M a t h e m a t i k 1

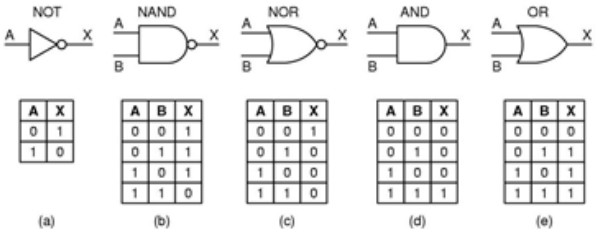
f ü r I n f o r m a t i k

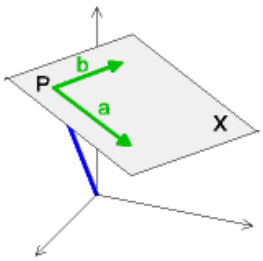
Grundlagen, Elemente der diskreten Mathematik und der linearen Algebra

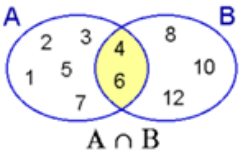
3. (korrigierte) Auflage Sommersemester 2020

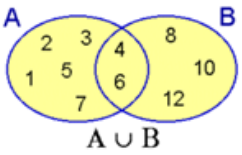
★

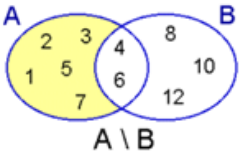
$$
\begin{aligned}
\det(\mathbf{A}-\lambda\mathbf{I}) &= \left|\begin{pmatrix} 2 & 0 & 1 \\ 0 & 3 & 1 \\ 0 & 6 & 2 \end{pmatrix} - \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}\right| \\
&= \begin{vmatrix} 2-\lambda & 0 & 1 \\ 0 & 3-\lambda & 1 \\ 0 & 6 & 2-\lambda \end{vmatrix} \\
&= (2-\lambda)\cdot\begin{vmatrix} 3-\lambda & 1 \\ 6 & 2-\lambda \end{vmatrix} \\
&= (2-\lambda)((3-\lambda)\cdot(2-\lambda)-1\cdot 6) \\
&= (\lambda-2)\lambda(\lambda-5)=0
\end{aligned}
$$

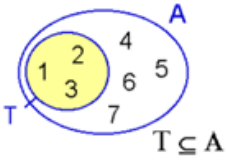












Prof. Dr. J. Kampmann, HS Osnabrück, Fakultät IuI

Inhaltsverzeichnis

1 Vorwort **3**
1.1 Vorwort zur 1. Auflage . . . 3
1.2 Vorwort zur 2. Auflage . . . 3
1.3 Vorwort zur 3. Auflage . . . 4

2 Literaturverzeichnis **4**

3 Mengen und Aussagen **5**
3.1 Mengen: Definitionen, Bezeichnungen und erste Eigenschaften . . . 5
3.2 Aussagen und Aussageformen: Definitionen und Bezeichnungen . . . 7
3.3 Aussageverknüpfungen: Rechenoperationen für Aussagen und Aussageformen . . . 9
3.4 Mengenalgebra: Rechenoperationen für Mengen . . . 11
3.5 Kartesische Produkte, Relationen und Abbildungen . . . 12

4 Zahlsysteme und algebraische Strukturen **19**
4.1 Einführung: Aufbau unseres Zahlsystems . . . 19
4.2 Die Menge $\mathbb{N}_0$ der natürlichen Zahlen mit Null und die Menge $\mathbb{N}$ . . . 20
4.2.1 Vollständige Induktion und rekursive (induktive) Definition . . . 22
4.2.2 Elementare Kombinatorik und endliche Summen . . . 24
4.3 Die Menge $\mathbb{R}$ der reellen Zahlen . . . 30
4.3.1 Die ganzen Zahlen $\mathbb{Z}$ . . . 30
4.3.2 Die rationalen Zahlen $\mathbb{Q}$: Brüche und Dezimaldarstellung rationaler Zahlen . . . 31
4.3.3 Dezimaldarstellung reeller Zahlen . . . 35
4.3.4 Exkurs: Maschinenzahlen . . . 36
4.3.5 Die Anordnung in $\mathbb{R}$ . . . 38
4.3.6 Weitere Rechenoperationen und Rechenregeln in $\mathbb{R}$ . . . 40
4.4 Algebraische Strukturen . . . 48
4.4.1 Halbgruppen und Gruppen . . . 49
4.4.2 Ringe . . . 49
4.4.3 Körper . . . 50

5 Elementare Zahlentheorie **51**
5.1 Einführung: Teilen in $\mathbb{Z}$ . . . 51
5.2 Der euklidische Algorithmus . . . 55
5.3 Modulare Arithmetik: Rechnen mit Restklassen . . . 57
5.4 Der Chinesische Restsatz . . . 63
5.5 Die Grundidee der RSA-Algorithmus . . . 66

6 Lineare Gleichungssysteme und der Gaußalgorithmus **72**
6.1 Einleitende Beispiele und Begriffe . . . 72
6.2 Klassifikation linearer Gleichungssysteme und die Struktur der Lösungsmenge . . . 79

6.3 Der Gaußalgorithmus 84
6.4 Das Gauß-Schema zur Formalisierung des Gauß-Algorithmus 93
6.5 Quadratische Gleichungssysteme 95
6.6 Übersicht zur Struktur der Lösungsmenge: Bedeutung von Rang und Corang 95

7 Vektoren und Vektorraum 96
7.1 Einführung 96
7.2 $\mathbb{R}^2$ und $\mathbb{R}^3$ als Punktmenge und Vektorraum 97
7.3 Anschauliche Deutung der Rechenoperationen im Vektorraum $\mathbb{R}^2$ und $\mathbb{R}^3$ 102
7.4 Weitere grundlegende Definitionen 104
7.5 Ebenen im Raum 107
7.6 Das Skalarprodukt 110
7.7 Das Kreuzprodukt/Vektorprodukt 119
7.8 Der Vektorraum $\mathbb{R}^n$ 129
7.9 Lineare Unabhängigkeit 130
7.9.1 Einführung 130
7.9.2 Linear unabhängige Vektoren, Linearkombination, Basis und Dimension 131
7.9.3 Basis und Komponentendarstellung 135

8 Matrizen 136
8.1 Der Begriff der Matrix 136
8.2 Rechnen mit Matrizen, das Matrizenprodukt 144
8.3 Quadratische Matrizen und die Umkehrmatrix (inverse Matrix) 148
8.4 Die Determinante 162
8.4.1 Einführung und Definition 162
8.4.2 Berechnung der Determinante mit dem Gauß-Algorithmus 167
8.5 Eigenwerte und Eigenvektoren 170
8.5.1 Einführung 170
8.5.2 Definitionen und Eigenwertberechnung 171
8.5.3 Berechnung der Eigenvektoren 172
8.6 Diagonalisierbarkeit von Matrizen 176

★

1 Vorwort

1.1 Vorwort zur 1. Auflage

Dieses **Skript zu „Mathematik 1 für Informatik “** dient zum Gebrauch **neben** der Vorlesung. Es ist kein Ersatz für die Vorlesung und auch keine identische Vorlage: **Ich lese nicht dieses Skript vor!**
Die Vorlesung wird weitere Beispiele, ergänzende Erläuterungen und Herleitungen und viele weiterführende Bemerkungen enthalten.

Ergänzend zu diesem Skript schlage ich **Lehrbücher** also Literatur vor. Lehrbücher anderer Autoren sprechen die Themen der Vorlesung oft in anderer Form und mit anderen/weiteren Beispielen an. Beschäftigung mit diesen Büchern wird Ihr Verständnis fördern und Ihren Zugang zur Mathematik erleichtern und erweitern. Oft werden andere Autoren Themen für Sie besser anders/präsentieren als ich. Ich beanspruche nicht, das pädagogisch-didaktische oder mathematische Nonplusultra zu sein. Vielleicht kommen Sie persönlich mit der Darstellung anderer Autoren besser klar! Versuchen Sie es!

Mathematik lernt man (wie z.B. auch das Spielen eines Instruments oder die Beherrschung einer Sportart) nur durch selber Üben!
Die Münze, mit der Sie dafür zahlen, ist Ihre Zeit! Ohne Investition von Zeit zum Üben wird es nicht gehen.
Damit ist Zeit außerhalb der Vorlesung und der Übungsgruppe gemeint, also Ihre Arbeitszeit jenseits der Präsenzveranstaltungen der Hochschule.

Was soll dieses Skript leisten?
Ich möchte Ihnen einen halbwegs strukturierten Aufbau des **Gedankengebäudes der Mathematik** vorstellen, nicht für Mathematiker (das wäre noch viel formaler und stringenter) sondern für Anwender. Außerdem sollen Sie einen Einblick in **mathematisches Argumentieren** im Sinn einer plausiblen Herleitung mathematischer Aussagen (nicht im strengen Sinn des mathematischen Beweises) bekommen. Last but not least sollen Sie **das mathematische Handwerkszeug für Ihr weiteres Studium und Berufsleben** dargestellt bekommen und **Methoden zum Weiterlernen** beim Umgang mit (formalen) Systemen innerhalb und außerhalb der Mathematik kennenlernen.

Fehler bleiben beim Schreiben eines Skripts nicht aus! Daher nehmen ich gerne Hinweise auf Fehler (inhaltlich und Druckfehler), Vorschläge für bessere Darstellungen und weitere Anregungen entgegen; eine Email an j.kampmann@hs-osnabrueck.de reicht aus.

1.2 Vorwort zur 2. Auflage

In der **2. Auflage** zum Wintersemester 2019/20 werden Druckfehler, Setzfehler und kleine Unstimmigkeiten verbessert. Ich danke allen Hinweisgebern!

Erweitert bzw. ergänzt werden die Abschnitte zu Teilen in $\mathbb{Z}$, zu Relationen, zum chinesischen Restsatz, zum Gauß-Schema bei linearen Gleichungssystemen, zum erweiterten Gauß-Schema bei der Matrixinversion und zu Eigenwerten und Eigenvektoren quadratischer Matrizen.

Neu ist ein Abschnitt zum RSA-Algorithmus der Kryptographie. Dieser Abschnitt enthält auch den Satz von Euler und den „kleinen“ Satz von Fermat aus der Zahlentheorie.

Die Kapitel 3 und 4 erscheinen Anfängern in der Regel unnötig formal. Sie dienen aber der **Hinführung zu mathematischem Denken, Argumentieren und Schreiben**!
Sie sollen in die Lage versetzt werden, Ihr mathematisches Handeln zu begründen.
Wer sich darauf einlässt, wird sich schnell daran gewöhnen und auch die Vorteile erkennen.

1.3 Vorwort zur 3. Auflage

Auch für die **3. Auflage** wurden Darstellungsfehler und kleiner Unstimmigkeiten bereinigt. Dafür danke ich insbesondere den Kollegen Prof. Dr. Frank M. Thiesing und Dipl.-Math. Jana Meyer.

Für Hinweise auf Fehler und Unstimmigkeiten bin ich weiterhin dankbar!

2 Literaturverzeichnis

Hier erhalten Sie eine kleine Auswahl eines riesigen Angebots an Lehrbuchliteratur zur Mathematik. Die Reihenfolge stellt keine Wertung dar. Sie können im Bibliothekskatalog der Hochschulbibliothek nach weiteren Angeboten suchen!
Die hier aufgeführten Bücher bekommen Sie über die Hochschulbibliothek **innerhalb des Hochschulnetzes zum freien Download als pdf-Datei** angeboten! Man kann also auch ohne Papier auf PC, Tablet, Notebook u.ä. lesen.

1) S. Goebbels, S. Richter
Mathematik verstehen und anwenden
Springer Verlag, 2. Aufl.

2) T. Arens, F. Hettlich, C. Karpfinger, U. Kockelkorn, K. Lichtenegger, H. Stachel
Mathematik
Springer Spektrum , 3. Aufl.

3) S. Iwanowski, R. Lang
Diskrete Mathematik mit Grundlagen
Springer Vieweg

4) K.-U. Witt
Lineare Algebra für die Informatik
Springer Vieweg

5) S. Goebbels, J. Rethmann
Mathematik für Informatiker
Springer Vieweg

6) A. Beutelspacher, M.-A. Zschiegner
Diskrete Mathematik für Einsteiger Springer Spektrum 5. Aufl.

7) S. Dreiseitl
Mathematik für Software Engineering
Springer Vieweg

3 Mengen und Aussagen

3.1 Mengen: Definitionen, Bezeichnungen und erste Eigenschaften

Zunächst werden grundlegende Begriffe der Mathematik und Redeweisen mathematischen Argumentierens eingeführt und vorgestellt.
Es handelt sich dabei um Begriffe und Verfahren aus der **elementaren Mengenlehre** und der **elementaren Aussagenlogik**.

Definition: (G. Cantor, 1845-1918)
Eine **Menge** ist eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen. Die Objekte, die zu einer Menge gehören, nennt man **Elemente** der Menge.

Mengen werden durch **Aufzählung ihrer Elemente** eingeschlossen in sogenannte Mengenklammenn {} angegeben, zur Bezeichnung verwendet man in der Regel Großbuchstaben.

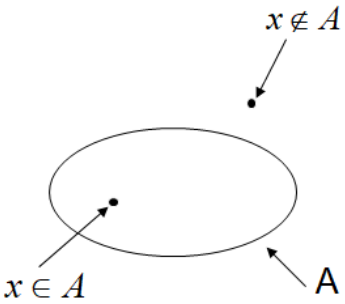
Beispiel: $M = \{a, b, c\}$ oder $K = \{\text{Hund, Katze, Affe, Maus}\}$.

Wenn ein Element x zur Menge A gehört, schreibt man $x \in A$.

Wenn ein Element x **nicht** zur Menge A gehört, schreibt man $x \notin A$.

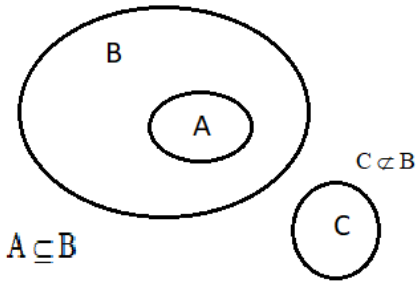
Beispiel: $M = \{a, b, c\}$ und $a \in M$, $u \notin M$ oder $K = \{\text{Hund, Katze, Affe, Maus}\}$ und $Tiger \notin K$.

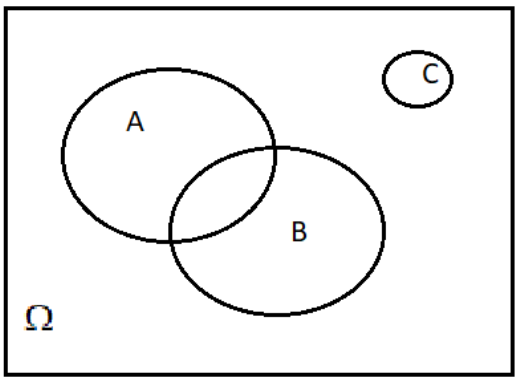
Zur grafischen Darstellung von Mengen und Beziehungen zwischen Mengen werden **Venn-Diagramme(J. Venn, 1834-1923)** verwendet, bei denen Mengen durch berandete Flächen dargestellt werden:



Definition: (B. Russell, 1872-1970)

1. Die Menge, die kein Element enthält, heißt **leere Menge**, man schreibt dafür $\emptyset$.
2. Eine **Menge A heißt Teilmenge der Menge B**, wenn jedes Element aus A auch Element von B ist (auch zu B gehört), man schreibt dann $A \subseteq B$.
Ist A nicht Teilmenge von B, schreibt man $A \not\subseteq B$.
3. Die **Allmenge** Ω ist die Menge aus allen im behandelten Themenumfeld betrachteten Objekten. Alle in diesem Themenumfeld betrachteten Mengen sind Teilmenge der Allmenge.
4. Die leere Menge $\emptyset$ ist Teilmenge jeder Menge.





Bemerkungen zur Mengengleichheit und Teilmengenbeziehung:

1. Zwei **Mengen** A und B **sind gleich**, geschrieben A=B, falls gilt: $A \subseteq B$ und $B \subseteq A$.

2. A ist **echte Teilmenge von B**, geschrieben $A \subset B$, falls gilt: $A \subseteq B$ und $A \neq B$.

3. Die **Menge aller Teilmengen** einer Menge B heißt **Potenzmenge von B**, man schreibt dafür: $\mathbb{P}(B) = \{A | A \subseteq B\}$. Es gilt immer $\emptyset \in \mathbb{P}(B)$ und $B \in \mathbb{P}(B)$.

Beispiel:

a) $A = \{a, b, c, d\}$ dann gilt: $A \subseteq A$, $\emptyset \subseteq A$, $\{a, b\} \subset A$.

b) $B = \{1, 2, 3\} \Rightarrow \mathbb{P}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, B\}$.

Zahlenmengen:
Ein wesentlicher Gegenstand der Mathematik sind Zahlen. Wir betrachten zunächst folgende **Mengen von Zahlen**:

a) Die Menge der **natürlichen Zahlen** $\mathbb{N} = \{1, 2, 3, \dots\}$

b) Die Menge der **natürlichen Zahlen mit Null** $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$

c) Die Menge der **ganzen Zahlen** $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

d) Die Menge der **rationalen Zahlen** $\mathbb{Q} = \{\frac{z}{n} | z \in \mathbb{Z} \wedge n \in \mathbb{N}\}$, z heißt **Zähler**, n heißt **Nenner**.

e) Es gilt $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$.

3.2 Aussagen und Aussageformen: Definitionen und Bezeichnungen

Definition:
Eine **Aussage** ist ein Satz einer menschlichen oder künstlichen Sprache, dem **eindeutig und unmissverständlich** genau einer der beiden **Wahrheitswerte „wahr“ (w bzw. 1)** oder **„falsch“ (f bzw. 0)** zugeordnet werden kann. Die **Nullaussage 0** ist immer falsch; die **Einsaussage 1** ist immer wahr.

Auch zur Bezeichnung von Aussagen verwendet man in der Regel Großbuchstaben. **Aussagen sind durch ihre Wahrheitswerte eindeutig bestimmt**.

Beispiele:

sprachlicher Ausdruck	Bewertung
Der Mond ist ein Trabant der Erde	Aussage, wahr
Borussia Dortmund ist die beste Fußballmannschaft	keine Aussage, Privatmeinung
In $\mathbb{Z}$ gilt: 2+3=-6	Aussage, falsch
Alle Primzahlen sind ungerade	Aussage, falsch
Der Sommer 2018 war überdurchschnittlich warm	Aussage, wahr
Der nächste Sommer wird noch wärmer als 2018	keine Aussage, Prognose
Bier schmeckt gut	keine Aussage, Privatmeinung

Definition:
Eine **Aussageform** ist ein Satz einer menschlichen oder künstlichen Sprache mit **mindestens einer Variablen (Veränderlichen)**, der zu einer Aussage wird, wenn die Variable durch einen konkreten Wert (eine Konstante) ersetzt wird. Die Menge der für die Variablen zulässigen Werte heißt **Definitionsbereich** oder **Definitionsmenge** der Aussageform. Aussageformen werden mit Großbuchstaben gefolgt von der Angabe der Variablen in runden Klammern angegeben.

Man schreibt z.B. $A(x)$ für die Aussageform A mit der Variablen x.

Beispiel:

Aussageform $A(x)$ = x ist ein Säugetier mit Definitionsbereich D = Menge aller Lebewesen.

Anwendung zur Definition von Mengen:
Mit Hilfe einer Aussageform $A(x)$ kann man auch Mengen angeben:
$M = \{x \in \Omega \mid A(x) \text{ ist wahr}\}$. Man nennt die Aussageform $A(x)$ dann auch die **charakterisierende Eigenschaft** der zugehörigen Menge.

Beispiele:

a) $G = \{x \in \mathbb{Z} \mid \text{x ist gerade}\}$

b) $S = \{x \in \Omega \mid \text{x ist an der HS Osnabrück als Studierende(r) eingeschrieben}\}$ mit Ω = Menge aller Menschen.

3.3 Aussageverknüpfungen: Rechenoperationen für Aussagen und Aussageformen

Definition:
Aussagen und Aussageformen werden durch **logische Operatoren (Junktoren)** miteinander verbunden. Diese Verbindungen nennt man **Aussageverknüpfungen**. Grundlegende **logische Operatoren (auch elementare Aussageverknüpfungen genannt)** sind:

1. die **Negation** (Verneinung): $\neg A$ oder $\overline{A}$
2. die **Konjunktion** (und-Verknüpfung): $A \wedge B$
3. die **Disjunktion** (oder-Verknüpfung): $A \vee B$
4. die **Implikation** (wenn-dann-Verknüpfung): $A \Rightarrow B$
5. die **Äquivalenz** (genau dann-wenn-Verknüpfung): $A \Leftrightarrow B$ oder $A = B$

Die Negation ist eine **einstellige Verknüpfung** (an der Verknüpfung ist nur eine Aussage beteiligt). Konjunktion, Disjunktion, Implikation und Äquivalenz sind **zweistellige Verknüpfungen** (zwei Aussagen werden miteinander verknüpft).
Allgemein: Werden n Ausssagen miteinander verknüpft, spricht man von einer **n-stellige Verknüpfung** oder **n-stelligen Binärfunktion**.

Eine Aussageverknüpfung ist eindeutig bestimmt, wenn ihr Wahrheitswert (Outputgröße) in Abhängigkeit vom Wahrheitswert der beteiligten Aussagen (Inputgrößen) festliegt. Dazu verwendet man Wahrheitstafeln/Wahrheitstabellen.

Die **elementaren Aussageverknüpfungen** sind durch folgende Wahrheitstafel eindeutig festgelegt:

A	B	$\neg A(\overline{A})$	A∧B	A∨B	A⇒ B	A⇔ B
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

Die folgende tabellarische Übersicht zeigt die **Rechengesetze der Aussagenlogik**

Name	und ($\wedge$)	oder ($\vee$)
Kommutativgesetz	$A \wedge B \Leftrightarrow B \wedge A$	$A \vee B \Leftrightarrow B \vee A$
Assoziativgesetz	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$	$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
Existenz neutraler Elemente	$A \wedge \mathbf{1} \Leftrightarrow A$	$A \vee \mathbf{0} \Leftrightarrow A$
Existenz komplementärer Elemente	$A \wedge \overline{A} \Leftrightarrow \mathbf{0}$	$A \vee \overline{A} \Leftrightarrow \mathbf{1}$
Distributivgesetze	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
DeMorgansche Regeln	$\overline{A \wedge B} \Leftrightarrow \overline{A} \vee \overline{B}$	$\overline{A \vee B} \Leftrightarrow \overline{A} \wedge \overline{B}$

Bemerkungen und „Sprachregelungen“ zur Aussagenlogik:

1. Die Aussage **„für alle $x \in A$ gilt...“** wird abgekürzt durch: $\forall x \in A$:

2. Die Aussage **„es gibt mindestens ein $x \in A$, für das gilt...“** wird abgekürzt durch: $\exists x \in A$:

3. Die Aussage **„es gibt genau ein $x \in A$, für das gilt...“** wird abgekürzt durch: $\exists! x \in A$:
   Die Symbole $\forall, \exists$ heißen **Quantoren**, genauer:
   $\forall$ **Allquantor** und $\exists$ **Existenzquantor**.

4. Eine Aussageverknüpfung, an der n Aussagen als „Input“ beteiligt sind, nennt man auch n-stellige Binärfunktion.

5. Eine Aussage, die **immer** den Wahrheitswert **w** hat, heißt **Tautologie**.
   Auf Tautologien beruhen die meisten mathematischen Beweisverfahren.

6. Für die **doppelte Verneinung** gilt: $\neg(\neg A) \Leftrightarrow A$.

Einige logische Äquivalenzen und Grundlagen mathematischer Beweise:

1. Implikation und Äquivalenz:
   $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$

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

2. Äquivalenz für die Implikation:
   $(A \Rightarrow B) \Leftrightarrow (\overline{A} \vee B)$

A	B	$\overline{A}$	$A \Rightarrow B$	$\overline{A} \vee B$	$(A \Rightarrow B) \Leftrightarrow (\overline{A} \vee B)$
w	w	f	w	w	w
w	f	f	f	f	w
f	w	w	w	w	w
f	f	w	w	w	w

3. Kontraposition:
   $(A \Rightarrow B) \Leftrightarrow (\overline{B} \Rightarrow \overline{A})$

A	B	$\overline{A}$	$\overline{B}$	$A \Rightarrow B$	$\overline{B} \Rightarrow \overline{A}$	$(A \Rightarrow B) \Leftrightarrow (\overline{B} \Rightarrow \overline{A})$
w	w	f	f	w	w	w
w	f	f	w	f	f	w
f	w	w	f	w	w	w
f	f	w	w	w	w	w

4. Modus ponens:
   $(A \wedge (A \Rightarrow B)) \Rightarrow B$

A	B	$A \Rightarrow B$	$(A \wedge (A \Rightarrow B)$	$(A \wedge (A \Rightarrow B) \Rightarrow B$
w	w	w	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	w

5. Modus tollens:
   $(\overline{B} \wedge (A \Rightarrow B)) \Rightarrow \overline{A}$

A	B	$\overline{A}$	$\overline{B}$	$A \Rightarrow B$	$(\overline{B} \wedge (A \Rightarrow B)$	$(\overline{B} \wedge (A \Rightarrow B) \Rightarrow \overline{A}$
w	w	f	f	w	f	w
w	f	f	w	f	f	w
f	w	w	f	w	f	w
f	f	w	w	w	w	w

Aus 2. und 1. folgt:
$(A \Rightarrow B) \Leftrightarrow (\overline{A} \vee B)$ und $(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$ und damit
$(A \Leftrightarrow B) \Leftrightarrow (\overline{A} \vee B) \wedge (\overline{B} \vee A))$
Es reichen also die Verneinung, die Konjunktion und die Disjunktion um alle Aussageverknüpfungen zu erzeugen.

3.4 Mengenalgebra: Rechenoperationen für Mengen

Im Folgenden wird vorausgesetzt, dass **alle vorkommenden Mengen Teilmengen einer gegebenen Allmenge** Ω sind. Dann erhält man mittels logischer Verknüpfungen folgende „Rechenregeln“ für Mengen (Mengenoperationen).

Definition:
Die **elementaren Mengenoperationen** sind definiert durch:

1. Die Vereinigung $A \cup B$: $x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B)$
2. Der Durchschnitt $A \cap B$: $x \in A \cap B \Leftrightarrow (x \in A) \wedge (x \in B)$
3. Die Differenz $A \backslash B$: $x \in A \backslash B \Leftrightarrow (x \in A) \wedge (x \notin B)$
4. Das (Mengen-)Komplement $\overline{A}$: $x \in \overline{A} \Leftrightarrow x \notin A$ genauer: $x \in \Omega \backslash A$.

Man nennt diese elementaren Rechenoperationen für Mengen auch **boolsche Operationen (G. Boole, 1815-1864)**.

Folgerung und Bemerkung:

Aus 3. und 4. folgt: $x \in A \backslash B \Leftrightarrow x \in A \wedge x \notin B \Leftrightarrow x \in A \wedge x \in \overline{B} \Leftrightarrow x \in A \cap \overline{B}$
Es gilt also: $A \backslash B = A \cap \overline{B}$

Zwei Mengen A, B heißen **disjunkt**, wenn ihr Durchschnitt die leere Menge ist: $A \cap B = \emptyset$

Beispiele:

a) $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, mit $\Omega = \mathbb{Z}$: $\overline{\mathbb{N}_0} = \{\ldots, -3, -2, -1\}$

b) $A = \{-3, -2, -1, -\frac{1}{2}, 0, 1, 2, \frac{5}{2}, 12\}$ und $B = \{-2, -3, 12, 0, 20, -100\} \Rightarrow$

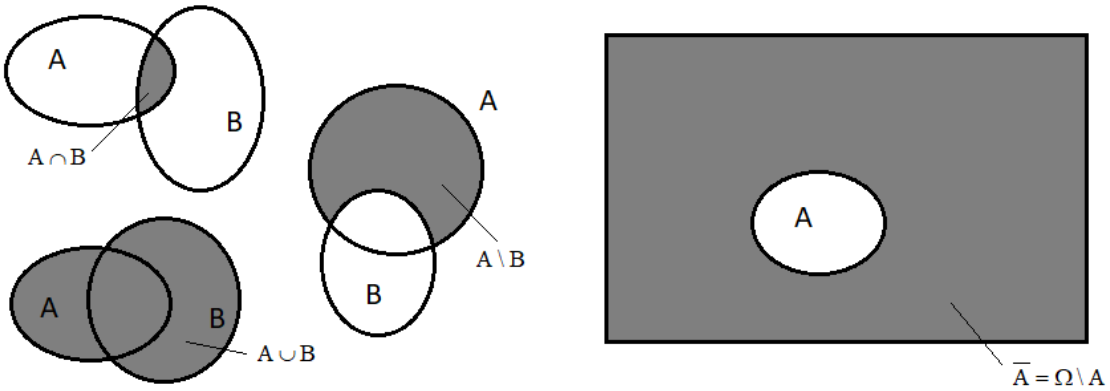
$A \backslash B = \{-1, -\frac{1}{2}, 1, 2, \frac{5}{2}\}$

c) $A \cap \mathbb{Z} = \{-3, -2, -1, 0, 1, 2, 12\}$

d) $A \cap \mathbb{N} = \{1, 2, 12\}$

Die folgende tabellarische Übersicht zeigt die **Rechengesetze der Mengenlehre**

Name	Durchschnitt ($\cap$)	Vereinigung ($\cup$)
Kommutativgesetz	$A \cap B \Leftrightarrow B \cap A$	$A \cup B \Leftrightarrow B \cup A$
Assoziativgesetz	$A \cap (B \cap C) \Leftrightarrow (A \cap B) \cap C$	$A \cup (B \cup C) \Leftrightarrow (A \cup B) \cup C$
Existenz neutraler Elemente	$A \cap \Omega \Leftrightarrow A$	$A \cup \emptyset \Leftrightarrow A$
Existenz komplementärer Elemente	$A \cap \overline{A} \Leftrightarrow \emptyset$	$A \cup \overline{A} \Leftrightarrow \Omega$
Distributivgesetze	$A \cap (B \cup C) \Leftrightarrow (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) \Leftrightarrow (A \cup B) \cap (A \cup C)$
DeMorgansche Regeln	$\overline{A \cap B} \Leftrightarrow \overline{A} \cup \overline{B}$	$\overline{A \cup B} \Leftrightarrow \overline{A} \cap \overline{B}$



3.5 Kartesische Produkte, Relationen und Abbildungen

Definition:

1. Gegeben sind zwei Mengen A und B. Das **kartesische Produkt (die Produktmenge)** ist definiert durch:

$$A \times B = \{(a, b) |\ a \in A \wedge b \in B\}$$

$(a, b) \in A \times B$ heißt **geordnetes Paar (geordnetes 2-Tupel)**.
(a, b) hat die **1. Komponente** $a \in A$ und die **2. Komponente** $b \in B$. Geordnetes Paar besagt, dass die Reihenfolge der Komponenten relevant ist.
Im Fall $A = B$ schreibt man $A^2 = A \times A$.

2. Gegeben sind n Mengen $A_1,\ A_2, \ldots, A_n$. Das **n-fache kartesische Produkt** ist definiert durch

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) |\ a_i \in A_i,\ 1 \leq i \leq n\}$$

$(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \ldots \times A_n$ heißt **geordnetes n-Tupel**.
$(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \ldots \times A_n$ hat die **i-te Komponente** $a_i \in A_i$ für $1 \leq i \leq n$.
Geordnetes n-Tupel besagt, dass die Reihenfolge der Komponenten relevant ist.
Im Fall $A_i = A$ für $1 \leq i \leq n$ schreibt man $A^n = A_1 \times A_2 \ldots \times A_n = \underbrace{A \times A \ldots \times A}_{n-mal}$.

Beispiele:

a) $V = \{\text{Willi, Otto}\}$, $N = \{\text{Schmidt, Meier}\} \Rightarrow$
$V \times N = \{\text{(Willi,Schmidt),(Willi,Meier),(Otto,Schmidt),(Otto,Meier)}\}$

b) $A = \{-3, -2, -1\}$ und $B = \{a, b, c\} \Rightarrow$
$A \times B = \{(-1, a), (-1, b), (-1, c), (-2, a), (-2, b), (-2, c), (-3, a), (-3, b), (-3, c)\}$
$B \times A = \{(a, -1), (a, -2), (a, -3), (b, -1), (b, -2), (b, -3), (c, -1), (c, -2), (c, -3)\} \Rightarrow$
es gilt: $A \times B \neq B \times A$.

c) $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(x, y) \mid x \in \mathbb{Z} \wedge y \in \mathbb{Z}\}$

d) $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R} \wedge y \in \mathbb{R}\}$

Definition:

1. Gegeben sind zwei Mengen A und B. Jede Teilmenge $R \subseteq A \times B$ ist eine **(zweistellige) Relation** über A, B.
Wenn $A = B$ gilt spricht man von einer zweistelligen Relation über A.

2. Gegeben sind n Mengen $A_1,\ A_2, \ldots, A_n$. Jede Teilmenge $R \subseteq A_1 \times A_2 \times \ldots \times A_n$ ist eine **(n-stellige) Relation** über $A_1,\ A_2, \ldots, A_n$.
Wenn $A_1 = A_2 = \ldots A_n$ gilt spricht man von einer n-stelligen Relation über A.

Einige besonders wichtige Arten von Relationen

Definition:
Eine (zweistellige) Relation $R \subseteq A \times A$, $A \neq \emptyset$ heißt **Äquivalenzrelation**, falls gilt:

1. Die Relation ist **reflexiv**, d.h. $(a, a) \in R \; \forall a \in A$.
2. Die Relation ist **transitiv**, d.h. $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.
3. Die Relation ist **symmetrisch**, d.h. $(a, b) \in R \Rightarrow (b, a) \in R$.

Definition:
Eine (zweistellige) Relation $R \subseteq A \times A$, $A \neq \emptyset$ heißt **Ordnungsrelation**, falls gilt:

1. Die Relation ist **reflexiv**, d.h. $(a, a) \in R \; \forall a \in A$.
2. Die Relation ist **transitiv**, d.h. $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.
3. Die Relation ist **antisymmetrisch**, d.h. $(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$.

Bemerkung: Eine Relation $R \subseteq A \times A$ ist **antisymmetrisch**, falls gilt:
$(a, b) \in R \wedge a \neq b \Rightarrow (b, a) \notin R$.

Beispiele:

1. Die (zweistellige) Relation $KG \subseteq \mathbb{N}_0 \times \mathbb{N}_0$ ist definiert durch
   $(a, b) \in KG \Leftrightarrow \exists n \in \mathbb{N}_0$ mit: $b = a + n$
   KG ist die „Kleiner-Gleich-Relation“: $(a, b) \in KG \Leftrightarrow a \leq b$. Diese Relation ist **reflexiv, transitiv und antisymmetrisch** also eine **Ordnungsrelation**.
2. Die (zweistellige) Relation $G \subseteq \mathbb{N}_0 \times \mathbb{N}_0$ ist definiert durch
   $(a, b) \in G \Leftrightarrow a = b$
   G ist die „Gleich-Relation“: $(a, b) \in G \Leftrightarrow a = b$. Diese Relation ist **reflexiv, transitiv und symmetrisch** also eine **Äquivalenzrelation**.
3. Die (zweistellige) Relation $K \subseteq \mathbb{N} \times \mathbb{N}$ ist definiert durch
   $(a, b) \in K \Leftrightarrow \exists n \in \mathbb{N}$ mit: $b = a + n$
   K ist die „Kleiner-Relation“: $(a, b) \in K \Leftrightarrow a < b$. Diese Relation ist **transitiv** aber **weder reflexiv noch symmetrisch** also keine der oben definierten besonderen Arten von Relationen.
4. Die drei Relationen K, KG, G sind analog als (zweistellige) Relationen über $\mathbb{Z}$ bzw. $\mathbb{Q}$ definiert.

Bezeichnungen:
Bei zweistelligen Relationen R über A (also $R \subseteq A \times A$)) schreibt man statt $(a, b) \in R$ auch aRb oder $a \sim b$ oder $a \equiv b$ oder definiert ein eigenes Zeichen wie z.B. $\leq$, also $a \leq b$ für $(a, b) \in KG$ aus dem 1. Beispiel.

Ein weiteres kleines Beispiel soll den Relationsbegriff einüben.

Beispiel:
Gegeben ist die Menge $A = \{a, b, c, d, e\}$ und die Relation
$R \subseteq A \times A = \{(a, a), (c, c), (a, b), (b, d), (e, e)\}$

1) Ergänzen Sie R zu R_1, so dass R_1 eine **Äquivalenzrelation** mit $R \subseteq R_1$ ist.

   Eine Äquivalenzrelation muss reflexiv, symmetrisch und transitiv sein:
   reflexiv: $(a, a), (b, b), (c, c), (d, d), (e, e) \in R_1$
   symmetrisch: $(a, b) \in R_1 \Rightarrow (b, a) \in R_1$ und $(b, d) \in R_1 \Rightarrow (d, b) \in R_1$
   transitiv: $(a, b) \in R_1 \wedge (b, d) \in R_1 \Rightarrow (a, d) \in R_1$
   symmetrisch: $(a, d) \in R_1 \Rightarrow (d, a) \in R_1$
   Damit insgesamt
   $R_1 = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (b, d), (d, b), (a, d), (d, a)\}$

2) Ergänzen Sie R zu R_2, so dass R_2 eine **Ordnungsrelation** mit $R \subseteq R_2$ ist.

   Eine Ordnungsrelation muss reflexiv, antisymmetrisch und transitiv sein:
   reflexiv: $(a, a), (b, b), (c, c), (d, d), (e, e) \in R_2$
   antisymmetrisch: $(a, b) \in R_2 \Rightarrow (b, a) \notin R_2$ und $(b, d) \in R_2 \Rightarrow (d, b) \notin R_2$
   transitiv: $(a, b) \in R_2 \wedge (b, d) \in R_2 \Rightarrow (a, d) \in R_2$
   antisymmetrisch: $(a, d) \in R_2 \Rightarrow (d, a) \notin R_2$
   Damit insgesamt $R_2 = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, d), (a, d)\}$

Äquivalenzrelationen und Äquivalenzklassen

Gegeben ist eine Äquivalenzrelation R über A, also eine reflexive, transitive und symmetrische Relation $R \subseteq A \times A$.

Definition:

1. Falls für $a, b \in A$ gilt: $(a, b) \in R$, sagt man: b ist **äquivalent** zu a.
2. Für $a \in R$ ist die **Äquivalenzklasse** $[a]$ (oder auch $\overline{a}$) definiert durch: $[a] = \overline{a} = \{b \in A \mid (a, b) \in R\}$. Die Äquivalenzklasse $[a] = \overline{a}$ ist also die Menge aller Elemente $b \in A$, die bezüglich der Relation R äquivalent zu a sind.

Beispiel:

$S = \{s \mid s$ ist Studierende(r) der Fakultät IuI$\}$. Die Relation $R \subseteq S \times S$ ist gegeben durch: $(a, b) \in R \Leftrightarrow a$ und b sind im selben Studiengang der Fakultät IuI.
R ist eine Äquivalenzrelation, denn $(a, a) \in R \, \forall a \in S$ (Reflexivität), $(a, b) \in R \Rightarrow (b, a) \in R$ (Symmetrie) und $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$ (Transitivität).

Wenn m (irgend)ein(e) Studierende(r) der Medieninformatik an der Fakultät IuI ist, dann ist die Äquivalenzklasse gegeben durch:
$[m] = \overline{m} = \{s \in S \mid (m, s) \in R\} =$
$\{s \in S \mid s$ studiert im Studiengang Medieninformatik der Fakultät IuI$\}$.
Die **Äquivalenzklassen** der Relation R entsprechen also den **Mengen der Studierenden eines Studiengangs der Fakultät IuI**.

Satz:
Für Äquivalenzklassen $[a], [b]$ mit $a, b \in A$ einer **Äquivalenzrelation** $R \subseteq A \times A$ gilt: Entweder ist $[a] \cap [b] = \emptyset$ oder $[a] = [b]$, d.h. **zwei Äquivalenzklassen sind entweder gleich oder disjunkt**.
Beweis:
Falls gilt $[a] \cap [b] \neq \emptyset$, gilt für jedes $x \in [a] \cap [b]$:
$x \in [a] \wedge x \in [b] \Rightarrow (a, x) \in R \wedge (b, x) \in R \Rightarrow$ (Symmetrie der Äquivalenzrelation)$(a, x) \in R \wedge (x, b) \in R \Rightarrow$ (Transitivität der Äquivalenzrelation)$(a, b) \in R \Rightarrow b \in [a]$
Völlig analog erhält man auch $a \in [b]$ und damit $[a] = [b]$.

Definition:
Gegeben ist eine (nichtleere) Menge A. Eine **(vollständige) Partition P** von A ist eine Menge von Teilmengen von A, also $P \subseteq \mathbb{P}(A)$ mit folgenden Eigenschaften:

1) A ist die Vereinigung aller Mengen aus P: $A = \bigcup_{B \in P} B$.

2) Voneinander verschiedene Mengen aus P sind disjunkt: $B_1, B_2 \in P \wedge B_1 \neq B_2 \Rightarrow B_1 \cap B_2 = \emptyset$.

Es gilt:

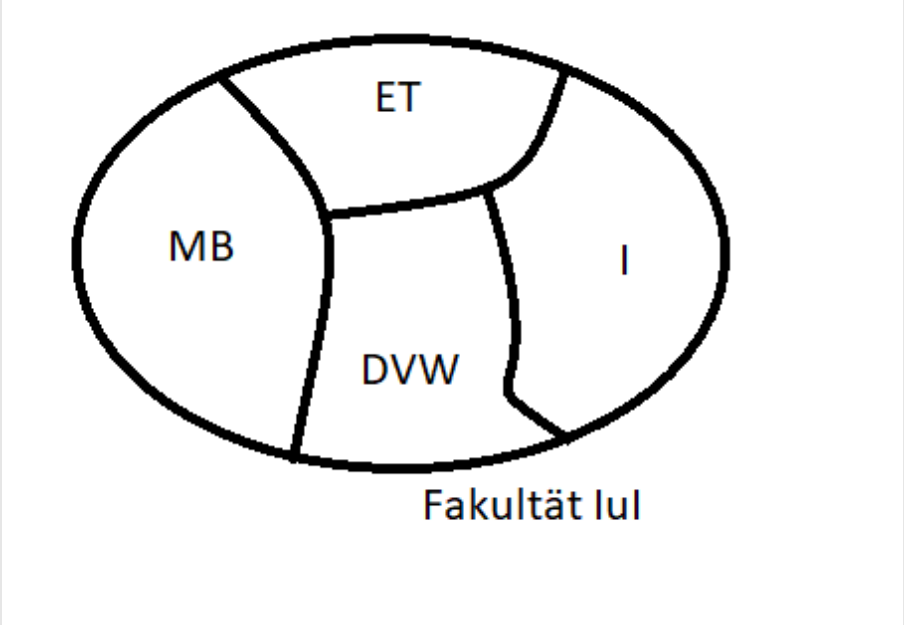
Zwei verschiedene Äquivalenzklassen einer Äquivalenzrelation $R \subseteq A \times A$ über A sind disjunkt. Wegen $(a, a) \in R \; \forall a \in A$ gilt $A = \bigcup_{a \in A} [a]$. Die **Menge aller Äquivalenzklassen** der Äquivalenzrelation $R \subseteq A \times A$ über A ist damit eine (vollständige) Partition von A.

Beispiel:

$S = \{s \mid s$ ist Studierende(r) der Fakultät IuI$\}$. Die Relation $R \subseteq S \times S$ ist gegeben durch: $(a, b) \in R \Leftrightarrow a$ und b sind im selben Studiengang der Fakultät IuI.
R ist eine Äquivalenzrelation, die **Äquivalenzklassen** sind:
$[MB] = \{s \in S \mid s$ studiert im Studiengang Maschinenbau$\}$
$[ET] = \{s \in S \mid s$ studiert im Studiengang Elektrotechnik$\}$

$[I] = \{s \in S \mid s \text{ studiert im Studiengang Informatik}\}$
$[DVW] = \{s \in S \mid s \text{ studiert im Studiengang Dental-/Verfahrens-/Werkstofftechnik}\}$

Das folgende Bild zeigt die zugehörige (vollständige) Partition $P = \{[MB], [ET], [I], [DVW]\}$ der Menge der Studierenden der Fakultät IuI an der Hochschule Osnabrück.



Ordnungsrelationen werden bei der **Anordnung** reeller Zahlen ins Spiel kommen, **Äquivalenzrelationen** werden in der **elementaren Zahlentheorie** eine Rolle spielen.

Mit Relationen kann man ebenfalls „rechnen"; dies spielt eine große Rolle in der Theorie **relationaler Datenbanken**. Hier finden Sie ein kleines Beispiel:

Beipiel: Verknüpfung von Relationen:
Zunächst benötigen wir folgende

Definition:
Gegeben sind die (zweistelligen) Relationen $R_1 \subseteq A \times B$ und $R_2 \subseteq B \times C$.
Dann ist die Verknüpfung $R_1 \circ R_2 \subseteq A \times C$ definiert durch: $(a, c) \in R_1 \circ R_2 \Leftrightarrow \exists x \in B : (a, x) \in R_1 \wedge (x, c) \in R_2$.

Nehmen wir konkret $A =$ Menge der Nachnamen der Studierenden der HS Osnabrück
$B =$ Menge der zulässigen Matrikelnummern der HS Osnabrück und
$C =$ Menge der Studiengänge der HS Osnabrück.

$R_1 \subseteq A \times B$ ordnet jedem Namen eines Studierenden eine Matrikelnummer zu; $R_2 \subseteq B \times C$ ordnet jeder Matrikelnummer einen Studiengang zu. Die Verknüpfung $R_1 \circ R_2$ liefert dann die Verbindung von Namen eines Studierenden zum Studiengang.
Die Relationen R_1, R_2 und $R_1 \circ R_2$ lassen sich durch **Tabellen** realisieren:

Für R_1:

Name	Matrikelnr.
...	...
Müller	834412
Meier	842211
Kunze	783222
...	...

und für R_2:

Matrikelnr.	Studiengang
834412	Medieninformatik
...	...
842211	Medieninformatik
783222	Maschinenbau
...	...

dann wird die Verknüpfung $R_1 \circ R_2$

durch folgende Tabelle realisiert:

Name	Matrikelnr.
...	...
Müller	Medieninformatik
Meier	Medieninformatik
Kunze	Maschinenbau
...	...

Abbildungen als Relationen

Abbildungen (Funktionen) spielen eine bedeutende Rolle in der Mathematik. Aus mengentheoretischer Sicht sind Abbildungen (Funktionen) zweistellige Relationen mit einer besonderen Eigenschaft.

Definition:
Gegeben sind die Mengen D und W ($D \neq \emptyset$, $W \neq \emptyset$).
Eine **Abbildung** $f : D \to W$ ist eine **zweistellige Relation** $R \subseteq D \times W$ über D,W (also $f \subseteq D \times W$) mit folgender Eigenschaft:
Zu jedem $x \in D$ gibt es genau ein $y \in W$ mit $(x, y) \in f$; man schreibt dann: $y = f(x)$.
D nennt man **Definitionsbereich (Definitionsmenge)** und W nennt man **Wertebereich (Wertemenge)** der Abbildung f.
Das **Bild von f (Bild(f))** ist definiert durch

$$Bild\,(f) = \{y \in W |\ \exists\, x \in D\ mit\ (x, y) \in f\}$$

Der **Graph von f (Graph(f))** ist definiert durch

$$Graph\,(f) = \{(x, y) \in D \times W |\ y = f\,(x)\}$$

Für $y \in W$ ist das **Urbild von y unter f** definiert durch

$$U_f\,(y) = \{x \in D |\ y = f\,(x)\}$$

Erläuterung zur Definition der Abbildung:
Die definierende Eigenschaft der Abbildung f (aufgefasst als Relation $f \subseteq D \times W$) ist:
Zu jedem $x \in D$ gibt es genau ein $y \in W$ mit $(x, y) \in f$.
Dies kann man auch (klassisch) deuten als:
Jedem $x \in D$ wird mittels der Abbildungsvorschrift f genau ein $y \in W$ zugeordnet: $x \in D \xrightarrow{f} y \in W$. Man schreibt dann $f : D \to W$ mit $f(x) = y$ bzw. $y = f(x)$.

