Mathematik für Informatiker I

Andreas Griewank

16. Februar 2005

Inhaltsverzeichnis

A Algebraische Grundstrukturen **4**

1 Algebraische Grundlagen **4**

2 Algebraische Teilstrukturen **6**

3 Algebraische Erweiterungen **8**
3.1 Hierarchie algebraischer Grundstrukturen 9

4 Äquivalenzrelationen und Quotientenstrukturen **10**

5 Modulare Arithmetik **12**
5.1 Zahlengerade 12
5.2 Multiplikation in $\mathbb{Z}_5$ 13
5.3 Addition und Subtraktion in $\mathbb{Z}_5$ 13
5.4 Division in $\mathbb{Z}_5$ 13
5.5 Anwendung: Hashing 13

6 Strukturerhaltende Abbildungen **15**

7 Teilbarkeit und partielle Ordnungen **18**

8 Verbandstruktur und größter gemeinsamer Teiler **20**

9 Euklidescher Algorithmus und Anwendungen **22**

10 Darstellungen ganzer Zahlen **26**

11 Polynome als Funktionen **29**
11.1 Beispiel – Lagrangepolynom 31

12 Der Ring der Polynome **33**

13 Faktorisierung und Nullstellen **35**

14 Die komplexen Zahlen **37**

B Lineare Algebra **40**

1 Einführung **40**

2 Vektoren im Anschauungsraum **42**
2.1 Länge und Richtungskosinus 43
2.2 Skalar- oder inneres Produkt 43
2.3 Vektor- oder Kreuzprodukt 44
2.4 Spatprodukt 46

3 Abstandsnormen **48**

4 Basen und Unterräume **50**
4.1 Unterräume und Linearkombinationen 51

5 Lineare Abbildungen **55**

6 Basistransformation **57**
6.1 Ausgangspunkt 57
6.2 Ziel 57
6.3 Verfahren 57
6.4 Beispiel 57
6.5 Probe: Umrechnung in kartesische Koordinaten 58

7 Orthogonalisierungsverfahren nach Gram-Schmidt **59**
7.1 Ausgangspunkt 59
7.2 Ziel 59
7.3 Verfahren 59
7.4 Beispiel 60

8 Matrizen und ihre Algebra **61**
8.1 Spezielle Matrixformen 64

9 Lösung linearer Gleichungssysteme **68**
9.1 Lösung Linearer Gleichungssysteme in Spezialfällen 68

10 Gauß - Elimination (1850) **70**
10.1 Lineare Systeme in zwei Variablen 70
10.2 Lösung von Systemen beliebiger Dimension 71
10.3 Interpretation als LU – Faktorisierung 72

11 Determinante und Inverse **74**
11.1 Entwicklungsatz 74
11.2 Determinantenprodukt 75
11.3 Cramersche Regel 76
11.4 Anwendung der Cramerschen Regel auf die Bestimmung der inversen Matrix A^{-1} 77

12 Eigenwerte und Eigenvektoren **80**
12.1 Komplexe Lineare Algebra 80
12.2 Eigenwerte bei speziellen Matrizen 83
12.3 Praktische Berechnung der Eigenwerte 85
12.4 Nutzung der Diagonalisierung 85
12.5 Kanonische Jordanform 85

Literatur

[Knuth] 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.

[Hartmann] 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] Vélu Jacques, 1er CYCLE. Méthodes mathématiques pour l´informatique. Cours et exercices corrigés. 3er edition. Dunod, Paris, 1999.

[Mazzola] 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

[Cormen] 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*

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

Teil A
Algebraische Grundstrukturen

> 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 mantain mathematical integrity as much as I can.
>
> Donald E. Knuth

1 Algebraische Grundlagen

Beispiel A.1. `unsigned char` in Programmiersprachen (`C`, `C++`, Java, etc.)
$a \in \mathcal{B} \equiv \left\{0, 1, 2, 3, \ldots, 254, 255\right\}$
wobei $255 = 2^8 - 1 = m - 1$ mit m $\equiv 256$

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

Definition A.2 (Verknüpfungseigenschaften). Für Verknüpfungen $\circ$ zwischen Elementen einer Menge $\mathcal{M}$ betrachtet man die Eigenschaften:

(i) $(a \circ b) \circ c = a \circ (b \circ c)$ **Assoziativität**

(ii) $e \circ b = b \circ e = b$ **Neutrales bzw. Einselement**

(iii) $a \circ b = b \circ a$ **Kommutativität**

(iv) $a \circ b = e$ **Inverse Elemente**

Definition A.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.4 *(Nichtkommutativer Monoid).* Alle Worte bzw Zeichenketten A^* über einem gegebenen Alphabet A, z.B. $\{0, 1\}$ oder $\{a, b, \cdots, z\}$ wobei + Konkatenation und e das Leere Wort sind, d.h

$$axz + yi = axzyi.$$

Beispiel A.5 *(Kommutativer Monoid).* $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ Menge der positiven natürlichen Zahlen bzgl. $*$ mit neutralem Element 1.

Beispiel A.6 *(Kommutative Gruppe).* $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ 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.7 (Ring). Eine Menge $\mathcal{M}$ heisst Ring falls

(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.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.9 *(Nichtkommutativer Ring mit 1).* $\mathbb{Z}^{2\times 2}$ d.h. die Menge allen 2×2 Matrizen mit ganzahligen Elementen.

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \qquad 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Lemma A.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.11 (Körper). Ein Ring $\mathcal{M}$ mit 1 heisst Körper falls $\mathcal{M}\backslash\{0\}$ 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.12 *(Kommutativer Körper).*

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

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

> Wahre Menschen, die Sinn und Wahrheit suchen, studieren Mathematik, Informatik, Psychologie usw. Wenn wir bei IBM eine solche eher seltene Mischung von Mitarbeitern haben, müssen wir auch dementsprechend artgerechtes Management betreiben.
>
> Gunter Dueck, IBM Global Services (N.D. 21.10.2004)

2 Algebraische Teilstrukturen

Definition A.1. Häufig hat eine Teilmenge $\mathcal{U} \subseteq \mathcal{M}$ einer Halbgruppe, eines Monoids, einer Gruppe, eines Ringes oder eines Körpers diesselben strukturellen Eigenschaften bezüglich der vorgegebenen Verknüpfungen. Sie heißt dann entsprechend Unter- oder Teil- Halbgruppe, Monoid, Gruppe, Ring oder Körper.

Lemma A.2 (*Schnittprinzip*)**.** *Der Durchschnitt zweier Unterhalbgruppen, Untergruppen, Unterringe oder Unterkörper ist wiederum eine Unterhalbgruppe, Untergruppe, Unterring, Unterkörper usw.*

Beispiel A.3. $\mathbb{N}$ ist Teilmonoid von $\mathbb{Z}$.

Beispiel A.4. $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$.

Beispiel A.5. $2\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \textit{ ist gerade}\}$ ist Untergruppe von $\mathbb{Z}$.

Beispiel A.6. $3\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \textit{ ist durch } 3 \textit{ teilbar}\}$ ist Untergruppe von $\mathbb{Z}$.

Beispiel A.7. $2\mathbb{Z} \cap 3\mathbb{Z} \equiv \{a \in \mathbb{Z} : a \textit{ ist durch } 6 \textit{ teilbar}\}$ ist Untergruppe von $\mathbb{Z}$.

Beispiel A.8. Geometrische Rotationen in der Ebene bilden eine kommutative Gruppe, die man mit $\mathcal{S}_1$ bezeichet. Links- oder Rechtsdrehungen um ein Vielfaches von 30 Grad bilden eine Untergruppe. Neutrales Element ist die Drehung um den Winkel Null.

Beispiel A.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.

Warnung:
Lemma A.2 gilt nicht für Vereinigungen.
Der Schnitt von Ringen mit 1 braucht keine 1 zu haben.

Definition A.10 (Hüllenbildung).

(i) 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 $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ von $\mathcal{U}$ bezeichnet.

(ii) Die Element dieser Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ lassen sich als Ergebnis beliebiger Verknüpfungen und Inversionen von Elementen aus $\mathcal{U}$ darstellen.

Man bezeichnet $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ deshalb auch als den Abschluss von $\mathcal{U}$ bezüglich der vorhandenen Verknüpfungen.

Lemma A.11 (Abschluss in Halbgruppe). *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 $u \in M$ 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.

Lemma A.12 (Abschluss in Gruppe). *Sei $\mathcal{U} \subset \mathcal{M}$ Teilmenge einer Gruppe $\mathcal{M}$ mit der Verknüpfung $+$ und $a - b = a + (-b)$. Dann besteht die Hülle $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ aus allen Elementen $u \in \mathcal{M}$ der Form*

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

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

Lemma A.13 (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 $\mathbf{span}_{\mathcal{M}}(\mathcal{U})$ aus allen Elementen $u \in \mathcal{M}$ der Form*

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

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

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.1. Die natürlichen Zahlen $\mathbb{N}$ sind bezüglich der Addition nur ein Monoid (d.h. Halbgruppe) mit den 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. Mann 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.2. Durch obige Konstruktion erhält man $\mathbb{Z}$, das 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 char**s $\mathcal{B}$, da dort $32 * 8 = 0$ gilt.

Hätte 8 in irgendeiner Erweiterung einen Kehrwert 8^{-1}, so wurde folgen $32 = 32 * 8 * 8^{-1} = 0 * 8^{-1} = 0$ was offensichtlich inkonsistent wäre.

Definition A.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.4 (Nullteiler oder Inverse). *In einem endlichen Ring ist jedes Element $a \neq 0$ entweder selbst Nullteiler oder hat ein multiplikatives Inverses der Form $a^{-1} = a^k = a * \cdots * a$ für ein $k \in \mathbb{N}$.*

Satz A.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

$\bigcap$ (Negativenbildung)

Ring $\mathbb{Z}$ Ganze Zahlen

$\bigcap$ (Quotientenbildung)

Körper $\mathbb{Q}$ Rationalen Zahlen

$\bigcap$ (Inf/Sup Bildung)

Körper $\mathbb{R}$ Reelle Zahlen

$\bigcap$ (Wurzelberechnung)

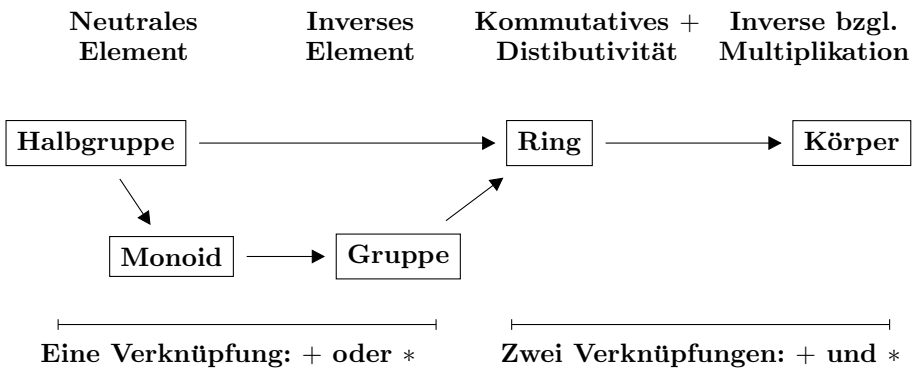
Körper $\mathbb{C} \simeq \mathbb{R} \times \mathbb{R}$ Komplexer Zahlen

$\bigcap$ (Mathemathischer 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.

3.1 Hierarchie algebraischer Grundstrukturen



4 Äquivalenzrelationen und Quotientenstrukturen

Bemerkung
Die Menge der **unsigned char**s $\mathcal{B}$ 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 φ_1, φ_2, deren Differenz ein ganzes Vielfaches von 2π ist, zusammengelegt werden, da sie als äquivalent betracht werden.

Definition A.1 (Äquivalenzrelationen). Man nennt $\mathcal{R} \subset \mathcal{M} \times \mathcal{M}$ eine Äquivalenzrelation auf $\mathcal{M}$ und schreibt dann

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

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

$$x \sim x \qquad \textbf{Reflexivität}$$

$$x \sim y \wedge y \sim z \Longrightarrow \quad x \sim z \qquad \textbf{Transitivität}$$

$$x \sim y \Longrightarrow y \sim x \qquad \textbf{Symmetrie}$$

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 $\mathcal{R}$ klar schreibt man einfach $[x]$.

Beispiel A.2. Für $x, y \in \mathbb{R}$ gilt:

$$x \sim y \quad \Longleftrightarrow \quad x * x = y * y \Longrightarrow [x] = \{+x, -x\}$$

Beispiel A.3. Geraden in der Ebene sind äquivalent, wenn sie parallel sind.
Äquivalenzmengen sind alle Geraden mit derselben Steigung.

Lemma A.4 (Quotientenäquivalenz). *Für $x = (x_1, x_2) \in \mathbb{Z} \times (\,\mathbb{Z} \backslash \{0\}\,) \ni y = (y_1, y_2)$ gilt:*

$$x \sim y \quad \Longleftrightarrow \quad x_1 * y_2 = y_1 * x_2$$

Lemma A.5 (Restklassen bezüglich Untergruppe). *$\mathcal{U} \subset \mathcal{G}$ kommutative Untergruppe impliziert, dass*

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

eine Äquivalenzrelation ist.

Beispiel A.6. Für festes $m \in \mathbb{Z}$ gilt: $x \sim y \Longleftrightarrow m$ teilt $x - y$.

Lemma A.7 (Partitionierung). *Sei $\sim$ Äquivalenzrelation auf $\mathcal{M}$.*

1. $[x] = [y] \quad \Longleftrightarrow \quad x \sim y$
2. $[x] \cap [y] = \emptyset \quad \Longleftrightarrow \quad x \not\sim y$
3. *Es existiert eine Repräsentantenmenge $\mathcal{M}' \subset \mathcal{M}$ so dass*

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

   und somit

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

   sowie

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

Beispiel A.8. Für Beispiel A.6 nehme Repräsentant $0 \leq x < m$.

Beispiel A.9. Für Lemma A.4 nehme gekürzten Bruch wo x_1 und x_2 teilerfremd sind.

Beispiel A.10. Für Beispiel A.3 nehme Gerade durch Nullpunkt.

Definition A.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.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.13 *(Symmetrische Gruppe).*

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

Beispiel A.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 sogar Ideal im Ring $\mathbb{Z}$ ist.

Definition A.15 (Ideal). Eine Untergruppe $U \subset \mathcal{M}$ heisst **Ideal des kommutativen Ringes** $\mathcal{M}$ falls

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

m.a.W. Produkte mit einem Faktor in $\mathcal{U}$ gehören auch zu $\mathcal{U}$.

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

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

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

Bemerkung:
Jedes Ideal ist insbesondere ein Unterrring. Körper haben keine Hauptideale außer sich selbst und $\{0\}$.

Beispiel A.16. $m\mathbb{Z}$ ist Hauptideal in $\mathbb{Z}$.

Beispiel A.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.18 (Quotientenringe). *Gilt Satz A.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

- $\mathcal{B} =$ `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.

5 Modulare Arithmetik

Satz A.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:*

$$a \;=\; qm + r \qquad \wedge \qquad 0 \leq r < m > 0.$$

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

Definition A.2 (Modulobezeichnung, Teilbarkeit, Primzahl).

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

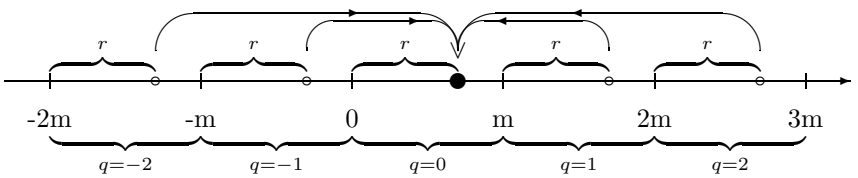
$$r = r_m(a) = a \bmod m$$

(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**.

5.1 Zahlengerade



Beispiel A.3. $7 \bmod 3 \;=\; r_3(7) \;=\; 1 \quad (q = 2)$

Beispiel A.4. $-13 \bmod 5 \;=\; r_5(-13) \;=\; 2 \quad (q = -3)$

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

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

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:

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

Satz A.5 (Modulare Arithmetik). *In $\mathbb{Z}_m \simeq \{0, 1, \cdots, m-1\}$ 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.6 (Fermat(1640)). *Falls m prim gilt für alle $0 \leq a < m$*

$$a^m = a \bmod m.$$

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

Korollar A.7. *$\mathbb{Z}_m$ ist genau dann ein Integritätsbereich und damit nach Satz A.5 ein Körper, wenn m eine Primzahl ist. Dann gilt für alle $a \in \mathbb{Z}_m$*

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

Beispiel A.8. In $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ gilt:

$$\begin{aligned}
\bar{1}^{-1} &= \bar{1} * \bar{1} * \bar{1} = \;\; 1 \bmod 5 = \bar{1} &\Longrightarrow\quad & \bar{1} * \bar{1} = \;\; 1 \bmod 5 = \bar{1}\\
\bar{2}^{-1} &= \bar{2} * \bar{2} * \bar{2} = \;\; 8 \bmod 5 = \bar{3} &\Longrightarrow\quad & \bar{2} * \bar{3} = \;\; 6 \bmod 5 = \bar{1}\\
\bar{3}^{-1} &= \bar{3} * \bar{3} * \bar{3} = 27 \bmod 5 = \bar{2} &\Longrightarrow\quad & \bar{3} * \bar{2} = \;\; 6 \bmod 5 = \bar{1}\\
\bar{4}^{-1} &= \bar{4} * \bar{4} * \bar{4} = 64 \bmod 5 = \bar{4} &\Longrightarrow\quad & \bar{3} * \bar{4} = 16 \bmod 5 = \bar{1}
\end{aligned}$$

5.2 Multiplikation in $\mathbb{Z}_5$

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

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

Subtraktion

Addition

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

5.4 Division in $\mathbb{Z}_5$

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

5.5 Anwendung: Hashing

Motivation:
Angenommen eine Firme 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 durchnumerierten Ablagen angelegt. Um schnell auf diese zugreifen zu können, sucht sie für $n = 10^{10}$ eine sogenannte **Hashfunktion**

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

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

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

nicht immer verhindern.

Das gilt auch für die einfache **Hashfunktion**

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

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

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

für $i = 1, 2, \cdots, (p-1)/2$, 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.9 (siehe Hartmann 4.24). *Ist p eine Primzahl mit $p \bmod 4 = 3$ so gilt:*

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

Mit anderen Worten: Alle Adressen werden durchsucht.

Beispiel A.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

6 Strukturerhaltende 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

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

lassen sich die Eindeutigkeitseigenschaften von Abbildungen wie folgt charakterisieren. ϕ 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. Inbesondere kann man jede Menge von $n < \infty$ Elementen darstellen als

$$\mathcal{M} \;=\; \{1, 2, \ldots, n-1, n\}$$

Definition A.1 (Permutationen). Eine bijektive Abbildung ϕ einer endlichen Menge in sich selbst heisst **Permutation** und lässt sich spezifizieren in der Tupelform

$$(\phi(1),\ \phi(2),\ \phi(3),\ \ldots,\ \phi(n)) \;\in\; \mathbb{N}^n$$

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

Beispiel A.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 ϕ_1 für $i = 1 \ldots 6$

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

Da ϕ_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

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

Die letzten beiden ϕ_5, ϕ_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.4 (Homomorphismus und Endomorphismus).

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

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

dann heisst ϕ 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 ϕ im obigen respektiert wird, nennt man ϕ einen Halbgruppenhomorphismus, Ringhomomorphismus usw.

Beispiel A.5. Für jede ganze Zahl $m > 1$ ist die Abbildung

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

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

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

Lemma A.6. *Für jedes feste $0 \neq m \in \mathbb{Z}$ ist die Abbildung*

$$\phi(a) \;=\; r_m(a) \;=\; a \; mod \; m$$

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

Definition A.7 (Isomorphismus).

1. Bijektive Homomorphismen heissen **Isomorphismen**. Gibt es einen Isomorphismus zwischen den algbraischen Strukturen $\mathcal{M}$ und $\mathcal{N}$, so nennt man diese **isomorph**.

2. 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 genau diesselbe 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 kann aber sogar isomorphe Endomorphismen geben, die nicht unbedingt auf der Hand liegen und sich insbesondere von der Indentität unterscheiden.

Beispiel A.8. Auf dem Matrizenring $\mathbb{Z}^{2\times 2}$ kann man ϕ definieren so dass

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

Mit anderen Worten: Die Zeilen und Spalten der 2×2 Matrizen werden ausgetauscht.

Man kann überprüfen, dass ϕ 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.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 ϕ.

Man kann $\mathbb{Z}$ natürlich auch isomorph in $\mathbb{Z}^{2\times 2}$ einbetten, wenn man a durch ϕ in das zweite Diagonalelement von A bringen lässt.
Kopiert ϕ 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 ϕ ist kein Ringhomomorphismus, sondern nur noch ein injektiver Gruppenhomorphismus (Siehe Übung). Und das, obwohl dann das aus allen strikt dreiecksförmigen Matrizen bestehende Bild $\phi(\mathbb{Z})$ sogar wiederum ein Ring ist.

Lemma A.10.

1. *Jeder surjektive Homomorphismus ϕ bildet die neutralen und inversen Elemente von $\mathcal{M}$ in die entsprechenden neutralen und inversen Element von $\mathcal{N}$ ab.*

2. *Die homomorphen Bilder $\phi(\mathcal{U}) \subset \mathcal{N}$ von Unter(halb)gruppen, Unterringen usw. $\mathcal{U} \subset \mathcal{M}$ bilden dieselben Unterstrukturen von $\mathcal{N}$.*

3. *Das* **Kern** *von ϕ genannte Urbild*

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

ist bei Gruppenhomomorphismen eine Unterguppe 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.11. *(i) Alle Endomorphismen einer Gruppe $\mathcal{M}$ in sich selbst bilden bezüglich der Hintereinanderausführung zunächst einen Monoid $Endo(\mathcal{M})$. Dessen neutrales Element ist die Indentitätsabbildung*

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

(ii) Die bijektiven Abbildungen bilden einen Untermonoid $Iso(\mathcal{M}) \subset Endo(\mathcal{M})$ mit multiplikativer nichtkommutativer Gruppenstruktur.

