

# Mathematik für Informatiker I

Andreas Griewank

(griewank@math.hu-berlin.de)

Vertretung :

Jürgen Geiser (geiser@mathematik.hu-berlin.de)

Wiss. Mitarbeiter:

Hans-Dietrich Niepage (niepage@mathematik.hu-berlin.de)

Holger Heitsch (heitsch@mathematik.hu-berlin.de)

Lutz Lehmann (llehmann@mathematik.hu-berlin.de)

Stefan Körkel (stefan.koerkel@mathematik.hu-berlin.de)

Institut für Angewandte Mathematik  
Humboldt Universität zu Berlin

28. Juni 2007

# Teil A

## Algebraische Grundstrukturen

Algebraische Grundlagen

Algebraische Teilstrukturen

Algebraische Erweiterungen

Äquivalenzrelationen und Quotientenstrukturen

Modulare Arithmetik

Strukturerhaltende Abbildungen

Teilbarkeit und partielle Ordnungen

## Literaturhinweise I



Donald E. Knuth,

Fundamental Algorithms. The art of computer programming. Vol I,II,III. Second Edition. Addison Wesley.

*Absoluter Klassiker sehr umfangreich und mathematisch. Bill Gates hat mal jedem einen Job versprochen, der 80 % der Übungen lösen kann.*



Peter Hartmann,

Mathematik für Informatiker. 3. überarbeitete Auflage, 2004, Vieweg.

Bei Lehmann's vorhanden, ca. 30€.

*Gute Grundlage, äusserst lesbar, nicht unbedingt an Eliteuniversitäten orientiert. ISBN: 3-528-23181-5*



Vélu Jacques,

1<sup>er</sup> CYCLE. Méthodes mathématiques pour l'informatique. Cours et exercices corrigés. 3<sup>er</sup> edition. Dunod, Paris, 1999.

## Literaturhinweise II



Guerino Mazzola, Gérard Milmeister, Jody Weissmann,  
Comprehensive Mathematics for Computer Scientists 1, 2004,  
Springer.

*Ziemlich axiomatisch und knapp geschrieben. Zweiter Band in Vorbereitung. Definitiv für höhere Ansprüche. Begleitender Kurs im Internet verfügbar. ca 30 €, ISBN: 3-540-20835-6*



Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest,  
Introduction to Algorithms. 2nd ed. 2001. The MIT Press.  
*ca 60 €, ISBN: 0-262-53196-8*



Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford  
Stein,  
Algorithmen – Eine Einführung. 2004, Oldenbourg.  
*ca 70 €, ISBN: 3-486-27515-1*

## Zitate

*It is generally very difficult to keep up with a field that is economically profitable.*

Donald E. Knuth

*Since, I myself profess to be a mathematician, it is my duty to maintain mathematical integrity as much as I can.*

Donald E. Knuth

## A-1 Algebraische Grundlagen

### Beispiel A-1.1

unsigned char in Programmiersprachen (C, C++, Java, etc.)

$$a \in \mathcal{B} \equiv \{0, 1, 2, 3, \dots, 254, 255\}$$

wobei  $255 = 2^8 - 1 = m - 1$  mit  $m \equiv 256$

### Fragen:

- ▶ Welche Eigenschaften haben Verknüpfungen  $+$  und  $*$  für sich allein und wie ist ihre Wechselwirkung?
- ▶ Wie klassifiziert man die Struktur von  $\mathcal{B}$  griffig?

## Definition A-1.2 (Verknüpfungseigenschaften)

Für Verknüpfungen  $\circ$  zwischen beliebigen Elementen  $a, b, c$  einer Menge  $\mathcal{M}$  und einem speziellen Element  $e$  betrachtet man die Eigenschaften:

- |   |                                   |
|---|-----------------------------------|
| (i) $(a \circ b) \circ c = a \circ (b \circ c)$ | <b>Assoziativität</b>             |
| (ii) $e \circ b = b \circ e = b$                | <b>Neutrales bzw. Einselement</b> |
| (iii) $a \circ b = b \circ a$                   | <b>Kommutativität</b>             |
| (iv) $a \circ b = e$                            | <b>Inverse Elemente</b>           |

## Definition A-1.3 (Halbgruppe, Monoid, Gruppe)

$\mathcal{M}$  heißt

*Halbgruppe* falls (i) gilt

*Monoid* falls zudem (ii) gilt

*Kommutativ* falls zudem (iii) gilt

*Gruppe* falls zudem für jedes  $a \in \mathcal{M}$   
ein Inverses  $b \in \mathcal{M}$  existiert, so daß (iv) gilt

## Beispiel A - 1.4 (Nichtkommutativer Monoid)

Alle Worte bzw Zeichenketten  $A^*$  über einem gegebenen Alphabet  $A$ , z.B.  $\{0, 1\}$  oder  $\{a, b, \dots, z\}$  wobei  $+$  Konkatenation und  $\epsilon$  das Leere Wort sind, d.h

$$axz + yi = axzyi.$$

## Beispiel A - 1.5 (Kommutativer Monoid)

$\mathbb{N}_+ = \{1, 2, 3, \dots\}$  Menge der positiven natürlichen Zahlen bzgl.  $*$  mit neutralem Element 1.

## Beispiel A - 1.6 (Kommutative Gruppe)

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$  Menge aller ganzen Zahlen bezüglich  $+$  mit neutralem Element  $e = 0$  und inversem Element  $-a$ .

### Warnung:

$\mathbb{Z}$  ist bezüglich  $*$  keine Gruppe, da im allgemein keine Reziproke (d.h. Kehrwerte) existieren, und ein solches für 0 auch nicht definiert werden kann. Allerdings ist  $\mathbb{Z}$  ein Ring.

## Definition A-1.7 (Ring)

Eine Menge  $\mathcal{M}$  heißt Ring falls für alle Elemente  $a, b, c \in \mathcal{M}$

- (i)  $\mathcal{M}$  ist kommutative Gruppe bezüglich Verknüpfung  $+$  mit  $a + 0 = a$   
und  $a + (-a) = 0$
- (ii)  $\mathcal{M}$  ist Halbgruppe bezüglich Verknüpfung  $*$
- (iii)  $a * (b + c) = a * b + a * c$  **Distributivität**
- (iv)  $a * b = b * a$  **Kommutativität**

Falls nur (iv) nicht gilt nennt man  $\mathcal{M}$  einen nichtkommutativen Ring.

Falls  $\mathcal{M}$  bezüglich  $*$  sogar ein Monoid ist, also ein multiplikatives Einselement besitzt, so heißt  $\mathcal{M}$  ein Ring mit 1.

## Beispiel A - 1.8 (Kommutativer Ring mit 1)

Neben  $\mathbb{Z}$  selbst auch  $\mathbb{Z}[x]$  d.h. die Menge aller Polynome mit Koeffizienten in  $\mathbb{Z}$  (siehe Abschnitt A2.4).

## Beispiel A - 1.9 (Nichtkommutativer Ring mit 1)

$\mathbb{Z}^{2 \times 2}$  d.h. die Menge allen  $2 \times 2$  Matrizen  $A$  mit ganzzahligen Elementen  $a, b, c, d \in \mathbb{Z}$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \text{mit} \quad 0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

wobei für  $A, A' \in \mathbb{Z}^{2 \times 2}$  Addition und Multiplikation definiert sind so dass

$$A + A' = \begin{bmatrix} a + a' & b + b' \\ c + c' & d + d' \end{bmatrix}, \quad A * A' = \begin{bmatrix} a * a' + b * c' & a * b' + b * d' \\ c * a' + d * c' & c * b' + d * d' \end{bmatrix}$$

## Lemma A-1.10 (Cartesisches Produkt)

*Für zwei Ringe  $\mathcal{R}$  und  $\mathcal{S}$  bildet die Menge aller geordneten Paare*

$$\mathcal{R} \times \mathcal{S} = \{(r, s) : r \in \mathcal{R}, s \in \mathcal{S}\}$$

*wiederrum einen Ring mit dem additiven Inversen  $(-r, -s)$  und dem neutralen Elementen  $(0_{\mathcal{R}}, 0_{\mathcal{S}})$ .*

*Hierbei bezeichnen  $0_{\mathcal{R}}$  und  $0_{\mathcal{S}}$  die Nullelemente von  $\mathcal{R}$  und  $\mathcal{S}$ .*

*Haben beide Ringe ein Einselemente  $1_{\mathcal{R}}$  bzw.  $1_{\mathcal{S}}$ , so ist  $(1_{\mathcal{R}}, 1_{\mathcal{S}})$  das Einselement von  $\mathcal{R} \times \mathcal{S}$ .*

## Definition A-1.11 (Körper)

Ein Ring  $\mathcal{M}$  mit 1 heißt Körper falls  $\mathcal{M} \setminus \{0\}$  eine Gruppe bezüglich  $*$  bildet d.h. für alle  $0 \neq a \in \mathcal{M}$  ein Inverses Element  $a^{-1} = 1/a$  existiert. Falls  $\mathcal{M}$  als Ring nicht kommutativ ist, heißt er *Schiefkörper*.

## Beispiel A-1.12 (Kommutativer Körper)

$$\mathbb{Q} = \left\{ \frac{p}{q} : q \neq 0, (p, q) \in \mathbb{Z}^2 \text{ teilerfrei} \right\}$$

### Bemerkung:

*Schiefkörper*, d.h. nicht kommutative Körper, spielen im Allgemeinen keine grosse Rolle.

## A-2 Algebraische Teilstrukturen

### Definition A-2.1

Häufig hat eine Teilmenge  $\mathcal{U} \subseteq \mathcal{M}$  einer Halbgruppe, eines Monoids, einer Gruppe, eines Ringes oder eines Körpers die selben strukturellen Eigenschaften bezüglich der vorgegebenen Verknüpfungen. Sie heißt dann entsprechend Unter- oder Teil- Halbgruppe, Monoid, Gruppe, Ring oder Körper.

### Lemma A-2.2 (*Schnittprinzip*)

*Der Durchschnitt zweier Unterhalbgruppen, Untergruppen, Unterringe oder Unterkörper ist wiederum eine Unterhalbgruppe, Untergruppe, Unterring, Unterkörper usw.*

### Beispiel A - 2.3

$\mathbb{N}$  ist Teilmonoid von  $\mathbb{Z}$ .

### Beispiel A - 2.4

$\mathbb{Z}$  ist Unterring von  $\mathbb{Q}$ .

### Beispiel A - 2.5

$2\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \text{ ist gerade}\}$  ist Untergruppe von  $\mathbb{Z}$ .

### Beispiel A - 2.6

$3\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \text{ ist durch 3 teilbar}\}$  ist Untergruppe von  $\mathbb{Z}$ .

### Beispiel A - 2.7

$2\mathbb{Z} \cap 3\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \text{ ist durch 6 teilbar}\}$  ist Untergruppe von  $\mathbb{Z}$ .

## Beispiel A - 2.8

Geometrische Rotationen in der Ebene bilden eine kommutative Gruppe, die man mit  $\mathcal{S}_1$  bezeichnet. Links- oder Rechtsdrehungen um ein Vielfaches von 30 Grad bilden eine Untergruppe. Neutrales Element ist die Drehung um den Winkel Null.

## Beispiel A - 2.9

Drehungen eines physikalischen Körpers im dreidimensionalen Raum bilden eine nichtkommutative Gruppe. Davon bilden alle Drehungen um eine vorgegebene Achse wiederum eine Untergruppe, die kommutativ ist.

### Bemerkung:

Unterstrukturen können stärkere Eigenschaften haben und insbesondere kommutativ sein, auch wenn dies für die Oberstruktur nicht gilt.

### Warnungen:

Lemma A-2.2 gilt nicht für Vereinigungen.

Der Schnitt von Ringen mit 1 braucht keine 1 zu haben.

## Definition A-2.10 (Abschluss und Hüllenbildung)

- (i) Eine Teilmenge  $\mathcal{U} \subset \mathcal{M}$  einer algebraischen Struktur  $\mathcal{M}$  heisst abgeschlossen bezüglich der in  $\mathcal{M}$  definierten binären Verknüpfung  $\circ \in \{+, -, *\}$  falls

$$u \in \mathcal{U} \ni v \Rightarrow u \circ v \in \mathcal{U} \ni v \circ u$$

- (ii) Für ein beliebiges  $\mathcal{U} \subset \mathcal{M}$  wird der Durchschnitt aller Halbgruppen bzw. Monoide, Gruppen, Ringe und Körper, die  $\mathcal{U}$  als Untermenge enthaltenden, als Hülle oder Abschluss  $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$  von  $\mathcal{U}$  bezeichnet. Wenn nicht alle strukturellen Eigenschaften von  $\mathcal{M}$  betrachtet werden so gibt man die entsprechenden Verknüpfungen explizit an. So bezeichnet z.B.  $\mathbf{span}_{\mathbb{Z}}^+(\mathcal{U})$  den Abschluss der Teilmenge  $\mathcal{U} \subset \mathbb{Z}$  in dem als additiver Monoid betrachteten Menge der ganzen Zahlen.
- (iii) Falls  $\mathbf{span}_{\mathcal{M}}^{\circ}(\mathcal{U}) = \mathcal{M}$  so heisst  $\mathcal{U} \subset \mathcal{M}$  ein erzeugendes System von  $\mathcal{M}$  bezüglich der Verknüpfung  $\circ$ .

## Lemma A-2.11 (Abschluss in Halbgruppe)

- (i) *Eine Teilmenge  $\mathcal{U} \subset \mathcal{M}$  einer multiplikativen Halbgruppe  $\mathcal{M}$  ist genau dann selbst eine Halbgruppe wenn sie bezüglich der Multiplikation  $*$  abgeschlossen ist.*
- (ii) *Sei  $\mathcal{U} \subset \mathcal{M}$  Teilmenge einer Halbgruppe  $\mathcal{M}$  mit der Verknüpfung  $*$ . Dann besteht die Hülle  $\mathbf{span}_{\mathcal{M}}^*(\mathcal{U})$  aus allen Elementen  $u \in \mathcal{M}$  der Form*

$$u = a_1 * a_2 * \cdots * a_n = \prod_{i=1}^n a_i,$$

*wobei  $n \in \mathbb{N}$  und  $a_i \in \mathcal{U}$  beliebig gewählt werden können.*

### Beispiel A - 2.12

$$\mathbb{N} = \mathbf{span}_{\mathbb{Z}}^{+}(\mathcal{U}) \quad \text{for } \mathcal{U} = \{0, 1\}$$

### Beispiel A - 2.13

$$\mathbb{Z} = \mathbf{span}_{\mathbb{Z}}^{+,-}(\mathcal{U}) \quad \text{for } \mathcal{U} = \{0, 1\}$$

### Beispiel A - 2.14

$$\mathcal{U} = \mathbf{span}_{\mathbb{Z}}^{*}(\mathcal{U}) \quad \text{for } \mathcal{U} = \{0, 1\}$$

### Beispiel A - 2.15

$$\mathbb{Z} = \mathbf{span}_{\mathbb{Z}}^{*}(\{\mathbb{Z} \ni p \text{ prim}\})$$

### Beispiel A - 2.16

$$5\mathbb{Z} = \mathbf{span}_{\mathbb{Z}}^{+}(\{5\})$$

## Lemma A-2.17 (Abschluss in Gruppe)

- (i) Eine Teilmenge  $\mathcal{U} \subset \mathcal{M}$  einer multiplikativen Gruppe  $\mathcal{M}$  ist genau dann selbst eine Gruppe wenn sie bezüglich der Multiplikation  $*$  und der Division  $/$  abgeschlossen ist, was insbesondere verlangt, dass  $1 \in \mathcal{U}$ .
- (ii) Sei  $\mathcal{U} \subset \mathcal{M}$  Teilmenge einer Gruppe  $\mathcal{M}$  mit der Verknüpfung  $+$  und  $a - b = a + (-b)$ . Dann besteht die Hülle  $\text{span}_{\mathcal{M}}^{+,-}(\mathcal{U})$  aus allen Elementen  $u \in \mathcal{M}$  der Form

$$\begin{aligned} u &= a_1 + a_2 + \cdots + a_n - (b_1 + b_2 + \cdots + b_m) \\ &= \sum_{i=1}^n a_i - \sum_{i=1}^m b_i, \end{aligned}$$

wobei  $n, m \in \mathbb{N}$  und  $a_i, b_i \in \mathcal{U}$  beliebig gewählt werden können.

## Lemma A-2.18 (Abschluss in Ring)

Sei  $\mathcal{U} \subset \mathcal{M}$  Teilmenge eines Ringes  $\mathcal{M}$  mit der Verknüpfungen  $+$ ,  $a - b = a + (-b)$  und  $a * b$ . Dann besteht die Hülle  $\text{span}_{\mathcal{M}}^{+, -, *}(\mathcal{U})$  aus allen Elementen  $u \in \mathcal{M}$  der Form

$$\begin{aligned} u &= \pm a_{11} * a_{12} * \cdots * a_{1n_1} \pm a_{21} * a_{22} * \cdots * a_{1n_2} \dots\dots \\ &= \sum_{i=1}^m \pm \prod_{j=1}^{n_i} a_{ij}, \end{aligned}$$

wobei  $m, n_i \in \mathbb{N}$  und  $a_{ij} \in \mathcal{U}$  beliebig.

## A-3 Algebraische Erweiterungen

### Bemerkung:

Häufig will man eine gegebene algebraische Struktur  $\mathcal{M}$  so erweitern, dass sie bezüglich einer wünschenswerten Eigenschaft abgeschlossen ist. Dazu konstruiert man geeignet neue Elemente, so dass der erzielte Abschluss diese stärkere Eigenschaft hat.

## Beispiel A - 3.1

Die natürlichen Zahlen  $\mathbb{N}$  sind bezüglich der Addition nur ein Monoid (d.h. Halbgruppe) mit dem neutralen Element 0. Um sie zu einer Gruppe zu erweitern, führt man für jedes Element  $n \in \mathbb{N}$  ein mit  $(-n)$  bezeichnetes neues Element ein, das gerade durch die Eigenschaft

$$(-n) + n = 0 = n + (-n)$$

gekennzeichnet ist. Man muss dann „nur“ noch zeigen, dass die Verknüpfung mit den neuen Elementen so definiert werden kann, dass die erhaltene Menge der ganzen Zahlen, nämlich  $\mathbb{Z}$ , wirklich eine Gruppe bezüglich  $+$  darstellt. Man erhält so die negativen Zahlen mit den bekannten Rechenregeln.

## Beispiel A - 3.2

Durch obige Konstruktion erhält man die Menge  $\mathbb{Z}$ , die bezüglich  $+$  und  $*$  sogar ein Ring ist. Um  $\mathbb{Z}$  noch zum Körper auszubauen, fügt man alle Quotienten  $a/b$  mit  $a, b \in \mathbb{Z}$  teilerfrei hinzu und erhält die rationalen Zahlen  $\mathbb{Q}$ .

### Bemerkung:

Nicht alle Ringe lassen sich wie  $\mathbb{Z}$  zu einem Körper erweitern. Das geht z.B nicht für die **unsigned chars**  $\mathcal{B}$ , da dort  $32 * 8 = 0$  gilt.

Hätte 8 in irgendeiner Erweiterung einen Kehrwert  $8^{-1}$ , so würde

$$32 = 32 * 8 * 8^{-1} = 0 * 8^{-1} = 0$$

folgen, was offensichtlich inkonsistent wäre.

### Definition A-3.3 (Integritätsbereich)

Ein Paar von Ringelementen  $a, b \in \mathcal{M}$  heißt Nullteiler, falls

$$a \neq 0 \neq b \quad \wedge \quad a * b = 0.$$

Ein Ring ohne Nullteiler heißt Integritätsbereich.

### Satz A-3.4 (Nullteiler oder Inverse)

*In einem endlichen Ring ist jedes Element  $a \neq 0$  entweder selbst Nullteiler oder hat ein multiplikatives Inverses der Form  $a^{-1} = a^k = a * \dots * a$  für ein  $k \in \mathbb{N}$ .*

### Satz A-3.5 (Körpererweiterung)

*Ein Ring  $\mathcal{M}$  mit 1 kann dann und nur dann zu einem Körper erweitert werden, wenn er ein Integritätsbereich ist, d.h. keine Nullteiler besitzt.*

*Alle endlichen Integritätsbereiche sind selbst Körper.*

## Resultierende Zahlenhierarchie:

**Monoid**  $\mathbb{N}$  Natürliche Zahlen

$\cap$  (Negativenbildung)

**Ring**  $\mathbb{Z}$  Ganze Zahlen

$\cap$  (Quotientenbildung)

**Körper**  $\mathbb{Q}$  Rationalen Zahlen

$\cap$  (Inf/Sup Bildung)

**Körper**  $\mathbb{R}$  Reelle Zahlen

$\cap$  (Wurzelberechnung)

**Körper**  $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$  Komplexe Zahlen

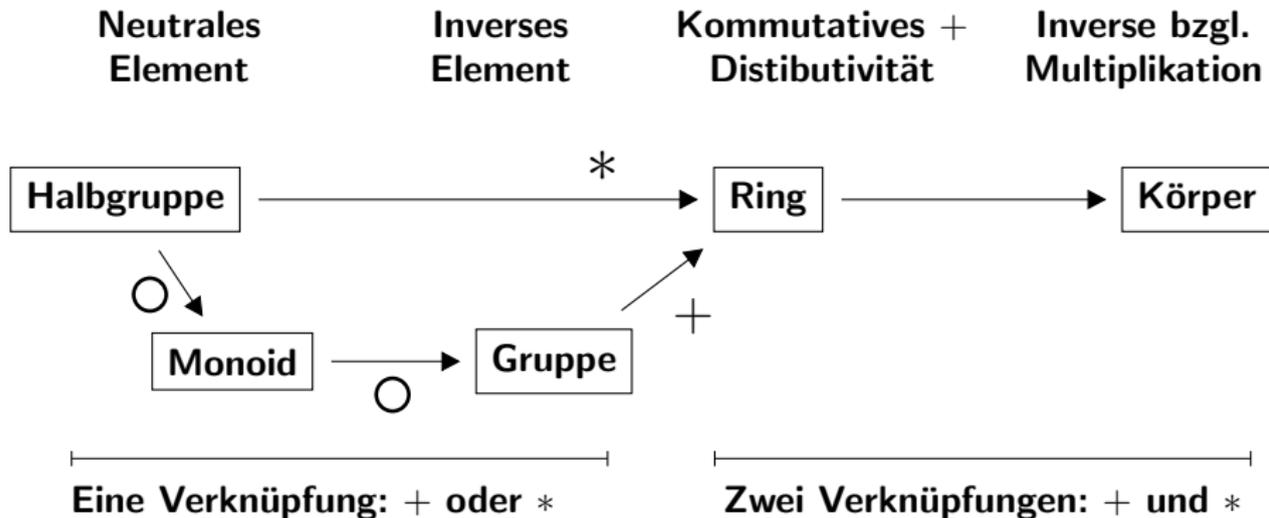
$\cap$  (Mathematischer Eifer)

**Schiefkörper**  $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$  Quaternionen

### Bemerkung:

Quaternionen sind nützlich bei der Beschreibung von Positionen und Drehungen im Raum.

# Hierarchie algebraischer Grundstrukturen



## A-4 Äquivalenzrelationen und Quotientenstrukturen

### Bemerkung

Die Menge der **unsigned chars**  $\mathcal{B}$  basiert nicht direkt auf der Zahlenhierarchie, sie ergibt sich als sogenannter Quotientenring von  $\mathbb{Z}$ .

Entsprechend bilden die Drehungen in der Ebene  $S^1$  eine Quotientengruppe von  $\mathbb{R}$ , wobei alle Drehwinkel  $\varphi_1, \varphi_2$ , deren Differenz ein ganzes Vielfaches von  $2\pi$  ist, zusammengelegt werden, da sie als äquivalent betrachtet werden.

## Definition A-4.1 (Äquivalenzrelationen)

Man nennt  $\mathcal{R} \subset \mathcal{M} \times \mathcal{M}$  eine Äquivalenzrelation auf  $\mathcal{M}$  und schreibt dann

$$x \sim y \iff (x, y) \in \mathcal{R}$$

wenn für alle  $x \in \mathcal{M}$  die folgenden Eigenschaften gelten :

$$x \sim x$$

$$x \sim y \wedge y \sim z \implies x \sim z$$

$$x \sim y \implies y \sim x$$

**Reflexivität**  
**Transitivität**  
**Symmetrie**

Für jedes  $x \in \mathcal{M}$  bezeichnet

$$[x]_{\mathcal{R}} \equiv \{y \in \mathcal{M} : x \sim y\}$$

die Äquivalenzklasse von  $x$  bezüglich  $\sim$ .

Falls  $\mathcal{R}$  im Kontext eindeutig ist, schreibt man einfach  $[x]$ .

### Beispiel A - 4.2

Für  $x, y \in \mathbb{R}$  gelte

$$x \sim y \iff x * x = y * y$$

Dann ergibt sich für alle  $x \in \mathbb{R}$  die Äquivalenzklasse  $[x] = \{+x, -x\}$

### Beispiel A - 4.3

Geraden in der Ebene seien äquivalent, wenn sie parallel sind.

Äquivalenzmengen sind dann alle Geraden mit derselben Steigung.

### Lemma A - 4.4 (Quotientenäquivalenz)

Für  $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  definiert

$$x \sim y \iff x_1 * y_2 = y_1 * x_2$$

eine Äquivalenzrelation.

## Lemma A-4.5 (Restklassen bezüglich Untergruppe)

$\mathcal{U} \subset \mathcal{G}$  kommutative Untergruppe impliziert, dass

$$x \sim y \iff x - y \in \mathcal{U} \iff \exists z \in \mathcal{U} : x = y + z$$

eine Äquivalenzrelation ist.

### Beispiel A-4.6

Für festes  $m \in \mathbb{Z}$  gelte:  $x \sim y \iff m$  teilt  $x - y$ .

Hier ist  $U = m\mathbb{Z}$  die Untergruppe aller durch  $m$  teilbaren ganzen Zahlen.

## Lemma A-4.7 (Partitionierung)

Sei  $\sim$  Äquivalenzrelation auf  $\mathcal{M}$ .

- (i)  $[x] = [y] \iff x \sim y$
- (ii)  $[x] \cap [y] = \emptyset \iff x \not\sim y$
- (iii) Es existiert eine Repräsentantenmenge  $\mathcal{M}' \subset \mathcal{M}$ , so dass

$$\forall y \in \mathcal{M}, x, z \in \mathcal{M}' \cap [y] \implies z = x$$

*M.a.W. Jede Äquivalenzklasse enthält genau ein Element aus  $\mathcal{M}'$ .  
Daraus folgt*

$$x, y \in \mathcal{M}' \wedge (x \neq y) \implies [x] \neq [y]$$

sowie

$$\mathcal{M} = \bigcup_{x \in \mathcal{M}'} [x]$$

### Beispiel A - 4.8

Für Beispiel A - 4.6 nehme Repräsentant  $0 \leq x < m$ .

### Beispiel A - 4.9

Für Lemma A - 4.4 nehme gekürzten Bruch wo  $x_1$  und  $x_2$  teilerfremd sind.

### Beispiel A - 4.10

Für Beispiel A - 4.3 nehme Gerade durch Nullpunkt.

## Definition A-4.11 (Quotientenmenge)

$$\mathcal{M}/R = \mathcal{M}/\sim = \{[x] : x \in \mathcal{M}\}$$

bezeichnet die Mengen aller **Äquivalenzklassen** von  $\sim$  in  $\mathcal{M}$ . Ihre Elemente werden häufig mit denen von  $\mathcal{M}'$  identifiziert.

## Satz A-4.12 (Quotientengruppe)

*Ist  $\sim$  durch eine Untergruppe  $\mathcal{U}$  der kommutativen Gruppe  $\mathcal{G}$  induziert so definiert die additive Verknüpfung*

$$[x] + [y] \equiv [x + y]$$

*auf der Partitionierung  $\mathcal{G}/\sim$  eine Gruppenstruktur, welche mit  $\mathcal{G}/\mathcal{U}$  bezeichnet wird. Die Restklasse  $[0]$  bildet die Null in  $\mathcal{G}/\mathcal{U}$  und  $[-x]$  das negative Element zu  $[x]$ .*

## Beispiele A-4.13 (Symmetrische Gruppe)

- ▶  $\mathcal{G} = \mathbb{R}, \mathcal{U} = \{2\pi k : k \in \mathbb{Z}\}$
- ▶  $\mathcal{S}^1 = \mathcal{G}/\mathcal{U} = \text{Richtungen in Ebene} = \{-\pi \leq x < \pi\} \equiv \mathcal{M}'$

## Beispiel A-4.14 (Restklassenringe)

$$\mathcal{G} = \mathbb{Z}, \quad \mathcal{U} = \{mx : x \in \mathbb{Z}\} = m\mathbb{Z},$$
$$\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z}) = \{x \in \mathbb{Z} : 0 \leq x < m\}$$

### Bemerkung:

$\mathbb{Z}_m$  ist nicht nur Gruppe, sondern sogar Ring, da  $\mathcal{U}$  nicht nur Untergruppe, sondern  $m$  folgenden Sinne sogar 'Ideal' im Ring  $\mathbb{Z}$  ist.

## Definition A-4.15 (Ideal)

Eine Untergruppe  $U \subset \mathcal{M}$  heißt **Ideal des kommutativen Ringes  $\mathcal{M}$**  falls

$$a \in U \wedge b \in \mathcal{M} \implies a * b \in U$$

m.a.W. alle Produkte mit einem Faktor in  $U$  gehören auch zu  $U$ .

Speziell ist für jedes  $a \in \mathcal{M}$  die *Gruppe*

$$U = a * \mathcal{M} = \{a * b : b \in \mathcal{M}\}$$

ein sogenanntes *Hauptideal* in  $\mathcal{M}$ .

### Bemerkung:

Jedes Ideal ist insbesondere ein Unterring.

Körper haben keine Hauptideale außer sich selbst und  $\{0\}$ .

### Beispiel A - 4.16

$m\mathbb{Z}$  ist Hauptideal in  $\mathbb{Z}$ .

### Beispiel A - 4.17

$\mathcal{M} = \mathbb{Z}[x]$  = Menge aller reellen Polynome enthält  $x * \mathcal{M} \equiv x * \mathbb{Z}[x] =$   
Menge aller Polynome, deren nullter Koeffizient (= konstanter Term)  
verschwindet.

## Satz A-4.18 (Quotientenringe)

*Gilt Satz A-4.12 und ist  $\mathcal{U}$  sogar Ideal im kommutativen Ring  $\mathcal{G}$ , dann macht die zusätzliche multiplikative Verknüpfung*

$$[x] * [y] \equiv [x * y]$$

*die Quotientengruppe  $\mathcal{G}/\mathcal{U}$  selbst zu einem kommutativen Ring. Hat  $\mathcal{G}$  die Eins 1, so ist die Äquivalenzklasse  $[1]$  die Eins im Quotientenring.*

## Schlussbemerkung

- ▶  $\mathcal{B} = \text{unsigned char} = \mathbb{Z}_{256} = \mathbb{Z}/256\mathbb{Z}$  ist ein endlicher kommutativer Ring mit Nullteilern. (z.B.  $[32] * [8] = [256] = [0]$ )
- ▶ Obwohl  $a/b$  für  $b \neq 0$  auf dem Rechner immer ein Ergebnis liefert, bedeutet dies nicht, dass  $a/b = a * b^{-1}$  für ein inverses Element  $b^{-1}$  in  $\mathbb{Z}_{256}$  gilt. Vielmehr gilt  $a/b = r_b(a)$  wie im Folgenden definiert.

## A-5 Modulare Arithmetik

### Satz A-5.1 (Teilung mit Rest)

In  $\mathcal{M} = \mathbb{Z}$  gibt es für jedes Paar  $a, m \in \mathcal{M}$  mit  $m > 0$  genau ein Paar  $q, r \in \mathcal{M}$ , so dass gilt:

$$a = qm + r \quad \wedge \quad 0 \leq r < m.$$

Dabei wird  $r$  **Rest** genannt,  $q$  ist der **Quotient**.

## Definition A - 5.2 (Modulbezeichnung, Teilbarkeit, Primzahl)

- (i) Da der Rest  $r$  oft wichtiger ist als der Quotient  $q$ , schreibt man

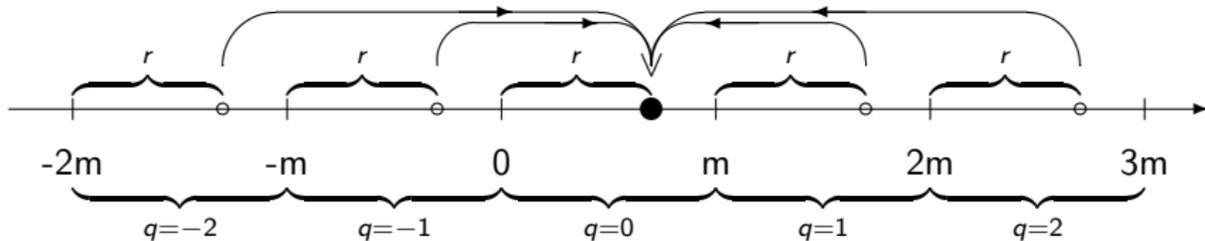
$$r = r_m(a) = a \bmod m$$

(sprich:  $r$  gleich „ $a$  modulo  $m$ “).

- (ii) Offenbar gilt  $r_m(a) = 0$  genau dann, wenn  $a$  durch  $m$  teilbar ist. Dann schreibt man  $m|a$  (sprich: „ $m$  teilt  $a$ “).
- (iii) Folgt aus  $m|a$  immer  $m \in \{1, a\}$  und ist  $a \neq 1$ , so heißt  $a$  **Primzahl**.

## Zahlengerade

Die Abbildung der beliebigen ganzen Zahl  $a$  in den Quotienten  $q$  und den Rest  $r$  für gegebenes festes  $m > 0$  kann man sich wie folgt vorstellen.



Alle offenen Kreisscheiben werden in den gleichen Rest, d.e. den vollen Punkt abgebildet. Dabei variiert nur der Quotient  $q$ , wie unten angegeben. Dieser ist wiederum in Intervallen der Breite  $m$  konstant.

### Beispiel A - 5.3

$$7 \bmod 3 = r_3(7) = 1 \quad (q = 2)$$

### Beispiel A - 5.4

$$-13 \bmod 5 = r_5(-13) = 2 \quad (q = -3)$$

### Bemerkung:

In der Programmiersprache C wird `mod` durch das Prozentzeichen `%` definiert:

$$a \% m = a - m(a/m) \quad \text{für } a \geq 0 < m.$$

Da das Vorzeichen des Restes für negative  $a$  abhängig von der Implementation (also dem verwendeten Compiler) ist, gilt obige Gleichung nicht unbedingt.

Es erfolgt aber immer eine Rundung in Richtung Null:

$$a/m = -(-a/m) \quad \text{für } a < 0 < m.$$

## Satz A-5.5 (Modulare Arithmetik)

In  $\mathbb{Z}_m \simeq \{0, 1, \dots, m-1\}$  wird durch

$$a +_m b := (a + b) \bmod m \equiv r_m(a + b)$$

und

$$a *_m b := (a * b) \bmod m \equiv r_m(a * b)$$

eine **kommutative Ringstruktur** definiert.

### Bemerkung

Bei komplexeren Ausdrücken ohne Division kann erst in  $\mathbb{Z}$  gerechnet und nur zum Schluß auf  $[0, m-1]$  modularisiert werden.

## Satz A-5.6 (Fermat(1640))

Falls  $m$  prim, gilt für alle  $a \in \mathbb{Z}$

$$a^m \equiv a \pmod{m}.$$

Ist  $m$  kein Teiler von  $a$ , so gilt  $a^{m-1} \equiv 1 \pmod{m}$ .

## Korollar A-5.7

$\mathbb{Z}_m$  ist genau dann ein Integritätsbereich und damit nach Satz A-3.5 ein Körper, wenn  $m$  eine Primzahl ist. Dann gilt für alle  $a \in \mathbb{Z}_m$

$$a^{-1} = a^{m-2}.$$

## Beispiel A-5.8

In  $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$  gilt:

$$\bar{1}^{-1} = \bar{1} * \bar{1} * \bar{1} = 1 \pmod{5} = \bar{1} \quad \implies \quad \bar{1} * \bar{1} = 1 \pmod{5} = \bar{1}$$

$$\bar{2}^{-1} = \bar{2} * \bar{2} * \bar{2} = 8 \pmod{5} = \bar{3} \quad \implies \quad \bar{2} * \bar{3} = 6 \pmod{5} = \bar{1}$$

$$\bar{3}^{-1} = \bar{3} * \bar{3} * \bar{3} = 27 \pmod{5} = \bar{2} \quad \implies \quad \bar{3} * \bar{2} = 6 \pmod{5} = \bar{1}$$

$$\bar{4}^{-1} = \bar{4} * \bar{4} * \bar{4} = 64 \pmod{5} = \bar{4} \quad \implies \quad \bar{4} * \bar{4} = 16 \pmod{5} = \bar{1}$$

## Multiplikation in $\mathbb{Z}_5$

*	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

## Addition und Subtraktion in $\mathbb{Z}_5$

### Subtraktion

A d d i t i o n

$+\backslash-$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{3}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{4}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

## Division in $\mathbb{Z}_5$

/	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	—	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	—	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	—	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{3}$
$\bar{3}$	—	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	—	$\bar{4}$	$\bar{2}$	$\bar{3}$	$\bar{1}$

## Anwendung: Hashing

### Motivation:

Angenommen, eine Firma hat allen ihren Angestellten eine 10-stellige Personalnummer  $k$  zugeordnet. Sie erwartet aber, nie mehr als  $m = 1000$  Angestellte zu haben, und hat deshalb eine Registratur mit 1000 durchnummerierten Ablagen angelegt. Um schnell auf diese zugreifen zu können, sucht sie für  $n = 10^{10}$  eine sogenannte **Hashfunktion**

$$h : \{1, 2, \dots, n\} \longrightarrow \{0, 1, 2, \dots, m - 1\},$$

so dass möglichst alle zu irgendeinem Zeitpunkt tatsächlich vorhandenen Personalnummern  $k$  einen „eigenen“ Funktionswert  $h(k)$  haben. Da die Menge  $\mathcal{K}$  der vorhandene  $k$  aus datenschutzrechtlichen Gründen nie bekannt ist, und sich zudem durch Personalfluktuation ändern kann, läßt sich für a priori gewählte  $h$  eine Kollision

$$h(k') = h(k) \quad \text{mit} \quad k \neq k' \quad \text{und} \quad k, k' \leq n$$

nicht immer verhindern.

## Fortsetzung: Hashing

Das gilt auch für die einfache **Hashfunktion**

$$h(k) = k \bmod p \quad \text{mit } p \geq m,$$

wobei  $p$  häufig als Primzahl gewählt wird.

Um für ein  $k$  mit einer bereits durch ein  $k'$  belegten Speicheradresse  $h(k) = h(k')$  ein freies Ablagefach zu finden, wird in der Nähe von  $h(k)$  **sondiert**.

Beim **quadratischen Sondieren** durchsucht man die Adressen

$$(h(k) + i^2) \bmod p \quad \text{und} \quad (h(k) - i^2) \bmod p$$

für  $i = 1, 2, \dots, (p-1)/2$ , bis freies Fach gefunden wurde.

Setzt man voraus, dass mindestens ein freies Fach vorhanden ist, garantiert der folgende Satz den Erfolg des **quadratischen Sondierens**.

## Satz A-5.9 (siehe Hartmann 4.24)

Ist  $p$  eine Primzahl mit  $p \bmod 4 = 3$ , so gilt:

$$\{\pm i^2 \bmod p : i = 1, 2, \dots, (p-1)/2\} = \{1, 2, \dots, p-1\}$$

Mit anderen Worten: Alle Adressen werden durchsucht.

### Beispiel A-5.10 ( $p = 11$ )

$i$	1	2	3	4	5
$i^2 \bmod 11$	1	4	9	5	3
$-i^2 \bmod 11$	10	7	2	6	8

## A-6 Strukturerehaltende Abbildungen

Wir betrachten Abbildungen

$$\phi : \mathcal{M} \mapsto \mathcal{N}$$

zwischen Mengen  $\mathcal{M}$  und  $\mathcal{N}$ , die gegebenenfalls deren algebraische Struktur erhalten. Mittels der Urbilder

$$\phi^{-1}(b) = \{a \in \mathcal{M} : \phi(a) = b\} \quad \text{für } b \in \mathcal{N}$$

lassen sich die Eindeutigkeitseigenschaften von Abbildungen wie folgt charakterisieren.  $\phi$  ist

**injektiv**, falls alle  $\phi^{-1}(b)$  höchstens ein Element enthalten.

**surjektiv**, falls alle  $\phi^{-1}(b)$  mindestens ein Element enthalten.

**bijektiv**, falls alle  $\phi^{-1}(b)$  genau ein Element enthalten.

Im letzteren Falle heißen  $\mathcal{M}$  und  $\mathcal{N}$  gleichmächtig.