Beispiel:
Wir setzen $D = \mathbb{N}_0$ und $W = \mathbb{N}_0$ und definieren $f \subseteq \mathbb{N}_0 \times \mathbb{N}_0$ durch
$f = \{(n, n^2) \mid n \in \mathbb{N}_0\}$.
In **klassischer Notation** hat man: $f : \mathbb{N}_0 \to \mathbb{N}_0$ mit $f(n) = n^2$.
In diesem Beispiel ist $Bild(f) = \{n^2 \mid n \in \mathbb{N}_0\} = \{0, 1, 4, 9, 16, 25, 36, 49, \ldots\}$ und z.B. $U_f(25) = \{5\}$, $U_f(49) = \{7\}$ und $U_f(3) = \emptyset$.

Weitere Beispiele für Abbildungen: Rechenoperationen auf Zahlenmengen
Die bekannten Rechenoperationen **Addition** und **Multiplikation** sind **Abbildungen**, nämlich:
Für $\mathbb{B} \in \{\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}\}$ gilt:
Die **Addition** ist eine Abbildung $+ : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$. Man schreibt $+(a, b) = a + b$ und nennt $a + b$ die **Summe** von a und b.
Die **Multiplikation** ist eine Abbildung $\cdot : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$. Man schreibt $\cdot(a, b) = a \cdot b$ und nennt $a \cdot b$ das **Produkt** von a und b.
Die **Rechenoperationen auf Zahlenmengen** werden auch **Verknüpfungen** genannt.
Mit **unserem Zahlsystem** beschäftigt sich der nächste Anschnitt.

4 Zahlsysteme und algebraische Strukturen

„Die ganzen Zahlen hat Gott gemacht, alles andere ist Menschenwerk“ (L. Kronecker, 1823-1891)

Im folgenden Kapitel werden die grundlegenden Eigenschaften und Darstellungsarten unseres Zahlsystems besprochen. Die im Zahlsystem vorhandenen algebraischen Strukturen werden zum Abschluss in verallgemeinerter Form heraugestellt.

4.1 Einführung: Aufbau unseres Zahlsystems

Im Kapitel zur Mengenlehre haben wir bereits Zahlenmengen angegeben. Wir betrachten folgende **Mengen von Zahlen**:

a) Die Menge der **natürlichen Zahlen** $\mathbb{N} = \{1, 2, 3, \dots\}$

b) Die Menge der **natürlichen Zahlen mit Null** $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$

c) Die Menge der **ganzen Zahlen** $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

d) Die Menge der **rationalen Zahlen** $\mathbb{Q} = \{\frac{z}{n} | z \in \mathbb{Z} \wedge n \in \mathbb{N}\}$, z heißt **Zähler**, n heißt **Nenner**.

e) Die Menge der **reellen Zahlen** $\mathbb{R}$.

Es gilt aus mengentheoretischer Sicht $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.
Zur Charakterisierung der reellen Zahlen kommen wir im Abschnitt 4.3.

4.2 Die Menge $\mathbb{N}_0$ der natürlichen Zahlen mit Null und die Menge $\mathbb{N}$

Streng formal erhält man die natürlichen Zahlen mit Null und die Addition und Multiplikation aus den **Peano-Axiomen (G. Peano, 1858-1932):**

1. 0 ist eine natürliche Zahl,
2. Jede natürliche Zahl n hat einen Nachfolger, der n‘ genannt wird, 0 ist nicht Nachfolger einer natürlichen Zahl, der Nachfolger der 0 heißt 1, also 0‘=1,
3. $n + 0 = n$ und $n + m‘ = (n + m)‘$ und damit: $n‘ = (n + 0)‘ = n + 0‘ = n + 1$ und $n+m$ ist der m-fache Nachfolger von n, also: $n+m = ((...(n+1)+1)+1)+...)+1)$,
4. $n \cdot 0 = 0$ und $n \cdot m‘ = n \cdot m + n$.

Später kommt noch ein **5. Axiom, das Induktionsaxiom** hinzu.
Es gilt für die **Menge der natürlichen Zahlen** $\mathbb{N} = \mathbb{N}_0 \backslash \{0\}$.

Zusammenfassend hat man:
Für die Menge $\mathbb{N}_0$ sind **zwei Rechenoperationen** definiert, nämlich:

1. Die **Addition** ist eine Abbildung $+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$. Man schreibt $+(a, b) = a + b$ und nennt $a + b$ die **Summe** von a und b.

2 Die **Multiplikation** ist eine Abbildung $\cdot : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$. Man schreibt $\cdot(a, b) = a \cdot b$ und nennt $a \cdot b$ das **Produkt** von a und b.

3. Es gelten folgende **„Rechenregeln“** $\forall a, b, c \in \mathbb{N}_0$:

Name	Addition $(+)$	Multiplikation $(\cdot)$
Kommutativgesetz	$a+b=b+a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a+(b+c)=(a+b)+c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a+0=a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$	$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$

Das **neutrale Element der Addition** ist die **Null (0)**, das **neutrale Element der Multiplikation** ist die **Eins (1)**. Die beiden neutralen Elemente sind eindeutig, d.h. es gibt genau eine 0 bzw. genau eine 1 mit der Eigenschaft neutrales Element der Addition bzw. Multiplikation zu sein.

Aus dieser Eindeutigkeit folgt für die „Rolle“ der 0 bei der Multiplikation die
Bemerkung:
Es gilt $\forall a \in \mathbb{N}_0 : a \cdot 0 = 0$
denn: Unter Beachtung der „Rechenregeln“ ist einerseits $a \cdot 0 = a \cdot (0+0) = (a \cdot 0) + (a \cdot 0)$ und andererseits $a \cdot 0 = (a \cdot 0) + 0$ und damit $(a \cdot 0) + (a \cdot 0) = (a \cdot 0) + 0$.
Die Eindeutigkeit der 0 als neutrales Element der Addition liefert damit: $a \cdot 0 = 0$.

Im Folgenden werden einige Beispiele für die Rechenregeln und Folgerungen aus den Rechenregeln dargestellt.

Definition:
Für $a \in \mathbb{N}$ sind **Potenzen** definiert durch:

1. $a^0 = 1 \ \forall a \in \mathbb{N}$ und $a^1 = a \ \forall a \in \mathbb{N}$.
2. $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n-mal} \ \forall a \in \mathbb{N} \wedge \forall n \in \mathbb{N}, n \geq 1$ ist das Produkt aus n Faktoren, die alle gleich a sind.
3. $0^n = 0 \ \forall n \in \mathbb{N}$ und 0^0 ist **nicht definiert**.

Beispiele und Bemerkungen:

a) $42 = 6 \cdot 7 = 7 \cdot 6$.

b) $15 = 3 \cdot 5 = 3 \cdot (3+2) = (3 \cdot 3) + (3 \cdot 2) = 9 + 6$.

c) Überlegen Sie bei jedem Rechenschritt, welche der Rechenregeln angewendet wird:
$(a+b)^2 = (a+b) \cdot (a+b) = ((a+b) \cdot a) + ((a+b) \cdot b) = (a^2 + b \cdot a) + (a \cdot b + b^2) = a^2 + (a \cdot b + a \cdot b) + b^2 = a^2 + (1+1) \cdot (a \cdot b) + b^2 = a^2 + 2 \cdot a \cdot b + b^2$

In Kurzform hat man die **1. binomische Formel**: $(a+b)^2 = a^2 + 2ab + b^2$.

d) $a^n \cdot a^k = (\underbrace{a \cdot a \ldots \cdot a}_{n-mal}) \cdot (\underbrace{a \cdot a \ldots \cdot a}_{k-mal}) = (\underbrace{a \cdot a \ldots \cdot a}_{n+k-mal}) = a^{n+k} \; \forall a \in \mathbb{N}.$

e) $(a^n)^k = \underbrace{(\underbrace{a \cdot a \ldots \cdot a}_{n-mal}) \cdot (\underbrace{a \cdot a \ldots \cdot a}_{n-mal}) \cdot \ldots \cdot (\underbrace{a \cdot a \ldots \cdot a}_{n-mal})}_{k-mal} = (\underbrace{a \cdot a \ldots \cdot a}_{n \cdot k-mal}) = a^{n \cdot k} \; \forall a \in \mathbb{N}.$

4.2.1 Vollständige Induktion und rekursive (induktive) Definition

Das **5. Peano-Axiom** heißt **Induktionsaxiom** und besagt in seiner Grundform

Induktionsaxiom:
Eine Aussageform $A(n)$ für $n \in \mathbb{N}_0$ bzw. $n \in \mathbb{N}$ ist **wahr** $\forall n \in \mathbb{N}_0$ bzw. $\forall n \in \mathbb{N}$, wenn gilt:

1) **Induktionsanfang:** $A(0)$ bzw. $A(1)$ ist **wahr**.

2) **Induktionsschluss:**
Für beliebiges $k \in \mathbb{N}_0$, $k \geq 0$ bzw. $k \in \mathbb{N}$, $k \geq 1$ gilt:
$\underbrace{A(k) \text{ ist } \textbf{wahr}}_{\textbf{Induktionsvoraussetzung}} \Rightarrow \underbrace{A(k+1) \text{ ist } \textbf{wahr}}_{\textbf{Induktionsbehauptung}}$

Bemerkung:
Eine (wie immer stark vereinfachende) „weltliche“ Erklärung zur vollständigen Induktion ist:
Um alle Stufen einer unendlich langen Leiter erreichen zu können, muss man zunächst eine „Einstiegsstufe“ finden. Dies leistet der Induktionsanfang. Dann muss man zeigen/nachweisen, dass man ausgehend von einer beliebigen Stufe k (Induktionsvoraussetzung) die nächste Stufe k+1 erreicht (Induktionsbehauptung); dieser Nachweis ist die wesentliche Arbeit beim Beweis durch vollständige Induktion !

Beispiel:
Für alle $n \in \mathbb{N}$ gilt: 7 teilt $2^{3n} - 1$, d.h. $\forall n \in \mathbb{N} \; \exists m \in \mathbb{N}$ mit $2^{3n} - 1 = 7 \cdot m$.
Induktionsanfang:
$n = 1 \Rightarrow 2^{3 \cdot 1} - 1 = 8 - 1 = 7 = 7 \cdot 1$, setze also $m = 1$ d.h. die Aussage $A(1)$ ist wahr.
Induktionsschluss:
Induktionsvoraussetzung: Die Aussage $A(k)$ ist wahr für $k \geqq 1$, d.h. $\exists m \in \mathbb{N}$ mit $2^{3k} - 1 = 7 \cdot m$.
Induktionsbehauptung: Die Aussage $A(k+1)$ ist wahr für $k \geqq 1$, d.h. $\exists \tilde{m} \in \mathbb{N}$ mit $2^{3(k+1)} - 1 = 7 \cdot \tilde{m}$.
Jetzt kommt die eigentliche Arbeit:

Beweis:
$2^{3(k+1)}-1 = 2^{3k}\cdot 2^3 - 1 = (2^{3k}-1+1)\cdot 2^3 - 1 = \underbrace{(2^{3k}-1)}_{\text{nach Induktionsvoraussetzung}=7\cdot m}\cdot 2^3 + (2^3-1) =$
$(7\cdot m)\cdot 2^3 + 7 = 7\cdot \underbrace{(m\cdot 2^3+1)}_{=\tilde{m}}$.
Die Induktionsbehauptung ist also wahr mit $\tilde{m} = (m\cdot 2^3+1)$.

Ein weiteres Beispiel soll das Verfahren der vollständigen Induktion einüben. Dabei wird weniger gerechnet, sondern mehr argumentiert.

Beispiel:
Gegeben ist eine Menge M mit n Elementen, $n \in \mathbb{N}_0$. Für alle $n \in \mathbb{N}_0$ gilt: Die Potenzmenge $\mathbb{P}(M)$ hat 2^n Elemente.
Induktionsanfang:
$n = 0 \Rightarrow M = \emptyset \Rightarrow \mathbb{P}(M) = \{\emptyset\} \Rightarrow \mathbb{P}(M)$ hat $1 = 2^0$ Elemente, d.h. die Aussage $A(0)$ ist wahr.
Induktionsschluss:
Induktionsvoraussetzung: Die Aussage $A(k)$ ist wahr für $k \geqq 0$, d.h. M hat k Elemente $\Rightarrow \mathbb{P}(M)$ hat 2^k Elemente.
Induktionsbehauptung: Die Aussage $A(k+1)$ ist wahr für $k \geqq 0$, d.h. M hat $k+1$ Elemente $\Rightarrow \mathbb{P}(M)$ hat 2^{k+1} Elemente.
Jetzt kommt die eigentliche Arbeit:
Beweis: Für ein beliebiges Element $a \in M$ gilt: Die Teilmengen von M bestehen aus zwei Gruppen nämlich aus den Teilmengen, die das Element a nicht enthalten und aus den Teilmengen, die das Element a enthalten.
Die Teilmengen, die a nicht enthalten, erhält man wie folgt: Betrachte die Menge $\tilde{M} = M\backslash\{a\}$ und bilde ihre Potenzmenge $\mathbb{P}(\tilde{M})$. Da $\tilde{M}$ nur k Elemente hat, folgt aus der **Induktionsvoraussetzung**, dass $\mathbb{P}(\tilde{M})$ 2^k Elemente hat.
Die Teilmengen, die a enthalten erhält man dann, indem man für jede Menge $A \in \mathbb{P}(\tilde{M})$ die Menge $A \cup \{a\}$ bildet. Das sind insgesamt auch 2^k Mengen.
Damit besteht $\mathbb{P}(M)$ aus insgesamt $2^k + 2^k = 2\cdot 2^k = 2^{k+1}$ Elementen.
Die Induktionsbehauptung ist also wahr.

Aus dem Prinzip der vollständigen Induktion folgt das **Verfahren der rekursiven/induktiven Definition**:
Ein Term $A(n)$ ist für alle $n \in \mathbb{N}_0$ bzw. $n \in \mathbb{N}$ oder $n \in \mathbb{N}$ mit $n \geq k$ definiert, falls

1) $A(0)$ (bzw. $A(1)$ oder $A(k)$) ist definiert als **Anker/Ausgangspunkt** der Definition;

2) Für $n > 0$ (bzw. $n > 1$ oder $n > k$) ist ein **Bildungsgesetz** der Form $A(n+1) = f(A(n))$ bzw. $A(n+1) = f(A(0), A(1), \ldots, A(n))$ oder $A(n+1) = f(A(1), A(2), \ldots, A(n))$ oder $A(n+1) = f(A(k), A(k+1), \ldots, A(n))$ definiert.

Es folgt ein Beispiel für eine rekursive/induktive Definition.

Definition und Beispiel (Fakultät):

Für $n \in \mathbb{N}_0$ ist **Fakultät von n (n!)** definiert durch

1) $0! = 1$

2) $(n+1)! = (n+1) \cdot n!$

Das Bildungsgesetz erlaubt, die zu berechnende Zahl „rekursiv“ zu ermitteln:
$5! = 5 \cdot 4! = 5 \cdot 4 \cdot 3! = 5 \cdot 4 \cdot 3 \cdot 2! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0!$
Der **Anker** liefert mit $0! = 1$ dann insgesamt
$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

Alternative Definition: Das Beispiel zeigt, dass man n! auch anders definieren kann: n! ist das Produkt der natürlichen Zahlen von 1 bis n:
$n! = 1 \cdot 2 \cdot 3 \cdot 4 \ldots \cdot (n-1) \cdot n$.

4.2.2 Elementare Kombinatorik und endliche Summen

Die **elementare Kombinatorik** handelt von der **Auswahl und/oder Anordnung von Elementen einer endlichen Menge**.

Zunächst betrachten wir das folgende unmittelbar einsehbare Multiplikationsprinzip:
Satz: (Elementares Multiplikationsprinzip)
Gegeben sind die Menge A mit n Elementen und die Menge B mit k Elementen, dann hat das kartesische Produkt $A \times B$ $n \cdot k$ Elemente.

Gegeben sind die Mengen A_i mit n_i Elementen $1 \leq i \leq k$, dann hat das kartesische Produkt $A_1 \times A_2 \times \cdots \times A_k$ $n_1 \cdot n_2 \cdot \cdots \cdot n_k$ Elemente.

Beweis:
$A \times B = \{(a,b) \mid a \in A \wedge b \in B\} \Rightarrow$ für die erste Komponente in (a,b) gibt es n Möglichkeiten. Jede dieser Möglichkeiten kann mit einer der k möglichen Elemente aus B als zweiter Komponenete kombiniert werden. Zusammen erhält man also $n \cdot k$ 2-Tupel $(a,b) \in A \times B$.

Der allgemeine Fall folgt mit denselben Argumenten (bzw. mit vollständiger Induktion).

Im Folgenden betrachten wir immer eine Menge A mit n Elementen!

Satz: (Anzahl möglicher k-Tupel)

1) Gegeben ist eine Menge A mit n Elementen und $k \in \mathbb{N}$ mit $k \leq n$.
Es gibt $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$ k-Tupel in A^k **ohne Wiederholungen**, d.h. ohne das Auftreten identischer Komponenten.

2) Gegeben ist eine Menge A mit n Elementen und eine beliebige Zahl $k \in \mathbb{N}$. Es gibt n^k k-Tupel in A^k, d.h. auch k-Tupel mit identischen Komponenten (**mit Wiederholungen**).

Beweisidee:

1) Die erste Komponente des k-Tupels kommt aus der Menge A, o.B.d.A. sei das a_1. Die zweite Komponente kommt aus $A_1 = A \backslash \{a_1\}$ - einer Menge mit $n-1$ Elementen, o.B.d.A. sei das a_2; die dritte Komponente kommt dann aus der Menge $A_2 = A_1 \backslash \{a_2\} = A \backslash \{a_1, a_2\}$, A_2 hat $n-2$ Elemente. Dieser Prozess setzt sich fort bis zur k-ten Komponente a_k, die aus der Menge $A_{k-1} = A \backslash \{a_1, a_2, \cdots, a_{k-1}\}$ mit $n-(k-1) = n-k+1$ Elementen stammt. Das gesamte k-Tupel mit Komponenten ohne Wiederholungen stammt daher aus dem kartesischen Produkt $A \times A_1 \times A_2 \times \ldots \times A_{k-1}$ und diese Menge hat nach dem elementaren Multiplikationsprinzip genau $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$ Elemente.

2) Für k-Tupel mit Wiederholungen stammt jede Komponente aus der Menge A, insgesamt erhält man daher alle Tupel aus $\underbrace{A \times A \times A \times \ldots \times A}_{k-mal} = A^k$ und diese Menge hat nach dem elementaren Multiplikationsprinzip $n \cdot n \cdot \ldots \cdot n = n^k$ Elemente.

Beispiele:

a) **Permutation von n Elementen**
Unter einer Permutation einer Menge A mit n Elementen versteht man eine Umordnung dieser Elemente, anders ausgedrückt: Eine Permutation der n-elementigen Menge A ist eine bijektive (eineindeutige) Abbildung $p : A \to A$. Jede Permutation ist also ein n-Tupel in A^n ohne Wiederholungen. Damit folgt:
Es gibt $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-n+1) = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$ **Permutationen einer n-elementigen Menge**.

b) Anzahl **2-stelliger Verknüpfungen von Aussagen/2-stelliger Binärfunktionen**
Die Konjunktion ist ein Beispiel einer 2-stelligen Verknüpfung von Aussagen. Sie ist durch folgende Wahrheitstafel eindeutig festgelegt:

A	B	A∧B
w	w	w
w	f	f
f	w	f
f	f	f

Die letzte Spalte für $A \wedge B$ in der Tabelle legt folgende Interpretation der 2-stelligen Verknüpfung nahe: Das Ergebnis einer 2-stelligen Aussageverknüpfung/2-stelligen Binärfunktion ist ein 4-Tupel aus der Menge A^4 für $A = \{w, f\}$.
Die Anzahl 2-stelliger Aussageverknüpfungen ist also die Anzahl 4-Tupel einer Menge A ($k = 4$) mit 2 Elementen ($n = 2$) (mit Wiederholungen)$\Rightarrow$ **Es gibt** $2^4 = 16$ **zweistellige Aussageverknüpfungen**.

Satz: (Anzahl k-elementiger Teilmengen)

Gegeben ist eine Menge A mit n Elementen und $k \in \mathbb{N}$ mit $k \leq n$.
Die Menge A hat genau $\frac{n!}{(n-k)! \cdot k!}$ k-elementige Teilmengen (Teilmengen mit k Elementen).

Anders formuliert: Die **Anzahl der Auswahlmöglichkeiten von k Elementen aus einer n-elementigen Menge (ohne Wiederholungen)** entspricht der Anzahl der k-elementigen Teilmengen einer n-elementigen Menge, d.h. es gibt $\frac{n!}{(n-k)! \cdot k!}$ Möglichkeiten aus n Elementen k Elemente auszuwählen (ohne Wiederholungen).

Beweisidee:
Es gibt $\frac{n!}{(n-k)!}$ Möglichkeiten k aus n Elementen auszuwählen ohne Wiederholungen. Jedes spezielle k-Tupel kann man auf $k!$ Arten „umordnen“ (Anzahl der Permutationen einer k-elementigen Menge), ohne die getroffene Auswahl zu verändern! Diese Möglichkeiten sind also ununterscheidbar; nach dem elementaren Multiplikationsprinzip ging ihre Anzahl als Faktor in die Berechnung der Gesamtanzahl der Möglichkeiten ein, der Faktor muss wegen der Ununterscheidbarkeit also wieder „herausdividiert“ werden. Man hat damit also (wie behauptet) $\frac{n!}{(n-k)! \cdot k!}$ Möglichkeiten.

Definition:
Für $n, k \in \mathbb{N}_0$ mit $k \leq n$ sind **Binomialkoeffizienten „n über k“** $\binom{n}{k}$ definiert durch

1) $\binom{n}{0} = 1 \ \forall n \in \mathbb{N}_0$

2) $\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!} \ \forall n \in \mathbb{N}, n \leq k.$

oder **rekursiv**

2') $\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1} \ \forall n \in \mathbb{N}, n \leq k.$

Eine Menge A mit n Elementen hat also $\binom{n}{k}$ k-elementige Teilmengen.
Die Potenzmenge $\mathbb{P}(A)$ besteht aus allen 0-elementigen, 1-elementigen, 2-elementigen, $\cdots$, n-elementigen Teilmengen. Da die Potenzmenge $\mathbb{P}(A)$ insgesamt 2^n Elemente enthält,

folgt also $2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$, d.h. **eine Menge mit n Elementen hat 2^n Teilmengen**.

Summiert werden also alle Binomialkoeffizienten $\binom{n}{k}$ für $0 \leq k \leq n$, dies kann man mit Hilfe des **Summenzeichens** $\sum$ prägnant und abkürzend schreiben:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}$$

Zur Summe wird der **Laufindex** - hier k - mit Angabe der **unteren Summationsgrenze** - hier 0 - und der **oberen Summationsgrenze** - hier n - angegeben. Hinter dem Summenzeichen stehen die (vom Laufindex abhängigen) **Summanden** - hier $\binom{n}{k}$.

Zusammenfassend ergibt sich folgende

Definition: (endliche Summe)
Gegeben sind $u, o \in \mathbb{N}_0$ mit $u \leq o$ und $o - u + 1$ Summanden a_k für $u \leq k \leq o$. Dann ist die **endliche Summe** dieser Summanden definiert durch: $\sum_{k=u}^{o} a_k = a_u + a_{u+1} + a_{u+2} + \cdots + a_{o-1} + a_o$.
u heißt untere Summationsgrenze, o heißt obere Summationsgrenze, k heißt Laufindex.

Bemerkung:

a) Der Name des Laufindex ist für die Summenbildung unerheblich solange die Summationsgrenzen und die Summanden unverändert bleiben, es ist
$\sum_{k=u}^{o} a_k = \sum_{i=u}^{o} a_i$

b) Im Fall $o = u$ setzt man $\sum_{k=u}^{o} a_k = a_u$

c) Im Fall konstanter Summanden, also $a_k = a \ \forall k$ mit $u \leq k \leq o$ hat man
$\sum_{k=u}^{o} a = \underbrace{a + a + \cdots + a}_{o-u+1-mal} = (o - u + 1) \cdot a.$

d) Die **Anzahl der Auswahlmöglichkeiten von k Elementen aus einer n-elementigen Menge (ohne Wiederholungen)** entspricht der Anzahl der k-elementigen Teilmengen einer n-elementigen Menge, d.h. es gibt $\binom{n}{k}$ Möglichkeiten aus n Elementen k Elemente auszuwählen (ohne Wiederholungen).

e) Rechenregeln für endliche Summen:
Für Faktoren s, t gilt: $\sum_{k=u}^{o} (s \cdot a_k + t \cdot b_k) = s \cdot \left(\sum_{k=u}^{o} a_k \right) + t \cdot \left(\sum_{k=u}^{o} b_k \right)$ insbesondere

$$s=1,t=1:\sum_{k=u}^{o}(a_k+b_k)=\left(\sum_{k=u}^{o}a_k\right)+\left(\sum_{k=u}^{o}b_k\right)$$
$$s=1,t=-1:\sum_{k=u}^{o}(a_k-b_k)=\left(\sum_{k=u}^{o}a_k\right)-\left(\sum_{k=u}^{o}b_k\right)$$
$$s=s,t=0:\sum_{k=u}^{o}(s\cdot a_k)=s\cdot\left(\sum_{k=u}^{o}a_k\right)$$

Rechenregeln für Binomialkoeffizienten:

1) $\binom{n}{0}=\binom{n}{n}=1$ und $\binom{n}{1}=\binom{n}{n-1}=n$
2) $\binom{n}{k}=\binom{n}{n-k}$
3) $\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k}$

Beweisideen:

1) $\binom{n}{0}=\frac{n!}{0!\cdot(n-0)!}=\frac{n!}{n!}=1,\ \binom{n}{n}=\frac{n!}{n!\cdot(n-n)!}=\frac{n!}{n!}=1,$

$\binom{n}{1}=\frac{n!}{1!\cdot(n-1)!}=\frac{n\cdot(n-1)!}{(n-1)!}=n,$

$\binom{n}{n-1}=\frac{n!}{(n-1)!\cdot(n-(n-1)!}=\frac{n\cdot(n-1)!}{(n-1)!}=n$

2) $\binom{n}{k}=\frac{n!}{k!\cdot(n-k)!}=\frac{n!}{(n-k)!\cdot k!}=\frac{n!}{(n-k)!\cdot(n-(n-k))!}=\binom{n}{n-k}$

3) Die letzte Identität erhält man über „Bruchrechnung “:

$\binom{n}{k-1}+\binom{n}{k}=\frac{n!}{(k-1)!\cdot(n-(k-1))!}+\frac{n!}{k!\cdot(n-k)!}=$

$\frac{n!}{(k-1)!\cdot(n-k+1)!}+\frac{n!}{k!\cdot(n-k)!}=\frac{n!\cdot k}{k\cdot(k-1)!\cdot(n-k+1)!}+\frac{n!\cdot(n-k+1)}{k!\cdot(n-k)!\cdot(n-k+1)}=$

$\frac{n!\cdot k}{k!\cdot(n-k+1)!}+\frac{n!\cdot(n-k+1)}{k!\cdot(n-k+1)!}=\frac{n!\cdot(k+(n-k+1))}{k!\cdot(n+1-k)!}=\frac{n!\cdot(n+1)}{k!\cdot((n+1)-k)!}=$

$\frac{(n+1)!}{k!\cdot((n+1)-k)!}=\binom{n+1}{k}$

Endliche Summen und vollständige Induktion

Summenformel von Gauß:
Für alle $n \in \mathbb{N}_0$ gilt: $\sum_{i=0}^{n} i = \frac{n \cdot (n+1)}{2}$.
Induktionsanfang:
$n = 0 \Rightarrow \sum_{i=0}^{0} i = 0 = \frac{0 \cdot (0+1)}{2}$, d.h. die Aussage $A(0)$ ist wahr.
Induktionsschluss:
Induktionsvoraussetzung: Die Aussage $A(k)$ ist wahr für $k \geqq 1$,
d.h. $\sum_{i=0}^{k} i = \frac{k \cdot (k+1)}{2}$.
Induktionsbehauptung: Die Aussage $A(k+1)$ ist wahr für $k \geqq 1$,
d.h. $\sum_{i=0}^{k+1} i = \frac{(k+1) \cdot ((k+1)+1)}{2} = \frac{(k+1) \cdot ((k+2)}{2}$.
Jetzt kommt die eigentliche Arbeit:
Beweis:
$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1) = \frac{k \cdot (k+1)}{2} + (k+1) = \frac{k \cdot (k+1) + 2 \cdot (k+1)}{2} = \frac{(k+1) \cdot (k+2)}{2}$. Die Induktionsbehauptung ist also wahr.

Endliche geometrische Summe:
Für alle $n \in \mathbb{N}_0$ gilt: Für $q \in \mathbb{R}, q \neq 1$ gilt $\sum_{i=0}^{n} q^i = \frac{1-q^{n+1}}{1-q}$.
Induktionsanfang:
$n = 0 \Rightarrow \sum_{i=0}^{0} q^i = q^0 = 1 = \frac{1-q^{0+1}}{1-q} = \frac{1-q}{1-q}$, d.h. die Aussage $A(0)$ ist wahr.
Induktionsschluss:
Induktionsvoraussetzung: Die Aussage $A(k)$ ist wahr für $k \geqq 1$,
d.h. $\sum_{i=0}^{k} q^i = \frac{1-q^{k+1}}{1-q}$.
Induktionsbehauptung: Die Aussage $A(k+1)$ ist wahr für $k \geqq 1$,
d.h. $\sum_{i=0}^{k+1} q^i = \frac{1-q^{(k+1)+1}}{1-q} = \frac{1-q^{k+2}}{1-q}$.
Jetzt kommt die eigentliche Arbeit:
Beweis:
$\sum_{i=0}^{k+1} q^i = \left(\sum_{i=0}^{k} q^i\right) + q^{k+1} = \frac{1-q^{k+1}}{1-q} + q^{k+1} = \frac{1-q^{k+1} + (1-q) \cdot q^{k+1}}{1-q} = \frac{1-q^{k+2}}{1-q}$.
Die Induktionsbehauptung ist also wahr.

4.3 Die Menge $\mathbb{R}$ der reellen Zahlen

Zunächst werden wir unser Zahlsystem über $\mathbb{N}_0$ hinaus erweitern. Dies machen wir durch axiomatische Definition neuer Zahlen und der Eigenschaften der neu hinzukommenden Zahlen.

4.3.1 Die ganzen Zahlen $\mathbb{Z}$

Definition:

1) Für $n \in \mathbb{N}$ ist $-n$ die **eindeutig bestimmte** Zahl, für die gilt: $n + (-n) = 0$; man nennt $-n$ die **additiv inverse Zahl** zu n.

2) Die **Menge der ganzen Zahlen** ist $\mathbb{Z} = \{-n \mid n \in \mathbb{N}\} \cup \mathbb{N}_0$ also $\mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$.

3) Die Addition wird (unter Beibehaltung der Rechenregeln) erweitert für $\mathbb{Z}$: Es gilt $n + (-k) = n - k \ \forall n, k \in \mathbb{N}_0$.
$n - k$ heißt **Differenz** von n und k; die Rechenoperation nennt man auch Subtraktion, d.h.:
Subtraktion $n - k$ = **Addition der additiv inversen Zahl** $-k$ zu n, also $n - k = n + (-k)$.

4) Es gelten folgende **„Rechenregeln“** $\forall a, b, c \in \mathbb{Z}$:

Name	Addition $(+)$	Multiplikation $(\cdot)$
Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
Existenz additiv inv. Elemente	$a + (-a) = 0$	

Bemerkungen und Beispiele:

Es gilt $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z}$.

Es gilt wie schon in $\mathbb{N}_0$: $\forall a \in \mathbb{Z} : a \cdot 0 = 0$;
denn: Unter Beachtung der „Rechenregeln“ ist einerseits $a \cdot 0 = a \cdot (0+0) = (a \cdot 0) + (a \cdot 0)$ und andererseits $a \cdot 0 = (a \cdot 0) + 0$ und damit $(a \cdot 0) + (a \cdot 0) = (a \cdot 0) + 0$. Die Eindeutigkeit der 0 als neutrales Element der Addition liefert damit: $a \cdot 0 = 0$.
Wegen $0 = (-a) + (-(-a)))$ und $(-a) + a = 0$ folgt auf Grund der Eindeutigkeit des inversen Elements der Addition: $-(-a) = a \ \forall a \in \mathbb{Z}$.
Es gilt für $a, b \in \mathbb{Z} : (a \cdot (-b)) + (a \cdot b) = a \cdot ((-b) + b) = a \cdot 0 = 0 \Rightarrow a \cdot (-b) = -(a \cdot b) = -a \cdot b$

Es gilt auch $0 = a \cdot 0 = a \cdot (1 + (-1)) = a + (-1) \cdot a \Rightarrow -a = (-1) \cdot a$

Überlegen Sie bei jedem Rechenschritt, welche der Rechenregeln angewendet wird:
$(a-b)^2 = (a+(-b))^2 = (a+(-b)) \cdot (a+(-b)) = ((a+(-b)) \cdot a) + ((a+(-b)) \cdot (-b)) =$
$(a^2 + (-b) \cdot a) + (a \cdot (-b) + (-b) \cdot (-b)) = a^2 + (a \cdot (-b) + a \cdot (-b)) + (-b)^2 =$
$a^2 + (1+1) \cdot (a \cdot (-b)) + (-b)^2 = a^2 + 2 \cdot a \cdot (-b) + b^2 = a^2 - 2 \cdot a \cdot b + b^2$

In Kurzform hat man die **2. binomische Formel**: $(a-b)^2 = a^2 - 2ab + b^2$.

Man erhält aus den Rechenregeln auch:
$(a+b) \cdot (a-b) = a^2 + a \cdot (-b) + b \cdot a + b \cdot (-b) = a^2 - a \cdot b + a \cdot b - b^2 = a^2 - b^2$

In Kurzform hat man die **3. binomische Formel**: $a^2 - b^2 = (a-b) \cdot (a+b)$.

Zur Übung: Für $a, b \in \mathbb{Z}$ gilt
$(3a - 5b)^2 = (3a)^2 - 2 \cdot (3a) \cdot (5b) + (5b)^2 = 9a^2 - 30a \cdot b + 25b^2$
$9a^2 - 16b^2 = (3a)^2 - (4b)^2 = (3a - 4b) \cdot (3a + 4b)$
$(a + 7b)^2 = a^2 + 2 \cdot a \cdot 7b + (7b)^2 = a^2 + 14 \cdot a \cdot b + 49b^2$

Die Rechenregeln haben noch eine „Lücke“ bezüglich multiplikativ inverser Elemente. Diese Lücke schließen wir jetzt durch eine weitere axiomatische Definition neu hinzukommender Zahlen und ihrer Eigenschaften

4.3.2 Die rationalen Zahlen $\mathbb{Q}$: Brüche und Dezimaldarstellung rationaler Zahlen

Definition:

1) Für $a \in \mathbb{Z}$ mit $a \neq 0$ ist $\frac{1}{a} = a^{-1}$ die **eindeutig bestimmte** Zahl, für die gilt: $a \cdot \frac{1}{a} = a \cdot a^{-1} = 1$; man nennt $\frac{1}{a} = a^{-1}$ die **multiplikativ inverse Zahl** zu a.

2) Die **Menge der rationalen Zahlen** ist $\mathbb{Q} = \{q = \frac{z}{n} = z \cdot \frac{1}{n} \mid z \in \mathbb{Z} \wedge n \in \mathbb{N}\}$; z heißt **Zähler** und n heißt **Nenner** des **Bruchs** $\frac{z}{n}$.

3) Die Multiplikation wird (unter Beibehaltung der Rechenregeln) erweitert für $\mathbb{Q}$:
Es gilt $a \cdot \frac{1}{a} = a \cdot a^{-1} = 1 \; \forall a \in \mathbb{Q} \backslash \{0\}$.
$\frac{z}{n}$ heißt **Quotient** von z und n; die Rechenoperation nennt man auch **Division**, d.h.:
Division $\frac{z}{n}$ = **Multiplikation der multiplikativ inversen Zahl** $\frac{1}{n}$ mit z, also $\frac{z}{n} = z \cdot \frac{1}{n}$.

4) Es gelten folgende **„Rechenregeln“** $\forall a, b, c \in \mathbb{Q}$:

Name	Addition $(+)$	Multiplikation $(\cdot)$
Kommutativgesetz	$a+b=b+a$	$a\cdot b=b\cdot a$
Assoziativgesetz	$a+(b+c)=(a+b)+c$	$a\cdot(b\cdot c)=(a\cdot b)\cdot c$
Existenz neutraler Elemente	$a+0=a$	$a\cdot 1=a$
Distributivgesetze	$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$	$(a+b)\cdot c=(a\cdot c)+(b\cdot c)$
Existenz inverser Elemente	$a+(-a)=0$	$a\cdot\frac{1}{a}=a\cdot a^{-1}=1, a\neq 0$

Die **Tabelle ist nicht vollkommen symmetrisch bezüglich Addition und Multiplikation**:
Jede Zahl $a\in\mathbb{Q}$ hat eine additiv inverse Zahl $-a\in\mathbb{Q}$, eine multiplikativ inverse Zahl $\frac{1}{a}=a^{-1}$ gibt es aber nur für von null verschiedene rationale Zahlen (also nur für $a\neq 0$).
Division durch 0 ist verboten (genauer: nicht definiert).

Bemerkungen und Beispiele:

Wir fassen einige aus den obigen Rechenregeln folgende Regeln zusammen.
Wegen $1\cdot 1=1$ und der Eindeutigkeit des multiplikativ inversen Elements von 1 gilt: $\frac{1}{1}=1^{-1}=1$

Für alle $z\in\mathbb{Z}: z=z\cdot 1=z\cdot\frac{1}{1}=\frac{z}{1}$ und damit $z\in\mathbb{Q}$, d.h:
Es gilt $\mathbb{N}\subset\mathbb{N}_0\subset\mathbb{Z}\subset\mathbb{Q}$.

Ist $z=k\cdot n$ hat man die **Kürzungsregel**: $\frac{z}{n}=\frac{k\cdot n}{n}=k\cdot\underbrace{(\frac{1}{n}\cdot n)}_{=1}=k$.

Ist $z=k\cdot a$ und $n=k\cdot b$ hat man eine weitere **Kürzungsregel**, nämlich: $\frac{z}{n}=\frac{k\cdot a}{k\cdot b}=\underbrace{(k\cdot\frac{1}{k})}_{=1}\cdot\frac{a}{b}=\frac{a}{b}$.

Den **Umgang mit dem Minuszeichen** regelt:
Es ist $-(-a)=a$, denn $0=(-a)+a$ und $0=(-a)+(-(-a))$, die Eindeutigkeit des additiv inversen Elements liefert dann $-(-a)=a$.

Es ist $-(a+b)=-a-b$, denn $0=(a+b)+(-(a+b))$ und $0=a+(-a)+b+(-b)=(a+b)+((-a)+(-b))=((a+b)+(-a-b)$, die Eindeutigkeit des additiv inversen Elements liefert dann $-(a+b)=-a-b$.

Es ergeben sich aus den Rechenregeln folgende **Bruchrechenregeln:**

$\frac{a}{b}+\frac{c}{b}=(a+c)\cdot\frac{1}{b}=\frac{a+c}{b}$ (Addition gleichnamiger Brüche)

$\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d}{b\cdot d}+\frac{c\cdot b}{b\cdot d}=\frac{a\cdot d+c\cdot b}{b\cdot d}$ (Addition ungleichnamiger Brüche)

$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ (Multiplikation von Brüchen)

Wegen $\frac{a}{b} \cdot \frac{1}{\frac{a}{b}} = 1$ und $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{a \cdot b} = 1$ und der Eindeutigkeit des multiplikativ inversen Elements folgt: $\frac{1}{\frac{a}{b}} = \frac{b}{a}$ (Kehrwertbildung)

$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{1}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c} = \frac{a \cdot d}{b \cdot c}$ (Division von Brüchen)

Dezimaldarstellung rationaler Zahlen:

Das **Dezimalsystem** zur Zahldarstellung ist ein **Stellenwertsystem** zur **Basis** 10. Wir haben 10 Ziffern, die die Ziffernmenge $Z = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ bilden, die Position der Ziffern legt ihren Wert fest, d.h. für $a_0, a_1, \ldots, a_n \in Z$ gilt:
Die Ziffernfolge $a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0$ repräsentiert die Zahl

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \ldots a_2 \cdot 10^2 + a_1 \cdot \underbrace{10^1}_{=10} + a_0 \cdot \underbrace{10^0}_{=1} = \sum_{i=0}^{n} a_i \cdot 10^i$$

Jede **ganze Zahl** $z \in \mathbb{Z}$ kann dann in der Form $z = \pm a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0 = \pm \sum_{i=0}^{n} a_i \cdot 10^i$ dargestellt werden.

Nimmt man Ziffern $a_{-1}, a_{-2}, \ldots, a_{-k}$ dazu, erhält man die Zahl

$$q = \sum_{i=-k}^{n} a_i \cdot 10^i$$
$$= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \ldots a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 + a_{-1} \cdot 10^{-1} + a_{-2} \cdot 10^{-2} \ldots a_{-k} \cdot 10^{-k} = a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0 + \frac{a_{-1} a_{-2} \ldots a_{-k}}{10^k} =$$
$$\frac{a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0 a_{-1} a_{-2} \ldots a_{-k}}{10^k} \in \mathbb{Q}.$$

Man schreibt dies als $q = a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0, a_{-1} a_{-2} \ldots a_{-k}$ und nennt die Ziffern $a_{-1} a_{-2} \ldots a_{-k}$ die **Nachkommastellen** sowie die Ziffern $a_n a_{n-1} a_{n-2} \ldots a_2 a_1 a_0$ die **Vorkommastellen** der Zahl $q \in \mathbb{Q}$.

Beispiele und Bemerkungen:

a) $34527 = 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 7 \cdot 10^0$

b) $28,123 = 2 \cdot 10^1 + 8 \cdot 10^0 + 1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 3 \cdot 10^{-3} = 28 + \frac{123}{10^3} = 28 + \frac{123}{1000} = \frac{28000}{1000} + \frac{123}{1000} = \frac{28123}{1000}$

c) **Jede Zahl in der Darstellung $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0, a_{-1} a_{-2} \dots a_{-k}$ ist also eine rationale Zahl, d.h. $\in \mathbb{Q}$ und darstellbar als Bruch.**

d) Mit dem **Algorithmus zur schriftlichen Division** kann man **Brüche**, also Zahlen $q \in \mathbb{Q}$ in Zahlen in Dezimaldarstellung umwandeln:
Der Algorithmus ist entweder endlich (d.h. nach endlich vielen Schritten ist der Divisionsrest $= 0$) und führt zu einer Dezimalzahl mit (höchstens) endlich vielen Nachkommastellen oder man erhält eine periodisch wiederkehrende Ziffernfolge also eine Dezimalzahl mit unendlich vielen Nachkommastellen, die sich ab einer bestimmten Stelle periodisch wiederholen (denn bei Division durch n gibt es höchstens n verschiedene Divisionsreste (nämlich $0, 1, \cdots, n-1$):

Beispiel mit endlich vielen Nachkommastellen:

$\frac{825}{40} \Rightarrow$

$825 : 40 = 20,625$
80

25
0

250
240

100
80

200
200

0

Die Zahl $\frac{825}{40} \in \mathbb{Q}$ hat also die Dezimaldarstellung $20,625$.

Beispiel mit unendlich vielen, periodisch wiederkehrenden Nachkommastellen:

$\frac{112}{3} \Rightarrow$

$112 : 3 = 37,3333\dots$
9

$$
\begin{array}{r}
\hline
22 \\
21 \\
\hline
10 \\
9 \\
\hline
10 \\
9 \\
\hline
10 \\
\vdots
\end{array}
$$

Die Zahl $\frac{112}{3} \in \mathbb{Q}$ hat also die Dezimaldarstellung $37,333\ldots$.

Man schreibt das als $37,\overline{3}$ und spricht „siebenunddreißig Komma drei Periode“.

Damit erhält man folgende

Charakterisierung der Menge $\mathbb{Q}$ der rationalen Zahlen:

$\mathbb{Q}$ besteht aus allen Zahlen, deren Dezimaldarstellung endlich viele Nachkommastellen hat oder unendlich viele Nachkommastellen, die sich ab einer bestimmten Stelle periodisch wiederholen.

4.3.3 Dezimaldarstellung reeller Zahlen

Was sind reelle Zahlen, also die Menge $\mathbb{R}$?

Definition:
Die **Menge der rellen Zahlen** ist gegeben durch
$\mathbb{R}$ besteht aus allen Zahlen, deren Dezimaldarstellung endlich viele Nachkommastellen oder unendlich viele Nachkommastellen hat.
Also $\mathbb{R} = \mathbb{Q} \cup \{r \mid \text{r hat unendlich viele Nachkommastellen ohne periodische Wiederholung}\}$

Es gilt also insbesondere $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Bemerkungen und Beispiele:

a) Es gilt z.B. $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$, $\pi \in \mathbb{R}\backslash\mathbb{Q}$, $e \in \mathbb{R}\backslash\mathbb{Q}$.
Es ist $\sqrt{2} = 1,41421356\cdots$, $\pi = 3,14159265\cdots$, $e = 2,71828182\cdots$.

b) Wir zeigen: $\sqrt{2} \notin \mathbb{Q}$:

Widerspruchsbeweis: Angenommen $\sqrt{2} \in \mathbb{Q} \Rightarrow \sqrt{2} = \frac{z}{n}$ mit $z \in \mathbb{Z}, n \in \mathbb{N}$ so dass z **und** n **keine gemeinsamen Teiler** haben (gemeinsame Faktoren sind gekürzt!)$\Rightarrow$
$2 = \frac{z^2}{n^2} \Rightarrow z^2 = 2 \cdot n^2 \Rightarrow$ **2 ist Teiler von** z^2 **und damit von** z, d.h. $\exists k \in \mathbb{Z}$ mit $z = 2 \cdot k \Rightarrow 4 \cdot k^2 = z^2 = 2 \cdot n^2 \Rightarrow n^2 = 2 \cdot k^2 \Rightarrow$ **2 ist Teiler von** n^2 **und damit von** $n \Rightarrow z$ und n haben den **gemeinsamen Teiler 2!**
Dies ist ein Widerspruch dazu, dass z **und** n **keine gemeinsamen Teiler** haben, also ist die Annahme falsch und damit ihre Verneinung wahr, d.h. $\sqrt{2} \notin \mathbb{Q}$.

Es gelten wie in $\mathbb{Q}$ folgende **„Rechenregeln“** in $\mathbb{R}$: $\forall a, b, c \in \mathbb{R}$:

Name	Addition $(+)$	Multiplikation $(\cdot)$
Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
Existenz inverser Elemente	$a + (-a) = 0$	$a \cdot \frac{1}{a} = a \cdot a^{-1} = 1, a \neq 0$

Diese fünf Rechenregeln nennt man auch die **5 Körperaxiome**.

4.3.4 Exkurs: Maschinenzahlen

Womit rechnen Taschenrechner und Computer?
Jeder Rechner (Taschenrechner/Computer) kann nur Zahlen mit endlich vielen Stellen verarbeiten und darstellen, d.h. die sogenannten **Maschinenzahlen** $\mathbb{M}$ sind eine Teilmenge von $\mathbb{Q}$: $\mathbb{M} \subset \mathbb{Q}$.
Das uns vertraute und zum täglichen Rechnen benutzte **Dezimalsystem** zur Zahldarstellung ist ein **Stellenwertsystem** zur **Basis** 10. Rechner arbeiten hingegen mit dem **Dualsystem** zur Zahldarstellung. Dies ist ist ein **Stellenwertsystem** zur **Basis** 2.