(iii) Ist $\mathcal{M}$ selbst kommutative Gruppe, so kann man für jeweils zwei Elemente $\phi, \psi \in Endo(\mathcal{M})$ ihre Summe $\eta = \phi + \psi$ definieren durch

$$\eta(a) \;=\; (\phi + \psi)(a) \;=\; \phi(a) + \psi(a) \quad für \quad a \in M$$

Bezüglich dieser Addition und der Hintereinanderausführung als Multiplikation bildet $Endo(\mathcal{M})$ 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 Isomorphie zwischen Ringen sprechen, von denen einer selbst aus Homomorphismen einer Gruppe besteht.

Bemerkung
Die letzte Isomorphieaussage im Lemma A.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.

7 Teilbarkeit und partielle Ordnungen

Lemma A.1 (Eigenschaften der Teilbarkeit). *Für $a, b, c \in \mathcal{M} = \mathbb{N}$ gilt:*

1. $a|b \ \wedge \ b|c \quad \Longrightarrow \quad a|c$ ***Transitivität***
2. $a|b \ \wedge \ b|a \quad \Longrightarrow \quad a = b$ ***Antisymmetrie***
3. $a|a$ ***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.2 (Ordnungsrelation).

1. Die durch eine Menge $\mathcal{R} \subset \mathcal{M} \times \mathcal{M}$, definierte Beziehung
$$a \prec b \quad \Longleftrightarrow \quad b \succ a \quad \Longleftrightarrow \quad (a, b) \in \mathcal{R},$$
heißt **Ordnungsrelation** falls
$$\begin{array}{lcll} a \prec b \ \wedge \ b \prec c & \Longrightarrow & a \prec c & \textbf{Transitivität} \\ a \prec b \ \wedge \ b \prec a & \Longrightarrow & a = b & \textbf{Antisymmetrie} \end{array}$$

2. Die Ordnungsrelation heißt **streng** falls für alle $a \in \mathcal{M}$ die folgenden äquivalenten Aussagen gelten
$$a \not\prec a \quad \Longleftrightarrow \quad \neg(a \prec a).$$
Dann wird durch
$$a \preceq b \quad \Longleftrightarrow \quad a \prec b \ \vee \ a = b$$
eine **reflexive** Ordnungsrelation definiert, so daß $a \preceq a$ für alle $a \in \mathcal{M}$. Umgekehrt ergibt sich strenge Ordnung durch
$$a \prec b \quad \Longleftrightarrow \quad a \preceq b \ \wedge \ a \neq b$$

3. 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.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.4. Koordinatenvektoren (x, y) in Ebene werden durch
$$a \ = \ (x_1, y_1) \ \leq \ b \ = \ (x_2, y_2) \quad \Longleftrightarrow \quad x_1 \leq x_2 \ \wedge \ y_1 \leq y_2$$
partiell geordnet.

Beispiel A.5. Die Enthaltenenseinsbeziehung von Mengen
$$\mathcal{M} \prec \mathcal{N} \quad \Longleftrightarrow \quad \mathcal{M} \subset \mathcal{N}$$
ist eine partielle nichtstrenge, d.h. reflexive Ordnung.

Definition A.6. Das Alphabet $\mathcal{A} = \{a, b, c, \ldots, x, y, z\}$ 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.
$$(a_1, a_2, \ldots, a_n) \quad \prec \quad (b_1, b_2, \ldots, b_m)$$
gilt genau dann wenn ein $k \leq \min(m, n)$ existiert so dass
$$a_i = b_i \text{ für } i \leq k \qquad \text{und} \qquad (\ a_{k+1} < b_{k+1} \quad \text{oder} \quad k = n < m)\,.$$

Beispiel A.7 *(Telefonbuch).*

$$\ldots \ \texttt{griewank} \prec \texttt{grünewald} \prec \quad \ldots \quad \prec \texttt{meier} \prec \texttt{meiers} \prec \ldots$$

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.

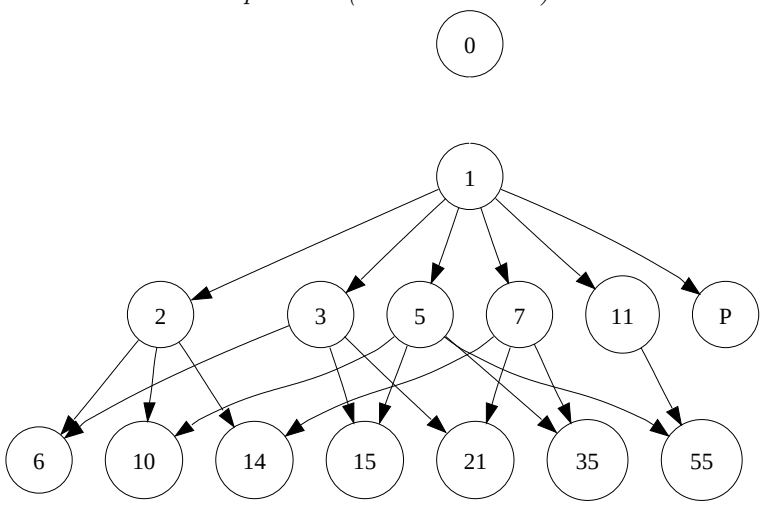
$$(a, b) \in \mathcal{K} \quad \Longleftrightarrow \quad a \prec b \ \wedge \ a \neq b \ \wedge \ (a \prec c \prec b \Longrightarrow c = a \ \vee \ c = b)\,.$$

Dann erhalten wir einen

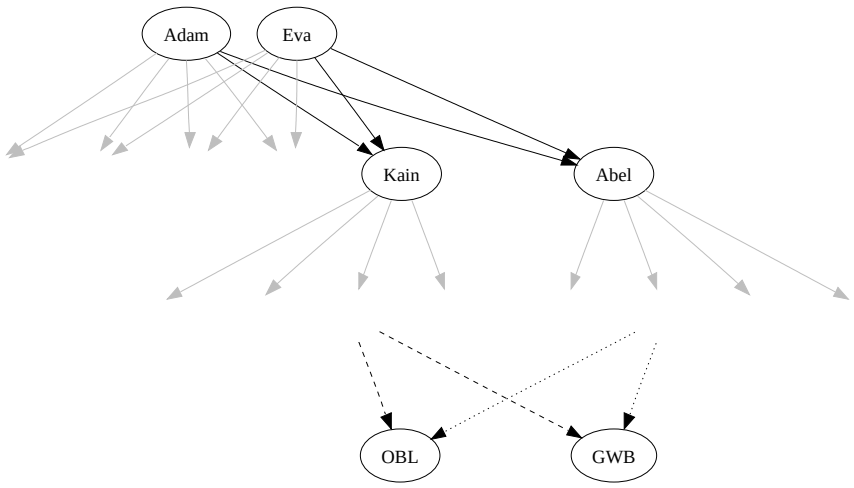
DAG ≡ Directed Acyclic Graph.

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

Beispiel A.8 *(Teilbarkeit in* $\mathbb{N}$*).*



Beispiel A.9 *(Stammbaum der Menscheit).*
$a \prec b$ 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.

8 Verbandstruktur und größter gemeinsamer Teiler

Definition A.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

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

und

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

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.2 (Rechenregeln in Verbänden).

(i) $\inf(a, a) = a \quad \wedge \quad \sup(a, a) = a$ ***Idempotenz***

(ii) $\inf(b, a) = \inf(a, b) \quad \wedge \quad \sup(b, a) = \sup(a, b)$ ***Kommutativität***

(iii) $\inf(a, \inf(b, c)) \ = \ \inf(\inf(a, b), c)$ ***Assoziativität***

$\sup(a, \sup(b, c)) \ = \ \sup(\sup(a, b), c)$

(iv) $\inf(a, \sup(a, b)) \ = \ a \quad \wedge \quad \sup(a, \inf(a, b)) \ = \ a$ ***Absorption***

(v) $a \preceq b \quad \Longleftrightarrow \quad \inf(a, b) = a \quad \Longleftrightarrow \quad \sup(a, b) = b$ ***Konsistenz***

Beispiel A.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:

- $B \prec C \quad \Longleftrightarrow \quad B \subset C$ **Inklusion**
- $\inf(B, C) \ = \ B \cap C$ **Schnittmenge**
- $\sup(B, C) \ = \ B \cup C$ **Vereinigung**

Beispiel A.4. $\mathcal{M} = \{0, 1\}$ mit Boolschen Verknüpfung $\begin{cases} \inf & = & \textit{Konjunktion} & \wedge \\ \sup & = & \textit{Disjunktion} & \vee \end{cases}$

inf	0	1
0	0	0
1	0	1

sup	0	1
0	0	1
1	1	1

Beispiel A.5. $\mathcal{M} = \mathbb{N}_+ = \mathbb{N} \setminus \{0\}$:

$$a \prec b \quad \Longleftrightarrow \quad a|b$$

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

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

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

$$(c|a \ \wedge \ c|b) \quad \wedge \quad (c'|a \ \wedge \ c'|b \Longrightarrow c'|c)$$

und ist dann wegen der Antisymmetrie der Teilbarkeitsrelation eindeutig.

Satz A.6 (Existenz des GGT). *Für $a, b \in \mathbb{N}_+$ gibt es $s, t \in \mathbb{Z}$, so daß*

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

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.

9 Euklidescher Algorithmus und Anwendungen

Lemma A.1.

1. $0 < a \quad \Longrightarrow \quad GGT(0, a) = a$
2. $0 < a < b \quad \Longrightarrow \quad GGT(a, b) = GGT(b \bmod a, a)$

Euklidischer Algorithmus:

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

```
r := b mod a
WHILE (0 ≠ r)
        b := a
        a := r
        r := b mod a
```

Output: a

Lemma A.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.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.4. *Die maximale Schrittzahl k erfüllt die Bedingung*

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

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.5. Für Beispiel $GGT(228, 612) = 12$ gilt: $3 \leq k_{max} \leq 16.6$, 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.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. $GGT(a, b) = 1$. Dann gilt*

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

Bemerkung
Bislang haben wir multiplikative Inverse von a unter den Potenzen $a^k \bmod b$ für $k = 0, 1, \ldots$ gesucht, was spätestens für $k = b - 2$ zum Erfolg führen muss (Satz A.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 Euklidschen 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

$$a = s_a * a_0 + t_a * b_0, \quad b = s_b * a_0 + t_b * b_0, \quad r = s_r * a_0 + t_r * b_0$$

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

$$s_r = s_b - q * s_a \quad \text{und} \quad t_r = t_b - q * t_a$$

Da die Koeffizienten bezüglich b_0 (nämlich t_a, t_b und t_r) uns letztlich nicht interessieren, ist die einzige Zusatzrechnung die Anweisung $s_r = s_b - q * s_a$ wobei allerdings das Ersetzen von (a, b) durch (r, b) mit durchgeführt werden muss. 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` $(0 \neq r)$
$\quad q := (b - r)/a$
$\quad b := a$
$\quad a := r$
$\quad t := v - q * s$
$\quad v := s$
$\quad s := t$
$\quad r := b \bmod a$

Output: $a,\ s \bmod b$

Beispiel A.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 Kongruenzengleichungen zu finden.
Wir betrachten zunächst ein Paar von Gleichungen

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

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

Nur falls $KGV(m,n) = m * n$ und äquivalenterweise $GGT(m,n) = 1$ kann man hoffen, dass es zwischen 0 und $n * m$ genau eine Lösung 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 Vorraussetzung, 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.8. *Vorrausgesetzt $GGT(m,n) = 1$ 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

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

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 $GGT(9,7) = 1$, 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.6 auswerten.

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

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 Interval $0, 1, \ldots n * m - 1$ zu landen.

Verallgemeinerung auf $n > 2$ Gleichungen
Betrachte ein System von Kongruenzen

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

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

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

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

Lemma A.9. *Für alle $i = 1 \ldots n$ 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

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

und somit

$$M_i \bmod m_j \;=\; 0 \quad \textit{falls} \quad j \neq i\,.$$

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

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

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

10 Darstellungen ganzer Zahlen

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

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

gibt. Mit ihrer Hilfe ergibt sich folgende Darstellung:

Satz A.1 (Primzahlzerlegung). *Jede natürliche Zahl $a > 1$ hat eine eindeutige Darstellung der Form*

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

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 $(e_j)_{j \le n}$ abzuspeichern. Läßt man auch negative e_j zu, so ergeben sich sogar alle rationalen Zahlen.

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

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

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.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 Ziffern $a_j \in \{0, 1, \cdots, b-1\}$ eindeutig darstellen:*