Die Elemente abzählbarer Mengen können durchnumeriert und dann mit ihrer Nummer identifiziert werden. Insbesondere kann man jede Menge von  $n < \infty$  Elementen darstellen als

$$\mathcal{M} = \{m_1, m_2, \dots, m_{n-1}, m_n\} \simeq \{1, 2, \dots, n-1, n\}$$

### Definition A-6.1 (Permutationen)

Eine bijektive Abbildung  $\phi$  einer endlichen Menge  $\mathcal{M}$  in sich selbst heißt **Permutation**, für  $\mathcal{M} = \{1, 2, \dots, n-1, n\}$  lässt sie sich als  $n$ -Tupel spezifizieren,

$$\phi = (\phi(1), \phi(2), \phi(3), \dots, \phi(n)) \in \{1, 2, \dots, n\}^n$$

### Lemma A-6.2

*Es gibt auf  $\mathcal{M} = \{1, 2, \dots, n-1, n\}$  genau  $n! = n \cdot (n-1) \cdots 2 \cdot 1$  unterschiedliche Permutationen, die bezüglich ihrer Hintereinanderausführung eine nichtkommutative Gruppe mit dem neutralen Element  $(1, 2, \dots, n)$  bilden.*

## Beispiel A - 6.3

Die dreielementige Menge  $\mathcal{M} = \{1, 2, 3\}$  hat die 6 Permutationen

$$\phi_1 = (1, 2, 3), \phi_2 = (2, 1, 3), \phi_3 = (1, 3, 2),$$

$$\phi_4 = (3, 2, 1), \phi_5 = (2, 3, 1), \phi_6 = (3, 1, 2)$$

Als neutrales Element erfüllt  $\phi_1$  für  $i = 1 \dots 6$

$$\phi_1 \circ \phi_i = \phi_i = \phi_i \circ \phi_1$$

Da  $\phi_i$  für  $i = 2, 3, 4$  jeweils ein Element von  $\mathcal{M} = \{1, 2, 3\}$  festhält und die anderen beiden austauscht, ist es sein eigenes Inverses, so dass

$$\phi_i \circ \phi_i = \phi_1 \quad \text{für } i = 2, 3, 4.$$

## Fortsetzung: Beispiel

Die letzten beiden  $\phi_5, \phi_6$  kann man interpretieren als Links- bzw. Rechtsverschiebung aller Elemente. Es gilt also

$$\phi_5 \circ \phi_6 = \phi_1 = \phi_6 \circ \phi_5 \quad \text{und} \quad \phi_5 \circ \phi_5 = \phi_6, \quad \phi_6 \circ \phi_6 = \phi_5$$

Die Nichtkommutativität sieht man zum Beispiel bei

$$\phi_2 \circ \phi_3 = \phi_5 \neq \phi_6 = \phi_3 \circ \phi_2 .$$

## Definition A-6.4 (Homomorphismus und Endomorphismus)

- (i) Falls auf  $\mathcal{M}$  und  $\mathcal{N}$  algebraische Verknüpfungen  $+$  und/oder  $*$  definiert sind, so dass für alle  $a, b \in \mathcal{M}$

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{und} \quad \phi(a * b) = \phi(a) * \phi(b)$$

gelten, dann heißt  $\phi$  ein **Homomorphismus** von  $\mathcal{M}$  nach  $\mathcal{N}$ .

- (ii) Falls  $\mathcal{M} = \mathcal{N}$ , die Struktur  $\mathcal{M}$  also in sich selbst abgebildet wird, spricht man auch von einem **Endomorphismus**.
- (iii) Je nachdem, welche Struktur in  $\mathcal{M}$  vorhanden und durch  $\phi$  im obigen respektiert wird, nennt man  $\phi$  einen Halbgruppenhomomorphismus, Ringhomomorphismus usw.

## Beispiel A - 6.5

Für jede ganze Zahl  $m > 1$  ist die Abbildung

$$\phi(a) = m * a \quad \text{für } a \in \mathbb{Z}$$

ein injektiver Gruppenendomorphismus von  $\mathbb{Z}$  in sich selbst. Obwohl  $\mathbb{Z}$  und das Bild  $\phi(\mathbb{Z})$  Ringe sind, ist  $\phi$  kein Ringhomomorphismus, da z.B.

$$\phi(m * m) = m^3 \quad \neq \quad m^4 = \phi(m) * \phi(m)$$

## Lemma A - 6.6

Für jedes feste  $0 \neq m \in \mathbb{Z}$  ist die Abbildung

$$\phi(a) = r_m(a) = a \text{ mod } m$$

ein surjektiver Ringhomomorphismus von  $\mathbb{Z}$  in den Restklassenring  $\mathbb{Z}_m$ .

## Definition A - 6.7 (Isomorphismus)

- (i) Bijektive Homomorphismen heißen **Isomorphismen**. Gibt es einen Isomorphismus zwischen den algebraischen Strukturen  $\mathcal{M}$  und  $\mathcal{N}$ , so nennt man diese **isomorph**.
- (ii) Bei injektiven Homomorphismen spricht man auch von einer isomorphen Einbettung von  $\mathcal{M}$  in  $\mathcal{N}$ .

### Bemerkung:

Sind  $\mathcal{M}$  und  $\mathcal{N}$  isomorph, so haben sie dieselbe Struktur und unterscheiden sich eigentlich nur in der Bezeichnung ihrer Elemente.

Bei isomorphen Einbettungen gilt diese Beziehung (nur) für  $\mathcal{M}$  und sein Bild  $\phi(\mathcal{M}) \subset \mathcal{N}$ .

Es gibt aber häufig isomorphe Endomorphismen geben, die nicht auf der Hand liegen und sich insbesondere von der Identität unterscheiden.

## Beispiel A - 6.8

Auf dem Matrizenring  $\mathbb{Z}^{2 \times 2}$  kann man  $\phi$  definieren so dass

$$\phi : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} d & c \\ b & a \end{bmatrix}$$

Mit anderen Worten: Die Zeilen und Spalten der  $2 \times 2$  Matrizen werden ausgetauscht.

Man kann überprüfen, dass  $\phi$  den Ring  $\mathbb{Z}^{2 \times 2}$  isomorph in sich selbst abbildet und sogar sein eigenes Inverses ist, da  $\phi(\phi(A)) = A$  für alle  $A \in \mathbb{Z}^{2 \times 2}$ .

## Beispiel A - 6.9

Ordnet man jedem  $a \in \mathbb{Z}$  das  $A \in \mathbb{Z}^{2 \times 2}$  zu, das  $a$  als erstes Diagonalelement hat und sonst nur aus Nullen besteht, so erhält man einen injektiven Ringhomomorphismus  $\phi$  von  $\mathbb{Z}$  nach  $\mathbb{Z}^{2 \times 2}$ .

Man kann  $\mathbb{Z}$  natürlich auch isomorph in  $\mathbb{Z}^{2 \times 2}$  einbetten, wenn man  $a$  durch  $\phi$  in das zweite Diagonalelement von  $A$  bringen lässt.

Kopiert  $\phi$  jedoch  $a$  in eines der beiden nichtdiagonalen Elemente, so geht die multiplikative Eigenschaft  $\phi(a * b) = \phi(a) * \phi(b)$  verloren.

Mit anderen Worten: Das resultierende  $\phi$  ist kein Ringhomomorphismus, sondern nur noch ein injektiver Gruppenhomomorphismus (Siehe Übung). Und das, obwohl dann das aus allen strikt dreiecksförmigen Matrizen bestehende Bild  $\phi(\mathbb{Z})$  sogar wiederum ein Ring ist.

## Lemma A-6.10

- (i) *Jeder surjektive Homomorphismus  $\phi$  bildet die neutralen und inversen Elemente von  $\mathcal{M}$  in die entsprechenden neutralen und inversen Element von  $\mathcal{N}$  ab.*
- (ii) *Die homomorphen Bilder  $\phi(\mathcal{U}) \subset \mathcal{N}$  von Unter(halb)gruppen, Unterringen usw.  $\mathcal{U} \subset \mathcal{M}$  bilden dieselben Unterstrukturen von  $\mathcal{N}$ .*
- (iii) *Das **Kern** von  $\phi$  genannte Urbild*

$$\text{Kern}(\phi) = \phi^{-1}(0) = \{a \in \mathcal{M} : \phi(a) = 0 \in \mathcal{N}\}$$

*ist bei Gruppenhomomorphismen eine Untergruppe und bei Ringhomomorphismen sogar ein Ideal. Die Quotientengruppe bzw. der Quotientenring von  $\mathcal{M}$  bezüglich der durch den Kern definierten Äquivalenz ist isomorph zu dem Bild  $\phi(\mathcal{M}) \subset \mathcal{N}$ .*

## Satz A-6.11

- (i) *Alle Endomorphismen einer Gruppe  $\mathcal{M}$  in sich selbst bilden bezüglich der Hintereinanderausführung zunächst einen Monoid  $\text{Endo}(\mathcal{M})$ . Dessen neutrales Element ist die Identitätsabbildung*

$$\text{id}_{\mathcal{M}} : \mathcal{M} \mapsto \mathcal{M} \quad \text{mit} \quad \text{id}_{\mathcal{M}}(a) = a \quad \text{für} \quad a \in \mathcal{M}$$

- (ii) *Die bijektiven Abbildungen bilden einen Untermonoid  $\text{Iso}(\mathcal{M}) \subset \text{Endo}(\mathcal{M})$  mit multiplikativer nichtkommutativer Gruppenstruktur.*
- (iii) *Ist  $\mathcal{M}$  selbst kommutative Gruppe, so kann man für jeweils zwei Elemente  $\phi, \psi \in \text{Endo}(\mathcal{M})$  ihre Summe  $\eta = \phi + \psi$  definieren durch*

$$\eta(a) = (\phi + \psi)(a) = \phi(a) + \psi(a) \quad \text{für} \quad a \in \mathcal{M}$$

*Bezüglich dieser Addition und der Hintereinanderausführung als Multiplikation bildet  $\text{Endo}(\mathcal{M})$  einen nichtkommutativen Ring mit Eins.*

## Beispiel

Für  $\mathcal{M} = \mathbb{Z} \times \mathbb{Z}$  erhält man einen Endomorphismenring, der zu dem von uns häufig betrachteten Matrixring  $\mathbb{Z}^{2 \times 2}$  isomorph ist. Beachte hier, dass algebraische Konzepte geschachtelt angewandt werden, da wir über Isomorphie zwischen Ringen sprechen, von denen einer selbst aus Homomorphismen einer Gruppe besteht.

## Bemerkung

Die letzte Isomorphieaussage im Lemma A-6.10 ist von eher theoretischer Bedeutung. Wir werden ihr später wiederbegegnen, wenn es um lineare Abbildungen als Homomorphismen zwischen sogenannten Vektorräumen geht. Nur in dem Zusammenhang muss diese Isomorphie wirklich verstanden werden.

## A-7 Teilbarkeit und partielle Ordnungen

### Lemma A-7.1 (Eigenschaften der Teilbarkeit)

Für  $a, b, c \in \mathcal{M} = \mathbb{N}$  gilt:

- (i)  $a|b \wedge b|c \implies a|c$
- (ii)  $a|b \wedge b|a \implies a = b$
- (iii)  $a|a$

**Transitivität**  
**Antisymmetrie**  
**Reflexivität**

### Bemerkung:

Offenbar folgt aus  $a|b$  daß  $a \leq b$ .

Die Umkehrung gilt aber nicht da z.B. weder  $3|7$  noch  $7|3$ .

Teilbarkeit repräsentiert eine partielle Ordnung im Sinne der folgenden Definition.

## Definition A-7.2 (Ordnungsrelation)

- (i) Die durch eine Menge  $\mathcal{R} \subset \mathcal{M} \times \mathcal{M}$ , definierte Beziehung

$$a \prec b \iff b \succ a \iff (a, b) \in \mathcal{R},$$

heißt **Ordnungsrelation** falls

$$a \prec b \wedge b \prec c \implies a \prec c$$

**Transitivität**

$$a \prec b \wedge b \prec a \implies a = b$$

**Antisymmetrie**

- (ii) Die Ordnungsrelation heißt **streng** falls für alle  $a \in \mathcal{M}$  die folgenden äquivalenten Aussagen gelten

$$a \not\prec a \iff \neg(a \prec a).$$

Dann wird durch

$$a \preceq b \iff a \prec b \vee a = b$$

eine **reflexive** Ordnungsrelation definiert, so daß  $a \preceq a$  für alle  $a \in \mathcal{M}$ . Umgekehrt ergibt sich strenge Ordnung durch

$$a \prec b \iff a \preceq b \wedge a \neq b$$

- (iii) Die Relation heißt **vollständig** oder eine **Wohlordnung** von  $\mathcal{M}$ , falls für alle  $a, b \in \mathcal{M}$  gilt

$$a \prec b \vee b \prec a \vee a = b.$$

Nicht vollständige Ordnungen heißen **partiell**.

### Beispiel A - 7.3

Die übliche *Kleiner*-Relation  $<$  in  $\mathbb{R}$  und Untermengen ist eine strenge Ordnung und  $\leq$  die entsprechende reflexive Variante. Beide sind vollständig.

### Beispiel A - 7.4

Koordinatenvektoren  $(x, y)$  in Ebene werden durch

$$a = (x_1, y_1) \leq b = (x_2, y_2) \iff x_1 \leq x_2 \wedge y_1 \leq y_2$$

partiell geordnet.

### Beispiel A - 7.5

Die Enthaltenseinsbeziehung von Mengen

$$\mathcal{M} \prec \mathcal{N} \iff \mathcal{M} \subset \mathcal{N}$$

ist eine partielle nichtstrenge, d.h. reflexive Ordnung.

## Definition A-7.6

Das Alphabet  $\mathcal{A} = \{a, b, c, \dots, x, y, z\}$  ist vollständig geordnet durch Reihenfolge der Buchstaben in obiger Auflistung der Menge  $\mathcal{A}$ , z.B.  $c \prec x$ . Diese Ordnung kann erweitert werden zur **lexikographische Ordnung** auf der Menge  $\mathcal{A}^*$  aller Worte, die aus dem Alphabet  $\mathcal{A}$  gebildet werden können.

$$(a_1, a_2, \dots, a_n) \prec (b_1, b_2, \dots, b_m)$$

gilt genau dann wenn ein  $k \leq \min(m, n)$  existiert so dass

$$a_i = b_i \text{ für } i \leq k \quad \text{und} \quad (a_{k+1} < b_{k+1} \text{ oder } k = n < m).$$

## Beispiel A-7.7 (Telefonbuch)

... griewank  $\prec$  grünwald  $\prec$  ...  $\prec$  meier  $\prec$  meiers  $\prec$  ...

## Graphische Interpretation:

Betrachte die Elemente einer Menge  $\mathcal{M}$  mit strenger Ordnung  $\prec$  als Knoten eines Graphen mit der Kantenmenge  $\mathcal{K}$

Zwei Knoten  $a, b \in \mathcal{M}$  werden durch eine gerichtete Kante  $(a, b) \in \mathcal{K}$  verbunden wenn  $a$  bzgl. der Ordnung  $\prec$  vor  $b$  kommt und kein Knoten  $c$  dazwischen liegt, d.h.

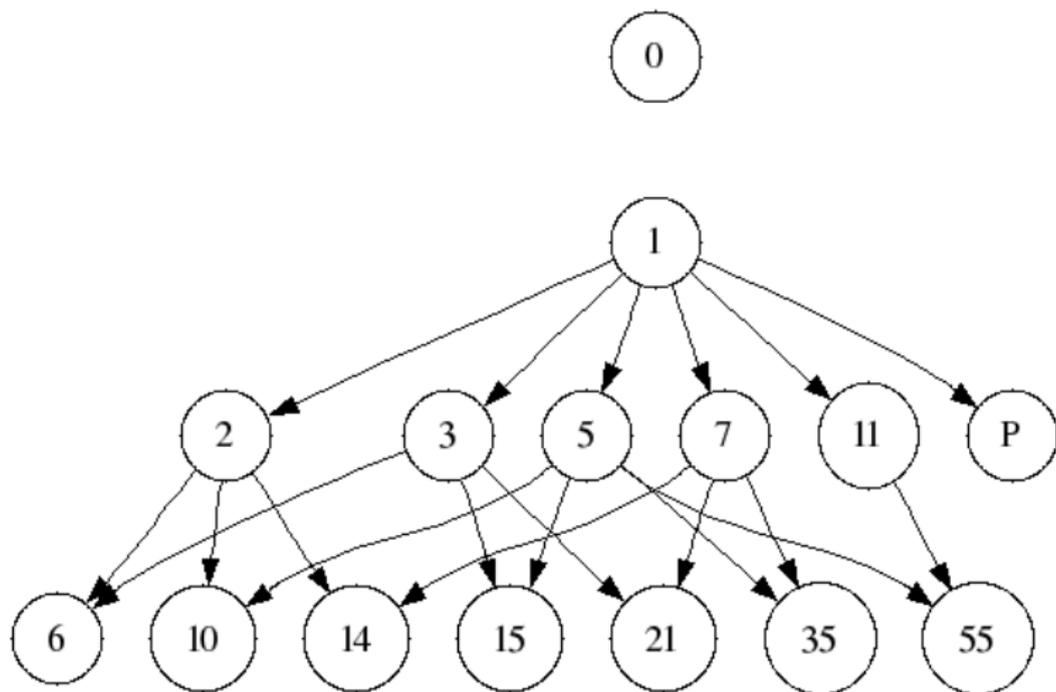
$$(a, b) \in \mathcal{K} \iff a \prec b \wedge a \neq b \wedge (a \prec c \prec b \implies c = a \vee c = b).$$

Dann erhalten wir einen

**DAG  $\equiv$  Directed Acyclic Graph.**

Dieser lässt sich immer so zeichnen daß alle Kanten eine negative vertikale Komponente haben.

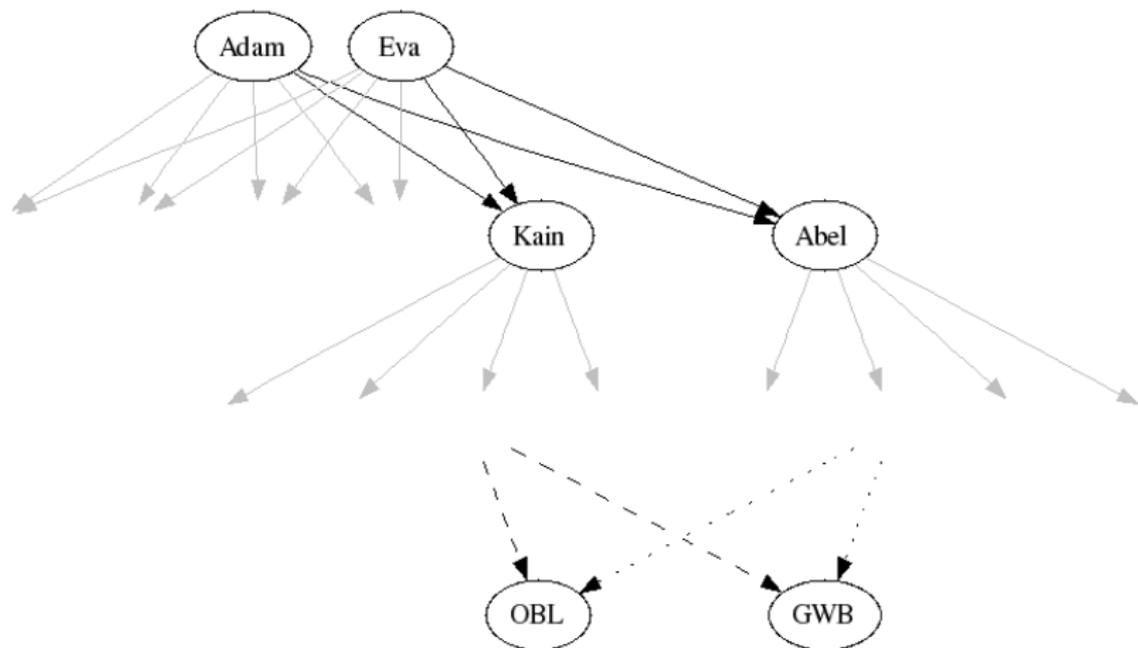
## Beispiel A - 7.8 (Teilbarkeit in $\mathbb{N}$ )



## Beispiel A - 7.9 (Stammbaum der Menschheit)

$a \prec b$  bedeutet:  $a$  ist Vorfahre von  $b$

$(a, b)$  bedeutet:  $b$  ist Kind von  $a$ , es gibt eine Kante von  $a$  zu  $b$  im DAG.



## Bemerkung:

Im Stammbaum der Menschheit ist die Frage zweier Personen:

„Wer war unser letzter gemeinsamer Vorfahre?“ im allgemeinen nicht eindeutig beantwortbar.

Theoretisch könnten z.B. sowohl Adam wie auch Eva letzte gemeinsame Vorfahren sein.

Diese Möglichkeit wird in *Verbände* genannten partiellen Ordnungen ausgeschlossen.

## A-8 Verbandstruktur und größter gemeinsamer Teiler

### Definition A-8.1 ( Verbandstruktur)

Eine partiell geordnete Menge  $\mathcal{M}$  heißt **Verband**, wenn es zu jedem Paar  $a, b \in \mathcal{M}$  eine **größte untere Schranke**  $c = \inf(a, b)$  und **kleinste obere Schranke**  $d = \sup(a, b)$  gibt, so daß für alle  $c', d' \in \mathcal{M}$  gilt

$$(c \prec a \wedge c \prec b) \wedge (c' \prec a \wedge c' \prec b \implies c' \prec c)$$

und

$$(d \succ a \wedge d \succ b) \wedge (d' \succ a \wedge d' \succ b \implies d' \succ d)$$

In der Literatur wird oft abgekürzt:

$$a \wedge b = \inf(a, b) \quad \text{und} \quad a \vee b = \sup(a, b)$$

Wir werden wegen der Gefahr der Verwechslung mit logischen Operationen diese Schreibweise vermeiden.

## Lemma A-8.2 (Rechenregeln in Verbänden)

- |       |  |                       |
|-------|--|-----------------------|
| (i)   | $\inf(a, a) = a \quad \wedge \quad \sup(a, a) = a$   | <b>Idempotenz</b>     |
| (ii)  | $\inf(b, a) = \inf(a, b) \quad \wedge \quad \sup(b, a) = \sup(a, b)$                       | <b>Kommutativität</b> |
| (iii) | $\inf(a, \inf(b, c)) = \inf(\inf(a, b), c)$<br>$\sup(a, \sup(b, c)) = \sup(\sup(a, b), c)$ | <b>Assoziativität</b> |
| (iv)  | $\inf(a, \sup(a, b)) = a \quad \wedge \quad \sup(a, \inf(a, b)) = a$                       | <b>Absorption</b>     |
| (v)   | $a \preceq b \iff \inf(a, b) = a \iff \sup(a, b) = b$                                      | <b>Konsistenz</b>     |

## Beispiel A - 8.3

$$\mathcal{M} = \mathcal{P}(A) = \{B : B \subset A\}, |\mathcal{M}| = 2^A$$

**Potenzmenge von A**

Für  $B, C \in \mathcal{P}(A)$  gilt:

▶  $B \prec C \iff B \subset C$

**Inklusion**

▶  $\inf(B, C) = B \cap C$

**Schnittmenge**

▶  $\sup(B, C) = B \cup C$

**Vereinigung**

## Beispiel A-8.4

$\mathcal{M} = \{0, 1\}$  mit der Booleschen Verknüpfung

$$\begin{cases} \text{inf} &= \textit{Konjunktion} \quad \wedge \\ \text{sup} &= \textit{Disjunktion} \quad \vee \end{cases}$$

inf	0	1
0	0	0
1	0	1

sup	0	1
0	0	1
1	1	1

## Beispiel A-8.5

$$\mathcal{M} = \mathbb{N}_+ = \mathbb{N} \setminus \{0\}:$$

$$a \prec b \iff a|b$$

$$\begin{aligned} \inf(a, b) = GGT(a, b) &= \max\{c \in \mathbb{N} : c|a \wedge c|b\} \\ \sup(a, b) = KGV(a, b) &= \min\{c \in \mathbb{N} : a|c \wedge b|c\} \end{aligned}$$

Hierbei kann Maximieren bzw. Minimieren bezüglich der üblichen Größenordnung in  $\mathbb{N}$  oder der Teilbarkeitsordnung vorgenommen werden.

### Beobachtung:

Falls ein größter gemeinsamer Teiler **GGT**( $a, b$ ) zweier Zahlen  $a, b \in \mathbb{N}_+$  tatsächlich existiert, erfüllt  $c = GGT(a, b)$  für alle  $c' \in \mathbb{Z}$

$$(c|a \wedge c|b) \wedge (c'|a \wedge c'|b \implies c'|c)$$

und ist dann wegen der Antisymmetrie der Teilbarkeitsrelation eindeutig.

## Satz A-8.6 (Existenz des GGT und KGV)

Für  $a, b \in \mathbb{N}_+$  gibt es  $s, t \in \mathbb{Z}$ , so daß

$$\text{GGT}(a, b) = s * a + t * b$$

sowie

$$\text{KGV}(a, b) = (a * b) / \text{GGT}(a, b)$$

### Bemerkung:

Der obige Existenzsatz ist nicht konstruktiv, da er kein Verfahren angibt, das den GGT berechnet.

Dazu benutzt man **Euklid's Algorithmus**, welcher rekursiv das vorgegebene Berechnungsproblem auf ein „kleineres“ Problem reduziert.

## A-9 Euklidischer Algorithmus und Anwendungen

### Lemma A-9.1

$$(i) \quad 0 < a \implies GGT(0, a) = a$$

$$(ii) \quad 0 < a < b \implies GGT(a, b) = GGT(b \bmod a, a)$$

### Euklidischer Algorithmus:

**Input:**  $a, b \in \mathbb{N}_+$  mit  $0 < a < b$

$r := b \bmod a$

WHILE ( $0 \neq r$ )

$b := a$

$a := r$

$r := b \bmod a$

**Output:**  $a$

### Lemma A-9.2 (Endlicher Abbruch)

Für alle Eingaben  $a, b \in \mathbb{N}_+$  mit  $a \leq b$  ergibt der Algorithmus nach endlichen vielen Durchläufen der WHILE-Schleife den  $GGT(a, b)$  als Ergebnis.

Beispiel A - 9.3 ( $a = 228$ ,  $b = 612$ ,  $GGT(228, 612) = 12$ )

i	b	a	r	q
0	612	228	156	2
1	228	156	72	1
2	156	72	12	2
3	72	12	0	6

## Frage:

Läßt sich die Zahl der Schritte a priori, d.h. durch die Größe von  $a$  und  $b$ , beschränken?

## Lemma A-9.4

Die maximale Schrittzahl  $k$  erfüllt die Bedingung

$$(3/2)^k \leq a + b \quad (\text{initial})$$

was äquivalent ist zu

$$k \leq \frac{1}{\lg_2(3/2)} \lg_2(a + b)$$

wobei  $\frac{1}{\lg_2(3/2)} \approx 1.71$

## Beispiel A-9.5

Für Beispiel  $GGT(228, 612) = 12$  gilt: Es werden  $3 \leq k_{\max} \approx 16.6$  Schritte benötigt. Was zeigt, dass die Schranke nicht sehr scharf (d.h. nicht sehr gut) ist.

## Bemerkung:

Die logarithmische Abhängigkeit der Schrittzahl von der Ausgangsgröße  $a + b$  des Problems ist recht vorteilhaft und wird hier wie bei vielen algorithmischen Problemen, wie z.B. dem Sortieren, durch Aufspaltung in kleinere Aufgaben ähnlicher Art erreicht.

Dabei wird davon ausgegangen, daß der eigentliche Rechenaufwand pro Schritt (also die Auswertung von  $b \bmod a$ ) konstant sei.

Allerdings ist diese implizite Annahme nicht ganz korrekt:

Wie wir später sehen werden, wächst dieser Aufwand (genau wie bei Addition und Multiplikation auch) mit  $\lg(a + b)$ . Der genaue Aufwand hängt von der Zahldarstellung und der entsprechenden Datenstruktur ab.

## Lemma A-9.6 (Existenz und Berechnung von Inversen in $\mathbb{Z}_b$ )

Die Zahl  $a < b$  hat genau dann ein multiplikatives Inverses  $a^{-1}$  im Restklassenring  $\mathbb{Z}_b$ , wenn  $a$  und  $b$  **relativ prim** sind, d.h.  $\text{GGT}(a, b) = 1$ .  
Dann gilt

$$a^{-1} = s \bmod b \quad \text{für} \quad 1 = s * a + t * b$$

### Bemerkung

Bislang haben wir multiplikative Inverse von  $a$  unter den Potenzen  $a^k \bmod b$  für  $k = 0, 1, \dots$  gesucht, was spätestens für  $k = b - 2$  zum Erfolg führen muss (Satz A-5.6). Jetzt können wir den Euklidischen Algorithmus so erweitern, dass er den Koeffizienten  $s$  gleich mitberechnet und damit das Inverse  $a^{-1}$  von  $a$  mit einem Aufwand proportional zu  $\log_2 b$  ergibt.

## Herleitung des Erweiterten Euklidischen Algorithmus

Im Euklidischen Algorithmus wird jeweils aus den aktuellen Werten  $a > 0$  und  $b > a$  das Residuum  $r = b - a * q < a$  berechnet. Wir bezeichnen nun die Ausgangswerte von  $a$  und  $b$  mit  $a_0$  und  $b_0$  und suchen jeweils Darstellungen

$$a \equiv s_a * a_0 \pmod{b_0}, \quad b \equiv s_b * a_0 \pmod{b_0}, \quad r \equiv s_r * a_0 \pmod{b_0}$$

Ganz am Anfang gelten diese Beziehungen mit  $s_a = 1$  und  $s_b = 0$ . Aus  $r = b - a * q$  folgt zudem, dass

$$s_r = s_b - q * s_a \quad \text{gilt.}$$

Im Übergang zum nächsten Schritt wird das Paar  $(a, b)$  durch das Paar  $(r, a)$  ersetzt. Dabei muss gleichzeitig  $(s_a, s_b)$  durch  $(s_r, s_a)$  ersetzt werden. Analog können Zahlen  $t_a, t_b, t_r$  definiert werden, so dass  $a - s_a * a_0 = t_a * b_0$ , etc. gelten.

Bezeichnen wir jeweils  $s_a$  mit  $s$  und  $s_b$  mit  $v$  so ergibt sich die folgende Prozedur.

## Erweiterter Euklidischer Algorithmus:

**Input:**  $a, b \in \mathbb{N}_+$  mit  $0 < a < b$   
 $r := b \bmod a; \quad s = 1; \quad v = 0;$   
WHILE ( $0 \neq r$ )  
     $q := (b - r)/a$   
     $b := a$   
     $a := r$   
     $t := v - q * s$   
     $v := s$   
     $s := t$   
     $r := b \bmod a$

**Output:**  $a, s \bmod b$

Beispiel A-9.7 ( $a = 16, b = 21$ )

i	q	b	a	v	s	r
0	-	21	16	0	1	5
1	1	16	5	1	-1	1
2	3	5	1	-1	4	0

## In Worten:

Der erweiterte Euklidische Algorithmus liefert uns  $GGT(16, 21) = 1$  (der letzte Wert von  $a$ ) und  $s = 4$ . Also existiert die Inverse von 16 in  $\mathbb{Z}_{21}$  und ist gegeben durch 4. Die Probe ergibt tatsächlich

$$16 * 4 \bmod 21 = 64 \bmod 21 = 1.$$

## Bemerkung

Die Fähigkeit, modulare Inverse effizient zu berechnen, kann benutzt werden, um die nach dem Chinesischen Restsatz existierenden Lösungen von Kongruenzgleichungen zu finden.

Wir betrachten zunächst ein Paar von Gleichungen

$$x \bmod m = r \quad \text{und} \quad x \bmod n = s,$$

wobei naturgemäß  $r < m$  und  $s < n$  sein müssen. Man sieht sofort, dass mit irgendeinem  $x$  auch alle ganzen Zahlen der Form  $x + k * \text{KGV}(m, n)$  für beliebiges  $k \in \mathbb{Z}$  Lösungen sind.

Nur falls  $\text{KGV}(m, n) = m * n$  und äquivalenterweise  $\text{GGT}(m, n) = 1$  gilt, kann man erwarten, dass es zu jedem möglichen Restepaar  $(r, s)$  genau eine Lösung  $x$  zwischen 0 und  $n * m$  gibt.

Dies ist in der Tat der Fall, wie wir im folgenden herleiten werden.

## Iterative Herleitung der Lösung

Offensichtlich ist  $x = r$  eine Lösung der ersten Gleichung. Um deren Gültigkeit nicht zu verletzen dürfen wir ein beliebiges Vielfaches von  $m$  zu  $r$  addieren, also  $x = r + q * m$ . Dabei ist  $q$  so zu wählen, dass die zweite Gleichung erfüllt ist, d.h.

$$s = (r + q * m) \bmod n = [r \bmod n + (m \bmod n) * (q \bmod n)] \bmod n$$

und somit

$$(s - r) \bmod n = [(m \bmod n) * (q \bmod n)] \bmod n$$

Aus der Voraussetzung, dass  $m$  und  $n$  relativ prim sind, ergibt sich nun die Existenz einer Inversen  $c \in \mathbb{Z}$  von  $m \bmod n$  so dass  $c * m \bmod n = 1$ .

Multiplizieren wir die obige Gleichung mit diesem  $c$ , so erhalten wir mit Hilfe der Assoziativität in  $\mathbb{Z}$  als mögliche Wahl für  $q$

$$q = [c * (s - r)] \bmod n.$$

Daraus ergibt sich die folgende Aussage:

## Lemma A-9.8

Vorrausgesetzt  $\text{GGT}(m, n) = 1$  und  $c = (m \bmod n)^{-1}$ , dann ist die Zahl

$$x = (r + [c * (s - r) \bmod n] * m) \bmod (m * n)$$

die einzige Lösung zwischen 0 und  $n * m - 1$  für die beiden Gleichungen

$$x \bmod m = r \quad \text{und} \quad x \bmod n = s.$$

## Beispielrechnung

Für  $m = 9$ ,  $r = 3$ ,  $n = 7$  und  $s = 6$  erhalten wir die Gleichungen

$$x \bmod 9 = 3 \quad \text{und} \quad x \bmod 7 = 6.$$

Sie sind sicherlich lösbar, da  $\text{GGT}(9, 7) = 1$ , ja 7 sogar eine Primzahl ist. Deswegen können wir die Inverse von  $m \bmod n = 9 \bmod 7 = 2$  in  $\mathbb{Z}_7$  einfacherweise nach dem kleinen Fermat'schen Satz A-5.6 auswerten.

$$2^{-1} = 2^{7-2} \bmod 7 = 32 \bmod 7 = 4$$

Probe:  $4 * 2 \bmod 7 = 1$ .

Die Lösung ergibt sich nach der obigen Formel als

$$\begin{aligned} x &= (3 + [4 * (6 - 3) \bmod 7] * 9) \bmod 63 \\ &= (3 + 45) \bmod 63 \\ &= 48 \end{aligned}$$

Probe:  $48 \bmod 9 = 3$  und  $48 \bmod 7 = 6$  wie erwünscht.

## Direkte Herleitung

Will man bei der Lösung jegliche Abhängigkeit von der Reihenfolge der Gleichungen vermeiden, kann man den folgenden direkten Ansatz benutzen:

$$x = (x_m * m + x_n * n) \bmod (n * m) \quad \text{mit} \quad x_m, x_n \in \mathbb{Z}$$

Daraus ergeben sich für  $x_m$  und  $x_n$  die Gleichungen

$$x \bmod m = (x_n * n) \bmod m = r \quad \text{und} \quad x \bmod n = (x_m * m) \bmod n = s$$

Mit  $c_n < m$  die Inverse von  $n$  in  $\mathbb{Z}_m$  and  $c_m < n$  die Inverse von  $m$  in  $\mathbb{Z}_n$  erhalten wir einfach

$$x_m = c_m * s < m * n \quad \text{und} \quad x_n = c_n * r < n * m$$

Hier erhält man für  $x$  zunächst einen Wert zwischen 0 und  $2 * n * m$ , von dem man gegebenenfalls einmal  $n * m$  abziehen muss um im Intervall  $0, 1, \dots, n * m - 1$  zu landen.

## Verallgemeinerung auf $n > 2$ Gleichungen

Betrachte ein System von Kongruenzen

$$x \bmod m_i = r_i < m_i \quad \text{für } i = 1 \dots n$$

unter der Voraussetzung, dass die  $m_i$  paarweise relativ prim sind, d.h.

$$\text{GGT}(m_i, m_j) = 1 \quad \text{für } 1 \leq i < j \leq n$$

Mit der Abkürzung  $M = \prod_{j=1}^n m_j$  ergibt sich zunächst:

### Lemma A-9.9

Für alle  $i = 1 \dots n$  ist das folgende Produkt relativ prim zu  $m_i$

$$M_i = \prod_{j=0}^{i-1} m_j \prod_{j=i+1}^n m_j = M/m_i,$$

aber ein Vielfaches aller anderen  $m_j$  mit  $j \neq i$ . Es gilt also

$$\text{GGT}(M_i, m_j) = \begin{cases} 1 & \text{falls } j = i \\ m_j & \text{falls } j \neq i \end{cases}$$

und somit

$$M_i \bmod m_j = 0 \quad \text{falls } j \neq i.$$

## Explizite Lösung

Nach obigem Lemma existieren Inverse  $c_i < m_i$  von  $(M_i \bmod m_i)$  in  $\mathbb{Z}_{m_i}$ , mit deren Hilfe wir eine Lösung direkt hinschreiben können:

$$\begin{aligned} x &= [r_1 * c_1 * M_1 + r_2 * c_2 * M_2 + \dots + r_n * c_n * M_n] \bmod M \\ &= \left[ \sum_{i=1}^n r_i * c_i * M_i \right] \bmod M \end{aligned}$$

$$\begin{aligned} \text{Probe : } x \bmod m_j &= \left[ \sum_{i=1}^n r_i * c_i * M_i \right] \bmod M \bmod m_j \\ &= \left[ \sum_{i=1}^n r_i * c_i * M_i \right] \bmod m_j \\ &= r_j * (c_j * M_j \bmod m_j) \\ &= r_j \end{aligned}$$

In den vorangegangenen Abschnitten wurden folgende Regeln benutzt:

### Lemma: (Einige) Rechenregeln für mod

- (i)  $n \mid m \implies (a \bmod m) \bmod n = a \bmod n$
- (ii)  $(a \pm b) \bmod n = (a \bmod n \pm b \bmod n) \bmod n$
- (iii)  $(a * b) \bmod n = (a \bmod n * b \bmod n) \bmod n$

### In Worten:

Die „äußere“ Anwendung von mod auf eine Summe/Differenz/Produkt kann nach „innen“, also auf die einzelnen Operanden, gezogen werden. Allerdings **muss** mod auf das entsprechende Resultat immer auch äußerlich angewandt werden.

## A-10 Darstellungen ganzer Zahlen

### Beobachtung:

Es ist wohl bekannt, daß es eine unendliche monoton steigende Folge von Primzahlen

$$p_1=2 < p_2=3 < p_3=5 < p_4=7 < \dots < p_8=19 < \dots$$

gibt. Mit ihrer Hilfe ergibt sich folgende Darstellung:

### Satz A-10.1 (Primzahlzerlegung)

*Jede natürliche Zahl  $a > 1$  hat eine eindeutige Darstellung der Form*

$$a = \prod_{j=0}^{\infty} p_j^{e_j} = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} p_{n+1}^0 p_{n+2}^0 \dots,$$

*wobei nur endlich viele der Exponenten  $e_j \in \mathbb{N}$  positiv (d.h. nicht null) sind.*

## Bemerkung:

Man könnte auf die Idee kommen, positive ganze Zahlen auf Rechnern als Folge ihrer Exponenten  $(e_j)_{j \leq n}$  abzuspeichern. Läßt man auch negative  $e_j$  zu, so ergeben sich sogar alle rationalen Zahlen.

Für **Produkt** und **Quotient** von  $a = \prod_{j=1}^n p_j^{e_j}$  und  $a' = \prod_{j=1}^{n'} p_j^{e'_j}$  gilt

$$a * a' = \prod_{j=1}^{\max(n, n')} p_j^{e_j + e'_j} \qquad a / a' = \prod_{j=1}^{\max(n, n')} p_j^{e_j - e'_j}$$

wobei  $e_j$  und  $e'_j$  für  $j > n$  bzw  $j > n'$  als Null angenommen werden.

Auch *GGT* und *KGV* lassen sich billig berechnen (siehe Übung), die Berechnung von Summen und Differenz gestaltet sich jedoch ziemlich aufwendig.

## Lemma A-10.2 (Zahldarstellung zur Basis $b$ )

Für  $b \in \mathbb{N}_+$  eine feste Basis (Radix) läßt sich jede beliebige positive Zahl  $a \in \mathbb{N}$  mit Hilfe von  $n + 1$  Ziffern  $a_j \in \{0, 1, \dots, b - 1\}$  ( $j = 0, \dots, n$ ,  $b^n \leq a < b^{n+1}$ ) eindeutig darstellen:

$$\begin{aligned} a &= (a_n a_{n-1} a_{n-2} \dots a_1 a_0)_b \\ &= \sum_{j=0}^n a_j b^j \\ &= a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0, \end{aligned}$$

wobei die führende Ziffer  $a_n \neq 0$  gewählt werden muss.

