x_k^2 c_1 = \sum_{k=0}^n y_k x_k$
    Gleichungssystem eindeutig lösbar (da $x_i \neq x_j$ für $i \neq j$).