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

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

Beispiel A.3. **Dezimalsystem** *Primaten mit 10 Fingern, Taschenrechner*

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

Beispiel A.4. **Binärsystem** *Computerspeicher*

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

Beispiel A.5. **Hexadezimalsystem** *Computerausgabe*

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 ≠ a)
        a_i := a mod b
        a  := (a − a_i) / b
        i  := i + 1
```

Output: $(a_i, a_{i-1}, \ldots, a_0)_b$ – Koeffizienten von a bzgl. Basis b

Beispiel A.6 *(* $a = (788)_{10} = (???)_3 \qquad b = 3$ *).*

i	0	1	2	3	4	5	6
a	788	262	87	29	9	3	1
a mod 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

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

Input: $(x)_b, (y)_b$
$q = 0$
`FOR` $i := 0, 1, 2, \ldots$
$r := (x_i + y_i + q) \bmod b$
$z_i := r$
$q := (x_i + y_i + q - r) \ / \ b$

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

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

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.7 *(Oktale Multiplikation).*

$$
\begin{aligned}
(303)_8 &= 3 \cdot 8^0 + 0 \cdot 8^1 + 3 \cdot 8^2 = (195)_{10} \\
(52)_8 &= 2 \cdot 8^0 + 5 \cdot 8^1 + 0 \cdot 8^2 = (42)_{10} \\
(303)_8 * (52)_8 &= 6 \cdot 8^0 + (17)_8 \cdot 8^1 + 6 \cdot 8^2 + (17)_8 \cdot 8^3 \\
&= 6 \cdot 8^0 + 7 \cdot 8^1 + 7 \cdot 8^2 + 7 \cdot 8^3 + 1 \cdot 8^4 \\
&= (8190)_{10}
\end{aligned}
$$

Bemerkung
Betrachtet man die Addition und Multiplikation von Ziffern mit eventuellem Übertrag als Konsteneinheit, so wächst der Aufwand quadratisch mit der Gesamtanzahl der Ziffern.
Das ähnelt schon sehr Polynommanipulationen.

11 Polynome als Funktionen

Definition A.1 (Polynom). Einen Ausdruck der Form

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

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

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

Beispiel A.2. Kubisches Polynom über dem Koeffizientenring $\mathbb{Z}$:

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

Beispiel A.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 einen Oberring $\mathcal{R}' \supset \mathcal{R}$, 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 $\mathcal{R}$ noch $\mathcal{R}$ oder $\mathcal{R}'$ nach $\mathcal{R}'$.

Lemma A.4 (Horner Schema). *Die Auswertung eines Polynomes mit Hilfe der Klammerung*

$$P(x) = c_0 \;+\; x * (c_1 \;+\; x * (\;\ldots\;\; (c_{n-1} \;+\; x * c_n \underbrace{)\ldots))}_{n-1}$$

verlangt lediglich n Multiplikationen und ebenso viele Additionen.

Algorithmus Horner-Schema:

Input: $x \in \mathbb{R}, c_i \in \mathbb{R}, i = 0, \ldots, n = \deg(P(x))$[.5em]
$y = 0$
`FOR` $i := n, n-1, \ldots, 1, 0$
$y := c_i + x * y$
Output: $y = P(x)$ ... Wert des Polynoms an der Stelle $x \in \mathbb{R}$

Beispiel A.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. [0.4cm] 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.6 (Lagrange - Interpolation). *Sei $\mathcal{R} = \mathbb{R}$ oder ein anderer Körper. Dann gilt:*

1. *Es existiert zu jeder Familie von Wertepaaren*
$$(x_i, y_i) \in \mathcal{R} \times \mathcal{R} \qquad \text{für } i = 0, 1, \ldots, n$$
mit unterschiedlichen "Abzissenwerten"
$$x_i \neq x_j \quad \text{für } i \neq j$$
ein Interpolationspolynom $P(x)$ vom Grad $\leq n$, so daß
$$P(x_i) = y_i \qquad \text{für } i = 0, 1, \ldots, n.$$

2. *Dieses Polynom ist eindeutig und läßt sich darstellen als*
$$P(x) = \sum_{i=0}^{n} y_i \underbrace{\frac{(x - x_0)\ldots(x - x_{i-1})(x - x_{i+1})\ldots(x - x_n)}{(x_i - x_0)\ldots(x_i - x_{i-1})(x_i - x_{i+1})\ldots(x_i - x_n)}}_{\equiv P_i(x)}$$

3. *Insbesondere folgt aus $y_i = 0$ für $i = 0, \ldots, n$, dass alle Koeffizienten c_i in $P(x) = c_0 + c_1 x + c_2 x^2 + \ldots$ verschwinden, d.h. es gilt*
$$c_i = 0 \qquad \text{für } i = 0, \ldots, n.$$

Beweis:

(i) Die Existenz folgt aus der Gültigkeit der Darstellung (ii), welche zunächst geprüft wird. Die Ausdrücke
$$P_i(x) = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)} \qquad \text{für } i = 0, \ldots, n$$
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
$$P(x_j) = \sum_{j=0}^{n} y_i P_i(x_j) = y_j.$$
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 $\deg(P) < n$.

(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
$$R(x) = \sum_{j=0}^{n} (p_j - q_j) x^j = P(x) - Q(x)$$
insbesondere
$$R(x_j) = P(x_j) - Q(x_j) = y_j - y_j = 0 \qquad \text{für } i = 0, \ldots, n.$$
Also folgt aus der letzten Aussage (iii) dass
$$p_j - q_j = 0 \qquad \text{für } j = 0, \ldots, n.$$
und damit die behauptete Eindeutigkeit.

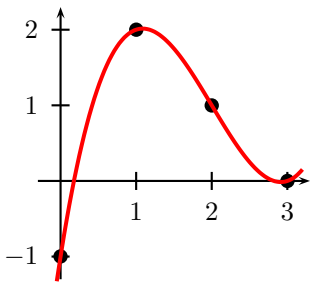
(iii) Beweis folgt später (mittels Polynomdivision)

□

11.1 Beispiel – Lagrangepolynom

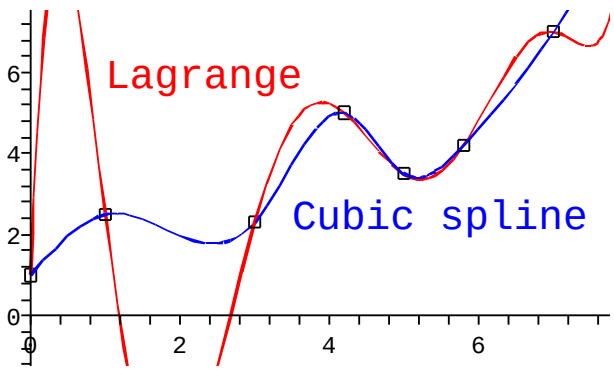
x_i	0	1	2	3
y_i	-1	2	1	0

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



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

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. $\Longrightarrow$ Cubic Splines, Finite Elemente.



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

$$P(x) = 0$$

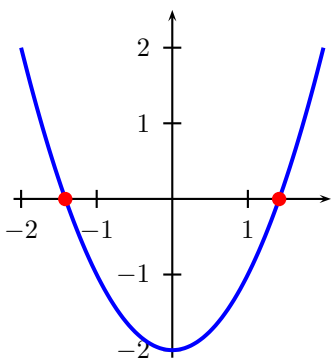
Die Nullstellen von Polynomen werden auch deren **Wurzeln** genannt. Wie wir später sehen werden, kann ein Polynom $P(x)$ über einem Körper nur $m \leq n = deg(P)$ unterschiedliche Wurzeln haben.

Beispiel A.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.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 jahrhundertelang versucht die Wurzeln allgemeiner Polynome durch sie auszudrücken. Das gelingt zum Beispiel im quadratischen Fall $n = 2$ wie folgt.

Lemma A.9 (Lösung einer quadratischen Gleichung). *Das Polynom*

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

hat im Falle $\gamma\alpha \leq \frac{1}{4}\beta^2$ *die reellen Wurzeln*

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

Lemma A.10 (Explizite Lösung einer kubischen Gleichung).
Das kubische Polynom

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

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

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

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 α. 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 Audrücken 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.

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 $m \geq n$ definiert als

$$E(x) = C(x) \ + \ D(x) = \sum_{j=0}^{m} e_j x^j \quad \text{mit} \quad e_j = \begin{cases} c_j + d_j & \text{für} \quad j \leq n \\ d_j & \text{für} \quad n < j \leq m \end{cases}$$

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

1. $P(x) = 0 = 0 \cdot x^0 + 0 \cdot x^1 + \cdots$ ***Nullelement***
2. $P(x) = 1 = 1 \cdot x^0 + 0 \cdot x^1$ ***Einselement***
3. *Den Grad des Nullelementes setzt man zu $deg(0) = -\infty$*
4. $deg(P(x)) = 0$ *genau dann wenn* $P(x) = c_0 \in \mathcal{R} \wedge c_0 \neq 0$
5. *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 $\mathbb{Z} \longrightarrow \mathbb{Q}$).
Damit ergibt sich die Frage nach der Division von Polynomen.

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

Satz A.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*

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

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.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.4 (Teilbarkeit in $\mathcal{R}[x]$).

1. Falls ein Polynom $0 \neq c(x) \in \mathcal{R}[x]$ eine Produktdarstellung
$$c(x) \;=\; a(x) * b(x) \qquad \text{mit } \; a(x), b(x) \in \mathcal{R}[x]$$
besitzt, heissen $a(x)$ und $b(x)$ **Teiler** von $c(x)$. Man schreibt dann wie üblich $a(x)|c(x)$ und $b(x)|c(x)$.

2. Falls sowohl $a(x)$ wie $b(x)$ nicht konstant sind, d.h.
$$\begin{aligned} 0 < \quad & deg(a(x)) \quad < deg(c(x)) \\ 0 < \quad & deg(b(x)) \quad < deg(c(x)), \end{aligned}$$
dann nennt man $a(x)$ und $b(x)$ **echte Teiler** von $c(x)$.

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

Lemma A.5. *Wie im Ring der ganzen Zahlen gilt für irreduzibles $c(x) \in \mathcal{R}[x]$ die Implikation*
$$c(x)|(a(x) * b(x)) \quad \Longrightarrow \quad c(x)|a(x) \;\vee\; c(x)|b(x)$$

Satz A.6. *Ist $\mathcal{R}$ ein Körper, so besitzt jedes Polynom $a(x) \in \mathcal{R}[x]$ eine Faktorisierung*
$$a(x) = p_1(x)\, p_2(x) \;\ldots\; p_m(x)$$
in irreduzible Polynome $p_j(x)$ für $j = 1 \ldots m$.
Diese sind eindeutig bis auf konstante Faktoren, d.h. aus
$$a(x) = p'_1(x) \;\ldots\; p'_m(x)$$
folgt (gegebenenfalls nach Umnumerierung)
$$p'_j(x) = \gamma_j p_j(x) \qquad \textit{mit} \quad \gamma_j \in \mathcal{R}\,.$$

Beispiel A.7.
$$x^3 - 1 = (x-1) * (x^2 + x + 1), \quad \text{da } x^2 + x + 1 \;\text{ und }\; x - 1 \quad \text{irreduzibel.}$$

Beobachtung:
Mit $b(x) = x - x_0$ für $x_0 \in \mathcal{R}$ als lineares Polynom ergibt sich aus Satz A.2 für ein beliebiges Polynom $a(x)$ mit $deg(a(x)) > 0$ die Darstellung
$$a(x) = q(x) * (x - x_0) + r_0 \qquad \text{mit} \qquad r_0 = a(x_0) \in R\,.$$
Die letzte Aussage folgt durch Einsetzten, da das Residuum r_0 vom Grad $0 < 1 = deg(b)$ sein muss.

Folgerung aus Definition A.4: Teilbarkeit in $\mathcal{R}[x]$

1. Offenbar folgt aus der Zerlegung $a(x) = q(x) * b(x) + r(x)$ dass
$$b(x)|a(x) \Longleftrightarrow r(x) = 0$$
so dass wir in $\mathcal{R}[x]$ einen konstruktiven Teilbarkeitstest haben.

2. 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 $1\mathcal{R}$ normalisiert wird.

3. Die Berechnung des $GGT(a(x), b(x))$ erfolgt wiederum durch den Euklidischen Algorithmus.

4. 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**.

13 Faktorisierung und Nullstellen

Korollar A.1.

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

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

2. *Man nennt $(x - x_0)$ einen* ***Linearfaktor*** *von $a(x)$ und es muss gelten*

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

3. *Die Koeffizienten q_i des Polynomes $q(x)$ ergeben sich aus $q_{n-1} = a_n$ gemäss dem Hornerschema als*

$$q_{i-1} = a_i + q_i * x_0 \quad \textit{für} \quad i = n - 1 \ldots 1$$

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 identisch gleich null ist. Im letzteren Fall ist auch $a(x)$ identisch gleich null.

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

Folgerung
Da immer

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

kann ein Polynom vom Grad n also höchstens n Nullstellen haben oder es verschwindet identisch. Damit ist auch Satz A.6(iii) bewiesen, da dort durch die Interpolationsbedingung $n + 1$ unterschiedliche Nullstellen verlangt werden.

Folgerung
Ein Polynom $a(x)$ kann also nur irreduzibel sein, wenn $deg(a(x)) = 1$ gilt. Damit ist $a(x)$ also selbst ein Linearfaktor oder besitzt keine Nullstellen im Koeffizientenkörper.

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

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

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 Multiplikatonen ausgewertet werden.

Beispiel A.2. $x^3 - 1$ hat genau eine Nullstelle $x_o = 1$ in $\mathcal{R} = \mathbb{R}$, da nach Abspaltung des Linearfaktors $(x - 1)$ das Polynom

$$x^2 + x + 1 = (x + \tfrac{1}{2})^2 + \tfrac{3}{4} \geq \tfrac{3}{4}$$

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 nichtkonstantens 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.
Mit anderen Worten:

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

Bemerkung:
Erweitert man $\mathbb{R}$ zu den komplexen Zahlen $\mathbb{C}$, so haben auch diese quadratische Polynome 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**.

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

14 Die komplexen Zahlen

Definition A.1 (Komplexe Zahlen).

1. Die beiden Wurzeln des Polynoms

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

(und damit die Lösungen der Gleichung $x^2 + 1 = 0$) werden mit $\mathbf{i}$ und $-\mathbf{i}$ bezeichnet, es gilt also

$$\mathbf{i^2 = -1}.$$

2. Ausdrücke der Form $z = x + iy$ mit $(x, y) \in \mathbb{R}^2$ nennt man **komplexe Zahlen** mit

$Re(z) = x$ **Realteil**

$Im(z) = y$ **Imaginärteil**

3. Die Menge der komplexen Zahlen wird mit $\mathbb{C}$ bezeichnet.

Definition A.2 (Addition und Multiplikation in $\mathbb{C}$). Für Addition und Multiplikation zweier komplexer Zahlen $z_1 = x_1 + iy_1$ und $z_2 = x_2 + iy_2$ gilt

$$\begin{aligned} z_1 + z_2 &= (x_1 + x_2) + i(y_1 + y_2) \\ z_1 * z_2 &= (x_1 * x_2 - y_1 * y_2) + i(x_1 * y_2 + x_2 * y_1) \end{aligned}$$

Lemma A.3 (Körpereigenschaft von $\mathbb{C}$). *Bezüglich der oben definierten Verknüpfungen $+$ und $*$ bildet $\mathbb{C}$ einen kommutativen Körper mit folgenden Eigenschaften:*

1. $0 = 0 + i * 0$ ***Nullelement***
2. $1 = 1 + i * 0$ ***Einselement***
3. $-(x + iy) = -x + i(-y)$ ***Inverses bzgl. +***
4. $(x + iy)^{-1} = (x - iy)/(x^2 + y^2)$, ***Inverses bzgl. ∗***
   wobei z^{-1} nur für $z \neq 0$ existiert.

Lemma A.4 (Lösung einer quadratischen Gleichung). *Das Polynom*

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

hat im Falle $\gamma\alpha > \frac{1}{4}\beta^2$ die komplexen Wurzeln

$$x_{0,1} = -\frac{1}{2}\frac{\beta}{\alpha}\left[1 \pm i\sqrt{4\alpha\gamma/\beta^2 - 1}\right]$$

Beispiel A.5.

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

$$x_{0,1} = -\frac{1}{2}\left[1 \pm i\sqrt{3}\right]$$

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

$$\begin{aligned} x_0^2 + x_0 + 1 &= (\tfrac{1}{4} - \tfrac{i}{2}\sqrt{3} + i^2\tfrac{3}{4}) - \tfrac{1}{2} + \tfrac{i}{2}\sqrt{3} + 1 \\ &= \tfrac{1}{4} - \tfrac{i}{2}\sqrt{3} - \tfrac{3}{4} - \tfrac{1}{2} + \tfrac{i}{2}\sqrt{3} + 1 \\ &= \underbrace{-\tfrac{i}{2}\sqrt{3} + \tfrac{i}{2}\sqrt{3}}_{=0} + \underbrace{\tfrac{1}{4} - \tfrac{3}{4} - \tfrac{1}{2} + 1}_{=0} \\ \textbf{Also:} \quad x_0^2 + x_0 + 1 &= \mathbf{0} \end{aligned}$$

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

$$x_1^2 + x_1 + 1 = \underbrace{\tfrac{i}{2}\sqrt{3} - \tfrac{i}{2}\sqrt{3}}_{=0} + \underbrace{\tfrac{1}{4} - \tfrac{3}{4} - \tfrac{1}{2} + 1}_{=0} = \mathbf{0}$$

Definition A.6. Betrachtet man $z = x + iy$ als Vektor in der Ebene mit den Koordinaten $(x, y) \in \mathbb{R}^2$, so ergibt sich

1. als Länge des Vektors der **Betrag** der komplexen Zahl z

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

2. durch Spiegelung an der Horizontalen die **konjugiert komplexe Zahl** von z

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

3. als Winkel zur Horizontalen des **Arguments**

$$arg(z) = \arctan(y, x) \in (-\pi, \pi)\,,$$

so dass $x = r\cos(\varphi)$ und $y = r\sin(\varphi)$.

Häufige Bezeichnung:

$$r = |z| \qquad \varphi = \arg(z)$$

Bemerkung
Alle Gleichungen aus dem Reellen gelten auch im Komplexen. Nur Ungleichungen, die Beträge enthalten, machen auch im Komplexen Sinn.

Lemma A.7. *In $\mathbb{C}$ gilt*

1. $z = |z|(\cos\varphi + i\sin\varphi) \qquad$ *für* $\quad \varphi = \arg(z)$
2. $Re(z) = \frac{1}{2}(z + \bar{z}), \qquad Im(z) = \frac{1}{2\mathrm{i}}(z - \bar{z})$
3. $|z|^2 = \bar{z} * z, \qquad z^{-1} = \bar{z}/|z|^2$
4. $\arg(z) = -\arg(\bar{z})$
5. $|z_1 + z_2| \leq |z_1| + |z_2|$ ***Dreiecksungleichung***
6. $|z_1 * z_2| = |z_1| * |z_2|$ $\arg(z_1 * z_2) = \arg(z_1) + \arg(z_2) \pm 2\pi k$
7. $|z_1/z_2| = |z_1|/|z_2|$ $\arg(z_1/z_2) = \arg(z_1) - \arg(z_2) \pm 2\pi k$

Erläuterung
Aus (ii) folgt, dass die Zahl $z \in \mathbb{C}$ genau dann zum Unterkörper der reellen Zahlen $\mathbb{R} \subset \mathbb{C}$ gehört, wenn sie mit ihrer konjugiert komplexen $\bar{z}$ übereinstimmt.
Entsprechend gilt $z = -\bar{z}$ genau dann wenn z rein imaginär, also gleich $i\,Im(z)$ ist.
Aussagen (iv) und (v) lassen sich so interpretieren, dass $|\cdot|$ und arg Gruppenhomomorphismen von $\mathbb{C} \setminus \{0\}$ bzw. $\mathbb{C}$ in die multiplikative Gruppe $\mathbb{R}_+$ bzw. die additive Gruppe $\mathbb{R}/(2\pi\mathbb{R})$ sind.

Lemma A.8.

1. *Konjugierung ist ein Körperhomomorphismus auf $\mathbb{C}$, d.h. es gilt für alle $z_1, z_2 \in \mathbb{C}$ dass*

$$\overline{z_1 \pm z_2} \;=\; \overline{z_1} \pm \overline{z_2} \qquad \overline{z_1 * z_2} \;=\; \overline{z_1} * \overline{z_2} \qquad \overline{z_1/z_2} \;=\; \overline{z_1}/\overline{z_2}\,.$$

2. *Daraus folgt durch Induktion dass für jedes komplexe Polynom $P(z) \in \mathbb{C}[z]$*

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

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

Korollar A.9. *Aus obigen Lemma folgt, dass für ein Polynom $P(z) \in \mathbb{R}[z]$ die Wurzeln jeweils in konjugiert komplexen Paaren auftreten, d.h.*

$$P(z) \;=\; 0 \quad \Leftrightarrow \quad P(\overline{z}) \;=\; 0$$

Diese Eigenschaft ist umgekehrt für ein beliebiges komplexes Polynom $P(z) \in \mathbb{C}[z]$ mit mindestens einem reellen Koeffizienten $p_i \in \mathbb{R}$, $i \in \{1, \ldots, n\}$, 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 vorrübergehend ins Komplexe geht. Dies gilt zum Beispiel für charakteristische Polynom in der linearen Algebra.

Eulers Formel und Einheitswurzeln
Ein weiterer Ausflug ins Komplexe wird notwendig, wenn man ein Polynom $P(z)$ wirklich sehr schnell und genau an $n = deg(P(x)) + 1$ geigneten Stützstellen z_j auswerten will. Dazu wählt man dann

$$z_j \;=\; cos(j \,*\, 2\pi/n) + i\, sin(j \,*\, 2\pi/n)$$

Da nach der sogenannten Eulerschen Formel für $\varphi = arg(z)$, $r = |z|$ und $k \in \mathbb{N}$

$$z^k \;=\; |z|^k [cos(k\varphi) + i\, sin(k\varphi)]$$

sind die obigen z_j für $j = 1 \ldots n$ genau die n Wurzeln des Polynomes $P_n(z) = z^n - 1$.