### Beispiel A - 10.3

#### Dezimalsystem

*Primaten mit 10 Fingern, Taschenrechner*

Basis  $b=10$ , Ziffern  $\{0, 1, 2, \dots, 8, 9\}$

### Beispiel A - 10.4

#### Binärsystem

*Computerspeicher*

Basis  $b=2$ , Ziffern  $\{0, 1\}$

### Beispiel A - 10.5

**Hexadezimalsystem** *Computerausgabe (Hexdump), 1 Byte  $\hat{=}$  2 Ziffern*

Basis  $b=16$ , Ziffern  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$

## Algorithmus: Darstellung von $a$ zur Basis $b$

**Input:**  $a \in \mathbb{N}$ ,  $b \in \mathbb{N}_+$

$i = 0$

WHILE ( $0 \neq a$ )

$a_i := a \bmod b$

$a := (a - a_i) / b$

$i := i + 1$

**Output:**  $n = i - 1$ ,  $(a_n, a_{n-1}, \dots, a_0)_b$  – Koeffizienten von  $a$  bzgl.  
Basis  $b$

Beispiel A - 10.6 (  $a = (788)_{10} = (???)_3$      $b = 3$  )

$i$	0	1	2	3	4	5	6
$a$	788	262	87	29	9	3	1
$a \bmod b$	2	1	0	2	0	0	1
$(a - a_i)/b$	262	87	29	9	3	1	0
$b^i$	1	3	9	27	81	243	729
$a_i$	2	1	0	2	0	0	1

$$(788)_{10} = (1002012)_3 = 1 \cdot 729 + 2 \cdot 27 + 1 \cdot 3 + 2 \cdot 1$$

## Bemerkung:

Es gibt verschiedene clevere Tricks, um negative Zahlen in das Zahlensystem einzuführen. Bei binärer Darstellung ist es das Einfachste, ein führendes Vorzeichenbit (Signbit) zu benutzen.

## Algorithmus: Addition für Basis $b$

$$\begin{array}{r} x = (x)_b = (x_n, x_{n-1}, \dots, x_1, x_0) \\ + \\ y = (y)_b = (y_n, y_{n-1}, \dots, y_1, y_0) \\ || \\ z = (z)_b = (z_n, z_{n-1}, \dots, z_1, z_0) \end{array}$$

**Input:**  $(x)_b, (y)_b$

$q = 0$

FOR  $i := 0, 1, 2, \dots$

$r := (x_i + y_i + q) \bmod b$

$z_i := r$

$q := (x_i + y_i + q - r) / b$

**Output:**  $(z)_b = (x)_b + (y)_b$  ist Summe von  $x$  und  $y$

Hierbei ist  $q$  die Übertragsziffer.

Der Aufwand wächst offensichtlich linear mit

$$n = \max \{ \log_b x, \log_b y \}$$

## Multiplikationsregel

$$\begin{aligned}x * y &= (x)_b * (y)_b = \sum_{i=0}^n x_i b^i \sum_{j=0}^m y_j b^j \\&= (x_0 + x_1 b + x_2 b^2 + \dots + x_n b^n) * (y_0 + y_1 b + y_2 b^2 + \dots + y_m b^m) \\&= x_0 y_0 + (x_0 y_1 + x_1 y_0) b + (x_0 y_2 + x_1 y_1 + x_2 y_0) b^2 + \dots + b^{m+n} \\&= \sum_{k=0}^{n+m} z_k b^k \quad \text{mit} \quad z_k = \sum_{j=0}^k x_j y_{k-j}\end{aligned}$$

Anschließend müssen die  $z_k$  wie bei der schriftlichen Multiplikation in Potenzen von  $b$  zerlegt und die Anteile auf die höheren Terme verteilt werden.

## Beispiel A - 10.7 (Oktale Multiplikation)

$$(303)_8 = 3 \cdot 8^0 + 0 \cdot 8^1 + 3 \cdot 8^2 = (195)_{10}$$

$$(52)_8 = 2 \cdot 8^0 + 5 \cdot 8^1 + 0 \cdot 8^2 = (42)_{10}$$

$$\begin{aligned}(303)_8 * (52)_8 &= 6 \cdot 8^0 + (17)_8 \cdot 8^1 + 6 \cdot 8^2 + (17)_8 \cdot 8^3 \\ &= 6 \cdot 8^0 + 7 \cdot 8^1 + 7 \cdot 8^2 + 7 \cdot 8^3 + 1 \cdot 8^4 \\ &= (8190)_{10}\end{aligned}$$

### Bemerkung

Betrachtet man die Addition und Multiplikation von Ziffern mit eventuellem Übertrag als Kosteneinheit, so wächst der Aufwand quadratisch mit der Gesamtanzahl der Ziffern. Das ähnelt der im folgenden beschriebenen Polynommanipulationen.

## A-11 Polynome als Funktionen

### Definition A-11.1 (Polynom)

Einen Ausdruck der Form

$$P(x) = c_0x^0 + c_1x^1 + c_2x^2 + \dots + c_nx^n$$

nennt man **Polynom**, wobei  $x$  eine unbekannte Variable bezeichnet und die **Koeffizienten**  $c_i$  für  $i = 0..n$  einem Ring  $\mathcal{R}$  angehören.

Die nichtnegative ganze Zahl  $n = \text{deg}(\mathcal{P})$  heißt der **Grad** oder die **höchste Potenz** (degree) des Polynoms.

Für  $n = 1, 2, 3$  spricht man von **linearen, quadratischen**, bzw. **kubischen** Polynomen.

Die Zahl  $\text{ord}(\mathcal{P}) = \text{deg}(\mathcal{P}) + 1 = n + 1$  heißt **Ordnung** von  $\mathcal{P}$  und gibt die Zahl der Koeffizienten  $c_0, c_1, \dots, c_n$  an.

## Warnung:

$\text{grad}(\mathcal{P})$  bezeichnet im Englischen wie im Deutschen häufig den Gradienten, d.h. den Vektor der partiellen Ableitungen von Polynomen und anderen Funktionen.

## Beispiel A - 11.2

Kubisches Polynom über dem Koeffizientenring  $\mathbb{Z}$ :

$$1 - x + 2x^2 + 17x^3$$

## Beispiel A - 11.3

Quadratisches Polynom über dem Koeffizientenring  $\mathbb{R}$ :

$$\sqrt{2} + \pi x - \frac{1}{2} e x^2$$

## Bemerkung:

Ersetzt man  $x$  durch ein Element von  $\mathcal{R}$  oder eines Oberrings  $\mathcal{R}' \supset \mathcal{R}$ , so erhält man als  $P(x)$  wiederum ein Element von  $\mathcal{R}$  oder  $\mathcal{R}'$ .

Durch diese „**Auswertung an der Stelle  $x$** “ wird  $\mathcal{P}$  zu einer Funktion bzw. Abbildung von  $\mathcal{R}$  nach  $\mathcal{R}$  oder  $\mathcal{R}'$  nach  $\mathcal{R}'$ .

## Lemma A-11.4 (Horner Schema)

*Die Auswertung eines Polynomes mit Hilfe der Klammerung*

$$P(x) = c_0 + x * (c_1 + x * ( \dots (c_{n-1} + x * c_n) \dots ))$$

$\underbrace{\hspace{10em}}_{n-1}$

*verlangt lediglich  $n$  Multiplikationen und ebenso viele Additionen.*

## Algorithmus Horner-Schema:

**Input:**  $x \in \mathcal{R}, c_i \in \mathcal{R}, i = 0, \dots, n = \deg(P(x))$

$$y = 0$$

FOR  $i := n, n-1, \dots, 1, 0$

$$y := c_i + x * y$$

**Output:**  $y = P(x)$  ... Wert des Polynoms an der Stelle  $x \in \mathcal{R}$

### Beispiel A-11.5

$$P(x) = 1 - x + 2x^2 + 5x^3 = 1 + x * (-1 + x * (2 + 5 * x))$$

Für  $x = \frac{1}{2}$

i	3	2	1	0
$c_i$	5	2	-1	1
y	5	$\frac{9}{2}$	$\frac{5}{4}$	$\frac{13}{8}$

## Bemerkung

Polynome sind als relativ einfache Funktionsmodelle nicht nur bei Algebraikern sondern vorallem auch bei Ingenieuren populär (*Vorsicht: Patentanspruch*).

Sie können sehr einfach gespeichert und manipuliert werden.

Allgemeinere Funktionen lassen sich häufig sehr gut durch Polynome oder besser noch Brüche von Polynomen annähern.

Ganz wesentlich ist dabei die folgende Interpolationseigenschaft.

## Satz A - 11.6 (Lagrange-Interpolation)

Sei  $\mathcal{R} = \mathbb{R}$  oder ein anderer Körper. Dann gilt:

(i) Es existiert zu jeder endlichen Folge von Wertepaaren

$$(x_i, y_i) \in \mathcal{R} \times \mathcal{R} \quad \text{für } i = 0, 1, \dots, n$$

mit unterschiedlichen „Abzissenwerten“

$$x_i \neq x_j \quad \text{bei } i \neq j$$

ein Interpolationspolynom  $P(x)$  vom Grad  $\leq n$ , so daß

$$P(x_i) = y_i \quad \text{für } i = 0, 1, \dots, n.$$

(ii) Dieses Polynom ist eindeutig und läßt sich darstellen als

$$P(x) = \sum_{i=0}^n y_i \underbrace{\frac{(x - x_0) \dots (x - x_{i-1})(x - x_{i+1}) \dots (x - x_n)}{(x_i - x_0) \dots (x_i - x_{i-1})(x_i - x_{i+1}) \dots (x_i - x_n)}}_{\equiv P_i(x)}$$

(iii) Insbesondere folgt aus  $y_i = 0$  für  $i = 0, \dots, n$ , dass alle Koeffizienten  $c_i$  in  $P(x) = c_0 + c_1x + c_2x^2 + \dots$  verschwinden, d.h. es gilt

$$c_i = 0 \quad \text{für } i = 0, \dots, n.$$

## Beweis:

- (i) Die Existenz folgt aus der Gültigkeit der Darstellung (ii), welche zunächst geprüft wird. Die Ausdrücke

$$P_i(x) = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)} \quad \text{für } i = 0, \dots, n$$

sind genau so definiert, dass

$$P_i(x_j) = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

Deshalb gilt wie erwünscht

$$P(x_j) = \sum_{i=0}^n y_i P_i(x_j) = y_j.$$

Außerdem kann man durch Ausmultiplizieren feststellen, dass die höchste Potenz von  $P_i(x)$  jeweils gegeben ist durch den Term

$$x^n / \prod_{j \neq i} (x_i - x_j).$$

Also ist  $P$  tatsächlich ein Polynom vom Grad  $\deg(P) \leq n$ . In speziellen Fällen können sich die höchsten Terme aufheben, so dass  $\deg(P) < n$  eintritt.

(ii) Ergibt sich aus (iii) wie folgt. Falls die Polynome

$$P(x) = \sum_{j=0}^n p_j x^j \quad \text{und} \quad Q(x) = \sum_{j=0}^n q_j x^j$$

beide die Paare  $(x_j, y_j)$  interpolieren, so gilt für ihre Differenz

$$R(x) = P(x) - Q(x) = \sum_{j=0}^n (p_j - q_j) x^j$$

insbesondere

$$R(x_j) = P(x_j) - Q(x_j) = y_j - y_j = 0 \quad \text{für } i = 0, \dots, n.$$

Also folgt aus der letzten Aussage (iii) dass

$$p_j - q_j = 0 \quad \text{für } j = 0, \dots, n.$$

und damit die behauptete Eindeutigkeit.

(iii) Beweis folgt später (mittels Polynomdivision)

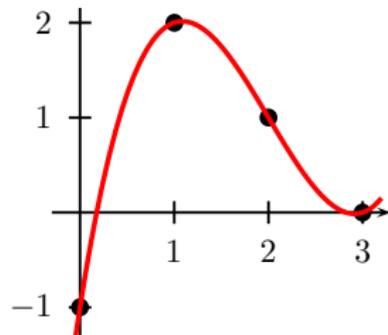


## Beispiel – Lagrangepolynom

$x_i$	0	1	2	3
$y_i$	-1	2	1	0

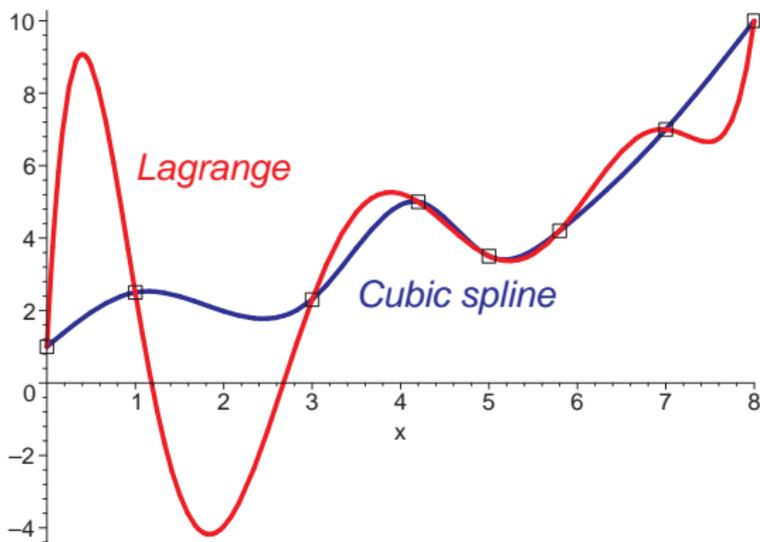
$$\begin{aligned}
 P(x) = & -1 \cdot \frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)} \\
 & + 2 \cdot \frac{(x-0)(x-2)(x-3)}{(1-0)(1-2)(1-3)} \\
 & + 1 \cdot \frac{(x-0)(x-1)(x-3)}{(2-0)(2-1)(2-3)} \\
 & + 0 \cdot \frac{(x-0)(x-1)(x-2)}{(3-0)(3-1)(3-2)}
 \end{aligned}$$

$$P(x) = \frac{2}{3}x^3 - 4x^2 + \frac{19}{3}x - 1$$



## Warnung:

Interpolationspolynome höherer Ordnung können zwischen den vorgegebenen Datenpunkten *sehr stark oszillieren*, deshalb wendet man in der Numerik lieber aus Polynomen niederer Ordnung zusammengesetzte Funktionsmodelle an.  $\implies$  (Kubische) Splines, Finite Elemente.



## Beobachtung zur Nullstellenberechnung

Wie bei Funktionen allgemein ergibt sich auch bei Polynomen häufig die Aufgabe deren **Nullstellen**  $x_j$  für  $j = 1, 2, \dots, m$  zu bestimmen. D.h. man sucht die Werte  $x = x_j$ , die die folgende Gleichung lösen:

$$P(x) = 0$$

Die Nullstellen von Polynomen werden auch deren **Wurzeln** genannt. Wie wir später sehen werden, kann ein Polynom  $P(x)$  über einem Körper nur  $m \leq n = \deg(P)$  unterschiedliche Wurzeln haben.

## Beispiel A - 11.7

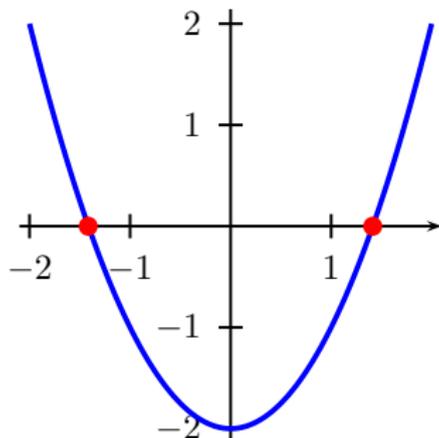
$$P(x) = x^2 - 2 = 0$$

hat die Lösungen  $x_{1,2} = \pm\sqrt{2}$ .

Beide Werte sind **irrational**, d.h.sie gehören nicht zum Körper der rationalen Zahlen  $\mathbb{Q}$ .

Ihre Berechnung gelingt deshalb immer nur annäherungsweise, was eigentlich das Verständnis der reellen bzw. komplexen Zahlen verlangt.

Vorerst benutzen wir nur die folgende Verallgemeinerung.



## Definition A-11.8 (Radikale)

Für jede natürliche Zahl  $n > 0$  und jede positive reelle Zahl  $a > 0$  hat die Gleichung

$$P(x) = x^n - a = 0$$

genau eine mit  $\sqrt[n]{a}$  bezeichnete positive Wurzel, die **Radikal** genannt wird.

## Bemerkung

Da man Radikale zu verstehen glaubte, hat man jahrhundertlang versucht die Wurzeln allgemeiner Polynome durch sie auszudrücken. Das gelingt zum Beispiel im quadratischen Fall  $n = 2$  wie folgt.

## Lemma A-11.9 (Lösung einer quadratischen Gleichung)

*Das Polynom*

$$P(x) = \alpha x^2 + \beta x + \gamma \quad \text{mit } \alpha, \beta, \gamma \in \mathbb{R}$$

*hat im Falle  $4\gamma\alpha \leq \beta^2$  die reellen Wurzeln*

$$x_{1,2} = -\frac{1}{2\alpha} \left[ \beta \pm \sqrt{\beta^2 - 4\alpha\gamma} \right]$$

## Lemma A-11.10 (Explizite Lösung einer kubischen Gleichung)

Das kubische Polynom

$$P(x) = x^3 + \gamma x + \delta \quad \text{mit } \gamma, \delta \in \mathbb{R}$$

immer mindestens eine reelle Lösung, die sich im Falle  $\gamma \geq -3\sqrt[3]{\frac{1}{4}\delta^2}$  nach der **Cardanschen Formel** ausdrücken lässt als

$$x_1 = u_+ + u_- \quad \text{mit} \quad u_{\pm} = \sqrt[3]{-\frac{\delta}{2} \pm \sqrt{\left(\frac{\gamma}{3}\right)^3 + \left(\frac{\delta}{2}\right)^2}}$$

Weitere Nullstellen lassen sich dann als Lösung einer quadratischen Gleichung nach der später diskutierten *Abspaltung eines Linearfaktors* berechnen.

## Bemerkung

Die obige Aussage setzt voraus, dass der führende, kubische Koeffizient gleich eins ist und der quadratische Koeffizient verschwindet. Diese Normalform lässt sich für ein allgemeines kubisches Polynom

$$P(x) = \alpha x^3 + \beta x^2 + \gamma x + \delta$$

immer durch folgende Transformation erreichen:

Zunächst dividiert man alle vier Terme des Polynomes durch  $\alpha$ . Dann wird  $x$  durch  $\tilde{x} - \beta/(3 * \alpha)$  ersetzt, wodurch der quadratische Term wegfällt. Von den für  $\tilde{x}$  erhaltenen Lösungen muss dann am Ende jeweils  $\beta/(3 * \alpha)$  abgezogen werden, um die entsprechende Nullstelle von  $x$  für die Ausgangsgleichung zu erhalten.

## Schlussbemerkung zur Nullstellensuche

Während es auch für Gleichungen 4. Ordnung noch explizite Lösungsformeln gibt, zeigte der geniale norwegische Mathematiker Abel mit algebraischen Methoden, dass die Wurzeln von Polynomen vom Grad  $n \geq 5$  sich im allgemeinen nicht mehr durch Radikale ausdrücken lassen.

Aus heutiger Sicht ist die Suche nach solchen, nur theoretisch expliziten Ausdrücken sowieso für praktische Berechnungen nutzlos. Schon die Cardanschen Formeln kommen selten zur Anwendung, da die Anwendung der Newton-Methode zur iterativen Berechnung von Nullstellen im allgemeinen einfacher, effizienter und häufig sogar genauer ist.

Schon die Auswertung der Radikale  $\sqrt[n]{a}$  erfolgt auf modernen Rechnern mit der Newton-Methode. Letztlich geht es meistens nicht darum die Wurzeln eines einzelnen Polynomes zu bestimmen, sondern mehrere nichtlineare Gleichungen in mehreren Variablen simultan zu lösen.

## A-12 Der Ring der Polynome

### Beobachtung:

Die Menge aller Polynome in  $x$  über einem Ring  $\mathcal{R}$  wird mit  $\mathcal{R}[x]$  bezeichnet. Sie bildet selbst einen kommutativen Ring. Hierbei sind Addition und Multiplikation von  $C(x) = \sum_{j=0}^n c_j x^j$  und  $D(x) = \sum_{j=0}^m d_j x^j$  mit  $c_n \neq 0 \neq d_m$  und  $m, n \in \mathbb{N}$  definiert als

$$E(x) = C(x) + D(x) = \sum_{j=0}^{\max(m,n)} e_j x^j \quad \text{mit} \quad e_j = c_j + d_j \quad \text{für} \quad j \leq \max(m, n),$$

– dabei wird formal  $c_j = 0$  für  $j > m$  und  $d_j = 0$  für  $j > n$  gesetzt – und

$$E(x) = C(x) * D(x) = \sum_{j=0}^{n+m} e_j x^j \quad \text{mit} \quad e_j = \sum_{i=0}^j c_i * d_{j-i} .$$

Wie zuvor schreiben wir  $\deg(C) = n$  und  $\deg(D) = m$ .

## Lemma A-12.1

Im Ring  $\mathcal{R}[x]$  gilt:

- (i)  $0 = 0 \cdot x^0 + 0 \cdot x^1 + \dots$  **Nullelement**
- (ii)  $1 = 1 \cdot x^0 + 0 \cdot x^1$  **Einselement**
- (iii) Den Grad des Nullelementes setzt man zu  $\deg(0) = -\infty$
- (iv)  $\deg(P(x)) = 0$  genau dann wenn  $P(x) = c_0 \in \mathcal{R} \wedge c_0 \neq 0$
- (v) Es gibt keine Nullteiler im Ring  $\mathcal{R}[x]$  genau dann, wenn  $\mathcal{R}$  selbst ein Integritätsbereich ist.

Mit der oben für das Nullpolynom getroffenen Vereinbarung gilt immer:

$$\begin{aligned} \deg(P \pm Q) &\leq \max(\deg(P), \deg(Q)), \\ \deg(P * Q) &= \deg(P) + \deg(Q), \end{aligned}$$

wobei

$$-\infty + n = -\infty = -\infty + (-\infty).$$

### Beobachtung:

Ist  $\mathcal{R}$  ein Körper, so ist der Polynomring  $\mathcal{R}[x]$  ein Integritätsbereich, der sich zum Körper der rationalen Funktionen (d.h. Quotienten von teilerfremden Polynomen) erweitern lässt (vergleiche Übergang  $\mathbb{Z} \rightarrow \mathbb{Q}$ ). Damit ergibt sich die Frage nach der Division von Polynomen.

Von jetzt ab betrachten wir nur noch den Fall, dass  $\mathcal{R}$  ein Körper ist.

## Satz A-12.2

Für jeden Körper  $\mathcal{R}$  ist  $\mathcal{R}[x]$  ein **Euklidischer Ring**, d.h. für je zwei Elemente  $a(x), b(x) \in \mathcal{R}[x]$  existieren Polynome  $q(x) \in \mathcal{R}[x]$  und  $r(x) \in \mathcal{R}[x]$ , so dass

$$a(x) = b(x)q(x) + r(x) \quad \text{mit } \deg(r(x)) < \deg(b(x))$$

Man schreibt dann wie im Fall  $\mathbb{R} = \mathbb{N}$  auch

$$r(x) = a(x) \bmod b(x)$$

## Bemerkung

Obiger Satz gilt in  $\mathbb{Z}$  mit  $\deg(x) = |x|$ , der gewöhnliche Betrag.

## Beispiel A - 12.3

$$(2x^5 + 5x^3 + x^2 + 7x + 1) = (2x^2 + 1) * (x^3 + 2x + 1/2) + (5x + 1/2)$$

### Bemerkung:

Wie die Bezeichnung **Euklidischer Ring** andeutet, lässt sich in jedem solchem Ring der in Sektion **A-8** zunächst für natürliche Zahlen definierte Euklidische Algorithmus ohne jegliche Veränderung einsetzen. Daraus folgt wiederum die Eindeutigkeit der Primfaktorzerlegung.

## Definition A-12.4 (Teilbarkeit in $\mathcal{R}[x]$ )

- (i) Falls ein Polynom  $0 \neq c(x) \in \mathcal{R}[x]$  eine Produktdarstellung

$$c(x) = a(x) * b(x) \quad \text{mit } a(x), b(x) \in \mathcal{R}[x]$$

besitzt, heißen  $a(x)$  und  $b(x)$  **Teiler** von  $c(x)$ . Man schreibt dann wie üblich  $a(x)|c(x)$  und  $b(x)|c(x)$ .

- (ii) Falls sowohl  $a(x)$  wie  $b(x)$  nicht konstant sind, d.h.

$$\begin{aligned} 0 < \deg(a(x)) &< \deg(c(x)) \\ 0 < \deg(b(x)) &< \deg(c(x)), \end{aligned}$$

dann nennt man  $a(x)$  und  $b(x)$  **echte Teiler** von  $c(x)$ .

- (iii) Falls  $0 \neq c(x) \in \mathcal{R}[x]$  keinerlei echte Teiler besitzt, heißt es **prim** oder **irreduzibel**.

## Lemma A-12.5

Wie im Ring der ganzen Zahlen gilt für irreduzibles  $c(x) \in \mathcal{R}[x]$  die Implikation

$$c(x)|(a(x) * b(x)) \implies c(x)|a(x) \vee c(x)|b(x)$$

## Satz A-12.6

Ist  $\mathcal{R}$  ein Körper, so besitzt jedes Polynom  $a(x) \in \mathcal{R}[x]$  eine Faktorisierung

$$a(x) = p_1(x) p_2(x) \dots p_m(x)$$

in irreduzible Polynome  $p_j(x)$  für  $j = 1 \dots m$ .

Diese sind eindeutig bis auf konstante Faktoren, d.h. aus

$$a(x) = p'_1(x) \dots p'_m(x)$$

folgt ( gegebenenfalls nach Umnummerierung )

$$p'_j(x) = \gamma_j p_j(x) \quad \text{mit} \quad \gamma_j \in \mathcal{R} \setminus \{0\}.$$

## Beispiel A - 12.7

$x^3 - 1 = (x - 1) * (x^2 + x + 1)$ , da  $x^2 + x + 1$  und  $x - 1$  in  $\mathbb{Q}[x]$  irreduzibel.

### Beobachtung:

Mit  $b(x) = x - x_0$  für  $x_0 \in \mathcal{R}$  als lineares Polynom ergibt sich aus Satz A - 12.2 für ein beliebiges Polynom  $a(x)$  mit  $\text{deg}(a(x)) > 0$  die Darstellung

$$a(x) = q(x) * (x - x_0) + r_0 \quad \text{mit} \quad r_0 = a(x_0) \in R.$$

Die letzte Aussage folgt durch Einsetzen, da das Residuum  $r_0$  vom Grad  $0 < 1 = \text{deg}(b)$  sein muss.

## Folgerung aus Definition A-12.4: Teilbarkeit in $\mathcal{R}[x]$

- (i) Offenbar folgt aus der Zerlegung  $a(x) = q(x) * b(x) + r(x)$  dass

$$b(x) | a(x) \iff r(x) = 0$$

so dass wir in  $\mathcal{R}[x]$  einen konstruktiven Teilbarkeitstest haben.

- (ii) Wie im Ring der ganzen Zahlen folgt die Existenz des größten gemeinsamen Teilers  $c(x) = GGT(a(x), b(x))$ , welcher allerdings nur bis auf die Multiplikation mit einer Konstanten eindeutig ist. O.B.d.A. können wir verlangen, dass der höchste Koeffizient  $c_{deg(c(x))}$  von  $c(x)$  zu  $1 \in \mathcal{R}$  normalisiert wird.
- (iii) Die Berechnung des  $GGT(a(x), b(x))$  erfolgt wiederum durch den Euklidischen Algorithmus.
- (iv) Falls  $deg(GGT(a(x), b(x))) = 1$  und somit nach Normalisierung  $GGT(a(x), b(x)) = 1$ , so heißen  $a(x)$  und  $b(x)$  **relativ prim zueinander** bzw. **teilerfremd**.

## A-13 Faktorisierung und Nullstellen

### Korollar A-13.1

- (i) Ein Körperelement  $x_0 \in \mathcal{R}$  ist genau dann eine **Wurzel** eines Polynoms  $a(x) \in \mathcal{R}[x]$ ,  $a(x_0) = 0$ , wenn es ein  $q(x) \in \mathcal{R}[x]$  gibt, so dass gilt

$$a(x) = (x - x_0) * q(x).$$

- (ii) Ist  $n = \deg(a(x)) > 0$ , so nennt man  $(x - x_0)$  einen **Linearfaktor** von  $a(x)$  und es gilt

$$\deg(q(x)) = n - 1$$

- (iii) Die Koeffizienten  $q_i$  des Polynomes  $q(x)$  ergeben sich aus denen von  $a(x)$  gemäß des Horner-Ruffini-Schemas als

$$q_{n-1} = a_n$$

$$q_{k-1} = a_k + q_k * x_0 \quad \text{für } k = n - 1, \dots, 2, 1.$$

## Folgerung

Durch wiederholtes Abspalten von Linearfaktoren erhält man eine Darstellung der Form

$$a(x) = (x - x_1)(x - x_2) \cdots (x - x_k)q(x),$$

wobei  $q(x)$  keine weiteren Nullstellen besitzt oder das Nullpolynom ist. Im letzteren Fall war auch schon  $a(x)$  das Nullpolynom.

Es kann durchaus vorkommen, dass derselbe Linearfaktor wiederholt abgespalten wird, man spricht dann von einer **mehrfachen Nullstelle**.

## Folgerung

Da immer

$$n = \deg(a(x)) = k + \deg(q(x)) \geq k$$

gilt, kann ein Polynom vom Grad  $n$  also höchstens  $n$  Nullstellen haben oder es verschwindet identisch. Damit ist auch Satz A-11.6(iii) bewiesen, da dort durch die Interpolationsbedingung  $n + 1$  unterschiedliche Nullstellen für ein Polynom vom Grad  $n$  verlangt werden.

## Folgerung

Ein Polynom  $a(x)$  kann also nur irreduzibel sein, wenn  $a(x)$  selbst ein Linearfaktor ist oder im Koeffizientenkörper keine Nullstellen besitzt.

Falls ein Polynom vom Grad  $\deg(a(x)) = n > 0$  auch  $n$  Nullstellen

$$x_i \in \mathcal{R} \quad \text{für} \quad i = 1 \dots n$$

besitzt, so gibt es für  $a(x)$  eine eindeutige Faktorisierung

$$a(x) = c_n(x - x_1)(x - x_2) \cdots (x - x_n)$$

Auch in dieser Form kann es mit einem Aufwand von  $n$  Multiplikationen ausgewertet werden.

## Beispiel A - 13.2

$x^3 - 1$  hat genau eine Nullstelle  $x_0 = 1$  in  $\mathcal{R} = \mathbb{R}$ , da nach Abspaltung des Linearfaktors  $(x - 1)$  das Polynom

$$x^2 + x + 1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} \geq \frac{3}{4}$$

übrig bleibt. Wäre es reduzibel, müsste es das Produkt von zwei linearen Faktoren der Form  $(x - x_1)$  und  $(x - x_2)$  mit  $x_1, x_2 \in \mathbb{R}$  sein und damit für  $x \in \{x_1, x_2\} \subset \mathbb{R}$  verschwinden, was der obigen Ungleichung widerspricht.

## Bemerkung:

Es lässt sich zeigen, dass ein nichtkonstantes Polynom  $q(x) \in \mathbb{R}[x]$ , das keine Nullstellen besitzt, sich immer als Produkt quadratischer Polynome  $q_j(x)$  mit  $\deg(q_j(x)) = 2$  darstellen lässt. (Gauß 1799)<sup>1</sup>

Mit anderen Worten:

*Ein Polynom  $p(x)$  ist genau dann irreduzibel in  $\mathbb{R}[x]$ , wenn es linear oder ein quadratisches Polynom ohne reelle Nullstelle ist.*

1: „Neuer Beweis des Satzes, dass jede algebraische, rationale, ganze Funktion einer Veränderlichen in reelle Faktoren des ersten und zweiten Grades zerlegt werden kann.“, Dissertation

## Bemerkung:

Erweitert man  $\mathbb{R}$  zu den im folgenden Abschnitt beschriebenen komplexen Zahlen  $\mathbb{C}$ , so haben auch diese quadratische Polynome Nullstellen und man erhält immer eine vollständige Zerlegung

$$a(x) = a_n(x - x_1)(x - x_2) \cdots (x - x_n),$$

wobei  $n = \deg(a(x))$  ist. Dabei müssen die Nullstellen  $x_j \in \mathbb{C}$  nicht alle verschieden sein.

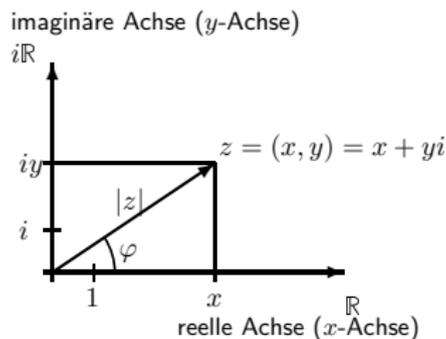
Diese Aussage nennt man **Fundamentalsatz der Algebra** (bzw. „FS der Lehre von den komplexen Zahlen“).

Komplexe Wurzeln spielen eine wesentliche Rolle als Eigenwerte von nicht symmetrischen Matrizen. Diese treten z.B. bei der Analyse dynamischer (d.h. zeitabhängiger) Systeme auf.

## A-14 Die komplexen Zahlen

Wir suchen eine Erweiterung von  $\mathbb{R}$ , in der  $x^2 + 1 = 0$  lösbar wird. Dazu identifizieren wir  $\mathbb{R}$  mit der horizontalen Geraden  $\mathbb{R} \times \{0\}$  in der Ebene  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ .

Punkte  $(x, y) \in \mathbb{R}^2$  notieren wir als  $x + iy$ , insbesondere entspricht  $1 = 1 + i \cdot 0$  dem Paar  $(1, 0)$  und  $i = 0 + i \cdot 1$  dem Paar  $(0, 1)$ .



Nun muss die *additive Gruppe*  $\mathbb{R}^2$  mit einer passenden Multiplikation  $*$  ausgestattet werden, so dass (wenigstens)

$$(1, 0) * (x, y) = (x, y) \quad \text{und} \quad (0, 1) * (0, 1) = (-1, 0),$$

d.h.,  $1 * (x + iy) = x + iy$  und  $i^2 = -1$  gelten.

## Definition A-14.1 (Addition und Multiplikation in $\mathbb{C}$ )

Addition und Multiplikation auf  $\mathbb{R}^2$  seien definiert als

$$\begin{aligned}(x_1 + \mathbf{i}y_1) + (x_2 + \mathbf{i}y_2) &= (x_1 + x_2) + \mathbf{i}(y_1 + y_2) \quad \text{und} \\ (x_1 + \mathbf{i}y_1) * (x_2 + \mathbf{i}y_2) &= (x_1x_2 - y_1y_2) + \mathbf{i}(x_1y_2 + y_1x_2)\end{aligned}$$

Als Menge  $\mathbb{C}$  der **komplexen Zahlen** wird die Struktur  $\mathbb{C} = (\mathbb{R}^2, +, *)$  bezeichnet.

„natürliche“ Realisierungen:

- ▶ als Unterring des Matrixrings  $\mathbb{R}^{2 \times 2}$ :

$$\mathbb{C} \simeq \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : x, y \in \mathbb{R} \right\}, \quad \mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

- ▶ als Quotientenring  $\mathbb{C} \simeq \mathbb{R}[u]/(u^2 + 1)$  nach dem von  $u^2 + 1$  aufgespannten Ideal im Polynomring  $\mathbb{R}[u]$ ,  $\mathbf{i} = \bar{u} = [u]_{(u^2+1)}$ .

## Lemma A-14.2 (Körper eigenschaft von $\mathbb{C}$ )

Bezüglich der oben definierten Verknüpfungen  $+$  und  $*$  bildet  $\mathbb{C}$  einen kommutativen Körper mit folgenden Eigenschaften:

- (i)  $0 = 0 + i0$  **Nullelement**
- (ii)  $1 = 1 + i0$  **Einselement**
- (iii)  $-(x + iy) = (-x) + i(-y)$  **Inverses bzgl.  $+$**
- (iv)  $(x + iy)^{-1} = (x - iy)/(x^2 + y^2)$ , **Inverses bzgl.  $*$**   
wobei  $z^{-1}$  nur für  $z \neq 0$  existiert.
- (v) Die **rein reellen** Zahlen  $x = x + i0$  bilden einen Unterkörper von  $\mathbb{C}$ , der zu  $\mathbb{R}$  isomorph ist.

zu (iv):

$$(x + iy) * (x - iy) = (x \cdot x - y \cdot (-y)) + i(x \cdot (-y) + y \cdot x) = x^2 + y^2 .$$

$z \neq 0 \implies x^2 + y^2 > 0$ , d.h.  $z^{-1} = (x - iy)/(x^2 + y^2)$  ist definiert und invers zu  $z = x + iy$ .

## Lemma A-14.3 (Lösung einer quadratischen Gleichung)

Das Polynom

$$P(x) = \alpha x^2 + \beta x + \gamma \quad \text{mit } \alpha, \beta, \gamma \in \mathbb{R}$$

hat im Falle  $4\alpha\gamma > \beta^2$  die komplexen Wurzeln

$$x_{1,2} = -\frac{1}{2\alpha} \left[ \beta \pm i\sqrt{4\alpha\gamma - \beta^2} \right]$$

**Herleitung durch Quadratisches Ergänzen:**

$$\begin{aligned} 0 &= 4\alpha P(x) = (2\alpha x)^2 + 2(2\alpha x)\beta + 4\alpha\gamma \\ &= (2\alpha x + \beta)^2 - i^2(4\alpha\gamma - \beta^2) \\ &= \left(2\alpha x + \beta + i\sqrt{4\alpha\gamma - \beta^2}\right) * \left(2\alpha x + \beta - i\sqrt{4\alpha\gamma - \beta^2}\right) \end{aligned}$$

## Beispiel A - 14.4

$$P(x) = x^2 + x + 1 = 0$$

$$x_{1,2} = -\frac{1}{2} \left[ 1 \pm i\sqrt{3} \right]$$

**Probe:**  $x_0 = -\frac{1}{2} + i\frac{1}{2}\sqrt{3}$

$$\begin{aligned} x_1^2 + x_1 + 1 &= \left( \frac{1}{4} - \frac{i}{2}\sqrt{3} + i^2\frac{3}{4} \right) - \frac{1}{2} + \frac{i}{2}\sqrt{3} + 1 \\ &= \frac{1}{4} - \frac{i}{2}\sqrt{3} - \frac{3}{4} - \frac{1}{2} + \frac{i}{2}\sqrt{3} + 1 \\ &= \underbrace{-\frac{i}{2}\sqrt{3} + \frac{i}{2}\sqrt{3}}_{=0} + \underbrace{\frac{1}{4} - \frac{3}{4} - \frac{1}{2} + 1}_{=0} \end{aligned}$$

**Also:**  $x_1^2 + x_1 + 1 = 0$

**Probe:**  $x_2 = -\frac{1}{2} - i\frac{1}{2}\sqrt{3}$

$$x_2^2 + x_2 + 1 = \underbrace{\frac{i}{2}\sqrt{3} - \frac{i}{2}\sqrt{3}}_{=0} + \underbrace{\frac{1}{4} - \frac{3}{4} - \frac{1}{2} + 1}_{=0} = 0$$

## Real- und Imaginärteil

Für jede komplexe Zahl  $z = x + iy$  werden

$$\operatorname{Re}(z) = x$$

$$\operatorname{Im}(z) = y$$

**Realteil** und  
**Imaginärteil**

genannt.

$\bar{z} = x - iy$  heißt **konjugiert komplexe Zahl** zu  $z = x + iy$ .

Es gelten

$$\frac{1}{2}(z + \bar{z}) = \frac{1}{2}((x + iy) + (x - iy)) = x = \operatorname{Re}(z)$$

$$\frac{1}{2i}(z - \bar{z}) = \frac{1}{2i}((x + iy) - (x - iy)) = y = \operatorname{Im}(z)$$

$$z * \bar{z} = (x + iy) * (x - iy) = x^2 + y^2$$

$$z = \bar{z} \iff \operatorname{Im}(z) = 0 \iff z \text{ ist rein reell.}$$

$$z = -\bar{z} \iff \operatorname{Re}(z) = 0 \iff z \text{ ist rein imaginär.}$$

## Lemma A-14.5

- (i) *Konjugation ist ein Körperhomomorphismus auf  $\mathbb{C}$ , d.h. es gilt für alle  $z_1, z_2 \in \mathbb{C}$ , dass*

$$\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2} \quad \& \quad \overline{z_1 * z_2} = \overline{z_1} * \overline{z_2} \quad \& \quad \overline{z_1/z_2} = \overline{z_1}/\overline{z_2}.$$

- (ii) *Daraus folgt durch vollständige Induktion, dass für jedes komplexe Polynom  $P(z) \in \mathbb{C}[z]$*

$$\overline{P(z)} = \overline{P}(\overline{z})$$

*gilt, wobei  $\overline{P}(z)$  dasjenige Polynom bezeichnet, dessen Koeffizienten gerade die Konjugierten der Koeffizienten von  $P(z)$  sind.*

## Korollar A - 14.6

- (i) *Aus obigen Lemma folgt, dass für ein Polynom  $P(z) \in \mathbb{R}[z]$  die komplexen Wurzeln stets in konjugiert komplexen Paaren auftreten, d.h.*

$$P(z) = 0 \iff P(\bar{z}) = 0$$

- (ii) *Diese Eigenschaft ist umgekehrt für ein beliebiges komplexes Polynom  $P(z) \in \mathbb{C}[z]$  mit mindestens einem reellen Koeffizienten  $p_i \in \mathbb{R}$ ,  $i \in \{0, \dots, \deg P\}$ , auch hinreichend dafür, dass alle seine Koeffizienten reell sind.*

## Bemerkung

Dieses Aussage ist immer dann wichtig, wenn man Polynome aus einem eigentlich reellen Modell erhält und nur mehr oder minder widerwillig und hoffentlich vorübergehend ins Komplexe geht. Dies gilt z. B. für charakteristische Polynome reeller Matrizen in der linearen Algebra.