Zahldarstellung im Dualsystem
Die Zahldarstellung $(z)_2 = b_n b_{n-1} b_{n-2} \ldots b_1 b_0, b_{-1} b_{-2} \ldots b_{-k}$ mit $b_j \in \{0, 1\}$ für $-k \leq j \leq n$ im **Dualsystem** entspricht der Zahl $z = \sum_{j=0}^{n} b_j \cdot 2^j + \sum_{j=1}^{k} b_{-j} \cdot 2^{-j}$.

Zum Beispiel gilt:
$(1101,101)_2 = 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 + 1\cdot 2^{-1} + 0\cdot 2^{-2} + 1\cdot 2^{-3} =$
$8 + 4 + 0 + 1 + \frac{1}{2} + 0 + \frac{1}{8} = 13 + \frac{5}{8} = (13,625)_{10}$.

Die IEEE 754-Norm legt eine Zahldarstellung (für sog. **Gleitkommazahlen**) in der Form $z = v \cdot m \cdot 2^e$ fest mit **Vorzeichen** v**, Mantisse** m **und Exponent** e. Für eine 32-Bit-Darstellung ist das Vorzeichen in einem Bit kodiert durch $s = 0$ oder $s = 1$ mit $v = (-1)^s$. Die Mantisse m hat als Dualzahl 23 Bit (23 Stellen) und der Exponent e hat als Dualzahl 8 Bit (8 Stellen).

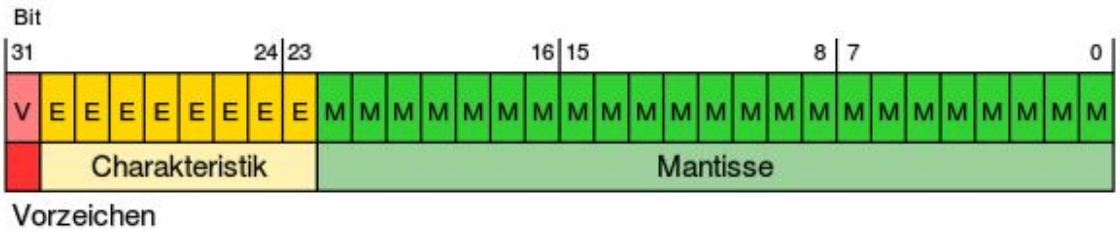
Eine der Folgen dieser Zahldarstellung ist die ungleiche Verteilung der Zahlen: In der Nähe der 0 liegen die Zahlen dichter beeinander als in der Nähe der größten darstellbaren Zahl. Das folgende Beispiel soll diese Tatsache im Dezimalsystem demonstrieren.

Beispiel:
Wir betrachten im **Dezimalsystem** Zahlen mit folgender Darstellung: $z = \pm m \cdot 10^{\pm e}$ mit einer Dezimalstelle für die Mantisse m und einer Dezimalstelle für den Exponenten e, genauer $m, e \in \{0, 1, 2, \cdots, 9\}$.
In dieser Darstellung sind die beiden kleinsten positiven Zahlen $z = +1 \cdot 10^{-9}$ und $z = +2 \cdot 10^{-9}$ mit Abstand 10^{-9}. Hingegen sind die beiden größten darstellbaren positiven Zahlen $z = +8 \cdot 10^{+9}$ und $z = +9 \cdot 10^{+9}$ mit Abstand 10^9.

Mit Hilfe einer endlichen geometrischen Summe erhält man:
Eine Zahl mit 8 Bit im Dualsystem ergibt als größten darstellbaren Wert $\underbrace{111\ldots1}_{8 \text{ mal}} =$

$$1\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^2 + \ldots + 1\cdot 2^7 = \sum_{k=0}^{7} 2^k = \frac{1-2^8}{1-2} = 2^8 - 1 = 255$$

Das folgende Bild (Quelle: https://de.wikipedia.org/wiki/IEEE_754)



zeigt die Speicherung einer Gleitkommazahl in 32-Bit-Darstellung nach der IEEE 754-Norm in Form von v(orzeichen)-C(harakteristik)-m(antisse). Aus der Charakteristik, die als vorzeichenlose Zahl interpretiert wird, berechnet sich der Exponent e für die Form $z = v \cdot m \cdot 2^e$ wie folgt:

Es gibt zwei **reservierte Bitfolgen** nämlich $= \underbrace{000\ldots0}_{8bit}$ für 0 und $= \underbrace{111\ldots1}_{8bit}$ für 255.
Es bleiben 253 „freie“ Werte für den Exponenten e in der Darstellung $z = \pm m \cdot 2^e$. Dieser Exponent ist für die nicht reservierten Bitfolgen (als Dezimalzahl) gegeben durch $(e)_{10} = (C)_{10} - 127$, dabei ist $(C)_{10}$ eine der 253 aus den nicht reservierten Bitfolgen der Charakteristik C ermittelte Dezimalzahl, d.h. $-126 = 1-127 \leq (e)_{10} \leq 127 = 254-127$. Damit sind auch **negative Exponenten** darstellbar $(-126 \leq (e)_{10} \leq 127)$!
Die betragsmäßig größte in dieser Form darstellbare Zahl liegt bei $\sim 2^{128}$, die betragsmäßig kleinste in dieser Form darstellbare Zahl liegt bei $\sim 2^{-126}$.

4.3.5 Die Anordnung in $\mathbb{R}$

Neben den **5 Körperaxiomen** gilt in $\mathbb{R}$ das

Anordnungsaxiom:
Für zwei reelle Zahlen $a, b \in \mathbb{R}$ gilt **genau eine** der drei folgenden **Alternativen**:

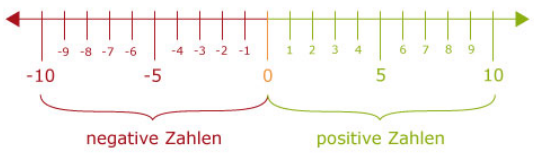
1) $a = b$
2) $a < b$
3) $a > b$

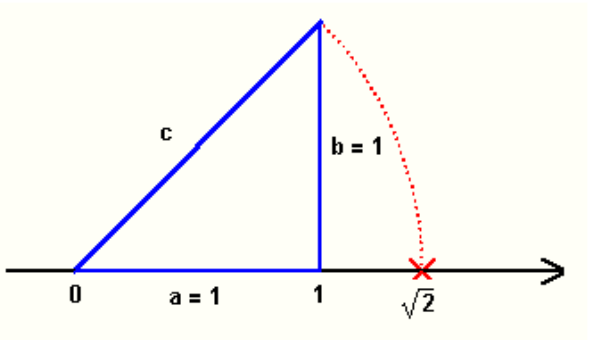
Das Anordnungsaxiom ermöglicht also immer einen **eindeutigen Größenvergleich** zwischen rellen Zahlen.

Bemerkung: Es gilt $\forall a, b \in \mathbb{R}$

a) $a < b \Leftrightarrow b > a$
b) $a \leq b \Leftrightarrow (a < b) \vee (a = b)$
c) $a \geq b \Leftrightarrow (a > b) \vee (a = b)$
d $a < b \Leftrightarrow a - b < 0$
e) $a > b \Leftrightarrow a - b > 0$

Zur **grafischen Veranschaulichung** verwendet man einen **Zahlenstrahl** (eine von links nach rechts gerichtete Gerade):
Auf dem Zahlenstrahl wird als Ausgangspunkt die 0 markiert und rechts davon die 1, um eine Skala festzulegen.
Jeder rellen Zahl entspricht ein Punkt auf dem Zahlenstrahl und umgekehrt gehört zu jedem Punkt auf dem Zahlenstrahl auch eine reelle Zahl.
Es gilt $a = b$, wenn a und b demselben Punkt auf dem Zahlenstrahl entsprechen, und $a < b$, wenn der Punkt zu a auf dem Zahlenstrahl links vom Punkt zu b auf dem Zahlenstrahl liegt.





Definition: Zur weiteren Vereinfachung definiert man

1) Die **Menge der positiven reellen Zahlen** ist $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$.

2) Die **Menge der positiven reellen Zahlen mit 0** ist $\mathbb{R}_+^0 = \{x \in \mathbb{R} \mid x \geqq 0\}$.

3) Die **Menge der negativen reellen Zahlen** ist $\mathbb{R}_- = \{x \in \mathbb{R} \mid x < 0\} = \mathbb{R} \backslash \mathbb{R}_+^0$.

4) Zum **Abschluss der Anordnung** werden die **Symbole** $+\infty$ und $-\infty$ eingeführt: Diese Symbole sind **keine reellen Zahlen**; für sie sind **keine Rechenoperationen** definiert. Es gilt lediglich bezüglich der Anordnung
$-\infty < a \ \forall a \in \mathbb{R}$ und $+\infty > a \ \forall a \in \mathbb{R}$.

Die Anordnung erlaubt uns auch, weitere Teilmengen der reellen Zahlen in kompakter Form darzustellen.

Definition:
Es gilt $\forall a, b \in \mathbb{R}$ mit $a \leqq b$

1) Das **offene Intervall** (a, b) ist definiert durch $(a, b) = \{x \in \mathbb{R} \mid (a < x) \wedge (x < b)\}$ in Kurzform $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.

2) Das **abgeschlossene Intervall** $[a, b]$ ist definiert durch $[a, b] = \{x \in \mathbb{R} \mid (a \leqq x) \wedge (x \leqq b)\}$ in Kurzform $[a, b] = \{x \in \mathbb{R} \mid a \leqq x \leqq b\}$.

3) Das **links halbabgeschlossene Intervall/rechts halboffene Intervall** $[a, b)$ ist definiert durch $[a, b) = \{x \in \mathbb{R} \mid (a \leqq x) \wedge (x < b)\}$ in Kurzform $[a, b) = \{x \in \mathbb{R} \mid a \leqq x < b\}$.

4) Das **rechts halbabgeschlossene Intervall/links halboffene Intervall** $(a, b]$ ist definiert durch $(a, b] = \{x \in \mathbb{R} \mid (a < x) \wedge (x \leqq b)\}$ in Kurzform $(a, b] = \{x \in \mathbb{R} \mid a < x \leqq b\}$.

Das **Zusammenspiel von Rechenoperationen und Anordnung** regelt folgender Satz

Satz:

a) $\forall c \in \mathbb{R}$ gilt: $a < b \Rightarrow a + c < b + c$.

b) $\forall a \in \mathbb{R}$ gilt: $a < 0 \Rightarrow -a > 0$.

c) $\forall c \in \mathbb{R}_+$ gilt: $a < b \Rightarrow a \cdot c < b \cdot c$.

d) $\forall c \in \mathbb{R}_-$ gilt: $a < b \Rightarrow a \cdot c > b \cdot c$.

e) $\forall a \in \mathbb{R}$ gilt: $a^2 = 0 \Leftrightarrow a = 0$ und $a^2 > 0$ für $a \in \mathbb{R}, a > 0$.

f) $\forall a, b \in \mathbb{R}$ mit $a \cdot b > 0$ gilt: $a > b \Rightarrow \frac{1}{a} < \frac{1}{b}$.

Die Regeln gelten analog für $>, \leq$ und $\geq$.

4.3.6 Weitere Rechenoperationen und Rechenregeln in $\mathbb{R}$

Neben den Grundrechenoperationen **Addition und Multiplikation** und den daraus über die Existenz entsprechender inverser Elemente abgeleitete Rechenoperationen **Subtraktion und Division** reeller Zahlen wollen wir weitere Rechenoperationen betrachten. Dazu dient zunächst die folgende

Definition:

1) Ein Term besteht aus syntaktisch korrekt gebildeten Wörtern oder Wortgruppen in der formalen Sprache der Mathematik, d.h. ein Term ist ein sinnvoller Ausdruck, der Zahlen, Variablen, Symbole für mathematische Verknüpfungen und Klammern enthalten kann.

2) Eine Gleichung ist eine Aussage über die Gleichheit (Äquvalenz) zweier Terme, $T_1 = T_2$. Das Symbol $=$ heißt Gleichheitszeichen.

3) Eine Ungleichung ist eine Aussage zum Größenvergleich zweier Terme, z.B. $T_1 < T_2$, oder $T_1 \gtrless T_2$. Die Symbole $<, >, \leq, \geq$ heißen Ungleichheitszeichen.

Lineare Gleichungen und Ungleichungen

a) Lineare Gleichung: Für $a \in \mathbb{R}\backslash\{0\}$ und $b, c \in \mathbb{R}$ hat man die lineare Gleichung $a \cdot x + b = c$. Die Lösung x erhält man schrittweise: Zunächst Subtraktion von b auf beiden Seiten, dies liefert $a \cdot x = c - b$, die Lösung x erhält man nach Division durch a auf beiden Seiten: $x = \frac{c-b}{a}$.

Die Lösungsmenge ist $\mathbb{L} = \left\{\frac{c-b}{a}\right\}$.

Konkret: $5x - 2 = -7 \Leftarrow 5x = -7 - (-2) = -7 + 2 = -5 \Leftarrow x = \frac{-5}{5} = -1$ und $\mathbb{L} = \{-1\}$

b) Lineare Ungleichung: Für $b, c \in \mathbb{R}$ hat man die lineare Ungleichung $a \cdot x + b < c$ mit $a \in \mathbb{R}\backslash\{0\}$.
Die Lösung x erhält man schrittweise: Zunächst Subtraktion von b auf beiden Seiten, dies liefert $a \cdot x < c - b$,
nach Division durch a auf beiden Seiten erhält man:

Für $a \in \mathbb{R}_+$: $x < \dfrac{c-b}{a}$:
Die Lösungsmenge ist $\mathbb{L} = \left\{ x \in \mathbb{R} \mid x < \dfrac{c-b}{a} \right\} = \left(-\infty, \dfrac{c-b}{a}\right)$.

Für $a \in \mathbb{R}_-$ folgt mit d) aus dem vorangehenden Satz: $x > \dfrac{c-b}{a}$.
Die Lösungsmenge ist $\mathbb{L} = \left\{ x \in \mathbb{R} \mid x > \dfrac{c-b}{a} \right\} = \left(\dfrac{c-b}{a}, +\infty\right)$.

Definition: (Potenzen und Wurzeln)

1) Potenzen reeller Zahlen

1.1) Für $a \in \mathbb{R}\backslash\{0\}$ ist $a^0 = 1$.

1.2) Für $n \in \mathbb{N}$ mit $n \geq 1$ ist $0^n = 0$ und für $a \in \mathbb{R}\backslash\{0\}$ ist $a^n = a \cdot a^{n-1}$ (rekursive Definition der n-ten Potenz).

1.3) Für $n \in \mathbb{N}$ mit $n \geq 1$ und für $a \in \mathbb{R}\backslash\{0\}$ ist $a^{-n} = \left(\dfrac{1}{a}\right)^n = \dfrac{1}{a^n}$.

2) Wurzeln reeller Zahlen

2.1) Für $n \in \mathbb{N}$, n **ungerade**, und $a \in \mathbb{R}$ ist $\sqrt[n]{a}$ die eindeutig bestimmte Lösung der Gleichung $x^n = a$.

2.2) Für $n \in \mathbb{N}$, n **gerade**, und $a \in \mathbb{R}_+^0$ ist $\sqrt[n]{a}$ die eindeutig bestimmte **nicht negative** Lösung der Gleichung $x^n = a$. Statt $\sqrt[2]{a}$ schreibt man kurz $\sqrt{a}$.

Bemerkungen und Beispiele:

a) $3^0 = 1$ und
$3^5 = 3 \cdot 3^4 = 3 \cdot 3 \cdot 3^3 = 3 \cdot 3 \cdot 3 \cdot 3^2 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3^1 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot \underbrace{3^0}_{=1} = \underbrace{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3}_{5 \text{ mal}}$

b) $2^{-3} = \left(\dfrac{1}{2}\right)^3 = \dfrac{1}{2^3} = \dfrac{1}{2 \cdot 2 \cdot 2} = \dfrac{1}{8}$

c) $\sqrt[5]{-32} = -2$, denn $x = -2$ löst die Gleichung $x^5 = -32$.

d) $\sqrt[2]{9} = \sqrt{9} = 3$, denn $x = 3$ ist die **nicht negative** Lösung der Gleichung $x^2 = 9$. Die **Lösungsmenge** der Gleichung $x^2 = 9$ ist jedoch $\mathbb{L} = \{-3, 3\}$!

e) **Rechenregeln für Potenzen und Wurzeln**

1) $a^n \cdot a^k = a^{n+k}$ und $(a^n)^k = a^{n \cdot k}$ sowie $\frac{a^n}{a^k} = a^n \cdot a^{-k} = a^{n-k}$

2) $(a \cdot b)^n = a^n \cdot b^n$ und $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$

3) $\sqrt[n]{a} = a^{\frac{1}{n}}$, $\left(\sqrt[n]{a}\right)^n = \left(a^{\frac{1}{n}}\right)^n = a^{\frac{1}{n} \cdot n} = a$

4) $\sqrt[k]{\sqrt[n]{a}} = \left(a^{\frac{1}{n}}\right)^{\frac{1}{k}} = a^{\frac{1}{n} \cdot \frac{1}{k}} = a^{\frac{1}{n \cdot k}} = \sqrt[n \cdot k]{a}$

5) $(\sqrt[n]{a})^k = \sqrt[n]{a^k} = a^{\frac{k}{n}}$

6) $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$ und $\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$

Potenzen und Summen:

Wie schon in $\mathbb{Z}$ (und $\mathbb{Q}$) erhält man die klassischen binomischen Formeln:

$(a+b)^2 = a^2 + 2 \cdot a \cdot b + b^2$, $(a-b)^2 = a^2 - 2 \cdot a \cdot b + b^2$ und $(a-b) \cdot (a+b) = a^2 - b^2$.

Was gilt für $(a+b)^n$ und $(a-b)^n$? Gibt es eine Verallgemeinerung von $(a-b) \cdot (a+b) = a^2 - b^2$?

Es gelten folgende **verallgemeinerte binomische Formeln**:

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^{n-k} \cdot b^k$, $(a-b)^n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot a^{n-k} \cdot b^k$ und für $a \neq b$ hat man $\frac{a^{n+1} - b^{n+1}}{a-b} = \sum_{k=0}^{n} a^{n-k} \cdot b^k$.

Da die $\binom{n}{k}$ in diesen Formeln als Koeffizienten vor den Produkten der Form $a^{n-k} \cdot b^k$ auftreten, nennt man sie **Binomialkoeffizienten**!

Beweisideen zu den verallgemeinerten binomischen Formeln:

Wir starten mit der letzten Formel, die formal keine binomische Formel ist, sondern aus der Formel für die endliche geometrische Summe folgt:

$$\frac{a^{n+1}-b^{n+1}}{a-b}=\frac{a^{n+1}\left(1-\frac{b^{n+1}}{a^{n+1}}\right)}{a\cdot\left(1-\frac{b}{a}\right)}=a^n\cdot\left(\frac{1-\left(\frac{b}{a}\right)^{n+1}}{1-\frac{b}{a}}\right)$$

Setzt man jetzt $q=\frac{b}{a}$, hat man unter Beachtung der Summenformel für die endliche geometrische Summe

$$a^n\cdot\left(\frac{1-\left(\frac{b}{a}\right)^{n+1}}{1-\frac{b}{a}}\right)=a^n\cdot\left(\frac{1-q^{n+1}}{1-q}\right)=a^n\cdot\sum_{k=0}^{n}q^n=a^n\cdot\sum_{k=0}^{n}(\tfrac{b}{a})^k=\sum_{k=0}^{n}a^{n-k}\cdot b^k.$$

Die beiden binomischen Formeln kann man mittels vollständiger Induktion beweisen (siehe: Goebbels/Ritter, Mathematik verstehen und anwenden, 2.Aufl., Springer Berlin, 2013, S.63); wir werden hier ein Argument aus der Kombinatorik benutzen:

Dazu starten wir mit
$(a+b)^3=(a+b)\cdot(a+b)^2=(a+b)\cdot(a^2+2\cdot a\cdot b+b^2)=$
$a^3+3\cdot a^2\cdot b+3\cdot a\cdot b^2+b^3=$
$\underbrace{a\cdot a\cdot a}_{3\text{ Faktoren}}+3\cdot\underbrace{a\cdot a\cdot b}_{3\text{ Faktoren}}+3\cdot\underbrace{a\cdot b\cdot b}_{3\text{ Faktoren}}+\underbrace{b\cdot b\cdot b}_{3\text{ Faktoren}}$

Wir haben also $4=3+1$ Summanden und in jedem Summenden Produkte mit 3 Faktoren, die aus a's und b's bestehen: Genauer 3 a's und 0 b's; 2 a's und 1 b, 1 a und 2 b's, 0 a's und 3 b's. Die drei Faktoren werden also durch Auswahl von k aus 3 Plätzen für b's und 3-k Plätzen für a's ($1\le k\le 3$) bestimmt. Diese Auswahl (von k aus 3) ergibt $\binom{3}{k}$ Möglichkeiten, d.h. der Summand mit $3-k$ a's und k b's kommt $\binom{3}{k}$-mal vor: er erhält den Koeffizienten $\binom{3}{k}$.
Mit $\binom{3}{0}=1,\binom{3}{1}=3,\binom{3}{2}=3$ und $\binom{3}{3}=1$ hat man
$(a+b)^3=a^3+3\cdot a^2\cdot b+3\cdot a\cdot b^2+b^3=\binom{3}{0}\cdot a^{3-0}\cdot b^0+\binom{3}{1}\cdot a^{3-1}\cdot b^1+\binom{3}{2}\cdot a^{3-3}\cdot b^2+\binom{3}{3}\cdot a^{3-3}\cdot b^3$

Verallgemeinert für $(a+b)^n$ folgt:
Wir haben $n+1$ Summenden mit Faktoren $a^{n-k}\cdot b^k$ und Koeffizienten $\binom{n}{k}$ für $0\le k\le n$ also
$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot a^{n-k}\cdot b^k.$$

Die verallgemeinerte zweite binomische Formel folgt dann aus dieser verallgemeinerten ersten binomischen Formel:

$$(a-b)^n=(a+(-b))^n=\sum_{k=0}^{n}\binom{n}{k}\cdot a^{n-k}\cdot\underbrace{(-b)^k}_{=(-1)^k\cdot b^k}=\sum_{k=0}^{n}(-1)^k\cdot\binom{n}{k}\cdot a^{n-k}\cdot b^k$$

Beispiele:

a) $(a+b)^3=\binom{3}{0}\cdot a^{3-0}\cdot b^0+\binom{3}{1}\cdot a^{3-1}\cdot b^1+\binom{3}{2}\cdot a^{3-2}\cdot b^2+\binom{3}{3}\cdot a^{3-3}\cdot b^3=$

$a^3 + 3 \cdot a^2 \cdot b + 3 \cdot a \cdot b^2 + b^3$

$(a-b)^3 = +\binom{3}{0} \cdot a^{3-0} \cdot b^0 - \binom{3}{1} \cdot a^{3-1} \cdot b^1 + \binom{3}{2} \cdot a^{3-2} \cdot b^2 - \binom{3}{3} \cdot a^{3-3} \cdot b^3 =$

$a^3 - 3 \cdot a^2 \cdot b + 3 \cdot a \cdot b^2 - b^3$

$(\sqrt[3]{a} - \sqrt[3]{b})^3 = a - 3\sqrt[3]{a^2} \cdot \sqrt[3]{b} + 3\sqrt[3]{a} \cdot \sqrt[3]{b^2} - b =$

$a - 3 \cdot \sqrt[3]{a^2 \cdot b} + 3 \cdot \sqrt[3]{a \cdot b^2} - b$

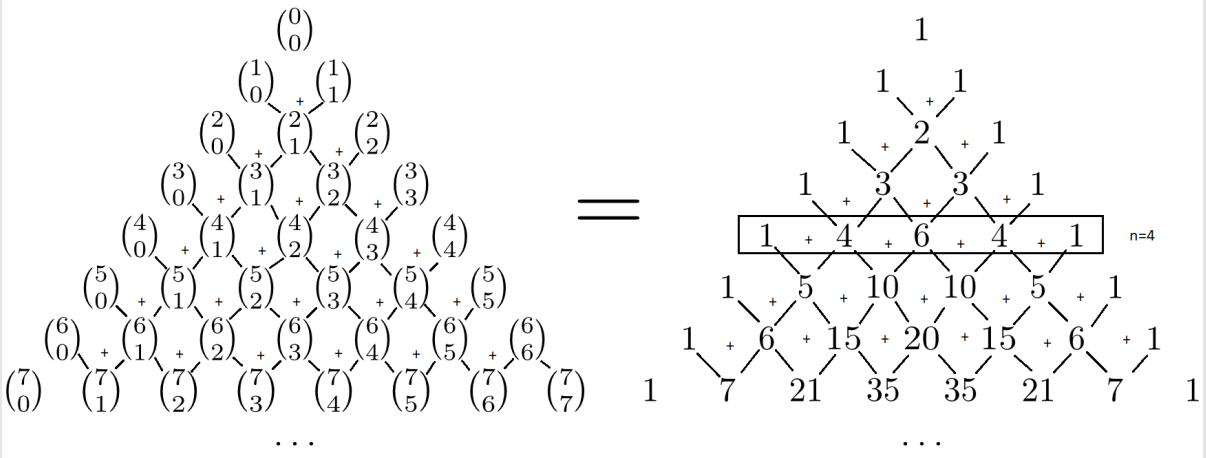
b) $(2x - \frac{1}{3} \cdot y)^3 = \binom{3}{0} \cdot 2^3 \cdot x^3 + \binom{3}{1} \cdot 2^2 \cdot x^2 \cdot \frac{1}{3} \cdot y + \binom{3}{2} \cdot 2 \cdot x \cdot \left(\frac{1}{3}\right)^2 \cdot y^2 + \binom{3}{3} \cdot \left(\frac{1}{3}\right)^3 \cdot y^3 =$
$8x^3 + 3 \cdot 4 \cdot x^2 \cdot \frac{1}{3} y + 3 \cdot 2 \cdot x \cdot \frac{1}{3^2} y^2 + \frac{1}{27} y^3 = 8x^3 + 4x^2 y + \frac{2}{3} x y^2 + \frac{1}{27} y^3$

Zur effektiven, einfachen Berechnung von Binomialkoeffizienten und binomischer Formeln trägt das Pascalsche Dreieck bei.

Das Pascalsche Dreieck (B. Pascal, 1623-1662):

Man ordnet die Binomialkoeffizienten in einem Dreieck an, unter Ausnutzung von

$\binom{n}{0} = \binom{n}{n} = 1$ und $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ erhält man:



So bekommt man z.B.: $(a+b)^4 = 1 \cdot a^4 + 4a^3 \cdot b + 6a^2 \cdot b^2 + 4a \cdot b^3 + 1 \cdot b^4$

Wegen $\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1 \in \mathbb{N}$ folgt aus dem Bildungsgesetz für das Pascalsche Dreeick,

dass gilt:

$\forall n, k \in \mathbb{N}_0, k \leq n$ gilt $\binom{n}{k} \in \mathbb{N}$

Binomialkoeffizienten sind also natürliche Zahlen!

Bevor wir uns mit weiteren Gleichungen und Ungleichungen beschäftigen, definieren wir den **Betrag** einer reellen Zahl.

Definition:
Für $a \in \mathbb{R}$ ist der **Betrag von a** definiert durch

$$|a| = \begin{cases} a & \text{für } a \geq 0 \\ -a & \text{für } a < 0 \end{cases}$$

Beispiele und Bemerkungen:

1) $|-23| = -(-23) = 23$, $|\sqrt{2}| = \sqrt{2}$, $|-\frac{3}{7}| = -(-\frac{3}{7}) = \frac{3}{7}$, $|0| = 0$.

2) **Rechenregeln für $|a|$:**

2.0) Als **alternative Definition** dient: $|a| = \sqrt{a^2}$ also z.B.
$|-3| = \sqrt{(-3)^2} = \sqrt{9} = 3$.

2.1) $\forall a \in \mathbb{R}$ gilt: $|a| \geq 0$ und $|a| = 0 \Leftrightarrow a = 0$.

2.2) $\forall a, b \in \mathbb{R}$ gilt: $|a \cdot b| = |a| \cdot |b|$ und $|a^n| = |a|^n$, $|\sqrt[n]{a}| = \sqrt[n]{|a|}$ $\forall n \in \mathbb{N}$.

2.3) $\forall a, b \in \mathbb{R}, b \neq 0$ gilt: $|\frac{a}{b}| = \frac{|a|}{|b|}$.

2.4) $\forall a \in \mathbb{R}$ gilt: $a \leq |a|$, genauer: $a < 0 \Rightarrow a < |a|$ und $a \geq 0 \Rightarrow |a| = a$.

2.5) Es gilt die **Dreiecksungleichung**: $\forall a, b \in \mathbb{R}$ gilt: $|a + b| \leq |a| + |b|$

Beweisidee zu den Rechenregeln für den Betrag:
Mit der alternativen Definition folgen 2.1), 2.2) und 2.3) direkt aus den Rechenregeln für Potenzen und Wurzeln! 2.4) folgt direkt aus der Definition.

Außerdem gilt $|a+b|^2 = (\sqrt{(a+b)^2})^2 = (a+b)^2 = a^2 + 2 \cdot a \cdot b + b^2 =$

$|a|^2 + 2 \cdot a \cdot b + |b|^2 \leq |a|^2 + 2 \cdot |a| \cdot |b| + |b|^2 = (|a| + |b|)^2$ also $|a+b|^2 \leq (|a| + |b|)^2$ und damit

$|a + b| = \sqrt{|a+b|^2} \leq \sqrt{(|a| + |b|)^2} = |a| + |b|$.

3) Konkretes Beispiel zur Dreiecksungleichung:
$|3+(-4)| = |-1| = 1$ und $|3|+|-4| = 3+4 = 7$: $1 \leq 7$ also $|3+(-4)| \leq |3|+|-4|$.

4) Lineare Ungleichung mit einem Betrag:
Zur Lösung von Ungleichungen der Form $|T(x)| \leq (\geq, <, >) f(x)$ ist eine **Fallunterscheidung**, die am „Vorzeichenwechsel" des Terms $T(x)$ zwischen den Betragsstrichen orientiert ist, notwendig. Der **1. Fall** ist $T(x) \geq 0$, dann ist $|T(x)| = T(x)$; der **2. Fall** ist $T(x) < 0$, dann ist $|T(x)| = -T(x)$.

4.1) Gesucht ist die Lösungsmenge $\mathbb{L}$ der Ungleichung $|x| < 5$
1. Fall: $x \geq 0 \Leftrightarrow x \in [0, +\infty)$
$|x| < 5 \Leftrightarrow x < 5 \Leftrightarrow x \in (-\infty, 5)$
Insgesamt $\mathbb{L}_1 = (-\infty, 5) \cap [0, +\infty) = [0, 5)$
2. Fall: $x < 0 \Leftrightarrow x \in (-\infty, 0)$
$|x| < 5 \Leftrightarrow -x < 5 \Leftrightarrow x > -5 \Leftrightarrow x \in (-5, +\infty)$
Insgesamt $\mathbb{L}_2 = (-\infty, 0) \cap (-5, +\infty) = (-5, 0)$
Aus beiden Fällen zusammen folgt
$\mathbb{L} = \mathbb{L}_2 \cup \mathbb{L}_1 = (-5, 0) \cup [0, 5) = (-5, 5)$

4.2) Gesucht ist die Lösungsmenge $\mathbb{L}$ der Ungleichung $|2 - 3x| \geq 1 + x$
1. Fall: $2 - 3x \geq 0 \Leftrightarrow 3x \leq 2 \Leftrightarrow x \leq \frac{2}{3} \Leftrightarrow x \in (-\infty, \frac{2}{3}]$
$|2 - 3x| \geq 1 + x \Leftrightarrow 2 - 3x \geq 1 + x \Leftrightarrow -4x \geq -1 \Leftrightarrow x \leq \frac{1}{4} \Leftrightarrow x \in (-\infty, \frac{1}{4}]$
Insgesamt $\mathbb{L}_1 = (-\infty, \frac{2}{3}) \cap (-\infty, \frac{1}{4}) = (-\infty, \frac{1}{4}]$
2. Fall: $2 - 3x < 0 \Leftrightarrow -3x < -2 \Leftrightarrow x > \frac{2}{3} \Leftrightarrow x \in (\frac{2}{3}, +\infty)$
$|2 - 3x| \geq 1 + x \Leftrightarrow -(2 - 3x) \geq 1 + x \Leftrightarrow -2 + 3x \geq 1 + x \Leftrightarrow 2x \geq 3 \Leftrightarrow$
$x \geq \frac{3}{2} \Leftrightarrow x \in [\frac{3}{2}, +\infty)$
Insgesamt $\mathbb{L}_2 = (\frac{2}{3}, +\infty) \cap [\frac{3}{2}, +\infty) = [\frac{3}{2}, +\infty)$
Aus beiden Fällen zusammen folgt
$\mathbb{L} = \mathbb{L}_1 \cup \mathbb{L}_2 = (-\infty, \frac{1}{4}] \cup [\frac{3}{2}, +\infty) = \mathbb{R} \backslash (\frac{1}{4}, \frac{3}{2})$.

Quadratische Gleichungen und elementare quadratische Ungleichungen:

a) Für $a \in \mathbb{R}_+^0$ also $a \geq 0$ gilt: $x^2 = a \Leftrightarrow x = \sqrt{a} \vee x = -\sqrt{a}$
Die **Lösungsmenge** der Gleichung $x^2 = a$ ist also $\mathbb{L} = \{-\sqrt{a}, \sqrt{a}\}$.
Im Fall $a = 0$ hat man insbesondere nur eine Lösung, nämlich $x = 0$.
Für $a \in \mathbb{R}, a < 0$ gilt: Die Gleichung $x^2 = a$ hat **keine** Lösung, also $\mathbb{L} = \emptyset$; denn:
$\forall x \in \mathbb{R}$ gilt $x^2 \geq 0$.

b) Quadratische Gleichungen: Für $a_0, a_1, a_2 \in \mathbb{R}, a_2 \neq 0$ hat man die quadratische Gleichung $a_2 \cdot x^2 + a_1 \cdot x + a_0 = 0$.

Zur Lösung geht man wie folgt vor
$0 = a_2 \cdot x^2 + a_1 \cdot x + a_0 = a_2 \cdot \left(x^2 + \frac{a_1}{a_2} \cdot x + \frac{a_0}{a_2}\right)$.

Mit der Substitution $p = \frac{a_1}{a_2}$ und $q = \frac{a_0}{a_2}$ erhält man $a_2 \cdot \left(x^2 + p \cdot x + q\right) = 0 \Leftrightarrow$
$x^2 + p \cdot x + q = 0$
Die letzte Form nennt man „quadratische Gleichung in Normalform “; zur Lösung führt eine **quadratische Ergänzung**:
$x^2 + p \cdot x + q = 0 \Leftrightarrow x^2 + 2 \cdot \frac{p}{2} \cdot x + (\frac{p}{2})^2 + q - (\frac{p}{2})^2 = 0 \Leftrightarrow$
$x^2 + 2 \cdot \frac{p}{2} \cdot x + (\frac{p}{2})^2 = (\frac{p}{2})^2 - q \Leftrightarrow (x + \frac{p}{2})^2 = (\frac{p}{2})^2 - q$
Nach a) hat diese Gleichung **keine Lösung**, falls gilt: $(\frac{p}{2})^2 - q < 0$,
genau eine Lösung nämlich $x + \frac{p}{2} = 0 \Leftrightarrow x = -\frac{p}{2}$ falls gilt: $(\frac{p}{2})^2 - q = 0$ und
zwei Lösungen nämlich $x + \frac{p}{2} = -\sqrt{(\frac{p}{2})^2 - q}, x + \frac{p}{2} = \sqrt{(\frac{p}{2})^2 - q} \Leftrightarrow$
$x_1 = -\frac{p}{2} - \sqrt{(\frac{p}{2})^2 - q}, x_2 = -\frac{p}{2} + \sqrt{(\frac{p}{2})^2 - q}$, falls gilt: $(\frac{p}{2})^2 - q > 0$.

Mit $p = \frac{a_1}{a_2}$ und $q = \frac{a_0}{a_2}$ erhält man

$$x_{1,2} = -\frac{a_1}{2 \cdot a_2} \pm \sqrt{\frac{a_1^2}{4 \cdot a_2^2} - \frac{a_0}{a_2}} = -\frac{a_1}{2 \cdot a_2} \pm \sqrt{\frac{a_1^2 - 4 \cdot a_0 \cdot a_2}{4 \cdot a_2^2}} \Rightarrow$$

$$x_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4 \cdot a_0 \cdot a_2}}{2 \cdot a_2}$$

Diese Formel ist auch als **Mitternachtsformel** bekannt!

c) Für $a \in \mathbb{R}_+^0$ gilt: $x^2 < a \Leftrightarrow |x| < \sqrt{a} \Leftrightarrow -\sqrt{a} < x < \sqrt{a} \Leftrightarrow x \in (-\sqrt{a}, \sqrt{a})$
Für $a \in \mathbb{R}_+^0$ gilt: $x^2 \leq a \Leftrightarrow |x| \leq \sqrt{a} \Leftrightarrow -\sqrt{a} \leq x \leq \sqrt{a} \Leftrightarrow x \in [-\sqrt{a}, \sqrt{a}]$
Für $a \in \mathbb{R}_+^0$ gilt: $x^2 > a \Leftrightarrow |x| > \sqrt{a} \Leftrightarrow x < -\sqrt{a} \vee x > \sqrt{a} \Leftrightarrow x \in (-\infty, -\sqrt{a}) \cup (\sqrt{a}, +\infty) = \mathbb{R} \backslash [-\sqrt{a}, \sqrt{a}]$
Für $a \in \mathbb{R}_+^0$ gilt: $x^2 \geq a \Leftrightarrow |x| \geq \sqrt{a} \Leftrightarrow x \leq -\sqrt{a} \vee x \geq \sqrt{a} \Leftrightarrow x \in (-\infty, -\sqrt{a}] \cup [\sqrt{a}, +\infty) = \mathbb{R} \backslash (-\sqrt{a}, \sqrt{a})$

Der Begriff des Logarithmus

Unabhängig von der Einführung der Logarithmusfunktion als Umkehrfunktion der Exponentialfunktion (dies ist Bestandteil von Mathematik 2 für Informatik) soll hier der Logarithmus als „Rechenvorschrift “ eingeführt werden.

Definition:
Für $a, b \in \mathbb{R}_+$ ist der **Logarithmus von a zur Basis b** $\log_b(a)$ definiert als Lösung der Gleichung $b^x = a$, also: $x = \log_b(a) \Leftrightarrow b^x = a$.

Bemerkungen und Beispiele:

a) Folgende Bezeichnungen sind üblich: $\log_{10}(a) = \log(a) = \lg(a)$, $\log_2(a) = \mathrm{ld}(a)$, $\log_e(a) = \ln(a)$.

b) Rechenregeln für den Logarithmus:

1) $\log_b(1) = 0, \log_b(b) = 1$

2) $\log_b(a_1 \cdot a_2) = \log_b(a_1) + \log_b(a_2)$

3) $\log_b(\frac{a_1}{a_2}) = \log_b(a_1) - \log_b(a_2)$

4) $\log_b(a^\alpha) = \alpha \cdot \log_b(a)$

c) $\log_{10}(1000) = \log_{10}(10^3) = \lg(10^3) = 3$, $\log_{10}(\frac{1}{100}) = \lg(\frac{1}{100}) = \lg(10^{-2}) = -2$

$\log_5(625) = \log_5(25 \cdot 25) = \log_5(25) + \log_5(25) = \log_5(5^2) + \log_5(5^2) = 2 + 2 = 4$

$\log_2(1024) = \mathrm{ld}(1024) = \mathrm{ld}(2^{10}) = 10$

d) Lösen Sie die Gleichung $2^{2 \cdot x} - 5 \cdot 2^x + 6 = 0$

$2^{2 \cdot x} - 5 \cdot 2^x + 6 = 0 \Leftrightarrow (2^x)^2 - 5 \cdot 2^x + 6 = 0$, die Substitution $t = 2^x$ liefert
$t^2 - 5 \cdot t + 6 = 0 \Leftrightarrow (t-2) \cdot (t-3) = 0 \Leftrightarrow t_1 = 2 \vee t_2 = 3$.
Rücksubstitution ergibt dann:
$2^{x_1} = t_1 = 2 \Rightarrow x_1 = \mathrm{ld}(2) = 1$, $2^{x_2} = t_2 = 3 \Rightarrow x_2 = \mathrm{ld}(3)$
Die Lösungsmenge der Gleichung ist damit $\mathbb{L} = \{1, \mathrm{ld}(3)\}$

Probe:

$2^{2 \cdot 1} - 5 \cdot 2^1 + 6 = 4 - 10 + 6 = 0$ und

$2^{2 \cdot \mathrm{ld}(3)} - 5 \cdot 2^{\mathrm{ld}(3)} + 6 = (2^{\mathrm{ld}(3)})^2 - 5 \cdot 3 + 6 = 3^2 - 5 \cdot 3 + 6 = 9 - 15 + 6 = 0$

4.4 Algebraische Strukturen

Die aus dem Rechnen in $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ bekannten „Rechengesetze“ für $+$ und $\cdot$ geben Anlass zu folgenden **verallgemeinernden Überlegungen** bezüglich der dargestellten Strukturen.

4.4.1 Halbgruppen und Gruppen

Definition:
Eine **Verknüpfung (Rechenoperation)** auf einer Menge $M, M \neq \emptyset$ ist eine Abbildung $\otimes : M \times M \to M$, d.h. $(a, b) \in M \times M \to a \otimes b \in M$

Einem Tupel $(a, b) \in M \times M$ wird also ein Element $a \otimes b$ aus M zugeordnet. **Beispiele** für Verknüpfungen (Rechenoperationen) sind die **Addition** oder die **Multiplikation** auf $M = \mathbb{Z}$ oder $M = \mathbb{Q}$ oder $M = \mathbb{R}$.

Definiton:
Gegeben ist eine Menge $M, M \neq \emptyset$ und eine Verknüpfung (Rechenoperation) $\otimes : M \times M \to M$.

1) $(M, \otimes)$ ist eine **Halbgruppe**, wenn gilt
Assoziativgesetz: $a \otimes (b \otimes c) = (a \otimes b) \otimes c, \forall a, b, c \in M$

2) $(M, \otimes)$ ist eine **Gruppe**, wenn gilt
Assoziativgesetz: $a \otimes (b \otimes c) = (a \otimes b) \otimes c, \forall a, b, c \in M$
Existenz eines neutralen Elements: $\exists n \in M : a \otimes n = a, \forall a \in M$
Existenz inverser Elemente: $\forall a \in M \, \exists a^{-1} \in M : a \otimes a^{-1} = n$,
gilt **zusätzlich** das
Kommutativgesetz: $a \otimes b = b \otimes a, \forall a, b \in M$
heißt $(M, \otimes)$ **abelsche Gruppe**.

Beispiele:$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind **abelsche Gruppen**; das **neutrale Element** ist die 0 und das **inverse Element** zu a ist $a^{-1} = -a$.
$(\mathbb{N}, +)$ ist eine **Halbgruppe**, in der zusätzlich das Kommutativgesetz gilt.
$(\mathbb{Z}, \cdot)$ ist eine **Halbgruppe**, in der zusätzlich das Kommutativgesetz gilt und ein neutrales Element (die 1) existiert.
$(\mathbb{Z}, \cdot)$ ist aber **keine abelsche Gruppe**, da z.B. zu $2 \in \mathbb{Z}$ bezüglich der Verknüpfung $\cdot$ kein inverses Element existiert (denn $2^{-1} = \frac{1}{2}$ ist kein Element von $\mathbb{Z}$).
$(\mathbb{Q}, \cdot)$ ist auch **keine abelsche Gruppe**, da zu $0 \in \mathbb{Q}$ bezüglich der Verknüpfung $\cdot$ kein inverses Element existiert!
Für $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$ gilt jedoch: $(\mathbb{Q}^*, \cdot)$ ist eine **abelsche Gruppe**, da zu $a \in \mathbb{Q}^*$ bezüglich der Verknüpfung $\cdot$ das inverse Element $a^{-1} = \frac{1}{a}$ existiert (denn $a \neq 0$).
Für $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ gilt ebenfalls: $(\mathbb{R}^*, \cdot)$ ist eine **abelsche Gruppe**, da zu $a \in \mathbb{R}^*$ bezüglich der Verknüpfung $\cdot$ das inverse Element $a^{-1} = \frac{1}{a}$ existiert (denn $a \neq 0$).

4.4.2 Ringe

Definition:
Gegeben sind eine Menge $M, M \neq \emptyset$ und **zwei** Verknüpfungen (Rechenoperationen)

$\oplus : M \times M \to M$ und $\otimes : M \times M \to M$.

$(M, \oplus, \otimes)$ ist ein **Ring**, falls gilt:

1) $(M, \oplus)$ ist eine **abelsche Gruppe**

2) $(M, \otimes)$ ist eine **Halbgruppe**

3) Es gilt das **Distributivgesetz**: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)\ \forall a, b, c \in M$.

Hat $(M, \otimes)$ zusätzlich ein **neutrales Element**, nennt man $(M, \oplus, \otimes)$ einen **Ring mit Eins**. Gilt in einem Ring mit Eins zusätzlich in $(M, \otimes)$ das **Kommutativgesetz**, nennt man $(M, \oplus, \otimes)$ einen **kommutativen Ring mit Eins**.

Beispiel:

a) $(\mathbb{Z}, +, \cdot)$ ist ein **kommutativer Ring mit 1**.

b) $(\mathbb{N}_0, +, \cdot)$ ist **kein Ring**, denn $(\mathbb{N}_0, +)$ ist keine abelsche Gruppe.

4.4.3 Körper

Definition:
Gegeben sind eine Menge $M, M \neq \emptyset$ und **zwei** Verknüpfungen (Rechenoperationen) $\oplus : M \times M \to M$ und $\otimes : M \times M \to M$.

$(M, \oplus, \otimes)$ ist ein **Körper**, falls gilt:

1) $(M, \oplus)$ ist eine **abelsche Gruppe**, $0 \in M$ bezeichnet das neutrale Element in $(M, \oplus)$.

2) $(M \backslash \{0\}, \otimes)$ ist eine **abelsche Gruppe**

3) Es gelten die **Distributivgesetze**: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)\ \forall a, b, c \in M$ und $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)\ \forall a, b, c \in M$.

Bemerkung:
Ein Körper $(M, \oplus, \otimes)$ genügt also bezüglich der Verknüpfungen (Rechenoperationen) folgenden **5 Körperaxiomen** $\forall a, b, c \in M$:

Name	$\oplus$	$\otimes$
Kommutativgesetz	$a \oplus b = b \oplus a$	$a \otimes b = b \otimes a$
Assoziativgesetz	$a \oplus (b \oplus c) = (a \oplus b) \oplus c$	$a \otimes (b \otimes c) = (a \otimes b) \otimes c$
Existenz neutraler Elemente	$a \oplus 0 = a$	$a \otimes 1 = a$
Existenz inverser Elemente	$a \oplus (-a) = 0$	$a \otimes a^{-1} = 1 \forall a \neq 0$
Distributivgesetze	$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$	$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Beispiel: Ein Körper $\mathbb{K}$ mit zwei Elementen

Wir betrachten die Menge $\mathbb{K} = \{0, 1\}$ mit den durch die folgenden Tabellen (Verknüpfungstabellen) gegebenen Rechenoperationen Addition und Multiplikation

$+$	0	1
0	0	1
1	1	0

$\bullet$	0	1
0	0	0
1	0	1

$(\mathbb{K}, +, \bullet)$ ist ein Körper. 0 ist das neutrale Element der Addition, 1 ist das neutrale Element der Multiplikation. Mit $0 + 0 = 0$ und $1 + 1 = 0$ sind auch die inversen Elemente zu 0, 1 bezüglich der Addition bestimmt.
Wegen $1 \bullet 1 = 1$ ist 1 das inverse Element der Multiplikation zum einzigen Element $1 \in \mathbb{K}^* = \mathbb{K} \backslash \{0\}$.

Weitere Beispiele für **Halbgruppen, Gruppen, Ringe und Körper** liefert das folgende 5. Kapitel.