Vorrausgesetzt $n = 2 * m$, dann ergibt sich für $j = 1, \ldots m$ durch Quadratbildung

$$z_j^2 \;=\; cos(2j \,*\, 2\pi/n) + i\, sin(2j \,*\, 2\pi/n) = cos(j\, 2\pi/m) + i\, sin(j * 2\pi/m) \;=\; z_{j+m}^2$$

Es gibt also nur m unterschiedliche Werte von z_j^2 für $j = 1, \ldots n$, welche genau die Wurzeln von $P_m(x) = x^m - 1$ sind.

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 Kommunitativität 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

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 (Vektorraum $\mathcal{V}$ bzw. linearer Raum). Zwei Vektoren $\mathbf{u}, \mathbf{v} \in \mathcal{V}$ werden addiert und ergeben dabei einen neuen Vektor $\mathbf{w} \in \mathcal{V}$:

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

Die Addition muß so definiert sein, daß für beliebige $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{V}$ gilt:

- $(\mathbf{u} + \mathbf{v}) + \mathbf{w} \;=\; \mathbf{u} + (\mathbf{v} + \mathbf{w})$ **Assoziativität**
- $\mathbf{u} + \mathbf{v} \;=\; \mathbf{v} + \mathbf{u}$ **Kommutativität**
- $\mathbf{u} + \mathbf{0} \;=\; \mathbf{u}$ **Neutrales Element**
- $\mathbf{u} + (-\mathbf{u}) \;=\; \mathbf{0}$ **Inverses Element**

Weiterhin muß für die Multiplikation von Vektoren mit beliebigen Skalaren $\lambda, \gamma \in \mathbb{R}$ gelten:

- $\lambda(\gamma\mathbf{u}) \;=\; (\lambda\gamma)\mathbf{u}$
- $1\,\mathbf{u} = \mathbf{u}$
- $\lambda(\mathbf{u} + \mathbf{v}) \;=\; \lambda\mathbf{u} + \lambda\mathbf{v}$
- $(\lambda + \gamma)\mathbf{u} \;=\; \lambda\mathbf{u} + \gamma\mathbf{u}$

Beispiel: Euklidischer Raum
Für beliebiges aber festes n kann man geordnete Mengen von jeweils n reellen Zahlen ν_i für $i = 1 \ldots n$ als Vektoren $\mathbf{v}$ definieren. Man schreibt dann

$$\mathbf{v} \;=\; (\nu_1, \nu_2, \ldots \nu_n)^T \quad \text{oder} \quad \mathbf{v} \;=\; (\nu_i)_{i=1}^n\,.$$

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

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

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

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

Beispiel: Formale Potenzreihen
Für $x_0 = 0$ oder sonst einen gemeinsamen Entwicklungspunkt bilden die Potenzreihen

$$\mathbf{u} \;=\; \sum_{i=0}^{\infty} \mu_i x^i, \quad \mathbf{v} \;=\; \sum_{i=0}^{\infty} \nu_i x^i,$$

einen reellen Vektorraum bezüglich der Operationen

$$\mathbf{u} + \mathbf{v} \;=\; \sum_{i=0}^{\infty} (\mu_i + \nu_i) x^i, \quad \gamma\mathbf{v} \;=\; \sum_{i=0}^{\infty} (\gamma\nu_i) x^i\,.$$

Wenn die Potenzreihen für bestimmte Werte von x konvergieren, so entsprechen Addition und Multiplikation der analogen Operationen auf den Summenwerten, die man dann als Funktionen von x interpretieren kann. Das ist aber für die Vektorraumeigenschaft nicht nötig, weshalb man auch vom Raum der formalen Potenzreihen spricht.

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

Problem B.2. *Gegeben seien eine Familie von r Vektoren $\mathbf{v}_i (i = 1, \ldots, r)$ und ein spezieller Vektor $\mathbf{v}$ aus einem gemeinsamen Vektorraum $\mathcal{V}$.*
Gibt es nun eine Familie von Skalaren $\lambda_i (i = 1, \ldots, r)$, so daß

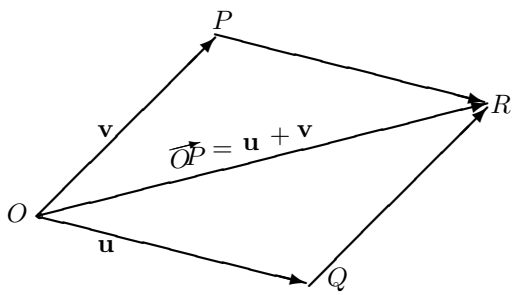
$$\mathbf{v} \;=\; \lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \ldots + \lambda_r \mathbf{v}_r \;=\; \sum_{i=1}^{r} \lambda_i \mathbf{v}_i$$

gilt, und wenn ja, wie kann man geeignete Koeffizienten λ_i möglicherweise eindeutig berechnen.

Unter anderem lassen sich Fragen nach Basisdarstellungen sowie die Suche nach den Lösungen linearer Gleichungen in dieser Art formulieren.

2 Vektoren im Anschauungsraum

Für $\mathbf{v} = \overrightarrow{OP}$ und $\mathbf{u} = \overrightarrow{OQ}$ ergibt sich $\mathbf{w} = \mathbf{u}+\mathbf{v}$ als $\mathbf{w} = \overrightarrow{OR}$, wobei der Vektor $\mathbf{v}$, wenn man seinen Anfang in den Punkt Q legt, mit seiner Spitze den Punkt R erreicht. Umgekehrt kann man auch zu R gelangen, indem man $\mathbf{u}$ an der Spitze von $\mathbf{v}$ ansetzt. Diese Beliebigkeit in der Reihenfolge der Ausführung 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

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

Inbesondere erhält man die **Basisvektoren** selbst als

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

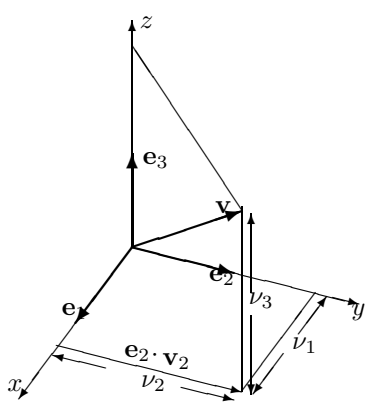
Addition, Subtraktion und Multiplikation erfolgen nun komponentenweise, z.B. für

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

ergibt sich

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

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



2.1 Länge und Richtungskosinus

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

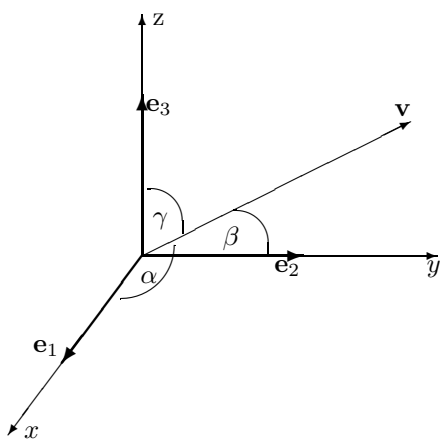
Definition B.1 (Länge eines Vektors, Euklidische Norm).
Der Vektor $\mathbf{v} = (\nu_1, \nu_2, \nu_3)$ hat die **Länge**

$$|\mathbf{v}| \;=\; \left(\nu_1^2 + \nu_2^2 + \nu_3^2\right)^{\frac{1}{2}} \;.$$

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 Kosinusse von drei Winkeln $\alpha, \beta, \gamma \in [0, \pi]$ dargestellt werden können. Es gilt also

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



Wie aus der Zeichnung ersichtlich ist, bilden α, β und γ 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.

2.2 Skalar- oder inneres Produkt

Definition B.2 (Skalar- oder inneres Produkt). Für zwei beliebige Vektoren $\mathbf{u} = (\mu_1, \mu_2, \mu_3)^T$ und $\mathbf{v} = (\nu_1, \nu_2, \nu_3)^T$ nennt man den Skalar

$$\mathbf{u} \cdot \mathbf{v} \;=\; \mu_1\nu_1 + \mu_2\nu_2 + \mu_3\nu_3$$

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

Lemma B.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:*

$$\begin{array}{lcr}
\mathbf{v} \cdot \mathbf{u} & = & \mathbf{u} \cdot \mathbf{v} \\
\lambda(\mathbf{u} \cdot \mathbf{v}) & = & (\lambda\mathbf{u}) \cdot \mathbf{v} \;=\; \mathbf{u} \cdot (\lambda\mathbf{v}) \\
\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) & = & \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w} \\
\mathbf{u} \cdot \mathbf{u} & = & |\mathbf{u}|^2 \geq 0
\end{array}$$

Interpretation inneres Produkt im Anschauungsraum
Man betrachte das Dreieck mit den Kanten $\mathbf{u}, \mathbf{v}$ und $\mathbf{u} - \mathbf{v}$, deren Längen nach dem Kosinussatz die Gleichung

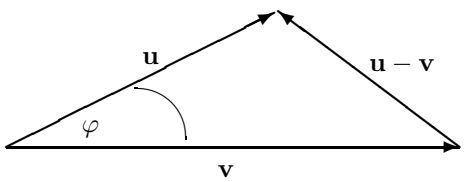
$$|\mathbf{u} - \mathbf{v}|^2 = |\mathbf{u}|^2 + |\mathbf{v}|^2 - 2|\mathbf{u}||\mathbf{v}|\cos(\varphi)$$

erfüllen. Hierbei ist φ der von $\mathbf{u}$ und $\mathbf{v}$ eingeschlossene Winkel. Andererseits gilt für $|\mathbf{u}-\mathbf{v}|^2$ nach den oben aufgeführten Regeln

$$\begin{aligned} |\mathbf{u}-\mathbf{v}|^2 &= (\mathbf{u}-\mathbf{v})\cdot(\mathbf{u}-\mathbf{v}) \\ &= (\mathbf{u}-\mathbf{v})\cdot\mathbf{u}+(\mathbf{u}-\mathbf{v})\cdot(-1\mathbf{v}) \\ &= \mathbf{u}\cdot\mathbf{u}-\mathbf{v}\cdot\mathbf{u}-\mathbf{u}\cdot\mathbf{v}+\mathbf{v}\cdot\mathbf{v} \\ &= |\mathbf{u}|^2+|\mathbf{v}|^2-2\mathbf{u}\cdot\mathbf{v}\ . \end{aligned}$$

Vergleicht man nun die beiden rechten Seiten, so folgt für φ notwendigerweise

$$\cos(\varphi) \;=\; \frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|} \in [-1,1]\ .$$



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

Auch ohne diese Voraussetzung folgt aus $|\cos(\varphi)| \leq 1$ die sogenannte

Lemma B.4 (Schwarzsche Ungleichung).

$$|\mathbf{u}\cdot\mathbf{v}| \;\leq\; |\mathbf{u}||\mathbf{v}|$$

Bemerkung:
Die beiden Seiten sind nur dann genau gleich, wenn $\mathbf{v}=\lambda\mathbf{u}$ oder $\mathbf{u}=\lambda\mathbf{v}$ sind für ein λ, das auch Null sein kann.

Definition B.5 (Orthogonale Vektoren). Man bezeichnet zwei Vektoren u und $\mathbf{v}$ als orthogonal zueinander, wenn der von ihnen eingeschlossene Winkel $\pi/2$ ist, oder wenn einer von ihnen verschwindet, d.h. gleich Null ist. Formelmäßig schreibt man

$$\mathbf{u}\perp\mathbf{v}\ , \quad \text{falls} \quad \mathbf{u}\cdot\mathbf{v} \;=\; 0 \quad .$$

Beispiel B.6. Die Einheitsvektoren $\mathbf{e}_i$ bilden ein Orthogonalsystem in dem Sinne, daß

$$\mathbf{e}_i\cdot\mathbf{e}_j \;=\; 0 \quad \text{falls} \quad i\neq j \quad .$$

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

2.3 Vektor- oder Kreuzprodukt

Dieses Produkt ist nur im dreidimensionalen Anschauungsraum eindeutig definiert.

Definition B.7 (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.

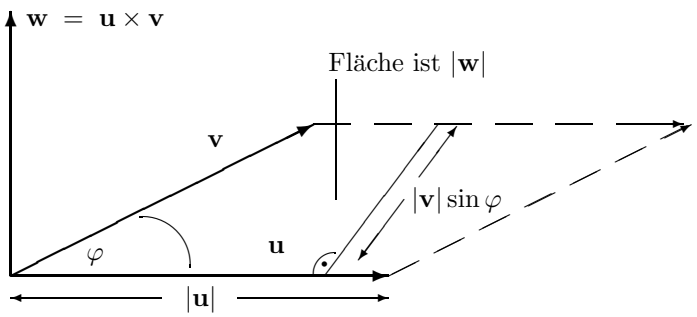
Es soll also gelten:

$$\begin{aligned} |\mathbf{w}| &= |\mathbf{u}||\mathbf{v}||\sin(\varphi)| \\ &= |\mathbf{u}||\mathbf{v}|\left(1-\cos^2(\varphi)\right)^{\frac{1}{2}} \\ &= \left[|\mathbf{u}|^2\,|\mathbf{v}|^2-(\mathbf{u}\cdot\mathbf{v})^2\right]^{\frac{1}{2}}\ . \end{aligned}$$

Bemerkung:
Man beachte, daß auf der letzten rechten Seite der Ausdruck unter der Wurzel nach der Schwarzschen Ungleichung im allgemeinen nicht negativ sein kann.

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:

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



Lemma B.8 (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.9 (Bilinearität). *Für beliebige Vektoren* $\mathbf{u}, \mathbf{v}, \mathbf{w}$ *und Skalare* λ *gilt:*

$$\begin{aligned} \mathbf{u} \times (\mathbf{v} + \mathbf{w}) &= \mathbf{u} \times \mathbf{v} + \mathbf{u} \times \mathbf{w} \\ (\mathbf{u} + \mathbf{v}) \times \mathbf{w} &= \mathbf{u} \times \mathbf{w} + \mathbf{v} \times \mathbf{w} \\ \lambda(\mathbf{u} \times \mathbf{v}) &= (\lambda \mathbf{u}) \times \mathbf{v} \;=\; \mathbf{u} \times (\lambda \mathbf{v}) \;=\; -\lambda(\mathbf{v} \times \mathbf{u}) \end{aligned}$$

Damit ergibt sich
Lemma B.10 (Komponentenweise Berechnungsvorschrift).

$$(\mu_1, \mu_2, \mu_3)^T \times (\nu_1, \nu_2, \nu_3)^T \;=\; (\mu_2\nu_3 - \mu_3\nu_2, \nu_1\mu_3 - \nu_3\mu_1, \mu_1\nu_2 - \mu_2\nu_1)^T$$

Diese Regel merkt man sich am besten indem man sie als die Determinante einer (3×3) Matrix interpretiert. Und zwar gilt

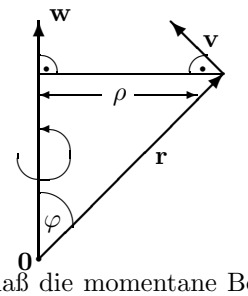
$$\mathbf{u} \times \mathbf{v} \;=\; \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix} .$$

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. Regeln für das Berechnen von Determinanten werden ii einem der nächsten Abschnitte behandelt.

Eine wichtige Anwendung des Kreuzproduktes in der Mechanik ist die **Drehung eines Körpers um eine feste Achse mit der konstanten Winkelgeschwindigkeit** ω. 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 ω mal dem Abstand von der Achse,also $|\mathbf{r}|\sin(\phi)$, ist.
Hierbei ist φ 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.

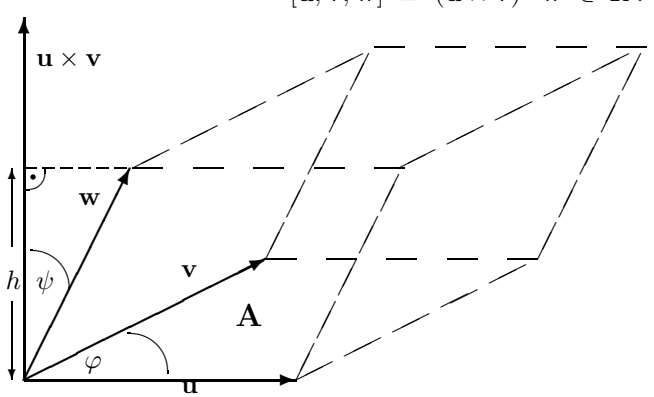
$$\mathbf{w} \cdot \mathbf{v} \;=\; 0 \;=\; \mathbf{r} \cdot \mathbf{v}$$

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

2.4 Spatprodukt

Definition B.11 (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.12 (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.13. *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.14 (Vorzeichen Spatprodukt).
Für das ***Vorzeichen*** *gilt die folgende Regel:*

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

Hierbei bezeichnet der Begriff ***linear abhängig*** *den Zustand, daß die drei Vektoren in einer Ebene liegen und es deshalb nicht triviale Koeffizienten α, β, γ gibt, für die*

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

Lemma B.15 (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.*

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' bei einander liegen.

Definition B.1 (Norm und normierter Raum). Ein linearer Vektorraum $\mathcal{V}$ heisst **normiert**, wenn es zu jedem $\mathbf{u} \in \mathcal{V}$ eine reele Zahl $\|\mathbf{u}\|$ gibt, so dass für beliebige $\lambda \in \mathbb{R}$ und $\mathbf{v} \in \mathcal{V}$ gilt:

- $\|\mathbf{u}\| \geq 0 \quad \text{mit} \quad \|\mathbf{u}\| = 0 \Leftrightarrow \mathbf{u} = 0$ **Definitheit**
- $\|\lambda\,\mathbf{u}\| \;=\; |\lambda|\|\mathbf{u}\|$ **Homogenität**
- $\|\mathbf{u}+\mathbf{v}\| \;\leq\; \|\mathbf{u}\| + \|\mathbf{v}\|$ **Dreiecksungleichung**

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

Aus der (Cauchy-)Schwarz-Ungleichung folgt unmittelbar die Dreiecksungleichung, da

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

Auch die Homogenität ist gewährleistet, da

$$\|\lambda\mathbf{u}\| = \sqrt{\lambda\mathbf{u}\cdot\lambda\mathbf{u}} \;=\; |\lambda|\sqrt{\mathbf{u}\cdot\mathbf{u}}$$

Also haben die sogenannten **Hilbert-Normen** $\|\mathbf{u}\| = \sqrt{\mathbf{u} * \mathbf{u}}$ in der Tat die verlangten Normeigenschaften.
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

$$\|\mathbf{v}\|_p \;=\; \|(\nu_1, \nu_2, \ldots \nu_n)^T\|_p \;=\; [|\nu_1|^p + |\nu_2|^p + \ldots |\nu_n|^p]^{1/p}$$

- Für $p = 2$ erhält man wiederum die Euklidische Norm $\|\mathbf{v}\|_2 = \|\mathbf{v}\|$. Im Grenzfall $p = \infty$ setzt man

$$\|\mathbf{v}\|_\infty \;=\; \|(\nu_1, \nu_2, \ldots \nu_n)^T\|_\infty \;=\; \max\{|\nu_1|, |\nu_2|, \ldots |\nu_n|\}$$

- 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.2 (Weitere Normeigenschaften).

- *Per Induktion ergibt sich für die* ***Summe*** *endlich vieler Vektoren $v_i, i = 1 \ldots m$, die Ungleichung*

$$\left\|\sum_{i=1}^{m} \nu_i\right\| \;\leq\; \sum_{i=1}^{m} \|\nu_i\|$$

- *Aus der Dreiecksungleichung folgt für alle Normen die sogenannte* ***umgekehrte Dreiecksungleichung***

$$\|\mathbf{u}-\mathbf{v}\| \;\geq\; |\|\mathbf{u}\|-\|\mathbf{v}\||$$

- *Eine Norm* $\|\mathbf{v}\|$ *ist genau dann eine Hilbert-Norm, wenn sie die folgende sogenannte* ***Parallelogrammgleichung*** *erfüllt*

$$\|\mathbf{u}-\mathbf{v}\|^2+\|\mathbf{u}+\mathbf{v}\|^2 \quad = \quad 2(\|\mathbf{u}\|^2+\|\mathbf{v}\|^2)$$

Bemerkung:
Im letzteren Fall lässt sich die Identität

$$\mathbf{u}\cdot\mathbf{v} \;=\; \tfrac{1}{4}\left[\|\mathbf{u}+\mathbf{v}\|^2-\|\mathbf{u}-\mathbf{v}\|^2\right]$$

auch als Definition des Inneren Produktes interpretieren.

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.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 λ_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

$$\sum_{i=1}^n \lambda_i \mathbf{v}_i \;=\; \mathbf{0} \quad \Rightarrow \quad \sum_{i=1}^n |\lambda_i| \;=\; 0\,.$$

Folgerung B.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.3. *Zwei Vektoren $\mathbf{v}_1, \mathbf{v}_2$ sind genau dann linear abhängig, wenn sie parallel sind, da*

$$\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 \;=\; \mathbf{0}\,,\; \lambda_1 \neq 0 \quad \Longrightarrow \quad \mathbf{v}_1 = -(\lambda_2/\lambda_1)\mathbf{v}_2\,.$$

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. *Zwei nicht verschwindende, zueinander orthogonale Vektoren $\mathbf{v}_1 \perp \mathbf{v}_2$ sind auf jeden Fall linear unabhängig.*

Beweisidee:
Um dies zu zeigen, bilde 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

$$\lambda_1 \mathbf{v}_1 \cdot \mathbf{v}_1 + \lambda_2 \mathbf{v}_1 \cdot \mathbf{v}_2 = 0 = \lambda_1 |\mathbf{v}_1|^2$$

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 $\mathbf{v}_2$. □

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 $\mathbf{v}_i \cdot \mathbf{v}_j = 0$, $v_i \neq \mathbf{0}$, für $i \neq j$ durchführen. Deshalb sollte man Orthogonalität als eine besonders starke Form linearer Unabhängigkeit betrachten.

Folgerung B.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.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 **unendlich dimensional** und setzt $\dim(\mathcal{V}) = \infty$.

Beispiel B.7. Der Raum aller Polynome ist unendlich dimensional, da die Familie von sogenannten Monomen (reinen Potenzen)

$$x^j \qquad j = 0, 1, \ldots, n$$

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.8 (Eindeutige Koeffizientendarstellung). *Sei $\{v_i\}_{i=1\ldots m}$ eine Familie linear unabhängiger Vektoren irgendeines linearen Raumes $\mathcal{V}$. Dann besitzt jeder Vektor $v \in \mathcal{V}$, der zusammen mit den $\{v_i\}_{i=1\ldots m}$ keine linear unabhängige Menge bildet, eine eindeutige Darstellung*

$$\mathbf{v} = \sum_{i=1}^{m} \lambda_i * \mathbf{v}_i$$

Hierbei verschwinden alle λ_i genau dann wenn $\mathbf{v} = 0$.

Lemma B.9 (Austauschsatz). *Sei $\{v_i\}_{i=1\ldots m}$ eine Familie linear unabhängiger Vektoren irgendeines linearen Raumes $\mathcal{V}$.*
Dann gilt für jeden nichtverschwindenden Vektor $v \neq 0$
entweder

- *Die Vereinigung $\{v_i\}_{i=1\ldots m+1}$ ist mit $v_{m+1} \equiv v$ auch linear unabhängig.*

oder

- *Es gibt einen Index $j \leq m$, so dass $\{v_i\}_{i=1\ldots m}$, mit v_j durch 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.10 (Eindeutigkeit der Dimension). *Seien $\{v_i\}_{i=1\ldots m}$ und $\{w_i\}_{i=1\ldots n}$ 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

$$\sum_{i=1}^{n} \alpha_i v_i \;=\; u \;=\; \sum_{i=1}^{n} \beta_i w_i \;.$$

4.1 Unterräume und Linearkombinationen

Gerade in unendlich dimensionalen Räumen muß man oft praktische Untersuchungen auf einen endlich dimensionalen Unterraum beschränken (z.B. indem man den Grad von Polynomen mehr oder minder willkürlich beschränkt).

Definition B.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 $\mathbf{u}, \mathbf{v} \in \mathcal{V}$ und $\lambda \in \mathbb{R}$ die Implikation

$$\mathbf{u}, \mathbf{v} \in \mathcal{U} \qquad \Longrightarrow \qquad \mathbf{u} + \mathbf{v} \in \mathcal{U}, \quad \lambda \mathbf{u} \in \mathcal{U} \;.$$

Beispiel B.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.13 *(Orthogonales Komplement).* Ein interessanteres Beispiel ist das **orthogonale Komplement**