## Definition A-14.7

Betrachtet man  $z = x + iy$  als Vektor in der Ebene mit den Koordinaten  $(x, y) \in \mathbb{R}^2$ , so ergibt sich

- (i) als Länge des Vektors der **Betrag** der komplexen Zahl  $z$

$$|z| = \sqrt{x^2 + y^2} \in \mathbb{R}_+,$$

- (ii) durch Spiegelung an der Horizontalen die **konjugiert komplexe Zahl** von  $z$

$$\bar{z} = x + i(-y) \in \mathbb{C},$$

- (iii) als Winkel zur Horizontalen des Strahls vom Ursprung durch  $(x, y)$  das **Argument**

$$\arg(z) = \arctan(y/x) \pm k\pi \in (-\pi, \pi).$$

Dabei ist  $k \in \{-1, 0, 1\}$  so zu wählen, dass  $x = |z| \cos(\arg(z))$  und  $y = |z| \sin(\arg(z))$  gelten.

Notation für Polarkoordinaten:  $r = |z|$  und  $\phi = \arg(z)$

## Bemerkung

Alle Gleichungen aus dem Reellen gelten auch im Komplexen.  
Ungleichungen sind nur dann sinnvoll, wenn sie Beträge enthalten und damit auf beiden Seiten reell sind.

## Lemma A-14.8

In  $\mathbb{C}$  gilt

- (i)  $z = |z|(\cos \varphi + i \sin \varphi)$  für  $\varphi = \arg(z)$  **Euler-Moivre-Formel**
- (ii)  $|z| = |\bar{z}| \wedge \arg(z) = -\arg(\bar{z})$
- (iii)  $|z_1 + z_2| \leq |z_1| + |z_2|$  **Dreiecksungleichung**
- (iv)  $|z_1 * z_2| = |z_1| * |z_2| \wedge \arg(z_1 * z_2) = \arg(z_1) + \arg(z_2) \pm 2\pi k$
- (v)  $|z_1/z_2| = |z_1|/|z_2| \wedge \arg(z_1/z_2) = \arg(z_1) - \arg(z_2) \pm 2\pi k$

## Erläuterung

Aussagen (iv) und (v) lassen sich so interpretieren, dass  $|\cdot|$  und  $\arg$  Gruppenhomomorphismen von  $\mathbb{C} \setminus \{0\}$  in die multiplikative Gruppe  $(\mathbb{R}_+, \cdot)$  bzw. die additive Gruppe  $(\mathbb{R}/(2\pi\mathbb{Z}), +)$  sind.

## Eulers Formel und Einheitswurzeln

Aus der Euler-Moivre-Formel und den Additionstheoremen des Sinus und Kosinus ergibt sich für  $z = r(\cos \varphi + i \sin \varphi)$ :

$$z^n = r^n \left( \cos(n\varphi) + i \sin(n\varphi) \right) \quad \forall n \in \mathbb{Z} .$$

Jede Lösung von  $z^n = R \left( \cos(\alpha) + i \sin(\alpha) \right)$  erfüllt in Polarkoordinaten  $r^n = R$  und  $n\phi = \alpha + 2k\pi$  für ein  $k \in \mathbb{Z}$ , d.h.

$$z = \sqrt[n]{R} \left( \cos\left(\frac{\alpha}{n} + k\frac{2\pi}{n}\right) + i \sin\left(\frac{\alpha}{n} + k\frac{2\pi}{n}\right) \right)$$

$k$  und  $k + jn$ ,  $j \in \mathbb{Z}$  bel., ergeben dabei dieselbe Lösung. Jeder Restklasse modulo  $n$  ist daher genau eine Lösung zugeordnet, d.h. mit  $k = 0, \dots, n - 1$  sind alle Lösungen erfasst.

Die  $N$  verschiedenen Zahlen

$$z_j = \cos\left(j \frac{2\pi}{N}\right) + i \sin\left(j \frac{2\pi}{N}\right), \quad j = 0, \dots, N-1,$$

sind für  $j = 0, \dots, N-1$  die  $N$  Lösungen des **Kreisteilungspolynoms**  $P_N(z) = z^N - 1$ .

Diese bilden die Eckpunkte eines regelmäßigen  $N$ -Ecks auf dem Einheitskreis.

Mit  $N = 2K$  ergibt sich für jedes  $j = 0, \dots, K-1$

$$\begin{aligned} z_{j+K} &= \cos\left((j+K) \frac{2\pi}{2K}\right) + i \sin\left((j+K) \frac{2\pi}{2K}\right) \\ &= \cos\left(j \frac{2\pi}{2K} + \pi\right) + i \sin\left(j \frac{2\pi}{2K} + \pi\right) \\ &= -z_j, \end{aligned}$$

und durch Quadratbildung

$$\begin{aligned} z_j^2 &= z_{j+K}^2 = \cos\left(2j \frac{2\pi}{N}\right) + i \sin\left(2j \frac{2\pi}{N}\right) \\ &= \cos\left(j \frac{2\pi}{K}\right) + i \sin\left(j \frac{2\pi}{K}\right). \end{aligned}$$

Es gibt also nur  $K$  unterschiedliche Werte von  $z_j^2$  für  $j = 0, \dots, N-1$ , welche gerade die Wurzeln von  $P_K(x) = x^K - 1$  sind.

## Schnelle Polynommultiplikation

Die Polynommultiplikation  $c(z) = a(z) * b(z)$  kann auch durch

- (i) Auswerten beider Faktoren an  $N > \deg(a(z)) + \deg(b(z))$  verschiedenen Stützstellen  $z_1, \dots, z_N \in \mathbb{C}$ ,
- (ii) Multiplikation der Funktionswerte  $w_k = a(z_k) * b(z_k)$ ,  $k = 1, \dots, N$  und
- (iii) Bestimmen des Interpolationspolynoms  $c(z)$  durch die Punkte  $(z_1, w_1), \dots, (z_N, w_N)$

erfolgen.

Die Stützstellen können z.B. auf der reellen Achse gewählt werden.

Nachteil: teils sehr große Funktionswerte. Ein besonders einfacher und schneller Auswertungs- und Interpolationsalgorithmus – die **schnelle**

**diskrete Fouriertransformation** – ergibt sich jedoch, wenn

$N = 2^n > \deg(a(z)) + \deg(b(z))$  eine Zweierpotenz und die  $z_k$  die  $N$ -ten **Einheitswurzeln** sind.

## Auswertung durch Schnelle Fouriertransformation (FFT)

Sammelt man die geraden und ungeraden Koeffizienten eines beliebigen Polynoms mit  $\deg a(x) < N$ , so ergibt sich die Zerlegung

$$a(x) = a_g(x^2) + x \cdot a_u(x^2)$$

mit Polynomen  $a_g(x)$  und  $a_u(x)$  vom Grad  $< K = N/2$ .

Die Auswertung von  $a(x)$  an den  $N = 2K$ -ten Einheitswurzeln kann nun erfolgen als

$$a(z_j) = a_g(z_j^2) + z_j \cdot a_u(z_j^2)$$

$$a(z_{j+K}) = a_g(z_j^2) - z_j \cdot a_u(z_j^2)$$

Die Auswertung von  $a_g(x)$  und  $a_u(x)$  an den  $K$  Wurzeln von  $P_K(x) = x^K - 1$  stellt nun jeweils das Ausgangsproblem der halben Größe dar. Für Potenzen  $N = 2^n$  erfüllt die Zahl  $M_n$  der zur Auswertung an allen  $N$ -ten Einheitswurzeln benötigten (komplexen) Multiplikationen die Rekursion

$$M_n = 2 \cdot M_{n-1} + 2^{n-1} \iff (2^{-n} M_n) = (2^{-(n-1)} M_{n-1}) + \frac{1}{2}.$$

Mit  $M_0 = 0$  (konstante Polynome) folgt daraus unmittelbar

$$M_n = \frac{1}{2} n 2^n \iff M_{\log_2(N)} = \frac{1}{2} \cdot N \cdot \log_2(N).$$

## Interpolation durch Inverse FFT

Mit derselben Notation gilt weiter

$$a(x) = a_g(x^2) + x \cdot a_u(x^2),$$

d.h. die Koeffizienten von  $a(x)$  ergeben sich aus denen von  $a_g(x)$  und  $a_u(x)$  durch alternierendes Einsetzen ohne weitere Rechenoperationen.

Zur Interpolation von  $a_g(x)$  und  $a_u(x)$  werden die jeweiligen Werte an den  $K$ -ten Einheitswurzeln  $z_j^2$ ,  $j = 0, \dots, K - 1$ , benötigt.

Wegen  $z_{j+K} = -z_j$  ergeben sich diese aus

$$\left. \begin{array}{l} a(z_j) = a_g(z_j^2) + z_j \cdot a_u(z_j^2) \\ a(z_{j+K}) = a_g(z_j^2) - z_j \cdot a_u(z_j^2) \end{array} \right\} \iff \begin{cases} a_g(z_j^2) = \frac{1}{2} (a(z_j) + a(z_{j+K})) \\ a_u(z_j^2) = \frac{1}{2} z_{N-j} (a(z_j) - a(z_{j+K})) \end{cases}$$

Mit  $N = 2^n$  folgt die Anzahl der Multiplikationen wieder der Rekursion

$$M_n = 2M_{n-1} + 2^{n-1} \iff (2^{-n} M_n) = (2^{-(n-1)} M_{n-1}) + \frac{1}{2},$$

wegen  $M_0 = 0$  (konstante Polynome) also  $M_n = 2^{n-1} n$  oder

$$M_{\log_2(N)} = \frac{1}{2} N \log_2(N).$$

## Schlussbemerkung

Bei der Erweiterung von den reellen auf die komplexen Zahlen verliert man die Möglichkeit, alle Zahlen eindeutig nach einer „sinnvollen Größe“ zu ordnen.

Beim Übergang zum nächsten Erweiterungskörper, nämlich den sogenannten Quaternionen, geht (notwendigerweise) auch noch die Kommutativität der Multiplikation verloren.

Darüberhinaus kann es keine Oberkörper mehr geben. Stattdessen bedient man sich in der Mathematik zur Beschreibung umfangreicherer, aber nicht notwendigerweise komplexerer Strukturen sogenannter **Module** über Ringen und **Vektorräume** oder **Algebren** über Körpern.

Ähnlich wie bei Polynomringen spielen dabei die Ring- bzw. Körperelemente als „Koeffizienten“ eine zentrale Rolle, mit deren Hilfe sich alle „praktischen“ Berechnungen durchführen lassen.





# Teil B

## Lineare Algebra

Einführung

Vektoren im Anschauungsraum

Abstandsnormen

Basen und Unterräume

Lineare Abbildungen

Orthogonalisierungsverfahren nach GRAM-SCHMIDT

Matrizen und ihre Algebra

## B - 1 Einführung

Der Grundbegriff der linearen Algebra ist der des **Vektorraumes**, mit dessen Hilfe sich eine Vielzahl von mathematischen Objekten und Anwendungsmodellen beschreiben läßt.

## Definition B-1.1 (Vektorraum $\mathcal{V}$ bzw. linearer Raum: I)

Ein reeller Vektorraum ist eine Menge  $\mathcal{V}$ , auf der eine Addition zweier Vektoren und eine Multiplikation eines Vektors mit einer reellen Zahl definiert sind. Zwei beliebige  $\mathbf{u}, \mathbf{v} \in \mathcal{V}$  werden addiert und ergeben einen Vektor  $\mathbf{w} \in \mathcal{V}$ ,

$$\mathbf{w} = \mathbf{u} + \mathbf{v} \in \mathcal{V} .$$

Dabei erfüllt  $\mathcal{V}$  mit der Addition die Axiome einer additiven Gruppe, d.h. es gibt einen Nullvektor  $\mathbf{0} \in \mathcal{V}$  und für beliebige  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{V}$  gilt:

▶  $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w}),$

▶  $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u},$

▶  $\mathbf{u} + \mathbf{0} = \mathbf{u},$

▶  $\exists(-\mathbf{u}) \in \mathcal{V} : \mathbf{u} + (-\mathbf{u}) = \mathbf{0}.$

**Assoziativität**

**Kommutativität**

**Neutrales Element**

**Inverses Element**

## Definition B-1.2 (Vektorraum $\mathcal{V}$ bzw. linearer Raum: II)

Eine reelle Zahl  $\lambda \in \mathbb{R}$  wird mit einem Vektor  $\mathbf{v} \in \mathcal{V}$  multipliziert und ergibt einen Vektor  $\mathbf{w} \in \mathcal{V}$ ,

$$\mathbf{w} = \lambda \mathbf{v} \in \mathcal{V} .$$

Die skalare Multiplikation soll mit der reellen Multiplikation verträglich sein, d.h. für beliebige  $\lambda, \gamma \in \mathbb{R}$  gelte

- ▶  $1 \mathbf{u} = \mathbf{u}$ ,
- ▶  $\lambda(\gamma \mathbf{u}) = (\lambda\gamma) \mathbf{u}$

Schließlich soll die Kombination von Addition und Multiplikation sich analog zu den entsprechenden reellen Operationen verhalten:

- ▶  $\lambda(\mathbf{u} + \mathbf{v}) = \lambda \mathbf{u} + \lambda \mathbf{v}$ ,
- ▶  $(\lambda + \gamma) \mathbf{u} = \lambda \mathbf{u} + \gamma \mathbf{u}$ .

**Distributivgesetze**

### Bemerkungen

- ▶ Auf natürliche Weise ist  $\mathbb{R}$  ein reeller Vektorraum, ebenso  $\mathbb{C}$ .
- ▶ Man kann Vektorräume über beliebigen Skalarkörpern (z.B.  $\mathbb{Q}, \mathbb{C}, \mathbb{Z}_7$ ) definieren, die reellen Faktoren sind dann durch Körperelemente zu ersetzen.

## Beispiel B - 1.3 (Spaltenvektorraum)

Für jedes  $n \in \mathbb{N}_+$  ist der Spaltenvektorenraum  $\mathbb{R}^n$  mit komponentenweisen Operationen auch ein  $\mathbb{R}$ -Vektorraum.

Ein Spaltenvektor  $\mathbf{v}$  aus  $n$  reellen Zahlen  $\nu_i$ ,  $i = 1, \dots, n$ , wird notiert als

$$\mathbf{v} = (\nu_i)_{i=1}^n = (\nu_i)_{i=1, \dots, n} \cdot \begin{cases} \mathbf{u} + \mathbf{v} = (\mu_i)_{i=1}^n + (\nu_i)_{i=1}^n & = (\mu_i + \nu_i)_{i=1}^n, \\ \lambda \mathbf{v} = \lambda (\nu_i)_{i=1}^n & = (\lambda \nu_i)_{i=1}^n \end{cases}$$

## Beispiel B - 1.4 (Funktionsräume)

Für je zwei reellwertige Funktionen  $f, g : \mathcal{D} \rightarrow \mathbb{R}$  mit gemeinsamen Definitionsbereich  $\mathcal{D}$  kann man die Summe  $h = f + g$  als die Funktion mit den Werten

$$h(x) = f(x) + g(x) \quad \text{für } x \in \mathcal{D}$$

definieren. Entsprechend erhält man  $h = \lambda f$  als die Funktion mit den Werten

$$h(x) = \lambda f(x) \quad \text{für } x \in \mathcal{D}.$$

## Beispiel B-1.5 (Zahlenfolgen)

Funktionen des Typs  $\mathbf{a} : \mathbb{N} \rightarrow \mathbb{R}$  nennt man **Zahlenfolgen** und notiert diese als

$$\mathbf{a} = (\alpha_n)_{n \in \mathbb{N}}, \quad \mathbf{b} = (\beta_n)_{n \in \mathbb{N}}.$$

Addition und Multiplikation mit Skalaren werden gliedweise durchgeführt,

$$\mathbf{a} + \mathbf{b} = (\alpha_n + \beta_n)_{n \in \mathbb{N}} \quad \text{und} \quad \lambda \mathbf{a} = (\lambda \alpha_n)_{n \in \mathbb{N}}.$$

Die Zahlenfolgen mit diesen Operationen bilden den reellen Vektorraum  $\ell(\mathbb{N}, \mathbb{R})$ .

Man kann für jedes  $k \in \mathbb{N}$  die eingliedrige Folge  $\mathbf{d}^k = (\delta^k_n)_{n \in \mathbb{N}}$  mit

$$\delta^k_n = \begin{cases} 1 & \text{für } k = n \\ 0 & \text{sonst bei } k \neq n \end{cases}$$

definieren.

Mittels Addition und skalarer Multiplikation lassen sich aus diesen elementaren Folgen **immer nur** Folgen  $\mathbf{a} = (\alpha_n)_{n \in \mathbb{N}}$  endlicher Länge konstruieren, d.h. es gibt immer ein  $K \in \mathbb{N}$  mit  $\alpha_n = 0$  für  $n > K$ .

Die meisten Untersuchungen und Ergebnisse der linearen Algebra beschäftigen sich mit Variationen der folgende Frage:

## Problem B - 1.6

*Gegeben seien eine Familie von  $r$  Vektoren  $\mathbf{v}_i$  ( $i = 1, \dots, r$ ) und ein spezieller Vektor  $\mathbf{w}$  aus einem gemeinsamen Vektorraum  $\mathcal{V}$ .*

*Gibt es nun eine Familie von Skalaren  $\lambda_i$  ( $i = 1, \dots, r$ ), so dass*

$$\mathbf{w} = \lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \dots + \lambda_r \mathbf{v}_r = \sum_{i=1}^r \lambda_i \mathbf{v}_i$$

*gilt? Wenn ja, wie kann man geeignete Koeffizienten  $\lambda_i$  berechnen? Sind diese dann eindeutig bestimmt?*

Unter anderem lassen sich Fragen nach Basisdarstellungen sowie die Suche nach den Lösungen linearer Gleichungssysteme

$$b_1 = a_{11} x_1 + a_{12} x_2 + \dots + a_{1n} x_n$$

$$b_2 = a_{21} x_1 + a_{22} x_2 + \dots + a_{2n} x_n$$

$$\vdots$$

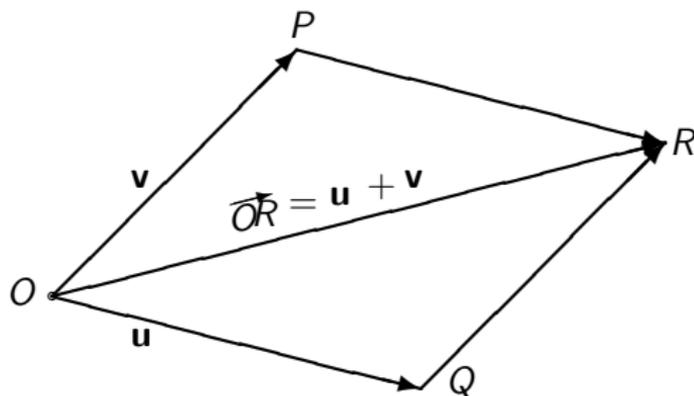
$$b_m = a_{m1} x_1 + a_{m2} x_2 + \dots + a_{mn} x_n$$

in dieser Art formulieren.

## B-2 Vektoren im Anschauungsraum

Man kann Verschiebungen im Raum als Vektoren auffassen. Vektoren  $\mathbf{v} = \overrightarrow{OP}$  und  $\mathbf{u} = \overrightarrow{OQ}$  sind dann diejenigen Verschiebungen, die den Ursprungspunkt  $O$  nach  $P$  bzw.  $Q$  verschieben. Die Summe zweier Verschiebungen ergibt sich als  $\mathbf{w} = \mathbf{u} + \mathbf{v} = \overrightarrow{OR}$ , wobei sich der Punkt  $R$  sowohl als Verschiebung von  $Q$  um  $\mathbf{v}$  als auch als Verschiebung von  $P$  um  $\mathbf{u}$  ergibt.

Bildlich liegt  $R$  an der Spitze des Pfeils  $\mathbf{v}$  (bzw.  $\mathbf{u}$ ), wenn dessen Anfang in den Punkt  $Q$  (bzw.  $P$ ) gelegt wird. Die Beliebigkeit in der Reihenfolge der Ausführung der Verschiebungen ist gleichbedeutend mit der Kommutativität der Vektoraddition.



Legt man den Ursprungspunkt  $O$  fest, so lassen sich alle **Raumpunkte**  $P$  mit ihren sogenannten **Ortsvektoren**  $\mathbf{v} = \overrightarrow{OP}$  identifizieren und man schreibt auch  $P = P(\mathbf{v})$ .

Vereinbart man weiterhin ein System von *drei rechtwinkligen Koordinatenachsen* mit geeigneter Skalierung, so lässt sich jeder Vektor  $\mathbf{v}$  mit Hilfe von drei Koordinaten  $\nu_1, \nu_2, \nu_3 \in \mathbb{R}$  wie folgt darstellen:

$$\mathbf{v} = \nu_1 \mathbf{e}_1 + \nu_2 \mathbf{e}_2 + \nu_3 \mathbf{e}_3$$

Hierbei verlaufen die drei **Einheitsvektoren**  $\mathbf{e}_1$ ,  $\mathbf{e}_2$  und  $\mathbf{e}_3$  entlang der  $x$ -,  $y$ - bzw.  $z$ -Achse. Sie bilden eine sogenannte **Basis** des Anschauungsraumes und werden zuweilen auch mit  $\vec{i}$ ,  $\vec{j}$  und  $\vec{k}$  bezeichnet. Hat man sich auf ein bestimmtes Koordinatensystem festgelegt, so kann man die Vektoren mit ihren entsprechenden **Koordinatentripeln** identifizieren und schreibt dann einfach

$$\mathbf{v} = (\nu_1, \nu_2, \nu_3) \in \mathbb{R}^3 .$$

Inbesondere erhält man die **Basisvektoren** selbst als **kanonische Basisvektoren** des  $\mathbb{R}^3$ ,

$$\mathbf{e}_1 = (1, 0, 0), \quad \mathbf{e}_2 = (0, 1, 0), \quad \mathbf{e}_3 = (0, 0, 1) .$$

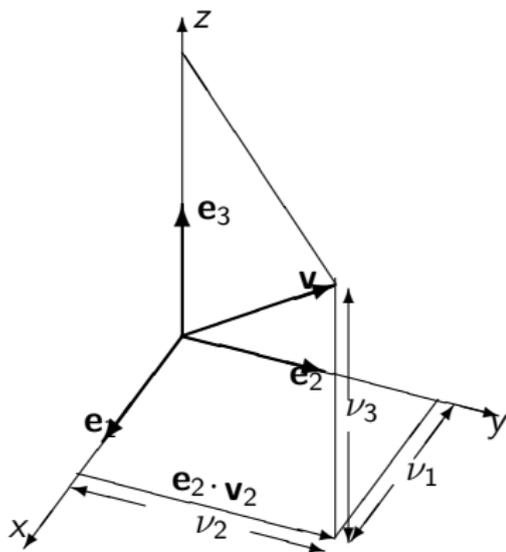
Addition, Subtraktion und Multiplikation erfolgen nun komponentenweise, z.B. für

$$\mathbf{u} = (3, -1, 2) \quad \text{und} \quad \mathbf{v} = (0, 2, 4)$$

ergibt sich

$$\mathbf{u} + \mathbf{v} = (3, 1, 6), \quad \mathbf{u} - \mathbf{v} = (3, -3, -2) \quad \text{und} \quad 3\mathbf{u} = (9, -3, 6) ,$$

wobei der Faktor 3 in der letzten Gleichung die Rolle eines Skalars spielt.



## Länge und Richtungskosinus

Wegen der vorausgesetzten Rechtwinkligkeit der Koordinatenachsen ergibt sich aus dem Satz des Pythagoras

### Definition B-2.1 (Länge eines Vektors, Euklidische Norm)

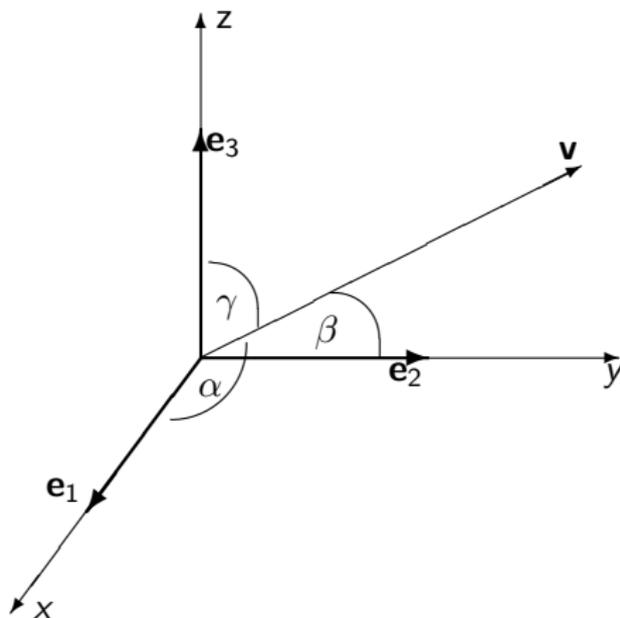
Der Vektor  $\mathbf{v} = (\nu_1, \nu_2, \nu_3)$  hat die **Länge**

$$\|\mathbf{v}\| = \sqrt{\nu_1^2 + \nu_2^2 + \nu_3^2}.$$

Diese nichtnegative reelle Zahl ist eine Verallgemeinerung des Betrages von reellen oder komplexen Zahlen und wird auch die **euklidische Norm** des Vektors  $\mathbf{v}$  genannt.

Dividiert man nun einen Vektor  $\mathbf{v} \neq 0$  durch seinen Betrag, so erhält man einen Vektor der Länge 1, dessen Komponenten als Kosinus von drei Winkeln  $\alpha, \beta, \gamma \in [0, \pi]$  dargestellt werden können. Es gilt also

$$\frac{\mathbf{v}}{\|\mathbf{v}\|} = \left( \frac{\nu_1}{\|\mathbf{v}\|}, \frac{\nu_2}{\|\mathbf{v}\|}, \frac{\nu_3}{\|\mathbf{v}\|} \right) = (\cos \alpha, \cos \beta, \cos \gamma)$$



Wie aus der Zeichnung ersichtlich ist, bilden  $\alpha$ ,  $\beta$  und  $\gamma$  die Winkel zwischen  $\mathbf{v}$  und den Basisvektoren  $\mathbf{e}_1$ ,  $\mathbf{e}_2$  und  $\mathbf{e}_3$ . Man kann also einen Vektor eindeutig durch diese drei Winkel und seine Länge definieren.

## Skalar- oder inneres Produkt

Neben den Normen tritt die Summe über die gliedweisen Produkte der Komponenten beider Vektoren auf.

### Definition B-2.2 (Skalar- oder inneres Produkt)

Für zwei beliebige Vektoren  $\mathbf{u} = (\mu_1, \mu_2, \mu_3)$  und  $\mathbf{v} = (\nu_1, \nu_2, \nu_3)$  nennt man den Skalar

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mu_1\nu_1 + \mu_2\nu_2 + \mu_3\nu_3$$

das **euklidische Skalar- oder innere Produkt** von  $\mathbf{u}$  und  $\mathbf{v}$ .

von  $\mathbf{u}$  und  $\mathbf{v}$  wird **euklidisches Skalarprodukt** genannt und als

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mu_1\nu_1 + \mu_2\nu_2 + \mu_3\nu_3$$

notiert.

## Lemma B-2.3 (Eigenschaften Skalarprodukt)

Es läßt sich nun leicht nachprüfen, daß für alle  $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$  und  $\lambda \in \mathbb{R}$  gilt:

$$\begin{aligned}\langle \mathbf{v}, \mathbf{u} \rangle &= \langle \mathbf{u}, \mathbf{v} \rangle \\ \lambda \langle \mathbf{u}, \mathbf{v} \rangle &= \langle \lambda \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{u}, \lambda \mathbf{v} \rangle \\ \langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle &= \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle \\ \langle \mathbf{u}, \mathbf{u} \rangle &= \|\mathbf{u}\|^2 \geq 0\end{aligned}$$

Weiter gilt die

## Lemma B-2.4 (Cauchy-Schwarzsche Ungleichung)

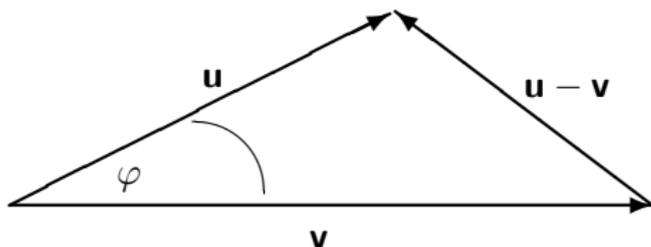
$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\| \|\mathbf{v}\|$$

### Bemerkung:

Die beiden Seiten sind nur dann genau gleich, wenn  $\varphi = 0$  oder  $\varphi = \pi = 180^\circ$ , d.h.  $\mathbf{v} = \lambda \mathbf{u}$  oder  $\mathbf{u} = \lambda \mathbf{v}$  sind für ein  $\lambda$ , das auch Null sein kann.

## Interpretation inneres Produkt im Anschauungsraum

Man betrachte das Dreieck  $\triangle ABC$  mit den Kanten  $\mathbf{u} = AB$ ,  $\mathbf{v} = AC$  und  $\mathbf{v} - \mathbf{u} = BC$ .



Für  $\|\mathbf{u} - \mathbf{v}\|^2$  gilt nach den oben aufgeführten Regeln

$$\begin{aligned}\|\mathbf{u} - \mathbf{v}\|^2 &= \langle \mathbf{u} - \mathbf{v}, \mathbf{u} - \mathbf{v} \rangle \\ &= \langle \mathbf{u} - \mathbf{v}, \mathbf{u} \rangle - \langle \mathbf{u} - \mathbf{v}, \mathbf{v} \rangle \\ &= \langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{v}, \mathbf{u} \rangle - \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle \\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2 \langle \mathbf{u}, \mathbf{v} \rangle .\end{aligned}$$

Sei  $\varphi$  der von  $\mathbf{u}$  und  $\mathbf{v}$  eingeschlossene Winkel. Setzt man nun

$$\langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u}\| \|\mathbf{v}\| \cos \varphi$$

in diese Gleichung ein, so ergibt sich der

### Lemma B-2.5 (Kosinussatz)

$$\begin{aligned} \|\mathbf{u} - \mathbf{v}\|^2 &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\| \|\mathbf{v}\| \cos \varphi \quad \text{bzw.} \\ |BC|^2 &= |AB|^2 + |AC|^2 - 2|AB| |AC| \cos(\sphericalangle BAC) \end{aligned}$$

Hierbei haben wir natürlich vorausgesetzt, dass weder  $\mathbf{u}$  noch  $\mathbf{v}$  gleich dem Nullvektor ist.

## Definition B-2.6 (Orthogonale Vektoren)

Man bezeichnet zwei Vektoren  $\mathbf{u}$  und  $\mathbf{v}$  als orthogonal zueinander, wenn der von ihnen eingeschlossene Winkel  $\pi/2 = 90^\circ$  ist, oder wenn einer von ihnen verschwindet, d.h. gleich Null ist. Formelmäßig schreibt man

$$\mathbf{u} \perp \mathbf{v}, \quad \text{falls} \quad \langle \mathbf{u}, \mathbf{v} \rangle = 0.$$

## Beispiel B-2.7

Die Einheitsvektoren  $\mathbf{e}_i$  bilden ein Orthogonalsystem in dem Sinne, dass

$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0 \quad \text{falls} \quad i \neq j.$$

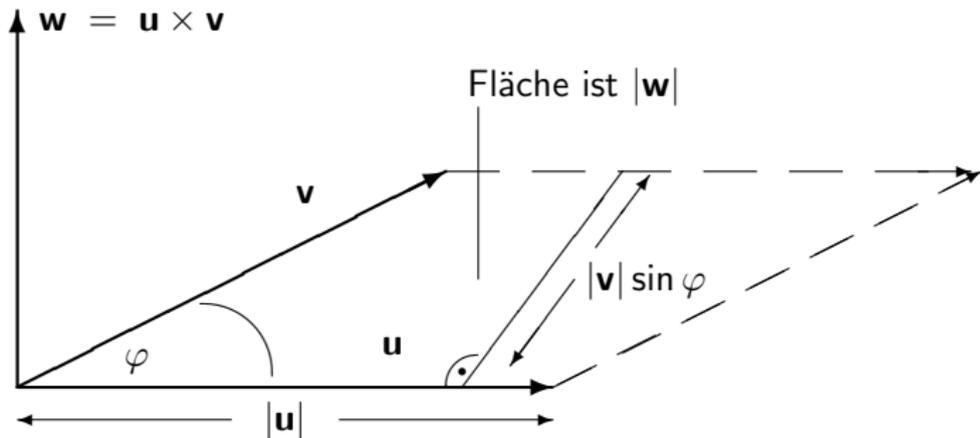
Es gibt aber auch noch andere Vektortripel mit dieser Eigenschaft. Das innere Produkt lässt sich entsprechend auf allen endlich dimensional Räumen definieren, es gibt dazu sogar mehrere Möglichkeiten.

## Vektor- oder Kreuzprodukt

Dieses Produkt ist nur im dreidimensionalen Anschauungsraum eindeutig definiert.

### Definition B-2.8 (Vektor- oder Kreuzprodukt)

Zu je zwei nicht verschwindenden Vektoren  $\mathbf{u}$  und  $\mathbf{v}$  bezeichnet man als **Vektor- oder Kreuzprodukt** den Vektor  $\mathbf{w} = \mathbf{u} \times \mathbf{v}$ , dessen Richtung zu  $\mathbf{u}$  und  $\mathbf{v}$  orthogonal ist und dessen Länge  $|\mathbf{w}|$  gleich der Fläche des von  $\mathbf{u}$  und  $\mathbf{v}$  aufgespannten Parallelogramms ist. Weiter sei, von der Spitze von  $\mathbf{w}$  betrachtet,  $\mathbf{v}$  weniger als  $\pi = 180^\circ$  gegen den Uhrzeigersinn von  $\mathbf{u}$  weggedreht.



## Rechtssystem

Zeigt man mit dem Daumen und dem Zeigefinger längs der Vektoren  $\mathbf{u}$  und  $\mathbf{v}$ , so muss  $\mathbf{w}$  in die Richtung des nach innen abgeknickten Mittelfingers zeigen.

In diesem Sinne sind auch die drei Basisvektoren  $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$  rechtshändig orientiert.

Gemäß den oben genannten Anforderungen gilt nun insbesondere:

$$\begin{aligned} \mathbf{e}_1 \times \mathbf{e}_2 &= \mathbf{e}_3, & \mathbf{e}_1 \times \mathbf{e}_3 &= -\mathbf{e}_2 \\ \mathbf{e}_2 \times \mathbf{e}_1 &= -\mathbf{e}_3, & \mathbf{e}_2 \times \mathbf{e}_3 &= \mathbf{e}_1 \\ \mathbf{e}_3 \times \mathbf{e}_1 &= \mathbf{e}_2, & \mathbf{e}_3 \times \mathbf{e}_2 &= -\mathbf{e}_1. \end{aligned}$$

Es lässt sich zeigen, dass ausserdem gilt:

### Lemma B-2.9 (Vorzeichen des Vektorproduktes)

*Werden die Vektoren  $\mathbf{u}$  und  $\mathbf{v}$  im Vektorprodukt vertauscht, dann ändert sich nur das Vorzeichen des Vektorproduktes:*

$$\mathbf{u} \times \mathbf{v} = -(\mathbf{v} \times \mathbf{u})$$

### Lemma B-2.10 (Bilinearität)

*Für beliebige Vektoren  $\mathbf{u}, \mathbf{v}, \mathbf{w}$  und Skalare  $\lambda$  gilt:*

$$\mathbf{u} \times (\mathbf{v} + \mathbf{w}) = \mathbf{u} \times \mathbf{v} + \mathbf{u} \times \mathbf{w}$$

$$(\mathbf{u} + \mathbf{v}) \times \mathbf{w} = \mathbf{u} \times \mathbf{w} + \mathbf{v} \times \mathbf{w}$$

$$\lambda(\mathbf{u} \times \mathbf{v}) = (\lambda\mathbf{u}) \times \mathbf{v} = \mathbf{u} \times (\lambda\mathbf{v}) = -\lambda(\mathbf{v} \times \mathbf{u})$$

## Lemma B-2.11

Auf Grund der Bilinearität ergibt sich nun für beliebiges  $\mathbf{u} = (\mu_1, \mu_2, \mu_3)^T$  und  $\mathbf{v} = (\nu_1, \nu_2, \nu_3)^T$

$$\mathbf{w} = \mathbf{u} \times \mathbf{v} = \begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix} = \begin{pmatrix} \mu_2\nu_3 - \mu_3\nu_2 \\ \mu_3\nu_1 - \mu_1\nu_3 \\ \mu_1\nu_2 - \mu_2\nu_1 \end{pmatrix}$$

Diese Bildungsvorschrift merkt man sich am besten, indem man sie als die (formale) Determinante einer  $(3 \times 3)$  Matrix interpretiert. (Determinanten werden in einem der nächsten Abschnitte behandelt.) Und zwar gilt

$$\mathbf{u} \times \mathbf{v} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix}.$$

### Bemerkung:

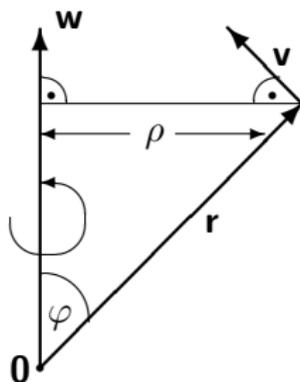
Hierbei handelt es sich allerdings nicht um eine gewöhnliche Matrix, da die drei Elemente in der ersten Zeile Vektoren, die Elemente der zweiten und dritten Zeile aber Skalare sind.

Eine wichtige Anwendung des Kreuzproduktes in der Mechanik ist die **Drehung eines Körpers um eine feste Achse mit der konstanten Winkelgeschwindigkeit**  $\omega$ . Man beschreibt diese Rotation durch einen Vektor  $\mathbf{w}$ , dessen Richtung  $\frac{\mathbf{w}}{\|\mathbf{w}\|}$  parallel zur Rotationsachse ist und dessen Länge die Winkelgeschwindigkeit repräsentiert, so dass  $\omega = \|\mathbf{w}\|$  ist.

Der Vektor  $\mathbf{w}$  ist so orientiert, dass die Drehung beim Blicken entlang seiner Richtung im Uhrzeigersinn erfolgt.

Ohne wesentliche Beschränkung der Allgemeinheit nehme man nun an, daß die Drehachse genau durch den Ursprung verläuft.

Dann erhält man den momentanen Geschwindigkeitsvektor  $\mathbf{v}$  eines Körperpunktes  $P$  mit derzeitigem Ortsvektor  $\mathbf{r} = \overrightarrow{OP}$  als  $\mathbf{v} = \mathbf{w} \times \mathbf{r}$ .



Diese Formel ergibt sich gemäß der Zeichnung aus der Beobachtung, daß die momentane Bewegungsrichtung  $\mathbf{v}/\|\mathbf{v}\|$  orthogonal zu  $\mathbf{w}$  und  $\mathbf{r}$  sein muß und dass der Geschwindigkeitsbetrag  $\|\mathbf{v}\|$  gleich  $\omega$  mal dem Abstand von der Achse, also  $\|\mathbf{r}\| \sin(\phi)$ , ist.