5 Elementare Zahlentheorie

5.1 Einführung: Teilen in $\mathbb{Z}$

Wir betrachten die Menge der ganzen Zahlen $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ und ihre (echten) Teilmengen $\mathbb{N} = \{1, 2, 3, 4, ...\}$ und $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, die natürlichen Zahlen und die natürlichen Zahlen inklusive der 0.
Zunächst werden einige elementare Begriffe und Sachverhalte geklärt.

Definition:

a) Für $a, b \in \mathbb{Z}$ mit $b \neq 0$ gilt: a **teilt** b (in Kurzform $a \mid b$), falls eine Zahl $k \in \mathbb{Z}$, $k \neq 0$, existiert mit $b = k \cdot a$.
Man nennt a dann einen (echten) **Teiler** von b.

b) Eine Zahl $p \in \mathbb{N}$ heißt **Primzahl**, falls gilt: $p > 1$ und p hat nur die Teiler 1 und p.
Die **Menge der Primzahlen** wird mit $\mathbb{P}$ bezeichnet.

c) Für $b \in \mathbb{Z}$ ist die **Teilermenge von** b definiert als: $T(b) = \{a \in \mathbb{Z} \mid a \text{ teilt } b \text{ kurz } (a \mid b)\}$.

Bemerkung:

1. Für alle $b \in \mathbb{Z}$ gilt: $T(b) \neq \emptyset$, denn $1 \mid b \, \forall b \in \mathbb{Z}$ und $b \mid b \, \forall b \in \mathbb{Z} \Rightarrow 1 \in T(b), b \in T(b)$ $\forall b \in \mathbb{Z}$.

2. Für alle $b \in \mathbb{Z}$ gilt: $0 \notin T(b)$, denn $k \cdot 0 = 0 \; \forall k \in \mathbb{Z}$, d.h. 0 ist Teiler **keiner** ganzen Zahl!

3. $p \in \mathbb{P} \Leftrightarrow T(p) = \{1, p\}$.

4. Es gilt für alle $b \in \mathbb{Z}$: $T(b) = T(-b)$, denn $a \in T(b) \Rightarrow b = k \cdot a \Rightarrow -b = (-k) \cdot a \Rightarrow$ $a \in T(-b)$ also $T(b) \subseteq T(-b)$. Die Inklusion $T(-b) \subseteq T(b)$ zeigt man analog.
Für viele Aussagen zur Teilbarkeit reicht es daher aus, $T(b)$ **für** $b \in \mathbb{N}$ **zu betrachten!**

5. Es gelten folgende Aussagen für $a, b, c \in \mathbb{Z}$:
$a|b \Rightarrow -a|b$
$a|b \wedge c \neq 0 \Rightarrow a \cdot c|b \cdot c$
$a|b \wedge b|c \Rightarrow a|c$
$a|b \wedge a|c \Rightarrow a|k \cdot b + l \cdot c$ für alle $k, l \in \mathbb{Z}$
$a|b \wedge b|a \Rightarrow (a = b) \vee (a = -b)$.

Satz:
Die Teilermenge $T(b)$ jeder Zahl $b \in \mathbb{Z}$ ist **endlich**, d.h. $T(b)$ hat nur **endlich viele** Elemente.
Beweis:
$a \in T(b) \Rightarrow \exists k \in \mathbb{Z}\backslash\{0\}$ mit $b = k \cdot a \Rightarrow \mid k \mid \geq 1$ und $|b| = |k| \cdot |a|$ mit $|k| \geq 1$. Wegen $|k| \geq 1$ ist $\frac{1}{|k|} \leq 1$ und damit $|a| = \frac{1}{|k|} \cdot |b| \leq |b|$. Damit gilt $a \in [-|b|, |b|] \cap \mathbb{Z}$ und das sind höchstens endlich viele ganze Zahlen!

Definition:

a) Für $a, b \in \mathbb{Z}\backslash\{0\}$ ist die **Menge der gemeinsamen Teiler** definiert als $T(a, b) = T(a) \cap T(b)$.

b) Der **größte gemeinsame Teiler** ggT(a, b) ist das Maximum (größte Element) der Menge $T(a, b)$ der gemeinsamen Teiler von a, b.

c) Die Zahlen $a, b \in \mathbb{Z}\backslash\{0\}$ heißen **teilerfremd**, wenn gilt ggT$a, b) = 1$, d.h. die 1 ist der einzige und damit auch größte gemeinsame Teiler von a und b.

Bemerkung:

1. Es gilt $1 \in T(a, b)$ für alle $a, b \in \mathbb{Z}\backslash\{0\}$, also ist $T(a, b) \neq \emptyset$.
2. $T(a, b) = T(a) \cap T(b)$ ist als Durchschnitt der endlichen Mengen $T(a)$ und $T(b)$ ebenfalls eine endliche Menge, daher ist ggT(a, b) als größtes Element aus einer endlichen Menge von Zahlen immer definiert!
3. Für alle $a \in \mathbb{Z}\backslash\{0\}$ und für alle Primzahlen $p \in \mathbb{P}$ gilt: ggT$(a, p) = 1$ falls $a \neq p$ ist.

Satz: (Teilen mit Rest)

Für $b \in \mathbb{Z}\backslash\{0\}$ und $m \in \mathbb{Z}\backslash\{0\}$ gilt:

Es gibt **eindeutig bestimmte** Zahlen $k \in \mathbb{Z}$ und $r \in \mathbb{Z}$ mit $0 \leq r < |m|$, so dass gilt: $b = k \cdot m + r$.

Bemerkung:

a) r ist der **Rest** von b bei Division durch m; man schreibt dafür $r = b$ **mod** m. Dabei ist **mod** die Abkürzung für „**modulo**“.

b) Es reicht, die Behauptung für $m > 0$ zu zeigen, denn:
$m < 0 \Rightarrow -m > 0$ und damit liefert der Satz angewandt mit $-m > 0$ auf $-b$:
Es ist $-b = k^* \cdot (-m) + r^*$ mit $k^* \in \mathbb{Z}$ und $r^* \in \mathbb{Z}$ mit $0 \leq r^* < -m \Rightarrow b = k^* \cdot m - r^*$.
Für $r^* = 0$ ist der Beweis erbracht, man hat nämlich $b = k^* \cdot m + 0$.
Gilt $r^* > 0$ hat man $b = k^* \cdot m - r^* = (k^* + 1) \cdot m - m - r$. Mit $k = k^* + 1$ und $r = -m - r^*$ hat man die gewünschte Darstellung $b = k \cdot m + r$. Wegen $0 < r^* < -m$ hat man (wie im Satz gefordert) $0 < -m - r^* < -m \Leftrightarrow 0 < r < |m|$.

c) Es reicht, die Behauptung für $b > 0$ zu zeigen, denn: Nach b) können wir $m > 0$ voraussetzen. Sei $b < 0 \Rightarrow -b > 0$ und damit liefert der Satz angewandt mit $m > 0$ auf $-b$:
Es ist $-b = \tilde{k} \cdot m + \tilde{r}$ mit $\tilde{k} \in \mathbb{Z}$ und $\tilde{r} \in \mathbb{Z}$ sowie $0 \leq \tilde{r} < m \Rightarrow b = -\tilde{k} \cdot m - \tilde{r} = (-\tilde{k} - 1) \cdot m + m - \tilde{r}$. Mit $k = -\tilde{k} - 1$ und $r = m - \tilde{r}$ hat man wie gewünscht $b = k \cdot m + r$ und wegen $0 \leq \tilde{r} < m \Rightarrow 0 \leq m - \tilde{r}$ gilt auch $0 \leq r < m$.

Beweis des Satzes über das Teilen mit Rest unter der Voraussetzung $b \in \mathbb{N}$ und $m \in \mathbb{N}$ mit $m \geq 2$ durch vollständige Induktion:

Behauptung:
Gegeben ist $m \in \mathbb{N}$. Dann gibt es für jedes $b \in \mathbb{N}$ Zahlen $k \in \mathbb{N}$ und $r \in \mathbb{N}_0$ mit $b = k \cdot m + r$ und $0 \leq r < m$.

Induktionsanfang: $b = 1$

Wegen $m \in \mathbb{N}$ mit $m \geq 2$ gilt $b \leq m$. Setzt man $k = 0$ und $r = b$ folgt $b = 0 \cdot m + b = k \cdot m + r$ mit $0 \leq r < m$.

Induktionsvoraussetzung: Für $b = u$ gilt $u = k \cdot m + r$ mit $k, r, u \in \mathbb{Z}, 0 \leq r < m$.

Induktionsbehauptung: Für $b = u + 1$ gilt $u + 1 = k^* \cdot m + r^*$ mit $k^*, r^* \in \mathbb{Z}, 0 \leq r^* < m$.

Beweis:

Aus der Induktionsvoraussetzung folgt $u + 1 = (k \cdot m + r) + 1 = k \cdot m + (r + 1)$ mit $0 \leq r < m$. Also ist $1 \leq r + 1 < m + 1$. Wir haben zwei Fälle, nämlich $1 \leq r + 1 < m$ und $1 \leq r + 1 = m$
1. Fall: $r + 1 < m$
Dann ist die Induktionsbehauptung mit $k^* = k$ und $r^* = r + 1$ erfüllt:
$u + 1 = (k \cdot m + r) + 1 = k \cdot m + (r + 1) = k \cdot m + r^*$ mit $0 \leq r^* < m$.
2. Fall: $r + 1 = m$
$u + 1 = (k \cdot m + r) + 1 = k \cdot m + (r + 1) = k \cdot m + m = (k + 1) \cdot m$. Mit $k^* = k + 1$ und $r^* = 0$ hat man also $u + 1 = k^* \cdot m + r^*$ mit $0 \leq r^* < m$.

Die Teilbarkeitsrelation:

1. **Die Teilbarkeitsrelation über $\mathbb{Z}$:**
   Die Teilbarkeitsrelation $T \subseteq \mathbb{Z} \times \mathbb{Z}$ ist definiert durch:
   $(a, b) \in T \Leftrightarrow a \mid b$.
   Es gilt $a \mid a \Leftrightarrow (a, a) \in T$ also ist T **reflexiv**.
   Es gilt $(a \mid b \wedge b \mid c \Rightarrow a \mid c) \Leftrightarrow ((a, b) \in T \wedge (b, c) \in T \Rightarrow (a, c) \in T)$ also ist T **transitiv**.
   Es gilt z.B. $3 \mid -6$ aber -6 ist kein Teiler von 3 $\Rightarrow$ T ist nicht symmetrisch.
   Es gilt z.B. $2 \mid -2$ und $-2 \mid 2$ aber $2 \neq -2 \Rightarrow$ T ist nicht antisymmetrisch.

2. **Die Teilbarkeitsrelation über $\mathbb{N}$:**
   Die Teilbarkeitsrelation $T \subseteq \mathbb{N} \times \mathbb{N}$ ist definiert durch:
   $(a, b) \in T \Leftrightarrow a \mid b$.
   Es gilt $a \mid a \Leftrightarrow (a, a) \in T$ also ist T **reflexiv**.
   Es gilt $(a \mid b \wedge b \mid c \Rightarrow a \mid c) \Leftrightarrow ((a, b) \in T \wedge (b, c) \in T \Rightarrow (a, c) \in T)$ also ist T **transitiv**.
   Es gilt: $((a, b) \in T \wedge (b, a) \in T) \Leftrightarrow (a \mid b \wedge b \mid a) \Leftrightarrow (a = k \cdot b \wedge b = n \cdot a)$
   also gilt in $\mathbb{N}$: $a = k \cdot b = k \cdot (n \cdot a) = (k \cdot n) \cdot a$
   In $\mathbb{N}$ folgt damit $k \cdot n = 1 \Rightarrow (k = 1 \wedge n = 1) \Rightarrow a = b$ also ist T **antisymmetrisch**.
   Damit ist insgesamt gezeigt, dass $T \subseteq \mathbb{N} \times \mathbb{N}$ eine **Ordnungsrelation** ist.

5.2 Der euklidische Algorithmus

Der **euklidische Algorithmus** ist ein Verfahren zur Berechnung des größten gemeinsamen Teilers zweier Zahlen $a, b \in \mathbb{N}$.

Gegeben sind $a, b \in \mathbb{N}$ mit $b \geq a$.

a) **Vorbemerkung 1**
Für $b = a$ gilt: $\text{ggT}(a, b) = \text{ggT}(a, a) = a$.

b) **Vorbemerkung 2**
Für $b > a$ gilt: Nach dem **Satz über Teilen mit Rest** hat man die Darstellung $b = k \cdot a + r$ mit $0 \leq r < a$ und es gilt $\text{ggT}(a, b) = \text{ggT}(r, a)$ denn für die Teilermengen gilt $T(a, b) = T(r, a)$.
Beweis: $q \in T(a, b) \Rightarrow q \mid a$ und $q \mid b$ also $a = n \cdot q$ und $b = \tilde{n} \cdot q$ und damit $r = b - k \cdot a = (\tilde{n} \cdot q) - (k \cdot n \cdot q) = (\tilde{n} - k \cdot n) \cdot q \Rightarrow q \mid r \Rightarrow q \in T(r, a)$.
Es folgt ebenfalls $q \in T(r, a) \Rightarrow q \mid a$ und $q \mid r$ also $a = n \cdot q$ und $r = \tilde{n} \cdot q$ und damit $b = k \cdot a + r = k \cdot \ (n \cdot q) + \tilde{n} \cdot q = (k \cdot n + \tilde{n}) \cdot q \Rightarrow q \in T(a, b)$.

c) **euklidischer Algorithmus**
Der größte gemeinsame Teiler $\text{ggT}(a, b)$ wird jetzt durch iterierte Anwendung des Satzes vom Teilen mit Rest berechnet:

1. Setze $x_0 = b$ und $x_1 = a$
2. Teilen mit Rest $x_0 = k \cdot x_1 + r$
3. Solange $r \neq 0$ setze $x_0 = x_1$ und $x_1 = r$ und gehe zu 2.
4. Wenn $r = 0$ ist, ist $\text{ggT}(a, b) = x_0$

Für weitere Beweise benötigen wir eine weitere Version der **vollständigen Induktion**:

Eine Aussage(form) $A(n)$ für $n \in \mathbb{N}$ ist **wahr für alle** $n \in \mathbb{N}$ **mit** $n \geq n_0$, falls gilt:

1. $A(n_0)$ ist wahr (Induktionsanfang).
2. Für $n \geq n_0$ gilt: $A(n)$ ist wahr für alle $k \in \mathbb{N}, k < n \Rightarrow A(n)$ ist wahr (Induktionsschluss).

Dabei ist im Induktionsschluss die **Induktionsvoraussetzung**:
$A(n)$ ist wahr für alle $k \in \mathbb{N}, k < n$.
Die zu beweisende **Induktionsbehauptung** ist $A(n)$ ist wahr.

Satz: (Lemma von Bézout)
Gegeben sind $a, b \in \mathbb{Z}, b \geq a$. Dann gibt es Zahlen $s, t \in \mathbb{Z}$ mit:

$$\text{ggT}(a, b) = s \cdot a + t \cdot b.$$

Beweis:
Der Beweis wird für $a, b \in \mathbb{N}$ geführt. 1. $b = a$: Dann ist $\text{ggT}(a, b) = \text{ggT}(a, a) = a = 1 \cdot a + 0 \cdot b$.
Die Aussage gilt also mit $s = 1, t = 0$.

2. $b > a$: Beweis mit vollständiger Induktion bezüglich $b \in \mathbb{N}$.

Induktionsanfang: $b = 2, a = 1$ ($b = 1, a = 1$ siehe 1.)
$\text{ggT}(a, b) = \text{ggT}(1, 2) = 1 = 1 \cdot a + 0 \cdot b$. Die Aussage gilt also mit $s = 1, t = 0$.
Induktionsvoraussetzung: Für alle $c \in \mathbb{N}, c < b$ gilt: Es gibt (eindeutig bestimmte) Zahlen $s, t \in \mathbb{Z}$ mit: $\text{ggT}(a, c) = s \cdot a + t \cdot c$.
Induktionsbehauptung: Es gibt (eindeutig bestimmte) Zahlen $\tilde{s}, \tilde{t} \in \mathbb{Z}$ mit: $\text{ggT}(a, b) = \tilde{s} \cdot a + \tilde{t} \cdot b$.

Beweis:
Teilen mit Rest liefert $b = k \cdot a + r$ mit $\text{ggT}(a, b) = \text{ggT}(a, r)$. Damit erhält man $r = b - k \cdot a$.
Da $r < a < b$ gilt, liefert die Induktionsvoraussetzung, dass es Zahlen $s, t \in \mathbb{Z}$ mit: $\text{ggT}(a, r) = s \cdot a + t \cdot r$ und damit
$\text{ggT}(a, b) = \text{ggT}(a, r) = s \cdot a + t \cdot r = s \cdot a + t \cdot (b - k \cdot a) = (s - k \cdot t) \cdot a + t \cdot b$.
Das entspricht der Behauptung mit $\tilde{s} = s - k \cdot t$ und $\tilde{t} = t$.

Beispiele:

1. $378 = 8 \cdot 45 + 18$
   $45 = 2 \cdot 18 + 9$
   $18 = 2 \cdot 9 + 0$
   $\Rightarrow \text{ggT}(378, 45) = \text{ggT}(45, 18) = \text{ggT}(18, 9) = 9$

   Aus der vorletzten Zeile kann man „zurückrechnen“, um die Aussage des Lemmas von Bézout zu bekommen:

   $9 = 45 - 2 \cdot 18$ und mit der übergeordneten Zeile
   $9 = 45 - 2 \cdot (378 - 8 \cdot 45) = 17 \cdot 45 - 2 \cdot 378$

   Gemäß dem Lemma von Bézout folgt also:
   $9 = \text{ggT}(45, 378) = s \cdot 45 + t \cdot 378$ mit $s = 17$ und $t = -2$.

2. $2520 = 17 \cdot 143 + 89$
   $143 = 1 \cdot 89 + 54$

$89 = 1 \cdot 54 + 35$
$54 = 1 \cdot 35 + 19$
$35 = 1 \cdot 19 + 16$
$19 = 1 \cdot 16 + 3$
$16 = 5 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$
$\Rightarrow \text{ggT}(2520, 143) = \text{ggT}(143, 89) = \text{ggT}(89, 54) = \text{ggT}(54, 35) = \text{ggT}(35, 19) = \text{ggT}(19, 16) = \text{ggT}(16, 3) = \text{ggT}(3, 1) = 1.$

Die Zahlen 2520 und 143 sind also teilerfremd.

Aus der vorletzten Zeile kann man „zurückrechnen“, um die Aussage des Lemmas von Bézout zu bekommen:

$1 = \text{ggT}(143, 2520) = 16 - 5 \cdot 3$
$= 16 - 5 \cdot (19 - 1 \cdot 16) = -5 \cdot 19 + 6 \cdot 16$
$= -5 \cdot 19 + 6 \cdot (35 - 1 \cdot 19) = 6 \cdot 35 - 11 \cdot 19$
$= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35) = -11 \cdot 54 + 17 \cdot 35$
$= -11 \cdot 54 + 17 \cdot (89 - 1 \cdot 54) = 17 \cdot 89 - 28 \cdot 54$
$= 17 \cdot 89 - 28 \cdot (143 - 1 \cdot 89) = -28 \cdot 143 + 45 \cdot 89$
$= -28 \cdot 143 + 45 \cdot (2520 - 17 \cdot 143) = -793 \cdot 143 + 45 \cdot 2520$

Gemäß dem Lemma von Bézout folgt also:
$1 = \text{ggT}(143, 2520) = s \cdot 143 + t \cdot 2520$ mit $s = -793$ und $t = 45$.

5.3 Modulare Arithmetik: Rechnen mit Restklassen

Unter „modularer Arithmetik“ bzw. „modularem Rechnen“ versteht man (seit Gauß) das Rechnen mit Resten bei der Division durch eine natürliche Zahl $m \in \mathbb{N}$, die **Modul** genannt wird.

Gegeben der Modul $m \in \mathbb{N}$. Für $b \in \mathbb{Z}$ liefert der Satz vom Teilen mit Rest die eindeutige Darstellung $b = k \cdot m + r$ mit $0 \leq r < m$. Der **Rest** r ist der “Rest beim (ganzzahligen) Teilen von $b \in \mathbb{Z}$ durch m“, man schreibt (s.o.) $r = b \bmod m$.

Beispiele und Bemerkungen:

1. Mit $m = 7$ hat man
   $1 = 15 \bmod 7$, denn $15 = 2 \cdot 7 + 1$.
   $3 = -25 \bmod 7$, denn $-25 = (-4) \cdot 7 + 3$.

$0 = 63 \bmod 7$, denn $63 = 9 \cdot 7 + 0$

2. Man erhält
   $7 = 3237 \bmod 10$, denn $3237 = 323 \cdot 10 + 7$
   $37 = 3237 \bmod 100$, denn $3237 = 32 \cdot 100 + 37$
   $237 = 3237 \bmod 1000$, denn $3237 = 3 \cdot 1000 + 237$

   Im **Dezimalsystem** liefert also $r = b \bmod 10^k$ die **letzten k Dezimalstellen** der Zahl b.

3. Wegen $0 \leq r < m$ bei $r = b \bmod m \Leftrightarrow b = k \cdot m + r$ folgt:
   Die **möglichen Reste beim (ganzzahligen) Teilen durch** m sind
   $0, 1, 2, 3, ..., m-1$ also $r \in \{0, 1, 2, 3, ..., m-1\}$

Definition: (Restklassen)
Gegeben ist der Modul $m \in \mathbb{N}$. Dann ist für $n \in \mathbb{N}_0$ mit $0 \leq n \leq m-1$ die **Restklasse modulo m** definiert als Menge durch:

$$\overline{n} = \{b \in \mathbb{Z} | n = b \bmod m\} = \{b \in \mathbb{Z} | b = k \cdot m + n\}.$$

Bei gegebenem Modul $m \in \mathbb{N}$ enthält die Menge $\overline{n}$ alle Zahlen $b \in \mathbb{Z}$, die beim (ganzzahligen) Teilen durch m den Rest n lassen.

Die **Menge aller Restklassen modulo m** wird mit $\mathbb{Z}_m$ bezeichnet.
Es ist also $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$

Bemerkung:

1. Es ist also z.B. für $m = 5$:
   $\overline{0} = \{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\}$
   $\overline{1} = \{\cdots, -14, -9, -4, 1, 6, 11, 16, \cdots\}$
   $\overline{2} = \{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$
   $\overline{3} = \{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\}$
   $\overline{4} = \{\cdots, -11, -6, -1, 4, 9, 14, 19, \cdots\}$

2. Als Hinweis zum **Rechnen mit Resten/Restklassen** berechnet man bei gegebenem Modul $m = 5 \in \mathbb{N}$ zum Beispiel für $b_1 \in \overline{1} (\Leftrightarrow 1 = b_1 \bmod 5)$ und $b_2 \in \overline{3} (\Leftrightarrow 3 = b_2 \bmod 5)$;
   b_1 bzw. b_2 nennt man **Repräsentanten/Vertreter** der Restklassen $\overline{1}$ bzw. $\overline{3}$ modulo 5. Man erhält:

$b_1 = k_1 \cdot 5 + 1, b_2 = k_2 \cdot 5 + 3 \Rightarrow b_1 + b_2 = (k_1 + k_2) \cdot 5 + 1 + 3 = (k_1 + k_2) \cdot 5 + 4 \Rightarrow 4 = (b_1 + b_2) \bmod 5$

Nun ist $4 = 1 + 3 = b_1 \bmod 5 + b_2 \bmod 5$, wir erhalten also als ersten Hinweis auf eine Rechenregel: $(b_1 + b_2) \bmod 5 = b_1 \bmod 5 + b_2 \text{mod} 5$

Betrachtet man jetzt $b_1 \in \overline{3} \Rightarrow 3 = b_1 \bmod 5$ und $b_2 \in \overline{4} \Rightarrow 4 = b_2 \bmod 5$ so erhält man
$b_1 = k_1 \cdot 5 + 3, b_2 = k_2 \cdot 5 + 4 \Rightarrow b_1 + b_2 = (k_1 + k_2) \cdot 5 + 4 + 3 = (k_1 + k_2) \cdot 5 + 7 = (k_1 + k_2) \cdot 5 + 5 + 2 = (k_1 + k_2 + 1) \cdot 5 + 2 \Rightarrow 2 = (b_1 + b_2) \bmod 5$.

Nun ist $2 = 7 \text{ mod} 5 = (3+4) \bmod 5 = (b_1 \bmod 5 + b_2 \bmod 5) \bmod 5$, wir erhalten also insgesamt als Hinweis auf eine Rechenregel: $(b_1 + b_2) \bmod 5 = (b_1 \bmod 5 + b_2 \bmod 5) \bmod 5$

Für die **Addition von Restklassen** bietet sich also folgende **Definition** an:

$$\overline{n} + \overline{k} = \overline{(n + k) \bmod m},$$

man berechnet also den **„Rest der Summe der Reste modulo m“**.

Beim Multiplizieren gilt
$b_1 \in \overline{3} \Rightarrow 3 = b_1 \bmod 5$ und $b_2 \in \overline{4} \Rightarrow 4 = b_2 \bmod 5$ so erhält man
$b_1 = k_1 \cdot 5 + 3, b_2 = k_2 \cdot 5 + 4 \Rightarrow b_1 \cdot b_2 = (k_1 \cdot 5 + 3) \cdot (k_2 \cdot 5 + 4) = ((k_1 \cdot k_2) \cdot 5 + 4 \cdot k_1 + 3 \cdot k_2) \cdot 5 + 12 = ((k_1 \cdot k_2) \cdot 5 + 4 \cdot k_1 + 3 \cdot k_2) \cdot 5 + 10 + 2 = ((k_1 \cdot k_2) \cdot 5 + 4 \cdot k_1 + 3 \cdot k_2 + 2) \cdot 5 + 2 \Rightarrow 2 = (b_1 \cdot b_2) \bmod 5$.

Für die **Multiplikation von Restklassen** bietet sich also folgende **Definition** an:

$$\overline{n} \cdot \overline{k} = \overline{(n \cdot k) \bmod m},$$

man berechnet also den **„Rest des Produkts der Reste modulo m“**.

Bemerkung und Beispiele:

1. Für kleine Zahlen $m \in \mathbb{N}$ also z.B. $n \leq 15$ stellt man die Rechenoperationen mittels Verknüpfungstabellen auf. Für $m = 5$ hat man

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2. Wie in $\mathbb{Z}$ sind auch in $\mathbb{Z}_m$ **Potenzen** definiert durch:
$$\bar{k}^l = \underbrace{\bar{k} \cdot \bar{k} \cdot \dots \cdot \bar{k}}_{l \text{ mal}}$$

Man erhält (mit dem oben erklären Vorgehen bei der Multiplikation):

$$\bar{k}^l = \overline{k^l \bmod m}$$

Beispiel:
In $\mathbb{Z}_7$ erhält man $\bar{4}^5 = \overline{4^5} = \overline{1024 \bmod 7} = \bar{2}$ denn $1024 = 1022 + 2 = 146 \cdot 7 + 2$
Man kann auch (vielleicht einfacher) folgendermaßen rechnen:
$\bar{4}^5 = \overline{4^5} = \overline{16 \cdot 16 \cdot 4} = \overline{16 \bmod 7} \cdot \overline{16 \bmod 7} \cdot \bar{4} = \bar{2} \cdot \bar{2} \cdot \bar{4} = \overline{16 \bmod 7} = \bar{2}$

Kongruenz als Äquivalenzrelation und Restklassen als Äquivalenzklassen

Definition:
Für $a, b \in \mathbb{Z}$ und den **Modul** $m \in \mathbb{N}$ ist die **Kongruenzrelation modulo m** definiert durch

$$b \equiv a \bmod m \Leftrightarrow m|(a-b).$$

Man sagt dann: **b ist kongruent zu a modulo m**.

Satz:
Die Kongruenzrelation modulo m ist eine **Äquivalenzrelation**, d.h.

1. Reflexivität: $a \equiv a \bmod m$;
2. Symmetrie: $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$;
3. Transitivität: $a \equiv b \bmod m \wedge b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$;

Beweis:
1. $a \equiv a \bmod m$, denn: $a|0 = (a-a)$;
2. $a \equiv b \bmod m \Rightarrow m|(b-a) \Rightarrow (b-a) = k \cdot m \Rightarrow (a-b) = (-k) \cdot m \Rightarrow m|(a-b) \Rightarrow b \equiv a \bmod m$;
3. $a \equiv b \bmod m \wedge b \equiv c \bmod m \Rightarrow m|(b-a) \wedge m|(c-b) \Rightarrow b-a = k \cdot m \wedge c-b = \tilde{k} \cdot m \Rightarrow c-a = (c-b)+(b-a) = \tilde{k} \cdot m + k \cdot m = (\tilde{k}+k) \cdot m \Rightarrow m|(c-a) \Rightarrow a \equiv c \bmod m$.

Diese Äquivalenzrelation erzeugt (paarweise disjunkte) **Äquivalenzklassen** modulo m, nämlich:
$\overline{a} = \{b \in \mathbb{Z} | b \equiv a \bmod m\} = \{b \in \mathbb{Z} | m|(a-b)\}$.

Es gilt $b \in \overline{a}$ genau dann, wenn a und b beim (ganzzahligen) Teilen durch m den selben

Rest lassen, also: $a \bmod m = b \bmod m$. Es ist also
$a \equiv b \bmod m \Leftrightarrow \overline{a} = \overline{b}$ in $\mathbb{Z}_m$.

Für $n \in \mathbb{N}$ entspricht die Äquivalenzklasse der Kongruenzrelation modulo m daher gerade der Restklasse $\overline{n}$ modulo m.

Damit folgt sofort, dass die Restklassen $\overline{n}$ paarweise disjunkt zueinander sind und eine (vollständige) Partition von $\mathbb{Z}$ bilden.

Bemerkung: Rechenregeln für die Kongruenzrelation modulo m

Für $a, b, c, d, e, m \in \mathbb{Z}$ mit $m \neq 0$ und $a \equiv b$ mod m, $c \equiv d$ mod m gilt:

a) $a \pm c \equiv (b \pm d)$ mod m

b) $a \cdot c \equiv (b \cdot d)$ mod m

c) $a \cdot e \equiv (b \cdot e)$ mod m

Für das **„Kürzen“** betrachte man folgendes

Beispiel:

$3 \cdot 4 \equiv 1 \cdot 4 \bmod 8 \not\Rightarrow 3 \equiv 1 \bmod 8$ man kann den gemeinsamen Faktor 4 also nicht „herauskürzen“; aber
$4 \cdot 3 \equiv 12 \cdot 3 \bmod 8 \Rightarrow 4 \equiv 12 \bmod 8$ hier kann man den gemeinsamen Faktor 3 „herauskürzen“!
Wo liegt der Unterschied? Es gilt $\text{ggT}(4, 8) = 4$ und $\text{ggT}(3, 8) = 1$, d.h. der Faktor 3 und der Modul $m = 8$ sind **teilerfremd**.

Allgemein gilt für das **„Kürzen“:**

d) Falls $\text{ggT}(e, m) = 1$ ist, gilt: $a \cdot e \equiv b \cdot e$ mod m $\Rightarrow a \equiv b$ mod m.

Algebraische Struktur von $\mathbb{Z}_m$

Auf der Menge $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$ sind zwei **Verknüpfungen/Rechenoperationen** nämlich die **Addition**

$$\overline{n} + \overline{k} = \overline{(n+k) \bmod m}$$

und die **Multiplikation**

$$\overline{n} \cdot \overline{k} = \overline{(n \cdot k) \bmod m}$$

definiert.

Aus den Rechenregeln für ganze Zahlen $\mathbb{Z}$ leiten sich folgende Rechenregeln für $\mathbb{Z}_m$ ab:

Für die **Addition** gilt:

Assoziativgesetz: $\overline{n} + (\overline{k} + \overline{l}) = (\overline{n} + \overline{k}) + \overline{l}$
Kommutativgesetz: $\overline{n} + \overline{k} = \overline{k} + \overline{n}$
Existenz des neutralen Elements $\overline{0}$: $\overline{n} + \overline{0} = \overline{n}$
Existenz des inversen Elements: Zu $\overline{n} \in \mathbb{Z}_m$ existiert $\overline{l} = \overline{m - n}$ mit $\overline{n} + \overline{l} = \overline{n + m - n} = \overline{m} = \overline{0}$

Damit ist $(\mathbb{Z}_m, +)$ eine **abelsche (kommutative) Gruppe**.

Für die **Multiplikation** gilt:

Assoziativgesetz: $\overline{n} \cdot (\overline{k} \cdot \overline{l}) = (\overline{n} \cdot \overline{k}) \cdot \overline{l}$
Kommutativgesetz: $\overline{n} \cdot \overline{k} = \overline{k} \cdot \overline{n}$
Existenz des neutralen Elements $\overline{1}$: $\overline{n} \cdot \overline{1} = \overline{n}$

Damit ist $(\mathbb{Z}_m, \cdot)$ eine **abelsche (kommutative) Halbgruppe mit Eins** und $(\mathbb{Z}_m, +, \cdot)$ ein Ring.

In Bezug auf **beide Verknüpfungen (Addition und Multiplikation)** gilt das

Distributivgesetz: $\overline{n} \cdot (\overline{l} + \overline{k}) = (\overline{n} \cdot \overline{l}) + (\overline{n} \cdot \overline{k})$

Inverse bezüglich der Mutiplikation in $\mathbb{Z}_m$:

Wir wollen folgende Frage klären: Unter welcher Bedingung hat $\overline{n} \neq \overline{0}$ ein **inverses Element bezüglich der Multiplikation** in $\mathbb{Z}_m$, also ein $\overline{k} \in \mathbb{Z}_m$ mit $\overline{n} \cdot \overline{k} = \overline{1}$?

Als Einstieg betrachten wir die Verknüpfungstabellen für die Multiplikation in $\mathbb{Z}_5$ und $\mathbb{Z}_4$:

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Wir betrachten die Zeilen zu $\overline{n}$ mit $n \neq 0$:
In der Tabelle zu $\mathbb{Z}_5$ findet man in jeder dieser Zeilen eine $\overline{1}$, d.h. in $\mathbb{Z}_5$ hat jede Zahl $\overline{n}$ mit $n \neq 0$ eine Inverse bezüglich der Multiplikation.

In der Tabelle zu $\mathbb{Z}_4$ findet man in der Zeile zu $\overline{2}$ keine $\overline{1}$, d.h. in $\mathbb{Z}_4$ hat die Zahl $\overline{2}$ keine Inverse bezüglich der Multiplikation.

Definition:
Die Menge $\mathbb{Z}_m^*$ ist die Menge der Elemente aus $\mathbb{Z}_m$, die eine Inverse bezüglich der Multiplikation haben, also:

$$\mathbb{Z}_m^* = \{\overline{i} \in \mathbb{Z}_m \setminus \{\overline{0}\} | \exists \overline{k} \in \mathbb{Z}_m \text{ mit } \overline{i} \cdot \overline{k} = \overline{1}\}$$

Beispiele: $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \mathbb{Z}_5 \setminus \{\overline{0}\}$ und $\mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}$

Satz:

a) $\overline{k} \in \mathbb{Z}_m$ hat ein **inverses Element bezüglich der Multiplikation**, wenn m und k **teilerfremd** sind, also:
$$\overline{k} \in \mathbb{Z}_m^* \Leftrightarrow 1 = \text{ggT}(k, m).$$

b) Wenn m eine **Primzahl** ist, gilt $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\overline{0}\}$, d.h. **jede Zahl** $\overline{n}$ mit $n \neq 0$ **hat eine Inverse bezüglich der Multiplikation in** $\mathbb{Z}_m$.
Damit ist $\mathbb{Z}_m$ für Primzahlen m ein **Körper**.

Beweis:

1. Mit dem Lemma von Bézout folgt im Fall $1 = \text{ggT}(k, m)$:
Es gibt $s, t \in \mathbb{Z}$ mit $1 = s \cdot k + t \cdot m \Rightarrow 1 = 1 \bmod m = (s \cdot k + t \cdot m) \bmod m \Rightarrow$
$1 = (s \cdot k) \bmod m + (t \cdot m) \bmod m = ((s \bmod m) \cdot (k \bmod m)) + ((t \bmod m) \cdot (m \bmod m)) \Rightarrow$
$\overline{1} = (\overline{s} \cdot \overline{k}) + (\underbrace{\overline{t} \cdot \overline{0}}_{=\overline{0}}) \Rightarrow \overline{1} = \overline{s} \cdot \overline{k}$.
$\overline{s}$ ist also die Inverse bezüglich der Multiplikation zu $\overline{k}$ in $\mathbb{Z}_m$.

2. Widerspruchsbeweis: Angenommen im Fall $d = \text{ggT}(k, m) > 1$ gibt es ein inverses Element bezüglich der Multiplikation zu $\overline{k}$, also ein $\overline{l}$ mit $\overline{k} \cdot \overline{l} = \overline{1}$.
Wegen $d = \text{ggT}(k, m)$ gibt es $i, j \in \mathbb{N}$ mit $k = d \cdot i$ und $m = d \cdot j$ und $\overline{l}$ mit $\overline{k} \cdot \overline{l} = \overline{1} \Rightarrow k \cdot l = s \cdot m + 1$ für ein $s \in \mathbb{Z} \Rightarrow 1 = k \cdot l - s \cdot m = d \cdot i \cdot l - d \cdot j \cdot s \Rightarrow$
$1 = d \cdot \underbrace{(i \cdot l - j \cdot s)}_{\in \mathbb{Z}}$. Wegen $d > 1$ ist das aber in $\mathbb{Z}$ nicht möglich, denn in $\mathbb{Z}$ haben die Zahlen $n \neq \pm 1$ keine Inverse bezüglich der Multiplikation.

3. Für eine Primzahl m gilt: $\text{ggT}(k, m) = 1 \forall k \in \mathbb{Z}$. Damit hat jede Zahl $\overline{k} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ ein inverses Element bezüglich der Multiplikation. Zusammen mit den weiter oben angegebenen Rechengesetzen sind die fünf Körperaxiome erfüllt.

5.4 Der Chinesische Restsatz

Ein einfaches Beispiel zur Einführung soll die Problematik erläutern:

Wenn man x parallele Prozesse auf drei Rechenkerne aufteilt, bleiben 2 Prozesse unbearbeitet. Wenn man diese parallelen Prozesse auf 5 Rechenkerne aufteilt bleiben 3 Prozesse unbearbeitet. Bestimmen Sie die Anzahl x der betrachteten Prozesse.

Wie kann man das Problem mathematisch fassen? Hier ein möglicher Ansatz:
Teilt man x durch 3, erhält man den Rest 2, d.h. $\overline{x} = \overline{2}$ in $\mathbb{Z}_3$.
Teilt man x durch 5, erhält man den Rest 3, d.h. $\overline{x} = \overline{3}$ in $\mathbb{Z}_5$.

Man muss also sogenannte **simultane Kongruenzen** lösen:
$\overline{x} = \overline{2}$ in $\mathbb{Z}_3 \wedge \overline{x} = \overline{3}$ in $\mathbb{Z}_5$

In diesem einfachen Fall reicht es aus, einfach auszuprobieren:
In $\mathbb{Z}_3$ gilt $\{2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, \ldots\} \subset \overline{2}$,
in $\mathbb{Z}_5$ gilt $\{3, 8, 13, 18, 23, 28, 33, 38, \ldots\} \subset \overline{3}$
Durch „Nachschauen “ sieht man: x=8 ist eine (die kleinste positive!) Lösung, aber auch x=23 und x=38 lösen das Problem.

Allgemein gilt:

Satz (chinesischer Restsatz für zwei simultane Kongruenzen):
Die simultanen Kongruenzen

$$\overline{x} = \overline{n} \text{ in } \mathbb{Z}_{m_1} \text{ und } \overline{x} = \overline{k} \text{ in } \mathbb{Z}_{m_2}$$

sind lösbar, wenn gilt: $\mathrm{ggT}(m_1, m_2) = 1$.

Es gilt dann: $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$ ist **eine** Lösung, falls gilt $\overline{a} \cdot \overline{m_2} = \overline{1}$ in $\mathbb{Z}_{m_1}$ und $\overline{b} \cdot \overline{m_1} = \overline{1}$ in $\mathbb{Z}_{m_2}$.

Weitere (positive) Lösungen sind $x = x_0 + i \cdot m_1 \cdot m_2$ für $i \in \mathbb{Z}$ (solange $x \geq 0$ gilt).

Beweisidee:
Wegen $\mathrm{ggT}(m_1, m_2) = 1$ gilt: $\exists \bar{a} \in \mathbb{Z}_{m_1}$ mit $\bar{a} \cdot \overline{m_2} = \bar{1}$ in $\mathbb{Z}_{m_1}$ und
$\exists \bar{b} \in \mathbb{Z}_{m_2}$ mit $\bar{b} \cdot \overline{m_1} = \bar{1}$ in $\mathbb{Z}_{m_2}$.
Wir können also die gewünschten Zahlen a und b und damit auch
$x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$ berechnen. Damit erhält man
in $\mathbb{Z}_{m_1}$ gilt: $\overline{x_0} = \overline{n} \cdot \underbrace{\overline{a} \cdot \overline{m_2}}_{=\bar{1}} + \overline{k} \cdot \underbrace{\overline{b} \cdot \overline{m_1}}_{=\bar{0}} = \overline{n}$ und
in $\mathbb{Z}_{m_2}$ gilt: $\overline{x_0} = \overline{n} \cdot \underbrace{\overline{a} \cdot \overline{m_2}}_{=\bar{0}} + \overline{k} \cdot \underbrace{\overline{b} \cdot \overline{m_1}}_{=\bar{1}} = \overline{k}$
Für $x = x_0 + i \cdot m_1 \cdot m_2$ gilt in $\mathbb{Z}_{m_1}$ und in $\mathbb{Z}_{m_2}$:
$\overline{x} = \overline{x_0} + \bar{i} \cdot \underbrace{\overline{m_1 \cdot m_2}}_{=\bar{0}} = \overline{x_0}$ für $i \in \mathbb{Z}$.

Beispiel:
Gesucht ist eine Lösung x der simultanen Kongruenzen
$\overline{x} = \overline{5}$ in $\mathbb{Z}_{34}$ und$\overline{x} = \overline{17}$ in $\mathbb{Z}_{65}$.

Nach dem chinesischen Restsatz existiert (mindestens) eine Lösung, denn $\text{ggT}(34, 65) = 1$; eine Lösung ist gegeben durch
$x = 5 \cdot a \cdot 65 + 17 \cdot b \cdot 34$ dabei ist $\overline{a}$ die Lösung von $\overline{a} \cdot \overline{65} = \overline{1}$ in $\mathbb{Z}_{34}$ und $\overline{b}$ die Lösung von $\overline{b} \cdot \overline{34} = \overline{1}$ in $\mathbb{Z}_{65}$.

Berechnung von a: Wir rechnen in $\mathbb{Z}_{34}$
In $\mathbb{Z}_{34}$ gilt wegen $65 = 34 + 31$: $\overline{65} = \overline{31}$. Damit gilt $\overline{a} \cdot \overline{65} = \overline{1} \Leftrightarrow \overline{a} \cdot \overline{31} = \overline{1}$.

$34 = 1 \cdot 31 + 3$
$31 = 10 \cdot 3 + 1 \Rightarrow$
$\text{ggT}(34, 31) = 1 \Rightarrow 1 = 31 - 10 \cdot 3 = 31 - 10 \cdot (34 - 1 \cdot 31) = 11 \cdot 31 - 10 \cdot 34 \Rightarrow$
$\overline{1} = \overline{11} \cdot \overline{31}$ in $\mathbb{Z}_{34} \Rightarrow a = 11$

Berechnung von b: Wir rechnen in $\mathbb{Z}_{65}$
Gesucht ist b mit $\overline{b} \cdot \overline{34} = \overline{1}$.

$65 = 1 \cdot 34 + 31$
$34 = 1 \cdot 31 + 3$
$31 = 10 \cdot 3 + 1 \Rightarrow$
$\text{ggT}(65, 34) = 1 \Rightarrow 1 = 31 - 10 \cdot 3 = 31 - 10 \cdot (34 - 1 \cdot 31) = -10 \cdot 34 + 11 \cdot 31 =$
$-10 \cdot 34 + 11 \cdot (65 - 1 \cdot 34) = 11 \cdot 65 - 21 \cdot 34 \Rightarrow$
$\overline{1} = \overline{-21} \cdot \overline{34} \Leftrightarrow \overline{1} = \overline{44} \cdot \overline{34}$ in $\mathbb{Z}_{65} \Rightarrow b = 44$

Berechnung von x_0:
$x_0 = 5 \cdot a \cdot 65 + 17 \cdot b \cdot 34 = 5 \cdot 11 \cdot 65 + 17 \cdot 44 \cdot 34 = 29007$

Weitere Lösungen sind $x_i = x_0 + i \cdot 34 \cdot 65 = x_0 + i \cdot 2210, i \in \mathbb{Z}$; für $i = -13$ erhält man $29007 - 13 \cdot 2210 = 277$ als **kleinste positive Lösung**.

Mit der selben Beweisidee erhält man

Satz (chinesischer Restsatz für mehrere simultane Kongruenzen):

Die n simultanen Kongruenzen

$$\overline{x} = \overline{n_i} \text{ in } \mathbb{Z}_{m_i} \text{ und } 1 \leq i \leq n$$

sind lösbar, wenn gilt: $\text{ggT}(m_i, m_j) = 1$ für $i \neq j$ mit $1 \leq i \leq n$.

Es gilt dann:
$x_0 = \sum_{i=1}^{n} n_i \cdot a_i \cdot \frac{M}{m_i}$

ist **eine** Lösung mit $M = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_n$ und mit $\overline{a_i}$ so dass $\overline{a_i} \cdot \overline{\frac{M}{m_i}} = \overline{1}$ in $\mathbb{Z}_{m_i}$ gilt.

Weitere (positive) Lösungen sind $x = x_0 + l \cdot M$ für $l \in \mathbb{Z}$ (solange $x \geq 0$ gilt).

Beispiel:
Gesucht ist eine Lösung x der simultanen Kongruenzen
$\overline{x} = \overline{2}$ in $\mathbb{Z}_3$, $\overline{x} = \overline{3}$ in $\mathbb{Z}_5$ und $\overline{x} = \overline{5}$ in $\mathbb{Z}_7$.

Nach dem chinesischen Restsatz existiert (mindestens) eine Lösung, denn $\text{ggT}(3,5) = 1, \text{ggT}(3,7) = 1$ und $\text{ggT}(5,7) = 1$;
eine Lösung ist gegeben durch
$x = 2 \cdot a_1 \cdot 35 + 3 \cdot a_2 \cdot 21 + 5 \cdot a_3 \cdot 15$, dabei ist $\overline{a_1}$ die Lösung von $\overline{a_1} \cdot \overline{35} = \overline{1}$ in $\mathbb{Z}_3$, $\overline{a_2}$ ist die Lösung von $\overline{a_2} \cdot \overline{21} = \overline{1}$ in $\mathbb{Z}_5$ und $\overline{a_3}$ ist die Lösung von $\overline{a_3} \cdot \overline{15} = \overline{1}$ in $\mathbb{Z}_7$.

Berechnung von a_1: Wir rechnen in $\mathbb{Z}_3$
In $\mathbb{Z}_3$ gilt wegen $35 = 33{+}2$: $\overline{35} = \overline{2}$. Damit gilt $\overline{a_1} \cdot \overline{35} = \overline{1} \Leftrightarrow \overline{a_1} \cdot \overline{2} = \overline{1} \Rightarrow \overline{a_1} = \overline{2} \Rightarrow a_1 = 2$.

Berechnung von a_2: Wir rechnen in $\mathbb{Z}_5$
Gesucht ist a_2 mit $\overline{a_2} \cdot \overline{21} = \overline{1}$.
In $\mathbb{Z}_5$ gilt wegen $21 = 20{+}1$: $\overline{21} = \overline{1}$. Damit gilt $\overline{a_2} \cdot \overline{21} = \overline{1} \Leftrightarrow \overline{a_2} \cdot \overline{1} = \overline{1} \Rightarrow \overline{a_2} = \overline{1} \Rightarrow a_2 = 1$.