$$v^{\perp} \equiv \mathcal{U} = \{\mathbf{u} \in \mathcal{V} \mid \mathbf{v} \cdot \mathbf{u} = 0\}$$

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 $\lambda \in \mathbb{R}$

$$\mathbf{v} \cdot \mathbf{u} = 0 = \mathbf{v} \cdot \mathbf{w} \qquad \Rightarrow \qquad \mathbf{v} \cdot (\mathbf{u} + \mathbf{w}) = 0 = \mathbf{v} \cdot (\lambda \mathbf{u}) \ .$$

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.14 (Schnittprinzip, siehe auch Lemma A.2). *Für zwei Unterräume $\mathcal{U}, \mathcal{W} \subset \mathcal{V}$ bildet deren Durchschnitt*

$$\mathcal{U} \cap \mathcal{W} \equiv \{\mathbf{v} \in \mathcal{V} \mid \mathbf{v} \in \mathcal{U},\ \mathbf{v} \in \mathcal{W}\}$$

einen Unterraum.

Satz B.15. *Der Schnitt mehrerer und sogar unendlich vieler Unterräume bildet einen Unterraum.*

Beispiel B.16. Für eine beliebige Menge von Vektoren $\mathcal{M} \subset \mathcal{V}$ ergibt sich das orthogonale Komplement als

$$\mathcal{M}^{\perp} \equiv \bigcap_{\mathbf{v} \in \mathcal{M}} \mathbf{v}^{\perp} \quad = \quad \{\mathbf{u} \in \mathcal{V} \mid \mathbf{v} \in \mathcal{M} \Rightarrow \mathbf{u} \cdot \mathbf{v} = 0\} \ .$$

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:

$$\mathcal{U} + \mathcal{W} = \{\mathbf{u} + \mathbf{w} | \mathbf{u} \in \mathcal{U}, \mathbf{w} \in \mathcal{W}\} \ .$$

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.17 (Linearkombination der Vektoren). Für eine Familie $\{\mathbf{v}_i\}_{i=1}^r \subset \mathcal{V}$ bezeichnet man jeden Vektor der Form

$$\mathbf{v} = \sum_{i=1}^{r} \lambda_i \mathbf{v}_i$$

als eine **Linearkombination der Vektoren** $\mathbf{v}_i$.

Definition B.18 (Lineare Hülle, vergleiche A.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**

$$\mathbf{span}(\mathcal{U}) \quad = \quad \left\{ \mathbf{v} = \sum\nolimits_{i=1}^{r} \lambda_i \mathbf{v}_i \ \middle|\ \lambda_i \in \mathbb{R}, v_i \in \mathcal{U} \right\} \ .$$

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.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.20. *Aus der vorausgesetzten linearen Unabhängigkeit folgt die Eindeutigkeit der Darstellung eines beliebigen Vektors* $\mathbf{v}$ *als Linearkombination.*

Lemma B.21. *Bezüglich einer bestimmten Basis $\{\mathbf{v}_i\}_{i=1}^r$ hat jeder Vektor $\mathbf{v} \in \mathcal{V}$ eine eindeutige Darstellung*

$$\mathbf{v} \;=\; \sum_{i=1}^{r} \lambda_i \mathbf{v}_i$$

Beweis. Aus

$$\sum_{i=1}^{r} \lambda_i \mathbf{v}_i \;=\; \mathbf{v} \;=\; \sum_{i=1}^{r} \gamma_i \mathbf{v}_i$$

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 $\mathbf{v}$ bezüglich der gewählten Basis eindeutig bestimmt. □

Beispiel B.22. Es sei

$$\mathcal{P}_n \;\equiv\; \left\{ \sum\nolimits_{i=0}^{n-1} \gamma_i x^i \,\middle|\, \gamma_i \in \mathbb{R} \right\}$$

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.

Beweisidee:
Die lineare Unabhängigkeit zeigt man wie üblich, indem man annimmt, daß eine Linearkombination der Vektorfamilie verschwindet, d.h.

$$P(x) \;\equiv\; \sum_{i=1}^{n} \lambda_i \, \mathbf{v}_i \;=\; \sum_{i=1}^{n} \lambda_i \, x^{i-1} \;=\; 0 \;.$$

Die Null repräsentiert hierbei das Nullpolynom, daß für alle x den Wert $0 \in \mathbb{R}$ hat. Jedes $x \in \mathbb{R}$ muß also eine Nullstelle von $P(x)$ sein. Dies ist nur möglich wenn alle Koeffizienten λ_i von $P(x)$ gleich Null sind (siehe Folgerung aus Korollar A.1), da $P(x)$ sich sonst als Produkt von Linearfaktoren $x - x_j$ darstellen ließe und deshalb nur höchstens $n-1$ Nullstellen hätte. Die Monome $\{v_i = x^{i-1}\}_{i=1}^n$ bilden also eine Basis des Vektorraumes $\mathcal{P}_n$, der deshalb n-dimensional ist. □

Bemerkung:
Obwohl die monomiale Basis 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 in entsprechenden Abschnitt weiter unten behandelt wird.

Bemerkung: Orthogonalitätsbedingung, orthonormale Basis
Rechnerisch besonders angenehm sind Basen, welche die **Orthogonalitätsbedingung**

$$\mathbf{v}_i \cdot \mathbf{v}_j \;=\; \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

erfüllen. Bei solchen sogenannten **orthonormalen** Basen lassen sich die Koeffizienten λ_i eines beliebigen Vektors $\mathbf{v}$ leicht berechnen:

Aus dem Ansatz

$$\mathbf{v} \;=\; \sum_{j=1}^{n} \lambda_j \mathbf{v}_j$$

folgt durch die Bildung des inneren Produktes mit einem bestimmten Basisvektor $\mathbf{v}_i$ sofort

$$\mathbf{v}_i \cdot \mathbf{v} \;=\; \sum_{j=1}^{n} \lambda_j \, \mathbf{v}_i \cdot \mathbf{v}_j \;=\; \lambda_i \;,$$

da alle Summanden mit $j \neq i$ verschwinden.

Beispiel B.23. In einem gewissen verallgemeinerten Sinne bilden die trigonometrischen Funktionen

$$\mathbf{v}_{2i} \equiv \sin(i\,x) \quad \text{und} \quad \mathbf{v}_{2i+1} \equiv \cos(i\,x) \qquad \text{für } i = 1, 2, \ldots$$

zusammen mit der konstanten Funktion $\mathbf{v}_1 \equiv 1$ eine Basis des unendlich dimensionalen Raumes aller Funktionen $f(x)$, die auf dem Intervall $[-\pi, \pi]$ periodisch und quadratisch integrierbar sind.

Letzteres bedeutet, daß $f^2(x)$ ein endliches Integral auf $[-\pi, \pi]$ hat, was zum Beispiel dann der Fall ist, 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

$$f \cdot g = \int_{-\pi}^{\pi} f(x)g(x)dx \; .$$

Fortsetzung Beispiel
Die Orthogonalitätseigenschaften lassen sich hier mittels wiederholter partieller Integration oder mit Hilfe geeigneter trigonometrischer Umformungen leicht nachweisen. Allerdings müssen die Funktionen $\mathbf{v}_i$ noch geeignet skaliert werden, so daß dann $||\mathbf{v}_i|| = 1$ gilt. Auf jeden Fall lassen sich die Koeffizienten einer beliebigen Funktion $f(x)$ bezüglich der Basisfunktion $\sin(i\,x)$ aus dem inneren Produkt

$$\int_{-\pi}^{\pi} f(x)\sin(i\,x)dx$$

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**.

5 Lineare Abbildungen

Definition B.1 (Lineare Abbildung). Eine Abbildung $\mathbf{F} : \mathcal{V} \mapsto \mathcal{W}$ 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:

$$\mathbf{F}(\mathbf{u}+\mathbf{v}) \;=\; \mathbf{F}(\mathbf{u}) + \mathbf{F}(\mathbf{v}) \qquad \textbf{Additivität}$$

$$\mathbf{F}(\lambda\mathbf{u}) \;=\; \lambda\mathbf{F}(\mathbf{u}) \qquad \textbf{Homogenität}$$

Bemerkung
Mit anderen Worten F ist ein Vektorraumhomomorphismus im Sinne der auf Gruppen und Ringe zugeschnittenen algebraischen Definition A.62.

Folgerung
Entsprechend zum Lemma A.68 ergibt sich nun auch folgende Aussage über Null, Bild und Kern.

Lemma B.2.

1. *Jede lineare Abbildung bildet die Null von $\mathcal{V}$ in die Null von $\mathcal{W}$ ab.*
2. *Die linearen Bilder $F(\mathcal{U}) \subset \mathcal{W}$ von Unterräumen $\mathcal{U} \subset \mathcal{V}$ bilden Unterräume von $\mathcal{W}$.*
3. *Das* **Kern** *von* $\mathbf{F}$ *genannte Urbild*

$$Kern(F) \;=\; \mathbf{F}^{-1}(\mathbf{0}) \;=\; \{\mathbf{u} \in \mathcal{V} : F(\mathbf{u}) = \mathbf{0} \in \mathcal{W}\}$$

ist ein linearer Unterraum von $\mathcal{V}$. Die mit $\mathcal{V}/Kern(F)$ bezeichnete Quotientenraum von $\mathcal{W}$ bezüglich der durch den Kern definierten Äquivalenz ist isomorph zum Bild $F(\mathcal{V}) \subset \mathcal{W}$.

Lemma B.3 (Restklassen bezüglich Untergruppe). *$\mathcal{U} \subset \mathcal{V}$ linearer Unterraum impliziert, dass*

$$\mathbf{u} \sim w \quad \Longleftrightarrow \quad \mathbf{u} - \mathbf{w} \in \mathcal{U} \quad \Longleftrightarrow \quad \exists \mathbf{v} \in \mathcal{U} : \mathbf{u} = \mathbf{w} + \mathbf{v}$$

eine Äquivalenzrelation ist.

Die entspechenden Äquivalenzklassen

$$[\mathbf{u}] \quad \equiv \quad \{\mathbf{w} \in \mathcal{V} : \mathbf{w} \sim \mathbf{u}\}$$

bilden einen Vektorraum bezüglich der Operationen

$$[\mathbf{u}] + [\mathbf{w}] \;=\; [\mathbf{u}+\mathbf{w}] \quad \textit{und} \quad \lambda[\mathbf{u}] = [\lambda\mathbf{u}]\,.$$

Beispiel B.4. Betrachte $\mathcal{V} = \mathcal{W} = \mathcal{P}_n$, den Raum der Polynome mit reellen Koeffizienten vom Grad kleiner $n = \dim(\mathcal{P}_n)$ in einer Variablen x. Dann ist die **Differentiation**

$$\mathbf{w} \;=\; \mathbf{F}(\mathbf{v}) \;=\; \mathbf{v}' = d\mathbf{v}/dx$$

eine lineare Operation, deren Ergebnis wiederum ein Polynom $\mathbf{w} \in \mathcal{V}$ 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

$$\omega_i = i\,\nu_{i+1} \quad \text{für} \quad i = 1 \ldots n-1$$

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 ω_n verschwindet.

Folgerung B.5. *Wir haben dann im $n-1$ dimensionalen Bildbereich den Wertevorrat*

$$Range(\mathbf{F}) \;=\; \left\{ \sum_{i=1}^{n-1} \omega_i x^{i-1} \;\middle|\; \omega_i \in \mathbb{R} \right\} \;=\; \mathcal{P}_{n-1} \;.$$

Umgekehrt fällt der Koeffizient ν_1 der konstanten Funktion $x^0 = 1$ bei der Differentiation weg, und wir haben den eindimensionalen Kern

$$Kern(\mathbf{F}) \;=\; \{\nu_1 x^0 | \nu_1 \in \mathbb{R}\} \;=\; \mathcal{P}_1 \;.$$

Mit anderen Worten, die Differentiation bildet genau diejenigen Funktionen auf die Nullfunktion ab, die konstant sind. Wie in diesem speziellen Fall, gilt für beliebige lineare Abbildungen zwischen endlich dimensionalen Räumen

$$\dim(Range(\mathbf{F})) \;=\; \dim(Dom(\mathbf{F})) - \dim(Kern(\mathbf{F})) \;,$$

wobei $Dom(\mathbf{F}) = \mathcal{V}$ den **Definitionsbereich** von $\mathbf{F}$ bezeichnet.

Von besonderem Interesse sind Abbildungen, die **regulär** sind in dem Sinne, daß ihr Kern trivial ist, d.h. nur aus dem Nullvektor $\mathbf{0}$ besteht. Diese Voraussetzung ist äquivalent zu der Eigenschaft, daß es für jedes $\mathbf{w} \in Range(\mathbf{F})$ genau ein Urbild $\mathbf{v} \in \mathcal{V}$ gibt mit $\mathbf{w} = \mathbf{F}(\mathbf{v})$. Dieser Zusammenhang ergibt sich aus der Linearität wie folgt:

$$\mathbf{F}(\mathbf{u}) = \mathbf{F}(\mathbf{v}) \quad \Longleftrightarrow \quad \mathbf{F}(\mathbf{v}) - \mathbf{F}(\mathbf{u}) = \mathbf{F}(\mathbf{v} - \mathbf{u}) = \mathbf{0} \quad \Leftrightarrow \quad \mathbf{v} - \mathbf{u} \in Kern(\mathbf{F}) \;.$$

Mit anderen Worten: die Lösung der sogenannten **inhomogenen** Gleichung $\mathbf{F}(\mathbf{v}) = \mathbf{w}$ ist eindeutig genau dann, wenn die entsprechende **homogene** Gleichung $\mathbf{F}(\mathbf{v}) = \mathbf{0}$ nur die triviale Lösung $\mathbf{v} = \mathbf{0}$ hat. Im regulären Falle bezeichnet man die Zuordnung des Urbildes $\mathbf{v} \in \mathcal{V}$ zum gegebenen Bilde $\mathbf{w} = \mathbf{F}(\mathbf{v}) \in \mathcal{W}$ als die Umkehrabbildung oder die inverse Abbildung

$$\mathbf{F}^{-1} \;:\; Range(\mathbf{F}) \mapsto Dom(\mathbf{F}) \;.$$

Falls sie überhaupt existiert, ist die Inverse einer linearen Abbildung auch immer linear, d.h. es gilt für $\mathbf{v}, \mathbf{w} \in W$

$$\begin{aligned} \mathbf{F}^{-1}(\mathbf{v} + \mathbf{w}) &= \mathbf{F}^{-1}(\mathbf{v}) + \mathbf{F}^{-1}(\mathbf{w}) \\ \mathbf{F}^{-1}(\lambda \mathbf{w}) &= \lambda \mathbf{F}^{-1}(\mathbf{w}) \;. \end{aligned}$$

Das Auffinden von $\mathbf{v} = \mathbf{F}^{-1}(\mathbf{w})$ für gegebenes $\mathbf{w}$ bezeichnet man auch als **Lösen** der Vektorgleichung $\mathbf{F}(\mathbf{v}) = \mathbf{w}$. Im Gegensatz zu skalaren Gleichungen bezeichnet man Vektorgleichungen auch als Gleichungssysteme, vor allem wenn sie bezüglich geeigneter Basen komponentenweise dargestellt werden können.

Die effektive und genaue Lösung von linearen Gleichungssystemen bei gleichzeitiger Untersuchung ihrer Regularität ist nach wie vor eine zentrale Aufgabe im sogenannten 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 die Anwendung sehr wichtige Aufgabe ist die Lösung sogenannter Eigenwertprobleme, d.h. die Berechnung von aus einem Vektor $\mathbf{v}$ und einem Skalar λ bestehenden Paaren 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 λ einen **Eigenwert** und $\mathbf{v}$ einen **Eigenvektor** der linearen Abbildung $\mathbf{F}$. Die Lösung des Eigenwertproblems wird dadurch erschwert, daß die Eigenwerte und -vektoren oft komplex sind und $\mathbf{F}$ deswegen auf einer komplexen Erweiterung von $\mathcal{V}$ definiert werden muß.
Die praktische Lösung von linearen Gleichungen und Eigenwertproblemen verlangt die komponentenweise Darstellung linearer Abbildungen mittels Matrizen genannter Felder von Skalaren.

6 Basistransformation

Umrechnung eines Vektors auf eine neue Basis

6.1 Ausgangspunkt

Gegeben sei eine Basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} = \{\mathbf{v}_i\}_{i=1\ldots n}$ des linearen Vektorraumes $\mathcal{V}$. Mittels des *Gram-Schmidtschen* - Orthogonali- sierungsverfahrens sei eine neue **orthonormale Basis** $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\} = \{\mathbf{b}_i\}_{i=1\ldots n}$ erzeugt worden. Die dabei erzeugten Zwischengrössen $\tilde{\mathbf{b}}_i$, $i = 1 \ldots n$, und α_{ij}, $i = 1 \ldots n$, $j = 1 \ldots (i-1)$, seien verfügbar.

6.2 Ziel

Es soll eine Formel ermittelt werden, mit deren Hilfe jeder bezüglich der Basis $\{\mathbf{v}_i\}_{i=1\ldots n}$ gegebene Vektor $u_{[\mathbf{v}]} \in \mathcal{V}$ in eine Darstellung $u_{[\mathbf{b}]}$ bezüglich der Basis $\{\mathbf{b}_i\}_{i=1\ldots n}$ umgewandelt werden kann.

6.3 Verfahren

Der Ansatz des *Gram-Schmidtschen*-Orthogonalisierungsverfahrens

$$\tilde{\mathbf{b}}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j \qquad\qquad i = 1, \ldots, n$$

kann nach $\mathbf{v}_i$ umgestellt werden. Mit $\mathbf{b}_i = \tilde{\mathbf{b}}_i / \|\tilde{\mathbf{b}}_i\|$ erhält man

$$\mathbf{v}_i = \|\tilde{\mathbf{b}}_i\| \mathbf{b}_i - \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j \qquad\qquad i = 1, \ldots, n\,.$$

Mit dem Übergang von α_{ij} zu $\tilde{\alpha}_{ij} = -\alpha_{ij}$, $i = 1 \ldots n$, $j = 1 \ldots i-1$, und durch zusätzliche Einführung von $\tilde{\alpha}_{ii} = \|\tilde{\mathbf{b}}_i\|$, $i = 1 \ldots n$, folgt

$$v_i = \tilde{\alpha}_{ii} \mathbf{b}_{ii} + \sum_{j=1}^{i-1} \tilde{\alpha}_{ij} \mathbf{b}_j \;=\; \boxed{\sum_{j=1}^{i} \tilde{\alpha}_{ij} \mathbf{b}_j = \mathbf{v}_i} \qquad\qquad i = 1, \ldots, n\,.$$

Damit hat man eine Darstellung der Basisvektoren $\mathbf{v}_i$, $i = 1 \ldots n$, als Linearkombination der neuen Basisvektoren $\mathbf{b}_i$.
Ersetzt man nun die Basisvektoren $\mathbf{v}_i$ in einem gegebenen Vektor

$$\mathbf{u} = \mathbf{u}_{[v]} = (\mu_1, \ldots, \mu_n)^T_{[\mathbf{v}]} = \sum_{i=1}^{n} \mu_i \mathbf{v}_i$$

durch die neue Basis $\{\mathbf{b}_i\}_{i=1\ldots n}$ erhält man

$$\mathbf{u}_{[v]} = \sum_{i=1}^{n} \mu_i \mathbf{v}_i = \sum_{i=1}^{n} \mu_i \sum_{j=1}^{i} \tilde{\alpha}_{ij} \mathbf{b}_j = \boxed{\sum_{i=1}^{n} \mu_i \sum_{j=1}^{i} \tilde{\alpha}_{ij} \mathbf{b}_j = \mathbf{u}_{[\mathbf{b}]}}$$

also die gesuchte Formel zur Darstellung $\mathbf{u}_{[\mathbf{b}]}$ des Vektors $\mathbf{u}$ bezüglich der Basis $\{\mathbf{b}_i\}_{i=1\ldots n}$.

6.4 Beispiel

Alte Basis ($n = 3$): $\mathbf{v}_1 = (2, 2, 0)^T \qquad \mathbf{v}_2 = (1, 0, 2)^T \qquad \mathbf{v}_3 = (0, 2, 1)^T$
Gegebener Vektor bezüglich Basis $\{\mathbf{v}_i\}_{i=1\ldots 3}$:

$$\mathbf{u}_{[\mathbf{v}]} = (\mu_1, \mu_2, \mu_3)^T_{[\mathbf{v}]} = (1, -2, \tfrac{1}{2})^T_{[\mathbf{v}]}$$

Neue Basis aus *Gram-Schmidt*:

$$\mathbf{b}_1 = (\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T \qquad \mathbf{b}_2 = (\tfrac{\sqrt{2}}{6}, -\tfrac{\sqrt{2}}{6}, \tfrac{2\sqrt{2}}{3})^T \qquad \mathbf{b}_3 = (-\tfrac{2}{3}, \tfrac{2}{3}, \tfrac{1}{3})^T$$

Koeffizienten α_{ij} aus *Gram-Schmidt*:

$$\alpha_{11} = -2\sqrt{2} \qquad \alpha_{21} = -\tfrac{1}{\sqrt{2}} \qquad \alpha_{22} = -\tfrac{3}{\sqrt{2}} \qquad \alpha_{31} = -\sqrt{2} \qquad \alpha_{32} = -\tfrac{\sqrt{2}}{3} \qquad \alpha_{33} = -\tfrac{5}{3}$$

Neue Koeffizienten
$\tilde{\alpha}_{ij} = -\alpha_{ij}$, $i = 1 \dots n$, $j = 1 \dots i-1$, und $\tilde{\alpha}_{ii} = \|\tilde{\mathbf{b}}_i\|$, $i = 1 \dots n$:

$$\tilde{\alpha}_{11} = 2\sqrt{2} \qquad \tilde{\alpha}_{21} = \tfrac{1}{\sqrt{2}} \qquad \tilde{\alpha}_{22} = \tfrac{3}{\sqrt{2}} \qquad \tilde{\alpha}_{31} = \sqrt{2} \qquad \tilde{\alpha}_{32} = \tfrac{\sqrt{2}}{3} \qquad \tilde{\alpha}_{33} = \tfrac{5}{3}$$

Nun **Umrechnung** auf neue Basis $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$:

$$\begin{aligned}
\mathbf{u}_{\mathbf{b}} &= \sum_{i=1}^{3} \mu_i \sum_{j=1}^{i} \tilde{\alpha}_{ij} \mathbf{b}_j \\
&= \mu_1 \tilde{\alpha}_{11} \mathbf{b}_1 + \mu_1(\tilde{\alpha}_{21}\mathbf{b}_1 + \tilde{\alpha}_{22}\mathbf{b}_2) + \mu_3(\tilde{\alpha}_{31}\mathbf{b}_1 + \tilde{\alpha}_{32}\mathbf{b}_2 + \tilde{\alpha}_{32}\mathbf{b}_3) \\
&= \underbrace{(\mu_1\tilde{\alpha}_{11} + \mu_2\tilde{\alpha}_{21} + \mu_3\tilde{\alpha}_{31})}_{\substack{= 2\sqrt{2} - 2\frac{1}{\sqrt{2}} + \frac{1}{2}\sqrt{2} \\ = 2\sqrt{2} - \sqrt{2} + \frac{\sqrt{2}}{2}}} \mathbf{b}_1 + \underbrace{(\mu_2\tilde{\alpha}_{22} + \mu_3\tilde{\alpha}_{32})}_{\substack{= -2\frac{3}{\sqrt{2}} + \frac{1}{2} \cdot \frac{\sqrt{2}}{3} \\ = -3\sqrt{2} + \frac{1}{6}\sqrt{2}}} \mathbf{b}_2 + \underbrace{\mu_3\tilde{\alpha}_{33}}_{= \frac{1}{2} \cdot \frac{5}{3}} \mathbf{b}_3 \\
&\qquad \boxed{\beta_1 = \tfrac{3\sqrt{2}}{2}} \qquad\qquad \boxed{\beta_2 = -\tfrac{17}{6}\sqrt{2}} \qquad\qquad \boxed{\beta_3 = \tfrac{5}{6}}
\end{aligned}$$

und damit

$$\mathbf{u}_{[\mathbf{v}]} = (\mu_1, \mu_2, \mu_3)^T_{[\mathbf{v}]} = (1, -2, \tfrac{1}{2})^T_{[\mathbf{v}]} = \boxed{(\tfrac{3\sqrt{2}}{2}, -\tfrac{17}{6}\sqrt{2}, \tfrac{5}{6})^T_{[\mathbf{b}]} = \mathbf{u}_{[\mathbf{b}]}} = (\beta_1, \beta_2, \beta_3)^T_{[\mathbf{b}]}$$

6.5 Probe: Umrechnung in kartesische Koordinaten