Hierbei ist  $\varphi$  der von den Vektoren  $\mathbf{w}$  und  $\mathbf{r}$  eingeschlossene Winkel und die Orientierung der resultierenden Geschwindigkeit  $\mathbf{v}$  ist so, daß  $\mathbf{w}$ ,  $\mathbf{r}$ ,  $\mathbf{v}$  ein rechtshändiges System bilden.

$$\mathbf{w} \cdot \mathbf{v} = 0 = \mathbf{r} \cdot \mathbf{v}$$

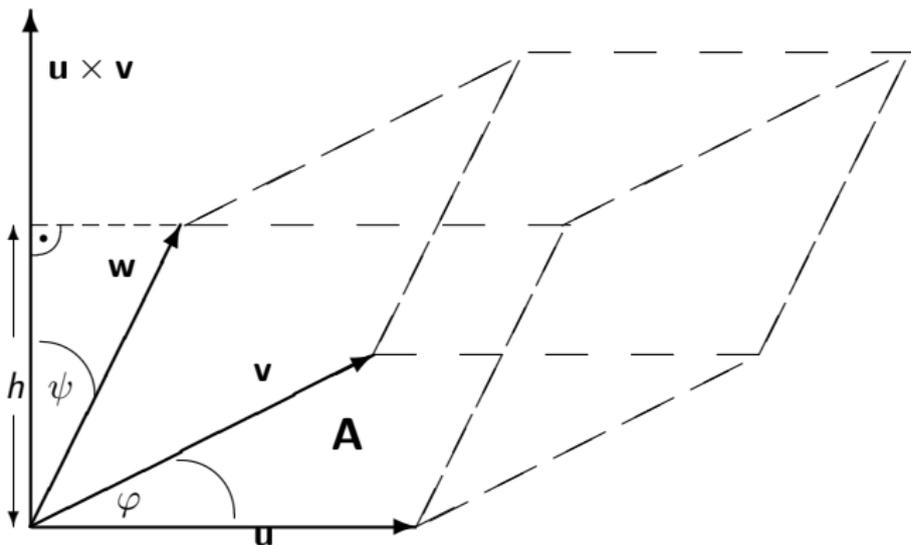
$$\|\mathbf{v}\| = \rho\omega = \|\mathbf{r}\| |\sin \varphi| \|\mathbf{w}\| = \|\mathbf{r} \times \mathbf{w}\|$$

## Spatprodukt

### Definition B-2.12 (Spatprodukt)

Bildet man das Skalarprodukt zwischen  $\mathbf{u} \times \mathbf{v}$  und einem dritten Vektor  $\mathbf{w}$ , so ergibt sich das sogenannte Spatprodukt:

$$[\mathbf{u}, \mathbf{v}, \mathbf{w}] \equiv (\mathbf{u} \times \mathbf{v}) \cdot \mathbf{w} \in \mathbb{R}.$$



## Lemma B-2.13 (Betrag Spatprodukt)

*Gemäß der Zeichnung ergibt der Betrag*

$$|[\mathbf{u}, \mathbf{v}, \mathbf{w}]| = \underbrace{(\|\mathbf{u}\| \|\mathbf{v}\| \sin(\varphi))}_A \underbrace{\|\mathbf{w}\| \cos(\psi)}_h$$

*genau das Volumen des Parallelepipeds mit der Grundfläche  $A$  und der Höhe  $h$ .*

## Folgerung B-2.14

*Daraus sieht man unmittelbar, daß das Spatprodukt bis auf das Vorzeichen von der Reihenfolge der Vektoren  $\mathbf{u}$ ,  $\mathbf{v}$ ,  $\mathbf{w}$  unabhängig ist, da diese immer das gleiche Parallelepiped aufspannen.*

## Lemma B-2.15 (Vorzeichen Spatprodukt)

Für das **Vorzeichen** gilt die folgende Regel:

$$[\mathbf{u}, \mathbf{v}, \mathbf{w}] \begin{cases} > 0 & \text{falls } (\mathbf{u}, \mathbf{v}, \mathbf{w}) \text{ Rechtssystem} \\ < 0 & \text{falls } (\mathbf{u}, \mathbf{v}, \mathbf{w}) \text{ Linkssystem} \\ = 0 & \text{falls } (\mathbf{u}, \mathbf{v}, \mathbf{w}) \text{ linear abhängig} \end{cases}$$

Hierbei bezeichnet der Begriff **linear abhängig** den Zustand, dass die drei Vektoren in einer Ebene liegen und es deshalb nicht triviale Koeffizienten  $\alpha, \beta, \gamma$  gibt, für die

$$\alpha \mathbf{u} + \beta \mathbf{v} + \gamma \mathbf{w} = \mathbf{0} \quad \text{gilt.}$$

## Lemma B-2.16 (Identität im Anschauungsraum)

$$[\mathbf{u}, \mathbf{v}, \mathbf{w}] = \begin{vmatrix} \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \\ \omega_1 & \omega_2 & \omega_3 \end{vmatrix},$$

wobei  $\mathbf{w} = (\omega_1, \omega_2, \omega_3)$  ist.

## B-3 Abstandsnormen

Eine ganz zentrale Rolle in der linearen Algebra und (allgemeiner der sogenannten Funktionalanalysis) spielt der Begriff des **Abstandes** zwischen zwei Vektoren (z.B. auch Funktionen). Dadurch ergibt sich die Möglichkeit, „Kugeln“ und andere „Umgebungen“ von Vektoren zu betrachten die „nahe“ beieinander liegen.

### Definition B-3.1 (Norm und normierter Raum)

Ein linearer Vektorraum  $\mathcal{V}$  heisst **normiert**, wenn es zu jedem  $\mathbf{u} \in \mathcal{V}$  eine reelle Zahl  $\|\mathbf{u}\|$  gibt, so dass für beliebige  $\lambda \in \mathbb{R}$  und  $\mathbf{v} \in \mathcal{V}$  gilt:

$$\blacktriangleright \|\mathbf{u}\| \geq 0 \quad \text{mit} \quad \|\mathbf{u}\| = 0 \iff \mathbf{u} = \mathbf{0}$$

**Definitheit**

$$\blacktriangleright \|\lambda \mathbf{u}\| = |\lambda| \|\mathbf{u}\|$$

**Homogenität**

$$\blacktriangleright \|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$$

**Dreiecksungleichung**

Hier ist  $|\lambda|$  der gewöhnliche Betrag reeller Zahlen.

Aus der Cauchy-Schwarz-Ungleichung folgt unmittelbar die Dreiecksungleichung für die euklidische Norm  $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle} = \sqrt{\mathbf{u}^T \mathbf{u}}$ , da

$$\begin{aligned}\|\mathbf{u} + \mathbf{v}\|^2 &= \langle \mathbf{u}, \mathbf{u} \rangle + 2 \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle \\ &\leq \|\mathbf{u}\|^2 + 2 |\langle \mathbf{u}, \mathbf{v} \rangle| + \|\mathbf{v}\|^2 \\ &\leq \|\mathbf{u}\|^2 + 2 \|\mathbf{u}\| \|\mathbf{v}\| + \|\mathbf{v}\|^2 \\ &= (\|\mathbf{u}\| + \|\mathbf{v}\|)^2\end{aligned}$$

Auch die Homogenität ist gewährleistet, da

$$\|\lambda \mathbf{u}\| = \sqrt{\langle \lambda \mathbf{u}, \lambda \mathbf{u} \rangle} = |\lambda| \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$$

Dies gilt auch für verallgemeinerte Skalarprodukte, deren **Hilbert-Normen**  $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$  ebenfalls die Normeigenschaften erfüllen.

Man nennt den Vektorraum dann auch **Hilbert-Raum**.

In numerischen Anwendungen der Lineare Algebra werden neben der Euklidischen Norm häufig folgende anderen Normen benutzt:

- ▶ Für festes  $1 \leq p \leq \infty$  setze

$$\|\mathbf{v}\|_p = \|(\nu_1, \nu_2, \dots, \nu_n)^T\|_p = [|\nu_1|^p + |\nu_2|^p + \dots + |\nu_n|^p]^{1/p}$$

- ▶ Für  $p = 2$  erhält man wiederum die Euklidische Norm  $\|\mathbf{v}\|_2 = \|\mathbf{v}\|$ .  
Im Grenzfall  $p = \infty$  setzt man

$$\|\mathbf{v}\|_\infty = \|(\nu_1, \nu_2, \dots, \nu_n)^T\|_\infty = \max\{|\nu_1|, |\nu_2|, \dots, |\nu_n|\}$$

- ▶ Die Menge der Vektoren  $\mathbf{u}$  mit  $\|\mathbf{u}\|_1 \leq 1$  und  $\|\mathbf{u}\|_\infty \leq 1$  bilden für  $n = 2$  (d.h. in der Ebene) ein achsenparalleles bzw. diagonal orientiertes Quadrat.
- ▶ Bei den Zwischenwerten  $1 < p < \infty$  und insbesondere der Euklidischen Norm  $\|\mathbf{u}\|_2$  haben die verallgemeinerten Kugeln  $\{\mathbf{v} \in \mathcal{V} : \|\mathbf{u}\|_p \leq 1\}$  dagegen keine Ecken.
- ▶ Die beiden Grenzfälle  $p = 1$  und  $p = \infty$  haben den Vorteil, dass die entsprechenden Normen billig auswertbar sind.

## Lemma B- 3.2 (Weitere Normeigenschaften)

- ▶ Per Induktion ergibt sich für die **Summe** endlich vieler Vektoren  $\mathbf{v}_i, i = 1 \dots m$ , die Ungleichung

$$\left\| \sum_{i=1}^m \mathbf{v}_i \right\| \leq \sum_{i=1}^m \|\mathbf{v}_i\|$$

- ▶ Aus der Dreiecksungleichung folgt für alle Normen die sogenannte **umgekehrte Dreiecksungleichung**

$$\|\mathbf{u} - \mathbf{v}\| \geq \left| \|\mathbf{u}\| - \|\mathbf{v}\| \right|$$

- ▶ Eine Norm  $\|\mathbf{v}\|$  ist genau dann eine **Hilbert-Norm**, wenn sie die folgende **Parallelogrammgleichung** erfüllt

$$\|\mathbf{u} - \mathbf{v}\|^2 + \|\mathbf{u} + \mathbf{v}\|^2 = 2(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2)$$

### Bemerkung:

Im letzteren Fall lässt sich die Identität

$$\langle \mathbf{u}, \mathbf{v} \rangle = \frac{1}{4} [\|\mathbf{u} + \mathbf{v}\|^2 - \|\mathbf{u} - \mathbf{v}\|^2]$$

auch als Definition des Inneren Produktes interpretieren.

## B-4 Basen und Unterräume

Im vorigen Abschnitt wurde festgestellt, dass im Anschauungsraum drei Vektoren **linear abhängig** sind (d.h. in einer Ebene liegen), wenn ihr Spatprodukt verschwindet.

Das Konzept der linearen Abhängigkeit bzw. Unabhängigkeit ist von zentraler Bedeutung für die Untersuchung beliebiger Räume und ihrer sogenannten Unterräume.

## Definition B-4.1 (Lineare Abhängigkeit und Unabhängigkeit)

Eine Familie (= Menge) von Vektoren  $\{\mathbf{v}_i\}_{i=1}^r \subset \mathcal{V}$  heißt **linear abhängig**, wenn es Skalare  $\{\lambda_i\}_{i=1}^r \subset \mathbb{R}$  gibt so daß gilt

$$\sum_{i=1}^n \lambda_i \mathbf{v}_i = \mathbf{0} \quad \text{und} \quad \sum_{i=1}^n |\lambda_i| \neq 0.$$

Die zweite Bedingung schließt die Möglichkeit aus, dass alle  $\lambda_i$  verschwinden, in welchem Falle die erste Bedingung trivialerweise für jede Familie  $\{\mathbf{v}_i\}_{i=1}^r \subset \mathcal{V}$  zuträfe.

Umgekehrt heißt eine Familie  $\{\mathbf{v}_i\}_{i=1}^r \subset \mathcal{V}$  **linear unabhängig**, falls

$$\sum_{i=1}^n \lambda_i \mathbf{v}_i = \mathbf{0} \quad \implies \quad \sum_{i=1}^n |\lambda_i| = 0.$$

## Folgerung B-4.2

*Man sieht leicht, daß eine Obermenge linear abhängiger Vektoren auch linear abhängig ist, während eine Untermenge linear unabhängiger Vektoren auch linear unabhängig ist.*

## Folgerung B-4.3

*Zwei Vektoren  $\mathbf{v}_1, \mathbf{v}_2$  sind genau dann linear abhängig, wenn sie parallel sind, da*

$$\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 = \mathbf{0}, \lambda_1 \neq 0 \implies \mathbf{v}_1 = -(\lambda_2/\lambda_1) \mathbf{v}_2 .$$

## Bemerkung:

Hierbei haben wir ohne Beschränkung der Allgemeinheit vorausgesetzt, dass  $\lambda_1 \neq 0$ . Entsprechendes gilt, wenn  $\lambda_2 \neq 0$ , aber möglicherweise  $\lambda_1 = 0$ .

## Folgerung B-4.4

Zwei nicht verschwindende, zueinander orthogonale Vektoren  $\mathbf{v}_1 \perp \mathbf{v}_2$  sind auf jeden Fall linear unabhängig.

### Beweis:

Um dies zu zeigen, bildet man das Skalarprodukt von  $\mathbf{v}_1$  mit beiden Seiten der Gleichung

$$\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 = \mathbf{0}$$

und erhält

$$\lambda_1 \langle \mathbf{v}_1, \mathbf{v}_1 \rangle + \lambda_2 \langle \mathbf{v}_1, \mathbf{v}_2 \rangle = 0 = \lambda_1 |\mathbf{v}_1|^2$$

und somit  $\lambda_1 = 0$ .

Entsprechend folgt aus dem Skalarprodukt mit  $\mathbf{v}_2$  die Gleichung  $\lambda_2 = 0$  und damit die behauptete lineare Unabhängigkeit von  $\mathbf{v}_1$  und  $\mathbf{v}_2$ .  $\square$

### Beobachtung:

Dieselbe Schlussfolgerung kann man leicht für eine Familie von beliebig vielen paarweise orthogonalen Vektoren  $\{\mathbf{v}_i\}_{i=1}^r \subset \mathcal{V}$  mit  $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0$ ,  $\mathbf{v}_i \neq \mathbf{0}$ , für  $i \neq j$  durchführen. Deshalb sollte man Orthogonalität als eine besonders starke Form linearer Unabhängigkeit betrachten.

## Folgerung B-4.5 (Lineare Unabhängigkeit im $\mathbb{R}^3$ )

*Man kann zeigen, dass es im Anschauungsraum  $\mathbb{R}^3$  jeweils maximal drei linear unabhängige Vektoren ( wie z.B.  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ ) gibt.*

## Definition B-4.6 (Dimension eines Vektorraumes)

Die maximale Zahl linear unabhängiger Vektoren in einem Raum  $\mathcal{V}$  wird als dessen **Dimension**  $\dim(\mathcal{V})$  bezeichnet.

Falls es Familien linear unabhängiger Vektoren mit beliebig vielen Elementen in einem Raum  $\mathcal{V}$  gibt, so bezeichnet man ihn als **unendlichdimensional** und setzt  $\dim(\mathcal{V}) = \infty$ .

## Beispiel B-4.7

Der Raum aller Polynome ist unendlichdimensional, da die Familie der Monome (reine Potenzen von  $x$ )

$$x^j \quad j = 0, 1, \dots, n$$

für ein beliebiges  $n$  linear unabhängig ist.

## Bemerkung:

Im folgenden geht es darum nachzuweisen, dass der Dimensionsbegriff eindeutig ist und dass jede Menge linear unabhängiger Vektoren zu einer Basis (d.h. Menge von  $\dim \mathcal{V}$  linear unabhängigen Vektoren) erweitert werden kann.

## Lemma B-4.8 (Eindeutige Koeffizientendarstellung)

*Sei  $\{v_i\}_{i=1\dots m}$  eine Familie linear unabhängiger Vektoren irgendeines linearen Raumes  $\mathcal{V}$ . Dann besitzt jeder Vektor  $v \in \mathcal{V}$ , der zusammen mit den  $\{v_i\}_{i=1\dots m}$  keine linear unabhängige Menge bildet, eine eindeutige Darstellung*

$$\mathbf{v} = \sum_{i=1}^m \lambda_i \mathbf{v}_i$$

*Hierbei verschwinden alle  $\lambda_i$  genau dann wenn  $\mathbf{v} = 0$ .*

## Lemma B-4.9 (Austauschsatz)

Sei  $\{\mathbf{v}_i\}_{i=1\dots m}$  eine Familie linear unabhängiger Vektoren irgendeines linearen Raumes  $\mathcal{V}$ .

Dann gilt für jeden nichtverschwindenden Vektor  $\mathbf{v} \neq 0$

**entweder**

- ▶ Die Vereinigung  $\{\mathbf{v}_i\}_{i=1\dots m+1}$  ist mit  $\mathbf{v}_{m+1} \equiv \mathbf{v}$  auch linear unabhängig.

**oder**

- ▶ Es gibt einen Index  $j \leq m$ , so dass

$$\{\mathbf{v}_1, \dots, \mathbf{v}_{j-1}, \mathbf{v}, \mathbf{v}_{j+1}, \dots, \mathbf{v}_m\}$$

( $\mathbf{v}_j$  wurde durch  $\mathbf{v}$  ersetzt) weiterhin linear unabhängig ist.

## Bemerkung:

Wir nennen eine Familie von Vektoren **maximal linear unabhängig**, wenn die Hinzunahme irgendeines anderen Vektors die lineare Unabhängigkeit zerstört. Man nennt eine solche Menge dann auch **Basis des Raumes**. Der folgende Satz zeigt, dass alle Basen dieselbe Anzahl von Elementen haben: die Dimension des Raumes.

## Satz B-4.10 (Eindeutigkeit der Dimension)

Seien  $\{\mathbf{v}_i\}_{i=1\dots m}$  und  $\{\mathbf{w}_i\}_{i=1\dots n}$  zwei maximal unabhängige Familien von Vektoren.

Dann gilt  $m = n = \dim(\mathcal{V})$  und für jeden Vektor  $u \in \mathcal{V}$  gibt es eindeutige Koeffizienten  $\{\alpha_i\}_{i=1}^n \subset \mathbb{R}$  und  $\{\beta_i\}_{i=1}^n \subset \mathbb{R}$  so dass

$$\sum_{i=1}^n \alpha_i \mathbf{v}_i = \mathbf{u} = \sum_{i=1}^n \beta_i \mathbf{w}_i .$$

## Unterräume und Linearkombinationen

Gerade in unendlichdimensionalen Räumen muss man oft praktische Untersuchungen auf einem endlichdimensionalen Unterraum beschränken (z.B. indem man den Grad von Polynomen mehr oder minder willkürlich beschränkt).

### Definition B-4.11 (Unterraum)

Ein **Unterraum** ist eine **Menge**  $\mathcal{U} \subset \mathcal{V}$ , die bezüglich der Addition von Vektoren und deren Multiplikation mit Skalaren **abgeschlossen** ist, d.h. es gilt für alle  $\mathbf{u}, \mathbf{v} \in \mathcal{U}$  und  $\lambda \in \mathbb{R}$  die Implikation

$$\mathbf{u}, \mathbf{v} \in \mathcal{U} \quad \implies \quad \mathbf{u} + \mathbf{v} \in \mathcal{U}, \quad \lambda \mathbf{u} \in \mathcal{U}.$$

### Beispiel B-4.12

Triviale Beispiele von Unterräumen sind  $\mathcal{V}$  selbst und der nur aus dem Nullvektor bestehende Raum  $\{\mathbf{0}\}$ , den man als nulldimensional betrachtet.

## Beispiel B-4.13 (Orthogonales Komplement)

Ein interessanteres Beispiel ist das **orthogonale Komplement**

$$\mathbf{v}^\perp \equiv \mathcal{U} = \{\mathbf{u} \in \mathcal{V} \mid \langle \mathbf{v}, \mathbf{u} \rangle = 0\}$$

eines fest vorgegebenen Vektors  $\mathbf{v}$ .

Die Abgeschlossenheit und damit Unterraumeigenschaft ersieht man aus der Tatsache, daß für alle  $\mathbf{u}, \mathbf{w} \in \mathcal{U}$  und  $\lambda \in \mathbb{R}$

$$\langle \mathbf{v}, \mathbf{u} \rangle = 0 = \langle \mathbf{v}, \mathbf{w} \rangle \quad \implies \quad \langle \mathbf{v}, \mathbf{u} + \mathbf{w} \rangle = 0 = \langle \mathbf{v}, \lambda \mathbf{u} \rangle .$$

Mit anderen Worten: Gehören  $\mathbf{u}$  und  $\mathbf{w}$  zum orthogonalen Komplement von  $\mathbf{v}$ , so gilt dies auch für die Summe  $\mathbf{u} + \mathbf{w}$  und das Produkt  $\lambda \mathbf{u}$ .

## Satz B-4.14 (Schnittprinzip, siehe auch Lemma A-2.2)

Für zwei Unterräume  $\mathcal{U}, \mathcal{W} \subset \mathcal{V}$  bildet deren Durchschnitt

$$\mathcal{U} \cap \mathcal{W} = \{\mathbf{v} \in \mathcal{V} \mid \mathbf{v} \in \mathcal{U} \wedge \mathbf{v} \in \mathcal{W}\}$$

einen Unterraum.

## Satz B-4.15

Der Schnitt mehrerer und sogar unendlich vieler Unterräume bildet einen Unterraum.

## Beispiel B-4.16

Für eine beliebige Menge von Vektoren  $\mathcal{M} \subset \mathcal{V}$  ergibt sich das orthogonale Komplement als

$$\mathcal{M}^\perp \equiv \bigcap_{\mathbf{v} \in \mathcal{M}} \mathbf{v}^\perp = \{\mathbf{u} \in \mathcal{V} \mid \forall \mathbf{v} \in \mathcal{M} : \langle \mathbf{u}, \mathbf{v} \rangle = 0\}.$$

## Bemerkung:

Im Gegensatz zum Durchschnitt ist die mengentheoretische Vereinigung von zwei Unterräumen  $\mathcal{U}, \mathcal{W} \subset \mathcal{V}$  nur dann selbst ein Unterraum, wenn  $\mathcal{U}$  schon in  $\mathcal{W}$  oder  $\mathcal{W}$  schon in  $\mathcal{U}$  enthalten ist (siehe Warnung in **A-2**). Es gibt jedoch einen kleinsten Unterraum von  $\mathcal{V}$ , der sowohl  $\mathcal{U}$  als auch  $\mathcal{W}$  enthält und mit  $\mathcal{U} + \mathcal{W}$  bezeichnet wird.

Diese Bezeichnung ist sinnvoll, denn es gilt:

$$\mathcal{U} + \mathcal{W} = \{ \mathbf{u} + \mathbf{w} \mid \mathbf{u} \in \mathcal{U}, \mathbf{w} \in \mathcal{W} \}.$$

Man sagt dann auch, daß die Summe  $\mathcal{U} + \mathcal{W}$  von  $\mathcal{U}$  und  $\mathcal{W}$  aufgespannt wird.

Natürlich kann man auch die Summe mehrerer Unterräume bilden, was besonders dann von Interesse ist, wenn diese jeweils eindimensional sind.

## Definition B-4.17 (Linearkombination der Vektoren)

Für eine Familie  $\{\mathbf{v}_i\}_{i=1}^r \subset \mathcal{V}$  bezeichnet man jeden Vektor der Form

$$\mathbf{v} = \sum_{i=1}^r \lambda_i \mathbf{v}_i \quad \lambda_1, \dots, \lambda_r \in \mathbb{R}$$

als eine **Linearkombination der Vektoren  $\mathbf{v}_i$** .

## Definition B-4.18 (Lineare Hülle, vergleiche A-2.10)

Die Menge aller möglichen Linearkombinationen von Vektoren  $\{\mathbf{v}_i\}_{i=1}^r = \mathcal{U}$  aus einer Teilmenge  $\mathcal{U} \subset \mathcal{V}$  bezeichnet man als deren **lineare Hülle**

$$\text{span}(\mathcal{U}) = \left\{ \mathbf{v} = \sum_{i=1}^r \lambda_i \mathbf{v}_i \mid \lambda_i \in \mathbb{R}, \mathbf{v}_i \in \mathcal{U} \right\} .$$

Die lineare Hülle ist abgeschlossen. Man bezeichnet sie deshalb auch als den von  $\{\mathbf{v}_i\}_{i=1}^r = \mathcal{U} \subset \mathcal{V}$  **aufgespannten Unterraum**.

## Definition B-4.19 (Basis eines Unterraumes)

Falls die Vektoren  $\{\mathbf{v}_i\}_{i=1}^r$  linear unabhängig sind, bezeichnet man sie als eine **Basis** des von ihnen aufgespannten Unterraumes.

## Folgerung B-4.20

*Aus der vorausgesetzten linearen Unabhängigkeit folgt die Eindeutigkeit der Darstellung eines beliebigen Vektors  $\mathbf{v}$  als Linearkombination.*

## Lemma B-4.21

Bezüglich einer bestimmten Basis  $\{\mathbf{v}_i\}_{i=1}^r$  hat jeder Vektor  $\mathbf{w} \in \mathcal{V}$  eine eindeutige Darstellung

$$\mathbf{w} = \sum_{i=1}^r \lambda_i \mathbf{v}_i$$

### Beweis.

Aus

$$\sum_{i=1}^r \lambda_i \mathbf{v}_i = \mathbf{w} = \sum_{i=1}^r \gamma_i \mathbf{v}_i$$

erhält man durch Abzug der rechten Seite von der linken

$$0 = \sum_{i=1}^r (\lambda_i \mathbf{v}_i - \gamma_i \mathbf{v}_i) = \sum_{i=1}^r (\lambda_i - \gamma_i) \mathbf{v}_i,$$

so dass wegen der linearen Unabhängigkeit der Basisvektoren notwendigerweise alle  $\lambda_i - \gamma_i = 0$  sind. Also sind die Koeffizienten  $\lambda_i = \gamma_i$  von  $\mathbf{w}$  bezüglich der gewählten Basis eindeutig bestimmt. □

## Beispiel B - 4.22

Es sei

$$\mathcal{P}_n \equiv \left\{ \sum_{i=0}^{n-1} \gamma_i x^i \mid \gamma_i \in \mathbb{R} \right\}$$

die Menge aller Polynome mit reellen Koeffizienten vom Grade kleiner  $n$ .  
 Bezüglich der üblichen Addition von Polynomen und ihrer Multiplikation mit reellen Skalaren ist  $\mathcal{P}_n$  ein Vektorraum.

Die Monome  $\{\mathbf{v}_i = x^{i-1}\}_{i=1}^n$  bilden eine Basis des Vektorraumes  $\mathcal{P}_n$ , der deshalb  $n$ -dimensional ist.

### Beweisidee:

Zur linearen Unabhängigkeit: Es gebe eine nichttriviale Linearkombination, die das Nullpolynom ergibt,

$$P(x) = \sum_{i=1}^n \lambda_i \mathbf{v}_i = \sum_{i=1}^n \lambda_i x^{i-1} = 0.$$

Einerseits kann  $P(x)$  nur maximal  $n - 1$  Nullstellen haben, siehe Folgerung aus Korollar A - 13.1. Im Widerspruch dazu ist jedes  $x \in \mathbb{R}$  eine Nullstelle von  $P(x)$ .

Also müssen alle Koeffizienten  $\lambda_i$  von  $P(x)$  gleich Null sein. □

### Bemerkung:

Obwohl die Monombasis von  $\mathcal{P}_n$  sehr natürlich erscheint, ist sie keineswegs für alle im Zusammenhang mit Polynomen auftretenden mathematischen Aufgaben geeignet.

Allgemein kommen in linearen Räumen oftmals verschiedene Basen zur Anwendung, je nachdem, welche Art von Berechnung oder Untersuchung durchgeführt werden soll. Das Umrechnen der Koeffizienten eines Vektors von einer Basis auf eine andere nennt man Basistransformation. Diese verlangt normalerweise die Lösung eines linearen Gleichungssystems, wie sie im entsprechenden Abschnitt weiter unten behandelt wird.

## Bemerkung: Orthogonalitätsbedingung, orthonormale Basis

Rechnerisch besonders angenehm sind Basen, welche die **Orthogonalitätsbedingung**

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

erfüllen. Bei solchen **orthonormalen** Basen lassen sich die Koeffizienten  $\lambda_j$  eines beliebigen Vektors  $\mathbf{w}$  leicht berechnen:

Aus dem Ansatz 
$$\mathbf{w} = \sum_{j=1}^n \lambda_j \mathbf{v}_j$$

folgt durch die Bildung des inneren Produktes mit einem bestimmten Basisvektor  $\mathbf{v}_i$  sofort

$$\langle \mathbf{v}_i, \mathbf{w} \rangle = \sum_{j=1}^n \lambda_j \langle \mathbf{v}_i, \mathbf{v}_j \rangle = \lambda_i,$$

da alle Summanden mit  $j \neq i$  verschwinden.

## Beispiel B - 4.23

In einem verallgemeinerten Sinne des Basisbegriffs bilden die trigonometrischen Funktionen

$$\mathbf{v}_{2j} \equiv \sin(jx) \quad \text{und} \quad \mathbf{v}_{2j+1} \equiv \cos(jx) \quad \text{für } j = 1, 2, \dots$$

zusammen mit der konstanten Funktion  $\mathbf{v}_1 \equiv 1$  eine Basis des unendlichdimensionalen Raumes aller Funktionen  $f(x)$ , die auf dem Intervall  $[-\pi, \pi]$  periodisch und quadratisch integrierbar sind.

Letzteres bedeutet, dass die Funktion  $f^2(x)$  ein endliches Integral auf  $[-\pi, \pi]$  hat. Das ist zum Beispiel dann der Fall, wenn  $f(x)$  bis auf endlich viele Sprungstellen **stetig** ist. Das innere Produkt, bezüglich dessen die trigonometrischen Funktionen eine orthogonale Basis bilden, ist nun das Integral

$$\langle f, g \rangle = \int_{-\pi}^{\pi} f(x)g(x) dx .$$

## Fortsetzung Beispiel

Die Orthogonalitätseigenschaften lassen sich hier mittels wiederholter partieller Integration oder mit Hilfe geeigneter trigonometrischer Umformungen leicht nachweisen. Allerdings müssen die Funktionen  $\mathbf{v}_j$  noch geeignet skaliert werden, so daß dann  $\|\mathbf{v}_j\| = 1$  gilt.

Dies vorausgesetzt lassen sich die Koeffizienten einer beliebigen Funktion  $f(x)$  bezüglich der Basisfunktion  $\sin(jx)$  als inneres Produkt

$$\int_{-\pi}^{\pi} f(x) \sin(jx) dx$$

berechnen.

## Warnung:

Da sich diese Integrale im allgemeinen nicht formelmäßig auswerten lassen, kommen hierbei in der Praxis oft Quadraturen, d.h. numerische Integrationsverfahren, zur Anwendung.

Streng genommen besteht der Vektorraum nicht aus den Funktionen selbst, sondern seine Elemente bilden Äquivalenzklassen von Funktionen, die sich nur an endlich vielen Punkten unterscheiden, so dass das Integral des Quadrates ihrer Differenz Null ergibt.

Die genauere Untersuchung und Beschreibung von Funktionenräumen und ihrer Basen ist der Ausgangspunkt der mathematischen Disziplin **Funktionalanalysis**.

## B-5 Lineare Abbildungen

### Definition B-5.1 (Lineare Abbildung)

Eine Abbildung  $\mathbf{F} : \mathcal{V} \rightarrow \mathcal{W}$  zwischen zwei reellen Vektorräumen  $\mathcal{V}$  und  $\mathcal{W}$  heißt linear, falls für alle  $\mathbf{u}, \mathbf{v} \in \mathcal{V}$  und  $\lambda \in \mathbb{R}$  gilt:

$$\mathbf{F}(\mathbf{u} + \mathbf{v}) = \mathbf{F}(\mathbf{u}) + \mathbf{F}(\mathbf{v})$$

**Additivität**

$$\mathbf{F}(\lambda \mathbf{u}) = \lambda \mathbf{F}(\mathbf{u})$$

**Homogenität**

### Bemerkung

Mit anderen Worten:  $F$  ist ein Vektorraumhomomorphismus im Sinne der auf Gruppen und Ringe zugeschnittenen algebraischen Definition A-6.4.

### Bemerkung

Die beiden definierenden Eigenschaften können auch zu der einen

$$F(\mathbf{u} + \lambda \mathbf{v}) = F(\mathbf{u}) + \lambda F(\mathbf{v}) \text{ für alle } \mathbf{u}, \mathbf{v} \in \mathcal{V}$$

$\lambda \in \mathbb{R}$  zusammengefasst werden.

## Assoziierte Unterräume

Entsprechend zum Lemma A-6.10 kann man zu einer linearen Abbildung  $F : \mathcal{U} \rightarrow \mathcal{V}$  als Gruppenhomomorphismus die Teilmengen

- ▶ **Kern**  $F = \{\mathbf{u} \in \mathcal{U} : F(\mathbf{u}) = \mathbf{0} \in \mathcal{V}\} = F^{-1}(\{\mathbf{0}\})$  und
- ▶ **Bild**  $F = \{F(\mathbf{u}) \in \mathcal{V} : \mathbf{u} \in \mathcal{U}\} = F(\mathcal{U})$

konstruieren.

Es ergeben sich folgende Aussage über Null, Bild und Kern.

### Lemma B- 5.2

- (i) *Jede lineare Abbildung bildet die Null von  $\mathcal{U}$  in die Null von  $\mathcal{V}$  ab.*
- (ii) *Die Bildmenge  $F(\mathcal{W}) \subset \mathcal{V}$  jedes Unterraums  $\mathcal{W} \subset \mathcal{U}$  ist ein Unterraum von  $\mathcal{V}$ .*
- (iii) *Der Kern von  $F$  ist ein linearer Unterraum von  $\mathcal{U}$ .*

## Beispiele linearer Abbildungen

### Beispiel B - 5.3 (Kreuzprodukt)

Im  $\mathbb{R}^3$  definiert das Kreuzprodukt für fest vorgegebenes  $\mathbf{u} \in \mathbb{R}^3$  eine lineare Abbildung  $K_{\mathbf{u}} : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  mit

$$\begin{aligned} \mathbf{v} \mapsto K_{\mathbf{u}}(\mathbf{v}) &= \mathbf{u} \times \mathbf{v} = \mathbf{u} \times \sum_{k=1}^3 v_k \mathbf{e}_k \\ &= v_1(\mathbf{u} \times \mathbf{e}_1) + v_2(\mathbf{u} \times \mathbf{e}_2) + v_3(\mathbf{u} \times \mathbf{e}_3) \\ &= \sum_{j,k=1}^3 u_j v_k \mathbf{e}_j \times \mathbf{e}_k = \sum_{i=1}^3 \left( \sum_{j,k=1}^3 \epsilon_{ijk} u_j v_k \right) \mathbf{e}_i \end{aligned}$$

Die letzte Schreibweise benutzt den sog. „Epsilon-Tensor“ mit den Werten

$$\epsilon_{ijk} = \begin{cases} 1 & \text{für die geraden Permutationen } (i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2); \\ -1 & \text{für die ungeraden Permutationen } (i, j, k) = (3, 2, 1), (2, 1, 3), (1, 3, 2); \\ 0 & \text{sonst für alle Nichtpermutationen.} \end{cases}$$

## Beispiel B-5.4 (Ableitung im Polynomraum)

Betrachte den Raum  $\mathcal{U} = \mathcal{V} = \mathcal{P}_n$  der Polynome mit reellen Koeffizienten vom Grad kleiner  $n = \dim(\mathcal{P}_n)$  in einer Variablen  $x$ . Dann ist die

### Differentiation

$$\mathbf{w} = \mathbf{F}(\mathbf{v}) = \mathbf{v}' = \frac{d\mathbf{v}}{dx}$$

eine lineare Operation, deren Ergebnis wiederum ein Polynom  $\mathbf{w} \in \mathcal{U}$  ist. Mit den Koeffizientendarstellungen

$$\mathbf{v} = \sum_{i=1}^n \nu_i x^{i-1} \quad \text{und} \quad \mathbf{w} = \sum_{i=1}^n \omega_i x^{i-1}$$

gilt  $\mathbf{w} = \mathbf{F}(\mathbf{v})$  genau dann, wenn

$$\omega_i = i \nu_{i+1} \quad \text{für} \quad i = 1 \dots n-1$$

und  $\omega_n = 0$ . Ein beliebiges  $\mathbf{w} \in \mathcal{V}$  ist also genau dann das Bildelement  $\mathbf{F}(\mathbf{v})$  für ein geeignetes  $\mathbf{v}$ , wenn der höchste Koeffizient  $\omega_n$  verschwindet.

## Folgerung B - 5.5

Wir erhalten im Wertevorrat  $\mathcal{V} = \mathcal{P}_n$  den  $(n - 1)$ -dimensionalen Bildbereich

$$\text{Bild}(\mathbf{F}) = \left\{ \sum_{i=1}^{n-1} \omega_i x^{i-1} \mid \omega_i \in \mathbb{R} \right\} = \mathcal{P}_{n-1}.$$

Umgekehrt fällt der Koeffizient  $\nu_1$  der konstanten Funktion  $x^0 = 1$  bei der Differentiation weg, und wir haben den eindimensionalen Kern

$$\text{Kern}(\mathbf{F}) = \{ \nu_1 x^0 \mid \nu_1 \in \mathbb{R} \} = \mathcal{P}_1.$$

Mit anderen Worten, die Differentiation bildet genau diejenigen Funktionen auf die Nullfunktion ab, die konstant sind. Es gilt also

$$\dim(\text{Bild}(\mathbf{F})) = n - 1 = \dim(\text{Dom}(\mathbf{F})) - \dim(\text{Kern}(\mathbf{F})),$$

wobei  $\text{Dom}(\mathbf{F}) = \mathcal{U}$  den **Definitionsbereich** von  $\mathbf{F}$  bezeichnet. Diese **Dimensionsformel** gilt auch im allgemeinen Fall linearer Abbildungen.

# Lineare Unabhängigkeit

## Lemma B - 5.6

*Linear abhängige Vektoren werden unter einer linearen Abbildung in linear abhängige Bildvektoren transformiert.*

Umkehrung:

Sind die Bildvektoren  $\mathbf{v}_1 = F(\mathbf{u}_1), \mathbf{v}_2 = F(\mathbf{u}_2), \dots, \mathbf{v}_k = F(\mathbf{u}_k)$  linear unabhängig, so sind es auch die Urbildvektoren  $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$ .

## Lemma B - 5.7

*Sei  $F : \mathcal{U} \rightarrow \mathcal{V}$  linear und  $\mathbf{u}_1, \dots, \mathbf{u}_n$  eine Basis von  $\mathcal{U}$ . Dann kann aus den Bildvektoren  $\mathbf{v}_1 = F(\mathbf{u}_1), \mathbf{v}_2 = F(\mathbf{u}_2), \dots, \mathbf{v}_n = F(\mathbf{u}_n)$  eine Basis des Bildunterraumes  $F(\mathcal{U}) = \text{Bild } F$  ausgewählt werden.*

Folgerung:

Ist  $\mathcal{U}$  endlichdimensional, so auch  $\text{Bild } F = F(\mathcal{U})$ .

## Satz B-5.8 (Dimensionsformel)

Seien  $\mathcal{U}, \mathcal{V}$  endlichdimensional und  $F : \mathcal{U} \rightarrow \mathcal{V}$  linear. Dann gilt

$$\dim \mathcal{U} = \dim \text{Kern } F + \dim \text{Bild } F$$

### Beweis

Seien  $\mathbf{b}_1, \dots, \mathbf{b}_r \in \mathcal{V}$  eine Basis von  $\text{Bild } F$  und  $\mathbf{n}_1, \dots, \mathbf{n}_s \in \mathcal{U}$  eine Basis von  $\text{Kern } F$ .

Dann gibt es  $\mathbf{a}_1, \dots, \mathbf{a}_r \in \mathcal{U}$  mit  $\mathbf{b}_1 = F(\mathbf{a}_1), \dots, \mathbf{b}_r = F(\mathbf{a}_r)$ .

Zu zeigen:

Das System  $\mathbf{a}_1, \dots, \mathbf{a}_r, \mathbf{n}_1, \dots, \mathbf{n}_s$  ist eine Basis von  $\mathcal{U}$ , d.h.

- (i) es erzeugt  $\mathcal{U}$  und
- (ii) es ist linear unabhängig.

Ist dies gezeigt, so folgt die Behauptung aus

$$\dim \mathcal{U} = r + s = \dim \text{Bild } F + \dim \text{Kern } F .$$

zu (i): Das System  $\mathbf{a}_1, \dots, \mathbf{a}_r, \mathbf{n}_1, \dots, \mathbf{n}_s$  erzeugt  $\mathcal{U}$ .