Berechnung von a_3: Wir rechnen in $\mathbb{Z}_7$
Gesucht ist a_3 mit $\overline{a_3} \cdot \overline{15} = \overline{1}$.
In $\mathbb{Z}_7$ gilt wegen $15 = 14{+}1$: $\overline{15} = \overline{1}$. Damit gilt $\overline{a_3} \cdot \overline{15} = \overline{1} \Leftrightarrow \overline{a_3} \cdot \overline{1} = \overline{1} \Rightarrow \overline{a_3} = \overline{1} \Rightarrow a_3 = 1$.

Berechnung von x_0:
$x_0 = 2 \cdot a_1 \cdot 35 + 3 \cdot a_2 \cdot 21 + 5 \cdot a_3 \cdot 15 = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 5 \cdot 1 \cdot 15 = 278$

Weitere Lösungen sind $x_i = x_0 + i \cdot 3 \cdot 5 \cdot 7 = x_0 + i \cdot 105, i \in \mathbb{Z}$; für $i = -2$ erhält man $278 - 2 \cdot 105 = 68$ als **kleinste positive Lösung**.

5.5 Die Grundidee der RSA-Algorithmus

Der nach den „Entdeckern“ Rivest, Shamir und Adelman benannte RSA-Algorithmus ist ein Verfahren zur **asymmetrischen Verschlüsselung** von Daten. Die Bezeichnung „asymmetrisch“ bezieht sich darauf, dass der Sender der Daten und der Empfänger der Daten nicht über denselben Schlüssel verfügen. Es muss keine geheime Übereinkunft über den Schlüssel getroffen werden!

Das Grundprinzip des Verfahrens ist: Der Empfänger hat einen „privaten Schlüssel“ und einen „öffentlichen Schlüssel“. Den privaten Schlüssel hält der Empfänger geheim, den öffentlichen Schlüssel stellt er jedem zur Verfügung.

Der Sender verschlüsselt seine Daten mit dem öffentliche Schlüssel des Empfängers und sendet dem Empfänger dann die verschlüsselten Daten. Nur der Empfänger kann diese verschlüsselten Daten mit seinem privaten Schlüssel entschlüsseln!
Das Verfahren beruht auf Erkenntnissen der Zahlentheorie; die zu verschlüsselnden Daten müssen daher zunächst in „Zahlen“ transformiert werden.

Beispiel:
Der Empfänger E (Prof. K.) soll eine Nachricht des Senders S (Student S.) bekommen. S möchte dem Professor mitteilen, dass Mathe sein Lieblingsfach ist. Diese „uncoole“ Nachricht soll geheim bleiben. Sie muss also verschlüsselt werden. Der Sender S weiß, dass der Empfänger E seinen öffentlichen Schlüssel zur RSA-Verschlüsselung bereitstellt. Um diesen Schlüssel nutzen zu können, muss er zunächst seine Nachricht (Daten) in Zahlen transformieren. Dies macht er einfach:
Den 26 Buchstaben des deutschen Alphabets wird jeweils eindeutig eine natürliche Zahl zugeordnet

Text	A	B	C	...	Z
Zahl	1	2	3	...	26

Der „Klartext“ **MATHE** ergibt damit die Zahlenfolge **13 1 20 8 5**.
Diese Zahlen werden vom Sender S mit dem öffentlichen Schlüssel des Empfängers E verschlüsselt und dann zum Empfänger gesendet.

Wie bekommt der Empfänger E seinen öffentlichen und seinen privaten Schlüssel? Der Empfänger muss **modulare Arithmetik**, das Rechnen mit Restklassen, beherrschen.

1) Zunächst nimmt der Empfänger E eine (sehr) große natürliche Zahl $N \in \mathbb{N}$, die das Produkt zweier ebenfalls (sehr) großer Primzahlen p, q ist: $N = p \cdot q$.
Wenn p und q mehrere hundert Dezimalstellen haben, ist es zur Zeit nicht in endlicher Zeit möglich, die Zahl N in das Produkt $N = p \cdot q$ zu „faktorisieren“.

2) Der Empfänger E bestimmt $\tilde{N} = (p-1) \cdot (q-1)$ und rechnet dann in $\mathbb{Z}_{\tilde{N}}$.
Er bestimmt eine Zahl e mit $1 < e < \tilde{N}$ und $\text{ggT}(e, \tilde{N}) = 1$, damit hat $\overline{e}$ in $\mathbb{Z}_{\tilde{N}}$ eine multiplikative Inverse $\overline{d}$ in $\mathbb{Z}_{\tilde{N}}$ also $\overline{e} \cdot \overline{d} = \overline{1}$ in $\mathbb{Z}_{\tilde{N}}$.

3) Der **öffentliche Schlüssel** des Empfängers E ist (N, e).
Der **private Schlüssel** des Empfängers E ist (N, d).
Da N nicht in endlicher Zeit faktorisierbar ist, kann kein Anderer mit Kenntnis von e und N die Zahl d berechnen!

Wie kann der Sender S seinen „Klartext“ damit verschlüsseln? Der Sender muss ebenfalls **modulare Arithmetik**, das Rechnen mit Restklassen, beherrschen.

4) Der Sender S transformiert seinen Text in eine Zahlenfolge und kann dann seien Text, genauer die daraus ermittelte Zahlenfolge $a_1 a_2 a_3 \dots a_k$ (es soll $\text{ggT}(a_i, N) = 1, 1 \leq i \leq k$ gelten), mit dem **öffentlichen Schlüssel** des Empfängers E verschlüsseln.

Dazu rechnet der Sender S in $\mathbb{Z}_N$.
Für jede Zahl a_i, $1 \leq i \leq k$, seiner Zahlenfolge berechnet er $\overline{A_i} = \overline{a_i^e}$ in $\mathbb{Z}_N$, $1 \leq i \leq k$.
Damit geht die Folge $a_1a_2a_3 \ldots a_k$ (der Klartext) in die verschlüsselte Folge $A_1A_2A_3 \ldots A_k$ über.

5) Der Sender S sendet die verschlüsselte Folge $A_1A_2A_3 \ldots A_k$ an den Empfänger E.

Wie kann der Empfänger E den verschlüsselten Text entschlüsseln?

6) Der Empfänger E entschlüsselt die so empfangene verschlüsselte Zahlenfolge $A_1A_2A_3 \ldots A_k$ mit Hilfe seines **privaten Schlüssels** (N, d).
Dazu berechnet er in $\mathbb{Z}_N$ die Zahlen $\overline{A_i}^d$, $1 \leq i \leq k$.
Es gilt $\overline{A_i}^d = \overline{a_i}$, $1 \leq i \leq k$. Damit kennt er den „Klartext“ $a_1a_2a_3 \ldots a_k$.

Wir betrachten zunächst ein **Beispiel** und werden danach klären, **warum dieses Verfahren funktioniert**.

Beispiel:
Für das Beispiel nehmen wir bewusst kleine Zahlen (damit ist das Verfahren natürlich extrem unsicher, da die Faktorisierung leicht zu berechnen ist, z.B. durch Ausprobieren).

1) Der Empfänger E (Prof. K.) wählt $N = 33 = 3 \cdot 11$ also $p = 3$ und $q = 11$.

2) Der Empfänger berechnet $\tilde{N} = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$ und rechnet jetzt in $\mathbb{Z}_{20}$. Der Empfänger wählt z.B. $e = 7$ mit $\text{ggT}(7, 20) = 1$ und bestimmt d mit $\overline{e} \cdot \overline{d} = \overline{1}$ in $\mathbb{Z}_{20}$:

$20 = 2 \cdot 7 + 6$ $\qquad$ $1 = 7 - 1 \cdot 6$
$7 = 1 \cdot 6 + 1$ $\qquad$ $1 = 7 - 1 \cdot (20 - 2 \cdot 7)$
$6 = 6 \cdot 1 + 0 \Rightarrow \text{ggT}(7, 20) = 1$ $\qquad$ $1 = -1 \cdot 20 + 3 \cdot 7$

In $\mathbb{Z}_{20}$ gilt also $\overline{1} = \overline{7} \cdot \overline{3}$, d.h. die multiplikative Inverse von $\overline{7}$ in $\mathbb{Z}_{20}$ ist $\overline{3}$.

3) Der **öffentliche Schlüssel** des Empfängers E ist $(33, 7)$.
Der **private Schlüssel** des Empfängers E ist $(33, 3)$.

4) Die **Verschlüsselung** durch den Sender geschieht jetzt wie folgt:
Klartext: MATHE $\Rightarrow$ Transformation in Zahlenfolge **13 1 20 8 5**
Es gilt $\text{ggT}(13, 33) = \text{ggT}(1, 33) = \text{ggT}(8, 33) = \text{ggT}(5, 33) = 1$.
Zur Verschlüsselung rechnet der Sender S mit dem öffentlichen Schlüssel $(33, 7)$ in $\mathbb{Z}_{33}$:

$\overline{13^7} = \overline{62748517} = \overline{7}$ denn $62748517 = 1901470 \cdot 33 + 7$
$\overline{1^7} = \overline{1}$ denn $1 = 0 \cdot 33 + 1$
$\overline{20^7} = \overline{1280000000} = \overline{26}$ denn $1280000000 = 38787878 \cdot 33 + 26$
$\overline{8^7} = \overline{2097152} = \overline{2}$ denn $2097152 = 63550 \cdot 33 + 2$
$\overline{5^7} = \overline{78125} = \overline{14}$ denn $78125 = 2367 \cdot 33 + 14$

Damit wird die Zahlenfolge **13 1 20 8 5** verschlüsselt in **7 1 15 2 15**.

5) Der Sender S sendet die verschlüsselte Zahlenfolge **7 1 26 2 14** an den Empfänger E.

6) Zum Entschlüsseln rechnet auch der Empfänger E in $\mathbb{Z}_{33}$, und zwar mit seinem privaten Schlüssel (33,3):

$\overline{7^3} = \overline{343} = \overline{13}$ denn $343 = 10 \cdot 33 + 13$
$\overline{1^3} = \overline{1}$ denn $1 = 0 \cdot 33 + 1$
$\overline{26^3} = \overline{17567} = \overline{20}$ denn $17576 = 532 \cdot 33 + 20$
$\overline{2^3} = \overline{8}$ denn $8 = 0 \cdot 33 + 8$
$\overline{14^3} = \overline{2744} = \overline{5}$ denn $2744 = 83 \cdot 33 + 5$

Die entschlüsselte Zahlenfolge ist also **13 1 20 8 5**; dies ist die dem Klartext zugeordnete Zahlenfolge und die Rücktransformation ergibt:

Zahl	13	1	20	8	5
Text	M	A	T	H	E

Warum funktioniert dieses Verfahren?
Zur Beantwortung dieser Frage benötigen wir noch etwas Zahlentheorie.

Definition:
Für $n \in \mathbb{N}$ ist definiert:

a) $\Phi(n) = \{k \in \mathbb{N} | 1 \leq k < n \wedge \text{ggT}(k, n) = 1\}$
Dies ist die Menge der zu n teilerfremden natürlichen Zahlen kleiner als n.

b) Die Funktion $\phi : \mathbb{N} \to \mathbb{N}$ mit $\phi(n) = |\Phi(n)|$
Dabei ist $|\Phi(n)|$ die **Anzahl der Elemente** der Menge $\Phi(n)$. Diese Funktion heißt **Eulersche phi-Funktion**.

Beispiele:

a) $n = 20 \Rightarrow \Phi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\} \Rightarrow \phi(20) = 8$

b) $n = 21 \Rightarrow \Phi(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\} \Rightarrow \phi(21) = 12$

c) $n = 7 \Rightarrow \Phi(7) = \{1, 2, 3, 4, 5, 6\} \Rightarrow \phi(7) = 6 = 7 - 1$

d) $n = 3 \Rightarrow \Phi(3) = \{1, 2\} \Rightarrow \phi(3) = 2 = 3 - 1$

e) Die drei vorhergehenden Beispiele zeigen:
$12 = \phi(21) = \phi(3 \cdot 7) = \phi(3) \cdot \phi(7) = 2 \cdot 6$

Man sieht sofort

Bemerkung:

1) $p \in \mathbb{N}$ Primzahl $\Rightarrow \phi(p) = p - 1$, denn p hat keine (echten) Teiler$<p$.

2) $p, q \in \mathbb{N}$ Primzahlen $\Rightarrow \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p - 1) \cdot (q - 1)$, denn Teiler von $p \cdot q$ müssen Teiler von p oder q sein und p und q haben als Primzahlen keine gemeinsamen (echten) Teiler.

Der Beweis der Korrektheit des RSA-Verfahrens beruht auf folgendem Satz.

Satz: Satz von Euler

Gegeben sind $a, N \in \mathbb{N}$ mit $\text{ggT}(a, N) = 1$, d.h. a und N sind teilerfremd. Dann gilt

$$a^{\phi(N)} \equiv 1 \bmod N \text{ oder anders formuliert } \overline{a^{\phi(N)}} = \overline{1} \text{ in } \mathbb{Z}_N$$

Beweis:

Setze $\phi(N) = l$, dann ist $\Phi(N) = \{k_1, k_2, k_3, \ldots, k_l\}$ mit $\text{ggT}(k_i, N) = 1, 1 \leq i \leq l$, die Menge aller natürlichen Zahlen kleiner N, die teilerfremd zu N sind.
In $\mathbb{Z}_N$ heißt das: $\overline{k_1}, \overline{k_2}, \overline{k_3}, \ldots, \overline{k_l}$ sind genau die Elemente aus $\mathbb{Z}_N$, die bezüglich der Multiplikation invertierbar sind: $\{\overline{k_1}, \overline{k_2}, \overline{k_3}, \ldots, \overline{k_l}\} = \mathbb{Z}_N^*$.
Jetzt betrachtet man die Zahlen $a \cdot k_i, 1 \leq i \leq l$: Wegen $\text{ggT}(a, N) = 1$ und $\text{ggT}(k_i, N) = 1$ ist auch $\text{ggT}(a \cdot k_i, N) = 1 \Rightarrow \overline{a \cdot k_i} \in \mathbb{Z}_N^*$ für $1 \leq i \leq l$ oder anders formuliert
$\mathbb{Z}_N^* = \{\overline{k_1}, \overline{k_2}, \overline{k_3}, \ldots, \overline{k_l}\} = \{\overline{a \cdot k_1}, \overline{a \cdot k_2}, \overline{a \cdot k_3}, \ldots, \overline{a \cdot k_l}\}$ (beim Rechnen „modulo N“ liefert die Multiplikation mit a nur eine Vertauschung (Permutation) der Restklassen!).
Damit folgt sofort $k_1 \cdot k_2 \cdot k_3 \cdot \ldots \cdot k_l \equiv (a \cdot k_1) \cdot (a \cdot k_2) \cdot (a \cdot k_3) \cdot \ldots \cdot (a \cdot k_l) \bmod N \Rightarrow$
$k_1 \cdot k_2 \cdot k_3 \cdot \ldots \cdot k_l \equiv a^l \cdot k_1 \cdot k_2 \cdot k_3 \cdot \ldots \cdot k_l \bmod N$.
Wegen $\text{ggT}(k_i, N) = 1, 1 \leq i \leq l$ kann man „kürzen“ und erhält:
$1 \equiv a^l \bmod N$; mit $l = \phi(N)$ ist das die Aussage $a^{\phi(N)} \equiv 1 \bmod N$.

Beispiel:

Für $N = 8, a = 3$ wird beispielhaft der wesentliche Argumentationsschritt des Beweises gezeigt: $\Phi(8) = \{1, 3, 5, 7\} \Rightarrow \phi(8) = 4$
$k_1 = 1, k_2 = 3, k_3 = 5, k_4 = 7 \Rightarrow \mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$
mit $a = 3$: $a \cdot k_1 = 3, a \cdot k_2 = 9, a \cdot k_3 = 15, a \cdot k_4 = 21 \Rightarrow$ in $\mathbb{Z}_8$

$\{\overline{a \cdot k_1}, \overline{a \cdot k_2}, \overline{a \cdot k_3}, \overline{a \cdot k_4}\} = \{\overline{3}, \overline{9}, \overline{15}, \overline{21}\} = \{\overline{3}, \overline{1}, \overline{7}, \overline{5}\} = \mathbb{Z}_8^*$,
wir erhalten also durch Multiplikation mit $a = 3$ nur eine Vertauschung (Permutation) der Restklassen in $\mathbb{Z}_8$.

Bemerkungen:
Aus dem Satz von Euler folgt

1) **Der „kleine" Satz von Fermat**
Für $a \in \mathbb{N}$ und jede **Primzahl** $p \in \mathbb{N}$ gilt: $a^{p-1} \equiv 1 \bmod p \Leftrightarrow a^p \equiv a \bmod p$.

   Dies folgt direkt aus dem Satz von Euler wegen $\phi(p) = p - 1$ und durch Multiplikation mit a.

2) **Anwendungsbeispiel:**
Wir haben z.B. $37562 = 37560 + 2 = 3756 \cdot 10 + 2 \Rightarrow 37562 \equiv 2 \bmod 10$, d.h. Rechnen modulo 10 liefert die **letzte Dezimalstelle** einer gegebenen Zahl n.

Aufgabe: Bestimmen Sie die letzte Dezimalstelle der Zahl 7^{333}.
$333 = 4 \cdot 83 + 1 \Rightarrow 7^{333} = 7^{4 \cdot 83 + 1} = (7^4)^{83} \cdot 7$.
Nun gilt auch $\Phi(10) = \{1, 3, 7, 9\}$ und damit $\phi(10) = 4$ sowie mit dem **Satz von Euler** $7^4 \equiv 1 \bmod 10$. Zusammen erhält man:
$7^{333} \bmod 10 = ((7^4)^{83} \cdot 7) \bmod 10 = ((7^4) \bmod 10)^{83} \cdot (7 \bmod 10) = (1^{83}) \cdot (7 \bmod 10) = 1 \cdot (7 \bmod 10) = 7$
Die letzte Dezimalstelle von 7^{333} ist damit 7.

Mit diesem „Werkzeug" können wir die Korrektheit des wesentlichen Schritts im RSA-Verfahren beweisen:

Öffentlicher Schlüssel (N, e), privater Schlüssel (N, d) mit $N = p \cdot q$ für Primzahlen p und q. Es ist $\phi(N) = \phi(p \cdot q) = (p-1) \cdot (q-1) = \tilde{N}$ und $\overline{e} \cdot \overline{d} = \overline{1}$ in $\mathbb{Z}_{\tilde{N}} = \mathbb{Z}_{\phi(N)}$. Der Klartext k (als Zahl) mit $\mathrm{ggT}(k, N) = 1$ wird verschlüsselt als $\overline{k^e}$ in $\mathbb{Z}_N$ und entschlüsselt als $\overline{(k^e)^d} = \overline{k^{e \cdot d}}$ in $\mathbb{Z}_N$; wir berechnen also zum Entschlüsseln $k^{e \cdot d} \bmod N$. Nun gilt $\overline{e} \cdot \overline{d} = \overline{1}$ in $\mathbb{Z}_{\phi(N)}$, d.h. $\exists i \in \mathbb{N}$ mit $e \cdot d = i \cdot \phi(N) + 1$ und damit $k^{e \cdot d} \bmod N = k^{i \cdot \phi(N) + 1} \bmod N = k^{i \cdot \phi(N)} \cdot (k \bmod N) = (\underbrace{k^{\phi(N)} \bmod N}_{=1 \bmod N \text{ (Satz von Euler)}})^i \cdot (k \bmod N) \Rightarrow$ Klartext k.

6 Lineare Gleichungssysteme und der Gaußalgorithmus

6.1 Einleitende Beispiele und Begriffe

Man trifft häufig auf die Situation, dass unbekannte Größen durch lineare Gleichungen voneinander abhängen. Erfüllen diese Gleichungen geeignete Bedingungen (was das genau bedeutet, werden wir in diesem Abschnitt sehen), so lassen sich diese Unbekannten aus ihnen bestimmen. Wir beginnen mit drei typischen Beispielen:

1. Beispiel: Wir betrachten ein System mit drei Gleichungen und den drei Unbekannten x_1, x_2 und x_3:

$$\begin{array}{rcrcrcll} x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ 3x_1 & + & 2x_2 & + & x_3 & = & 10 & \text{(II)} \\ 5x_1 & + & x_2 & + & 2x_3 & = & 13 & \text{(III)} \end{array}$$

Um dieses Gleichungssystem lösen zu können, formen wir es in mehreren Schritten um:

1. Die zweite und dritte Gleichung werden „x_1–frei“ gemacht:

$$\begin{array}{rcl} \text{(II)} & \longrightarrow & \text{(II)} - 3 \cdot \text{(I)} \\ \text{(III)} & \longrightarrow & \text{(III)} - 5 \cdot \text{(I)} \end{array}$$

   Das heißt: Das Dreifache der ersten Gleichung wird von der zweiten Gleichung abgezogen, und von der dritten Gleichung wird das Fünffache der ersten Gleichung abgezogen. Das Gleichungssystem wird dadurch zu

$$\begin{array}{rcrcrcrl} x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ & - & 4x_2 & - & 8x_3 & = & -32 & \text{(II)} \\ & - & 9x_2 & - & 13x_3 & = & -57 & \text{(III)} \end{array}$$

2. Die zweite Gleichung wird normiert, indem sie durch -4, den Koeffizienten von x_2 geteilt wird:

$$\text{(II)} \longrightarrow -\tfrac{1}{4} \cdot \text{(II)}$$

$$\begin{array}{rcrcrcrl} & x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ \Rightarrow & & & x_2 & + & 2x_3 & = & 8 & \text{(II)} \\ & & - & 9x_2 & - & 13x_3 & = & -57 & \text{(III)} \end{array}$$

3. In der dritten Gleichung wird x_3 eliminiert:

$$\text{(III)} \longrightarrow \text{(III)} + 9 \cdot \text{(II)}$$

$$\begin{array}{rcrcrcrl} & x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ \Rightarrow & & & x_2 & + & 2x_3 & = & 8 & \text{(II)} \\ & & & & & 5x_3 & = & 15 & \text{(III)} \end{array}$$

Nun können wir, bei der letzten Gleichung beginnend, ausrechnen:

$$\begin{aligned} x_3 &= 3 \\ x_2 &= 8 - 2x_3 = 2 \\ x_1 &= 14 - 2x_2 - 3x_3 = 14 - 4 - 9 = 1 \end{aligned}$$

Dieses Gleichungssystem ist eindeutig lösbar, seine Lösungsmenge besteht nur aus einem Element: $L = \{(1, 2, 3)\}$.

2. Beispiel: Auch dieses System mit drei Gleichungen mit drei Unbekannten wird in mehreren Schritten umgeformt:

$$\begin{array}{rcrcrcll} x_1 & + & 2x_2 & + & 3x_3 & = & 1 & \text{(I)} \\ 7x_1 & + & 5x_2 & + & 8x_3 & = & 0 & \text{(II)} \\ 10x_1 & + & 2x_2 & + & 4x_3 & = & 1 & \text{(III)} \end{array}$$

1. x_1 wird aus der zweiten und dritten Gleichung eliminiert:

$$\begin{array}{rcl} \text{(II)} & \longrightarrow & \text{(II)} - 7 \cdot \text{(I)} \\ \text{(III)} & \longrightarrow & \text{(III)} - 10 \cdot \text{(I)} \end{array}$$

$$\begin{array}{rrcrcrcrl} & x_1 & + & 2x_2 & + & 3x_3 & = & 1 & \text{(I)} \\ \Rightarrow & & - & 9x_2 & - & 13x_3 & = & -7 & \text{(II)} \\ & & - & 18x_2 & - & 26x_3 & = & -9 & \text{(III)} \end{array}$$

2. x_2 wird aus der dritten Gleichung eliminiert:

$$\text{(III)} \longrightarrow \text{(III)} - 2 \cdot \text{(I)}$$

$$\begin{array}{rrcrcrcrl} & x_1 & + & 2x_2 & + & 3x_3 & = & 1 & \text{(I)} \\ \Rightarrow & & - & 9x_2 & - & 13x_3 & = & -7 & \text{(II)} \\ & & & & & 0x_3 & = & 5 & \text{(III)} \end{array}$$

Der letzte Schritt führte auch zur Eliminierung von x_3 in der dritten Gleichung. Man muss aber erkennen: das Gleichungssystem ist unlösbar: Welchen Wert man auch für x_3 einsetzt, es ist immer

$$0 = 0 \cdot x_3 \neq 5$$

Das Gleichungssystem kann also nicht erfüllt werden, seine Lösungsmenge ist leer: $L = \emptyset$!

3. Beispiel:

$$\begin{array}{rcrcrcll} x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ 7x_1 & + & 5x_2 & + & 8x_3 & = & 35 & \text{(II)} \\ 10x_1 & + & 2x_2 & + & 4x_3 & = & 14 & \text{(III)} \end{array}$$

Wir nehmen die üblichen Umformungen vor:

1. x_1 wird aus der zweiten und dritten Gleichung eliminiert:

$$\begin{array}{rcl} \text{(II)} & \longrightarrow & \text{(II)} - 7 \cdot \text{(I)} \\ \text{(III)} & \longrightarrow & \text{(III)} - 10 \cdot \text{(I)} \end{array}$$

$$\begin{array}{rrcrcrcll} & x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ \Rightarrow & & - & 9x_2 & - & 13x_3 & = & -63 & \text{(II)} \\ & & - & 18x_2 & - & 26x_3 & = & -126 & \text{(III)} \end{array}$$

2. x_2 wird aus der dritten Gleichung eliminiert:

$$\text{(III)} \longrightarrow \text{(III)} - 2 \cdot \text{(I)}$$

$$\begin{array}{rrcrcrcll} & x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ \Rightarrow & & - & 9x_2 & - & 13x_3 & = & -63 & \text{(II)} \\ & & & & & 0x_3 & = & 0 & \text{(III)} \end{array}$$

Der letzte Schritt führte auch hier zusätzlich zur Eliminierung von x_3 in der dritten Gleichung. Gleichzeitig ist die rechte Seite der dritten Gleichung Null geworden. Daraus folgt: man kann für x_3 einen beliebigen Wert einsetzen, die Gleichung

$$0 = 0 \cdot x_3 = 0$$

gilt immer! Hat man einen Wert für x_3 eingesetzt, so kann man die Werte von x_1 und x_2 aus (II) und (I) berechnen:

$$\begin{array}{rcll} x_2 & = & 7 - \frac{13}{9}x_3 & \\ x_1 & = & 14 - 2x_2 - 3x_3 & \text{jetzt } x_2 \text{ einsetzen} \\ & = & 14 - 2 \cdot (7 - \frac{13}{9}x_3) - 3x_3 & \\ & = & -\frac{1}{9}x_3 & \end{array}$$

Die Lösungsmenge hat wegen der freien Wählbarkeit von x_3 unendlich viele Elemente: Man wählt $x_3 = \lambda$ als **„freien Parameter“** und erhält so die Lösungsmenge:

$$L = \left\{ \left(-\frac{1}{9}\lambda, 7 - \frac{13}{9}\lambda, \lambda \right) \mid \lambda \in \mathbb{R} \right\}$$

Für jede spezielle Wahl von λ erhält man also eine gültige Lösung!
Die Lösungen sind damit abhängig von dem einen reellen Parameter λ!

Welche **Rechenmethodik** können wir aus diesen Beispielen ableiten?

1) Zunächst wird versucht, **von oben nach unten** Unbekannte aus den Gleichungen zu eliminieren, dieser Prozess heißt **Vorwärtselimination**.

2) Dann werden die Gleichungen nacheinander **von unten nach oben** gelöst, dieser Prozess heißt **Rück(wärts)substitution**. Dabei müssen eventuell **freie Parameter** gewählt werden, um die Lösbarkeit der gerade betrachteten Gleichung zu garantieren.

Bevor wir diese Rechenmethodik im Gaußschen Verfahren (Gauß-Algorithmus) verallgemeinern können, müssen wir einige formale Aspekte zu linearen Gleichungssystemen klären.
Die **allgemeine Form eines linearen Gleichungssystems mit m Gleichungen für n Unbekannte** ($m \leq n$) liefert die folgende

Definition:
Ein System der Form

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

heißt **lineares Gleichungssystem mit m Gleichungen für n Unbekannte** ($m \leq n$).
Es gibt also höchstens so viele Gleichungen wie Unbekannte.
Die Unbekannten sind $x_1, \ldots, x_n$, die Koeffizienten sind a_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$ und die rechten Seiten sind $b_1, \ldots, b_m$. Eine abkürzende Schreibweise ist

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \qquad \text{für } i = 1, \ldots, m$$

Ist $b_1 = b_2 = \cdots = b_m = 0$, so heißt das Gleichungssystem **homogen**, andernfalls **inhomogen**.
Das Gleichungssystem mit denselben Koeffizienten $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$, aber mit den rechten Seiten $\tilde{b}_1 = \tilde{b}_2 = \cdots = \tilde{b}_m = 0$ heißt das **zugehörige homogene Gleichungssystem**:

$$\sum_{j=1}^{n} a_{ij}x_j = 0 \qquad \text{für } i = 1, \ldots, m.$$

Eine Lösung eines linearen Gleichungssystems mit n Unbekannten besteht aus n Werten, die, für die Unbekannten eingesetzt, die Gleichungen erfüllen. Wir stellen die Unbekannten mit ihren n Komponenten durch einen sogenannten Spaltenvektor dar, indem wir schreiben:

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Einen Spaltenvektor bezeichnen wir durch einen kleinen Buchstaben mit einem Pfeil.

Beispiel: Das Gleichungssystem des Beispiels auf Seite 72 besitzt den Vektor der Unbekannten

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$\vec{u} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

ist der Lösungsvektor dieses linearen Gleichungssystems

Die reellen Zahlen $a_{ij} (1 \leq i \leq m,\ 1 \leq j \leq n)$ heißen Koeffizienten des linearen Gleichungssystems. Sie werden in der Koeffizientenmatrix (einem rechteckigen Zahlenschema aus m Zeilen und n Spalten)

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

zusammengefasst.
Man schreibt dafür auch abkürzend

$$\underline{\underline{A}} = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$$

Beispiel: Das Gleichungssystem des Beispiels auf Seite 72 hat die Koeffizientenmatrix

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 5 & 1 & 2 \end{pmatrix} \tag{2}$$

Die Zahlen $b_1, b_2, \dots, b_m \in \mathbb{R}$ bilden den Vektor der rechten Seite

$$\vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^m,$$

für $b_1 = b_2 = \dots = b_m = 0$ erhält man den Nullvektor

$$\vec{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^m.$$

Das inhomogene lineare Gleichungssystem schreibt man dann abkürzend

$$\underline{\underline{A}} \cdot \vec{x} = \vec{b} \quad (\Leftrightarrow \sum_{j=1}^{n} a_{ij} x_j = b_i \quad \text{für} \quad i = 1, \ldots, m)$$

und das (zugehörige) homogene lineare Gleichungssystem schreibt man abkürzend

$$\underline{\underline{A}} \cdot \vec{x} = \vec{0} \quad (\Leftrightarrow \sum_{j=1}^{n} a_{ij} x_j = 0 \quad \text{für} \quad i = 1, \ldots, m)$$

Wir fassen die Lösungsmenge L eines linearen Gleichungssystems als Teilmenge der Menge $\mathbb{R}^n$ aller n–Tupel auf:

$$L \subset \mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \ldots, x_n \in \mathbb{R} \right\}$$

Beispiele: In den drei einleitenden Beispielen auf Seite 72 haben wir gesehen, dass für die Lösungsmenge eines linearen Gleichungssystems drei Möglichkeiten bestehen

$$L_1 = \{\vec{u}\} = \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \right\}$$ Es gibt genau eine Lösung.

$$L_2 = \emptyset$$ Das Gleichungssystem ist unlösbar.

$$L_3 = \left\{ \begin{pmatrix} -\frac{1}{9}\lambda \\ 7 - \frac{13}{9}\lambda \\ \lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$ Das Gleichungssystem hat unendlich viele Lösungen in Abhängigkeit von (mindestens) einem freien Parameter.

Wir werden sehen, dass dieses alle Möglichkeiten sind. Wie man eine Lösung findet, erkennt man an den drei einleitenden Beispielen (siehe Seite 72 ff): Durch zulässige Umformungen verringert man die Anzahl der Unbestimmten von einer Gleichung zur nächsten und löst anschließend das Gleichungssystem, bei der letzten Gleichung beginnend, auf.
Das **Ziel** der Umformungsschritte ist eine Form des Gleichungssystems, in der die Unbestimmte x_1 ab der zweiten Gleichung nicht mehr erscheint, x_2 ab der dritten Gleichung nicht mehr erscheint und x_3 ab der vierten Gleichung nicht mehr erscheint und so weiter, falls das Gleichungssystem mehr als drei Unbestimmte besitzt.
Zulässige Umformungen (elementare Umformungen) eines Gleichungssystems sind solche, die die **Lösungsmenge des Gleichungssystems unverändert lassen**; davon gibt es **drei Arten**:

- **Multiplikation einer Gleichung mit einer reellen Zahl $\lambda \neq 0$ (bzw. Division durch ein $\lambda \neq 0$)**
- **zu einer Gleichung das Vielfache einer anderen addieren**
- **zwei Gleichungen vertauschen**

Zwei Gleichungssysteme, die durch zulässige Umformungen auseinander hervorgehen, heißen **äquivalent**.
Aus diesen drei grundlegenden zulässigen Umformungen bekommt man durch Hintereinanderausführung sofort eine für die Rechentechnik hilfreiche weitere **zulässige Umformung**

- **Bilden einer Linearkombination von Gleichungen, d.h. Ersetzen einer Gleichung durch eine Summe aus einem Vielfachen dieser Gleichung und dem Vielfachen einer anderen Gleichung des linearen Gleichungssystems.**

In diesem Abschnitt soll es nicht nur darum gehen, Wege zum Lösen linearer Gleichungssysteme aufzuzeigen, sondern wir wollen uns eingehender mit der Struktur linearer Gleichungssysteme befassen.
Bei dem Umgang mit linearen Gleichungssystemen sind die beiden folgenden Fragen von Bedeutung:

Frage 1: Unter welchen Umständen ist ein Gleichungssystem mit gegebenen Koeffizienten $(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ immer lösbar?

Frage 2: Was kann man über die Lösungsmenge eines linearen Gleichungssystems sagen? Wann ist insbesondere ein Gleichungssystem eindeutig lösbar?

Unser Ziel ist die Beantwortung dieser beiden Fragen.

Beispiele:

1. Bei dem 1. Beispiel auf Seite 72 lässt sich immer eine eindeutige Lösung ausrechnen, auch wenn man die Werte auf der rechten Seite beliebig verändert.
2. Bei dem 2. Beispiel auf Seite 73 gibt es keine Lösung, falls (wie in diesem Beispiel) am Ende der Vorwärtselimination $\tilde{b}_3 \neq 0$ ist.
3. Bei dem 3. Beispiel auf Seite 74 gibt es (unendlich) viele Lösungen in Abhängigkeit von einem freien Parameter.

Um uns den Antworten auf diese Fragen anzunähern, wenden wir uns zunächst besonders einfachen Gleichungssystemen, nämlich den homogenen Gleichungssystemen zu.

6.2 Klassifikation linearer Gleichungssysteme und die Struktur der Lösungsmenge

Homogene Gleichungssysteme sind solche, bei denen auf der rechten Seite nur Nullen stehen.

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &=& 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &=& 0 \\ \vdots \quad + \quad \vdots \quad + \vdots + \quad \vdots &=& \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &=& 0 \end{array}$$

Homogene Gleichungssysteme besitzen mit Sicherheit immer mindestens eine Lösung, nämlich die Null:

$$\vec{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Eine weitere Besonderheit homogener Gleichungssysteme ist:
Satz:
Die Lösungsmenge L eines **homogenen Gleichungssystems** ist abgeschlossen gegenüber komponentenweiser Addition und Multiplikation mit reellen Zahlen, d. h.:

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in L \quad \text{und} \quad \vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in L \quad \Rightarrow \quad \vec{u} + \vec{v} = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix} \in L$$

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \in L \quad \text{und} \quad \lambda \in \mathbb{R} \quad \Rightarrow \quad \lambda\vec{u} = \begin{pmatrix} \lambda u_1 \\ \vdots \\ \lambda u_n \end{pmatrix} \in L$$

Beweis: $\vec{u} \in L$ und $\vec{v} \in L$ bedeutet, dass beide das homogene Gleichungssystem erfüllen, d. h.:

$$\begin{array}{rcl} \sum_{j=1}^{n} a_{ij}u_j &=& 0 \\ \sum_{j=1}^{n} a_{ij}v_j &=& 0 \end{array} \qquad \text{für} \quad i = 1, \ldots, m$$

Die Addition beider Gleichungen liefert:

$$\begin{aligned}
&\sum_{j=1}^{n} a_{ij}u_j \quad + \quad \sum_{j=1}^{n} a_{ij}v_j \quad = \quad \sum_{j=1}^{n} a_{ij}(u_j + v_j) \\
\Rightarrow \quad & 0 \quad + \quad 0 \quad = \quad \sum_{j=1}^{n} a_{ij}(u_j + v_j) \qquad \text{für} \quad i = 1, \ldots, m \\
\Rightarrow \quad & \vec{u} + \vec{v} = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix} \quad \text{erfüllt das homogene Gleichungssystem} \\
\Rightarrow \quad & \vec{u} + \vec{v} \in L
\end{aligned}$$

Den zweiten Teil der Behauptung erhält man, in dem man für $i = 1, \ldots, m$ beide Seiten der Gleichung

$$\sum_{j=1}^{n} a_{ij}u_j \quad = \quad 0$$

mit $\lambda \in \mathbb{R}$ multipliziert.

□

Eine einfache Folgerung aus dem Satz ist dieses: Hat ein homogenes Gleichungssystem zwei verschiedene Lösungen, so hat es bereits unendlich viele Lösungen. Sind nämlich $\vec{u}$ und $\vec{v}$ zwei Lösungen, so muss mindestens eine von ihnen ungleich Null sein; ist etwa $\vec{u} \neq 0$, so ist nach dem Satz für jedes $\lambda \in \mathbb{R}$ auch $\lambda\vec{u}$ eine Lösung; dieses sind unendlich viele verschiedene!

Bei der Behandlung beliebiger (d. h. insbesondere inhomogener) Gleichungssysteme ist es nützlich, das zugehörige homogene Gleichungssystem[1] zu betrachten. Einen ersten Zusammenhang zwischen einem allgemeinen Gleichungssystem und seinem zugehörigen homogenen Gleichungssystem gibt der folgende

Hilfssatz:
Sei L die Lösungsmenge des **inhomogenen** linearen Gleichungssystems

$$\sum_{j=1}^{n} a_{ij}x_j \quad = \quad b_i \qquad \text{für} \quad i = 1, \ldots, m$$

und L^H die Lösungsmenge des zugehörigen homogenen Gleichungssystems, dann gilt

$$\vec{u}, \vec{v} \in L \quad \Rightarrow \quad \vec{u} - \vec{v} = \begin{pmatrix} u_1 - v_1 \\ \vdots \\ u_n - v_n \end{pmatrix} \in L^H$$

Das bedeutet: Die Differenz zweier Lösungen ist Lösung des zugehörigen homogenen Systems.

[1] d. h. das Gleichungssystem mit denselben Koeffizienten, das auf der rechten Seite nur Nullen hat

Beweis: $\vec{u}$ und $\vec{v}$ sind Lösungen, d. h. sie erfüllen das Gleichungssystem:

$$\begin{array}{rcl} \sum_{j=1}^{n} a_{ij}u_j & = & b_i \\ & & \text{für} \quad i = 1, \ldots, m \\ \sum_{j=1}^{n} a_{ij}v_j & = & b_i \end{array}$$

Die Subtraktion beider Gleichungen liefert für $i = 1, \ldots, m$

$$\begin{array}{rcl} \sum_{j=1}^{n} a_{ij}u_j - \sum_{j=1}^{n} a_{ij}v_j & = & b_i - b_i = 0 \\ \Rightarrow \quad \sum_{j=1}^{n} a_{ij}(u_j - v_j) & = & 0 \qquad \text{für} \quad i = 1, \ldots, m \\ \Rightarrow \quad \vec{u} - \vec{v} = \begin{pmatrix} u_1 - v_1 \\ \vdots \\ u_n - v_n \end{pmatrix} & & \text{ist Lösung des homogenen Systems} \end{array}$$

qed

Beispiel: Das Beispiel Nr. 3 auf Seite 74

$$\begin{array}{rcrcrcll} x_1 & + & 2x_2 & + & 3x_3 & = & 14 & \text{(I)} \\ 7x_1 & + & 5x_2 & + & 8x_3 & = & 35 & \text{(II)} \\ 10x_1 & + & 2x_2 & + & 4x_3 & = & 14 & \text{(III)} \end{array}$$

hatte, wie berechnet, die Lösungsmenge

$$L = \left\{ \begin{pmatrix} -\frac{1}{9}\lambda \\ 7 - \frac{13}{9}\lambda \\ \lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

Sind etwa $\vec{u}$ und $\vec{v}$ die beiden Lösungen, die zu $\lambda = 18$ und $\lambda = 0$ gehören, so rechnet man leicht nach, dass deren Differnz $\vec{u} - \vec{v}$ eine Lösung des zugehörigen homogenen Systems ist:

$$\vec{u} - \vec{v} = \begin{pmatrix} -2 \\ -19 \\ 18 \end{pmatrix} - \begin{pmatrix} 0 \\ 7 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ -26 \\ 18 \end{pmatrix} \in L^H$$

Den endgültigen Zusammenhang zwischen L und L^H beschreibt der folgende

Satz:
Sei

$$\vec{x}_0 = \begin{pmatrix} x_{01} \\ \vdots \\ x_{0n} \end{pmatrix}$$

eine fest gewählte (man sagt: eine spezielle) Lösung des linearen Gleichungssystems. Man erhält alle weiteren Lösungen dadurch, daß man zu $\vec{x}_0$ beliebige Lösungen des zugehörigen homogenen Systems addiert. Man schreibt diese Aussage in der Form

$$L = \vec{x}_0 + L^H = \{\vec{u} \mid \vec{u} = \vec{x}_0 + \vec{v} \text{ mit } \vec{v} \in L^H\}$$

Beweis: 1. Schritt: Wir müssen zeigen, dass jeder Summe der Form

$$\vec{u} = \vec{x}_0 + \vec{v} = \begin{pmatrix} x_{01} + v_1 \\ \vdots \\ x_{0n} + v_n \end{pmatrix} \quad \text{mit} \quad \vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in L^H$$

das lineare Gleichungssystem erfüllt. Wir testen das aus, indem wir ganz einfach $\vec{u} = \vec{x}_0 + \vec{v}$ in das Gleichungssystem einsetzen:
Für $i = 1, \ldots, m$ ist dann

$$\sum_{j=1}^{n} a_{ij}(x_{0j} + v_{0j}) = \sum_{j=1}^{n} a_{ij}x_{0j} + \sum_{j=1}^{n} a_{ij}v_j$$

Nun ist für $i = 1, \ldots, m$

$$\sum_{j=1}^{n} a_{ij}x_{0j} = b_i$$

denn $\vec{x}_0$ ist Lösung des Gleichungssystems

$$\sum_{j=1}^{n} a_{ij}v_j = 0$$

denn $\vec{v}$ ist Lösung des homogenen Gleichungssystems

Verwendet man dieses, so ist für $i = 1, \ldots, m$ schließlich

$$\begin{aligned} \sum_{j=1}^{n} a_{ij}(x_{0j} + v_j) &= \sum_{j=1}^{n} a_{ij}x_{0j} + \sum_{j=1}^{n} a_{ij}v_j \\ &= b_i + 0 \\ &= b_i \end{aligned}$$

Also:

$$\vec{x}_0 + \vec{v} \in L \qquad \text{für jedes } \vec{v} \in L^H$$

2. Schritt: Sei $\vec{u} \in L$ beliebig, wir müssen zeigen, dass sich $\vec{u}$ in der Form

$$\vec{u} = \vec{x}_0 + \vec{v} \quad \text{mit} \quad \vec{v} \in L^H$$

darstellen lässt. Zu finden ist ein geeignetes $\vec{v} \in L^H$; wir setzen dazu an

$$\vec{v} \;=\; \vec{u} - \vec{x}_0 \;=\; \begin{pmatrix} u_1 - x_{01} \\ \vdots \\ u_n - x_{0n} \end{pmatrix}$$

Da $\vec{x}_0$ und $\vec{u}$ beides Lösungen des Gleichungssystems sind, ist nach dem vorangegangenen Hilfssatz (siehe Seite 80) $\vec{v} = \vec{u} - \vec{x}_0$ eine Lösung des zugehörigen homogenen Systems; $\vec{v}$ leistet daher das Gewünschte: es ist

$$\vec{u} \;=\; \vec{x}_0 + (\vec{u} - \vec{x}_0) \;=\; \vec{x}_0 + \vec{v} \quad \text{mit} \quad \vec{v} \in L^H$$

Damit ist alles bewiesen.

qed

Dieser Satz besitzt eine ähnliche Folgerung wie der Satz auf Seite 79: hat ein allgemeines lineares Gleichungssystem zwei verschiedene Lösungen $\vec{u}_1 \neq \vec{u}_2$, so besitzt es bereit unendlich viele Lösungen: Es ist nämlich

$$0 \;\neq\; \vec{u}_1 - \vec{u}_2 \;\in\; L^H \quad \Rightarrow \quad \lambda \cdot (\vec{u}_1 - \vec{u}_2) \;\in\; L^H \quad \text{für alle } \lambda \in \mathbb{R}$$

Daraus gewinnt man die unendlich vielen Lösungen

$$\vec{u}_1 + \lambda \cdot (\vec{u}_1 - \vec{u}_2) \;\in\; L$$

Eine weitere Folgerung aus dem Satz, die uns dicht an die Antwort von Frage 2 (siehe Seite 78) heranführen wird, ist
Folgerung: Ein lösbares lineares Gleichungssystem sei gegeben. Das Gleichungssystem ist genau dann eindeutig lösbar, wenn das zugehörige homogene System nur die Lösung 0 besitzt.
Beweis: Die Aussage folgt aus

$$L \;=\; \vec{x}_0 + L^H \qquad \text{mit einem speziellen } \vec{x}_0 \in L$$

L hat nur dann genau die einzige Lösung $\vec{x}_0$, wenn L^H nur die Nulllösung enthält.

qed

Wir müssen jetzt noch klären,

- wann ein homogenes System nur die Nulllösung besitzt;
- wie man feststellt, ob ein Gleichungssystem mindestens eine spezielle Lösung $\vec{x}_0$ besitzt;
- wie man die spezielle Lösung $\vec{x}_0$ findet.

Um dieses zu erkennen, müssen wir das Gleichungssystem geeignet umformen. Dieses ist Inhalt des Gaußschen Eliminationsverfahrens.
Wir werden mit dessen Hilfe entdecken, dass es neben der Anzahl der Unbestimmten n und der Anzahl der Gleichungen m noch zwei Maßzahlen für ein lineares Gleichungssystem gibt: dessen Rang r und Corang s.
Mit Hilfe von r und s werden wir die beiden Fragen auf Seite 78 beantworten können.