$$\mathbf{u}_{[\mathbf{v}]} = \sum_{i=1}^{3} \mu_i \mathbf{v}_i = 1 \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} + \tfrac{1}{2} \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2-2+0 \\ 2-0+1 \\ 0-4+\frac{1}{2} \end{pmatrix} = \boxed{\begin{pmatrix} 0 \\ 3 \\ -\frac{7}{2} \end{pmatrix} = \mathbf{u}}$$

$$\mathbf{u}_{[\mathbf{b}]} = \textstyle\sum_{i=1}^{3} \beta_i \mathbf{b}_i = \frac{3\sqrt{2}}{2} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} - \frac{17}{6}\sqrt{2} \begin{pmatrix} \frac{\sqrt{2}}{6} \\ -\frac{\sqrt{2}}{6} \\ \frac{2\sqrt{2}}{3} \end{pmatrix} + \frac{5}{6} \begin{pmatrix} -\frac{2}{3} \\ \frac{2}{3} \\ \frac{1}{3} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{3}{2} - \frac{34}{36} - \frac{10}{18} \\ \frac{3}{2} + \frac{34}{36} + \frac{10}{18} \\ 0 - \frac{68}{18} - \frac{5}{18} \end{pmatrix} = \begin{pmatrix} \frac{3}{2} - \frac{27}{18} \\ \frac{3}{2} + \frac{27}{18} \\ 0 - \frac{63}{18} \end{pmatrix} = \begin{pmatrix} \frac{3}{2} - \frac{3}{2} \\ \frac{3}{2} + \frac{3}{2} \\ 0 - \frac{7}{2} \end{pmatrix} = \boxed{\begin{pmatrix} 0 \\ 3 \\ -\frac{7}{2} \end{pmatrix} = \mathbf{u}}$$

und damit

$$\mathbf{u}_{[\mathbf{v}]} = \mathbf{u}_{[\mathbf{b}]} = \mathbf{u}\,.$$

7 Orthogonalisierungsverfahren nach Gram-Schmidt

7.1 Ausgangspunkt

Gegeben sei eine Basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} = \{\mathbf{v}_i\}_{i=1\ldots n}$ des linearen Vektorraumes $\mathcal{V}$.

7.2 Ziel

Mittels des *Gram-Schmidtschen* - Orthogonalisierungsverfahrens soll eine neue **orthonormale Basis** $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\} = \{\mathbf{b}_i\}_{i=1\ldots n}$ des Vektorraumes $\mathcal{V}$ erzeugt werden.

7.3 Verfahren

Gegeben: $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} = \{\mathbf{v}_i\}_{i=1\ldots n}$ Basis von $\mathcal{V}$

Gesucht:$\{\mathbf{b}_1, \ldots, \mathbf{b}_n\} = \{\mathbf{b}_i\}_{i=1\ldots n}$ **orthonormale Basis** von $\mathcal{V}$ so dass

$$\mathbf{span}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \mathbf{span}(\mathbf{v}_1, \ldots, \mathbf{v}_n) \qquad i = 1, \ldots, n$$

sowie

$$\|\mathbf{b}_i\| = 1 \ \wedge \ \mathbf{b}_i \perp \mathbf{b}_j \qquad 1 \leq \{i, j\} \leq n, j \neq i$$

Ansatz: Wegen der Forderung

$$\mathbf{b}_i \in \mathbf{span}(\mathbf{v}_1, \ldots, \mathbf{v}_i) = \mathbf{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1}, \mathbf{v}_i)$$

wählt man den Ansatz

$$\tilde{\mathbf{b}}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j = \|\tilde{\mathbf{b}}_i\| \, \mathbf{b}_i \qquad i = 1, \ldots, n\,.$$

Da $\mathbf{b}_i$ durch Normalisierung aus $\tilde{\mathbf{b}}_i$ gebildet wird, ist auch $\tilde{\mathbf{b}}_i$ orthogonal zu allen Vektoren $\mathbf{b}_j$, $j = 1 \ldots i-1$.
Damit gilt (für festes i)

$$0 = \mathbf{b}_j \cdot \mathbf{v}_i + \alpha_{ij} \qquad j = 1 \ldots i-1$$

und somit

$$\alpha_{ij} = -\mathbf{b}_j \cdot \mathbf{v}_i \qquad j = 1 \ldots i-1\,.$$

Dann wird $\tilde{\mathbf{b}}_i$ entsprechend dem Ansatz

$$\tilde{\mathbf{b}}_i = \mathbf{v}_i + \sum_{j=1}^{i-1} \alpha_{ij} \mathbf{b}_j$$

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 $i = 1 \ldots n$ zu lösen, danach ist die neue Basis berechnet.

7.4 Beispiel

Gegebene Basis ($n = 3$): $\mathbf{v}_1 = (2,2,0)^T$ $\mathbf{v}_2 = (1,0,2)^T$ $\mathbf{v}_3 = (0,2,1)^T$

i = 1:

$$\begin{aligned}
\tilde{\mathbf{b}}_1 &= \mathbf{v}_1 = (2,2,0)^T \\
\|\tilde{\mathbf{b}}_1\| &= \sqrt{2^2+2^2+0} = \sqrt{8} = 2\sqrt{2} \\
\mathbf{b}_1 &= \frac{\tilde{\mathbf{b}}_1}{\|\tilde{\mathbf{b}}_1\|} = \frac{1}{2\sqrt{2}}(2,2,0)^T = \boxed{(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T = \mathbf{b}_1}
\end{aligned}$$

i = 2:

$$\begin{aligned}
\alpha_{21} &= -\mathbf{b}_1 \cdot \mathbf{v}_2 = -(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T \cdot (1,0,2)^T = -\tfrac{1}{\sqrt{2}} \\
\tilde{\mathbf{b}}_2 &= \mathbf{v}_2 + \alpha_{21}\mathbf{b}_1 = (1,0,2)^T - \frac{1}{\sqrt{2}}(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T = (\tfrac{1}{2}, -\tfrac{1}{2}, 2)^T \\
\|\tilde{\mathbf{b}}_2\| &= \sqrt{\tfrac{1}{2}^2 + \tfrac{1}{2}^2 + 2^2} = \sqrt{\tfrac{9}{2}} = \tfrac{3}{\sqrt{2}} \\
\mathbf{b}_2 &= \tfrac{\tilde{\mathbf{b}}_2}{\|\tilde{\mathbf{b}}_2\|} = \tfrac{\sqrt{2}}{3}\,(\tfrac{1}{2}, -\tfrac{1}{2}, 2)^T = \boxed{(\tfrac{\sqrt{2}}{6}, -\tfrac{\sqrt{2}}{6}, 2\tfrac{\sqrt{2}}{3})^T = \mathbf{b}_2}
\end{aligned}$$

i = 3:

$$\begin{aligned}
\alpha_{31} &= -\mathbf{b}_1 \cdot \mathbf{v}_3 = -(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T \cdot (0,2,1)^T = -\sqrt{2} \\
\alpha_{32} &= -\mathbf{b}_2 \cdot \mathbf{v}_3 = -(\tfrac{\sqrt{2}}{6}, -\tfrac{\sqrt{2}}{6}, 2\tfrac{\sqrt{2}}{3})^T \cdot (0,2,1)^T = \tfrac{\sqrt{2}}{3} - \tfrac{2\sqrt{2}}{3} - \tfrac{\sqrt{2}}{3} \\
\tilde{\mathbf{b}}_3 &= \mathbf{v}_3 + \alpha_{31}\mathbf{b}_1 + \alpha_{32}\mathbf{b}_2 \\
&= (0,2,1)^T - \sqrt{2}\,(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T - \tfrac{\sqrt{2}}{3}\,(\tfrac{\sqrt{2}}{6}, -\tfrac{\sqrt{2}}{6}, 2\tfrac{\sqrt{2}}{3})^T \\
&= (-\tfrac{10}{9}, \tfrac{10}{9}, \tfrac{5}{9})^T \\
\|\tilde{\mathbf{b}}_3\| &= \sqrt{\left(\tfrac{10}{9}\right)^2 + \left(\tfrac{10}{9}\right)^2 + \left(\tfrac{5}{9}\right)^2} = \sqrt{\tfrac{225}{81}} = \tfrac{15}{9} = \tfrac{5}{3} \\
\mathbf{b}_3 &= \tfrac{\tilde{\mathbf{b}}_3}{\|\tilde{\mathbf{b}}_3\|} = \tfrac{3}{5}\,(-\tfrac{10}{9}, \tfrac{10}{9}, \tfrac{5}{9})^T = \boxed{(-\tfrac{2}{3}, \tfrac{2}{3}, \tfrac{1}{3})^T = \mathbf{b}_3}
\end{aligned}$$

Die somit berechnete neue Basis ist

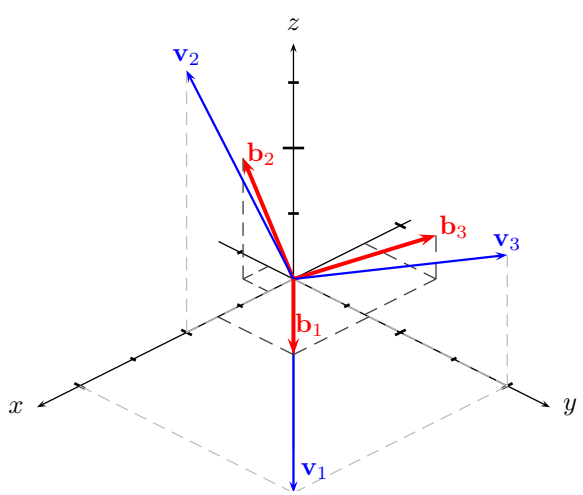
$$\boxed{\mathbf{b}_1 = (\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T \qquad \mathbf{b}_2 = (\tfrac{\sqrt{2}}{6}, -\tfrac{\sqrt{2}}{6}, \tfrac{2\sqrt{2}}{3})^T \qquad \mathbf{b}_3 = (-\tfrac{2}{3}, \tfrac{2}{3}, \tfrac{1}{3})^T}$$

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:

$\mathbf{b}_1 = (\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}, 0)^T$
$\mathbf{b}_2 = (\tfrac{\sqrt{2}}{6}, -\tfrac{\sqrt{2}}{6}, \tfrac{2\sqrt{2}}{3})^T$
$\mathbf{b}_3 = (-\tfrac{2}{3}, \tfrac{2}{3}, \tfrac{1}{3})^T$



8 Matrizen und ihre Algebra

Definition B.1 (Matrix). Ein Zahlenschema

$$A \;=\; (\alpha_{ij})_{i=1\ldots m}^{j=1\ldots n} \;=\; \begin{pmatrix} \alpha_{1\,1} & \alpha_{1\,2} & \cdots & \alpha_{1\,n} \\ \alpha_{2\,1} & \alpha_{2\,2} & \cdots & \alpha_{2\,n} \\ & \cdots\cdots\cdots\cdots & & \\ \alpha_{m\,1} & \alpha_{m\,2} & \cdots & \alpha_{m\,n} \end{pmatrix}$$

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.8).

Die Elemente in der i-ten Zeile von A bilden den sogenannten Zeilenvektor $(\alpha_{i\,j})_{j=1\ldots n} \in \mathbb{R}^n$ und die Elemente in der j-ten Spalte den Spaltenvektor $(\alpha_{i\,j})_{i=1\ldots m} \in \mathbb{R}^m$.

Der Zusammenhang zwischen Matrizen und linearen Abbildungen ergibt sich nun wie folgt.
Sind $(\mathbf{v}_j)_{j=1\ldots n}$ und $(\mathbf{w}_i)_{i=1\ldots m}$ Basen von $\mathcal{V}$ und $\mathcal{W}$, so gibt es genau eine lineare Abbildung $F : \mathcal{V} \mapsto \mathcal{W}$ mit der Eigenschaft

$$F(\mathbf{v}_j) \;=\; \sum_{i=1}^{m} \alpha_{i\,j}\, \mathbf{w}_i \;.$$

Dann gilt für beliebige Vektoren $\mathbf{v} = \sum \nu_j \mathbf{v}_j$

$$\begin{aligned} F(\mathbf{v}) \quad &= \quad \sum_{j=1}^{n} \nu_j F(\mathbf{v}_j) \\ &= \quad \sum_{j=1}^{n} \nu_j \left(\sum_{i=1}^{m} \alpha_{i\,j} \mathbf{w}_i \right) \\ &= \quad \sum_{i=1}^{m} \mathbf{w}_i \underbrace{\sum_{j=1}^{n} \alpha_{i\,j} \nu_j}_{\omega_i} \;. \end{aligned}$$

Definition B.2 (Matrix-Vektor-Produkt). Die durch die letzte Gleichung implizierte Rechenvorschrift nennt man ein **Matrix–Vektor–Produkt** und schreibt einfach

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_m \end{pmatrix} \;=\; \begin{pmatrix} \alpha_{1\,1} & \alpha_{1\,2} & \cdots & \alpha_{1\,n} \\ \alpha_{2\,1} & \alpha_{2\,2} & \cdots & \alpha_{2\,n} \\ & \cdots\cdots\cdots\cdots & & \\ \alpha_{m\,1} & \alpha_{m\,2} & \cdots & \alpha_{m\,n} \end{pmatrix} \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_n \end{pmatrix}$$

oder kurz

$$\mathbf{w} = A\mathbf{v} \;.$$

Diese Matrix-Vektor-Gleichung ist eine Abkürzung für die komponentenweise Identität

$$\boxed{\omega_i \;=\; \sum_{j=1}^{n} \alpha_{i\,j} \nu_j \qquad \text{für} \quad i \;=\; 1, \ldots, m} \tag{1}$$

Beispiel B.3. Bezüglich der monomialen Basis hat die schon im Beispiel B.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 $i = 1, \ldots, 5$ aus der Grundbeziehung

$$F(\mathbf{v}_i) = \mathbf{v}_i' = (i-1)\,\mathbf{v}_{i-1} \qquad \text{da} \quad \mathbf{v}_i = x^{i-1}\,,$$

wobei hier $\mathcal{W} = \mathcal{V}$ und deshalb $\mathbf{w}_i = \mathbf{v}_i$.

Definition B.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 $\{\mathbf{u}_k\}_{k=1\ldots p}$ von $\mathcal{U}$, $\{\mathbf{v}_j\}_{j=1\ldots n}$ von $\mathcal{V}$ und $\{\mathbf{w}_i\}_{i=1\ldots m}$ von $\mathcal{W}$ entsprechen den Abbildungen F und G Matrizen

$$A = (\alpha_{i\,j})_{i=1\ldots m}^{j=1\ldots n} \quad \text{und} \quad B = (\beta_{j\,k})_{j=1\ldots n}^{k=1\ldots p}\,.$$

Hierbei entspricht die Spaltenzahl von A der Zeilenzahl von B, da diese beide gleich der Dimension n des Zwischenbereiches $\mathcal{V}$ sind.

Definition B.5 (Matrixmultiplikation). Unter diesen Bedingungen kann man nun durch wiederholte Anwendung von (1) die Koeffizienten ω_i eines Bildes $\mathbf{w} = F(G(\mathbf{u}))$ direkt aus den Koeffizienten μ_k von $\mathbf{u}$ berechnen. Und zwar gilt für jedes $i = 1 \ldots m$

$$\omega_i \;=\; \sum_{j=1}^{n} \alpha_{i\,j}\nu_j \;=\; \sum_{j=1}^{n} \alpha_{i\,j} \left(\sum_{k=1}^{p} \beta_{j\,k}\mu_k \right) \;=\; \sum_{k=1}^{p} \mu_k \underbrace{\sum_{j=1}^{n} \alpha_{i\,j}\beta_{j\,k}}_{\gamma_{i\,k}}\,.$$

Mittels der $(m \times p)$ Matrix $(\gamma_{i\,k})_{i=1,\ldots m}^{k=1,\ldots p}$ erhält man also das neue Matrix–Vektor–Produkt

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_m \end{pmatrix} = \begin{pmatrix} \gamma_{1\,1} & \gamma_{1\,2} & \cdots & \gamma_{1\,p} \\ \gamma_{2\,1} & \gamma_{2\,2} & \cdots & \gamma_{2\,p} \\ & \cdots\cdots\cdots & & \\ \gamma_{m\,1} & \gamma_{m\,2} & \cdots & \gamma_{m\,p} \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_p \end{pmatrix}\,.$$

Definition B.6 (Matrix-Matrix Schreibweise). Den Zusammenhang zwischen den $\alpha_{i\,j}$, $\beta_{j\,k}$ und den resultierenden $\gamma_{i\,k}$ nennt man ein **Matrix–Matrix–Produkt** (kurz **Matrix-Produkt**) und schreibt

$$\begin{pmatrix} \gamma_{1\,1} & \cdots & \gamma_{1\,p} \\ & \cdots\cdots & \\ \gamma_{m\,1} & \cdots & \gamma_{m\,p} \end{pmatrix} = \begin{pmatrix} \alpha_{1\,1} & \cdots & \alpha_{1\,n} \\ & \cdots\cdots & \\ \alpha_{m\,1} & \cdots & \alpha_{m\,n} \end{pmatrix} \begin{pmatrix} \beta_{1\,1} & \cdots & \beta_{1\,p} \\ & \cdots\cdots & \\ \beta_{n\,1} & \cdots & \beta_{n\,p} \end{pmatrix}$$

oder ganz kurz

$$C \;=\; (\gamma_{i\,k})_{i=1\ldots m}^{k=1\ldots p} \;=\; A\,B$$

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 γ_{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. Man betrachte die beiden (3×3) Matrizen

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad , \quad B = \begin{pmatrix} \sigma & \sigma & 0 \\ -\sigma & \sigma & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad ,$$

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

$$\begin{pmatrix} \sigma & \sigma & 0 \\ 0 & 0 & 1 \\ -\sigma & \sigma & 1 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \sigma & \sigma & 0 \\ -\sigma & \sigma & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

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

$$\begin{pmatrix} \sigma & 0 & \sigma \\ -\sigma & 1 & \sigma \\ 0 & 1 & 0 \end{pmatrix} \quad = \quad \begin{pmatrix} \sigma & \sigma & 0 \\ -\sigma & \sigma & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} .$$

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

$$(A\,B)\,C \;=\; A\,(B\,C)$$

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 $\mathbf{u} \in Dom(H)$ nach $F(G(H(\mathbf{u}))$ abgebildet.
Diese Eindeutigkeit der Komposition von Abbildungen überträgt sich auch auf die Multiplikation von Matrizen.

Definition B.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.

$$A + B = (\alpha_{i\,j} + \beta_{i\,j})_{i=1\ldots m}^{j=1\ldots n} \quad \text{und} \quad \lambda\,A = (\lambda\,\alpha_{i\,j})_{i=1\ldots m}^{j=1\ldots n}$$

für beliebige Matrizen

$$A = (\alpha_{i\,j}) \in \mathbb{R}^{m\times n}, B = (\beta_{i\,j}) \in \mathbb{R}^{m\times n}$$

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:**

$$\begin{aligned} A\,(B + C) &= A\,B + A\,C \\ (A + B)\,C &= A\,C + B\,C\,. \end{aligned}$$

Definition B.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 angebende Index n kann wegfallen, wenn er sich aus dem Zusammenhang ergibt. Es gilt nun insbesondere

$$I_m A \;=\; A \;=\; A\, I_n \quad \text{für} \quad A \in \mathbb{R}^{m\times n} .$$

Definition B.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 $\beta_{i\,j} = \alpha_{j\,i}$, so daß in Matrixschreibweise

$$A^T \;=\; \begin{pmatrix} \alpha_{1\,1} & \alpha_{2\,1} & \cdots & \alpha_{m\,1} \\ \alpha_{1\,2} & \alpha_{2\,2} & \cdots & \alpha_{m\,2} \\ & \cdots\cdots\cdots & & \\ \alpha_{1\,n} & \alpha_{2\,n} & \cdots & \alpha_{m\,n} \end{pmatrix} \;=\; (\beta_{i\,j})_{i=1\ldots n}^{j=1\ldots m} .$$

Bemerkung:
Nur die Diagonalelemente $(\alpha_{i\,i})_{i=1\ldots\min(m,n)}$ bleiben bei der Transposition unverändert, die anderen Elemente tauschen den Platz mit ihrem Gegenüber auf der anderen Seite der Diagonalen.

Lemma B.11 (Transpositionsregeln). *Man kann sich leicht davon überzeugen, daß die folgenden Regeln für das Transponieren gelten:*

$$\begin{aligned} (A^T)^T &= A \\ (A+B)^T &= A^T + B^T \\ (\lambda A)^T &= \lambda A^T \\ (A\,B)^T &= B^T A^T \quad . \end{aligned}$$

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.

8.1 Spezielle Matrixformen

Je nach ihrem Format, der Verteilung nicht verschwindender Elemente und gewissen algebraischen Eigenschaften unterscheidet man die folgenden häufig auftretenden Matrix Typen.

Zeilenvektor

$$A \in \mathbb{R}^{1\times n} \Rightarrow A = (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1n})$$

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 $\mathbf{a}^T = [(\alpha_i)_{i=1\ldots n}]^T \in \mathbb{R}^{1\times n}$ mit einem Spaltenvektor $\mathbf{b} = (\beta_i)_{i=1\ldots m} \in \mathbb{R}^{m\times 1}$ 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 1×1 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

$$\mathbf{b}\mathbf{a}^T = (b_i a_j)_{j=1\ldots n}^{i=1\ldots m} \in \mathbb{R}^{m\times n}$$

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 $\mathbf{v} \in R^n$ genau $m \cdot n$ skalare Multiplikationen. Ist jedoch $A = \mathbf{b}\mathbf{a}^T$ ein äusseres Produkt so berechnet man viel billiger

$$A\mathbf{v} \;=\; (\mathbf{b}\mathbf{a}^T)\mathbf{v} \;=\; \mathbf{b}(\mathbf{a}^T v)\,.$$

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 sehr effizient mittels der sogenannten **Dynamischen Programmierung** geloest werden.

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

$$A \;=\; \underbrace{\tfrac{1}{2}(A + A^T)}_{symmetrisch} + \underbrace{\tfrac{1}{2}(A - A^T)}_{schiefsymmetrisch}\quad .$$

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 $A = (\alpha_{i\,j}) \in \mathbb{R}^{n\times n}$

$$i > j \Rightarrow \alpha_{i\,j} = 0$$

gilt, so daß

$$A = \begin{pmatrix} \alpha_{1\,1} & \cdots & \cdots & \alpha_{1\,n} \\ 0 & \alpha_{2\,2} & \cdots & \alpha_{2\,n} \\ & \cdots\cdots\cdots & & \\ 0 & \cdots & \cdots & \alpha_{n\,n} \end{pmatrix} ,$$

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 $i \neq j \Rightarrow \alpha_{i\,j} = 0$ gilt, also

$$A = \begin{pmatrix} \alpha_{1\,1} & 0 & \cdots & 0 \\ 0 & \alpha_{2\,2} & \cdots & 0 \\ & \cdots\cdots\cdots & & \\ 0 & 0 & \cdots & \alpha_{n\,n} \end{pmatrix} .$$

Man schreibt dann kurz $A = diag(\alpha_{i\,i})_{i=1\ldots n}$.

Insbesondere gilt

$$I = diag(1)_{i=1\ldots n} .$$

Summen und Produkte von diagonalen Matrizen sind wiederum diagonal:

$$\boxed{\begin{array}{c} A = diag(\alpha_i)_{i=1\ldots n} \\ B = diag(\beta_i)_{i=1\ldots n} \end{array}} \quad \Longrightarrow \quad \boxed{\begin{array}{c} A + B = diag(\alpha_i + \beta_i)_{i=1\ldots n} \\ A\,B = diag(\alpha_i\,\beta_i)_{i=1\ldots n} \end{array}} .$$

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 $\mathbf{a}_j = (\alpha_{i\,j})_{i=1\ldots n}$ den j-ten Spaltenvektor von A, so ist die Bedingung $A^T A = I$ äquivalent zu

$$\mathbf{a}_i \cdot \mathbf{a}_j = \begin{cases} 0 & \text{falls} \quad i \neq j \\ 1 & \text{falls} \quad i = j \end{cases}$$

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.12 *(Drehungen in der Ebene).*

$$A = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \quad \Rightarrow \quad A^T = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

$$A^T A = \begin{pmatrix} \cos(\varphi)^2 + \sin(\varphi)^2 & \cos(\varphi)\sin(\varphi) \cdot (1-1) \\ \sin(\varphi)\cos(\varphi) \cdot (1-1) & \cos(\varphi)^2 + \sin(\varphi)^2 \end{pmatrix} = I$$

9 Lösung linearer Gleichungssysteme

Lineare Systeme
Für eine lineare Abbildung

$$F : \mathcal{V} = Span\{\mathbf{v}_j\}_{j=1\ldots n} \quad \rightarrow \quad \mathcal{W} = Span\{\mathbf{w}_i\}_{i=1\ldots m}$$

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 $\mathbf{v} = \sum_{j=1\ldots n} x_j \mathbf{v}_j$ mit $F(\mathbf{v}) = \mathbf{w}$ durch Lösen des Gleichungssystems

$$\begin{array}{ccccccccc}
\alpha_{1\,1}x_1 & + & \alpha_{1\,2}x_2 & + & \ldots + \alpha_{1\,j}x_j \ldots + \alpha_{1\,n}x_n & = & b_1 \\