Sei  $\mathbf{u} \in \mathcal{U}$  beliebig. Dann gibt es  $x_1, \dots, x_r \in \mathbb{R}$  mit

$$F(\mathbf{u}) = x_1 \mathbf{b}_1 + \dots + x_r \mathbf{b}_r = F(x_1 \mathbf{a}_1 + \dots + x_r \mathbf{a}_r).$$

Daher ist  $\mathbf{u} - (x_1 \mathbf{a}_1 + \dots + x_r \mathbf{a}_r) \in \text{Kern } F$  und es gibt  $y_1, \dots, y_s \in \mathbb{R}$  mit

$$\begin{aligned} \mathbf{u} - (x_1 \mathbf{a}_1 + \dots + x_r \mathbf{a}_r) &= y_1 \mathbf{n}_1 + \dots + y_s \mathbf{n}_s \\ \iff \mathbf{u} &= x_1 \mathbf{a}_1 + \dots + x_r \mathbf{a}_r + y_1 \mathbf{n}_1 + \dots + y_s \mathbf{n}_s. \end{aligned}$$

zu(ii): Das System  $\mathbf{a}_1, \dots, \mathbf{a}_r, \mathbf{n}_1, \dots, \mathbf{n}_s$  ist linear unabhängig

Für jede Linearkombination  $\mathbf{0} = x_1 \mathbf{a}_1 + \dots + x_r \mathbf{a}_r + y_1 \mathbf{n}_1 + \dots + y_s \mathbf{n}_s$  gilt

$$\mathbf{0} = F(\mathbf{0}) = x_1 \mathbf{b}_1 + \dots + x_r \mathbf{b}_r + \mathbf{0} \implies x_1 = \dots = x_r = 0.$$

Dann ist aber

$$\mathbf{0} = \mathbf{0} + y_1 \mathbf{n}_1 + \dots + y_s \mathbf{n}_s \implies y_1 = \dots = y_s = 0.$$

# Abbildungseigenschaften

## Folgerung B-5.9

*Eine lineare Abbildung  $F : \mathcal{U} \rightarrow \mathcal{V}$  endlichdimensionaler Vektorräume ist genau dann injektiv, wenn  $\text{Kern } F = \{0\}$  gilt, was wiederum genau dann der Fall ist, wenn*

$$\dim \mathcal{U} = \dim \text{Bild } F$$

*gilt.*

*$F$  ist surjektiv, wenn  $\text{Bild } F = \mathcal{V}$  gilt, hier also genau dann, wenn*

$$\dim \text{Bild } F = \dim \mathcal{V}$$

*gilt.*

*$F$  ist also bijektiv genau dann, wenn*

$$\dim \mathcal{U} = \dim \text{Bild } F = \dim \mathcal{V}$$

*gilt.*

## Vektorgleichungen

Sei  $\mathbf{F} : \mathcal{U} \rightarrow \mathcal{V}$  linear und ein Vektor  $\mathbf{w} \in \mathcal{V}$  gegeben. Dann interessiert man sich für die Lösungen  $\mathbf{u} \in \mathcal{U}$  der **Vektorgleichung**

$$\mathbf{F}(\mathbf{u}) = \mathbf{w} .$$

Diese ist genau dann **lösbar**, wenn  $\mathbf{w} \in \text{Bild } \mathbf{F}$ . Für zwei Lösungen  $\mathbf{u}_1, \mathbf{u}_2 \in \mathcal{U}$  gilt

$$\mathbf{0} = \mathbf{w} - \mathbf{w} = \mathbf{F}(\mathbf{u}_2) - \mathbf{F}(\mathbf{u}_1) = \mathbf{F}(\mathbf{u}_2 - \mathbf{u}_1) ,$$

d.h. die Differenz zweier Lösungen ist ein Kernvektor,  $\mathbf{v} = \mathbf{u}_2 - \mathbf{u}_1 \in \text{Kern } \mathbf{F}$ . Ist umgekehrt  $\mathbf{u}$  eine Lösung und  $\mathbf{v} \in \text{Kern } \mathbf{F}$ , so gilt

$$\mathbf{F}(\mathbf{u} + \mathbf{v}) = \mathbf{F}(\mathbf{u}) + \mathbf{F}(\mathbf{v}) = \mathbf{w} + \mathbf{0} = \mathbf{w} ,$$

die Lösungsmenge ist somit die um die **spezielle inhomogene Lösung**  $\mathbf{u}$  verschobene **homogene Lösungsmenge**, wie der Kernunterraum auch genannt wird.

## Lemma B- 5.10 (Restklassen bezüglich eines Unterraums)

$\mathcal{W} \subset \mathcal{U}$  linearer Unterraum impliziert, dass

$$\mathbf{u} \sim \mathbf{w} \iff \mathbf{u} - \mathbf{w} \in \mathcal{W} \iff \exists \mathbf{v} \in \mathcal{W} : \mathbf{u} = \mathbf{w} + \mathbf{v}$$

eine Äquivalenzrelation ist.

Die entsprechenden Äquivalenzklassen

$$[\mathbf{u}] = \{\mathbf{w} \in \mathcal{U} : \mathbf{w} \sim \mathbf{u}\}$$

bilden einen Vektorraum  $\mathcal{U}/\mathcal{W}$  bezüglich der Operationen

$$[\mathbf{u}] + [\mathbf{w}] = [\mathbf{u} + \mathbf{w}] \quad \text{und} \quad \lambda[\mathbf{u}] = [\lambda\mathbf{u}].$$

Voneinander verschiedene Restklassen sind disjunkt. Elemente innerhalb einer Restklasse unterscheiden sich um ein Element von  $\mathcal{W}$ . D.h. die Restklassen bilden eine „Blätterung“ von  $\mathcal{U}$  in parallele Ebenen, die sich als Parallelverschiebungen des Unterraums  $\mathcal{W}$  ergeben.

## Folgerung B-5.11

Sei  $F : \mathcal{U} \rightarrow \mathcal{V}$  linear. Die Restklassen von  $\mathcal{U} / \text{Kern } F$  entsprechen den Urbildmengen von  $F$ , denn

$$\begin{aligned} [\mathbf{u}] &= \{\mathbf{w} \in \mathcal{U} : \mathbf{w} - \mathbf{u} \in \text{Kern } F\} \\ &= \{\mathbf{w} \in \mathcal{U} : F(\mathbf{w}) = F(\mathbf{u})\} = F^{-1}(\{F(\mathbf{u})\}) \end{aligned}$$

Daraus folgt die Isomorphie

$$\mathcal{U} / \text{Kern } F \simeq \text{Bild } F ,$$

dabei ist die Restklasse  $[\mathbf{u}]$  eindeutig dem Vektor  $F(\mathbf{u})$  zugeordnet.

Von besonderem Interesse sind lineare Abbildungen  $\mathbf{F} : \mathcal{U} \rightarrow \mathcal{V}$ , die **regulär** sind in dem Sinne, dass Lösungen  $\mathbf{u} \in \mathcal{U}$  von  $\mathbf{F}(\mathbf{u}) = \mathbf{w}$ , wenn sie überhaupt existieren, eindeutig sind.

Dies ist die Eigenschaft der Injektivität von  $\mathbf{F}$ , was äquivalent zu  $\text{Kern } \mathbf{F} = \{\mathbf{0}\}$  ist.

Mit anderen Worten: die Lösung der **inhomogenen** Vektorgleichung  $\mathbf{F}(\mathbf{v}) = \mathbf{w}$  ist eindeutig genau dann, wenn die entsprechende **homogene** Gleichung  $\mathbf{F}(\mathbf{u}) = \mathbf{0}$  nur die triviale Lösung  $\mathbf{u} = \mathbf{0}$  hat.

Im regulären Falle bezeichnet man die Zuordnung des Urbildes  $\mathbf{u} \in \mathcal{U}$  zum gegebenen Bildvektor  $\mathbf{w} = \mathbf{F}(\mathbf{v}) \in \text{Bild } \mathbf{F} \subset \mathcal{V}$  als die **Umkehrabbildung** oder die **inverse Abbildung**

$$\mathbf{F}^{-1} : \text{Bild}(\mathbf{F}) \rightarrow \text{Dom}(\mathbf{F}) .$$

Falls sie überhaupt existiert, ist die Inverse einer linearen Abbildung auch immer linear, d.h. es gilt für  $\mathbf{v}, \mathbf{w} \in \text{Bild } \mathbf{F} \subset \mathcal{V}$

$$\begin{aligned}\mathbf{F}^{-1}(\mathbf{v} + \mathbf{w}) &= \mathbf{F}^{-1}(\mathbf{v}) + \mathbf{F}^{-1}(\mathbf{w}) \\ \mathbf{F}^{-1}(\lambda \mathbf{w}) &= \lambda \mathbf{F}^{-1}(\mathbf{w}) .\end{aligned}$$

Das Auffinden von  $\mathbf{v} = \mathbf{F}^{-1}(\mathbf{w})$  für gegebenes  $\mathbf{w}$  bezeichnet man auch als **Lösen** der Vektorgleichung  $\mathbf{F}(\mathbf{v}) = \mathbf{w}$ . Stellt man eine Vektorgleichung bezüglich gewählter Basen in  $\mathcal{U}$  und  $\mathcal{V}$  komponentenweise dar, so ergibt sich ein **System skalarer Gleichungen**, ein **lineares Gleichungssystem**.

Das effektive und genaue Lösen von linearen Gleichungssystemen bei gleichzeitiger Untersuchung ihrer Regularität ist nach wie vor eine zentrale Aufgabe im „**Wissenschaftlichen Rechnen**“. Dabei werden Ergebnisse und Methoden der Informatik und Numerischen Mathematik eingesetzt, um Systeme mit Tausenden oder sogar Millionen von Unbekannten zumindest näherungsweise zu lösen.

Eine zweite, für Anwendungen sehr wichtige Aufgabe ist die Lösung von **Eigenwertproblemen**. Ist eine lineare Abbildung  $F : \mathcal{V} \rightarrow \mathcal{V}$  gegeben, so werden Vektoren  $\mathbf{v} \in \mathcal{V}$  gesucht, deren Bildvektor zu  $\mathbf{v}$  parallel ist. D.h. es sind Paare aus einem Vektor  $\mathbf{v}$  und einem Skalar  $\lambda$  zu bestimmen mit der Eigenschaft

$$\mathbf{F}(\mathbf{v}) = \lambda \mathbf{v} \quad \text{und} \quad \mathbf{v} \neq \mathbf{0} .$$

Gilt diese Gleichung, so nennt man  $\lambda$  einen **Eigenwert** und  $\mathbf{v}$  einen **Eigenvektor** der linearen Abbildung  $\mathbf{F}$ .

Die Lösung des Eigenwertproblems wird dadurch erschwert, dass die Eigenwerte komplex sein können und  $\mathbf{F}$  deswegen auf einer komplexen Erweiterung von  $\mathcal{V}$  definiert werden muss.

Die praktische Lösung von linearen Gleichungssystemen und Eigenwertproblemen verlangt die komponentenweise Darstellung linearer Abbildungen mittels Matrizen.

## B-6 Orthogonalisierungsverfahren nach GRAM-SCHMIDT

### Ausgangspunkt

Gegeben sei eine Basis  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \{\mathbf{v}_i\}_{i=1\dots n}$  des linearen Vektorraumes  $\mathcal{V}$ .

### Ziel

Mittels des *Gram-Schmidtschen* - Orthogonalisierungsverfahrens soll eine neue **orthonormale Basis**  $\{\mathbf{b}_1, \dots, \mathbf{b}_n\} = \{\mathbf{b}_i\}_{i=1\dots n}$  des Vektorraumes  $\mathcal{V}$  erzeugt werden.

## Verfahren

**Gegeben:**  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \{\mathbf{v}_i\}_{i=1\dots n}$  Basis von  $\mathcal{V}$

**Gesucht:**  $\{\mathbf{b}_1, \dots, \mathbf{b}_n\} = \{\mathbf{b}_i\}_{i=1\dots n}$  **orthonormale Basis** von  $\mathcal{V}$  so dass

$$\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_n) = \text{span}(\mathbf{v}_1, \dots, \mathbf{v}_n) \quad i = 1, \dots, n$$

sowie

$$\|\mathbf{b}_i\| = 1 \wedge \mathbf{b}_i \perp \mathbf{b}_j \quad 1 \leq \{i, j\} \leq n, j \neq i$$

**Ansatz:** Wegen der Forderung

$$\mathbf{b}_i \in \text{span}(\mathbf{v}_1, \dots, \mathbf{v}_i) = \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{v}_i)$$

wählt man den Ansatz

$$\tilde{\mathbf{b}}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j = \|\tilde{\mathbf{b}}_i\| \mathbf{b}_i \quad i = 1, \dots, n.$$

Da  $\mathbf{b}_i$  durch Normalisierung aus  $\tilde{\mathbf{b}}_i$  gebildet wird, ist auch  $\tilde{\mathbf{b}}_i$  orthogonal zu allen Vektoren  $\mathbf{v}_j$  und  $\mathbf{b}_j$ ,  $j = 1 \dots i - 1$ .

Damit gilt (für festes  $i$  und  $j < i$ )

$$0 = \langle \mathbf{v}_i, \mathbf{b}_j \rangle + \alpha_{ij} \quad j = 1 \dots i - 1$$

und somit

$$\alpha_{ij} = -\langle \mathbf{v}_i, \mathbf{b}_j \rangle \quad j = 1 \dots i - 1.$$

Nun wird  $\tilde{\mathbf{b}}_i$  entsprechend dem Ansatz

$$\tilde{\mathbf{b}}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j = \mathbf{v}_i - \sum_{j=1}^{i-1} \langle \mathbf{v}_i, \mathbf{b}_j \rangle \mathbf{b}_j$$

berechnet. Schließlich erhält man den  $i$ -ten neuen Basisvektor aus

$$\mathbf{b}_i = \frac{\tilde{\mathbf{b}}_i}{\|\tilde{\mathbf{b}}_i\|}.$$

Die letzten drei Gleichungen sind für  $i = 1 \dots n$  zu lösen, danach ist die neue Basis berechnet.

## Beispiel

Gegebene Basis ( $n = 3$ ):  $\mathbf{v}_1 = (2, 2, 0)^T$   $\mathbf{v}_2 = (1, 0, 2)^T$   $\mathbf{v}_3 = (0, 2, 1)^T$   
 $\mathbf{i} = 1$ :

$$\tilde{\mathbf{b}}_1 = \mathbf{v}_1 = (2, 2, 0)^T$$

$$\|\tilde{\mathbf{b}}_1\| = \sqrt{2^2 + 2^2 + 0} = \sqrt{8} = 2\sqrt{2}$$

$$\mathbf{b}_1 = \frac{\tilde{\mathbf{b}}_1}{\|\tilde{\mathbf{b}}_1\|} = \frac{1}{2\sqrt{2}}(2, 2, 0)^T = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)^T = \mathbf{b}_1$$

$\mathbf{i} = 2$ :

$$\alpha_{21} = -\langle \mathbf{v}_2, \mathbf{b}_1 \rangle = -(1, 0, 2) \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)^T = -\frac{1}{\sqrt{2}}$$

$$\tilde{\mathbf{b}}_2 = \mathbf{v}_2 + \alpha_{21}\mathbf{b}_1 = (1, 0, 2)^T - \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)^T = \left(\frac{1}{2}, -\frac{1}{2}, 2\right)^T$$

$$\|\tilde{\mathbf{b}}_2\| = \sqrt{\frac{1}{2}^2 + \frac{1}{2}^2 + 2^2} = \sqrt{\frac{9}{2}} = \frac{3}{\sqrt{2}}$$

$$\mathbf{b}_2 = \frac{\tilde{\mathbf{b}}_2}{\|\tilde{\mathbf{b}}_2\|} = \frac{\sqrt{2}}{3} \left(\frac{1}{2}, -\frac{1}{2}, 2\right)^T = \left(\frac{\sqrt{2}}{6}, -\frac{\sqrt{2}}{6}, 2\frac{\sqrt{2}}{3}\right)^T = \mathbf{b}_2$$

**i = 3:**

$$\alpha_{31} = -\langle \mathbf{v}_3, \mathbf{b}_1 \rangle = -(0, 2, 1) \left( \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0 \right)^T = -\sqrt{2}$$

$$\alpha_{32} = -\langle \mathbf{v}_3, \mathbf{b}_2 \rangle = -(0, 2, 1) \left( \frac{\sqrt{2}}{6}, -\frac{\sqrt{2}}{6}, 2\frac{\sqrt{2}}{3} \right)^T = \frac{\sqrt{2}}{3} - \frac{2\sqrt{2}}{3} - \frac{\sqrt{2}}{3}$$

$$\tilde{\mathbf{b}}_3 = \mathbf{v}_3 + \alpha_{31}\mathbf{b}_1 + \alpha_{32}\mathbf{b}_2$$

$$= (0, 2, 1)^T - \sqrt{2} \left( \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0 \right)^T - \frac{\sqrt{2}}{3} \left( \frac{\sqrt{2}}{6}, -\frac{\sqrt{2}}{6}, 2\frac{\sqrt{2}}{3} \right)^T$$

$$= \left( -\frac{10}{9}, \frac{10}{9}, \frac{5}{9} \right)^T$$

$$\|\tilde{\mathbf{b}}_3\| = \sqrt{\left(\frac{10}{9}\right)^2 + \left(\frac{10}{9}\right)^2 + \left(\frac{5}{9}\right)^2} = \sqrt{\frac{225}{81}} = \frac{15}{9} = \frac{5}{3}$$

$$\mathbf{b}_3 = \frac{\tilde{\mathbf{b}}_3}{\|\tilde{\mathbf{b}}_3\|} = \frac{3}{5} \left( -\frac{10}{9}, \frac{10}{9}, \frac{5}{9} \right)^T = \boxed{\left( -\frac{2}{3}, \frac{2}{3}, \frac{1}{3} \right)^T = \mathbf{b}_3}$$

Die somit berechnete neue Basis ist

$$\boxed{\mathbf{b}_1 = \left( \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0 \right)^T \quad \mathbf{b}_2 = \left( \frac{\sqrt{2}}{6}, -\frac{\sqrt{2}}{6}, \frac{2\sqrt{2}}{3} \right)^T \quad \mathbf{b}_3 = \left( -\frac{2}{3}, \frac{2}{3}, \frac{1}{3} \right)^T}$$

Gegebene Basis:

$$\mathbf{v}_1 = (2, 2, 0)^T$$

$$\mathbf{v}_2 = (1, 0, 2)^T$$

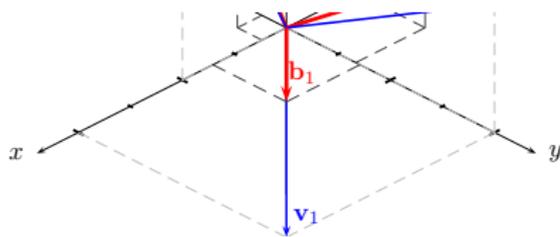
$$\mathbf{v}_3 = (0, 2, 1)^T$$

Orthonormale Basis:

$$\mathbf{b}_1 = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right)^T$$

$$\mathbf{b}_2 = \left(\frac{\sqrt{2}}{6}, -\frac{\sqrt{2}}{6}, \frac{2\sqrt{2}}{3}\right)^T$$

$$\mathbf{b}_3 = \left(-\frac{2}{3}, \frac{2}{3}, \frac{1}{3}\right)^T$$



## Umrechnung eines Vektors auf eine neue Basis

### Ausgangspunkt

Gegeben sei eine Basis  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \{\mathbf{v}_i\}_{i=1\dots n}$  des linearen Vektorraumes  $\mathcal{V}$ . Mittels des *Gram-Schmidtschen* - Orthogonalisierungsverfahrens sei eine neue **orthonormale Basis**

$\{\mathbf{b}_1, \dots, \mathbf{b}_n\} = \{\mathbf{b}_i\}_{i=1\dots n}$  erzeugt worden. Die dabei erzeugten Zwischengrößen  $\mathbf{b}_i$ ,  $i = 1 \dots n$ , und  $\alpha_{ij}$ ,  $i = 1 \dots n$ ,  $j = 1 \dots (i - 1)$ , seien verfügbar.

### Ziel

Es soll eine Formel ermittelt werden, mit deren Hilfe jeder bezüglich der Basis  $\{\mathbf{v}_i\}_{i=1\dots n}$  gegebene Vektor  $u_{[\mathbf{v}]} \in \mathcal{V}$  in eine Darstellung  $u_{[\mathbf{b}]}$  bezüglich der Basis  $\{\mathbf{b}_i\}_{i=1\dots n}$  umgewandelt werden kann.

## Verfahren

Der Ansatz des *Gram-Schmidtschen-Orthogonalisierungsverfahrens*

$$\tilde{\mathbf{b}}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j \quad i = 1, \dots, n$$

kann nach  $\mathbf{v}_i$  umgestellt werden. Mit  $\mathbf{b}_i = \tilde{\mathbf{b}}_i / \|\tilde{\mathbf{b}}_i\|$  erhält man

$$\mathbf{v}_i = \|\tilde{\mathbf{b}}_i\| \mathbf{b}_i - \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j \quad i = 1, \dots, n.$$

Mit dem Übergang von  $\alpha_{ij}$  zu  $\tilde{\alpha}_{ij} = -\alpha_{ij}$ ,  $i = 1 \dots n$ ,  $j = 1 \dots i - 1$ , und durch zusätzliche Einführung von  $\tilde{\alpha}_{ii} = \|\tilde{\mathbf{b}}_i\|$ ,  $i = 1 \dots n$ , folgt

$$\mathbf{v}_i = \tilde{\alpha}_{ii} \mathbf{b}_{ii} + \sum_{j=1}^{i-1} \tilde{\alpha}_{ij} \mathbf{b}_j = \boxed{\sum_{j=1}^i \tilde{\alpha}_{ij} \mathbf{b}_j = \mathbf{v}_i} \quad i = 1, \dots, n.$$

Damit hat man eine Darstellung der Basisvektoren  $\mathbf{v}_i$ ,  $i = 1 \dots n$ , als Linearkombination der neuen Basisvektoren  $\mathbf{b}_i$ .

Ersetzt man nun die Basisvektoren  $\mathbf{v}_i$  in einem gegebenen Vektor

$$\mathbf{u} = \mathbf{u}_{[\mathbf{v}]} = (\mu_1, \dots, \mu_n)_{[\mathbf{v}]}^T = \sum_{i=1}^n \mu_i \mathbf{v}_i$$

durch die neue Basis  $\{\mathbf{b}_i\}_{i=1\dots n}$  erhält man

$$\mathbf{u}_{[\mathbf{v}]} = \sum_{i=1}^n \mu_i \mathbf{v}_i = \sum_{i=1}^n \mu_i \sum_{j=1}^i \tilde{\alpha}_{ij} \mathbf{b}_j = \boxed{\sum_{i=1}^n \mu_i \sum_{j=1}^i \tilde{\alpha}_{ij} \mathbf{b}_j = \mathbf{u}_{[\mathbf{b}]}}$$

also die gesuchte Formel zur Darstellung  $\mathbf{u}_{[\mathbf{b}]}$  des Vektors  $\mathbf{u}$  bezüglich der Basis  $\{\mathbf{b}_i\}_{i=1\dots n}$ .

## Beispiel

Alte Basis ( $n = 3$ ):  $\mathbf{v}_1 = (2, 2, 0)^T$      $\mathbf{v}_2 = (1, 0, 2)^T$      $\mathbf{v}_3 = (0, 2, 1)^T$

Gegebener Vektor bezüglich Basis  $\{\mathbf{v}_i\}_{i=1\dots 3}$ :

$$\mathbf{u}_{[\mathbf{v}]} = (\mu_1, \mu_2, \mu_3)_{[\mathbf{v}]}^T = (1, -2, \frac{1}{2})_{[\mathbf{v}]}^T$$

Neue Basis aus *Gram-Schmidt*:

$$\mathbf{b}_1 = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)^T \quad \mathbf{b}_2 = (\frac{\sqrt{2}}{6}, -\frac{\sqrt{2}}{6}, \frac{2\sqrt{2}}{3})^T \quad \mathbf{b}_3 = (-\frac{2}{3}, \frac{2}{3}, \frac{1}{3})^T$$

Koeffizienten  $\alpha_{ij}$  aus *Gram-Schmidt*:

$$\alpha_{21} = -\frac{1}{\sqrt{2}} \\ \alpha_{31} = -\sqrt{2} \quad \alpha_{32} = -\frac{\sqrt{2}}{3}$$

Neue Koeffizienten

$\tilde{\alpha}_{ij} = -\alpha_{ij}$ ,  $i = 1 \dots n$ ,  $j = 1 \dots i - 1$ , und  $\tilde{\alpha}_{ii} = \|\tilde{\mathbf{b}}_i\|$ ,  $i = 1 \dots n$ :

$$\tilde{\alpha}_{11} = 2\sqrt{2} \\ \tilde{\alpha}_{21} = \frac{1}{\sqrt{2}} \quad \tilde{\alpha}_{22} = \frac{3}{\sqrt{2}} \\ \tilde{\alpha}_{31} = \sqrt{2} \quad \tilde{\alpha}_{32} = \frac{\sqrt{2}}{3} \quad \tilde{\alpha}_{33} = \frac{5}{3}$$

Nun **Umrechnung** auf neue Basis  $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$ :

$$\begin{aligned}
 \mathbf{u}_b &= \sum_{i=1}^3 \mu_i \sum_{j=1}^i \tilde{\alpha}_{ij} \mathbf{b}_j \\
 &= \mu_1 \tilde{\alpha}_{11} \mathbf{b}_1 + \mu_1 (\tilde{\alpha}_{21} \mathbf{b}_1 + \tilde{\alpha}_{22} \mathbf{b}_2) + \mu_3 (\tilde{\alpha}_{31} \mathbf{b}_1 + \tilde{\alpha}_{32} \mathbf{b}_2 + \tilde{\alpha}_{33} \mathbf{b}_3) \\
 &= \underbrace{(\mu_1 \tilde{\alpha}_{11} + \mu_2 \tilde{\alpha}_{21} + \mu_3 \tilde{\alpha}_{31})}_{\beta_1} \mathbf{b}_1 + \underbrace{(\mu_2 \tilde{\alpha}_{22} + \mu_3 \tilde{\alpha}_{32})}_{\beta_2} \mathbf{b}_2 + \underbrace{\mu_3 \tilde{\alpha}_{33}}_{\beta_3} \mathbf{b}_3 \\
 &= 2\sqrt{2} - 2\frac{1}{\sqrt{2}} + \frac{1}{2}\sqrt{2} &= -2\frac{3}{\sqrt{2}} + \frac{1}{2} \cdot \frac{\sqrt{2}}{3} &= \frac{1}{2} \cdot \frac{5}{3} \\
 &= 2\sqrt{2} - \sqrt{2} + \frac{\sqrt{2}}{2} &= -3\sqrt{2} + \frac{1}{6}\sqrt{2} & \\
 &\boxed{\beta_1 = \frac{3\sqrt{2}}{2}} &\boxed{\beta_2 = -\frac{17}{6}\sqrt{2}} &\boxed{\beta_3 = \frac{5}{6}}
 \end{aligned}$$

und damit

$$\mathbf{u}_{[\mathbf{v}]} = (\mu_1, \mu_2, \mu_3)_{[\mathbf{v}]}^T = (1, -2, \frac{1}{2})_{[\mathbf{v}]}^T = \boxed{(\frac{3\sqrt{2}}{2}, -\frac{17}{6}\sqrt{2}, \frac{5}{6})_{[\mathbf{b}]}^T} = \mathbf{u}_{[\mathbf{b}]} = (\beta_1, \beta_2, \beta_3)_{[\mathbf{b}]}^T$$

## Probe: Umrechnung in kartesische Koordinaten

$$\mathbf{u}_{[\mathbf{v}]} = \sum_{i=1}^3 \mu_i \mathbf{v}_i = 1 \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 - 2 + 0 \\ 2 - 0 + 1 \\ 0 - 4 + \frac{1}{2} \end{pmatrix} = \boxed{\begin{pmatrix} 0 \\ 3 \\ -\frac{7}{2} \end{pmatrix}} = \mathbf{u}$$

$$\mathbf{u}_{[\mathbf{b}]} = \sum_{i=1}^3 \beta_i \mathbf{b}_i = \frac{3\sqrt{2}}{2} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} - \frac{17}{6} \sqrt{2} \begin{pmatrix} \frac{\sqrt{2}}{6} \\ -\frac{\sqrt{2}}{6} \\ \frac{2\sqrt{2}}{3} \end{pmatrix} + \frac{5}{6} \begin{pmatrix} -\frac{2}{3} \\ 2 \\ 3 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{3}{2} - \frac{34}{36} - \frac{10}{18} \\ \frac{3}{2} + \frac{34}{36} + \frac{10}{18} \\ 0 - \frac{68}{18} - \frac{5}{18} \end{pmatrix} = \begin{pmatrix} \frac{3}{2} - \frac{27}{18} \\ \frac{3}{2} + \frac{27}{18} \\ 0 - \frac{63}{18} \end{pmatrix} = \begin{pmatrix} \frac{3}{2} - \frac{3}{2} \\ \frac{3}{2} + \frac{3}{2} \\ 0 - \frac{7}{2} \end{pmatrix} = \boxed{\begin{pmatrix} 0 \\ 3 \\ -\frac{7}{2} \end{pmatrix}} = \mathbf{u}$$

und damit

$$\mathbf{u}_{[\mathbf{v}]} = \mathbf{u}_{[\mathbf{b}]} = \mathbf{u}.$$

## B-7 Matrizen und ihre Algebra

### Definition B-7.1 (Matrix)

Ein Zahlenschema

$$A = (\alpha_{ij})_{\substack{j=1\dots n \\ i=1\dots m}} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix}$$

heißt eine **reelle** ( $m \times n$ ) **Matrix**, die aus  $m$  Zeilen und  $n$  Spalten besteht. Man sagt auch  $A$  ist vom Typ oder Format  $(m, n)$  und schreibt  $A \in \mathbb{R}^{m \times n}$  (siehe Definition B-7.8).

Die Elemente in der  $i$ -ten Zeile von  $A$  bilden den sogenannten Zeilenvektor  $(\alpha_{ij})_{j=1\dots n} \in \mathbb{R}^n$  und die Elemente in der  $j$ -ten Spalte den Spaltenvektor  $(\alpha_{ij})_{i=1\dots m} \in \mathbb{R}^m$ .

Der Zusammenhang zwischen Matrizen und linearen Abbildungen ergibt sich nun wie folgt.

Sind  $(\mathbf{v}_j)_{j=1\dots n}$  und  $(\mathbf{w}_i)_{i=1\dots m}$  Basen von  $\mathcal{V}$  und  $\mathcal{W}$ , so gibt es genau eine lineare Abbildung  $F : \mathcal{V} \mapsto \mathcal{W}$  mit der Eigenschaft

$$F(\mathbf{v}_j) = \sum_{i=1}^m \alpha_{ij} \mathbf{w}_i .$$

Dann gilt für beliebige Vektoren  $\mathbf{v} = \sum \nu_j \mathbf{v}_j$

$$\begin{aligned} F(\mathbf{v}) &= \sum_{j=1}^n \nu_j F(\mathbf{v}_j) \\ &= \sum_{j=1}^n \nu_j \left( \sum_{i=1}^m \alpha_{ij} \mathbf{w}_i \right) \\ &= \sum_{i=1}^m \mathbf{w}_i \underbrace{\sum_{j=1}^n \alpha_{ij} \nu_j}_{\omega_i} . \end{aligned}$$

## Definition B - 7.2 (Matrix-Vektor-Produkt)

Die durch die letzte Gleichung implizierte Rechenvorschrift nennt man ein **Matrix-Vektor-Produkt** und schreibt einfach

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_m \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_n \end{pmatrix}$$

oder kurz

$$\mathbf{w} = A\mathbf{v}.$$

Diese Matrix-Vektor-Gleichung ist eine Abkürzung für die komponentenweise Identität

$$\boxed{\omega_i = \sum_{j=1}^n \alpha_{ij} \nu_j \quad \text{für } i = 1, \dots, m} \quad (1)$$

## Beispiel B-7.3

Bezüglich der monomialen Basis hat die schon im Beispiel B-5.4 erwähnte Abbildung durch **Differentiation** in  $\mathcal{P}_n$  für  $n = 5$  die Matrix-Darstellung

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Diese Matrix ergibt sich für  $i = 1, \dots, 5$  aus der Grundbeziehung

$$F(\mathbf{v}_i) = \mathbf{v}'_i = (i-1) \mathbf{v}_{i-1} \quad \text{da} \quad \mathbf{v}_i = x^{i-1},$$

wobei hier  $\mathcal{W} = \mathcal{V}$  und deshalb  $\mathbf{w}_i = \mathbf{v}_i$ .

## Definition B-7.4 (Hintereinanderausführung linearer Abbildungen)

Betrachtet man zwei lineare Abbildungen

$$G : \mathcal{U} \mapsto \mathcal{V} \quad \text{und} \quad F : \mathcal{V} \mapsto \mathcal{W},$$

so ist deren **Komposition** oder **Hintereinanderausführung**

$$F \circ G : \mathcal{U} \mapsto \mathcal{W} \quad \text{mit} \quad (F \circ G)(\mathbf{u}) = F(G(\mathbf{u}))$$

eine lineare Abbildung von  $\mathcal{U}$  nach  $\mathcal{W}$ .

Bezüglich geeigneter Basen  $\{\mathbf{u}_k\}_{k=1\dots p}$  von  $\mathcal{U}$ ,  $\{\mathbf{v}_j\}_{j=1\dots n}$  von  $\mathcal{V}$  und  $\{\mathbf{w}_i\}_{i=1\dots m}$  von  $\mathcal{W}$  entsprechen den Abbildungen  $F$  und  $G$  Matrizen

$$A = (\alpha_{ij})_{i=1\dots m}^{j=1\dots n} \quad \text{und} \quad B = (\beta_{jk})_{j=1\dots n}^{k=1\dots p}.$$

Hierbei entspricht die Spaltenzahl von  $A$  der Zeilenzahl von  $B$ , da diese beide gleich der Dimension  $n$  des Zwischenbereiches  $\mathcal{V}$  sind.

## Definition B-7.5 (Matrixmultiplikation)

Unter diesen Bedingungen kann man nun durch wiederholte Anwendung von (1) die Koeffizienten  $\omega_i$  eines Bildes  $\mathbf{w} = F(G(\mathbf{u}))$  direkt aus den Koeffizienten  $\mu_k$  von  $\mathbf{u}$  berechnen. Und zwar gilt für jedes  $i = 1 \dots m$

$$\omega_i = \sum_{j=1}^n \alpha_{ij} \nu_j = \sum_{j=1}^n \alpha_{ij} \left( \sum_{k=1}^p \beta_{jk} \mu_k \right) = \sum_{k=1}^p \mu_k \underbrace{\sum_{j=1}^n \alpha_{ij} \beta_{jk}}_{\gamma_{ik}} .$$

Mittels der  $(m \times p)$  Matrix  $(\gamma_{ik})_{i=1, \dots, m}^{k=1, \dots, p}$  erhält man also das neue Matrix-Vektor-Produkt

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_m \end{pmatrix} = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1p} \\ \gamma_{21} & \gamma_{22} & \cdots & \gamma_{2p} \\ \dots & \dots & \dots & \dots \\ \gamma_{m1} & \gamma_{m2} & \cdots & \gamma_{mp} \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_p \end{pmatrix} .$$

## Definition B-7.6 (Matrix-Matrix Schreibweise)

Den Zusammenhang zwischen den  $\alpha_{ij}$ ,  $\beta_{jk}$  und den resultierenden  $\gamma_{ik}$  nennt man ein **Matrix-Matrix-Produkt** (kurz **Matrix-Produkt**) und schreibt

$$\begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1p} \\ \cdots & \cdots & \cdots \\ \gamma_{m1} & \cdots & \gamma_{mp} \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \cdots & \cdots & \cdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \beta_{11} & \cdots & \beta_{1p} \\ \cdots & \cdots & \cdots \\ \beta_{n1} & \cdots & \beta_{np} \end{pmatrix}$$

oder ganz kurz

$$C = (\gamma_{ik})_{i=1\dots m}^{k=1\dots p} = AB$$

mit  $A \in \mathbb{R}^{m \times n}$ ,  $B \in \mathbb{R}^{n \times p}$  und deshalb  $C \in \mathbb{R}^{m \times p}$ .

Dabei ist das Element  $\gamma_{ik}$  in der  $i$ -ten Zeile und  $k$ -ten Spalte des Produktes  $C$  gerade das innere Produkt der  $i$ -ten Zeile des linken Faktors  $A$  und der  $k$ -ten Spalte des rechten Faktors  $B$ .

## Faustregel Matrix-Multiplikation

**Zeile · Spalte**

## Beispiel B-7.7

Man betrachte die beiden  $(3 \times 3)$  Matrizen

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \sigma & \sigma & 0 \\ -\sigma & \sigma & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

wobei  $\sigma = 1/\sqrt{2}$  ist.

Bezüglich der kartesischen Basis des dreidimensionalen Anschauungsraumes

beschreibt  $A$  die **Spiegelung** aller Vektoren  $\mathbf{v} = x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3$  an der diagonalen Fläche  $y = z$ .

$B$  beschreibt bezüglich der kartesischen Basis eine **Achtel-Drehung entgegen dem Uhrzeigersinn** um die  $z$ -Achse  $\mathbf{e}_3$  (Achtung: Rechtssystem!!).

## Fortsetzung Beispiel

Wird nun *zuerst rotiert und dann reflektiert*, so ergibt sich die Matrix

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

Hier ergab sich zum Beispiel das Element in der dritten Zeile und zweiten Spalte des Produktes als  $(0, 1, 0) \cdot (\sigma, \sigma, 0)^T = 0 \cdot \sigma + 1 \cdot \sigma + 0 \cdot 0 = \sigma$ .

Tauscht man jedoch die Reihenfolge der Faktoren aus, so erhält man die Matrix

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

Diese Matrix beschreibt die *Hintereinanderausführung der Spiegelung und dann der Drehung*, was zu unterschiedlichen Ergebnissen führt.

## Bemerkung:

Wie das Beispiel zeigt, ist die Matrixmultiplikation **nicht kommutativ**. Sie ist allerdings assoziativ in dem Sinne, daß

$$(AB)C = A(BC)$$

für beliebige Matrizen  $A, B$  und  $C$  ist, vorausgesetzt die Spaltenzahl von  $A$  gleicht der Zeilenzahl von  $B$  und die Spaltenzahl von  $B$  gleicht der Zeilenzahl von  $C$ , da die Produkte sonst gar nicht definiert wären. Diese Identität kann man durch Ausmultiplizieren überprüfen oder aus der Tatsache ableiten, daß die Hintereinander ausführung von Abbildungen auch assoziativ ist, d.h. es gilt  $(F \circ G) \circ H = F \circ (G \circ H)$ , vorausgesetzt der Bildbereich von  $H$  gehört zum Definitionsbereich der Abbildung  $G$  und der Bildbereich von  $G$  gehört zum Definitionsbereich von  $F$ . In jedem Falle wird hier ein gegebenes Element  $\mathbf{u} \in \text{Dom}(H)$  nach  $F(G(H(\mathbf{u})))$  abgebildet.

Diese Eindeutigkeit der Komposition von Abbildungen überträgt sich auch auf die Multiplikation von Matrizen.

## Definition B-7.8 (Vektorraum $\mathbb{R}^{m \times n}$ )

Alle **reellen Matrizen eines gegebenen Typs**  $(m, n)$  bilden eine Menge, die man mit  $\mathbb{R}^{m \times n}$  bezeichnet. Diese Menge ist sogar ein reeller **Vektorraum** bezüglich komponentenweiser Addition und Multiplikation, d.h.

$$A + B = (\alpha_{ij} + \beta_{ij})_{i=1 \dots m}^{j=1 \dots n} \quad \text{und} \quad \lambda A = (\lambda \alpha_{ij})_{i=1 \dots m}^{j=1 \dots n}$$

für beliebige Matrizen

$$A = (\alpha_{ij}) \in \mathbb{R}^{m \times n}, B = (\beta_{ij}) \in \mathbb{R}^{m \times n}$$

und  $\lambda \in \mathbb{R}$ .

Vorausgesetzt die Typen von  $A$ ,  $B$  und  $C$  sind kompatibel, so daß die folgenden Ausdrücke überhaupt definiert sind, gelten die

**Distributivgesetze:**

$$\begin{aligned} A(B + C) &= AB + AC \\ (A + B)C &= AC + BC. \end{aligned}$$

## Definition B-7.9 (Identitätsmatrix)

Bezüglich der Multiplikation von Matrizen gibt es ein neutrales Element, nämlich die **Einheits-** oder **Identitätsmatrix**

$$I = I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Der die Größe der Matrix angegebende Index  $n$  kann wegfallen, wenn er sich aus dem Zusammenhang ergibt. Es gilt nun insbesondere

$$I_m A = A = A I_n \quad \text{für } A \in \mathbb{R}^{m \times n}.$$

## Definition B-7.10 (Transposition)

Eine einfache aber wichtige Operation auf Matrizen ist die **Transposition**, die aus einer  $(m \times n)$  Matrix  $A$  eine  $(n \times m)$  Matrix  $B = A^T$  macht. Hierbei gilt  $\beta_{ij} = \alpha_{ji}$ , so daß in Matrixschreibweise

$$A^T = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{m1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{m2} \\ \dots & \dots & \dots & \dots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{mn} \end{pmatrix} = (\beta_{ij})_{i=1 \dots n}^{j=1 \dots m}.$$

### Bemerkung:

Nur die Diagonalelemente  $(\alpha_{ii})_{i=1 \dots \min(m,n)}$  bleiben bei der Transposition unverändert, die anderen Elemente tauschen den Platz mit ihrem Gegenüber auf der anderen Seite der Diagonalen.

## Lemma B-7.11 (Transpositionsregeln)

*Man kann sich leicht davon überzeugen, daß die folgenden Regeln für das Transponieren gelten:*

$$\begin{aligned}(A^T)^T &= A \\(A + B)^T &= A^T + B^T \\(\lambda A)^T &= \lambda A^T \\(AB)^T &= B^T A^T .\end{aligned}$$

### Bemerkung:

Die Transposition ist also eine lineare Abbildung von  $\mathbb{R}^{m \times n}$  nach  $\mathbb{R}^{n \times m}$  und als solche sogar ihre eigene Inverse. Die letzte Gleichung bedeutet, daß die Transponierte eines Produktes gleich dem Produkt der transponierten Faktoren in umgekehrter Reihenfolge ist. Hierbei müssen wir natürlich wieder davon ausgehen, daß die Formate der Faktoren bezüglich der Produktbildung verträglich sind, was dann entsprechend für die Transponierten folgt.

## Spezielle Matrixformen

Je nach ihrem Format, der Verteilung nicht verschwindender Elemente und gewissen algebraischen Eigenschaften unterscheidet man die folgenden häufig auftretenden Matrix Typen.

### Zeilenvektor

$$A \in \mathbb{R}^{1 \times n} \Rightarrow A = (\alpha_{11}, \alpha_{12}, \dots, \alpha_{1n})$$

In diesem Falle nennt man  $A$  einen **Zeilenvektor**.