6.3 Der Gaußalgorithmus

Um weitergehende Aussagen über ein lineares Gleichungssystem zu gewinnen, muss man das Gleichungssystem auf die Art umformen, wie es in den ersten Beispielen dieses Abschnitts (siehe Seite 72) erfolgte. Hier dürfen natürlich nur die zulässigen Umformungen (siehe Seite 77) benutzt werden. Diese Vorgehensweise ist genau der Inhalt des Gaußschen Satzes. Zunächst dazu aber noch ein

Beispiel: Wir wollen das 5×5–Gleichungssystem

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 2 \\ -2x_1 - 10x_2 - 5x_3 + x_4 - 2x_5 &= -6 \\ -2x_1 - 10x_2 - 9x_3 + 6x_4 + 4x_5 &= 3 \\ x_1 + 5x_2 + 5x_3 - 2x_4 - 6x_5 &= -1 \\ -x_1 - 5x_2 - 5x_3 + 5x_4 &= 4 \end{aligned} \tag{3}$$

lösen. Wir beginnen, indem wir das 2–Fache der ersten Gleichung zur zweiten und dritten Gleichung addieren, die erste Gleichung von der vierten abziehen und die erste Gleichung zur letzten addieren; wir erhalten

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 2 \\ x_3 - x_4 - 2x_5 &= -2 \\ -3x_3 + 4x_4 + 4x_5 &= 7 \\ 2x_3 - x_4 - 6x_5 &= -3 \\ -2x_3 + 4x_4 &= 6 \end{aligned}$$

Wir addieren jetzt das Dreifache der zweiten Gleichung zur dritten, ziehen das Doppelte der zweiten von der vierten ab, addieren das Doppelte der zweiten zur fünften und erhalten

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 2 \\ x_3 - x_4 - 2x_5 &= -2 \\ x_4 - 2x_5 &= 1 \\ x_4 - 2x_5 &= 1 \\ 2x_4 - 4x_5 &= 2 \end{aligned}$$

Als letztes ziehen wie noch die dritte Gleichung bzw. deren Doppeltes von der vierten und fünften Gleichung ab und erhalten die fertige Umformung:

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 2 \\ x_3 - x_4 - 2x_5 &= -2 \\ x_4 - 2x_5 &= 1 \\ 0x_5 &= 0 \\ 0x_5 &= 0 \end{aligned} \tag{4}$$

Diese Form des Gleichungssystems ist dadurch gekennzeichnet, dass

- die Variable x_i (spätestens) ab der $i+1$ Gleichung nicht mehr erscheint,
- einige der Variablen einmal an einer „Stufe“ mit Koeffizienten 1 vorkommen (x_1, x_3, x_4), andere Variablen hingegen nur im „Inneren“ der Gleichungen auftauchen (x_2, x_5),
- die beiden letzten Gleichungen entartete „Nullgleichungen“ sind, alle Koeffizienten in ihnen sind Null.

Da auch ihre rechten Seiten der Nullgleichungen Null sind, ist dieses Gleichungssystem lösbar.

Jetzt zur Verallgemeinerung!

Satz: (**Gaußsches Eliminationsverfahren - Teil 1: Vorwärtselimination**)
Gegeben sei ein lineares Gleichungssystem:

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

Hierzu gibt es ein äquivalentes[2] Gleichungssystem in sogenannter **reduzierter Form** oder **Zeilenstufenform**.
Schreibt man nur die Koeffizienten der Zeilenstufenform auf, so erhält man ein Schema der folgenden Art:

[2] d. h. durch zulässige Umformungen gewonnenes

$$
\begin{array}{|ccccccccccc||c}
\hline
1 & * & * & * & * & * & * & \cdots & * & \cdots & * & \beta_1 \\
0 & 0 & 1 & * & * & * & * & \cdots & * & \cdots & * & \beta_2 \\
 & & 0 & 0 & 1 & * & * & & \vdots & & \vdots & \beta_3 \\
 & & \vdots & & 0 & 0 & 0 & & & & & \vdots \\
 & & 0 & \cdots & & & 0 & 1 & * & \cdots & * & \beta_r \\
 & & 0 & \cdots & & & 0 & 0 & 0 & \cdots & 0 & \beta_{r+1} \\
 & & \vdots & & & & \vdots & \vdots & & \cdots & \vdots & \vdots \\
 & & 0 & \cdots & & & 0 & 0 & 0 & \cdots & 0 & \beta_m \\
\hline
\end{array}
$$

Hierbei sind die $*$ irgendwelche Zahlen, die β_i sind die rechten Seiten der umgeformten Gleichungen.
Die genaue Darstellung der reduzierten Form lautet:

$$
\begin{array}{cccccccccc}
x_1 + \alpha_{12}\cdot x_2 & + \alpha_{13}\cdot x_3 + & \alpha_{14}\cdot x_4 & + \ldots + & \alpha_{1n}\cdot x_n & = & \beta_1 \\
0 + x_2 & + \alpha_{23}\cdot x_3 + & \alpha_{24}\cdot x_4 & + \ldots + & \alpha_{2n}\cdot x_n & = & \beta_2 \\
\vdots + \vdots & + \vdots + & \vdots & + \ldots + & \vdots & = & \vdots \\
0 + 0 & + x_r + & \alpha_{rr+1}\cdot x_{r+1} & + \ldots + & \alpha_{rn}\cdot x_n & = & \beta_r \\
\hline
0 + 0 & + 0 + & 0\cdot x_{r+1} & + \ldots + & 0\cdot x_n & = & \beta_{r+1} \\
\vdots + \vdots & + \vdots + & \vdots & + \ldots + & \vdots & = & \vdots \\
0 + 0 & + 0 + & 0\cdot x_{r+1} & + \ldots + & 0\cdot x_n & = & \beta_m
\end{array}
\tag{5}
$$

Dabei ist $1 \le r \le m \le n$.

Hiermit **endet die Vorwärtselimination** im Gauß-Algorithmus: Das Gleichungssystem ist überführt in ein **äquivalentes** lineares Gleichungssystem in **Zeilenstufenform**. Unterhalb der r-ten Zeile stehen links vom Gleichheitszeichen nur noch Nullen als Koeffizienten vor den Unbekannten; ab der r+1-ten Gleichung (r+1-ten Zeile) haben die Gleichungen also die Form $0 = \beta_j, \quad r+1 \le j \le m$. Links vom Gleicheitszeichen hat man hier also eine sog. **Nullzeile**.

Wie erhält man die Zeilenstufenform?
Die Beweisidee vom 1. Teil: Vorwärtselimination:
Nach eventuellem Zeilentausch kann man davon ausgehen, dass $\alpha_{11} \neq 0$ gilt. Dann wird (beginnend mit der nächsten Zeile) Zeile für Zeile durch **zulässige Umformungen** der Form

(neue i-te Zeile) = alte i-te Zeile $-\alpha_{i1}/\alpha_{11}\cdot$(erste Zeile) für $2 \le i \le m$

so umgeformt, dass an der ersten Stelle jeder neuen Zeile eine Null, genauer $0 \cdot x_1$ steht. Danach sucht man den Koeffizienten $\alpha_{ij} \neq 0$ mit kleinstem Zeilenindex i und kleinstem Spaltenindex j und wiederholt das zuvor durchgeführte Verfahren beginnend in der i-ten Zeile.
Dieser Prozess wird so lange durchgeführt, bis alle m Zeilen des Gleichungssystems bearbeitet sind. Durch wiederholten Zeilentausch werden die eventuell vorhandenen Nullzeilen schließlich nach unten gebracht.
Abschließend führt in jeder **Nichtnullzeile Division durch den führenden Koeffizienten** dazu, dass die Zeilen mit einer 1 als Koeffizienten beginnen.

Wir konnten bereits in unseren einleitenden Beispielen erkennen, dass die **Auswahl der vorgenommenen Umformungsschritte der Vorwärtselimination nur von den Koeffizienten auf der linken Seite** abhing:
Alle Rechenschritte der Vorwärtselimination orientieren sich an den Koeffizienten $(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ des linearen Gleichungssystems, die Werte auf der rechten Seite $(b_i)_{1\leq i\leq m}$ spielen für die Auswahl der Rechenschritte der Vorwärtselimination keine Rolle.

Definition:
Die Zahl r aus dem Satz heißt **Rang** des Gleichungssystems, $s = n - r$ heißt **Corang**. Der **Rang r** eines linearen Gleichungssystems ist die **Anzahl der Nichtnullzeilen links vom Gleichheitszeichen** am Ende der Vorwärtselimination des Gauß-Algorithmus. Der **Corang** ist die **Anzahl der Unbekannten minus Rang** des linearen Gleichungssystems. Der **erweiterte Rang $\bar{r}$** ist die **Anzahl der Nichtnullzeilen** am Ende der Vorwärtselimination des Gauß-Algorithmus unter Berücksichtigung aller Terme also **links und rechts vom Gleichheitszeichen**.

Beispiel: Das Gleichungssystem auf Seite 84 hat die reduzierte Form (Zeilenstufenform)

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 2 \\ x_3 - x_4 - 2x_5 &= -2 \\ x_4 - 2x_5 &= 1 \\ 0x_5 &= 0 \\ 0x_5 &= 0 \end{aligned}$$

Wir erkennen zwei komplette Nullzeilen, damit gilt:

Rang r = 3

Corang s = 5 - 3 = 2

erweiterter Rang $\bar{r} = 3$

In diesem Fall gilt also r=$\bar{r}$, der Rang ist gleich dem erweiterten Rang.

Satz: (**Gaußsches Eliminationsverfahren - Teil 2: Rück(wärts)substitution**)
Gegeben ist ein lineares Gleichungssystem in **Zeilenstufenform**

$$\begin{array}{cccccccccccc}
x_1 & + & \alpha_{12}\cdot x_2 & + & \alpha_{13}\cdot x_3 & + & \alpha_{14}\cdot x_4 & + \ldots + & \alpha_{1n}\cdot x_n & = & \beta_1 \\
0 & + & x_2 & + & \alpha_{23}\cdot x_3 & + & \alpha_{24}\cdot x_4 & + \ldots + & \alpha_{2n}\cdot x_n & = & \beta_2 \\
\vdots & + & \vdots & + & \vdots & + & \vdots & + \ldots + & \vdots & = & \vdots \\
0 & + & 0 & + & x_r & + & \alpha_{rr+1}\cdot x_{r+1} & + \ldots + & \alpha_{rn}\cdot x_n & = & \beta_r \\
\hline
0 & + & 0 & + & 0 & + & 0\cdot x_{r+1} & + \ldots + & 0\cdot x_n & = & \beta_{r+1} \\
\vdots & + & \vdots & + & \vdots & + & \vdots & + \ldots + & \vdots & = & \vdots \\
0 & + & 0 & + & 0 & + & 0\cdot x_{r+1} & + \ldots + & 0\cdot x_n & = & \beta_m
\end{array} \tag{6}$$

dann gilt:

1) Das **inhomogene lineare Gleichungssystem** ist **nur lösbar**, wenn gilt: r = r̄, also **Rang = erweiterter Rang**.
   Das **homogene lineare Gleichungssystem ist immer lösbar**, $\vec{x} = \vec{0}$ ist immer eine Lösung.

2) Ist $s = n - r > 0$, also **Corang > 0**, so hat das lineare Gleichungssystem **unendlich viele Lösungen**, die Lösungen enthalten **s freie Parameter**.

3) Das lineare Gleichungssystem hat **genau eine Lösung**, wenn gilt: r = r̄ = n und damit $s = 0$.
   Da r die Anzahl von Nichtnullzeilen unter insgesamt m Zeilen (Anzahl der Gleichungen) ist, ist Eindeutigkeit für $m < n$ (d.h. weniger Gleichungen als Unbekannte) nicht möglich!

4) Die **Lösungsmenge** berechnet man nach folgendem Algorithmus, der sog. **Rück(wärts)substitution**:

   Die Beweisidee vom 2. Teil: Rück(wärts)substitution:
   Man löst die **letzte (unterste) Nichtnullzeile** nach der **führenden Unbekannten** auf. Wenn danach rechts vom Gleichheitszeichen Unbekannte stehen, ersetzt man diese durch **freie Parameter**.
   Dann arbeitet man sich **zeilenweise nach oben (zurück/rückwärts)** und löst auch diese Zeilen jeweils nach der führenden Unbekannten auf. Die Unbekannten rechts vom Gleichheitszeichen **substituiert** man (d.h. ersetzt man) durch die zuvor berechneten Ausdrücke für die jeweilige Unbekannte. Ist eine Substitution nicht möglich, ersetzt man diese Unbekannte durch einen weiteren freien Parameter.

Beispiel: Das Gleichungssystem auf Seite 84 hat die reduzierte Form (Zeilenstufenform)

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 2 \\ x_3 - x_4 - 2x_5 &= -2 \\ x_4 - 2x_5 &= 1 \\ 0x_5 &= 0 \\ 0x_5 &= 0 \end{aligned}$$

In diesem Fall gilt also r=$\bar{\text{r}}$=3, der Rang ist gleich dem erweiterten Rang und Corang s=2, d.h.:
Das lineare Gleichungssystem ist lösbar, die Lösungsmenge enthält unendlich viele Elemente abhängig von 2 freien Parametern.
Man findet die Lösungen, indem man die unterste Nichtnullzeile nach der führenden Unbekannten x_4 auflöst und $x_5 = \lambda_1$ als 1. freien Parameter setzt:

$$x_4 = 1 + 2x_5 = 1 + 2\lambda_1$$

und anschließend zeilenweise nach oben (zurück/rückwärts) berechnet:

$$x_3 = -2 + x_4 + 2x_5 = -2 + (1 + 2\lambda_1) + 2\lambda_1 = -1 + 4\lambda_1$$

$$x_1 = 2 - 5x_2 - 3x_3 + x_4 = 6 - 5x_2 - 10\lambda_1$$

dabei setzt man $x_2 = \lambda_2$ als weiteren (2.) freien Parameter, man erhält so:

$$x_1 = 6 - 10\lambda_1 - 5\lambda_2$$

Als Ergebnis bekommen wir die Lösungsmenge

$$L = \left\{ \begin{pmatrix} 6 - 10\lambda_1 - 5\lambda_2 \\ \lambda_2 \\ -1 + 4\lambda_1 \\ 1 + 2\lambda_1 \\ \lambda_1 \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\} \tag{7}$$

Für jede spezielle Wahl der freien Parameter λ_1 und λ_2 bekommt man eine spezielle Lösung des linearen Gleichungssystems, z.B. für $\lambda_1 = 1$ und $\lambda_2 = 0$:

$$\vec{x_s} = \begin{pmatrix} -4 \\ 0 \\ 3 \\ 3 \\ 1 \end{pmatrix} \tag{8}$$

Folgerung: Ein Gleichungssystem ist genau dann eindeutig lösbar, wenn sein Rang gleich der Anzahl der Unbekannten ist:

$$r = n$$

Man sagt: Das Gleichungssystem besitzt **vollen Rang**.

Beispiel: Das Gleichungssystem von Seite 72 besitzt die reduzierte Form

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 14 \\ x_2 + 2x_3 &= 8 \\ x_3 &= 3 \end{aligned}$$

Sein Rang ist $r = 3 = n$, und es gibt nur eine Lösung $\vec{u} = (1, 2, 3)$.
Beispiel: Das Gleichungssystem von Seite 74 mit der reduzierten Form

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 14 \\ x_2 + \frac{13}{9}x_3 &= 7 \\ 0x_3 &= 0 \end{aligned}$$

besitzt keinen vollen Rang, es ist hier $r = 2 < 3 = n$. Wie wir gesehen haben, ist es nicht eindeutig lösbar, die Lösungsmenge ist unendlich

$$L = \left\{ \begin{pmatrix} -(1/9)\lambda \\ 7 - (13/9)\lambda \\ \lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

in Abhängigkeit von $1 = 3 - 2 = s = n - r$ freiem Parameter λ.

Wir sind jetzt dicht an der Antwort zu Frage 2 auf Seite 78. Wir kommen jetzt nochmal auf homogene Gleichungssysteme zurück.

Satz:
Ein homogenes Gleichungssystem mit n Unbekannten besitzt genau dann nur die Lösung $\vec{x} = \vec{0}$, wenn sein Rang $r = n$ ist.
Beweis: Nach der Folgerung auf Seite 90 ist eine Gleichungssystem genau dann höchstens eindeutig lösbar, wenn $r = n$ ist. Da ein homogenes Gleichungssystem immer die Lösung $\vec{x} = \vec{0}$ besitzt, ist $\vec{x} = \vec{0}$ in diesem Falle die einzige Lösung.

qed

Satz:
Ein homogenes Gleichungssystem mit Corang $s > 0$ besitzt s sogenannte **Grundlösungen** (oder **Basislösungen**)

$$\vec{x}_1, \ldots, \vec{x}_s$$

so dass für die Lösungsmenge L^H des homogenen Systems gilt

$$L^H = \{\lambda_1\vec{x}_1 + \cdots + \lambda_s\vec{x}_s \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\}$$

Diese Aussage besagt, dass sich alle Lösungen eines homogenen Systems als Summe von Vielfachen endlich vieler fest gewählter Lösungen darstellen lassen. Die Faktoren $\lambda_1, \ldots, \lambda_s$ sind dabei **freie Parameter** oder auch Freiheitsgrade.

Anstelle eines Beweises geben wir nur an, wie man die Grundlösungen $\vec{x}_1, \ldots, \vec{x}_s$ erhält. Bei den freien Parametern

$$\lambda_1, \ldots, \lambda_s$$

, die bei Corang $s > 0$ im Gaußschen Eliminationsverfahren gesetzt werden, geben wir immer genau einem Parameter den Wert 1 und den anderen Parametern den Wert 0. Wir erhalten so $\vec{x}_i$, indem wir

$$\lambda_i = 1,\ \lambda_j = 0,\ \ldots, j \neq i,\ 1 \leq i, j \leq s$$

setzen.

Beispiel: Wir betrachten das zu dem Gleichungssystem (3) auf Seite 84 gehörige homogene System, seine reduzierte Form unterscheidet sich von (4) nur dadurch, dass auf der rechten Seite nur Nullen stehen:

$$\begin{aligned} x_1 + 5x_2 + 3x_3 - x_4 &= 0 \\ x_3 - x_4 - 2x_5 &= 0 \\ x_4 - 2x_5 &= 0 \\ 0x_5 &= 0 \\ 0x_5 &= 0 \end{aligned}$$

Man erkennt: der Corang ist $s = 2$ und die Lösungsmenge ist

$$L^H = \left\{ \begin{pmatrix} -10\lambda_1 - 5\lambda_2 \\ \lambda_2 \\ 4\lambda_1 \\ 2\lambda_1 \\ \lambda_1 \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\} \tag{9}$$

Wir wollen die beiden Grundlösungen $\vec{x}_1$ und $\vec{x}_2$ berechnen:

$\vec{x}_1$: Man setzt

$$\lambda_1 = 1 \quad \textit{und} \quad \lambda_2 = 0 \Rightarrow \vec{x}_1 = \begin{pmatrix} -10 \\ 0 \\ 4 \\ 2 \\ 1 \end{pmatrix}$$

$\vec{x}_2$: Man setzt

$$\lambda_1 = 0 \quad und \quad \lambda_2 = 1 \Rightarrow \vec{x}_2 = \begin{pmatrix} -5 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Insgesamt ergibt sich die Lösungsmenge des homogenen Systems

$$L^H = \left\{ \lambda_1 \cdot \begin{pmatrix} -10 \\ 0 \\ 4 \\ 2 \\ 1 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} -5 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\} = L \tag{10}$$

Wir fassen jetzt die beiden Sätze auf den Seiten 82 und 90 zusammen und erhalten als ein Endergebnis dieses Abschnitts den

Satz:

Ein allgemeines Gleichungssystem, besitzt, sofern es lösbar ist, die Lösungsmenge

$$L = \{\vec{x}_0 + \lambda_1\vec{x}_1 + \ldots + \lambda_s\vec{x}_s \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\} \tag{11}$$

Dabei ist $\vec{x}_0$ eine spezielle Lösung des Gleichungssystems mit Corang s und $\vec{x}_1, \ldots, \vec{x}_s$ sind die s Grundlösungen des zugehörigen homogenen Systems.

Beweis: Es ist

$$\begin{aligned} L &= \vec{x}_0 + L^H && \text{nach dem Satz auf Seite 82} \\ &= \vec{x}_0 + \{\lambda_1\vec{x}_1 + \ldots + \lambda_s\vec{x}_s \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\} && \text{nach dem Satz auf Seite 90} \\ &= \{\vec{x}_0 + \lambda_1\vec{x}_1 + \ldots + \lambda_s\vec{x}_s \mid \lambda_1, \ldots, \lambda_s \in \mathbb{R}\} \end{aligned}$$

qed

Beispiel: Nimmt man die obige Gleichung (10) und die in dem Beispiel auf Seite 89 berechnete spezielle Lösung (7), so erhält man die Lösungsmenge des Gleichungssystems (3):

$$L = \left\{ \begin{pmatrix} -4 \\ 0 \\ 3 \\ 3 \\ 1 \end{pmatrix} + \lambda_1 \cdot \begin{pmatrix} -5 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} -10 \\ 0 \\ 4 \\ 2 \\ 1 \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\}$$

Nun haben wir auf die beiden zentralen Fragen dieses Abschnitts (siehe Seite 78) Antworten gefunden:

Antwort auf Frage 1: Ein Gleichungssystem mit gegebenen Koeffizienten $(a_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ ist genau dann immer lösbar, wenn $r = \bar{r}$ also Rang gleich erweitertem Rang ist.

Antwort auf Frage 2: Die Lösungsmenge eines linearen Gleichungssystems wird durch (11) beschrieben. Das Gleichungssystem ist insbesondere nur eindeutig lösbar, wenn $n - r = s = 0$ bzw. $r = n$ ist (siehe Seite 90).

Zusammenfassend folgt hier noch einmal eine Liste der Schritte, die man beim Lösen eines gegebenen linearen Gleichungssystems ausführt:

1. Herstellen der reduzierten Form mit dem Gaußschen Verfahren
2. Beachten der Nullgleichungen: Sind Nullzeilen vorhanden, die auf der rechten Seite von Null verschiedene Werte besitzen, so kann man wegen der Unlösbarkeit des Gleichungssystems den Lösungsvorgang abbrechen.
3. Im Falle eines inhomogenen Systems Bestimmung einer speziellen Lösung $\vec{x}_0$
4. Im Falle von $s > 0$: Bestimmung der s Grundlösungen $\vec{x}_1, \ldots, \vec{x}_s$ des zugehörigen homogenen Systems.
5. Aufstellen der Lösungsmenge nach (11)

6.4 Das Gauß-Schema zur Formalisierung des Gauß-Algorithmus

Gegeben ist das lineare Gleichungssystem $\underline{\underline{A}} \cdot \vec{x} = \vec{b}$ mit der **Koeffizientenmatrix** $\underline{\underline{A}}$, dem **Vektor der Unbekannten** $\vec{x}$ und dem **Vektor der rechten Seite** $\vec{b}$ (auch kurz „rechte Seite“ genannt).
Wie wir gesehen haben, kommt es bei der Durchführung der Vorwärtselimination des Gauß-Algorithmus nicht auf die Bezeichnung (Namen) der Unbekannten sondern nur auf die **Koeffizientenmatrix** $\underline{\underline{A}}$ und den **Vektor der rechten Seite** $\vec{b}$ an.

Daher kann man das Verfahren **stark formalisiert** im sogenannten **Gauß-Schema** durchführen. Das Gauß-Schema ist eine **Tabelle** mit zwei Spalten (linke Spalte und rechte Spalte), die jeweils links eine Matrix und rechts einen Vektor enthält. Jede elementare Umformung der Vorwärtselimination, die simultan in der linken und rechten Spalte durchgeführt wird, erzeugt eine neue Spalte diesen Typs. Man startet in der ersten Zeile mit der Koeffizientenmatrix $\underline{\underline{A}}$ in der linken Spalte und dem Vektor der rechten Seite $\vec{b}$ in der rechten Spalte (vereinfacht ohne Klammern geschrieben). Am Ende der Vorwärtselimination hat man in der linken Spalte eine Matrix in Dreiecks- bzw. Trapezform (mit Nullzeilen) und in der rechten Spalte einen Vektor.
Dann kann man folgende Größen ermitteln:

1) Der **Rang** von $\underline{\underline{A}}$ ist die Anzahl der Nichtnullzeilen in der linken Spalte des Schemas.

2) Der **erweiterte Rang** ist die Anzahl der Nichtnullzeilen im kompletten Schema, d.h. unter Berücksichtigung der linken Spalte und der rechten Spalte.

3) Gilt **Rang≠erweiterter Rang**, ist das Gleichungssystem nicht lösbar.
Gilt **Rang=erweiterter Rang** kann die **Rück(wärts)substitution** zur Lösung des linearen Gleichungssystems beginnen.

Falls das Gleichungssystem lösbar ist,kann man dann anschließend durch **Rücksubstitution/Rückwärtseinsetzen** die Lösungen berechnen.
Das folgende Beispiel demonstriert das gerade beschriebene Vorgehen.

Beispiel:
Gegeben ist das lineare Gleichungssystem

$$\underline{\underline{A}} \cdot \vec{x} = \vec{b} \Leftrightarrow \begin{pmatrix} -2 & -1 & 3 \\ 2 & 2 & 3 \\ 4 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

Das **zugehörige Gauß-Schema** ist dann

−2	−1	3	1	
2	2	3	2	
4	1	−3	3	II+I und III+2·I
−2	−1	3	1	
0	1	6	3	
0	−1	3	5	III+II
−2	−1	3	1	
0	1	6	3	
0	0	9	8	

Dabei wurde gerechnet (römische Ziffern bezeichnen die Gleichungen des Systems):
1. Schritt (von erster Zeile zu zweiter Zeile der Tabelle): II+I und III+2·I
2. Schritt (von zweiter Zeile zu dritter Zeile der Tabelle): III+II

Man sieht: Rang=erweiterter Rang ⇒ das Gleichungssystem ist lösbar,
Corang=0 ⇒ man benötigt keine freien Parameter,
die Rücksubstitution startet in der letzten Zeile des Gleichungssystems:
$x_3 = \frac{8}{9}$ und durch Rückwärtseinsetzen erhält man $x_2 = 3 - 6 \cdot x_3 = -\frac{7}{3}$ und $x_1 = -\frac{1}{2} \cdot (1 + x_2 - 3 \cdot x_3) = -\frac{1}{2} \cdot (1 - \frac{7}{3} - 3 \cdot \frac{8}{9}) = -\frac{1}{2} \cdot (-4) = 2$

6.5 Quadratische Gleichungssysteme

Von besonderem Interesse und am häufigsten vorkommend sind die quadratischen Gleichungssysteme. **Ein Gleichungssystem heißt quadratisch, wenn die Anzahl seiner Unbekannten gleich der Anzahl seiner Gleichungen ist, d.h. n=m**

Das Bemerkenswerte an quadratischen Gleichungssystemen ist, dass die Beantwortung der beiden Fragen (Seite 78) zusammenfällt. Dieses findet Ausdruck in dem folgenden
Satz:
Ein quadratisches Gleichungssystem (wie (1) auf Seite 75 jedoch mit $n = m$) ist genau dann für jede rechte Seite $b_1, \ldots, b_n$ lösbar, wenn für den Rang $r = n$ gilt, dann ist die Lösung auch immer eindeutig bestimmt.

Eine hierzu gleichwertige Aussage wird uns bei der Polynominterpolation nützlich sein:
Satz:
Ein quadratisches Gleichungssystem ist genau dann für jede rechte Seite $b_1, \ldots, b_n$ lösbar, wenn sein zugehöriges homogenes System nur die Nulllösung besitzt.

Die Beweise dieser beiden Sätze ergeben sich ohne Rechenaufwand direkt aus den Sätzen dieses Abschnitts. Die Beweise werden als Übung empfohlen; man erhält sie auch unmittelbar aus dem zweiten Teil der folgenden Übersicht.

6.6 Übersicht zur Struktur der Lösungsmenge: Bedeutung von Rang und Corang

Wir betrachten ein **lineares Gleichungssystem mit m Gleichungen für n Unbekannte, $m \leq n$:**

1. Es ist $r \leq m = min(m, n)$.
2. $r = m < n \quad \Leftrightarrow$ Das Gleichungssystem ist für jede rechte Seite $\vec{b}$ lösbar.
3. $s = n - r > 0 \quad \Leftrightarrow$ Es gibt genau s verschiedene Grundlösungen des zugehörigen homogenen Gleichungssystems.
4. Für $n = m$, d. h. für ein quadratisches System gilt:

	Für jede rechte Seite $\vec{b}$ gibt es höchstens eine Lösung. (Eindeutigkeit)
$\Leftrightarrow$	Das homogene System besitzt nur die Lösung $\vec{x} = \vec{0}$.
$\Leftrightarrow$	Das Gleichungssystem ist für jede rechte Seite $\vec{b}$ lösbar.
$\Leftrightarrow$	$r = n \Leftrightarrow r = m \Leftrightarrow s = 0$

7 Vektoren und Vektorraum

7.1 Einführung

Lösungsmenge eines homogenen linearen Gleichungssystems:
Gegeben ist das homogene lineare Gleichungssystem

$$\underline{\underline{A}} \cdot \vec{x} = \vec{0}, \quad \vec{x} \in \mathbb{R}^n$$

mit Rang r und Corang $s = n - r > 0$. Fassen wir zusammen, was wir aus der Lösungstheorie wissen:

1. Die Lösungsmenge L^H enthält Objekte(Lösungen des homogenen linearen Gleichungssystems geschrieben als Spaltenvektoren des $\mathbb{R}^n$), für die zwei Rechenoperationen erklärt sind, nämlich:
   Die Addition (als Addition der Komponenten)

$$\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \Rightarrow \vec{u} + \vec{v} = \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{pmatrix}$$

   und die der Multiplikation mit einer reellen Zahl[3] (als Komponentenweise Multiplikation)

$$\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}, \quad t \in \mathbb{R} \Rightarrow t \cdot \vec{u} = \begin{pmatrix} tu_1 \\ tu_2 \\ \vdots \\ tu_n \end{pmatrix}$$

2. L^H ist abgeschlossen gegenüber diesen Rechenoperationen, d.h.

[3] In der Literatur findet man auch: Multiplikation mit einem Skalar oder skalare Multiplikation

$\vec{u}, \vec{v} \in L^H \Rightarrow \vec{u} + \vec{v} \in L^H$
$\vec{u} \in L^H, t \in \mathbb{R} \Rightarrow t \cdot \vec{u} \in L^H$

und damit auch:

$\vec{u}, \vec{v} \in L^H,\ t_1, t_2 \in \mathbb{R} \Rightarrow t_1 \cdot \vec{u} + t_2 \cdot \vec{v} \in L^H$

3. Für die beiden Rechenoperationen gelten folgende Gesetze(diese folgen aus den Rechengesetzen auf $\mathbb{R}$ auf Grund der komponentenweisen Definition der Rechenoperationen):

$\vec{u} + \vec{v} = \vec{v} + \vec{u}$ (Kommutativgesetz)

$(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$ (Assoziativgesetz)

$\vec{u} + \vec{0} = \vec{u}$ für $\vec{0} \in L^H$ ($\vec{0}$ als neutrales Element der Addition)

$\vec{u} \in L^H \Rightarrow$ es gibt $-\vec{u} = (-1) \cdot \vec{u} \in L^H$ mit $\vec{u} + (-\vec{u}) = \vec{u} - \vec{u} = \vec{0}$
($-\vec{u}$ als inverses Element der Addition)

$$\left.\begin{array}{c} t \cdot (\vec{u} + \vec{v})) = t \cdot \vec{u} + t \cdot \vec{v} \\ (t_1 + t_2) \cdot \vec{u} = t_1 \cdot \vec{u} + t_2 \cdot \vec{u} \end{array}\right\} \text{Distributivgesetz}$$

$t_1 \cdot (t_2 \cdot \vec{u}) = (t_1 \cdot t_2) \cdot \vec{u} = (t_2 \cdot t_1) \cdot \vec{u} = t_2 \cdot (t_1 \cdot \vec{u})$
$1 \cdot \vec{u} = \vec{u}$ für $1 \in \mathbb{R}$

Diese Struktureigenschaften liefern folgende

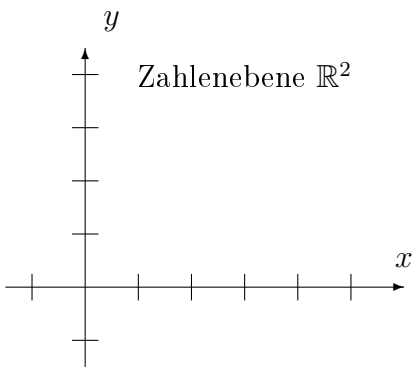
Definition: Eine Menge von Objekten, für die zwei Rechenoperationen (Addition und Multiplikation mit einer reellen Zahl) mit den Eigenschaften 2 und 3 definiert sind, nennt man **Vektorraum**. Die Elemente dieser Menge (also die Objekte) heißen **Vektoren**.

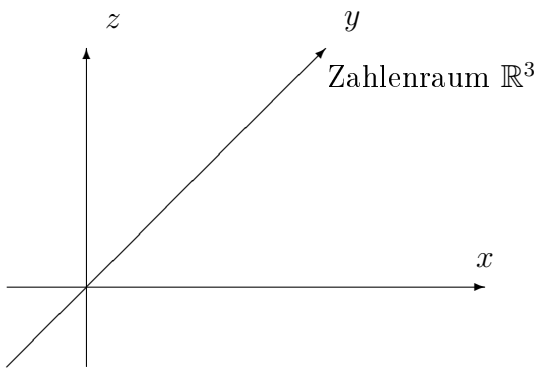
Mit dieser (abstrakten) Definition können wir also sagen:
L^H ist ein Vektorraum, jede Lösung des homogenen linearen Gleichungssystems ist ein Vektor dieses Vektorraums.

Wir werden jetzt im $\mathbb{R}^2$ und $\mathbb{R}^3$ eine anschauliche Herleitung und Deutung des Vektorbegriffs geben.

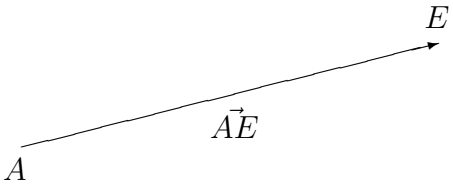
7.2 $\mathbb{R}^2$ und $\mathbb{R}^3$ als Punktmenge und Vektorraum

Die Zahlebene, $\mathbb{R}^2$, und der Zahlenraum, $\mathbb{R}^3$, werden mittels Kartesischer Koordinaten als Menge von Punkten beschrieben:





Zwei Punkte [4] $A(a_1|a_2|a_3)$ und $E(e_1|e_2|e_3)$ bestimmen einen Pfeil $\vec{AE}$ (gerichtete Strecke) vom Anfangspunkt A zum Endpunkt E.



Zwei Pfeile $\vec{AE}$ und $\vec{A'E'}$ sind äquivalent, wenn gilt:

$$e_1 - a_1 = e'_1 - a'_1$$

$$e_2 - a_2 = e'_2 - a'_2$$

$$e_3 - a_3 = e'_3 - a'_3$$

Was messen diese einzelnen Größen?

- $e_1 - a_1 = e'_1 - a'_1$ misst die Distanz, die man in x-Richtung zurücklegen muss, um von A nach E bzw. von A' nach E' zu gelangen.
- $e_2 - a_2 = e'_2 - a'_2$ misst die Distanz, die man in y-Richtung zurücklegen muss, um von A nach E bzw. von A' nach E' zu gelangen.
- $e_3 - a_3 = e'_3 - a'_3$ misst die Distanz, die man in z-Richtung zurücklegen muss, um von A nach E bzw. von A' nach E' zu gelangen.

Diese drei Zahlenwerte kann man also als relative Koordinaten des jeweiligen Endpunkts bezogen auf den Anfangspunkt verstehen. Zwei Pfeile sind also äquivalent, wenn die drei relativen Koordinaten übereinstimmen, d.h. wenn dieselbe Information ausreicht um von Anfangspunkt zum Endpunkt zu gelangen unabhängig von der expliziten Position der Punkte!
Zwei äquivalente Pfeile lassen sich geometrisch durch eine Parallelverschiebung ineinander überführen!

Die Menge alles Pfeile, die zu einem gegebenen Pfeil $\vec{AE}$ äquivalent sind, bezeichnet

[4] Im $\mathbb{R}^2$ gilt das analog; man hat jedoch nur zwei Komponenten

man als **Äquivalenzklasse von** $\vec{AE}$:

$$[\vec{AE}] = \{\vec{A'E'} | \vec{A'E'} \text{ ist äquivalent zu } \vec{AE}\}$$

Für alle Pfeile $\vec{A'E'}$ aus $[\vec{AE}]$ gilt also:

$$\left.\begin{array}{l} v_1 = e'_1 - a'_1 = e_1 - a_1 \\ v_2 = e'_2 - a'_2 = e_2 - a_2 \\ v_3 = e'_3 - a'_3 = e_3 - a_3 \end{array}\right\} v_1, v_2, v_3 \text{ sind also die relativen Koordinaten, die für jeden der äquivalenten Pfeile angeben, wie man vom Anfangs- zum Endpunkt gelangt.}$$

Dies führt zu folgender

Definition:

$\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$ mit $v_i \in \mathbb{R}$ $(1 \leq i \leq 3)$ heißt Vektor; er repräsentiert die **Äquivalenzklasse von Pfeilen** $[\vec{AE}]$, falls gilt:

$$v_1 = e_1 - a_1, \quad v_2 = e_2 - a_2, \quad v_3 = e_3 - a_3$$

Die Zahlen

$$v_1, \quad v_2, \text{ und } v_3$$

nennt man die (kartesischen) Komponenten oder Koordinaten des Vektors $\vec{v}$.

Man bezeichnet mit $0(0|0|0)$ den Koordinatenursprung des Kartesischen Koordinatensystems.
Jeden Punkt $P(x_p|y_p|z_p)$ im $\mathbb{R}^3$ kann man auffassen als Endpunkt des Pfeils $\vec{0P}$.
Die Äquivalenzklasse $[\vec{0P}]$ wird dann repräsentiert durch den Vektor $\vec{p} = \begin{pmatrix} x_p \\ y_p \\ z_p \end{pmatrix}$.
Jedem Punkt $P(x_p|y_p|z_p)$ im $\mathbb{R}^3$ entspricht also der Vektor $\vec{p} = \begin{pmatrix} x_p \\ y_p \\ z_p \end{pmatrix}$[5], und umgekehrt kann man jedem Vektor $\vec{p}$ dem Punkt $P(x_p|y_p|z_P)$ zuordnen.
Die Punktmenge $\mathbb{R}^3$ entspricht somit also eindeutig der Menge der Vektoren $\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$, $v_i \in \mathbb{R}$ $(1 \leq i \leq 3)$!

Ob wir $\mathbb{R}^3$ als Punktmenge oder als Menge von Vektoren auffassen ist also gleichwertig.
Fasst man $\mathbb{R}^3$ als Menge von Vektoren auf, kann man folgende Rechenoperationen für Vektoren definieren:

[5] Man nennt diesen Vektor $\vec{p}$ den Ortsvektor zum Punkt P

1. Addition (Komponentenweise Addition)

$$\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, \quad \vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \Rightarrow \vec{v} + \vec{u} = \begin{pmatrix} v_1 + u_1 \\ v_2 + u_2 \\ v_3 + u_3 \end{pmatrix}$$

2. Multiplikation mit einer reellen Zahl (Komponentenweise)

$$\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \Rightarrow \lambda \cdot \vec{v} = \begin{pmatrix} \lambda v_1 \\ \lambda v_2 \\ \lambda v_3 \end{pmatrix} \quad \text{für} \quad \lambda \in \mathbb{R}$$

Da die Rechenoperationen komponentenweise definiert sind und in jeder Komponente „ganz normal“ mit reellen Zahlen gerechnet wird, „erben“ die beiden Rechenoperationen für Vektoren folgende Rechenregeln von den Rechenregeln für reelle Zahlen:

Rechenregeln für Vektoren

$\vec{u} + \vec{v} = \vec{v} + \vec{u}$

$(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$

Es gibt $\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ mit $\vec{u} + \vec{0} = \vec{u}$

Zu $\vec{u}$ gibt es $-\vec{u}$ mit $\vec{u} + (-\vec{u}) = \vec{u} - \vec{u} = \vec{0}$

$\lambda \cdot (\vec{u} + \vec{v}) = \lambda \cdot \vec{u} + \lambda \cdot \vec{v}$

$(\lambda_1 + \lambda_2) \cdot \vec{u} = \lambda_1 \cdot \vec{u} + \lambda_2 \cdot \vec{u})$

$\lambda_1 \cdot (\lambda_2 \cdot \vec{u}) = (\lambda_1 \cdot \lambda_2) \cdot \vec{u} = (\lambda_2 \cdot \lambda_1 \cdot \vec{u}) = \lambda_2 \cdot (\lambda_1 \cdot \vec{u})$

$1 \cdot \vec{u} = \vec{u} (\Rightarrow -\vec{u} = (-1) \cdot \vec{u})$

Beispiele:

1) Addition von Vektoren im $\mathbb{R}^3$

$$\vec{a} = \begin{pmatrix} -2 \\ 3 \\ 4 \end{pmatrix}, \quad \vec{b} = \begin{pmatrix} 5 \\ -1 \\ 2 \end{pmatrix}$$

$$\Rightarrow \vec{a} + \vec{b} = \begin{pmatrix} (-2) + 5 \\ 3 + (-1) \\ 4 + 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 6 \end{pmatrix}$$

Es wird also komponentenweise addiert,d.h. in jeder der drei Vektorkomponenten wird die ganz normale Addition in $\mathbb{R}$ ausgeführt

2) Multiplikation mit einer reellen Zahl bei Vektoren im $\mathbb{R}^3$

$$\vec{a} = \begin{pmatrix} \frac{3}{5} \\ -3 \\ \sqrt{3} \end{pmatrix}, \ 5 \in \mathbb{R}$$

$$\Rightarrow \ 5 \cdot \vec{a} = 5 \cdot \begin{pmatrix} \frac{3}{5} \\ -3 \\ \sqrt{3} \end{pmatrix} = \begin{pmatrix} 5 \cdot \frac{3}{5} \\ 5 \cdot (-3) \\ 5 \cdot \sqrt{3} \end{pmatrix} = \begin{pmatrix} 3 \\ -15 \\ 5 \cdot \sqrt{3} \end{pmatrix}$$

Es wird also komponentenweise multipliziert,d.h. in jeder der drei Vektorkomponenten wird die ganz normale Multiplikation in $\mathbb{R}$ ausgeführt

3) Rechnen mit Vektoren im $\mathbb{R}^3$: Auflösen (linearer) Gleichungen mit Vektoren

Gegeben sind die Vektoren $\vec{a} = \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix}$ und $\vec{b} = \begin{pmatrix} \frac{3}{2} \\ \frac{3}{4} \\ -\frac{3}{8} \end{pmatrix}$, gesucht ist der Vektor $\vec{x}$ mit

$2 \cdot \vec{a} + 3 \cdot \vec{x} = 4 \cdot \vec{b}$

Zunächst rechnet man „abstrakt“ wie im Fall einer (reellen) Gleichung mit Variablen a, b, x:

$2 \cdot \vec{a} + 3 \cdot \vec{x} = 4 \cdot \vec{b}$

$\Rightarrow 3 \cdot \vec{x} = 4 \cdot \vec{b} - 2 \cdot \vec{a}$

$\Rightarrow \vec{x} = \frac{4}{3} \cdot \vec{b} - \frac{2}{3} \cdot \vec{a}$

Erst jetzt rechnet man mit den konkret gegebenen Vektoren, also:

$$\Rightarrow \vec{x} = \frac{4}{3} \cdot \begin{pmatrix} \frac{3}{2} \\ \frac{3}{4} \\ -\frac{3}{8} \end{pmatrix} - \frac{2}{3} \cdot \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} \Rightarrow \vec{x} = \begin{pmatrix} 2 \\ 1 \\ -\frac{1}{2} \end{pmatrix} - \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 2-2 \\ 1-4 \\ -\frac{1}{2}-6 \end{pmatrix}$$

$$\Rightarrow \vec{x} = \begin{pmatrix} 0 \\ -3 \\ -\frac{13}{2} \end{pmatrix}$$

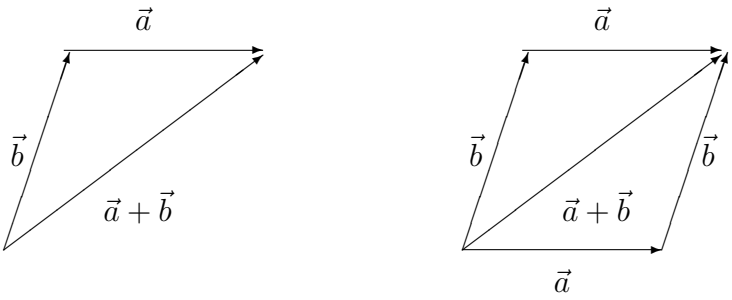
Die dargestellten Rechenregeln für Vektoren im $\mathbb{R}^3$ sind genau die Rechenregeln, die für Spaltenvektoren des $\mathbb{R}^n$ in der Lösungsmenge L^H einer homogenen linearen Gleichungssystems gelten.
Damit ist der $\mathbb{R}^3$ aufgefasst als Menge von Vektoren mit den eben definierten Rechenoperationen ein Vektorraum. Neben L^H ist dies ein zweites (auf Grund der Verbindung zu den Pfeilen $\vec{AE}$) anschauliches Beispiel für einen Vektorraum.

7.3 Anschauliche Deutung der Rechenoperationen im Vektorraum $\mathbb{R}^2$ und $\mathbb{R}^3$

1. Addition
   Zu $\vec{u}$ gehört der Pfeil $\vec{AE}$, zu $\vec{v}$ der Pfeil $\vec{A'E'}$.
   Dann gehört zu $\vec{u}+\vec{v}$ der Pfeil, der durch "Hintereinanderhängen" der beiden Pfeile $\vec{AE}$ und $\vec{A'E'}$ entsteht, genauer:
   Man hängt $\vec{A'E'}$ so an $\vec{AE}$, dass E und A' zusammenfallen, dann ist $\vec{AE'}$ der zu $\vec{u}+\vec{v}$ zugehöriger Pfeil.

   Im folgenden wird die **Regel** zur Bildung der **Summe zweier Vektoren** $\vec{a}$ und $\vec{b}$ nochmals erläutert und grafisch dargestellt:

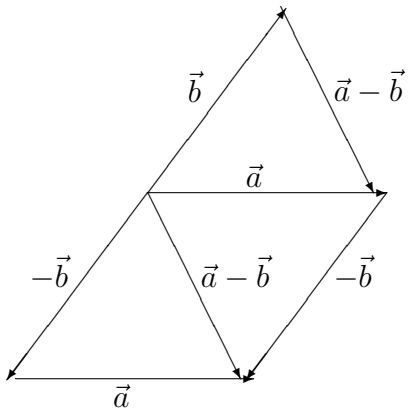
Regel: Man trage den Anfangspunkt des Vektors $\vec{a}$ an den Endpunkt des Vektors $\vec{b}$ an. Der Vektor $\vec{a}+\vec{b}$ verläuft dann vom Anfangspunkt von $\vec{b}$ bis zum Endpunkt von $\vec{a}$.
Trägt man beide Vektoren zweimal ein, einmal mit gemeinsamem Anfangspunkt und einmal so, dass der Anfangspunkt des einen mit dem Endpunkt des anderen zusammenfällt, so ist $\vec{a}+\vec{b}$ gerade die Diagonale des entstehenden Parallelogrammes.



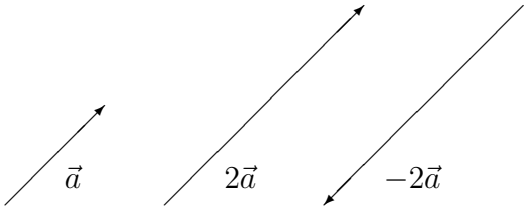
Die **Subtraktion zweier Vektoren** erfolgt dadurch, dass zu dem einen das Negative des anderen addiert wird:

$$\vec{a} - \vec{b} = \vec{a} + (-\vec{b})$$

Anschaulich erhält man den Differenzvektor $\vec{a}-\vec{b}$ als Pfeil, der vom Endpunkt des Subtrahenden $\vec{b}$ bis zum Endpunkt des Minuenden $\vec{a}$ verläuft. Man erhält natürlich $\vec{a}-\vec{b}$ auch als Diagonale des aus $\vec{a}$ und $\vec{b}$ gebildeten Parallelogrammes.



2. Multiplikation mit einer reellen Zahl
Zu $\vec{u}$ gehört der Pfeil $\vec{AE}$. Dann gehört zu $\lambda \cdot \vec{u}$ der um den Faktor $|\lambda|$ verkürzte bzw. verlängerte Pfeil.
Ist $\lambda > 0$ behält der Pfeil seine ursprüngliche Richtung,
ist $\lambda < 0$ wird die Pfeilrichtung umgedreht.