\alpha_{2\,1}x_1 & + & \alpha_{2\,2}x_2 & + & \ldots + \alpha_{2\,j}x_j \ldots + \alpha_{2\,n}x_n & = & b_2 \\
 & & \ldots\ldots\ldots\ldots\ldots\ldots & & & & \\
\alpha_{i\,1}x_1 & + & \alpha_{i\,2}x_2 & + & \ldots + \alpha_{i\,j} \ldots + \alpha_{i\,n}x_n & = & b_i \\
 & & \ldots\ldots\ldots\ldots\ldots\ldots & & & & \\
\alpha_{m\,1}x_1 & + & \alpha_{m\,2}x_2 & + & \ldots + \alpha_{m\,j} \ldots + \alpha_{m\,n}x_n & = & b_m
\end{array}$$

Matrix–Vektor–Schreibweise
Äquivalenterweise ergibt sich in Matrix–Vektor–Schreibweise

$$A\mathbf{x} = \begin{pmatrix} \alpha_{1\,1} & \ldots & \alpha_{1\,j} & \ldots & \alpha_{1\,n} \\ \alpha_{2\,1} & \ldots & \alpha_{2\,j} & \ldots & \alpha_{2\,n} \\ & & \ldots\ldots\ldots\ldots & & \\ \alpha_{m\,1} & \ldots & \alpha_{m\,j} & \ldots & \alpha_{m\,n} \end{pmatrix} \mathbf{x} = \mathbf{b}$$

wobei $\mathbf{x} = (x_1, \ldots, x_j, \ldots, x_n)^T$ und $\mathbf{b} = (b_1, \ldots, b_i, \ldots, b_m)^T$ sind (unter Verletzung der Konvention, daß alle Skalare mit griechischen Buchstaben benannt sein sollten).

Man bezeichnet das lineare System von m Gleichungen in n Unbekannten als

unterbestimmt	wenn $m < n$
quadratisch	wenn $m = n$
überbestimmt	wenn $m > n$

Definition B.1 (Regularität). Eine Abbildung $F : \mathbb{R}^n \rightarrow \mathbb{R}^n$ und entsprechende Matrizen A heißen regulär, falls

$$A\mathbf{x} = F(\mathbf{x}) = 0 \qquad \text{g.d.w.} \qquad \mathbf{x} = 0\,,$$

andernfalls heißen sie singulär.

Lemma B.2. *Falls A regulär ist, dann hat $A\mathbf{x} = \mathbf{b}$ genau eine eindeutige Lösung für jedes $\mathbf{b}$.*

Ein Kriterium, ob eine Matrix regulär oder singulär ist, liefert die im Abschnitt **B-9** eingeführte **Determinante** $\det(A)$.

Wünschenswerte Lösungsalgorithmen prüfen die Regularität und liefern entweder die eindeutige Lösung oder Singularitätsbeschreibungen.

9.1 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.3 (Lösung orthogonaler Systeme). *Falls A orthogonal ist, gilt:*

$$A\mathbf{x} = \mathbf{b} \quad \Leftrightarrow \quad A^T A\mathbf{x} = \mathbf{x} = A^T\mathbf{b}$$

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.4 (Lösung diagonaler Systeme). *Falls $A = diag(\alpha_i)_{i=1\ldots n}$ 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 α_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.5 (Lösung von Dreieckssystemen). *Ist A eine untere Dreiecksmatrix, hat das entsprechende Gleichungssystem $A\mathbf{x} = \mathbf{b}$ die folgende "gestaffelte" Form:*

$$\begin{array}{lcl}
\alpha_{1\,1}x_1 & = & b_1 \\
\alpha_{2\,1}x_1 + \alpha_{2\,2}x_2 & = & b_2 \\
\vdots & \vdots & \\
\alpha_{i\,1}x_1 + \alpha_{i\,2}x_2 + \cdots + \alpha_{i\,i}x_i & = & b_i \\
\vdots & \vdots & \\
\alpha_{n\,1}x_1 + \alpha_{n\,2}x_2 + \cdots + \alpha_{n,\,n-1}x_{n-1} + \alpha_{n\,n}x_n & = & b_n
\end{array}$$

Vorwärtssubstitution
Nun kann man zunächst aus der ersten Gleichung x_1 bestimmen, dann diesen Wert in die Zweite einsetzten, um x_2 zu erhalten, und so weiter. Unter der Regularitätsbedingung aus Lemma B.4, daß wiederum keines der diagonalen Elemente $\alpha_{i\,i}$ verschwindet, hat man also

$$\begin{array}{lcl}
x_1 & = & b_1/\alpha_{1\,1} \\
x_2 & = & (b_2 - \alpha_{2\,1}x_1)/\alpha_{2\,2} \\
x_3 & = & (b_3 - \alpha_{3\,1}x_1 - \alpha_{3\,2}x_2)/\alpha_{3\,3} \\
 & \vdots & \\
x_i & = & (b_i - \alpha_{i\,1}x_1 - \cdots - \alpha_{i\,i-1}x_{i-1})/\alpha_{i\,i} \\
 & \vdots & \\
x_n & = & (b_n - \alpha_{n\,1}x_1 - \cdots - \alpha_{n\,j}x_j - \cdots - \alpha_{n\,n-1}x_{n-1})/\alpha_{n\,n}
\end{array}$$

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 $i = n, n-1, \ldots, 1$ durch die Formel

$$x_i = \frac{1}{\alpha_{i\,i}}\left(b_i - \sum_{j=i+1}^{n} \alpha_{i\,j}x_j\right) \qquad\qquad i = n,\, n-1, \ldots, 1$$

bestimmt sind. Regularitätsbedingung ist wiederum, daß keines der Diagonalelemente verschwindet und der Rechenaufwand ist auch hier von der Ordnung $n^2/2$ arithmetische 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).

10 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 λ gilt:

$$\boxed{\begin{aligned} f(\mathbf{x}) &= 0 \\ g(\mathbf{x}) &= 0 \end{aligned}} \quad \Longleftrightarrow \quad \boxed{\begin{aligned} f(\mathbf{x}) &= 0 \\ \underbrace{g(\mathbf{x}) - \lambda f(\mathbf{x})}_{=:\,\tilde{g}(\mathbf{x})} &= 0 \end{aligned}}$$

Mit anderen Worten: Die Menge $\{\mathbf{x} | f(\mathbf{x}) = g(\mathbf{x}) = 0\}$ 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.

10.1 Lineare Systeme in zwei Variablen

Zunächst betrachten wir hier den Fall von zwei linearen Gleichungen in zwei Unbekannten.

$$\begin{aligned} \alpha_{1\,1} x_1 + \alpha_{1\,2} x_2 &= b_1 \\ \alpha_{2\,1} x_1 + \alpha_{2\,2} x_2 &= b_2 \end{aligned}$$

Ausnahmefall: $\alpha_{1\,1} = 0$
Tauscht man die beiden Gleichungen **aus**, so ergibt sich das gestaffelte Gleichungssystem

$$\begin{aligned} \alpha_{2\,1} x_1 + \alpha_{2\,2} x_2 &= b_2 \\ \alpha_{1\,2} x_2 &= b_1 \end{aligned} \Longleftrightarrow \tilde{A}\mathbf{x} = \begin{pmatrix} \tilde{\alpha}_{11} & \tilde{\alpha}_{12} \\ \tilde{\alpha}_{21} & \tilde{\alpha}_{22} \end{pmatrix} \mathbf{x} = \begin{pmatrix} \alpha_{21} & \alpha_{22} \\ 0 & \alpha_{12} \end{pmatrix} \mathbf{x} = \tilde{\mathbf{b}} = \begin{pmatrix} b_2 \\ b_1 \end{pmatrix} ,$$

wobei die Komponenten der rechten Seite auch vertauscht wurden. Damit hat die Matrix $\tilde{A}$ nun Dreiecksform. Vorausgesetzt die beiden neuen Diagonalelemente $\tilde{\alpha}_{1\,1}$ und $\tilde{\alpha}_{2\,2}$ sind beide nicht Null, ergibt somit sich durch Rückwärtssubstitution

$$x_2 = \tilde{b}_2 / \tilde{\alpha}_{2\,2} \quad \text{und} \quad x_1 = (\tilde{b}_1 - \tilde{\alpha}_{1\,2} x_2) / \tilde{\alpha}_{1\,1} \, .$$

Normalfall: $\alpha_{1\,1} \neq 0$
In diesem Fall läßt sich durch **Abziehen** des $\boxed{\lambda_{2\,1} \equiv \alpha_{2\,1} / \alpha_{1\,1}}$ - fachen **der ersten von der zweiten Gleichung** die Variable x_1 aus Letzterer **eliminieren**.
Man erhält also

$$\begin{array}{rcrcl} \alpha_{1\,1} x_1 & + & \alpha_{1\,2} x_2 & = & b_1 \\ \underbrace{(\alpha_{2\,1} - \lambda_{2\,1}\alpha_{1\,1})}_{\tilde{\alpha}_{2\,1} = 0} x_1 & + & \underbrace{(\alpha_{2\,2} - \lambda_{2\,1}\alpha_{1\,2})}_{\tilde{\alpha}_{2\,2}} x_2 & = & \underbrace{(b_2 - \lambda_{2\,1} b_1)}_{\tilde{b}_2} \end{array}$$

Da $\lambda_{2\,1}$ gerade so gewählt wurde, daß $\tilde{\alpha}_{2\,1}$ 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 $\lambda_{2\,1}$ auftretende Diagonalelement $\alpha_{1\,1}$ 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.

10.2 Lösung von Systemen beliebiger Dimension

Wir betrachten nun ein quadratisches Gleichungssystem von n Gleichungen mit n Unbekannten:

$$A\mathbf{x} = \begin{pmatrix} \alpha_{1\,1} & \alpha_{1\,2} & \dots & \alpha_{1\,j} & \dots & \alpha_{1\,n} \\ \alpha_{2\,1} & \alpha_{2\,2} & \dots & \alpha_{2\,j} & \dots & \alpha_{2\,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_{i\,1} & \alpha_{i\,2} & \dots & \alpha_{i\,j} & \dots & \alpha_{i\,n} \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_{n\,1} & \alpha_{n\,2} & \dots & \alpha_{n\,j} & \dots & \alpha_{n\,n} \end{pmatrix} \mathbf{x} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{pmatrix}$$

Erster Schritt

Eliminiere $\alpha_{i\,1}$ mit Hilfe des nichtverschwindenden Diagonalelementes $\alpha_{1\,1}$. Zu diesem Zwecke wird das $\lambda_{i\,1}$ - fache der ersten Zeile mit

$$\lambda_{i\,1} = \alpha_{i\,1}/\alpha_{1\,1} \qquad i = 2 \dots n$$

von allen anderen Zeilen abgezogen.

Dadurch erhalten die Elemente $\alpha_{i\,j}$ mit $i > 1$ und $j > 1$ die neuen Werte

$$\alpha_{i\,j} \leftarrow \alpha_{i\,j} - \lambda_{i\,1}\alpha_{1\,j} \qquad i, j = 2 \dots n$$

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 ˜ von den Alten unterschieden.)

Entsprechend werden auch die Komponenten der rechten Seite nach der Formel

$$b_i \leftarrow b_i - \lambda_{i\,1} b_1 \qquad i = 2 \dots n$$

"aufdatiert".

Anschließend hat das Gleichungssystem die Form

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1j} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2j} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & \alpha_{i2} & \dots & \alpha_{ij} & \dots & \alpha_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & \alpha_{n2} & \dots & \alpha_{nj} & \dots & \alpha_{nn} \end{pmatrix} \mathbf{x} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_i \\ \vdots \\ b_n \end{pmatrix}$$

Zwischenergebnis nach k-1 Schritten

$$A\mathbf{x} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1,k-1} & \alpha_{1k} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2,k-1} & \alpha_{2k} & \dots & \alpha_{2n} \\ 0 & 0 & \ddots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \alpha_{k-1,k-1} & \alpha_{k-1,k} & \dots & \alpha_{k-1,n} \\ \vdots & \vdots & & 0 & \alpha_{k,k} & \dots & \alpha_{k,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & \alpha_{nk} & \dots & \alpha_{nn} \end{pmatrix} \mathbf{x} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \\ \vdots \\ \vdots \\ b_n \end{pmatrix}$$

k-ter Schritt

Zur Elimination der letzten $n-k$ Elemente in der k-ten Spalte subtrahiert man nun für $i = k+1, \ldots, n$ das $\lambda_{i\,k}$–fache der k–ten Zeile mit

$$\lambda_{i\,k} \;=\; \alpha_{i\,k}/\alpha_{k\,k} \qquad\qquad i = k+1 \ldots n$$

von der i-ten Zeile.

Es gilt also für $j = k+1, \ldots, n$ die Aufdatierungsformel

$$\alpha_{i\,j} \;\leftarrow\; \alpha_{i\,j} - \lambda_{i\,k}\alpha_{k\,j} \qquad\qquad i, j = k+1 \ldots n$$

und entsprechend für die rechte Seite

$$b_i \;\leftarrow\; b_i - \lambda_{i\,k} b_k \qquad\qquad i = k+1 \ldots n\,.$$

Spaltenpivotierung
Findet sich im k-ten Schritt in der Diagonale ein Element $\alpha_{k\,k}$, 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 $\alpha_{i\,k}$ 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 $\alpha_{i\,k}$ 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.

10.3 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. Dann kann man die erneute Reduktion von A auf Dreiecksform vermeiden, da dieser Prozeß zwar auf die rechte Seite wirkt, aber nicht von ihr abhängig ist.

Mit anderen Worten: Man kann die Multiplikatoren $\lambda_{i\,k}$ statt der ursprünglichen $\alpha_{i\,k}$ unterhalb der Diagonale abspeichern (da wo Nullen enstanden sind) und dann die Aufdatierung der rechten Seite von der Elimination in A abtrennen.
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:

$$L \;=\; \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ \lambda_{21} & 1 & 0 & \ldots & 0 \\ \lambda_{31} & \lambda_{32} & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{n1} & \lambda_{n2} & \lambda_{n3} & \ldots & 1 \end{pmatrix}$$

Zu lösen bleibt

$$L(U\,\mathbf{x}) \;=\; L\,\mathbf{y} \;=\; \mathbf{c} \qquad \text{mit} \quad U\mathbf{x} \;=\; \mathbf{y}\,.$$

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.

11 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:

$$\det(A) \neq 0 \quad \Longleftrightarrow \quad A \textbf{ regulär}$$

Eine Dreiecksmatrix ist regulär, wenn alle ihre Diagonalelemente nicht Null sind. Man definiert also

$$\det(A) = \prod_{i=1}^{n} \alpha_{i\,i} \quad \text{für } A = \begin{pmatrix} \ddots & & \\ & \ddots & \\ & & \ddots \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} \ddots & & \\ & \ddots & \\ & & \ddots \end{pmatrix} .$$

Verlangt man nun noch

1. daß die Determinante konstant bleibt, wenn ein Vielfaches einer Zeile (Spalte) zu einer anderen Zeile (Spalte) addiert wird
2. 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.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.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.

11.1 Entwicklungsatz

Bei kleineren Matrizen läßt sich die Determinante auch rekursiv nach dem folgenden Entwicklungssatz berechnen.

Satz B.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 $A \in \mathbb{R}^{n\times n}$ hervorgegangenen sind, so gilt für beliebiges (aber festes) i*

bzw. j

$$\begin{aligned}\det(A) &= \sum_{k=1}^{n} \alpha_{i\,k} \det(A_{i\,k})(-1)^{i+k} \\ &= \sum_{k=1}^{n} \alpha_{k\,j} \det(A_{k\,j})(-1)^{j+k} \quad = \quad \det(A^T)\end{aligned}$$

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

$$\det(A) \quad = \quad \sum \alpha_{1\,j_1}\alpha_{2\,j_2}\ldots\alpha_{n\,j_n} sgn(j_1, j_2, \ldots, j_n\,)$$

wobei die Spaltenindizes $(j_1, j_2, \ldots, j_n)$ alle möglichen Permutationen der Zahlen $(1, 2, \ldots, n)$ durchlaufen. Das jeweilige $sgn(j_1, j_2, \ldots, j_n)$ ist entweder $+1$ oder -1, je nach dem ob die Permutation durch eine gerade oder ungerade Zahl von Nachbar-Vertauschungen aus der Grundpermutation $(1, 2, \ldots, n)$ gebildet werden kann.

Da die Gesamtzahl der Permutationen und damit der Summanden in der Leibnitzschen Formel **n**! ist, wird diese in der Praxis selten angewandt.

Beispiel B.4. Im folgenden wird der Entwicklungssatz zunächst auf die dritte Spalte, die zwei Nullen enthält (damit bleiben nur 2 Summanden übrig), angewendet.

$$\begin{aligned}\begin{vmatrix} 1 & 2 & 0 & 2 \\ 2 & 1 & 4 & 3 \\ 3 & 6 & 0 & 4 \\ 0 & 1 & 2 & 1 \end{vmatrix} &= -\,4 \begin{vmatrix} 1 & 2 & 2 \\ 3 & 6 & 4 \\ 0 & 1 & 1 \end{vmatrix} - \,2 \begin{vmatrix} 1 & 2 & 2 \\ 2 & 1 & 3 \\ 3 & 6 & 4 \end{vmatrix} \\ &= -\,4 \begin{vmatrix} 6 & 4 \\ 1 & 1 \end{vmatrix} + \,4 \cdot 3 \begin{vmatrix} 2 & 2 \\ 1 & 1 \end{vmatrix} - \,2 \begin{vmatrix} 1 & 3 \\ 6 & 4 \end{vmatrix} \\ &\quad + \,4 \begin{vmatrix} 2 & 2 \\ 6 & 4 \end{vmatrix} - \,6 \begin{vmatrix} 2 & 2 \\ 1 & 3 \end{vmatrix} \\ &= -\,4 \cdot 2 \,+\, 12 \cdot 0 \,-\, 2(-14) \,+\, 4(-4) \,-\, 6 \cdot 4 \\ &= -\,8 \,+\, 28 \,-\, 16 \,-\, 24 \,=\, -20\end{aligned}$$

11.2 Determinantenprodukt

Während sich die Determinante der Summe zweier Matrizen nicht leicht berechnen läßt, ergibt sich für Matrixprodukte die folgende multiplikative Regel:

Satz B.5. *Sind* A, B *Matrizen vom Typ* (n, n)*, so gilt:*

$$\det(AB) \;=\; \det(A) \cdot \det(B)$$

Beweis

$$A \;=\; (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n) \qquad B \;=\; \begin{bmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1n} \\ \vdots & \vdots & & \vdots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn} \end{bmatrix}$$

$$C \;=\; A\,B \;=\; \left(\underbrace{\sum_{i=1}^{n} \beta_{i1}\mathbf{a}_i,}_{\mathbf{c}_1} \quad \underbrace{\sum_{i=1}^{n} \beta_{i2}\mathbf{a}_i,}_{\mathbf{c}_2} \;\ldots,\; \underbrace{\sum_{i=1}^{n} \beta_{in}\mathbf{a}_i,}_{\mathbf{c}_n} \right)$$

Wir betrachten z.B. $\tilde{B} \;=\; (\mathbf{b}_1 + \lambda\mathbf{b}_2, \mathbf{b}_2, \ldots, \mathbf{b}_n) \Longrightarrow \det(\tilde{B}) \;=\; \det(B)$

$$\tilde{C} \;=\; A\tilde{B} \;=\; (\mathbf{c}_1 + \lambda\mathbf{c}_2, \mathbf{c}_2, \ldots, \mathbf{c}_n) \Longrightarrow \det(A\tilde{B}) \;=\; \det(AB)$$

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

$$D \;=\; diag(\delta_1, \ldots, \delta_n)$$

umformen, wobei

$$\det(AB) \;=\; \det(AD), \quad \det(D) \;=\; \det(B)$$

$$AD \;=\; (\delta_1\mathbf{a}_1, \delta_2\mathbf{a}_2, \ldots, \delta_n\mathbf{a}_n)$$

$$\det(AD) \;=\; \det(A)\cdot\prod_{i=1}^{n}\delta_i \;=\; \det(A)\det(D) \;=\; \det(A)\;\det(B)$$

□

11.3 Cramersche Regel

Gabriel Cramer (1704 – 1752)

Vorbetrachtung:

$$\det(A) \;=\; \sum_{i=1}^{n}(-1)^{i+j}\alpha_{i\,j}\det(\,A_{i\,j}) \qquad \text{Entwicklung nach der j–ten Spalte}$$

$$\sum_{i=1}^{n}(-1)^{i+j}\alpha_{i\,k}\det(\,A_{i\,j}) \;=\; 0 \quad \text{für} \quad k \neq j$$

An die Stelle des Spaltenvektors $\mathbf{a}_j$ wird $\mathbf{a}_k$ gesetzt, $\tilde{A}$ enthält zwei gleiche Spalten!!

Lineares Gleichungssystem: $\quad A\mathbf{x} = \mathbf{b}$

$$\left.\begin{array}{ll}
\alpha_{1\,1}x_1 + \alpha_{1\,2}x_2 + \cdots + \alpha_{1\,n}x_n \;=\; b_1 & |\,(-1)^{1+j}\;\det(\,A_{1\,j}\,) \\
\vdots & \\
\alpha_{i\,1}x_1 + \alpha_{i\,2}x_2 + \cdots + \alpha_{i\,n}x_n \;=\; b_i & |\,(-1)^{i+j}\;\det(\,A_{i\,j}\,) \\
\vdots & \\
\alpha_{n\,1}x_1 + \alpha_{n\,2}x_2 + \cdots + \alpha_{n\,n}x_n = \; b_n & |\,(-1)^{n+j}\;\det(\,A_{n\,j}\,)
\end{array}\right\}\;\text{geeignete Multiplikationen, anschließend Summation}$$

$$x_1\underbrace{\sum_{i=1}^{n}(-1)^{i+j}\alpha_{i\,1}\det(\,A_{i\,j})}_{0} + \cdots + \; x_j\underbrace{\sum_{i=1}^{n}(-1)^{i+j}\alpha_{i\,j}\det(\,A_{i\,j})}_{\det(A)} + \ldots$$

$$= \sum_{i=1}^{n}(-1)^{i+j}b_i\det(A_{i\,j}) \;=\; \det(A_j|\mathbf{b})$$

$A_j|\mathbf{b}$ bedeutet Ersetzung des Spaltenvektors $\mathbf{a}_j$ durch Vektor $\mathbf{b}$

Satz B.6 (Cramersche Regel, 1850). *Falls* $\det(A) \neq 0$, *dann kann die eindeutige Lösung des Gleichungssystems* $A\mathbf{x} \;=\; b$ *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 $\alpha_{i\,j}$ z. B. funktionelle Ausdrücke sind oder wenn eventuell nur eine der Unbekannten x_j benötigt wird.

Beispiel B.7.

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \Longrightarrow \det(A) = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$$

$$\left.\begin{aligned} x_1 &= \tfrac{1}{2} \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix} = \tfrac{1}{2} \\ x_2 &= \tfrac{1}{2} \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix} = \tfrac{1}{2} \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = -\tfrac{1}{2} \\ x_3 &= \tfrac{1}{2} \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{vmatrix} = \tfrac{1}{2} \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = \tfrac{1}{2} \end{aligned}\right\} \quad \boxed{x = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}}$$