### Spaltenvektor

$$A \in \mathbb{R}^{m \times 1} \Rightarrow A = \begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{m1} \end{pmatrix}$$

In diesem Falle nennt man  $A$  einen **Spaltenvektor**. Er kann von links mit einer  $m$ -spaltigen Matrix multipliziert werden, in diesem Fall stimmt das Matrix-Vektor-Produkt und das übliche Matrix-Matrix-Produkt überein.

## Äusseres oder dyadisches Produkt

Das Produkt eines Zeilenvektors  $\mathbf{a}^T = [(\alpha_i)_{i=1\dots n}]^T \in \mathbb{R}^{1 \times n}$  mit einem Spaltenvektor  $\mathbf{b} = (\beta_i)_{i=1\dots m} \in \mathbb{R}^{m \times 1}$  der gleichen Länge  $m = n$  ergibt

$$\mathbf{a}^T \mathbf{b} = (\mathbf{a} * \mathbf{b}) = \mathbf{b}^T \mathbf{a} = \sum_{i=1}^n \alpha_i \beta_i \in \mathbb{R}^{1 \times 1}.$$

Diese  $1 \times 1$  Matrix kann man also als Skalar mit dem inneren Produkt zwischen  $\mathbf{a}$  und  $\mathbf{b}$  identifizieren. Wechselt man jedoch die Reihenfolge der Faktoren, so ergibt sich auch fuer  $n \neq m$  die wohldefinierte Matrix

$$\mathbf{b} \mathbf{a}^T = (b_i a_j)_{i=1\dots m, j=1\dots n} \in \mathbb{R}^{m \times n}$$

Diese nennt man auch das **äussere** oder **dyadische Produkt** von  $\mathbf{a}$  und  $\mathbf{b}$ .

## Verbilligte Produkte

Normalerweise kostet für  $A \in \mathbb{R}^{m \times n}$  die Berechnung des Produktes  $A\mathbf{v}$  mit einem Vektor  $\mathbf{v} \in \mathbb{R}^n$  genau  $m \cdot n$  skalare Multiplikationen. Ist jedoch  $A = \mathbf{b}\mathbf{a}^T$  ein äusseres Produkt so berechnet man viel billiger

$$A\mathbf{v} = (\mathbf{b}\mathbf{a}^T)\mathbf{v} = \mathbf{b}(\mathbf{a}^T\mathbf{v}).$$

Beachte, dass  $\mathbf{b}(\mathbf{a}^T\mathbf{v})$  durch Bildung des Inneren Produktes  $\mathbf{a}^T\mathbf{v} = \mathbf{a} \cdot \mathbf{v}$  und seine anschliessende Multiplikation mit  $\mathbf{b}$  nur  $n + m$  skalare Multiplikationen verlangt. Demgegenüber kostet alleine die explizite Berechnung des äusseren Produktes  $\mathbf{b}\mathbf{a}^T$  genau  $m \cdot n$  Multiplikationen. Entsprechend berechnet man das Produkt mit einer Matrix  $V \in \mathbb{R}^{n \times p}$  als

$$(\mathbf{b}\mathbf{a}^T)V = \mathbf{b}(\mathbf{a}^T V) = \mathbf{b}(V^T \mathbf{a})^T$$

Die Produktbildung  $\mathbf{b}(V^T \mathbf{a})^T$  kostet nur  $(m + n) \cdot p$  skalare Multiplikationen während die Berechnung in der Form  $(\mathbf{b}\mathbf{a}^T)V$  mehr als  $m \cdot n \cdot p$  solche Operationen verlangt. Allgemeiner bezeichnet man die Fragestellung, in welcher Reihenfolge ein Produkt mehrerer Matrizen am billigsten berechnet werden kann, als **Matrixketten-Problem**. Es kann

## Quadratische Matrix

$$A \in \mathbb{R}^{n \times n} \Rightarrow A^T \in \mathbb{R}^{n \times n}$$

Eine Matrix, deren Zeilenzahl gleich ihrer Spaltenzahl ist, heißt **quadratisch**. Alle linearen Abbildungen eines Raumes in sich selbst werden durch quadratische Matrizen beschrieben.

## Symmetrische Matrix

$$A^T = A \in \mathbb{R}^{n \times n}$$

Quadratische Matrizen, die bezüglich der Transposition invariant sind, heißen **symmetrisch**. Diese bilden einen Unterraum von  $\mathbb{R}^{n \times n}$ . Dieser Unterraum hat die Dimension  $n(n+1)/2$ , da man lediglich die  $n$  Elemente in der Diagonale und entweder die  $n(n-1)/2$  Elemente darüber oder die gleiche Zahl darunter frei wählen kann.

## Schief symmetrische Matrix

$$A^T = -A \in \mathbb{R}^{n \times n}$$

Quadratische Matrizen mit dieser Eigenschaft heißen **schief symmetrisch**. Wie wir später sehen werden, sind alle ihre Eigenwerte rein imaginär.

Für jede quadratische Matrix gilt

$$A = \underbrace{\frac{1}{2}(A + A^T)}_{\text{symmetrisch}} + \underbrace{\frac{1}{2}(A - A^T)}_{\text{schiefsymmetrisch}} .$$

Diese additive Zerlegung ist allerdings nicht sehr nützlich in Bezug auf die Eigenwerte, da diese in stark nichtlinearer Weise von der Matrix abhängen.

## Dreiecksmatrix

Falls für  $A = (\alpha_{ij}) \in \mathbb{R}^{n \times n}$

$$i > j \Rightarrow \alpha_{ij} = 0$$

gilt, so daß

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \alpha_{nn} \end{pmatrix},$$

dann nennt man  $A$  eine **obere Dreiecksmatrix**.

Analog definiert man auch die **untere Dreiecksmatrix**, deren oberhalb der Hauptdiagonale stehenden Elemente Null sind.

## Diagonale Matrizen

$A \in \mathbb{R}^{n \times n}$  heißt **diagonal**, wenn  $i \neq j \Rightarrow \alpha_{ij} = 0$  gilt, also

$$A = \begin{pmatrix} \alpha_{11} & 0 & \cdots & 0 \\ 0 & \alpha_{22} & \cdots & 0 \\ & \cdots & \cdots & \\ 0 & 0 & \cdots & \alpha_{nn} \end{pmatrix}.$$

Man schreibt dann kurz  $A = \text{diag}(\alpha_i)_{i=1 \dots n}$ .

Insbesondere gilt

$$I = \text{diag}(1)_{i=1 \dots n}.$$

Summen und Produkte von diagonalen Matrizen sind wiederum diagonal:

$$A = \text{diag}(\alpha_i)_{i=1 \dots n}$$

$$B = \text{diag}(\beta_i)_{i=1 \dots n}$$

$\Rightarrow$

$$A + B = \text{diag}(\alpha_i + \beta_i)_{i=1 \dots n}$$

$$AB = \text{diag}(\alpha_i \beta_i)_{i=1 \dots n}.$$

## Orthogonale Matrizen

$A \in \mathbb{R}^{n \times n}$  heißt **orthogonal**, falls

$$A^T A = I = A A^T$$

wobei sich zeigen läßt, daß die zweite Identität aus der ersten folgt.

Bezeichnet man mit  $\mathbf{a}_j = (\alpha_{ij})_{i=1 \dots n}$  den  $j$ -ten Spaltenvektor von  $A$ , so ist die Bedingung  $A^T A = I$  äquivalent zu

$$\langle \mathbf{a}_i, \mathbf{a}_j \rangle = \begin{cases} 0 & \text{falls } i \neq j \\ 1 & \text{falls } i = j \end{cases}$$

Das heißt: Die Matrix  $A$  ist genau dann orthogonal, wenn ihre Spaltenvektoren eine orthonormale Basis von  $\mathbb{R}^n$  bilden.

Da mit  $A$  auch  $A^T$  orthogonal ist, gilt dasselbe für die Zeilen von  $A$ , die ja die Spalten von  $A^T$  sind.

## Produkt orthogonaler Matrizen

Für zwei orthogonale Matrizen  $A$  und  $B$  ist jeweils auch deren Produkt orthogonal, da

$$(AB)^T(AB) = (B^T A^T)(AB) = B^T(A^T A)B = B^T B = I.$$

Die Summe von orthogonalen Matrizen hat im allgemeinen nicht diese Eigenschaft. So ist zum Beispiel mit  $A$  auch  $-A$  orthogonal, aber deren Summe, die Nullmatrix  $A - A = 0$ , sicherlich nicht.

## Beispiel B - 7.12 (Drehungen in der Ebene)

$$A = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

$$A^T A = \begin{pmatrix} \cos(\varphi)^2 + \sin(\varphi)^2 & \cos(\varphi) \sin(\varphi) \cdot (1 - 1) \\ \sin(\varphi) \cos(\varphi) \cdot (1 - 1) & \cos(\varphi)^2 + \sin(\varphi)^2 \end{pmatrix} = I$$

## B-8 Lösung linearer Gleichungssysteme

### Lineare Systeme

Für eine lineare Abbildung

$$F : \mathcal{V} = \text{Span}\{\mathbf{v}_j\}_{j=1\dots n} \rightarrow \mathcal{W} = \text{Span}\{\mathbf{w}_i\}_{i=1\dots m}$$

und eine vorgegebene "Rechte Seite"  $\mathbf{w} = \sum_{i=1}^m b_i \mathbf{w}_i$  mit  $b_i \in \mathbb{R}$  findet man ein  $\mathbf{v} = \sum_{j=1\dots n} x_j \mathbf{v}_j$  mit  $F(\mathbf{v}) = \mathbf{w}$  durch Lösen des Gleichungssystems

$$\begin{array}{rcccccc} \alpha_{11}x_1 & + & \alpha_{12}x_2 & + & \dots & + & \alpha_{1j}x_j \dots & + & \alpha_{1n}x_n & = & b_1 \\ \alpha_{21}x_1 & + & \alpha_{22}x_2 & + & \dots & + & \alpha_{2j}x_j \dots & + & \alpha_{2n}x_n & = & b_2 \\ & & & & \dots & & & & & & \\ \alpha_{i1}x_1 & + & \alpha_{i2}x_2 & + & \dots & + & \alpha_{ij} \dots & + & \alpha_{in}x_n & = & b_i \\ & & & & \dots & & & & & & \\ \alpha_{m1}x_1 & + & \alpha_{m2}x_2 & + & \dots & + & \alpha_{mj} \dots & + & \alpha_{mn}x_n & = & b_m \end{array}$$

## Matrix–Vektor–Schreibweise

Äquivalenterweise ergibt sich in Matrix–Vektor–Schreibweise

$$A\mathbf{x} = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ \alpha_{21} & \dots & \alpha_{2j} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_{m1} & \dots & \alpha_{mj} & \dots & \alpha_{mn} \end{pmatrix} \mathbf{x} = \mathbf{b}$$

wobei  $\mathbf{x} = (x_1, \dots, x_j, \dots, x_n)^T$  und  $\mathbf{b} = (b_1, \dots, b_j, \dots, b_m)^T$  sind.

Man bezeichnet das lineare System von  $m$  Gleichungen in  $n$  Unbekannten als

<b>unterbestimmt</b>	wenn $m < n$
<b>quadratisch</b>	wenn $m = n$
<b>überbestimmt</b>	wenn $m > n$

Im Allgemeinen haben **unterbestimmte** Gls. unendlich viele und **überbestimmte** Gls. keine Lösung. **Aber:** Für spezielle Gls. wird diese Regel verletzt, es gibt unterbestimmte Gls. ohne und überbestimmte Gls. mit Lösung.

## Definition B- 8.1 (Regularität)

Eine Abbildung  $F : \mathbb{R}^n \rightarrow \mathbb{R}^n$  und entsprechende Matrizen  $A$  heißen regulär, falls

$$Ax = F(x) = 0 \quad \text{g.d.w.} \quad x = 0,$$

andernfalls heißen sie singular.

## Lemma B- 8.2

*Falls  $A$  regulär ist, dann hat  $Ax = \mathbf{b}$  genau eine eindeutige Lösung für jedes  $\mathbf{b}$ .*

Ein Kriterium, ob eine Matrix regulär oder singular ist, liefert die im Abschnitt **B-9** eingeführte **Determinante**  $\det(A)$ .

Wünschenswerte Lösungsalgorithmen prüfen die Regularität und liefern entweder die eindeutige Lösung oder Singularitätsbeschreibungen.

## Lösung Linearer Gleichungssysteme in Spezialfällen

Ist  $A$  eine Orthogonal-, Diagonal- oder Dreiecksmatrix (das sind diejenigen, deren Struktur sich auf das Produkt überträgt), so lassen sich die entsprechenden linearen Systeme  $A\mathbf{x} = \mathbf{b}$  relativ leicht lösen.

### Lemma B-8.3 (Lösung orthogonaler Systeme)

*Falls  $A$  orthogonal ist, gilt:*

$$A\mathbf{x} = \mathbf{b} \Leftrightarrow A^T A\mathbf{x} = \mathbf{x} = A^T \mathbf{b}$$

*In diesem Falle kann das Gleichungssystem also einfach durch die Multiplikation der rechten Seite  $\mathbf{b}$  mit der Transponierten  $A^T$  gelöst werden.*

## Lemma B-8.4 (Lösung diagonalen Systeme)

*Falls  $A = \text{diag}(\alpha_i)_{i=1\dots n}$  eine Diagonalmatrix ist, so reduziert sich das lineare System auf die Gleichungen  $\alpha_i x_i = b_i$ . Diese werden für beliebige  $b_i$  durch  $x_i = b_i / \alpha_i$  genau dann erfüllt, wenn keines der Diagonalelemente  $\alpha_i$  gleich Null ist.*

*Falls diese Regularitätsbedingung verletzt ist, muss  $\mathbf{b}$  die Konsistenzbedingung*

$$\alpha_i = 0 \quad \Rightarrow \quad b_i = 0$$

*erfüllen. Die entsprechenden Lösungskomponenten  $x_i$  sind dann beliebig, so dass das Gleichungssystem  $A\mathbf{x} = \mathbf{b}$  mehrdeutig lösbar ist.*

## Lemma B - 8.5 (Lösung von Dreieckssystemen)

*Ist  $A$  eine untere Dreiecksmatrix, hat das entsprechende Gleichungssystem  $A\mathbf{x} = \mathbf{b}$  die folgende „gestaffelte“ Form:*

$$\begin{array}{rcl} \alpha_{11}x_1 & = & b_1 \\ \alpha_{21}x_1 + \alpha_{22}x_2 & = & b_2 \\ \vdots & & \vdots \\ \alpha_{i1}x_1 + \alpha_{i2}x_2 + \cdots + \alpha_{ij}x_j & = & b_i \\ \vdots & & \vdots \\ \alpha_{n1}x_1 + \alpha_{n2}x_2 + \cdots + \alpha_{n,n-1}x_{n-1} + \alpha_{nn}x_n & = & b_n \end{array}$$

## Vorwärtssubstitution

Nun kann man zunächst aus der ersten Gleichung  $x_1$  bestimmen, dann diesen Wert in die Zweite einsetzen, um  $x_2$  zu erhalten, und so weiter. Unter der Regularitätsbedingung aus Lemma B-8.4, dass wiederum keines der diagonalen Elemente  $\alpha_{ij}$  verschwindet, hat man also

$$\begin{aligned}x_1 &= b_1/\alpha_{11} \\x_2 &= (b_2 - \alpha_{21}x_1)/\alpha_{22} \\x_3 &= (b_3 - \alpha_{31}x_1 - \alpha_{32}x_2)/\alpha_{33} \\&\vdots \\x_i &= (b_i - \alpha_{i1}x_1 - \cdots - \alpha_{ii-1}x_{i-1})/\alpha_{ii} \\&\vdots \\x_n &= (b_n - \alpha_{n1}x_1 - \cdots - \alpha_{nj}x_j - \cdots - \alpha_{nn-1}x_{n-1})/\alpha_{nn}\end{aligned}$$

Man braucht  $n(n-1)/2$  Multiplikationen und Additionen sowie  $n$  Divisionen.

## Rückwärtssubstitution

Bei einer oberen Dreiecksmatrix  $A$  ergibt sich entsprechend das Verfahren der **Rückwärtssubstitution**, wobei jetzt die  $x_i$  für  $i = n, n - 1, \dots, 1$  durch die Formel

$$x_i = \frac{1}{\alpha_{ii}} \left( b_i - \sum_{j=i+1}^n \alpha_{ij} x_j \right) \quad i = n, n - 1, \dots, 1$$

bestimmt sind. Regularitätsbedingung ist wiederum, dass keines der Diagonalelemente verschwindet. Der Rechenaufwand ist auch hier von der Ordnung  $n^2/2$  arithmetischer Operationen.

Zur Lösung allgemeiner linearer Systeme kann man die Matrix  $A$  so modifizieren, daß sie eine der oben genannten speziellen Formen annimmt oder das Produkt solcher spezieller Matrizen wird. Das klassische Verfahren für eine solche Transformation ist die **Elimination nach Carl Friedrich Gauß** (1777 – 1855).

## B-9 Gauß-Elimination (1850)

Die Grundlage dieses Verfahrens ist die Beobachtung, dass für zwei Funktionen  $f(\mathbf{x})$  und  $g(\mathbf{x})$  eines Vektors  $\mathbf{x}$  und jeden beliebigen Skalar  $\lambda$  gilt:

$$\boxed{\begin{array}{l} f(\mathbf{x}) = 0 \\ g(\mathbf{x}) = 0 \end{array}} \iff \boxed{\begin{array}{l} f(\mathbf{x}) = 0 \\ g(\mathbf{x}) - \lambda f(\mathbf{x}) = 0 \end{array}}$$

$\underbrace{\hspace{10em}}_{=: \tilde{g}(\mathbf{x})}$

Mit anderen Worten: Die Menge  $\{\mathbf{x} \mid f(\mathbf{x}) = g(\mathbf{x}) = 0\}$  der Lösungen  $\mathbf{x}$  des Gleichungspaares  $f(\mathbf{x}) = 0$  und  $g(\mathbf{x}) = 0$  ist genau dieselbe wie die Lösungsmenge des Gleichungspaares  $f(\mathbf{x}) = 0$  und  $\tilde{g}(\mathbf{x}) = 0$ . Hierbei wurde die neue zweite Gleichung  $\tilde{g}(\mathbf{x}) = 0$  durch **Subtraktion eines Vielfachen der ersten von der alten zweiten Gleichung** erhalten.

Selbst wenn  $f(\mathbf{x})$  und  $g(\mathbf{x})$  nichtlinear sind, kann man gelegentlich durch solche Umformungen ein System von zwei oder mehreren Gleichungen sukzessive vereinfachen, bis eine explizite Lösung gelingt.

## Lineare Systeme in zwei Variablen

Zunächst betrachten wir hier den Fall von zwei linearen Gleichungen in zwei Unbekannten.

$$\alpha_{11}x_1 + \alpha_{12}x_2 = b_1$$

$$\alpha_{21}x_1 + \alpha_{22}x_2 = b_2$$

**Ausnahmefall:**  $\alpha_{11} = 0$

**Tauscht** man die beiden Gleichungen **aus**, so ergibt sich das gestaffelte Gleichungssystem

$$\begin{array}{l} \alpha_{21}x_1 + \alpha_{22}x_2 = b_2 \\ \alpha_{12}x_2 = b_1 \end{array} \iff \tilde{A}\mathbf{x} = \begin{pmatrix} \tilde{\alpha}_{11} & \tilde{\alpha}_{12} \\ \tilde{\alpha}_{21} & \tilde{\alpha}_{22} \end{pmatrix} \mathbf{x} = \begin{pmatrix} \alpha_{21} & \alpha_{22} \\ 0 & \alpha_{12} \end{pmatrix} \mathbf{x} = \tilde{\mathbf{b}} = \begin{pmatrix} b_2 \\ b_1 \end{pmatrix},$$

wobei die Komponenten der rechten Seite auch vertauscht wurden.

Damit hat die Matrix  $\tilde{A}$  nun Dreiecksform. Vorausgesetzt, die beiden neuen Diagonalelemente  $\tilde{\alpha}_{11}$  und  $\tilde{\alpha}_{22}$  sind beide nicht Null, ergibt sich durch Rückwärtssubstitution

$$x_2 = \tilde{b}_2 / \tilde{\alpha}_{22} \quad \text{und} \quad x_1 = (\tilde{b}_1 - \tilde{\alpha}_{12}x_2) / \tilde{\alpha}_{11}.$$

## Normalfall: $\alpha_{11} \neq 0$

In diesem Fall läßt sich durch **Abziehen** des  $\boxed{\lambda_{21} \equiv \alpha_{21}/\alpha_{11}}$ -fachen **der ersten von der zweiten Gleichung** die Variable  $x_1$  aus Letzterer **eliminieren**.

Man erhält also

$$\underbrace{\alpha_{11}x_1 + (\alpha_{21} - \lambda_{21}\alpha_{11})x_1}_{\tilde{\alpha}_{21} = 0} + \underbrace{\alpha_{12}x_2 + (\alpha_{22} - \lambda_{21}\alpha_{12})x_2}_{\tilde{\alpha}_{22}} = \underbrace{b_1 + (b_2 - \lambda_{21}b_1)}_{\tilde{b}_2}$$

Da  $\lambda_{21}$  gerade so gewählt wurde, dass  $\tilde{\alpha}_{21}$  verschwindet, hat das System nun wieder eine gestaffelte Form und die Lösungskomponenten  $x_2$  und  $x_1$  können durch **Rückwärtssubstitution** berechnet werden.

## Pivotierung

Das im Nenner von  $\lambda_{21}$  auftretende Diagonalelement  $\alpha_{11}$  nennt man auch das **Pivotelement**.

Ist es ursprünglich gleich Null, so versucht man durch **Zeilenaustausch** (d.h. Umordnen der Gleichungen) ein nichtverschwindendes Pivotelement zu erhalten. Ist dies nicht möglich, so ist das Gleichungssystem singulär, d.h. nicht regulär. (Dieser Fall wird später betrachtet.)

Sind alle Diagonalelemente von  $A$  von Null verschieden, dann läßt sich  $A$  direkt durch  $n - 1$  sukzessive Eliminationsschritte **ohne** Zeilenaustausch auf Dreiecksform bringen.

# Lösung von Systemen beliebiger Dimension

Wir betrachten nun ein quadratisches Gleichungssystem von  $n$  Gleichungen mit  $n$  Unbekannten:

$$A\mathbf{x} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2j} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_{i1} & \alpha_{i2} & \dots & \alpha_{ij} & \dots & \alpha_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nj} & \dots & \alpha_{nn} \end{pmatrix} \mathbf{x} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{pmatrix}$$

## Erster Schritt

Eliminiere  $\alpha_{i1}$  mit Hilfe des nichtverschwindenden Diagonalelementes  $\alpha_{11}$ . Zu diesem Zwecke wird das  $\lambda_{i1}$ -fache der ersten Zeile mit

$$\lambda_{i1} = \alpha_{i1}/\alpha_{11} \quad i = 2 \dots n$$

von allen anderen Zeilen abgezogen.

Dadurch erhalten die Elemente  $\alpha_{ij}$  mit  $i > 1$  und  $j > 1$  die neuen Werte

$$\alpha_{ij} \leftarrow \alpha_{ij} - \lambda_{i1}\alpha_{1j} \quad i, j = 2 \dots n$$

Da die alten Werte nicht mehr gebraucht werden, kann man sie unmittelbar mit den Neuen überschreiben. (Deswegen haben wir hier nicht mehr wie im zweidimensionalen Fall die neuen Werte durch eine Tilde  $\sim$  von den Alten unterschieden.)

Entsprechend werden auch die Komponenten der rechten Seite nach der Formel

$$b_i \leftarrow b_i - \lambda_{i1} b_1 \quad i = 2 \dots n$$

"aufdatiert".

Anschließend hat das Gleichungssystem die Form

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2j} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & \alpha_{j2} & \dots & \alpha_{jj} & \dots & \alpha_{jn} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & \alpha_{n2} & \dots & \alpha_{nj} & \dots & \alpha_{nn} \end{pmatrix} \mathbf{x} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{pmatrix}$$

## Zwischenergebnis nach $k-1$ Schritten

$$\mathbf{Ax} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1,k-1} & \alpha_{1k} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2,k-1} & \alpha_{2k} & \dots & \alpha_{2n} \\ 0 & 0 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \alpha_{k-1,k-1} & \alpha_{k-1,k} & \dots & \alpha_{k-1,n} \\ \vdots & \vdots & & 0 & \alpha_{k,k} & \dots & \alpha_{k,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \alpha_{nk} & \dots & \alpha_{nn} \end{pmatrix} \mathbf{x} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \\ \vdots \\ \vdots \\ b_n \end{pmatrix}$$

## k-ter Schritt

Zur Elimination der letzten  $n - k$  Elemente in der  $k$ -ten Spalte subtrahiert man nun für  $i = k + 1, \dots, n$  das  $\lambda_{ik}$ -fache der  $k$ -ten Zeile mit

$$\lambda_{ik} = \alpha_{ik} / \alpha_{kk} \quad i = k + 1 \dots n$$

von der  $i$ -ten Zeile.

Es gilt also für  $j = k + 1, \dots, n$  die Aufdatierungsformel

$$\alpha_{ij} \leftarrow \alpha_{ij} - \lambda_{ik} \alpha_{kj} \quad i, j = k + 1 \dots n$$

und entsprechend für die rechte Seite

$$b_i \leftarrow b_i - \lambda_{ik} b_k \quad i = k + 1 \dots n.$$

## Spaltenpivotierung

Findet sich im  $k$ -ten Schritt in der Diagonale ein Element  $\alpha_{kk}$ , das gleich Null oder auch nur sehr klein ist, so sollte man einen Zeilenaustausch vornehmen.

Wenn die Matrix  $A$  regulär ist, dann muss mindestens eines der Elemente  $\alpha_{ik}$  mit  $i \geq k$  ungleich Null sein und kann dann durch Austausch der  $i$ -ten und  $k$ -ten Zeile in die Diagonale gebracht werden.

In Computerberechnungen wählt man im allgemeinen das  $\alpha_{ik}$  mit dem maximalen Betrag.

Bei Handrechnungen wählt man oft auch „glatte“ Zahlen, die die weitere Rechnung etwas erleichtern, auch wenn das ursprüngliche Diagonalelement nicht gleich Null ist.

## Aufwandsbetrachtung

Bei größeren Gleichungssystemen sind oft viele Elemente der gegebenen Matrix  $A$  gleich Null. Man kann dann bei der Pivotwahl darauf abzielen, möglichst viele von ihnen während der Aufdatierungen zu erhalten. Dadurch lassen sich Rechenaufwand und Speicherbedarf oft dramatisch reduzieren.

Sind alle Elemente von  $A$  ungleich Null, so beträgt der Rechenaufwand für die Gaußsche Elimination in etwa  $n^3/3$  Multiplikationen und Additionen.

Es ist bemerkenswert, dass dieser Aufwand nur einem Drittel des Aufwandes entspricht, der sich für die Multiplikation zweier quadratischer Matrizen im Standardverfahren ergibt.

## Zeilenoperationen mittels Elementarmatrizen

Wir betrachten das Gleichungssystem  $Ax = b$  bzw.  $[A, b]$ .

Die wichtigste Operation des Gaußschen Algorithmus ist es, das  $\lambda$ -fache der Zeile  $j$  von der Zeile  $k$  ( $\neq j$ ) abzuziehen. Das veränderte System in Matrixform ergibt sich durch Multiplikation beider Seiten von links mit der elementaren  $(m \times m)$ -Matrix

$$E_{kj}(\lambda) = I_m - \lambda e_k e_j^T, \quad \text{z.B.} \quad I_4 - 3 e_4 e_2^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -3 & 0 & 1 \end{pmatrix}.$$

Hat  $A$  in der ersten Spalte die Einträge  $(2, 1, 4, 3)^T$ , so wird durch Multiplikation mit der Beispielmatrix an der letzten Stelle eine Null erzeugt.

Diese Elementarmatrizen lassen sich leicht invertieren, es ist

$$(I_m + \lambda e_k e_j^T) \cdot (I_m - \lambda e_k e_j^T) = I_m + \lambda e_k e_j^T - \lambda e_k e_j^T - \lambda^2 e_k (e_j^T e_k) e_j^T = I_m.$$

Die Vertauschung zweier Zeilen  $j$  und  $k \neq j$  erfolgt mittels der Matrix

$$T_{j,k} = \sum_{i \neq j,k} e_i e_i^T + (e_j e_k^T + e_k e_j^T) = (I_m - e_j e_j^T - e_k e_k^T) + (e_j e_k^T + e_k e_j^T) .$$

$T_{j,k}$  ist zu sich selbst invers,  $T_{j,k}^2 = I_m$ .

Die Multiplikation der Zeile  $j$  mit einem Faktor  $\lambda \neq 0$  erfolgt mittels einer Diagonalmatrix

$$S_j(\lambda) = I_m + (\lambda - 1) e_j e_j^T = \text{Diag}(1, \dots, 1, \overbrace{\lambda}^j, 1, \dots, 1)$$

Es gilt  $S_j(\lambda) \cdot S_j(\lambda^{-1}) = I_m$ .

## Interpretation als LU-Faktorisierung

Angenommen, man hat den Gaußschen Algorithmus auf ein System  $[A, \mathbf{b}]$  angewandt und will nun ein System  $[A, \mathbf{c}]$  mit einer neuen rechten Seite lösen. Weiter sei angenommen, dass der Gaußsche Algorithmus ohne Zeilenvertauschungen und Skalierungen auskam, d.h. nur Vielfache oberer Zeilen zu unteren Zeilen hinzuaddiert wurden.

Dann kann man die erneute Reduktion von  $A$  auf Dreiecksform vermeiden, indem man sich die Elementaroperationen merkt und diese nur auf die neue rechte Seite  $\mathbf{c}$  wirken lässt.

Die Operation  $E_{j,k}(\lambda_{j,k})$  erzeugt eine Null an der Stelle  $(j, k)$  unterhalb der Diagonalen, d.h.  $j < k$ . An dieser nun freien Stelle kann der Multiplikator  $\lambda_{j,k}$  nun statt des ursprünglichen  $\alpha_{j,k}$  abgespeichert werden. Auf und oberhalb der Diagonalen verbleiben die Koeffizienten der vom Gauß-Algorithmus erzeugten oberen Dreiecksmatrix.

Vorausgesetzt, kein Zeilenaustausch war nötig, gilt für das ursprüngliche  $A$  und die aus der Gauß-Elimination resultierende obere (engl. **U**pper) Dreiecksmatrix  $U$

$$A = L U$$

wobei der linke Faktor  $L$  die folgende untere (engl. **L**ower) Dreiecksmatrix ist:

$$L = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ \lambda_{21} & 1 & 0 & \dots & 0 \\ \lambda_{31} & \lambda_{32} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{n1} & \lambda_{n2} & \lambda_{n3} & \dots & 1 \end{pmatrix}$$

Zu lösen bleibt

$$L(U\mathbf{x}) = L\mathbf{y} = \mathbf{c} \quad \text{mit} \quad U\mathbf{x} = \mathbf{y}.$$

Man löst also zunächst  $L\mathbf{y} = \mathbf{c}$  mittels Vorwärtssubstitution und dann  $U\mathbf{x} = \mathbf{y}$  mittels Rückwärtssubstitution. Der Gesamtaufwand entspricht recht genau  $n^2$  Operationen und damit einer Matrix-Vektor-Multiplikation.

## B - 10 Determinante und Inverse

Für jede quadratische Matrix  $A \in \mathbb{R}^{n \times n}$  läßt sich ein Skalarwert  $\det(A) \in \mathbb{R}$  berechnen, für den gilt:

$$\det(A) \neq 0 \iff A \text{ regulär}$$

Eine Dreiecksmatrix ist regulär, wenn alle ihre Diagonalelemente nicht Null sind. Man definiert also

$$\det(A) = \prod_{i=1}^n \alpha_{ii} \quad \text{für } A = \begin{array}{c} \triangle \\ \square \end{array} \quad \text{oder} \quad \begin{array}{c} \square \\ \triangle \end{array} .$$

Verlangt man nun noch

- (i) dass die Determinante konstant bleibt, wenn ein Vielfaches einer Zeile (Spalte) zu einer anderen Zeile (Spalte) addiert wird
- (ii) und daß sie lediglich das Vorzeichen wechselt, wenn zwei Zeilen (Spalten) ausgetauscht werden,

dann ist die Determinante schon eindeutig festgelegt.

## Berechnung durch Reduktion

Wie wir im Abschnitt **B-8 Gauss-Elimination** gesehen haben, läßt sich jede quadratische Matrix mittels elementarer Zeilen (Spalten)-Operationen und Zeilen (Spalten)-Vertauschungen in Dreiecksform überführen.

Dieses Vorgehen ist im allgemeinen auch der effizienteste Weg, eine Determinante zu berechnen.

### Beispiel B - 10.1

$$\begin{aligned} \det \begin{pmatrix} -1 & 1 & 1 \\ 3 & -1 & 1 \\ -1 & 3 & 4 \end{pmatrix} &= \det \begin{pmatrix} -1 & 1 & 1 \\ 0 & 2 & 4 \\ 0 & 0 & -1 \end{pmatrix} \\ &= -1 \cdot 2 \cdot (-1) = 2 \end{aligned}$$

## Beispiel B - 10.2

$$\det \begin{pmatrix} 1 & 3 & 2 & 4 \\ 2 & 6 & 4 & 12 \\ 4 & 15 & 7 & 11 \\ -2 & 3 & -6 & 1 \end{pmatrix} = -\det \begin{pmatrix} 1 & 3 & 2 & 4 \\ 0 & 3 & -1 & -5 \\ 0 & 0 & 0 & 4 \\ 0 & 9 & -2 & 9 \end{pmatrix}$$
$$\det \begin{pmatrix} 1 & 3 & 2 & 4 \\ 0 & 3 & -1 & -5 \\ 0 & 0 & 1 & 24 \\ 0 & 0 & 0 & 4 \end{pmatrix} = \begin{vmatrix} 1 & 3 & 2 & 4 \\ 0 & 3 & -1 & -5 \\ 0 & 0 & 1 & 24 \\ 0 & 0 & 0 & 4 \end{vmatrix} = 12$$

Der doppelte Vorzeichenwechsel resultiert aus den beiden Zeilenvertauschungen.

### Bemerkung

Die Betragstriche  $|A|$  stellen eine alternative Bezeichnung für  $\det(A)$  dar.

## Entwicklungssatz

Bei kleineren Matrizen läßt sich die Determinante auch rekursiv nach dem folgenden Entwicklungssatz berechnen.

### Satz B-10.3

*Bezeichnet man mit  $A_{ij}$  die  $(n-1) \times (n-1)$  Matrizen, die durch Weglassen der  $i$ -ten Zeile und  $j$ -ten Spalte aus  $A \in \mathbb{R}^{n \times n}$  hervorgegangen sind, so gilt für beliebiges (aber festes)  $i$  bzw.  $j$*

$$\begin{aligned}\det(A) &= \sum_{k=1}^n \alpha_{ik} \det(A_{ik}) (-1)^{i+k} \\ &= \sum_{k=1}^n \alpha_{kj} \det(A_{kj}) (-1)^{j+k} = \det(A^T)\end{aligned}$$

*Man sagt auch, die Determinante  $\det(A)$  wird **nach der  $i$ -ten Zeile** bzw.  **$j$ -ten Spalte entwickelt**.*

## HINWEISE

Der Satz ergibt sich ziemlich direkt aus einer auf Leibniz (Gottfried Wilhelm L., 1646 – 1716) zurückgehenden expliziten Formel für die Determinante. Es gilt nämlich

$$\det(A) = \sum \alpha_{1j_1} \alpha_{2j_2} \dots \alpha_{nj_n} \operatorname{sgn}(j_1, j_2, \dots, j_n)$$

wobei die Spaltenindizes  $(j_1, j_2, \dots, j_n)$  alle möglichen Permutationen der Zahlen  $(1, 2, \dots, n)$  durchlaufen. Das jeweilige  $\operatorname{sgn}(j_1, j_2, \dots, j_n)$  ist entweder  $+1$  oder  $-1$ , je nachdem, ob die Permutation durch eine gerade oder ungerade Zahl von Zweier-Vertauschungen aus der Grundpermutation  $(1, 2, \dots, n)$  gebildet werden kann.

Da die Gesamtzahl der Permutationen und damit der Summanden in der Leibnizschen Formel  $n!$  ist, wird diese in der Praxis selten angewandt.

## Beispiel B-10.4

Im folgenden wird der Entwicklungssatz zunächst auf die dritte Spalte, die zwei Nullen enthält (damit bleiben nur 2 Summanden übrig), angewendet.

$$\begin{aligned} \begin{vmatrix} 1 & 2 & 0 & 2 \\ 2 & 1 & 4 & 3 \\ 3 & 6 & 0 & 4 \\ 0 & 1 & 2 & 1 \end{vmatrix} &= -4 \begin{vmatrix} 1 & 2 & 2 \\ 3 & 6 & 4 \\ 0 & 1 & 1 \end{vmatrix} - 2 \begin{vmatrix} 1 & 2 & 2 \\ 2 & 1 & 3 \\ 3 & 6 & 4 \end{vmatrix} \\ &= -4 \begin{vmatrix} 6 & 4 \\ 1 & 1 \end{vmatrix} + 4 \cdot 3 \begin{vmatrix} 2 & 2 \\ 1 & 1 \end{vmatrix} - 2 \begin{vmatrix} 1 & 3 \\ 6 & 4 \end{vmatrix} \\ &\quad + 4 \begin{vmatrix} 2 & 2 \\ 6 & 4 \end{vmatrix} - 6 \begin{vmatrix} 2 & 2 \\ 1 & 3 \end{vmatrix} \\ &= -4 \cdot 2 + 12 \cdot 0 - 2(-14) + 4(-4) - 6 \cdot 4 \\ &= -8 + 28 - 16 - 24 = -20 \end{aligned}$$

## Fundamentale Eigenschaften der Determinante

- (i) Die Determinante ist *multilinear*. Sind  $\mathbf{a}_j, \tilde{\mathbf{a}}_j \in \mathbb{R}^n$ ,  $j = 1, \dots, n$  und ist  $\alpha \in \mathbb{R}$ , so gilt

$$\begin{aligned} \det(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}, \mathbf{a}_j + \alpha \tilde{\mathbf{a}}_j, \mathbf{a}_{j+1}, \dots, \mathbf{a}_n) \\ = \det(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}, \mathbf{a}_j, \mathbf{a}_{j+1}, \dots, \mathbf{a}_n) \\ + \alpha \det(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}, \tilde{\mathbf{a}}_j, \mathbf{a}_{j+1}, \dots, \mathbf{a}_n). \end{aligned}$$

- (ii) Die Determinante ist invariant unter Spalten-(Zeilen-)Operationen, ist  $\tilde{\mathbf{a}}_j = \mathbf{a}_k$  für ein  $k \neq j$ , so gilt

$$\det(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}, \mathbf{a}_j + \alpha \mathbf{a}_k, \mathbf{a}_{j+1}, \dots, \mathbf{a}_n) = \det(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}, \mathbf{a}_j, \mathbf{a}_{j+1}, \dots, \mathbf{a}_n)$$

- (iii) Die Determinante ist invariant unter Transposition,  $\det(A) = \det(A^T)$ .
- (iv) Die Determinante ist multiplikativ,  $\det(AB) = \det(A) \det(B)$ .

## Determinantenprodukt

Während sich die Determinante der Summe zweier Matrizen nicht leicht berechnen läßt, ergibt sich für Matrixprodukte die folgende multiplikative Regel:

### Satz B-10.5

Sind  $A, B$  Matrizen vom Typ  $(n, n)$ , so gilt:

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

### Beweis

$$A = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n) \quad B = \begin{bmatrix} \beta_{11} & \beta_{12} & \dots & \beta_{1n} \\ \vdots & \vdots & & \vdots \\ \beta_{n1} & \beta_{n2} & \dots & \beta_{nn} \end{bmatrix}$$

$$C = AB = \left( \underbrace{\sum_{i=1}^n \beta_{i1} \mathbf{a}_i}_{\mathbf{c}_1}, \underbrace{\sum_{i=1}^n \beta_{i2} \mathbf{a}_i}_{\mathbf{c}_2}, \dots, \underbrace{\sum_{i=1}^n \beta_{in} \mathbf{a}_i}_{\mathbf{c}_n} \right)$$

## Fortsetzung: Beweis

Wir betrachten z.B.  $\tilde{B} = (\mathbf{b}_1 + \lambda \mathbf{b}_2, \mathbf{b}_2, \dots, \mathbf{b}_n) \implies \det(\tilde{B}) = \det(B)$

$$\tilde{C} = A\tilde{B} = (\mathbf{c}_1 + \lambda \mathbf{c}_2, \mathbf{c}_2, \dots, \mathbf{c}_n) \implies \det(A\tilde{B}) = \det(AB)$$

D.h. werden an  $B$  Spaltenoperationen  $B \longrightarrow \tilde{B}$  durchgeführt, die  $\det(\tilde{B})$  nicht ändern, dann bleibt auch  $\det(A\tilde{B}) = \det(AB)$  unverändert.