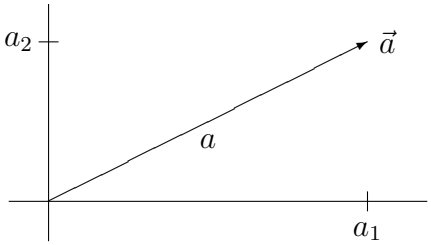


7.4 Weitere grundlegende Definitionen

Definition:
Der **Betrag** eines Vektors $\vec{a}$ ist die Länge des zugehörigen Pfeils, man schreibt dafür $||\vec{a}||$ oder auch $|\vec{a}|$.
Der Betrag eines Vektors ist immer eine nicht negative reelle Zahl:

$$||\vec{a}|| \in [0, \infty)$$

Es bleibt noch zu erwähnen, wie sich der Betrag eines Vektors aus dessen Komponenten errechnet. Man verwendet dazu den Satz des Pythagoras:



$$||\vec{a}|| = a = \sqrt{a_1^2 + a_2^2}$$

Ebenso hat man im Raum:

$$||\vec{a}|| = ||(a_1, a_2, a_3)^t|| = a = \sqrt{a_1^2 + a_2^2 + a_3^2}$$

Definition:
Der Nullvektor ist derjenige Vektor, bei dem Anfangs- und Endpunkt zusammenfallen:

$$\vec{0} = \vec{PP}$$

und in Koordinaten $\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$
Für einen Vektor $\vec{v}$ aus dem $\mathbb{R}^n$ mit den Komponenten/Koordinaten

$$\vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

gilt analog:

$$||\vec{v}|| = ||(v_1, v_2, \ldots, v_n)^t|| = a = \sqrt{v_1^2 + v_2^2 + v_3^2 + \ldots + v_n^2}$$

Bemerkung: Ein Vektor ist genau dann der Nullvektor, wenn er den Betrag Null besitzt:

$$||\vec{x}|| = 0 \quad \Leftrightarrow \quad \vec{x} = \vec{0}$$

Definition:
Ein Vektor der Länge 1 heißt **Einheitsvektor**:

$$||\vec{e}|| = 1 \quad \Leftrightarrow \quad \vec{e} \text{ ist Einheitsvektor.}$$

Einen Einheitsvektor verwendet man insbesondere dann, wenn es nur auf die Richtung und den Richtungssinn eines Vektors ankommt und dessen Länge unerheblich ist.

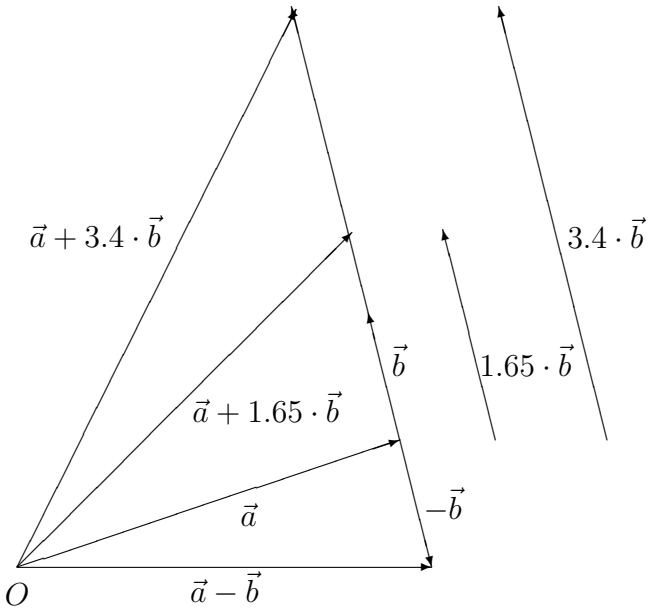
Die Vektoraddition liefert zusammen mit der skalaren Multiplikation eine sehr gute Möglichkeit zur Darstellung einer Geraden:
Man gibt einen Ortsvektor $\vec{a}$ und einen von Null verschiedenen Vektor $\vec{b}$ vor und bildet mit dem Parameter $t \in \mathbb{R}$ die Ortsvektoren

$$\vec{a} + t \cdot \vec{b}$$

Durchläuft der Parameter t die reellen Zahlen, so bilden die Endpunkte der Ortsvektoren $\vec{a} + t \cdot \vec{b}$ eine Gerade. Man schreibt für die Gerade

$$\mathcal{G} = \left\{ \vec{a} + t \cdot \vec{b} \mid t \in \mathbb{R} \right\} \tag{12}$$

Den Vektor $\vec{a}$ nennt man **Aufpunktvektor** und den Vektor $\vec{b}$ nennt man **Richtungsvektor** der Geraden. In der folgenden Zeichnung sind die Vektoren $\vec{a}+t\cdot\vec{b}$ für $t = 1.65,\ 3.4,\ -1$ eingezeichnet; man erkennt, dass die Endpunkte dieser Vektoren auf einer Geraden liegen.

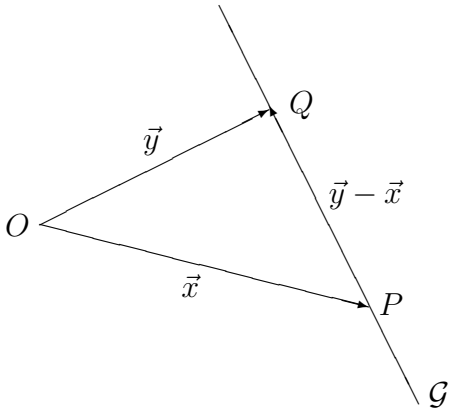


Durch zwei Punkte verläuft bekanntlich genau eine Gerade. Mit Hilfe der Vektorsubtraktion lässt sich zu zwei gegebenen Punkten P und Q sehr leicht diese Gerade konstruieren. Man stellt die Gerade in der Form (12) dar: Zunächst bildet man die zu den beiden Punkten gehörigen Ortsvektoren:

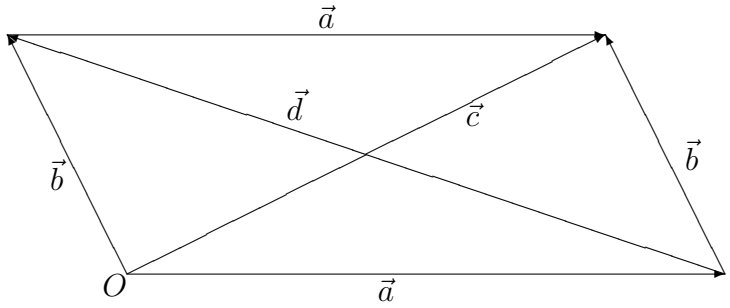
$$\vec{x} = \vec{OP} \qquad \text{und} \qquad \vec{y} = \vec{OQ}$$

Man wählt den einen dieser beiden Vektoren als Ortsvektor der Geraden und die Differenz der beiden Vektoren als Richtungsvektor der Geraden. Eine Darstellung der Geraden durch P und Q lautet damit

$$\mathcal{G} = \{\vec{x} + t \cdot (\vec{y} - \vec{x}) \mid t \in \mathbb{R}\} \tag{13}$$



Als Beispiel für eine Anwendung der Vektoraddition soll bewiesen werden, dass sich die Diagonalen eines Parallelogrammes halbieren.



Aus der Zeichnung erkennt man

$$\vec{c} = \vec{a} + \vec{b}, \qquad \vec{b} = \vec{a} + \vec{d}$$

Damit folgt:

$$\begin{aligned} & \text{Mittelpunkt der ersten Diagonalen} \\ = \quad & \frac{1}{2} \cdot \vec{c} = \frac{1}{2} \cdot \vec{a} + \frac{1}{2} \cdot \vec{b} \qquad (\text{hier } \vec{b} = \vec{a} + \vec{d} \text{ einsetzen}) \\ = \quad & \frac{1}{2} \cdot \vec{a} + \frac{1}{2}(\vec{a} + \vec{d}) \\ = \quad & \vec{a} + \frac{1}{2} \cdot \vec{d} \\ = \quad & \text{Mittelpunkt der zweiten Diagonalen} \end{aligned}$$

Fragen:

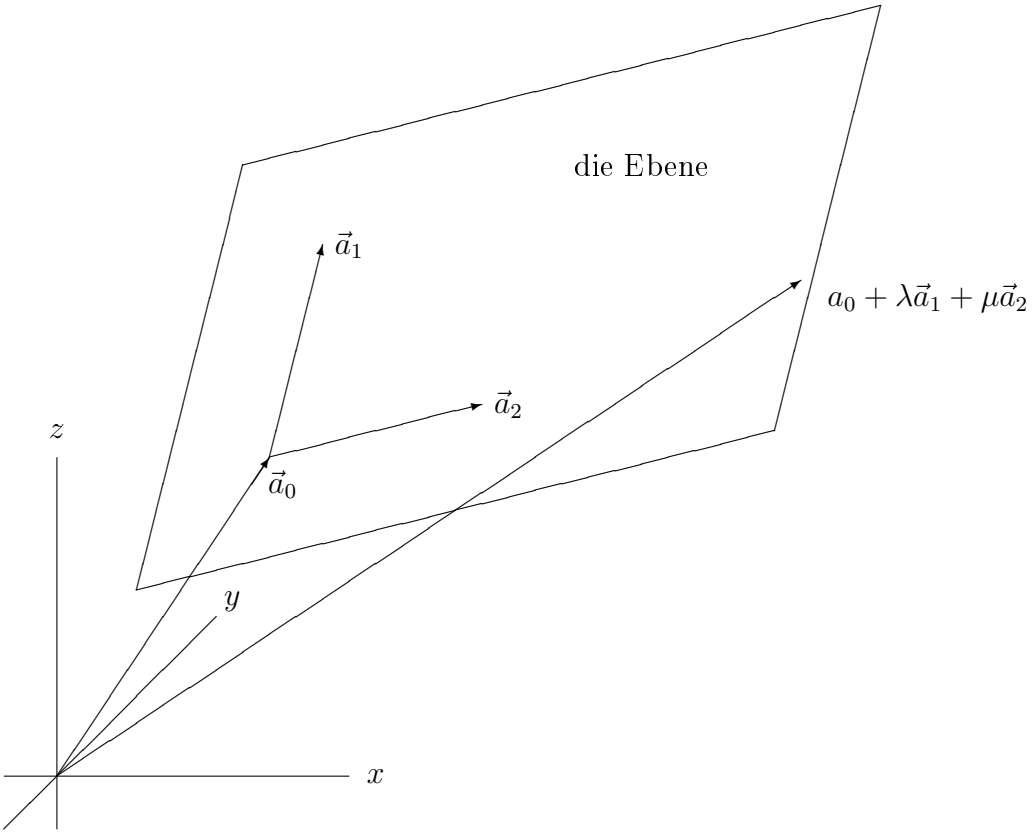
1. Man überlege sich anhand eines Beispiels, dass eine Gerade mehrere Darstellungen der Form (12) besitzt.
2. Warum muss bei der Geradendarstellung (12) vorausgesetzt werden, dass der Richtungsvektor nicht der Nullvektor ist.

7.5 Ebenen im Raum

Die Darstellung einer Ebene erfolgt ähnlich wie die Darstellung einer Geraden (siehe Seite 105); man benötigt nur einen zweiten Richtungsvektor, wobei die beiden Richtungsvektoren linear unabhängig sein müssen[6]:

$$\mathcal{E} = \{\vec{a}_0 + \lambda \cdot \vec{a}_1 + \mu \cdot \vec{a}_2 \mid \lambda, \mu \in \mathbb{R}\} \subset \mathbb{R}^3 \tag{14}$$

[6] siehe Kap. 7.9



Auf diese Weise seien jetzt zwei Ebenen gegeben:

$$\begin{aligned}\mathcal{E}_1 &= \{\vec{a}_0 + \lambda \cdot \vec{a}_1 + \mu \cdot \vec{a}_2 \mid \lambda, \mu \in \mathbb{R}\} \\ \mathcal{E}_2 &= \left\{\vec{b}_0 + l \cdot \vec{b}_1 + m \cdot \vec{b}_2 \mid l, m \in \mathbb{R}\right\}\end{aligned}$$

Der Durchschnitt $\mathcal{E}_1 \cap \mathcal{E}_2$ der beiden Ebenen soll untersucht werden: Liegt der Vektor $\vec{x}$ im Durchschnitt ($\vec{x} \in \mathcal{E}_1 \cap \mathcal{E}_2$), so lässt er sich gleichzeitig sowohl durch die definierenden Vektoren der einen als auch durch die der anderen Ebene darstellen. Es gibt daher Parameterwerte $\lambda, \mu, l, m \in \mathbb{R}$ mit

$$\vec{x} = \vec{a}_0 + \lambda \cdot \vec{a}_1 + \mu \cdot \vec{a}_2 = \vec{b}_0 + l \cdot \vec{b}_1 + m \cdot \vec{b}_2 \tag{15}$$

Da die Punkte im Durchschnitt $\mathcal{E}_1 \cap \mathcal{E}_2$ durch die in der Darstellung (15) vorkommenden Parameterwerte eindeutig bestimmt sind, reicht es, zur Beschreibung von $\mathcal{E}_1 \cap \mathcal{E}_2$ die Menge aller Kombinationen von Parameterwerten $\lambda, \mu, l, m \in \mathbb{R}$ zu beschreiben, die zu einer Darstellung der Art (15) gehören.
Nun stellt aber (15) ein Gleichungssystem der zu $\vec{x} \in \mathcal{E}_1 \cap \mathcal{E}_2$ gehörigen Parameterwerte dar. Formt man (15) so um, dass auf der rechten Seite nur die konstanten Summanden stehen, und setzt man die Komponenten der vorkommenden Vektoren ein, so lautet das Gleichungssystem

$$\begin{array}{rcrcrcrcl} \lambda \cdot a_{11} & + & \mu \cdot a_{12} & - & l \cdot b_{11} & - & m \cdot b_{12} & = & -a_{10} + b_{10} \\ \lambda \cdot a_{21} & + & \mu \cdot a_{22} & - & l \cdot b_{21} & - & m \cdot b_{22} & = & -a_{20} + b_{20} \\ \lambda \cdot a_{31} & + & \mu \cdot a_{32} & - & l \cdot b_{31} & - & m \cdot b_{32} & = & -a_{30} + b_{30} \end{array} \tag{16}$$

In Matrizenschreibweise lautet dieses Gleichungssystem:

$$\begin{pmatrix} a_{11} & a_{12} & -b_{11} & -b_{12} \\ a_{21} & a_{22} & -b_{21} & -b_{22} \\ a_{31} & a_{32} & -b_{31} & -b_{32} \end{pmatrix} \cdot \begin{pmatrix} \lambda \\ \mu \\ l \\ m \end{pmatrix} = \begin{pmatrix} -a_{10} + b_{10} \\ -a_{20} + b_{20} \\ -a_{30} + b_{30} \end{pmatrix} \tag{17}$$

Um $\mathcal{E}_1 \cap \mathcal{E}_2$ zu beschreiben, muss nun die Lösungsmenge des Gleichungssystems (17) untersucht werden. Die Lösungsmenge hängt vom Rang des Gleichungssystems ab; für den Rang von (17) gilt

$$\begin{aligned} \text{Rang} &\leq 3 = \text{Anzahl der Gleichungen} \\ \Rightarrow \quad \text{Corang} &= \text{Anzahl der Unbestimmten} - \text{Rang} \geq 4 - 3 = 1 \end{aligned}$$

Als erstes Ergebnis erhält man damit: Die Lösungsmenge des Gleichungssystems (17) besteht niemals nur aus einem Element. Angewandt auf $\mathcal{E}_1 \cap \mathcal{E}_2$ bedeutet dieses: zwei Ebenen im Raum schneiden sich niemals genau in einem Punkt.
Betrachtet man die möglichen Werte für den Rang im einzelnen, so erhält man:

1. Rang = 3: In diesem Fall ist der Rang gleich der Anzahl der Gleichungen, es gibt daher keine Nullgleichungen, und das Gleichungssystem ist sicher lösbar. Da der Corang gleich 1 ist, ist die Lösungsmenge durch eine spezielle Lösung $(\lambda_0, \mu_0, l_0, m_0)$ und durch eine Grundlösung $(\lambda_1, \mu_1, l_1, m_1)$ des zugehörigen homogenen Systems gegeben:

   $$\begin{pmatrix} \lambda_0 + t \cdot \lambda_1 \\ \mu_0 + t \cdot \mu_1 \\ l_0 + t \cdot l_1 \\ m_0 + t \cdot m_1 \end{pmatrix} \quad \text{mit} \quad t \in \mathbb{R} \tag{18}$$

   Welche Gestalt von $\mathcal{E}_1 \cap \mathcal{E}_2$ folgt hieraus? Da eine Grundlösung eines homogenen Systems nicht Null ist, muss mindestens eine der Zahlen $\lambda_1, \mu_1, l_1, m_1$ ungleich Null sein. Sei etwa $\lambda_1 \neq 0$ oder $\mu_1 \neq 0$, dann setzt man (18) in die Darstellung der Ebene $\mathcal{E}_1$ ein[7]:

   $$\begin{aligned} \vec{x} &= \vec{a}_0 + (\lambda_0 + t \cdot \lambda_1)\vec{a}_1 + (\mu_0 + t \cdot \mu_1)\vec{a}_2 \\ &= (\vec{a}_0 + \lambda_0\vec{a}_1 + \mu_0\vec{a}_2) + t \cdot (\lambda_1\vec{a}_1 + \mu_1\vec{a}_2) \\ &\quad \text{für alle} \quad t \in \mathbb{R} \end{aligned}$$

   Dieses ist die Darstellung einer Geraden. In diesem Fall handelt es sich bei $\mathcal{E}_1 \cap \mathcal{E}_2$ somit um eine Gerade. Zu beachten ist noch, dass die Gerade einen von Null verschiedenen Richtungsvektor $\lambda_1\vec{a}_1 + \mu_1\vec{a}_2$ besitzt; dieses liegt an der linearen Unabhängigkeit von $\vec{a}_1$ und $\vec{a}_2$.

2. Rang = 2: In diesem Fall besitzt das Gleichungssystem (17) nach Reduzierung eine Nullgleichung; abhängend von deren rechter Seite ergeben sich zwei Möglichkeiten:

[7] Andernfalls würde man (18) in die Darstellung der Ebene $\mathcal{E}_2$ einsetzen.

(a) Das Gleichungssystem ist unlösbar und damit $\mathcal{E}_1 \cap \mathcal{E}_2 = \emptyset$. Man kann zeigen, dass dieses genau dann der Fall ist, wenn die beiden Ebenen parallel aber nicht gleich sind.

(b) Das Gleichungssystem ist mit $2 = (4 - \text{Rang})$ Grundlösungen lösbar. In diesem Fall ist $\mathcal{E}_1 \cap \mathcal{E}_2$ eine Ebene und es gilt

$$\mathcal{E}_1 \cap \mathcal{E}_2 \;=\; \mathcal{E}_1 \;=\; \mathcal{E}_2$$

3. Rang $\leq$ 1: Man kann zeigen, dass dieser Fall nicht vorkommt. Die Annahme Rang $\leq$ 1 führt zu einem Widerspruch zur linearen Unabhängigkeit der beiden Richtungsvektoren $\vec{a}_1$ und $\vec{a}_2$ bzw. der beiden Richtungsvektoren $\vec{b}_1$ und $\vec{b}_2$

Bemerkung: Das hier vorgestellte Verfahren zur Beschreibung des Durchschnitts zweier Ebenen ist effektiv: mit ihm lässt sich der Durchschnitt zweier gegebener Ebenen konkret berechnen.

Aufgabe: Man führe eine entsprechende Überlegung zur Untersuchung des Durchschnitts zweier Geraden $\mathcal{G}_1 \cap \mathcal{G}_2$ durch. Man verwende für $\vec{x} \in \mathcal{G}_1 \cap \mathcal{G}_2$ die Darstellung durch die beiden Geradengleichungen:

$$\vec{x} \;=\; \vec{a}_0 + \lambda \cdot \vec{a}_1 \;=\; \vec{b}_0 + l \cdot \vec{b}_1$$

und leite daraus ein Gleichungssystem für die möglichen Parameterwerte ab. Dieses Gleichungssystem besitzt den Rang eins oder zwei; es besteht aus zwei oder drei Gleichungen, je nach dem ob es sich um ebene oder räumliche Geraden handelt.

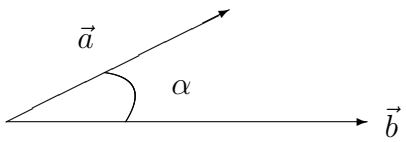
7.6 Das Skalarprodukt

Das Skalarprodukt ist eine Rechenvorschrift, durch die zwei Vektoren ein Skalar, d. h. eine reelle Zahl zugeordnet wird.

Definition: (Skalarprodukt im $\mathbb{R}^2$ und im $\mathbb{R}^3$):
Für zwei Vektoren $\vec{a}$ und $\vec{b}$ heißt

$$\vec{a} \cdot \vec{b} \;=\; ||\vec{a}|| \cdot ||\vec{b}|| \cdot \cos\alpha \tag{19}$$

das **Skalarprodukt** von $\vec{a}$ und $\vec{b}$. Dabei ist α der Winkel zwischen den beiden Vektoren $\vec{a}$ und $\vec{b}$:



Eine **andere Schreibweise** für das Skalarprodukt lautet: $(\vec{a}, \vec{b})$ oder $< \vec{a}, \vec{b} >$

Frage: Warum ist es für den Wert des Skalarproduktes unerheblich, ob der größere oder der kleinere Winkel zwischen den beiden Vektoren verwendet wird?
Bemerkung: Man beachte, dass der Wert des Ausdruckes (19) eine reelle Zahl, d. h. ein Skalar, ist.
Bemerkung: Ist einer der beiden Faktoren des Skalarproduktes der Nullvektor, so ist der Wert des Skalarproduktes Null. Anders als bei dem Produkt reeller Zahlen ist es beim Skalarprodukt jedoch möglich, dass sein Wert Null ist und trotzdem keiner seiner beiden Faktoren gleich dem Nullvektor ist (Beispiel?).

Bemerkung: Mit Hilfe des Skalarproduktes kann nachgerechnet werden,**ob zwei von Null verschiedene Vektoren $\vec{x}$ und $\vec{y}$ aufeinander senkrecht stehen**; es gilt nämlich (α ist der Winkel zwischen $\vec{x}$ und $\vec{y}$):

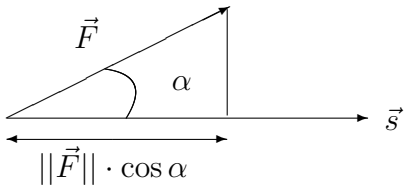
$$\begin{aligned} \vec{x} \perp \vec{y} &\Leftrightarrow \vec{x} \cdot \vec{y} = 0 \\ &\Leftrightarrow \cos\alpha = 0 \\ &\Leftrightarrow \alpha = \frac{1}{2}\pi, \frac{3}{2}\pi \end{aligned} \tag{20}$$

Für den Nullvektor $\vec{0}$ und einen beliebigen Vektors $\vec{x}$ liefert das Skalarprodukt den Wert

$$\vec{0} \cdot \vec{x} = 0$$

Hieraus folgt: Der Nullvektor steht auf jedem beliebigen Vektor senkrecht.

Man stößt auf das Skalarprodukt, wenn man berechnet, welche Arbeit bei Fortbewegung eines Massenpunktes längs eines gerichteten Streckenstückes $\vec{s}$ durch eine Kraft $\vec{F}$ geleistet wird. Ausschlaggebend für die geleistete Arbeit sind die Länge des Streckenstückes $||\vec{s}||$ sowie die Länge des Kraftanteils in Richtung von $\vec{s}$; ist α der Winkel zwischen $\vec{s}$ und $\vec{F}$, so beträgt diese Länge $||\vec{F}|| \cdot \cos\alpha$:



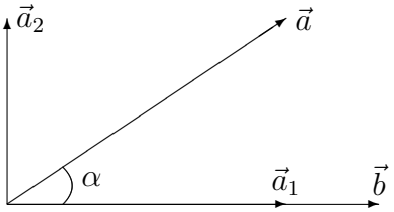
die geleistete Arbeit:
$W = ||\vec{s}|| \cdot ||\vec{F}|| \cdot \cos\alpha$

Dieser von den beiden Vektoren $\vec{s}$ und $\vec{F}$ abhängende Ausdruck ist nicht nur bei der Berechnung der geleisteten Arbeit von Bedeutung.

Das letzte Beispiel enthält unausgesprochen die Zerlegung der Kraft $\vec{F}$ in einen Anteil in Richtung des gerichteten Streckenstücks $\vec{s}$ und in Richtung eines auf diesem Vektor

senkrecht stehenden Vektors. Es soll nun hergeleitet werden, wie sich dieser **senkrechte Anteil** eines Vektors mit Hilfe des Skalarproduktes berechnen lässt. Zunächst muss aber geklärt werden, was genau darunter zu verstehen ist:
Gegeben seinen zwei vom Nullvektor verschiedene Vektoren $\vec{a}$ und $\vec{b}$. Gesucht ist eine Zerlegung des Vektors $\vec{a}$ in zwei Summanden:

$$\vec{a} = \vec{a}_1 + \vec{a}_2 \tag{21}$$



für die gelten soll:

$\vec{a}_1$: ein zu $\vec{b}$ paralleler und gleichgerichteter Vektor; man nennt $\vec{a}_1$ den Anteil von $\vec{a}$ in Richtung von $\vec{b}$ oder auch die **Projektion** von $\vec{a}$ auf $\vec{b}$

$\vec{a}_2$: ein zu $\vec{b}$ senkrechter Vektor; man nennt $\vec{a}_2$ den zu $\vec{b}$ senkrechten Anteil von $\vec{a}$

Der Anteil $\vec{a}_1$ ist leicht zu berechnen; die Zeichnung liefert den Ansatz

$$\text{Betrag} : ||\vec{a}|| \cdot \cos\alpha$$

$$\text{Richtung} : \frac{\vec{b}}{||\vec{b}||} \quad \text{ein Einheitsvektor in Richtung von } \vec{b}$$

Verwendet man dieses, so erhält man für $\vec{a}_1$:

$$\begin{aligned}
\vec{a}_1 &= (||\vec{a}|| \cdot \cos\alpha) \cdot \frac{\vec{b}}{||\vec{b}||} \\
&= (||\vec{a}|| \cdot ||\vec{b}|| \cdot \cos\alpha) \cdot \frac{\vec{b}}{||\vec{b}||^2} \qquad \text{(erweitert mit } ||\vec{b}||) \\
&= \frac{(\vec{a} \cdot \vec{b}) \cdot \vec{b}}{||\vec{b}||^2}
\end{aligned}$$

Der Nenner dieses Ausdrucks soll ebenso wie der Zähler durch das Skalarprodukt ausgedrückt werden. Beachtet man, dass der Vektor $\vec{b}$ mit sich selber den Winkel 0 Grad bildet, so liefert eine kleine Nebenrechnung

$$||\vec{b}||^2 = ||\vec{b}|| \cdot ||\vec{b}|| \cdot \cos 0 = \vec{b} \cdot \vec{b} \tag{22}$$

Dieses oben eingesetzt liefert die wichtige Formel für den Anteil von $\vec{a}$ in Richtung $\vec{b}$

$$\vec{a}_1 = \frac{(\vec{a} \cdot \vec{b})}{(\vec{b} \cdot \vec{b})} \cdot \vec{b} \tag{23}$$

Man beachte, dass in (23) die Punkte für unterschiedliche Multiplikationen stehen: die in Klammern stehenden Produkte sind Skalarprodukte; der Punkt hinter dem Bruch bezeichnet die Multiplikation einer reellen Zahl mit einem Vektor.

Nun ist auch offensichtlich, wie man den zu $\vec{b}$ senkrechten Anteil von $\vec{a}$ berechnet; aus (23) und (21) folgt sofort:

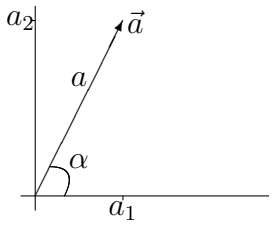
$$\vec{a}_2 \;=\; \vec{a} - \vec{a}_1 \;=\; \vec{a} - \frac{(\vec{a}\cdot\vec{b})}{(\vec{b}\cdot\vec{b})}\cdot\vec{b} \tag{24}$$

Gilt tatsächlich $\vec{a}_2 \perp \vec{b}$? Nach (20) ist dieses mit

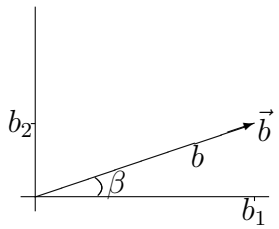
$$\vec{b}\cdot(\vec{a} - \vec{a}_1) \;=\; 0 \tag{25}$$

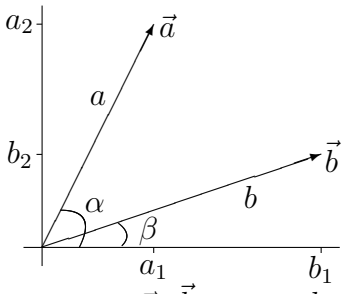
gleichbedeutend. Will man diese Gleichung nachrechnen, so stößt man im Augenblick noch bei der Berechnung von $\vec{b}\cdot(\vec{a} - \vec{a}_1)$ auf Schwierigkeiten. Um ein Skalarprodukt zu berechnen, dessen einer Faktor eine Summe oder eine Differenz ist, benötigt man noch einige weitere Eigenschaften des Skalarproduktes. Zu deren Herleitung wird als nächstes die **Komponentenschreibweise des Skalarproduktes** eingeführt.
Zu Vereinfachung soll nur der Fall zweidimensionaler Vektoren behandelt werden. Gegeben seien die beiden Vektoren $\vec{a}, \vec{b} \in \mathbb{R}^2$ mit den Beträgen a und b sowie den Winkeln α und β mit der x-Achse. Ausgangspunkt ist die Komponentendarstellung der beiden Vektoren:

$$\vec{a} \;=\; \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \;=\; \begin{pmatrix} a\cos\alpha \\ a\sin\alpha \end{pmatrix}$$



$$\vec{b} \;=\; \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \;=\; \begin{pmatrix} b\cos\beta \\ b\sin\beta \end{pmatrix}$$





Der Winkel zwischen den beiden Vektoren $\vec{a}$ und $\vec{b}$ beträgt

$$\alpha - \beta$$

Verwendet man dieses bei der Berechnung des Skalarproduktes von $\vec{a}$ und $\vec{b}$, so erhält man:

$$\begin{aligned}
\vec{a}\cdot\vec{b} &= a\cdot b\cdot\cos(\alpha-\beta) && \text{(Additionstheorem verwenden!)}\\
&= a\cdot b\cdot(\cos\alpha\,\cos\beta + \sin\alpha\,\sin\beta)\\
&= a\cos\alpha \cdot b\cos\beta + a\sin\alpha \cdot b\sin\beta\\
&= a_1 \cdot b_1 + a_2 \cdot b_2
\end{aligned}$$

Damit wurde gezeigt: Das Skalarprodukt kann berechnet werden, indem man die entsprechenden Komponenten der beiden Vektoren multipliziert und die entstehenden Produkte addiert. Die entsprechende Formel gilt für Vektoren im $\mathbb{R}^3$:

$$\vec{a} \cdot \vec{b} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = a_1 b_1 + a_2 b_2 + a_3 b_3$$

und ebenso für Vektoren beliebiger Dimension $n \in \mathbb{N}$:

Definition: (Skalarprodukt im $\mathbb{R}^n$:)

Für $\vec{a} \in \mathbb{R}^n$ und $\vec{b} \in \mathbb{R}^n$ ist definiert

$$< \vec{a}, \vec{b} >= \vec{a} \cdot \vec{b} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} a_i b_i \tag{26}$$

Die Gleichung (26) stellt eine Möglichkeit dar, das Skalarprodukt leicht zu berechnen; der Cosinus wird dabei nicht mehr benötigt. Weiterhin gestattet die Gleichung (26), die folgenden sehr wichtigen Recheneigenschaften des Skalarproduktes zu beweisen:

Satz:
Sei $\lambda \in \mathbb{R}$, und seien $\vec{a}, \vec{a}_1, \vec{a}_2, \vec{b}, \vec{b}_1, \vec{b}_2$ Vektoren. Dann gilt für das Skalarprodukt:

$$\begin{aligned} (\lambda \vec{a}) \cdot \vec{b} &= \lambda \cdot (\vec{a} \cdot \vec{b}) \\ \vec{a} \cdot (\lambda \vec{b}) &= \lambda \cdot (\vec{a} \cdot \vec{b}) \\ \vec{a} \cdot (\vec{b}_1 + \vec{b}_2) &= \vec{a} \cdot \vec{b}_1 + \vec{a} \cdot \vec{b}_2 \\ (\vec{a}_1 + \vec{a}_2) \cdot \vec{b} &= \vec{a}_1 \cdot \vec{b} + \vec{a}_2 \cdot \vec{b} \\ \vec{a} \cdot \vec{b} &= \vec{b} \cdot \vec{a} \\ \vec{a} \cdot \vec{a} &> 0 \quad \text{für} \quad \vec{a} \neq \vec{0} \end{aligned} \tag{27}$$

Beweis: Durch Nachrechnen mit der Komponentendarstellung (26) des Skalarproduktes.

Die Rechengesetze (27) des Skalarproduktes sollten einen an die entsprechenden Gesetze der reellen Zahlen erinnern: bei den beiden ersten Regeln handelt es sich um Assoziativgesetze, bei der dritten und vierten Regeln um Distributivgesetze und bei der vorletzten Regel um ein Kommutativgesetz. Ein Produkt, das die Rechengesetze (27) erfüllt, heißt **bilinear**.

Wir kommen zum senkrechten Anteil zurück. Nun kann leicht nachgerechnet werden, dass die Gleichung (25) erfüllt ist:

$$\begin{aligned}
\vec{a}_2 \cdot \vec{b} &= (\vec{a} - \vec{a}_1) \cdot \vec{b} && \text{(ausmultiplizieren und für } \vec{a}_1 \text{ einsetzen!)} \\
&= \vec{a} \cdot \vec{b} - \left(\frac{\vec{a} \cdot \vec{b}}{\vec{b} \cdot \vec{b}} \cdot \vec{b} \right) \cdot \vec{b} && \text{(die erste Regel aus (27) mit } \lambda = \tfrac{\vec{a}\cdot\vec{b}}{\vec{b}\cdot\vec{b}}\text{) anwenden!)} \\
&= \vec{a} \cdot \vec{b} - \frac{\vec{a} \cdot \vec{b}}{\vec{b} \cdot \vec{b}} \cdot (\vec{b} \cdot \vec{b}) \\
&= \vec{a} \cdot \vec{b} - \vec{a} \cdot \vec{b} = 0
\end{aligned}$$

Dieses ist gleichbedeutend mit $\vec{b} \perp \vec{a}_2$. Der Vektor $\vec{a}_2$ verdient somit zurecht den Namen zu $\vec{b}$ senkrechter Anteil von $\vec{a}$.

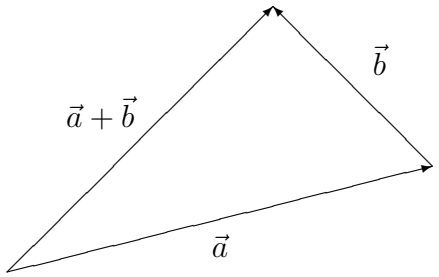
Mit Hilfe von (27) kann jetzt ein bedeutsamer Satz bewiesen werden, er beinhaltet zwei wichtige Ungleichungen:
Satz:
Für zwei Vektoren $\vec{a}$ und $\vec{b}$ gilt:

$$|\vec{a} \cdot \vec{b}| \leq ||\vec{a}|| \cdot ||\vec{b}|| \tag{28}$$

$$||\vec{a} + \vec{b}|| \leq ||\vec{a}|| + ||\vec{b}|| \tag{29}$$

Die Ungleichung (28) heißt **Cauchy-Schwarzsche Ungleichung**; die Ungleichung (29) heißt **Dreiecksungleichung**.

Die Dreiecksungleichung ist schon für reelle Zahlen bekannt, rechtfertigt aber erst im Zusammenhang mit Vektoren ihren Namen:
Die Dreiecksungleichung besagt, dass bei einem Dreieck eine Seite höchstens so lang ist wie die Summe der Längen der beiden anderen Seiten.



Beweis:

zu (28): $|\vec{a} \cdot \vec{b}| = ||\vec{a}|| \cdot ||\vec{b}|| \cdot \underbrace{|\cos\alpha|}_{\leq 1} \leq ||\vec{a}|| \cdot ||\vec{b}||$

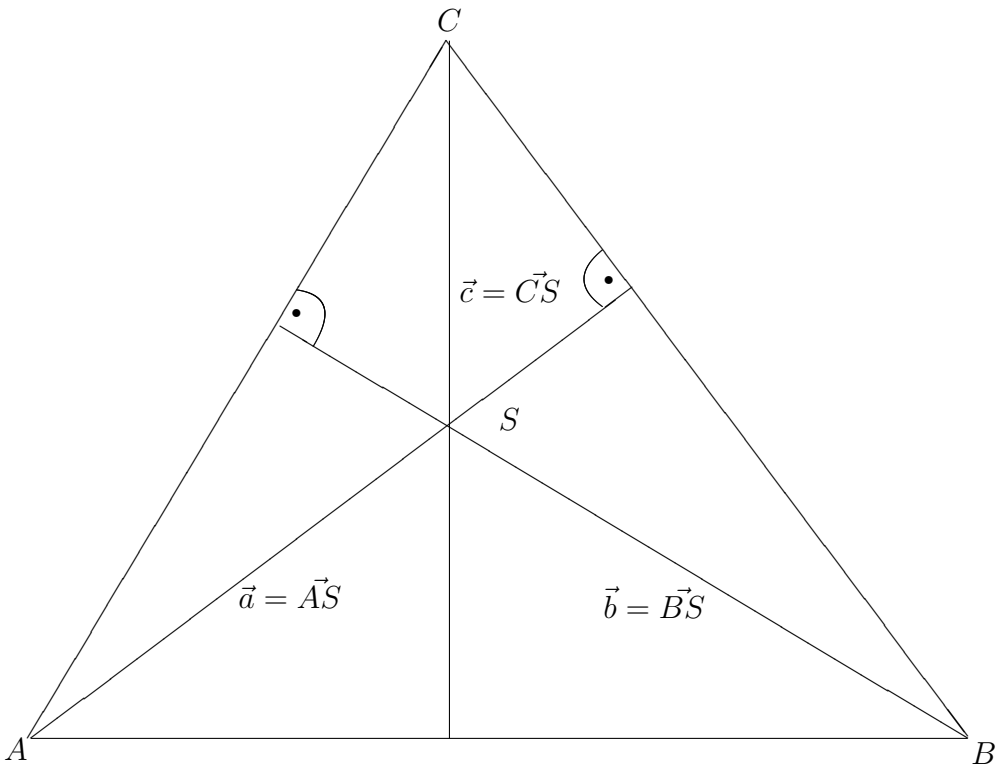
zu (29):

$\|\vec{a}+\vec{b}\|^2 = (\vec{a}+\vec{b}) \cdot (\vec{a}+\vec{b})$	vergleiche mit (22); ausmultiplizieren!
$= \|\vec{a}\|^2 + 2 \cdot \vec{a} \cdot \vec{b} + \|\vec{b}\|^2$	
$\leq \|\vec{a}\|^2 + 2 \cdot \|\vec{a} \cdot \vec{b}\| + \|\vec{b}\|^2$	Cauchy-Schwarzsche Ungleichung anwenden!
$\leq \|\vec{a}\|^2 + 2 \cdot \|\vec{a}\| \cdot \|\vec{b}\| + \|\vec{b}\|^2$	die erste Binomische Formel anwenden!
$= (\|\vec{a}\| + \|\vec{b}\|)^2$	aus beiden Seiten der Ungleichung die Wurzel ziehen
$\|\vec{a}+\vec{b}\| \leq \|\vec{a}\| + \|\vec{b}\|$	

qed.

Nach (20) liefert das Skalarprodukt eine einfache Möglichkeit, nachzurechnen, wann zwei Vektoren aufeinander senkrecht stehen: man braucht nur die Gleichung $\vec{x} \cdot \vec{y} = 0$ nachzuprüfen. Dieses wurde bereits im Zusammenhang mit dem senkrechten Anteil verwandt (siehe (25)). Als weiteres **Beispiel** für diese Anwendung des Skalarproduktes sowie auch für die Anwendung der Rechenregeln (27) soll hier ein einfacher geometrischer Sachverhalt nachgewiesen werden.
Es gilt nämlich: Die drei Höhen eines Dreiecks schneiden sich in einem Punkt.
Beweis dieser Aussage: Gegeben sei ein beliebiges Dreieck mit den drei Eckpunkten A, B und C. Die Höhen durch die beiden Punkte A und B werden eingezeichnet, deren Schnittpunkt werde mit S bezeichnet. Weiterhin seien die drei Vektoren von den Eckpunkten bis zu dem Punkt S gegeben:

$$\vec{a} = \vec{AS}, \quad \vec{b} = \vec{BS}, \quad \vec{c} = \vec{CS}$$



Die Behauptung ist bewiesen, wenn man zeigen kann, dass die durch C und S verlaufende Stecke die dritte Höhe des Dreiecks ist. Dieses ist gleichbedeutend damit, dass der Vektor $\vec{c}$ auf dem Vektor $\vec{AB}$ senkrecht steht. Zu zeigen bleibt daher (siehe (20)):

$$\vec{c} \cdot \vec{AB} \;=\; 0 \tag{30}$$

Aus der Zeichnung erkennt man sofort die Beziehungen

$$\vec{AB} \;=\; \vec{a} - \vec{b}, \quad \vec{BC} \;=\; \vec{b} - \vec{c}, \quad \vec{CA} \;=\; \vec{c} - \vec{a}$$

Weiterhin gilt, da nach Konstruktion $\vec{a}$ und $\vec{b}$ auf den Höhen durch A und B liegen:

$$\vec{a} \perp (\vec{b} - \vec{c}) \;\Leftrightarrow\; \vec{a} \cdot (\vec{b} - \vec{c}) = 0 \quad \text{und} \quad \vec{b} \perp (\vec{c} - \vec{a}) \;\Leftrightarrow\; \vec{b} \cdot (\vec{c} - \vec{a}) = 0$$

Nach diesen Vorüberlegungen kann (30) leicht nachgerechnet werden:

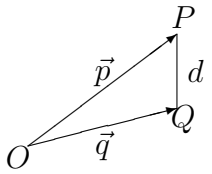
$$\begin{aligned}
\vec{c} \cdot \vec{AB} &= \vec{c} \cdot (\vec{a} - \vec{b}) && \text{(ausmultiplizieren!)} \\
&= \vec{c} \cdot \vec{a} \;-\; \vec{c} \cdot \vec{b} && \text{(geeignet ergänzen!)} \\
&= \vec{c} \cdot \vec{a} \underbrace{- \vec{b} \cdot \vec{a} + \vec{b} \cdot \vec{a}}_{=0} - \vec{c} \cdot \vec{b} && \text{(ausklammern!)} \\
&= \vec{a} \cdot (\vec{c} - \vec{b}) \;+\; \vec{b} \cdot (\vec{a} - \vec{c}) && \text{(siehe oben!)} \\
&= 0 + 0 \;=\; 0
\end{aligned}$$

qed.

Es folgen einige weitere nützliche Formeln, die auf dem Skalarprodukt beruhen:

Abstand zweier Punkte : Gegeben seien in der Ebene ($n = 2$) oder im Raum $n \geq 3$ die beiden Punkte P und Q, die zugehörigen Ortsvektoren seien

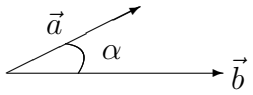
$$\vec{p} = \vec{OP} = \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \quad \text{und} \quad \vec{q} = \vec{OQ} = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$$



Der Abstand d zwischen ihnen ist die Länge des zugehörigen Differenzvektors, man berechnet ihn durch (siehe dazu (22) und (26), vergleiche auch mit 7.4)

$$d = ||\vec{p} - \vec{q}|| = \sqrt{(\vec{p} - \vec{q}) \cdot (\vec{p} - \vec{q})} = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2} \tag{31}$$

Den Winkel zwischen zwei Vektoren berechnet man mit der Darstellung (19) des Skalarproduktes:



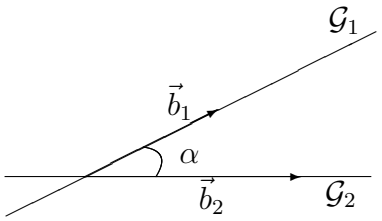
$$\alpha = \arccos\left(\frac{\vec{a} \cdot \vec{b}}{||\vec{a}|| \cdot ||\vec{b}||}\right) \tag{32}$$

Dabei wird in der Regel $\vec{a} \cdot \vec{b}$ durch die Komponentendarstellung (26) berechnet.

Der Schnittwinkel zweier sich schneidender Geraden ist genau der Winkel zwischen den beiden Richtungsvektoren: Sind die beiden Geraden

$$\mathcal{G}_1 = \left\{ \vec{a}_1 + t \cdot \vec{b}_1 \mid t \in \mathbb{R} \right\} \quad \text{und} \quad \mathcal{G}_2 = \left\{ \vec{a}_2 + t \cdot \vec{b}_2 \mid t \in \mathbb{R} \right\}$$

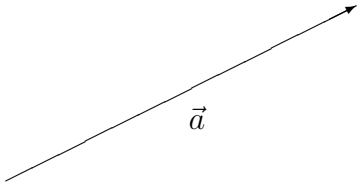
gegeben, so erhält man mit (32) für deren Schnittwinkel



$$\alpha = \arccos\left(\frac{\vec{b}_1 \cdot \vec{b}_2}{||\vec{b}_1|| \cdot ||\vec{b}_2||}\right) \tag{33}$$

Berechnung der Komponenten eines Vektors mit Hilfe des Skalarproduktes:

Gegeben sei ein Vektors $\vec{a}$ im Raum durch dessen Betrag und dessen Richtungswinkeln.



Gesucht ist die Komponentendarstellung des Vektors $\vec{a}$, was gleichbedeutend mit dessen Basisdarstellung durch die Einheitsvektoren ist (siehe (62), (63)):

$$\vec{a} \;=\; \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \;=\; a_1 \cdot \vec{e}_1 \,+\, a_2 \cdot \vec{e}_2 \,+\, a_3 \cdot \vec{e}_3$$

Zunächst beachte man, dass für das Skalarprodukt zweier Einheitsvektoren gilt

$$\vec{e}_i \cdot \vec{e}_j \;=\; \begin{cases} 1 & \text{für } \; i = j \\ 0 & \text{für } \; i \neq j \end{cases} \tag{34}$$

Die Gleichung (34) ergibt sich sofort aus der Komponentendarstellung der Einheitsvektoren und des Skalarproduktes. Man kann (34) auch nur mit (19) und ohne Verwendung der Komponenten begründen: ein Einheitsvektor besitzt die Länge $||\vec{e}_i|| = 1$, und zwei unterschiedliche Einheitsvektoren stehen aufeinander senkrecht.