11.4 Anwendung der Cramerschen Regel auf die Bestimmung der inversen Matrix A^{-1}

Bezeichnung $A^{-1} = B = (\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n), \quad A\,B = I$
Die gesuchte Matrix $B = A^{-1}$ läßt sich schrittweise aus den Gleichungssystemen

$$A\mathbf{b}_k = \mathbf{e}_k = (0, \ldots, 0, \underset{\llcorner\, k\text{–te Position}}{1}, 0, \ldots, 0)^T \qquad k = 1, \ldots, n$$

berechnen:

$$\boxed{\begin{aligned} b_{j\,k} &= \frac{1}{\det(A)} \det(A_j|\mathbf{e}_k) \\ &= \frac{(-1)^{j+k}}{\det(A)} \det(A_{k\,j}) \end{aligned}} \quad \text{mit } A_j|\mathbf{e}_k = \begin{array}{c} \begin{bmatrix} \alpha_{1\,1} & \ldots & 0 & \ldots & \alpha_{1\,n} \\ \vdots & & \vdots & & \vdots \\ \vdots & & 1 & & \vdots \\ \alpha_{n\,1} & \ldots & 0 & \ldots & \alpha_{n\,n} \end{bmatrix} \longleftarrow k \\ \begin{array}{ccccc} \mathbf{a}_1 & & \mathbf{a}_j & & \\ & & \uparrow & & \\ & & \mathbf{e}_k & & \end{array} \end{array}$$

Man beachte:
Vertauschung von Zeilen- bzw. Spaltenindex in $b_{j\,k} = \frac{(-1)^{j+k}}{\det(A)} \det(\,A_{k\,j}\,)$

Zweckmäßigerweise ergibt sich Darstellung:

$$\begin{aligned} A^{-1} &= \frac{1}{\det(A)} \left(\left((-1)^{i+j} \det(A_{i\,j}) \right)_{i=1\ldots n}^{j=1\ldots n} \right)^T \\ &= \frac{1}{\det(A)} \begin{pmatrix} +\det(A_{11}) & -\det(A_{21}) & +\det(A_{31}) & \ldots \\ -\det(A_{12}) & +\det(A_{22}) & -\det(A_{32}) & \ldots \\ +\det(A_{13}) & -\det(A_{23}) & +\det(A_{33}) & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \end{aligned}$$

Warnung:
Für rechteckige Matrizen läßt sich die Determinante nicht definieren.

Beispiel B.8.

$$A = \begin{bmatrix} 1 & 0 & 2 \\ -1 & 2 & 0 \\ 3 & 1 & 4 \end{bmatrix} \Longrightarrow \det(A) = \begin{vmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 1 & -2 \end{vmatrix} = \begin{vmatrix} 2 & 2 \\ 1 & -2 \end{vmatrix} = -6$$

$$A_{1\,1} = \begin{vmatrix} 2 & 0 \\ 1 & 4 \end{vmatrix} = 8\,, \quad A_{1\,2} = \begin{vmatrix} -1 & 0 \\ 3 & 4 \end{vmatrix} = -4\,, \quad A_{1\,3} = \begin{vmatrix} -1 & 2 \\ 3 & 1 \end{vmatrix} = -7$$

$$A_{2\,1} = \begin{vmatrix} 0 & 2 \\ 1 & 4 \end{vmatrix} = -2\,, \quad A_{2\,2} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = -2\,, \quad A_{2\,3} = \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 1$$

$$A_{3\,1} = \begin{vmatrix} 0 & 2 \\ 2 & 0 \end{vmatrix} = -4\,, \quad A_{3\,2} = \begin{vmatrix} 1 & 2 \\ -1 & 0 \end{vmatrix} = 2\,, \quad A_{3\,3} = \begin{vmatrix} 1 & 0 \\ -1 & 2 \end{vmatrix} = 2$$

$$A^{-1} = \frac{-1}{6} \begin{bmatrix} 8 & 4 & -7 \\ 2 & -2 & -1 \\ -4 & -2 & 2 \end{bmatrix}^T = \frac{-1}{6} \begin{bmatrix} 8 & 2 & -4 \\ 4 & -2 & -2 \\ -7 & -1 & 2 \end{bmatrix} = \frac{1}{6} \begin{bmatrix} -8 & -2 & 4 \\ -4 & 2 & 2 \\ 7 & 1 & -2 \end{bmatrix}$$

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 sogenannten **Rang** der $m \times n$ Matrix A ab. Diese natürliche Zahl $rang(A)$ erfüllt die folgenden äquivalenten Definitionen:

- maximale Zahl linear unabhängiger Spalten
- maximale Zahl linear unabhängiger Zeilen
- Dimension des Bildraumes $\{A\mathbf{x} : \mathbf{x} \in \mathbb{R}^n\}$
- $n - dim(kern(A))$ mit $kern(A) = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = 0\}$
- maximale Größe einer quadratischen Untermatrix $\tilde{A}$ mit nichtverschwindender Determinante $\det(\tilde{A})$

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

$$m\left\{\overbrace{\begin{bmatrix} \times & \times & \dots & \times & \times & \times & \dots & \times \\ 0 & \times & \dots & \times & \times & \times & \dots & \times \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \times & \times & \times & & \times \\ 0 & 0 & \dots & 0 & \times & \times & & \times \\ 0 & 0 & \dots & 0 & 0 & 0 & & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & & 0 \end{bmatrix}}^{n}\right. \begin{bmatrix} \times \\ \times \\ \vdots \\ \times \\ \times \\ \times \\ \vdots \\ \times \end{bmatrix} \begin{matrix} \left.\begin{matrix} \times \\ \times \\ \vdots \\ \times \\ \times \\ \times \end{matrix}\right\} r \\ \left.\begin{matrix} \vdots \\ \times \end{matrix}\right\} n-r \end{matrix} = \begin{bmatrix} \times \\ \times \\ \vdots \\ \times \\ \times \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{matrix} \left.\begin{matrix} \times \\ \times \\ \vdots \\ \times \\ \times \end{matrix}\right\} r \\ \left.\begin{matrix} 0 \\ \vdots \\ 0 \end{matrix}\right\} m-r \end{matrix}$$

$$\underbrace{\qquad\qquad\qquad}_{r} \quad \underbrace{\qquad\qquad}_{n-r}$$

wobei die ersten $r = rang(A)$ Elemente der Diagonale nicht Null sind.

Eigenschaften der Lösung 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:

$\mathbf{n} = \mathbf{r} = \mathbf{m}$: Für beliebiges $\mathbf{b}$ gibt es eine eindeutige Lösung $\mathbf{x}$

$\mathbf{n} = \mathbf{m} > \mathbf{r}$: Für bestimmte $\mathbf{b}$ (insbesondere $\mathbf{b} = 0$) existieren mehrere Lösungen $\mathbf{x}$, sonst keine

$\mathbf{m} = \mathbf{r} < \mathbf{n}$: Für beliebige $\mathbf{b}$ existieren mehrere $\mathbf{x}$

$\mathbf{n} = \mathbf{r} < \mathbf{m}$: Für bestimmte $\mathbf{b}$ existieren eindeutige $\mathbf{x}$, sonst keine

$\mathbf{n} > \mathbf{r} < \mathbf{m}$: Für bestimmte $\mathbf{b}$ existieren mehrere $\mathbf{x}$, sonst keine

12 Eigenwerte und Eigenvektoren

12.1 Komplexe Lineare Algebra

Für die Berechnung von Eigenwerten und Eigenvektoren von nicht symmetrischen reellen Matrizen besteht die Notwendigkeit, die bisher im Reellen betrachtete lineare Algebra auf die Räume $\mathbb{C}^{\mathbf{n}}$ der n-elementigen komplexen Vektoren $\mathbf{a} \in \mathbb{C}^n$ mit

$$\mathbf{a} = (\alpha_i)_{i\,=\,1\ldots n}, \qquad \alpha_i \;=\; Re\,(\alpha_i) + \mathbf{i}Im\,(\alpha_i) \in \mathbb{C}$$

zu erweitern. Zu jedem solchen Vektor $\mathbf{a}$ existiert der konjugiert–komplexe Vektor

$$\bar{\mathbf{a}} = (\bar{\alpha}_i)_{i\,=\,1\ldots n}, \qquad \bar{\alpha}_i \;=\; Re(\alpha_i) - \mathbf{i}Im(\alpha_i) \in \mathbb{C}.$$

Offensichtlich gilt, wie schon im skalaren Falle, für jeden **reellen Vektor** $\mathbf{a} \in \mathbb{R}^n$: $\bar{\mathbf{a}} = \mathbf{a}$.
Durch

$$\mathbf{a} \cdot \mathbf{b} \;=\; \bar{\mathbf{a}}^T\mathbf{b} \;=\; \sum_{i=1}^{n} \bar{\alpha}_i\beta_i \;\in\; \mathbb{C}$$

wird nun ein inneres Produkt (oder Skalarprodukt) definiert, welches im Gegensatz zum reellen Falle nicht kommutativ ist, d.h. es ist von der Reihenfolge der Faktoren abhängig:

$$\mathbf{b} \cdot \mathbf{a} \;=\; \bar{\mathbf{b}}^T\mathbf{a} \;=\; \overline{\bar{\mathbf{a}}^T\,\mathbf{b}} \;=\; \overline{\mathbf{a} \cdot \mathbf{b}}$$

Da nun $(\mathbf{a}, \mathbf{a})$ immer reell und nicht negativ ist läßt sich damit die innere Produktnorm

$$\|\mathbf{a}\| \;=\; \sqrt{\mathbf{a} \cdot \mathbf{a}} \;=\; \left[\sum_{i=1}^{n} |\alpha_i|^2\right]^{\frac{1}{2}}$$

definieren.
Es gelten die üblichen Normeigenschaften

$$\|\mathbf{a}\| \geq 0, \qquad \|\mathbf{a}\| = 0 \iff \mathbf{a} = 0, \qquad \|\gamma\mathbf{a}\| = |\gamma|\|\mathbf{a}\|$$

für beliebiges $\gamma \in \mathbb{C}$, sowie die Dreiecksungleichungen

$$\|\mathbf{a} + \mathbf{b}\| \leq \|\mathbf{a}\| + \|\mathbf{b}\|, \qquad \|\mathbf{a} - \mathbf{b}\| \geq \big|\|\mathbf{a}\| - \|\mathbf{b}\|\big| \,.$$

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** $\mathbf{v}_i \in \mathbb{C}^n$, $i \;=\; 1 \ldots r$, heißt **orthogonal**, wenn

$$\mathbf{v}_i \cdot \mathbf{v}_j \;=\; \bar{\mathbf{v}}_i^T\mathbf{v}_j \;=\; 0 \qquad \text{für } i \neq j\,,$$

was weiterhin lineare Unabhängigkeit impliziert. Eine quadratische **Matrix**

$$A \;=\; (\alpha_{ij})_{i=1\ldots n}^{j=1\ldots n} \in \mathbb{C}^{n\times n}$$

heißt **orthogonal**, wenn ihre Spalten paarweise orthogonal sind und ihre Norm jeweils gleich 1 ist. Mittels der **konjugiert transponierten Matrix**

$$\bar{A}^T \;=\; \begin{pmatrix} \bar{\alpha}_{1\,1} & \ldots & \bar{\alpha}_{n\,1} \\ \vdots & & \vdots \\ \bar{\alpha}_{1\,n} & \ldots & \bar{\alpha}_{n\,n} \end{pmatrix}$$

läßt sich die Orthogonalität von A durch die Beziehungen

$$\bar{A}^T A \;=\; I \;=\; A\bar{A}^T$$

beschreiben, wobei I weiterhin die Einheitsmatrix bezeichnet:

$$I \;=\; diag(1,1,\ldots,1) \in \mathbb{R}^{n\times n} \subset \mathbb{C}^{n\times n}\,.$$

Abgesehen von der Orthogonalität erfährt auch der Begriff der **Symmetrie** bei der Erweiterung auf komplexe Matrizen eine Veränderung. Man kann zwar eine Matrix $A \;=\; (\alpha_{i\,j}) \in \mathbb{C}^{n\times n}$ immer noch symmetrisch nennen, wenn $\alpha_{j\,i} \;=\; \alpha_{i\,j}$ gilt, diese Eigenschaft ist aber wesentlich weniger interessant als die Erfüllung der Bedingung

$$\bar{\alpha}_{j\,i} \;=\; \alpha_{i\,j} \quad \Rightarrow \quad \bar{A}^T \;=\; A\,.$$

Solche Matrizen nennt man **hermitesch** und die entsprechenden linearen Abbildungen auch **selbstadjungiert**, da für beliebige Vektoren $\mathbf{a},\mathbf{b} \in \mathbb{C}^n$

$$\mathbf{a}\cdot(A\mathbf{b}) \;=\; \bar{\mathbf{a}}^T A\mathbf{b} \;=\; (\bar{A}^T\mathbf{a})\cdot\mathbf{b} \;=\; (A\mathbf{a})\cdot\mathbf{b}$$

gilt. Für uns wird nur von Bedeutung sein, daß hermitesche Matrizen (wie ihre Untermenge der reell symmetrischen Matrizen) nur reelle Eigenwerte haben.

Definition B.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:

$$A\mathbf{v} \;=\; \lambda\mathbf{v} \quad \text{mit} \qquad \mathbf{v} \neq 0\,.$$

Folgerung B.2. *Daraus folgt unmittelbar, daß* $\mathbf{v}$ *eine nicht triviale Lösung des homogenen Systems*

$$(A-\lambda I)\,\mathbf{v} \;=\; 0$$

ist. Eine solche existiert genau dann, wenn der Rang von $(A-\lambda\,I)$ *kleiner als* n *ist, und damit äquivalenterweise gilt*

$$P(\lambda) \;\equiv\; \det(A-\lambda\,I) \;=\; 0\,.$$

$P(\lambda)$ *wird das* **charakteristische Polynom von** A *genannt.*

Satz B.3 (Polynomeigenschaft von $P(A)$). $P(\lambda)$ *ist ein Polynom* n*-ten Grades und hat die spezielle Form*

$$P(\lambda) \;=\; (-\lambda)^n + Tr(A)(-\lambda)^{n-1} + \;\ldots\; + \det(A)\,,$$

wobei

$$Tr(A) \;=\; \sum_{i=1}^{n} \alpha_{i\,i}$$

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, $n=1$: $\det(A-\lambda B) \;=\; \alpha_{1\,1} - \lambda\beta_{1\,1}$ ist offensichtlich ein Polynom vom Grade gleich 1.
Induktionsvorraussetzung: $\deg(\det(A-\lambda B)) \leq n$ sei erfüllt für n.
Induktionsschritt, $n \to n+1$:
Nach dem Entwicklungssatz gilt für zwei Matrizen $A,B \in \mathbb{R}^{(n+1)\times(n+1)}$

$$\det(A - \lambda B) \;=\; \sum_{j=1}^{n+1} (-1)^{(j+1)} (\alpha_{1\,j} - \lambda\beta_{1\,j}) \det(A_{1\,j} - \lambda B_{1\,j})$$

wobei $A_{1\,j}$ und $B_{1\,j}$ die durch Weglassen der ersten Zeile und j–ten Spalte aus A bzw. B gebildeten $n \times n$ Matrizen darstellen. Nach Induktionsvorraussetzung sind die Determinanten $\det(A_{1\,j} - \lambda B_{1\,j})$ Polynome vom Grade höchstens n, so daß die Multiplikation mit den linearen Faktoren $(\alpha_{1\,j} - \lambda\beta_{1\,j})$ den Grad höchstens auf $n+1$ erhöhen kann. □

Algebraische Vielfachheit

Nach dem Fundamentalsatz der Algebra gibt es $k \leq n$ verschiedene Nullstellen λ_i der Vielfachheit p_i, so daß das charakteristische Polynom geschrieben werden kann als

$$P(\lambda) \;=\; (\lambda_1 - \lambda)^{p_1} (\lambda_2 - \lambda)^{p_2} \ldots (\lambda_k - \lambda)^{p_k}$$

mit $\sum\limits_{i=1}^{k} p_i \;=\; n$. Daraus folgt

$$\sum_{i=1}^{k} \lambda_i \;=\; Tr(A)\,, \qquad\qquad \prod_{i=1}^{k} \lambda_i^{p_i} \;=\; \det(A)\,.$$

Die Zahl $p_i > 0$ heißt die **algebraische Vielfachheit** des Eigenwertes λ_i.

Beispiel B.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

$$Tr(A) \;=\; 0 + 0 \;=\; 0 \;=\; \mathbf{i} - \mathbf{i} \quad \text{und} \quad \det(A) \;=\; 1 \;=\; \mathbf{i}\,(-\mathbf{i}) = -\mathbf{i}^2 = -(-1)$$

Dabei ist $\mathbf{i}$ die *imaginäre Einheit* der komplexen Zahlen.

Berechnung der Eigenvektoren

Die zu einem Eigenwert λ_i gehörenden Eigenvektoren $\mathbf{v}_i$ lassen sich als Lösungen des homogenen Gleichungssystems

$$(A - \lambda_i\, I)\mathbf{v} \;=\; 0$$

bestimmen. Sie bilden einen linearen Unterraum der Dimension

$$q_i \;\equiv\; \dim(kern(A - \lambda_i\, I)) \;=\; n - rang(A - \lambda_i\, I)$$

Die Zahl $q_i > 0$ heißt die **geometrische Vielfachheit** des Eigenwertes λ_i und ist immer kleiner oder gleich der algebraischen Vielfachheit p_i von λ_i:

$$q_i \leq p_i \quad \text{für} \quad i \;=\; 1 \ldots k\,.$$

Eigenwerte λ_i mit $q_i < p_i$ heißen **defekt**.

Zum Eigenwert λ_i kann man immer q_i linear unabhängige Vektoren finden, die den Unterraum $kern(A - I\lambda_i)$ aufspannen. Weiterhin gilt die folgende Aussage bezüglich verschiedener Eigenwerte.

Lemma B.5. *Die zu r verschiedenen Eigenwerten λ_i, $i = 1 \ldots r$, gehörenden Eigenvektoren $(\mathbf{v}_i)_{i\,=\,1\ldots r}$ 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 $(\mathbf{v}_i)_{i\,=\,1\ldots r}$ sei linear unabhängig, d.h.

$$\sum_{i=1}^{r} \gamma_i \mathbf{v}_i \;=\; 0 \quad \Longrightarrow \quad \gamma_1 = \cdots = \gamma_r = 0\,.$$

Induktionsschritt, r → r+1: Es gelte für geeignete Koeffizienten γ_i

$$\sum_{i=1}^{r+1} \gamma_i \mathbf{v}_i \;=\; 0\,.$$

Multiplikation mit der Matrix A bzw. dem Skalar λ_{r+1} liefert

$$0 \;=\; A \cdot 0 \;=\; A \cdot \sum_{i=1}^{r+1} \gamma_i \mathbf{v}_i \;=\; \sum_{i=1}^{r+1} \gamma_i\, A\mathbf{v}_i \;=\; \boxed{\sum_{i=1}^{r} \gamma_i \lambda_i \mathbf{v}_i} + \boxed{\gamma_{r+1}\lambda_{r+1}\mathbf{v}_{r+1}}$$

bzw.

$$0 \;=\; \lambda_{r+1} \cdot 0 \;=\; \lambda_{r+1} \cdot \sum_{i=1}^{r+1} \gamma_i \mathbf{v}_i \;=\; \boxed{\sum_{i=1}^{r} \gamma_i \lambda_{r+1} \mathbf{v}_i} + \boxed{\gamma_{r+1}\lambda_{r+1}\mathbf{v}_{r+1}}$$

Aus der Differenz dieser beiden Gleichungen fällt der letzte Term mit $\mathbf{v}_{r+1}$ ganz heraus:

$$0 \;=\; \sum_{i=1}^{r} \gamma_i (\lambda_{r+1} - \lambda_i) \mathbf{v}_i\,.$$

Laut Induktionsannahme sind die $\mathbf{v}_i$, $i \;=\; 1\ldots r$, linear unabhängig, also müssen die zusammengesetzten Koeffizienten $\gamma_i(\lambda_{r+1} - \lambda_i)$ alle gleich Null sein. Da die λ_i verschieden sind, gilt $\lambda_{r+1} - \lambda_i \neq 0$, $i = 1\ldots r$. Dies kann aber nur bedeuten, daß die Koeffizienten γ_i für $i \;=\; 1\ldots r$ und damit auch γ_{r+1} gleich Null sind. Also ist auch die um einen Eigenvektor erweiterte Familie $\mathbf{v}_i$, $i \;=\; 1\ldots r+1$, linear unabhängig. □

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

$$V \;=\; [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n] \in \mathbb{C}^{n\times n}$$

zusammen, welche auf Grund der linearen Unabhängigkeit ihrer Spaltenvektoren eine Inverse V^{-1} besitzt. Nun kann man die n Vektorgleichungen $A\mathbf{v}_i \;=\; \lambda_i \mathbf{v}_i$ mit Hilfe der Diagonalmatrix $\Lambda \;=\; diag(\lambda_i)_{i\,=\,1\ldots n}$ zur Matrixgleichung

$$A\,V \quad = \quad V\,\Lambda$$

kombinieren. Multipliziert man von links bzw. von rechts mit V^{-1} so erhält man die Darstellung

$$\Lambda \;=\; V^{-1} A\, V \qquad \text{bzw.} \qquad A \;=\; V\,\Lambda\, V^{-1}\,.$$

12.2 Eigenwerte bei speziellen Matrizen

Definition B.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.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 λ 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 $\bar{\lambda}$ genau dann ein Eigenwert von $\bar{A}$ und damit auch $\bar{A}^T$ ist, wenn λ ein Eigenwert von A ist.
Da für reelle Matrizen $A \;=\; \bar{A}$ gilt, ist für diese mit jedem λ auch $\bar{\lambda}$ ein Eigenwert. Das heißt:

Folgerung B.8 (Eigenwerte reeller Matrizen).
Alle Eigenwerte reeller Matrizen sind entweder reell oder treten als konjugiert–komplexe Paare $(\lambda,\,\bar{\lambda})$ ***auf.***

Hermitesche Matrizen
Für diese Klasse von Matrizen sind alle Eigenwerte reell und die Eigenvektoren können sogar orthogonal zueinander gewählt werden. Es gilt nämlich

$$A\mathbf{v} \;=\; \lambda\mathbf{v} \quad\Leftrightarrow\quad \bar{\mathbf{v}}^T\bar{A}^T \;=\; \bar{\lambda}\bar{\mathbf{v}}^T\,,$$

und somit folgt durch Multiplikation der linken Gleichung von links mit $\bar{\mathbf{v}}^T$ und entsprechend der rechten Gleichung mit $\mathbf{v}$ von rechts, daß

$$\bar{\mathbf{v}}^T A\mathbf{v} \;=\; \lambda\bar{\mathbf{v}}^T\mathbf{v} \;=\; \bar{\lambda}\bar{\mathbf{v}}^T\mathbf{v}\,,$$

wobei wir die Voraussetzung $\bar{A}^T \;=\; A$ benutzt haben. Da nun $\bar{\mathbf{v}}^T\mathbf{v} \;=\; |\mathbf{v}|^2$ nicht Null ist, gilt $\lambda \;=\; \bar{\lambda}$, und der Eigenwert λ muß deshalb reell sein.

12.3 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. Ausserdem erhält man dann 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.

12.4 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 Vorraussetzung dass $A = V\Lambda V^{-1}$ so dass insbesondere $A^j = V\Lambda^j V^{-1}$. Mit anderen Worten: Man kann V aus dem Matrixpolynom $Q_k(A)$ herausziehen, so dass dessen Verhalten gerade fuer grosse k durch $Q_k(\Lambda) = diag(Q_k(\lambda_j))_{j+1\ldots n}$ beschrieben ist.

12.5 Kanonische Jordanform

Einige Matrizen (wie zum Beispiel $\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$) lassen sich nicht in die Form $A = V\Lambda V^{-1}$ mit Diagonalmatrix Λ bringen. Vielmehr bleiben in Λ 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. Allerdings ist die entsprechende Matrix V^{-1} dann sehr gross und explodiert, wenn man ε immer kleiner macht.

Zusammenfassend bleibt festzustellen, dass die Eigenwertzerlegung $A = V\Lambda V^{-1}$ ein wesentlich kniffligeres Problem darstellt als die Lösung linearer Gleichungsysteme $Ax = b$.