Man kann also  $B$  schrittweise in eine Dreiecks- bzw. sogar Diagonalmatrix

$$D = \text{diag}(\delta_1, \dots, \delta_n)$$

umformen, wobei

$$\det(AB) = \det(AD), \quad \det(D) = \det(B)$$

$$AD = (\delta_1 \mathbf{a}_1, \delta_2 \mathbf{a}_2, \dots, \delta_n \mathbf{a}_n)$$

$$\det(AD) = \det(A) \cdot \prod_{i=1}^n \delta_i = \det(A) \det(D) = \det(A) \det(B)$$



## Cramersche Regel

Gabriel Cramer (1704 – 1752)

Vorbetrachtung:

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

Entwicklung nach der  $j$ -ten Spalte

$$\sum_{i=1}^n (-1)^{i+j} \alpha_{ik} \det(A_{ij}) = 0$$

für  $k \neq j$

An die Stelle des Spaltenvektors  $\mathbf{a}_j$  wird  $\mathbf{a}_k$  gesetzt,  
 $\tilde{A}$  enthält zwei gleiche Spalten!!

## Lineares Gleichungssystem: $A\mathbf{x} = \mathbf{b}$

$$\left. \begin{array}{l} \alpha_{11}x_1 + \alpha_{12}x_2 + \dots + \alpha_{1n}x_n = b_1 \\ \vdots \\ \alpha_{i1}x_1 + \alpha_{i2}x_2 + \dots + \alpha_{in}x_n = b_i \\ \vdots \\ \alpha_{n1}x_1 + \alpha_{n2}x_2 + \dots + \alpha_{nn}x_n = b_n \end{array} \right\} \begin{array}{l} | (-1)^{1+j} \det(A_{1j}) \\ | (-1)^{i+j} \det(A_{ij}) \\ | (-1)^{n+j} \det(A_{nj}) \end{array} \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \begin{array}{l} \text{geeignete} \\ \text{Multiplikationen,} \\ \text{anschließend} \\ \text{Summation} \end{array}$$

$$\begin{aligned} & x_1 \underbrace{\sum_{i=1}^n (-1)^{i+j} \alpha_{i1} \det(A_{ij})}_0 + \dots + x_j \underbrace{\sum_{i=1}^n (-1)^{i+j} \alpha_{ij} \det(A_{ij})}_{\det(A)} + \dots \\ & = \sum_{i=1}^n (-1)^{i+j} b_i \det(A_{ij}) = \det(A_j | \mathbf{b}) \end{aligned}$$

$A_j | \mathbf{b}$  bedeutet Ersetzung des Spaltenvektors  $\mathbf{a}_j$  durch Vektor  $\mathbf{b}$

## Satz B - 10.6 (Cramersche Regel, 1850)

Falls  $\det(A) \neq 0$ , dann kann die eindeutige Lösung des Gleichungssystems  $Ax = b$  nach der **Cramerschen Regel** bestimmt werden:

$$x_j = \frac{1}{\det(A)} \det(A_j|\mathbf{b})$$

Dabei bedeutet  $A_j|\mathbf{b}$ , daß in  $A$  die  $j$ -te Spalte durch  $\mathbf{b}$  ersetzt wird.

### Bemerkung

Die Cramersche Regel ist rechnerisch sehr aufwendig und deshalb vorrangig von theoretischem Interesse. Sie wird angewandt in Fällen, wo die Koeffizienten  $\alpha_{ij}$  z. B. funktionelle Ausdrücke sind oder wenn eventuell nur eine der Unbekannten  $x_j$  benötigt wird.

## Beispiel B - 10.7

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \implies \det(A) = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$$

$$\left. \begin{aligned} x_1 &= \frac{1}{2} \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix} = \frac{1}{2} \\ x_2 &= \frac{1}{2} \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix} = \frac{1}{2} \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = -\frac{1}{2} \\ x_3 &= \frac{1}{2} \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{vmatrix} = \frac{1}{2} \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = \frac{1}{2} \end{aligned} \right\} \boxed{x = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}}$$

## Anwendung der Cramerschen Regel auf die Bestimmung der inversen Matrix $A^{-1}$

**Bezeichnung**  $A^{-1} = B = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$ ,  $AB = I$

Die gesuchte Matrix  $B = A^{-1}$  läßt sich schrittweise aus den Gleichungssystemen

$$A\mathbf{b}_k = \mathbf{e}_k = (0, \dots, 0, 1, 0, \dots, 0)^T \quad k = 1, \dots, n$$

↑  $k$ -te Position

berechnen:

$$\boxed{b_{jk} = \frac{1}{\det(A)} \det(A_j | \mathbf{e}_k) = \frac{(-1)^{j+k}}{\det(A)} \det(A_{kj})}$$

mit  $A_j | \mathbf{e}_k =$

$$\begin{bmatrix} \alpha_{11} & \dots & 0 & \dots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \vdots & & \textcircled{1} & & \vdots \\ \alpha_{n1} & \dots & 0 & \dots & \alpha_{nn} \end{bmatrix} \leftarrow k$$

$\mathbf{a}_1$                        $\mathbf{a}_j$

                                  ↑  
                                   $\mathbf{e}_k$

## Man beachte:

Vertauschung von Zeilen- bzw. Spaltenindex in  $b_{jk} = \frac{(-1)^{j+k}}{\det(A)} \det(A_{kj})$

Zweckmäßigerweise ergibt sich Darstellung:

$$\begin{aligned} A^{-1} &= \frac{1}{\det(A)} \left( \left( (-1)^{i+j} \det(A_{ij}) \right)_{i=1 \dots n}^{j=1 \dots n} \right)^T \\ &= \frac{1}{\det(A)} \begin{pmatrix} + \det(A_{11}) & - \det(A_{21}) & + \det(A_{31}) & \dots \\ - \det(A_{12}) & + \det(A_{22}) & - \det(A_{32}) & \dots \\ + \det(A_{13}) & - \det(A_{23}) & + \det(A_{33}) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \end{aligned}$$

## Warnung:

Für rechteckige Matrizen läßt sich die Determinante nicht definieren.

## Beispiel B-10.8

$$A = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 2 & 0 \\ 3 & 1 & 4 \end{bmatrix} \implies \det(A) = \begin{vmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 1 & -2 \end{vmatrix} = \begin{vmatrix} 2 & 2 \\ 1 & -2 \end{vmatrix} = -6$$

$$A_{11} = \begin{vmatrix} 2 & 0 \\ 1 & 4 \end{vmatrix} = 8, \quad A_{12} = \begin{vmatrix} -1 & 0 \\ 3 & 4 \end{vmatrix} = -4, \quad A_{13} = \begin{vmatrix} -1 & 2 \\ 3 & 1 \end{vmatrix} = -7$$

$$A_{21} = \begin{vmatrix} 0 & 2 \\ 1 & 4 \end{vmatrix} = -2, \quad A_{22} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = -2, \quad A_{23} = \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 1$$

$$A_{31} = \begin{vmatrix} 0 & 2 \\ 2 & 0 \end{vmatrix} = -4, \quad A_{32} = \begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} = 2, \quad A_{33} = \begin{vmatrix} 1 & 0 \\ -1 & 2 \end{vmatrix} = 2$$

$$A^{-1} = \frac{-1}{6} \begin{bmatrix} 8 & 4 & -7 \\ 2 & -2 & -1 \\ -4 & -2 & 2 \end{bmatrix}^T = \frac{-1}{6} \begin{bmatrix} 8 & 2 & -4 \\ 4 & -2 & -2 \\ -7 & -1 & 2 \end{bmatrix} = \frac{1}{6} \begin{bmatrix} -8 & -2 & 4 \\ -4 & 2 & 2 \\ 7 & 1 & -2 \end{bmatrix}$$

**Probe:**  $A \cdot A^{-1} = I$

## Lösung allgemeiner linearer Systeme ( $m \neq n$ möglich)

Die Lösbarkeit eines linearen Systems

$$A\mathbf{x} = \mathbf{b} \in \mathbb{R}^m, \quad \mathbf{x} \in \mathbb{R}^n, \quad A \in \mathbb{R}^{m \times n}$$

hängt sehr stark vom **Rang** der  $m \times n$  Matrix  $A$  ab. Die natürliche Zahl  $\text{Rang}(A)$  ist gleichzeitig

- ▶ die maximale Zahl linear unabhängiger Spalten
- ▶ die maximale Zahl linear unabhängiger Zeilen
- ▶ die Dimension des Bildraumes  $\text{Bild}(A) = \{A\mathbf{x} : \mathbf{x} \in \mathbb{R}^n\}$
- ▶  $n - \dim(\text{kern}(A))$  mit  $\text{kern}(A) = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{0}\}$
- ▶ die maximale Größe einer quadratischen Untermatrix  $\tilde{A}$  (entsteht durch Streichen von geeigneten Zeilen und Spalten aus  $A$ ) mit nichtverschwindender Determinante  $\det(\tilde{A}) \neq 0$ .

Mittels der **Gauß-Elimination** läßt sich ein beliebiges, d.h. nicht notwendigerweise quadratisches, lineares System  $A\mathbf{x} = \mathbf{b}$  immer zu einem äquivalenten System  $\tilde{A}\tilde{\mathbf{x}} = \tilde{\mathbf{b}}$  umformen. Hierbei unterscheiden sich die Lösungsvektoren  $\tilde{\mathbf{x}}$  und  $\mathbf{x}$  nur in der Reihenfolge ihrer Elemente,  $\mathbf{x}$  kann also als Permutation von  $\tilde{\mathbf{x}}$  erhalten werden, wenn überhaupt Spaltenvertauschungen durchgeführt wurden. Die Matrix  $\tilde{A}$  hat Trapezform, so daß

$$\begin{array}{c}
 \left. \begin{array}{c} \times \quad \times \quad \dots \quad \times \quad \times \quad \times \quad \dots \quad \times \\
 0 \quad \times \quad \dots \quad \times \quad \times \quad \times \quad \dots \quad \times \\
 \vdots \quad \vdots \quad \ddots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
 0 \quad 0 \quad \dots \quad \times \quad \times \quad \times \quad \dots \quad \times \\
 0 \quad 0 \quad \dots \quad 0 \quad \times \quad \times \quad \dots \quad \times \\
 0 \quad 0 \quad \dots \quad 0 \quad 0 \quad 0 \quad \dots \quad 0 \\
 \vdots \quad \vdots \\
 0 \quad 0 \quad \dots \quad 0 \quad 0 \quad 0 \quad \dots \quad 0 \end{array} \right\} m \\
 \left. \begin{array}{c} \times \quad \times \quad \dots \quad \times \quad \times \quad \times \quad \dots \quad \times \\
 0 \quad \times \quad \dots \quad \times \quad \times \quad \times \quad \dots \quad \times \\
 \vdots \quad \vdots \quad \ddots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
 0 \quad 0 \quad \dots \quad \times \quad \times \quad \times \quad \dots \quad \times \\
 0 \quad 0 \quad \dots \quad 0 \quad \times \quad \times \quad \dots \quad \times \\
 0 \quad 0 \quad \dots \quad 0 \quad 0 \quad 0 \quad \dots \quad 0 \\
 \vdots \quad \vdots \\
 0 \quad 0 \quad \dots \quad 0 \quad 0 \quad 0 \quad \dots \quad 0 \end{array} \right\} n \\
 \underbrace{\hspace{10em}}_r \quad \underbrace{\hspace{10em}}_{n-r}
 \end{array}
 \quad \parallel \quad
 \begin{array}{c}
 \left. \begin{array}{c} \times \\
 \times \\
 \vdots \\
 \times \\
 \times \\
 \times \\
 \times \\
 \vdots \\
 \times \end{array} \right\} r \\
 \underbrace{\hspace{1em}}_{n-r}
 \end{array}
 \quad \parallel \quad
 \begin{array}{c}
 \left. \begin{array}{c} \times \\
 \times \\
 \vdots \\
 \times \\
 \times \\
 0 \\
 \vdots \\
 0 \end{array} \right\} r \\
 \underbrace{\hspace{1em}}_{m-r}
 \end{array}$$

wobei die ersten  $r = \text{rang}(A)$  Elemente der Diagonale nicht Null sind.

## Eigenschaften der Lösung $\mathbf{x}$

Aus der Trapezform des linearen Systems lässt sich unmittelbar ablesen:

- ▶ die letzten  $m - r$  Komponenten von  $\tilde{\mathbf{b}}$  müssen verschwinden, sonst gibt es keine Lösungen,
- ▶ gibt es überhaupt Lösungen, so sind die letzten  $n - r$  Komponenten von  $\tilde{\mathbf{x}}$  beliebig.

Aus diesen beiden Beobachtungen ergeben sich für die entsprechenden Größen  $\mathbf{b}$  und  $\mathbf{x}$  die folgenden möglichen Situationen ( $r \leq \min(m, n)$  gilt immer):

**$n = r$ :** Es gilt  $\dim \text{Kern } A = n - r = 0$ . Wenn es eine Lösung gibt, so ist sie eindeutig.

**$n = r = m$ :**  $A$  ist invertierbar, es gibt immer eine Lösung.

**$n = r < m$ :** Es gibt  $\mathbf{b}$ , für welche das System unlösbar ist.

**$r < n$ :** Es gilt  $\dim \text{Kern } A = n - r > 0$ . Wenn es eine Lösung  $\mathbf{x}$  gibt, so unendlich viele, die einen affinen Unterraum (Gerade, Ebene, ...) bilden.

**$m, n < r$ :** Es gibt  $\mathbf{b}$ , für welche das System unlösbar ist.

**$n < m = r$ :** Es gibt immer mindestens eine Lösung  $\mathbf{x}$ .

## B-11 Eigenwerte und Eigenvektoren

### Komplexe Lineare Algebra

Das charakteristische Polynom  $\det(A - \lambda I_n)$  einer reellen  $(n \times n)$ -Matrix wird im allgemeinen Fall komplexe Nullstellen besitzen. Um die zugehörige Eigenvektorgleichung  $A\mathbf{v} = \lambda\mathbf{v}$  zu lösen, müssen die Komponenten von  $\mathbf{v}$  auch in den komplexen Zahlen gesucht werden. Es entsteht die Notwendigkeit, die bisher im Reellen betrachtete lineare Algebra auf die Räume  $\mathbb{C}^n$  der  $n$ -elementigen komplexen Vektoren  $\mathbf{a} \in \mathbb{C}^n$  mit

$$\mathbf{a} = (\alpha_j)_{j=1\dots n}, \quad \alpha_j = \operatorname{Re}(\alpha_j) + \mathbf{i}\operatorname{Im}(\alpha_j) \in \mathbb{C}$$

zu erweitern. Zu jedem solchen Vektor  $\mathbf{a}$  existiert der konjugiert-komplexe Vektor

$$\bar{\mathbf{a}} = (\bar{\alpha}_j)_{j=1\dots n}, \quad \bar{\alpha}_j = \operatorname{Re}(\alpha_j) - \mathbf{i}\operatorname{Im}(\alpha_j) \in \mathbb{C}.$$

Offensichtlich gilt, wie schon im skalaren Falle, für jeden **reellen Vektor**  $\mathbf{a} \in \mathbb{R}^n$ :  $\bar{\mathbf{a}} = \mathbf{a}$ .

## Sesquilinearform und Norm

Durch

$$\langle \mathbf{a}, \mathbf{b} \rangle = \mathbf{a}^T \bar{\mathbf{b}} = \bar{\mathbf{b}}^T \mathbf{a} = \sum_{i=1}^n \alpha_i \bar{\beta}_i \in \mathbb{C}$$

wird nun ein inneres Produkt (oder Skalarprodukt) definiert, welches im Gegensatz zum reellen Falle nicht symmetrisch ist, d.h. es ist von der Reihenfolge der Faktoren abhängig:

$$\langle \mathbf{b}, \mathbf{a} \rangle = \mathbf{b}^T \bar{\mathbf{a}} = \overline{\bar{\mathbf{a}}^T \mathbf{b}} = \overline{\langle \mathbf{a}, \mathbf{b} \rangle}$$

Da nun  $\langle \mathbf{a}, \mathbf{a} \rangle$  immer reell und nichtnegativ ist, läßt sich damit eine Norm

$$\|\mathbf{a}\| = \sqrt{\langle \mathbf{a}, \mathbf{a} \rangle} = \left[ \sum_{i=1}^n |\alpha_i|^2 \right]^{\frac{1}{2}}$$

definieren. Unter der Isomorphie  $\mathbb{C}^n \simeq \mathbb{R}^{2n}$  (als reelle VR) ist dies die euklidische Norm.

Es gelten die üblichen Normeigenschaften

$$\|\mathbf{a}\| \geq 0, \quad \|\mathbf{a}\| = 0 \iff \mathbf{a} = \mathbf{0}, \quad \|\gamma\mathbf{a}\| = |\gamma|\|\mathbf{a}\|$$

für beliebiges  $\gamma \in \mathbb{C}$ , sowie die Dreiecksungleichungen

$$\|\mathbf{a} + \mathbf{b}\| \leq \|\mathbf{a}\| + \|\mathbf{b}\|, \quad \|\mathbf{a} - \mathbf{b}\| \geq \left| \|\mathbf{a}\| - \|\mathbf{b}\| \right|.$$

Erweitert man den Körper der Skalare von  $\mathbb{R}$  auf  $\mathbb{C}$ , so bleiben fast alle Definitionen und Sätze gültig. Das gilt insbesondere für die Begriffe

- Linearkombination
- Linearer Unterraum
- Dimension
- Lineare Unabhängigkeit
- Basis
- Lineare Abbildung

sowie Matrizen und ihre speziellen Formen.

Unterschiede ergeben sich lediglich dort, wo das innere Produkt eine wesentliche Rolle spielt:

Eine **Familie von Vektoren**  $\mathbf{v}_i \in \mathbb{C}^n$ ,  $i = 1 \dots r$ , heißt **orthogonal**, wenn

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \bar{\mathbf{v}}_i^T \mathbf{v}_j = 0 \quad \text{für } i \neq j,$$

was weiterhin lineare Unabhängigkeit impliziert. Eine quadratische **Matrix**

$$A = (\alpha_{ij})_{i=1 \dots n}^{j=1 \dots n} \in \mathbb{C}^{n \times n}$$

heißt **unitär**, wenn ihre Spalten paarweise orthogonal sind und ihre Norm jeweils gleich 1 ist. Mittels der **konjugiert transponierten Matrix**

$$A^H = \bar{A}^T = \begin{pmatrix} \bar{\alpha}_{11} & \dots & \bar{\alpha}_{n1} \\ \vdots & & \vdots \\ \bar{\alpha}_{1n} & \dots & \bar{\alpha}_{nn} \end{pmatrix}$$

läßt sich die Unitarität von  $A$  durch die Beziehungen

$$A^H A = \bar{A}^T A = I = A \bar{A}^T = A A^H$$

beschreiben, wobei  $I$  weiterhin die Einheitsmatrix bezeichnet:

$$I = \text{diag}(1, 1, \dots, 1) \in \mathbb{R}^{n \times n} \subset \mathbb{C}^{n \times n}.$$

Abgesehen von der Orthogonalität erfährt auch der Begriff der **Symmetrie** bei der Erweiterung auf komplexe Matrizen eine Veränderung. Man kann zwar eine Matrix  $A = (\alpha_{ij}) \in \mathbb{C}^{n \times n}$  immer noch symmetrisch nennen, wenn  $\alpha_{ji} = \alpha_{ij}$  gilt, diese Eigenschaft ist aber wesentlich weniger interessant als die Erfüllung der Bedingung

$$\bar{\alpha}_{ji} = \alpha_{ij} \quad \Rightarrow \quad A^H = \bar{A}^T = A.$$

Solche Matrizen nennt man **hermitesch** und die entsprechenden linearen Abbildungen auch **selbstadjungiert**, da für beliebige Vektoren  $\mathbf{a}, \mathbf{b} \in \mathbb{C}^n$

$$\langle \mathbf{a}, A\mathbf{b} \rangle = \mathbf{a}^T \overline{A\mathbf{b}} = (\bar{A}^T \mathbf{a})^T \bar{\mathbf{b}} = \langle A^H \mathbf{a}, \mathbf{b} \rangle = \langle A\mathbf{a}, \mathbf{b} \rangle$$

gilt. Für uns wird nur von Bedeutung sein, dass hermitesche Matrizen (wie ihre Untermenge der reell symmetrischen Matrizen) nur reelle Eigenwerte haben.

## Definition B-11.1 (Eigenwerte und Eigenvektoren)

Eine komplexe Zahl  $\lambda \in \mathbb{C}$  heißt **Eigenwert** einer quadratischen Matrix  $A \in \mathbb{C}^{n \times n}$ , wenn es einen entsprechenden **Eigenvektor**  $\mathbf{v} \in \mathbb{C}^n$  gibt, so dass gilt:

$$A\mathbf{v} = \lambda\mathbf{v} \quad \text{mit} \quad \mathbf{v} \neq 0.$$

## Folgerung B-11.2

*Daraus folgt unmittelbar, dass  $\mathbf{v}$  eine nichttriviale Lösung des homogenen Systems*

$$(A - \lambda I_n)\mathbf{v} = 0$$

*ist. Eine solche existiert genau dann, wenn der Rang von  $(A - \lambda I_n)$  kleiner als  $n$  ist, und damit äquivalenterweise gilt*

$$P(\lambda) \equiv \det(A - \lambda I_n) = 0.$$

$P(\lambda)$  wird das **charakteristische Polynom von  $A$**  genannt.

## Satz B-11.3 (Polynomeigenschaft von $P(\lambda)$ )

$P(\lambda)$  ist ein Polynom  $n$ -ten Grades und hat die spezielle Form

$$P(\lambda) = (-\lambda)^n + \text{Tr}(A)(-\lambda)^{n-1} + \dots + \det(A),$$

wobei

$$\text{Tr}(A) = \sum_{i=1}^n \alpha_{ii}$$

die Spur (engl. trace) der Matrix  $A$  bezeichnet. Falls alle Elemente von  $A$  reell sind, so gilt dies auch für die Koeffizienten des charakteristischen Polynoms (allerdings nicht für die Wurzeln).

### Bemerkung:

Die spezielle Form des  $n$ -ten,  $(n-1)$ -ten und konstanten Koeffizienten wird hier nicht bewiesen.

## Beweis:

Durch Induktion nach  $n$  beweisen wir die etwas allgemeinere Behauptung:

$P(\lambda) \equiv \det(A - \lambda B)$  ist für jedes Paar von Matrizen  $A, B \in \mathbb{C}^{n \times n}$  mit  $B = (\beta_{ij})$  ein Polynom vom Grade kleiner oder gleich  $n$ .

**Induktionsanfang,  $n = 1$ :**  $\det(A - \lambda B) = \alpha_{11} - \lambda\beta_{11}$  ist offensichtlich ein Polynom vom Grade gleich 1.

**Induktionsvoraussetzung:**  $\deg(\det(A - \lambda B)) \leq n$  sei erfüllt für  $n$ .

**Induktionsschritt,  $n \rightarrow n + 1$ :**

Nach dem Entwicklungssatz gilt für zwei Matrizen  $A, B \in \mathbb{R}^{(n+1) \times (n+1)}$

$$\det(A - \lambda B) = \sum_{j=1}^{n+1} (-1)^{(j+1)} (\alpha_{1j} - \lambda\beta_{1j}) \det(A_{1j} - \lambda B_{1j})$$

wobei  $A_{1j}$  und  $B_{1j}$  die durch Weglassen der ersten Zeile und  $j$ -ten Spalte aus  $A$  bzw.  $B$  gebildeten  $n \times n$  Matrizen darstellen. Nach Induktionsvoraussetzung sind die Determinanten  $\det(A_{1j} - \lambda B_{1j})$  Polynome vom Grade höchstens  $n$ , so dass die Multiplikation mit den linearen Faktoren  $(\alpha_{1j} - \lambda\beta_{1j})$  den Grad höchstens auf  $n + 1$  erhöhen kann. □

## Algebraische Vielfachheit

Nach dem Fundamentalsatz der Algebra gibt es  $k \leq n$  verschiedene Nullstellen  $\lambda_j$  der Vielfachheit  $p_j$ , so dass das charakteristische Polynom als

$$P(\lambda) = (\lambda_1 - \lambda)^{p_1} (\lambda_2 - \lambda)^{p_2} \dots (\lambda_k - \lambda)^{p_k}$$

geschrieben werden kann, es gilt  $\sum_{j=1}^k p_j = n$ . Daraus folgt

$$\sum_{j=1}^k p_j \lambda_j = \text{Tr}(A), \quad \prod_{j=1}^k \lambda_j^{p_j} = \det(A).$$

Die Zahl  $p_j > 0$  heißt die **algebraische Vielfachheit** des Eigenwertes  $\lambda_j$ .

## Beispiel B - 11.4

Die Matrix

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

hat das charakteristische Polynom

$$\begin{aligned} P(\lambda) &= \det \begin{pmatrix} -\lambda & 1 \\ -1 & -\lambda \end{pmatrix} \\ &= \lambda^2 + 1 = (\mathbf{i} - \lambda)(-\mathbf{i} - \lambda) \end{aligned}$$

Die Eigenwerte sind also  $\lambda_1 = \mathbf{i}$  und  $\lambda_2 = -\mathbf{i}$ , beide mit der algebraischen Vielfachheit  $p_1 = p_2 = 1$ . Man prüft leicht die Identitäten

$$\text{Tr}(A) = 0+0 = 0 = \mathbf{i}-\mathbf{i} \quad \text{und} \quad \det(A) = 1 = \mathbf{i}(-\mathbf{i}) = -\mathbf{i}^2 = -(-1)$$

Dabei ist  $\mathbf{i}$  die *imaginäre Einheit* der komplexen Zahlen.

## Berechnung der Eigenvektoren

Die zu einem Eigenwert  $\lambda_j$  gehörenden Eigenvektoren  $\mathbf{v}_j$  lassen sich als Lösungen des homogenen Gleichungssystems

$$(A - \lambda_j I)\mathbf{v} = 0$$

bestimmen. Sie bilden einen linearen Unterraum der Dimension

$$q_j \equiv \dim(\text{kern}(A - \lambda_j I_n)) = n - \text{rang}(A - \lambda_j I_n)$$

Die Zahl  $q_j > 0$  heißt die **geometrische Vielfachheit** des Eigenwertes  $\lambda_j$  und ist immer kleiner oder gleich der algebraischen Vielfachheit  $p_j$  von  $\lambda_j$ :

$$q_j \leq p_j \quad \text{für } j = 1 \dots k.$$

Eigenwerte  $\lambda_j$  mit  $q_j < p_j$  heißen **defekt**.

Zum Eigenwert  $\lambda_j$  kann man immer  $q_j$  linear unabhängige Vektoren finden, die den **Eigenunterraum**  $\text{kern}(A - I\lambda_j)$  aufspannen. Weiterhin gilt die folgende Aussage bezüglich verschiedener Eigenwerte.

## Lemma B-11.5

Die zu  $r$  verschiedenen Eigenwerten  $\lambda_j$ ,  $j = 1 \dots r$ , gehörenden Eigenvektoren  $(\mathbf{v}_j)_{j=1 \dots r}$  sind linear unabhängig.

### Beweis:

**Induktionsanfang,  $r=1$ :**  $\mathbf{v}_1$  ist wie jeder Eigenvektor definitionsgemäß ungleich Null und deshalb linear unabhängig, d.h.  $\gamma_1 \mathbf{v}_1 = 0$  kann nur mit  $\gamma_1 = 0$  erfüllt werden.

**Induktionsvoraussetzung,  $r$ :** Die Menge der Eigenvektoren  $(\mathbf{v}_j)_{j=1 \dots r}$  sei linear unabhängig, d.h.

$$\sum_{j=1}^r \gamma_j \mathbf{v}_j = 0 \quad \implies \quad \gamma_1 = \dots = \gamma_r = 0.$$

**Induktionsschritt,  $r \rightarrow r+1$ :** Es gelte für geeignete Koeffizienten  $\gamma_i$

$$\sum_{j=1}^{r+1} \gamma_j \mathbf{v}_j = 0.$$

## Fortsetzung: Beweis

Multiplikation mit der Matrix  $A$  bzw. dem Skalar  $\lambda_{r+1}$  liefert

$$0 = A \cdot 0 = A \cdot \sum_{j=1}^{r+1} \gamma_j \mathbf{v}_j = \sum_{j=1}^{r+1} \gamma_j A \mathbf{v}_j = \boxed{\sum_{j=1}^r \gamma_j \lambda_j \mathbf{v}_j} + \boxed{\gamma_{r+1} \lambda_{r+1} \mathbf{v}_{r+1}}$$

und

$$0 = \lambda_{r+1} \cdot 0 = \lambda_{r+1} \cdot \sum_{j=1}^{r+1} \gamma_j \mathbf{v}_j = \boxed{\sum_{j=1}^r \gamma_j \lambda_{r+1} \mathbf{v}_j} + \boxed{\gamma_{r+1} \lambda_{r+1} \mathbf{v}_{r+1}}$$

Aus der Differenz dieser beiden Gleichungen fällt der letzte Term mit  $\mathbf{v}_{r+1}$  ganz heraus:

$$0 = \sum_{j=1}^r \gamma_j (\lambda_j - \lambda_{r+1}) \mathbf{v}_j.$$

Laut Induktionsannahme sind die  $\mathbf{v}_i$ ,  $i = 1 \dots r$ , linear unabhängig, also müssen die zusammengesetzten Koeffizienten  $\gamma_j (\lambda_j - \lambda_{r+1})$  alle gleich Null sein. Da die  $\lambda_j$  verschieden sind, gilt  $\lambda_{r+1} - \lambda_j \neq 0$ ,  $i = 1 \dots r$ . Dies kann aber nur bedeuten, dass die Koeffizienten  $\gamma_j$  für  $j = 1 \dots r$  und damit auch  $\gamma_{r+1}$  gleich Null sind. Also ist auch die um einen Eigenvektor erweiterte Familie  $(\mathbf{v}_j)_{j=1 \dots r+1}$ , linear unabhängig.  $\square$

## Eigenwertzerlegung von Matrizen

Sind nun alle Eigenwerte einfach oder zumindest nicht defekt, so kann man einen vollen Satz von  $n$  linear unabhängigen Eigenvektoren  $\mathbf{v}_i$  finden. Diese faßt man als Spalten zu einer quadratischen Matrix

$$V = [\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n] \in \mathbb{C}^{n \times n}$$

zusammen, welche auf Grund der linearen Unabhängigkeit ihrer Spaltenvektoren eine Inverse  $V^{-1}$  besitzt. Nun kann man die  $n$  Vektorgleichungen  $A\mathbf{v}_j = \lambda_j\mathbf{v}_j$  mit Hilfe der Diagonalmatrix  $\Lambda = \text{diag}(\lambda_i)_{i=1\dots n}$  zur Matrixgleichung

$$AV = V\Lambda$$

kombinieren. Multipliziert man von links bzw. von rechts mit  $V^{-1}$  so erhält man die Darstellung

$$\Lambda = V^{-1}AV \quad \text{bzw.} \quad A = V\Lambda V^{-1}.$$

## Eigenwerte: Operationen und spezielle Matrizen

### Definition B-11.6 (Ähnlichkeitstransformation)

Gibt es für zwei Matrizen  $A, B \in \mathbb{C}^{n \times n}$  eine reguläre Matrix  $T$ , so dass

$$TA = TB \quad \text{und damit auch} \quad A = TBT^{-1} \quad \text{bzw.} \quad B = T^{-1}AT$$

gilt, so sagt man, die Matrizen  $A$  und  $B$  sind **ähnlich**. Die Überführung der Matrix  $B$  in  $A$  durch  $TBT^{-1}$  heisst **Ähnlichkeitstransformation**.

Daraus folgt mit  $\det(T) \det(T^{-1}) = 1$  unmittelbar:

### Folgerung B-11.7 (Eigenwerte ähnlicher Matrizen)

$$\begin{aligned} \det(A - \lambda I) &= \det(TBT^{-1} - \lambda TT^{-1}) \\ &= \det(T(B - \lambda I)T^{-1}) \\ &= \det(T) \det(B - \lambda I) \det(T^{-1}) \\ &= \det(B - \lambda I) \end{aligned}$$

*Also haben zueinander ähnliche Matrizen genau dasselbe charakteristische Polynom und damit auch dieselben Eigenwerte.*

## Verschiebung (Shift)

Addiert man zu einer Matrix  $A$  ein Vielfaches der Einheitsmatrix, so verschieben sich die Eigenwerte entsprechend, da

$$\det((A + \mu I) - \lambda I) = \det(A - (\lambda - \mu)I),$$

so dass  $\lambda$  genau dann ein Eigenwert von  $(A + \mu I)$  ist, wenn  $\lambda - \mu$  ein Eigenwert von  $A$  ist.

## Transponierung

Selbst bei komplexen Matrizen läßt die Transponierung den Determinantenwert unverändert, so daß

$$\det(A^T - \lambda I) = \det((A - \lambda I)^T) = \det(A - \lambda I).$$

Also haben  $A$  und  $A^T$  genau dieselben Eigenwerte, wobei die dazugehörigen Eigenvektoren im allgemeinen allerdings verschieden sind.

## Konjugierte und symmetrische Matrizen

Da die Konjugierung von komplexen Zahlen sich auf Faktoren und Summanden überträgt, gilt

$$\overline{\det(A - \lambda I)} = \det(\overline{A - \lambda I}) = \det(\overline{A} - \overline{\lambda I}) = \det(\overline{A} - \overline{\lambda} I),$$

so dass  $\overline{\lambda}$  genau dann ein Eigenwert von  $\overline{A}$  und damit auch  $\overline{A}^T$  ist, wenn  $\lambda$  ein Eigenwert von  $A$  ist.

Da für reelle Matrizen  $A = \overline{A}$  gilt, ist für diese mit jedem  $\lambda$  auch  $\overline{\lambda}$  ein Eigenwert. Das heißt:

### Folgerung B-11.8 (Eigenwerte reeller Matrizen)

**Alle Eigenwerte reeller Matrizen sind entweder reell oder treten als konjugiert-komplexe Paare  $(\lambda, \overline{\lambda})$  auf.**

## Hermiteische Matrizen

Für diese Klasse von Matrizen sind alle Eigenwerte **reell** und die Eigenvektoren können sogar **orthogonal** zueinander gewählt werden. Es gilt nämlich

$$\lambda \langle \mathbf{v}, \mathbf{v} \rangle = \mathbf{v}^H(\lambda \mathbf{v}) = \mathbf{v}^H(A\mathbf{v}) = \mathbf{v}^H A^H \mathbf{v} = (A\mathbf{v})^H \mathbf{v} = \bar{\lambda} \mathbf{v}^H \mathbf{v} = \bar{\lambda} \langle \mathbf{v}, \mathbf{v} \rangle,$$

wobei wir die Voraussetzung  $A^H = A$  benutzt haben. Da nun  $\mathbf{v}^H \mathbf{v} = |\mathbf{v}|^2$  nicht Null ist, gilt  $\lambda = \bar{\lambda}$ , und der Eigenwert  $\lambda$  muss deshalb **reell** sein.

Sind  $\lambda_1, \lambda_2 \in \mathbb{R}$  zwei verschiedene Eigenwerte,  $\lambda_1 \neq \lambda_2$  mit Eigenvektoren  $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{C}^n$ , so gilt analog

$$\lambda_1 \mathbf{v}_2^H \mathbf{v}_1 = \mathbf{v}_2^H A \mathbf{v}_1 = \mathbf{v}_2^H A^H \mathbf{v}_1 = \lambda_2 \mathbf{v}_1^H \mathbf{v}_2.$$

Also muss  $0 = (\lambda_2 - \lambda_1) \mathbf{v}_2^H \mathbf{v}_1 = (\lambda_2 - \lambda_1) \langle \mathbf{v}_1, \mathbf{v}_2 \rangle$  gelten, wegen  $\lambda_1 \neq \lambda_2$  muss  $\mathbf{v}_1$  **orthogonal** zu  $\mathbf{v}_2$  sein.

## Diagonalisierung hermitescher Matrizen

Sei  $A = A^H \in \mathbb{C}^{n \times n}$  eine hermitesche Matrix mit Eigenwerten  $\lambda_1, \dots, \lambda_m$ .

Definiere die **Eigenunterräume**

$$\mathcal{V}_k := \text{Kern}(A - \lambda_k I_n) \subset \mathbb{C}^n, \quad k = 1..m .$$

Nach der vorhergehenden Aussage gilt  $\mathcal{V}_j \perp \mathcal{V}_m$  für  $j \neq m$ .

Man kann zeigen, dass kein Eigenwert defekt ist. Daher spannen diese Unterräume schon den gesamten Raum vollständig auf,

$$\mathbb{C}^n = \mathcal{V}_1 + \mathcal{V}_2 + \dots + \mathcal{V}_m .$$

Sei  $(\mathbf{v}_{k,1}, \dots, \mathbf{v}_{k,n_k})$  eine orthonormale Basis von  $\mathcal{V}_k$ ,  $k = 1..m$ . Diese kann z.B. mit dem **Gram-Schmidt-Verfahren** (s. nächster Abschnitt) aus einer beliebigen Basis von  $\mathcal{V}_k$  bestimmt werden. Dann ist die aus diesen Spaltenvektoren gebildete Matrix

$$Q = (\mathbf{v}_{1,1}, \dots, \mathbf{v}_{1,n_1}, \mathbf{v}_{2,1}, \dots, \mathbf{v}_{m,n_m}) \in \mathbb{C}^{n \times n}$$

eine unitäre Matrix.



## Praktische Berechnung der Eigenwerte

Der offensichtliche Weg, Eigenwerte und die entsprechende Eigenvektoren zu berechnen, führt über das charakteristische Polynom  $P(\lambda) = \det(A - \lambda I)$ . Bei größeren Dimensionen ist jedoch schon die Berechnung der Koeffizienten von  $P(\lambda)$  sehr aufwendig. Rechnet man mit Standard-Datentypen, so erhält man außerdem die Eigenwerte als Nullstellen von  $P(\lambda)$  mit nur geringer Genauigkeit, da sie stark durch numerische Rundungsfehler beeinträchtigt werden.

Stattdessen führt man beim sogenannten **QR-Algorithmus** eine Folge von orthogonalen Ähnlichkeitstransformationen durch, die  $A$  sukzessive auf diagonale Form reduzieren (falls  $A$  wirklich diagonalisierbar ist). Der Gesamtaufwand dafür ist normalerweise mindestens  $5n^3$  skalare Multiplikationen und damit ein Vielfaches der Kosten für eine **LU-Faktorisierung**. Deswegen wird die Eigenwertzerlegung nur in ganz speziellen Fällen zur Lösung linearer Systeme  $Ax = b$  herangezogen.

## Nutzung der Diagonalisierung

Eigenwertzerlegungen spielen besonders bei der Analyse sogenannter dynamischer Systeme eine zentrale Rolle.

Betrachtet man zum Beispiel eine lineare Evolutionsgleichung

$$x_{neu} = Ax_{alt} + b ,$$

so ergibt deren wiederholte Anwendung den  $k$ -ten Zustand von  $x$  beginnend mit  $x = 0$  als einen Ausdruck der Form  $Q_k(A)b$  mit

$$Q_k(A) = \sum_{j=0}^{k-1} q_j A^j = V \sum_{j=0}^{k-1} q_j \Lambda^j V^{-1} = V Q_k(\Lambda) V^{-1} .$$

Hierbei gilt das Gleichheitszeichen unter der Voraussetzung, dass  $A = V \Lambda V^{-1}$  mit einer Diagonalmatrix  $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_n)$ .

Insbesondere gilt dann  $A^j = V \Lambda^j V^{-1}$ .

Mit anderen Worten: Man kann  $V$  aus dem Matrixpolynom  $Q_k(A)$  herausziehen, so dass dessen Verhalten gerade für große  $k$  durch  $Q_k(\Lambda) = \text{diag}(Q_k(\lambda_j))_{j=1 \dots n}$  beschrieben ist.

## Kanonische Jordanform

Einige Matrizen (wie zum Beispiel  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ ) lassen sich nicht in die Form  $A = V\Lambda V^{-1}$  mit Diagonalmatrix  $\Lambda$  bringen. Vielmehr bleiben in  $\Lambda$  noch einige Elemente in der Superdiagonalen zurück, die einen sogenannten **Jordanblock** bilden. Die vollständige Diagonalisierung gelingt hier nicht, weil der Eigenwert ( $\lambda_1 = 1$ ) eine höhere algebraische ( $p_1 = 2$ ) als geometrische Vielfachheit ( $q_1 = 1$ ) besitzt, dh. defekt ist.

Dieser Effekt ist sehr speziell, da für ein beliebig kleines  $\varepsilon \neq 0$  die gestörte Matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1+\varepsilon \end{bmatrix}$$

zwei unterschiedlichen Eigenwerte ( $1$  und  $1 + \varepsilon$ ) hat und deshalb diagonalisierbar ist mit  $V = \begin{bmatrix} 1 & 1 \\ 0 & \varepsilon \end{bmatrix}$ . Allerdings ist die entsprechende Matrix  $V^{-1} = \begin{bmatrix} 1 & -1/\varepsilon \\ 0 & 1/\varepsilon \end{bmatrix}$  dann sehr groß und explodiert, wenn man  $\varepsilon$  immer kleiner macht.

Zusammenfassend bleibt festzustellen, dass die Eigenwertzerlegung  $A = V\Lambda V^{-1}$  ein wesentlich kniffligeres Problem darstellt, als die Lösung linearer Gleichungssysteme  $Ax = b$ .