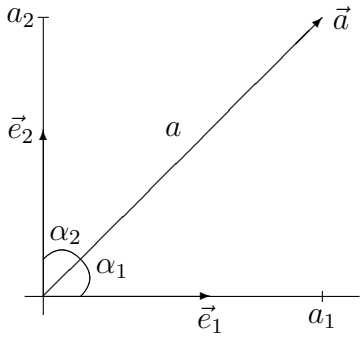
Zur Berechnung von a_1 macht man den Ansatz $\vec{a} = a_1\vec{e}_1 + a_2\vec{e}_2 + a_3\vec{e}_3$ und multipliziert[8] beide Seiten dieser Gleichung mit $\vec{e}_1$:

$$\begin{aligned} \vec{a} \cdot \vec{e}_1 &= (a_1 \cdot \vec{e}_1 \,+\, a_2 \cdot \vec{e}_2 \,+\, a_3 \cdot \vec{e}_3) \cdot \vec{e}_1 \\ &= a_1 \cdot \underbrace{\vec{e}_1 \cdot \vec{e}_1}_{=1} + a_2 \cdot \underbrace{\vec{e}_2 \cdot \vec{e}_1}_{=0} + a_3 \cdot \underbrace{\vec{e}_3 \cdot \vec{e}_1}_{=0} \\ &= a_1 \end{aligned}$$

Allgemein erhält auf diesem Wege:

$$\begin{aligned} a_i &= \vec{a} \cdot \vec{e}_i \\ &= ||\vec{a}|| \cdot ||\vec{e}_i|| \cdot \cos\alpha_i \;=\; a \cdot \cos\alpha_i \end{aligned} \tag{35}$$

Dabei ist $a = ||\vec{a}||$ und α_i der Winkel zwischen $\vec{a}$ und der i-ten Koordinatenachse:



7.7 Das Kreuzprodukt/Vektorprodukt

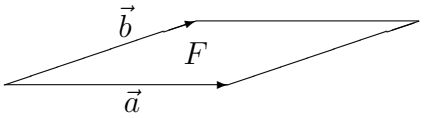
Definition:
Seien $\vec{a}, \vec{b} \in \mathbb{R}^3$; dann heißt der Vektor

$$\vec{c} \;=\; \vec{a} \times \vec{b}$$

das **Kreuz-** oder **Vektorprodukt** von $\vec{a}$ und $\vec{b}$, falls folgende Bedingungen erfüllt sind:

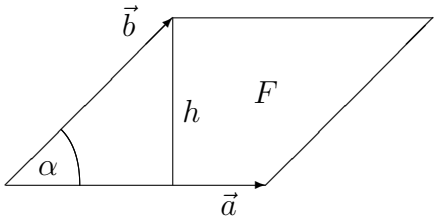
[8] durch das Skalarprodukt

1. Falls $\vec{a}$ und $\vec{b}$ linear abhängig sind, ist $\vec{c} = 0$.
2. Falls $\vec{a}$ und $\vec{b}$ linear unabhängig sind, gilt:
   (a) $\vec{c}$ steht senkrecht auf $\vec{a}$ und auf $\vec{b}$.
   (b) $||\vec{c}||$ ist der Flächeninhalt F des durch die beiden Vektoren $\vec{a}$ und $\vec{b}$ aufgespannten Parallelogrammes:



   (c) Die drei Vektoren $\vec{a}$, $\vec{b}$, $\vec{c}$ bilden ein Rechtssystem, d. h. schaut man in Richtung von $\vec{c}$ auf die von $\vec{a}$ und $\vec{b}$ aufgespannte Ebene, so verläuft die kürzere Drehung des ersten Faktors $\vec{a}$ auf den zweiten Faktor $\vec{b}$ im Uhrzeigersinn.[9]

Die Fläche F kann bekanntlich auf einfache Weise berechnet werden:



$$F = h \cdot ||\vec{a}|| = ||\vec{a}|| \cdot \underbrace{||\vec{b}|| \cdot |\sin\alpha|}_{h} = ||\vec{a} \times \vec{b}|| \tag{36}$$

Man beachte, dass nach Definition $(\vec{a} \times \vec{b}) \perp \vec{a}$ sowie $(\vec{a} \times \vec{b}) \perp \vec{b}$ gilt. Weitere wichtige Eigenschaften des Kreuzproduktes, die zum Umgang mit demselben unbedingt erforderlich sind, liefert der folgende Satz. Erst mit Hilfe des folgenden Satze ist es möglich, mit dem Kreuzproduktes in ähnlich einfacher Weise wie mit dem Skalarprodukt zu rechnen.

Satz:
Seien $\vec{a}$, $\vec{b}$, $\vec{c} \in \mathbb{R}^3$ und $\lambda \in \mathbb{R}$ beliebig. Dann gilt:

$$\vec{a} \times \vec{b} = -\vec{b} \times \vec{a} \tag{37}$$

$$\vec{a} \text{ und } \vec{b} \text{ linear abhängig} \quad \Leftrightarrow \quad \vec{a} \times \vec{b} = 0 \tag{38}$$

$$(\lambda \cdot \vec{a}) \times \vec{b} = \vec{a} \times (\lambda \cdot \vec{b}) = \lambda \cdot (\vec{a} \times \vec{b}) \tag{39}$$

$$(\vec{a} + \vec{b}) \times \vec{c} = \vec{a} \times \vec{c} + \vec{b} \times \vec{c} \tag{40}$$

(40) gilt entsprechend für den zweiten Faktor des Kreuzproduktes.

[9] Eine weitere Möglichkeit zur Darstellung der Richtung von $\vec{c}$ liefert die Rechtehandregel: Zeigt der Daumen der rechten Hand in Richtung von $\vec{a}$, der Zeigefinger in Richtung von $\vec{b}$, so verläuft deren Kreuzprodukt $\vec{c} = \vec{a} \times \vec{b}$ in Richtung des Mittelfingers.

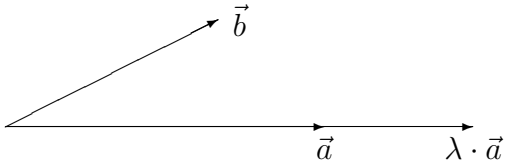
Beweis: Zu (37): Nach Konstruktion des Kreuzproduktes bewirkt eine Vertauschung der beiden Faktoren genau eine Umkehrung des Produktvektors.
Zu (38):

$$\vec{a} \text{ und } \vec{b} \text{ linear abhängig} \quad \Rightarrow \quad \vec{a} \times \vec{b} = 0 \quad \text{nach Konstruktion}$$

$$\vec{a} \text{ und } \vec{b} \text{ linear unabhängig} \quad \Rightarrow \quad \text{Die Fläche des Parallelogrammes ist positiv.}$$

Zu (39):

1. Sei $\lambda > 0$. Dann wird eine Seite des durch $\vec{a}$ und $\vec{b}$ gebildeten Parallelogrammes um den Faktor λ gestreckt oder gestaucht[10]:



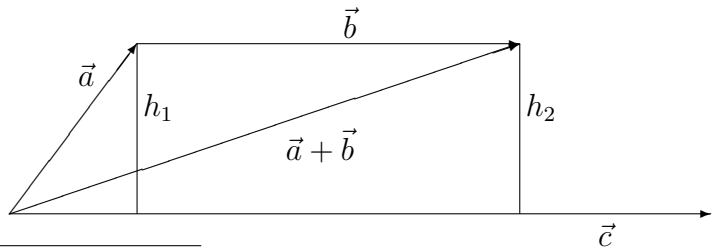
   Die Fläche wird dann ebenfalls mit dem Faktor λ multipliziert ($F \to \lambda \cdot F$).

2. Sei $\lambda < 0$. Dann ist $\lambda = -1 \cdot |\lambda|$. Dann folgt:

$$\begin{aligned}
(\lambda \cdot \vec{a}) \times \vec{b} &= |\lambda| \cdot (-1 \cdot \vec{a}) \times \vec{b} \\
&= |\lambda| \cdot (-\vec{a}) \times \vec{b} \\
&= |\lambda| \cdot (-(\vec{a} \times \vec{b})) \qquad \text{denn die Umorientierung eines Faktors } (\vec{a} \to -\vec{a}) \text{ bewirkt aufgrund der Regeln des Kreuzproduktes eine Umkehr der Richtung der Drehung von } \vec{a} \text{ auf } \vec{b} \text{ und damit nach Definition des Kreuzproduktes eine Umorientierung des Produktvektors.} \\
&= \lambda \cdot (\vec{a} \times \vec{b})
\end{aligned}$$

Zu (40):

1. Im ersten Fall seien $\vec{c}$ und $\vec{b}$ linear abhängig, d. h. es sei $\vec{b} = \lambda \cdot \vec{c}$:



[10] je nachdem, ob $\lambda > 1$ oder $\lambda < 1$ ist

Zunächst wird $\vec{a} \times \vec{c} = (\vec{a} + \vec{b}) \times \vec{c}$ gezeigt. Da die beiden Höhen h_1 und h_2 gleich sind, kann man schließen:

$$\begin{aligned} ||\vec{a} \times \vec{c}|| &= h_1 \cdot ||\vec{c}|| && \text{Die Fläche des von } \vec{a} \text{ und } \vec{c} \text{ aufgespannten Parallelogrammes} \\ &= h_2 \cdot ||\vec{c}|| && \text{Die Fläche des von } \vec{a} + \vec{b} \text{ und } \vec{c} \text{ aufgespannten Parallelogrammes} \\ &= ||(\vec{a} + \vec{b}) \times \vec{c}|| \end{aligned}$$

Nachdem so gezeigt wurde, dass die beiden Vektoren $(\vec{a}+\vec{b}) \times \vec{c}$ und $\vec{a} \times \vec{c}$ denselben Betrag besitzen, muss noch gezeigt werden, dass sie auch dieselbe Richtung und dieselbe Orientierung besitzen.

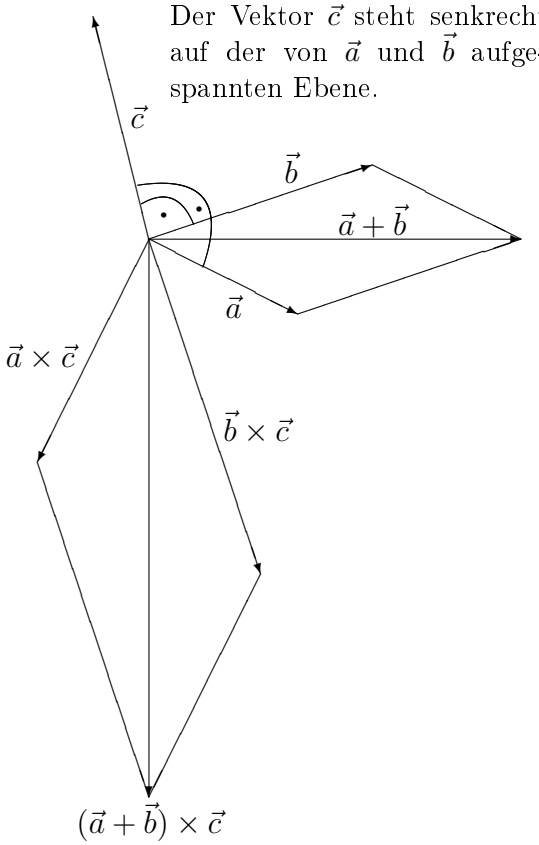
$\vec{a}$ und $\vec{c}$ einerseits sowie $(\vec{a} + \vec{b})$ und $\vec{c}$ andererseits spannen dieselbe Ebene auf, denn $\vec{b}$ und $\vec{c}$ sind linear abhängig (siehe Zeichnung). Da $\vec{a} \times \vec{c}$ und $(\vec{a}+\vec{b}) \times \vec{c}$ beide auf dieser Ebene senkrecht stehen, besitzen diese Vektoren dieselbe Richtung. Da weiterhin die Drehungen von $\vec{a}$ auf $\vec{c}$ und von $\vec{a}+\vec{b}$ auf $\vec{c}$ in derselben Drehrichtung verlaufen, besitzen die beiden Vektoren $\vec{a} \times \vec{c}$ und $(\vec{a} + \vec{b}) \times \vec{c}$ ebenfalls dieselbe Orientierung. Es folgt $\vec{a} \times \vec{c} = (\vec{a}+\vec{b}) \times \vec{c}$. Damit ergibt sich schließlich wegen (38)

$$(\vec{a}+\vec{b}) \times \vec{c} = \vec{a} \times \vec{c} = \vec{a} \times \vec{c} + \underbrace{\vec{b} \times \vec{c}}_{=0} \tag{41}$$

2. Es sei $\vec{c} \perp \vec{a}$ und $\vec{c} \perp \vec{b}$, d. h. $\vec{c}$ stehe sowohl auf $\vec{a}$ als auch auf $\vec{b}$ senkrecht. Damit ist ebenfalls $\vec{c} \perp (\vec{a} + \vec{b})$. Weiterhin ist dann hier wegen (36)

$$||\vec{a} \times \vec{c}|| = ||\vec{a}|| \cdot ||\vec{c}|| \tag{42}$$

(42) gilt in gleicher Weise für $\vec{b} \times \vec{c}$ sowie für $(\vec{a} + \vec{b}) \times \vec{c}$.



Nach Definition des Kreuzproduktes stehen $\vec{a}\times\vec{c}$, $\vec{b}\times\vec{c}$ sowie $(\vec{a}+\vec{b})\times\vec{c}$ ebenfalls senkrecht auf $\vec{c}$. Sie liegen damit in derselben Ebene wie $\vec{a}$ und $\vec{b}$, nämlich in der zu $\vec{c}$ senkrechten Ebene.
Da auch $\vec{a}\times\vec{c}$ auf $\vec{a}$ senkrecht steht, ergibt sich die Richtung von $\vec{a}\times\vec{c}$ durch eine Drehung von $\vec{a}$ um 90° in der zu $\vec{c}$ senkrechten Ebene. In gleicher Weise ergeben sich die Richtungen von $\vec{b}\times\vec{c}$ und $(\vec{a}+\vec{b})\times\vec{c}$, nämlich ebenfalls durch entsprechende Drehungen von $\vec{b}$ bzw. $\vec{a}+\vec{b}$ um 90°, wobei - aufgrund der Definition des Kreuzproduktes - die Drehrichtung dieselbe ist.

Insgesamt unterliegen die drei Vektoren $\vec{a}\times\vec{c}$, $\vec{b}\times\vec{c}$ und $(\vec{a}+\vec{b})\times\vec{c}$ damit derselben Drehstreckung[11]: einerseits ergeben sich die oben angegebenen Drehungen um 90°; andererseits werden wegen (42) alle Vektoren mit dem selben Faktor $||\vec{c}||$ multipliziert.

Nun betrachtet man die Diagonale des von $\vec{a}$ und $\vec{b}$ aufgespannten Parallelogrammes; diese ist durch $\vec{a}+\vec{b}$ gegeben und wird bei der Drehstreckung in die Diagonale des durch $\vec{a}\times\vec{c}$ und $\vec{b}\times\vec{c}$ aufgespannten Parallelogrammes, d. h. in $\vec{a}\times\vec{c}+\vec{b}\times\vec{c}$ überführt, also

$$\vec{a}+\vec{b} \quad\rightarrow\quad \vec{a}\times\vec{c}+\vec{b}\times\vec{c}$$

Andererseits ist das Ergebnis dieser Drehstreckung nach Definition ja gerade das Kreuzprodukt von $\vec{a}+\vec{b}$ mit dem Vektor $\vec{c}$. Damit ist in der Tat für diesen Fall:

$$(\vec{a}+\vec{b})\times\vec{c} = \vec{a}\times\vec{c}+\vec{b}\times\vec{c}$$

3. Seien nun $\vec{a},\vec{b},\vec{c}\in\mathbb{R}^3$ beliebig. Dann nimmt man für $\vec{a}$ und ebenso für $\vec{b}$ eine Aufspaltung in einen zu $\vec{c}$ senkrechten Anteil und einen Anteil, der parallel zu $\vec{c}$ ist, vor (siehe dazu (23), (24)):

$$\begin{aligned} \text{setze}\quad \vec{a} &= \vec{a}_1+\vec{a}_2 \quad \text{mit}\quad \vec{a}_1=\lambda_1\cdot\vec{c} \quad\text{und}\quad \vec{a}_2\perp\vec{c} \\ \vec{b} &= \vec{b}_1+\vec{b}_2 \quad \text{mit}\quad \vec{b}_1=\lambda_2\cdot\vec{c} \quad\text{und}\quad \vec{b}_2\perp\vec{c} \end{aligned} \tag{43}$$

[11] Als „Drehstreckung“ bezeichnet man die Drehung eines Vektors um einen bestimmten Winkel mit zusätzlicher Multiplikation dieses Vektors mit einer reellen Zahl.

$\lambda_1, \lambda_2 \in \mathbb{R}$ entsprechen dem Faktor auf der rechten Seite von (23). Die Zerlegungen (43) führen zu einer entsprechenden Zerlegung für den Summenvektor:

$$\begin{aligned} \vec{a} + \vec{b} &= (\vec{a}_1 + \vec{b}_1) + (\vec{a}_2 + \vec{b}_2) \\ \text{wobei gilt} \quad (\vec{a}_1 + \vec{b}_1) &= \lambda \cdot \vec{c} \quad \text{und} \quad (\vec{a}_2 + \vec{b}_2) \perp \vec{c} \end{aligned} \tag{44}$$

Hiermit berechnet man

$$\begin{aligned} (\vec{a} + \vec{b}) \times \vec{c} &= (\vec{a}_1 + \vec{a}_2 + \vec{b}_1 + \vec{b}_2) \times \vec{c} \\ &= (\vec{a}_1 + \vec{b}_1 + \vec{a}_2 + \vec{b}_2) \times \vec{c} \\ &= (\vec{a}_2 + \vec{b}_2) \times \vec{c} && \text{wegen (44), (41)} \\ &= \vec{a}_2 \times \vec{c} + \vec{b}_2 \times \vec{c} && \text{wegen (43) und wegen des 2. Falles (siehe Seite 122)} \\ &= (\vec{a}_1 + \vec{a}_2) \times \vec{c} + (\vec{b}_1 + \vec{b}_2) \times \vec{c} && \text{Hierbei wurde zweimal (41) angewandt.} \\ &= \vec{a} \times \vec{c} + \vec{b} \times \vec{c} \end{aligned}$$

qed.

Grundlegend sind die Werte des Kreuzproduktes bei den drei Einheitsvektoren $\vec{e}_1$, $\vec{e}_2$, $\vec{e}_3$. Da die drei Einheitsvektoren die Länge eins besitzen und paarweise aufeinander senkrecht stehen, folgt aus der Definition des Kreuzproduktes (bzw. mit der Rechtehandregel)[12]

$$\vec{e}_1 \times \vec{e}_2 = \vec{e}_3, \quad \vec{e}_2 \times \vec{e}_3 = \vec{e}_1, \quad \vec{e}_3 \times \vec{e}_1 = \vec{e}_2, \quad \vec{e}_i \times \vec{e}_i = 0 \tag{45}$$

$$\vec{e}_1 \times \vec{e}_3 = -\vec{e}_2, \quad \vec{e}_2 \times \vec{e}_1 = -\vec{e}_3, \quad \vec{e}_3 \times \vec{e}_2 = -\vec{e}_1, \tag{46}$$

Mit Hilfe des Satzes auf Seite 120 kann aus (45) die **Komponentendarstellung** des Kreuzproduktes gewonnen werden. Für zwei Vektoren $\vec{a}, \vec{b} \in \mathbb{R}^3$ setzt man dazu

$$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \sum_{i=1}^{3} a_i \cdot \vec{e}_i \quad \text{sowie} \quad \vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \sum_{j=1}^{3} b_j \cdot \vec{e}_j \tag{47}$$

[12] Die ersten drei Ausdrücke in (45) ergeben sich genau durch eine zyklische Vertauschung der drei Einheitsvektoren („Rechtssystem“).

und berechnet ausgehend von (47)

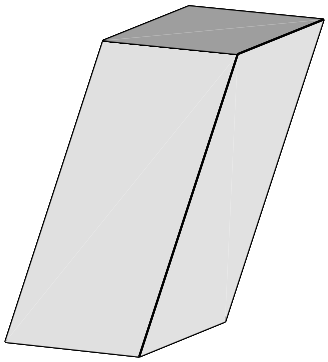
$$
\begin{aligned}
\vec{a} \times \vec{b} &= \left(\sum_{i=1}^{3} a_i \cdot \vec{e}_i\right) \times \vec{b} && \text{(nach (47))} \\
&= \sum_{i=1}^{3} a_i \cdot \left(\vec{e}_i \times \vec{b}\right) && \text{(nach (40), (39))} \\
&= \sum_{i=1}^{3} a_i \cdot \left(\vec{e}_i \times \sum_{j=1}^{3} b_j \cdot \vec{e}_j\right) && \text{(nach (47))} \\
&= \sum_{i=1}^{3}\sum_{j=1}^{3} a_i \cdot b_j \cdot \underbrace{(\vec{e}_i \times \vec{e}_j)}_{=0 \text{ für } i=j} && \text{(nach (40), (39))} \\
&= a_1 \cdot b_2 \cdot \underbrace{(\vec{e}_1 \times \vec{e}_2)}_{\vec{e}_3} + a_1 \cdot b_3 \cdot \underbrace{(\vec{e}_1 \times \vec{e}_3)}_{-\vec{e}_2} && \text{(nach (45),(46))} \\
&\quad + a_2 \cdot b_3 \cdot \underbrace{(\vec{e}_2 \times \vec{e}_3)}_{\vec{e}_1} + a_2 \cdot b_1 \cdot \underbrace{(\vec{e}_2 \times \vec{e}_1)}_{-\vec{e}_3} \\
&\quad + a_3 \cdot b_1 \cdot \underbrace{(\vec{e}_3 \times \vec{e}_1)}_{\vec{e}_2} + a_3 \cdot b_2 \cdot \underbrace{(\vec{e}_3 \times \vec{e}_2)}_{-\vec{e}_1} \\
&= \vec{e}_1 \cdot (a_2 \cdot b_3 - a_3 \cdot b_2) \\
&\quad + \vec{e}_2 \cdot (a_3 \cdot b_1 - a_1 \cdot b_3) \\
&\quad + \vec{e}_3 \cdot (a_1 \cdot b_2 - a_2 \cdot b_1)
\end{aligned}
$$

Wandelt man den letzten Ausdruck in Komponentendarstellung um (siehe Abschnitt 7.9.3), so liefert dieses die gesuchte und zum praktischen Rechnen sehr nützliche Komponentendarstellung des Kreuzproduktes:

$$
\vec{a} \times \vec{b} = \begin{pmatrix} a_2 \cdot b_3 - a_3 \cdot b_2 \\ a_3 \cdot b_1 - a_1 \cdot b_3 \\ a_1 \cdot b_2 - a_2 \cdot b_1 \end{pmatrix} \tag{48}
$$

Ein **Parallelotop** (auch *Spat*, *Parallelflach* oder *Parallelepiped* genannt) ist ein „dreidimensionales Parallelogramm“:

Parallelotop (Spat, Parallelflach, Parallelepipet)



Zur Berechnung des Volumens dieses dreidimensionalen Körpers wählt man eine seitliche Ansicht:
Hierbei ist h die Höhe des von $\vec{c}$, $\vec{a}$, $\vec{b}$ aufgespannten Parallelotops; für dessen Volumen gilt dann:

$$\begin{aligned}
\mathrm{vol}(\vec{c},\vec{a},\vec{b}) &= h \cdot \text{Grundfläche} \\
&= h \cdot ||\vec{a} \times \vec{b}|| \\
&= ||\vec{c}|| \cdot |\cos\alpha| \cdot ||\vec{a} \times \vec{b}|| \\
&= ||\vec{c}|| \cdot ||\vec{a} \times \vec{b}|| \cdot |\cos\alpha| \qquad \text{(Skalarprodukt)} \\
&= |\vec{c} \cdot (\vec{a} \times \vec{b})|
\end{aligned}$$

Der Ausdruck $\vec{c} \cdot (\vec{a} \times \vec{b})$ wird als **Spatprodukt** bezeichnet.

Zur Berechnung des Betrages des Kreuzproduktes $\vec{a} \times \vec{b}$ und damit der Fläche des von $\vec{a}$ und $\vec{b}$ aufgespannten Parallelogrammes kann das Skalarprodukt verwendet werden.
Satz:
Für $\vec{a}, \vec{b} \in \mathbb{R}^3$ gilt:

$$||\vec{a} \times \vec{b}||^2 = ||\vec{a}||^2 \cdot ||\vec{b}||^2 - (\vec{a} \cdot \vec{b})^2 \tag{49}$$

Beweis: α sei der von $\vec{a}$ und $\vec{b}$ eingeschlossene Winkel. Dann ist nach (36)

$$\begin{aligned} ||\vec{a} \times \vec{b}||^2 &= ||\vec{a}||^2 \cdot ||\vec{b}||^2 \cdot \sin^2 \alpha \\ &= ||\vec{a}||^2 \cdot ||\vec{b}||^2 \cdot (1 - \cos^2 \alpha) \\ &= ||\vec{a}||^2 \cdot ||\vec{b}||^2 - \underbrace{||\vec{a}||^2 \cdot ||\vec{b}||^2 \cdot \cos^2 \alpha}_{(\vec{a} \cdot \vec{b})^2} \qquad \text{(siehe (19))} \qquad \text{qed.} \end{aligned}$$

Eine in vielen Fällen recht nützliche Formel für die zweifache Anwendung des Kreuzproduktes liefert der folgende Satz.

Satz: (Entwicklungssatz für das Kreuzprodukt)
Für $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^3$ gilt:

$$\vec{c} \times (\vec{a} \times \vec{b}) = (\vec{b} \cdot \vec{c}) \cdot \vec{a} - (\vec{a} \cdot \vec{c}) \cdot \vec{b} \tag{50}$$

Zur teilweisen Plausibilisierung von (50) kann bemerkt werden, dass der Vektor $\vec{d} = \vec{c} \times (\vec{a} \times \vec{b})$ auf $\vec{a} \times \vec{b}$ senkrecht steht. Auf $\vec{a} \times \vec{b}$ stehen ebenso die beiden Vektoren $\vec{a}$ und $\vec{b}$ senkrecht. Folglich muss $\vec{d}$ in der von $\vec{a}$ und $\vec{b}$ aufgespannten Ebene enthalten sein und ist damit eine Linearkombination von $\vec{a}$ und $\vec{b}$.

Zum Beweis (von (50)): Zunächst berechnet man (50) für den Spezialfall $\vec{c} = \vec{e}_1$; zunächst wird dabei für $\vec{a} \times \vec{b}$ von Darstellung (48) ausgegangen:

$$\begin{aligned} \vec{e}_1 \times (\vec{a} \times \vec{b}) &= \vec{e}_1 \times \big((a_2b_3 - a_3b_2) \cdot \vec{e}_1 + (a_3b_1 - a_1b_3) \cdot \vec{e}_2 \\ &\qquad + (a_1b_2 - a_2b_1) \cdot \vec{e}_3\big) \\ &= (a_3b_1 - a_1b_3) \cdot \vec{e}_3 - (a_1b_2 - a_2b_1) \cdot \vec{e}_2 \qquad \text{(nach 45)} \\ &= \begin{pmatrix} 0 \\ b_1a_2 \\ b_1a_3 \end{pmatrix} - \begin{pmatrix} 0 \\ a_1b_2 \\ a_1b_3 \end{pmatrix} \\ &= \begin{pmatrix} b_1a_1 \\ b_1a_2 \\ b_1a_3 \end{pmatrix} - \begin{pmatrix} a_1b_1 \\ a_1b_2 \\ a_1b_3 \end{pmatrix} \\ &= b_1 \cdot \vec{a} - a_1 \cdot \vec{b} \\ &= (\vec{b} \cdot \vec{e}_1) \cdot \vec{a} - (\vec{a} \cdot \vec{e}_1) \cdot \vec{b} \end{aligned}$$

Damit hat man (50) für $\vec{c} = \vec{e}_1$ gezeigt:

$$\vec{e}_1 \times (\vec{a} \times \vec{b}) = (\vec{b} \cdot \vec{e}_1) \cdot \vec{a} - (\vec{a} \cdot \vec{e}_1) \cdot \vec{b} \tag{51}$$

Ganz entsprechend berechnet man

$$\vec{e}_2 \times (\vec{a} \times \vec{b}) = (\vec{b} \cdot \vec{e}_2) \cdot \vec{a} - (\vec{a} \cdot \vec{e}_2) \cdot \vec{b} \tag{52}$$

$$\vec{e}_3 \times (\vec{a} \times \vec{b}) = (\vec{b} \cdot \vec{e}_3) \cdot \vec{a} - (\vec{a} \cdot \vec{e}_3) \cdot \vec{b} \tag{53}$$

Für ein allgemeines $\vec{c} \in \mathbb{R}^3$ verwendet man die Darstellung $\vec{c} = c_1\vec{e}_1 + c_2\vec{e}_2 + c_3\vec{e}_3$ sowie (51), (52), (53):

$$\begin{aligned}
\vec{c} \times (\vec{a} \times \vec{b}) &= \left(\sum_{i=1}^{3} c_i\vec{e}_i\right) \times (\vec{a} \times \vec{b}) \\
&= \sum_{i=1}^{3} c_i \cdot \left(\vec{e}_i \times (\vec{a} \times \vec{b})\right) \qquad \text{(hier (51), (52), (53) einsetzen)} \\
&= \sum_{i=1}^{3} c_i \cdot \left((\vec{b} \cdot \vec{e}_i) \cdot \vec{a} - (\vec{a} \cdot \vec{e}_i) \cdot \vec{b}\right) \\
&= (\vec{b} \cdot \left(\sum_{i=1}^{3} c_i \cdot \vec{e}_i\right)) \cdot \vec{a} - (\vec{a} \cdot \left(\sum_{i=1}^{3} c_i \cdot \vec{e}_i\right)) \cdot \vec{b} \\
&= (\vec{b} \cdot \vec{c}) \cdot \vec{a} - (\vec{a} \cdot \vec{c}) \cdot \vec{b}
\end{aligned}$$

qed.

Zum Abschluss dieses Abschnitts folgen noch drei Anwendungen des Skalarproduktes:

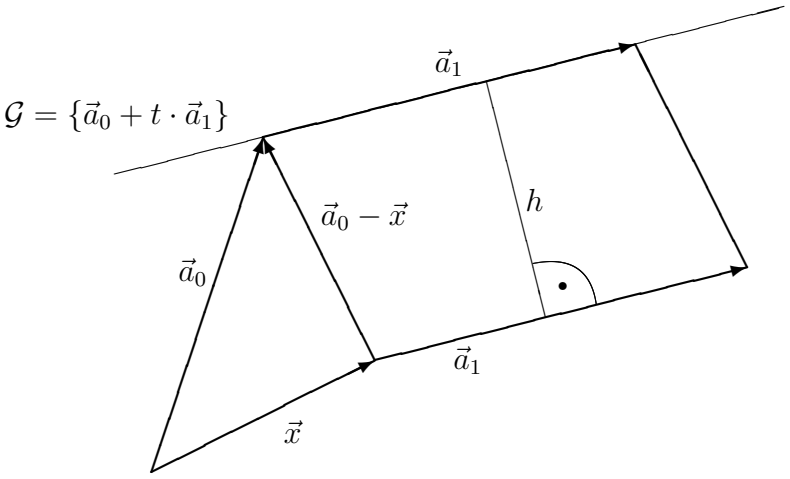
1. Einen Normalenvektor $\vec{n}$ zu einer Ebene

$$\mathcal{E} = \{\vec{a}_0 + \lambda\vec{a}_1 + \mu\vec{a}_2 \mid \lambda, \mu \in \mathbb{R}\}$$

d. h. einen auf $\mathcal{E}$ senkrecht stehenden Vektor der Länge 1 erhält man als normiertes Kreuzprodukt der beiden Richtungsvektoren:

$$\vec{n} = \frac{\vec{a}_1 \times \vec{a}_2}{||\vec{a}_1 \times \vec{a}_2||} \tag{54}$$

2. Der Abstand zwischen einem Punkt $\vec{x} \in \mathbb{R}^3$ und einer Geraden:



Der Abstand zwischen dem Punkt $\vec{x}$ und der Geraden $\mathcal{G}$ ist genau die Höhe h des vom Richtungsvektor $\vec{a}_1$ und vom Vektor $\vec{a}_0 - \vec{x}$ (einem von $\vec{x}$ nach $\mathcal{G}$ führenden Vektor) aufgespannten Parallelogrammes. Man erhält die Höhe h, indem man die Parallelogrammfläche (gegeben durch das Kreuzprodukt $\vec{a}_1 \times (\vec{a}_0 - \vec{x})$) durch die Länge der Grundlinie des Parallelogrammes (gegeben durch $\vec{a}_1$) teilt:

$$h = \frac{||\vec{a}_1 \times (\vec{a}_0 - \vec{x})||}{||\vec{a}_1||} \tag{55}$$

3. Ähnlich geht man bei der Berechnung des Abstands zweier Geraden

$$\mathcal{G}_1 = \{\vec{a}_0 + \lambda \cdot \vec{a}_1\}, \quad \mathcal{G}_2 = \{\vec{b}_0 + \mu \cdot \vec{b}_1\} \subset \mathbb{R}^3$$

in allgemeiner Lage[13] vor. Der Abstand ist gerade die Höhe d des von den beiden Richtungsvektoren $\vec{a}_1$ und $\vec{b}_1$ sowie dem Verbindungsvektor $\vec{a}_0 - \vec{b}_0$ zwischen den beiden Geraden aufgespannten Parallelotops. Die Höhe dieses Parallelotops berechnet man, indem man dessen Volumen durch dessen Grundfläche (gegeben durch das Kreuzprodukt der beiden Richtungsvektoren) teilt:

$$d = \frac{|(\vec{a}_0 - \vec{b}_0) \cdot (\vec{a}_1 \times \vec{b}_1)|}{||\vec{a}_1 \times \vec{b}_1||} \tag{56}$$

7.8 Der Vektorraum $\mathbb{R}^n$

Der Vektorraum $\mathbb{R}^n$ enthält als **Objekte** Spaltenvektoren $\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \in \mathbb{R}^n$, für die

zwei Rechenoperationen erklärt sind, nämlich:
Die **Addition** (als Addition der Komponenten)

$$\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}, \quad \vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \Rightarrow \vec{u} + \vec{v} = \begin{pmatrix} u_1 + v_1 \\ u_2 + v_2 \\ \vdots \\ u_n + v_n \end{pmatrix}$$

und die der **Multiplikation mit einer reellen Zahl**[14] (als komponentenweise Multiplikation)

$$\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}, \quad t \in \mathbb{R} \Rightarrow t \cdot \vec{u} = \begin{pmatrix} tu_1 \\ tu_2 \\ \vdots \\ tu_n \end{pmatrix}$$

Der Vektorraum $\mathbb{R}^n$ ist **abgeschlossen** gegenüber diesen Rechenoperationen, d.h.

[13] zweier sogenannter „windschiefer Geraden“
[14] In der Literatur findet man auch: Multiplikation mit einem Skalar oder skalare Multiplikation

$\vec{u}, \vec{v} \in \mathbb{R}^n \Rightarrow \vec{u} + \vec{v} \in \mathbb{R}^n$

$\vec{u} \in \mathbb{R}^n, t \in \mathbb{R} \Rightarrow t \cdot \vec{u} \in \mathbb{R}^n$

und damit auch:

$\vec{u}, \vec{v} \in \mathbb{R}^n,\ t_1, t_2 \in \mathbb{R} \Rightarrow t_1 \cdot \vec{u} + t_2 \cdot \vec{v} \in \mathbb{R}^n$

Für die beiden Rechenoperationen gelten folgende Gesetze (diese folgen aus den Rechengesetzen auf $\mathbb{R}$ auf Grund der komponentenweisen Definition der Rechenoperationen):

$\vec{u} + \vec{v} = \vec{v} + \vec{u}$ (Kommutativgesetz)

$(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$ (Assoziativgesetz)

$\vec{u} + \vec{0} = \vec{u}$ für $\vec{0} \in L^H$ ($\vec{0}$ als neutrales Element der Addition)

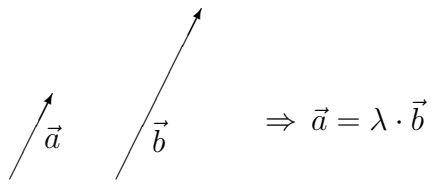
$\vec{u} \in \mathbb{R}^n \Rightarrow$ es gibt $-\vec{u} = (-1) \cdot \vec{u} \in \mathbb{R}^n$ mit $\vec{u} + (-\vec{u}) = \vec{u} - \vec{u} = \vec{0}$
($-\vec{u}$ als inverses Element der Addition)

$$\left.\begin{array}{c} t \cdot (\vec{u} + \vec{v}) = t \cdot \vec{u} + t \cdot \vec{v} \\ (t_1 + t_2) \cdot \vec{u} = t_1 \cdot \vec{u} + t_2 \cdot \vec{u} \end{array}\right\} \text{Distributivgesetz}$$

$t_1 \cdot (t_2 \cdot \vec{u}) = (t_1 \cdot t_2) \cdot \vec{u} = (t_2 \cdot t_1) \cdot \vec{u} = t_2 \cdot (t_1 \cdot \vec{u})$
$1 \cdot \vec{u} = \vec{u}$ für $1 \in \mathbb{R}$

7.9 Lineare Unabhängigkeit

7.9.1 Einführung



$\Rightarrow \vec{a} = \lambda \cdot \vec{b}$

Die beiden Vektoren $\vec{a}$ und $\vec{b}$ besitzen dieselbe Richtung; aus diesem Grund lässt sich der eine Vektor als Vielfaches des anderen darstellen. Man sagt in diesem Fall: Die Vektoren $\vec{a}$ und $\vec{b}$ sind **kollinear** oder **linear abhängig**.

Die beiden Vektoren $\vec{a}$ und $\vec{b}$ besitzen unterschiedliche Richtungen, bei ihnen besteht daher **keine** Beziehung der Form

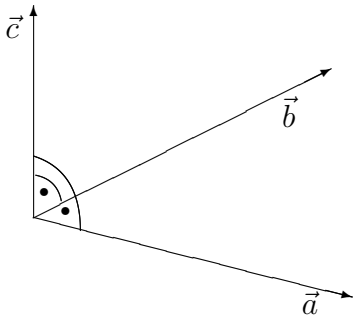
$$\vec{a} = \lambda \cdot \vec{b}$$

Die Vektoren $\vec{a}$ und $\vec{b}$ sind nicht kollinear, sondern sie sind **linear unabhängig.** Sie sind jedoch noch **komplanar**, das heißt sie liegen in einer Ebene.

Auf ähnliche Weise folgt für die drei Vektoren aus der Zeichnung: Es gibt keine Darstellung der Art

$$\vec{c} = \lambda\vec{a} + \mu\vec{b} \tag{57}$$

Die beiden Vektoren $\vec{a}$ und $\vec{b}$ liegen in einer Ebene, der Vektor $\vec{c}$ ragt aus dieser Ebene heraus.



Auch hier gilt: Die drei Vektoren $\vec{a}$, $\vec{b}$ und $\vec{c}$ sind **linear unabhängig**. Um dieses auszudrücken, ist eine Schreibweise der Form (57) ungeeignet. Man wählt eine Formulierung, in der die vorkommenden Vektoren in "gleichberechtigter Form" erscheinen. Dieses ist Inhalt der folgenden sehr wichtigen und grundlegenden Begriffsbildung.

7.9.2 Linear unabhängige Vektoren, Linearkombination, Basis und Dimension

Für alle vorkommenden Vektoren $\vec{a}, \vec{a}_i$ gilt $\vec{a}, \vec{a}_i \in \mathbb{R}^n$

Definition:
Sei $n \in \mathbb{N}$. Die n Vektoren $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ heißen **linear unabhängig**, falls eine Gleichung mit Koeffizienten $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ der Form

$$\sum_{i=1}^{n} \lambda_i \vec{a}_i = \lambda_1 \cdot \vec{a}_1 + \lambda_2 \cdot \vec{a}_2 + \ldots + \lambda_n \cdot \vec{a}_n = 0 \tag{58}$$

nur für

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$$

erfüllt ist. Ist hingegen eine Gleichung der Form

$$\sum_{i=1}^{n} \lambda_i \vec{a}_i = 0$$

erfüllt, bei der mindestens ein λ_i mit $\lambda_i \neq 0$ vorhanden ist, so heißen $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ **linear abhängig**.

Die Ausdrücke, die in der Definition der linearen Unabhängigkeit erscheinen, werden auch an anderer Stelle häufig vorkommen; man gibt ihnen daher einen Namen:

Definition:
Ein aus $n \in \mathbb{N}$ Vektoren $\vec{a}_1, \ldots, \vec{a}_n$ und n reellen Zahlen $\lambda_1, \ldots, \lambda_n$ gebildeter Ausdruck der Form

$$\sum_{i=1}^{n} \lambda_i \vec{a}_i = \lambda_1 \cdot \vec{a}_1 + \lambda_2 \cdot \vec{a}_2 + \ldots + \lambda_n \cdot \vec{a}_n \tag{59}$$

heißt **Linearkombination** der $\vec{a}_1, \ldots, \vec{a}_n$.

Bemerkungen:

1. Sind $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ **linear abhängig**, so lässt sich mindestens einer dieser Vektoren durch die übrigen darstellen. Genauer gilt: mindestens ein Vektor lässt sich durch eine Linearkombination der übrigen Vektoren darstellen.

   Wegen der linearen Abhängigkeit der $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n$ besteht eine Gleichung der Form (58), bei der mindestens ein Koeffizient λ_i von Null verschieden ist. Der zugehörige Vektor $\vec{a}_i$ ist dann gleich einer Linearkombination der übrigen Vektoren.

   Ist beispielsweise $\lambda_1 \neq 0$, so ist eine Teilung durch λ_1 möglich, und man kann die Gleichung

   $$\lambda_1 \cdot \vec{a}_1 + \lambda_2 \cdot \vec{a}_2 + \ldots + \lambda_n \cdot \vec{a}_n = 0 \qquad (\lambda_1 \neq 0)$$

   nach $\vec{a}_1$ auflösen:

   $$\vec{a}_1 = \sum_{i=2}^{n} \left(-\frac{\lambda_i}{\lambda_1} \right) \vec{a}_i$$

2. Ein einzelner Vektor $\vec{a}$ ist genau linear abhängig, wenn $\vec{a}$ der Nullvektor ist; es gilt nämlich:

   $$\vec{a} \neq 0 \quad \Leftrightarrow \quad \lambda \cdot \vec{a} \neq 0 \quad \text{für alle} \quad \lambda \neq 0$$

   $$\vec{a} = 0 \quad \Rightarrow \quad 1 \cdot \vec{a} = 0$$

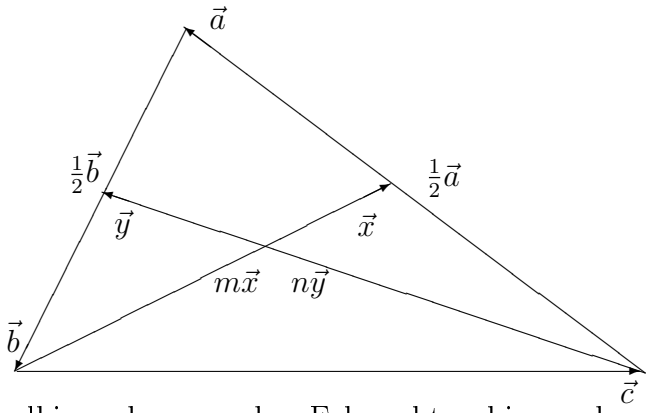
3. Befindet sich unter den Vektoren $\vec{a}_1, \ldots, \vec{a}_n$ der Nullvektor, so sind diese Vektoren linear abhängig. Ist etwa $\vec{a}_1 = 0$, so gilt:

   $$1 \cdot \vec{a}_1 + 0 \cdot \vec{a}_2 + \ldots + 0 \cdot \vec{a}_n = 0$$

   Der Koeffizient von $\vec{a}_1$ ist hier von Null verschieden.

Es folgt ein Beispiel für die Verwendung der linearen Unabhängigkeit: Es soll gezeigt werden, dass sich die Seitenhalbierenden eines Dreiecks im Verhältnis 2 : 1 schneiden.

Hierzu wird ein Dreieck durch drei Vektoren $\vec{a}$, $\vec{b}$ und $\vec{c}$ dargestellt. Dabei wird vorausgesetzt, dass die beiden Vektoren $\vec{a}$ und $\vec{b}$ linear unabhängig sind.
Die beiden Vektoren $\vec{x}$ und $\vec{y}$ stellen die Seitenhalbierenden auf die Seiten $\vec{a}$ und $\vec{b}$ dar.



Die Abschnitte auf den beiden Seitenhalbierenden von den Eckpunkten bis zu deren Schnittpunkt entsprechen den Vektoren $m \cdot \vec{x}$ und $n \cdot \vec{y}$. Die Behauptung ist gezeigt, wenn man

$$m = n = \frac{2}{3}$$

hergeleitet hat. Dazu werden einige Gleichungen mit Hilfe der Zeichnung aufgestellt:

$$\begin{aligned} \vec{a} + \vec{b} + \vec{c} &= 0 \quad \Rightarrow \quad \vec{c} = -\vec{a} - \vec{b} \\ \vec{x} &= \vec{c} + \frac{1}{2}\,\vec{a} \\ \vec{y} &= \vec{a} + \frac{1}{2}\,\vec{b} \\ m\,\vec{x} &= \vec{c} + n\,\vec{y} \end{aligned}$$

In die letzte Gleichung werden für $\vec{c}$, $\vec{x}$ und $\vec{y}$ die drei ersten Gleichungen eingesetzt:

$$-m\,\vec{a} - m\,\vec{b} + \frac{1}{2}m\,\vec{a} = -\vec{a} - \vec{b} + n\,\vec{a} + \frac{1}{2}n\,\vec{b}$$

Alle Glieder werden auf die rechte Seite dieser Gleichung gebracht, anschließend werden die Summanden mit $\vec{a}$ und $\vec{b}$ zusammengefaßt:

$$\begin{aligned} & -m\,\vec{b} - \tfrac{1}{2}m\,\vec{a} + \vec{a} + \vec{b} - n\,\vec{a} - \tfrac{1}{2}n\,\vec{b} = 0 \\ \Rightarrow \quad & \left(1 - \tfrac{1}{2}m - n\right)\vec{a} + \left(1 - \tfrac{1}{2}n - m\right)\vec{b} = 0 \end{aligned}$$

Da die beiden Vektoren $\vec{a}$ und $\vec{b}$ linear unabhängig sind, sind die Koeffizienten von $\vec{a}$ und $\vec{b}$ in der letzten Gleichung gleich Null:

$$\left.\begin{aligned} 1 - \tfrac{1}{2}m - n &= 0 \\ 1 - \tfrac{1}{2}n - m &= 0 \end{aligned}\right\} \quad \Leftrightarrow \quad \left\{\begin{aligned} \tfrac{1}{2}m + n &= 1 \\ m + \tfrac{1}{2}n &= 1 \end{aligned}\right.$$

Löst man dieses lineare Gleichungssystem in den unbekannten Werten m und n, so erhält man als eindeutige Lösung

$$m = \frac{2}{3} \quad \text{und} \quad n = \frac{2}{3}$$

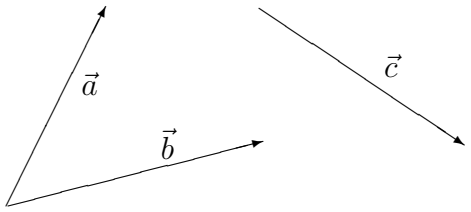
Damit ist die Behauptung gezeigt.

Definition:
Ist $n \in \mathbb{N}_0$ die maximale Anzahl zueinander linear unabhängiger Vektoren, so heißt dieses n die **Dimension** des zugehörigen Vektorraums.

Beispiel[15]

- In der Ebene gilt $n = 2$.
- Im (Anschauungsraum-) Raum gilt $n = 3$.

In der Ebene seien zwei linear unabhängige Vektoren $\vec{a}$ und $\vec{b}$ vorgegeben. Weiterhin sei ein beliebiger Vektor $\vec{c}$ gegeben:



Da es sich um drei Vektoren handelt und andererseits aus Dimensionsgründen nur höchstens zwei Vektoren voneinander linear unabhängig sein können, müssen diese drei Vektoren linear abhängig sein, d. h. es besteht eine Gleichung

$$\lambda \cdot \vec{a} + \mu \cdot \vec{b} + \nu \cdot \vec{c} = 0$$

bei der mindestens einer der drei Koeffizienten λ, μ und ν von Null verschieden ist. Insbesondere ist $\nu \neq 0$; wäre nämlich $\nu = 0$, so verbliebe die Gleichung

$$\lambda \cdot \vec{a} + \mu \cdot \vec{b} = 0$$

bei der nach wie vor ein Koeffizient ungleich Null ist, d. h. $\lambda \neq 0$ oder $\mu \neq 0$ ist; dieses ist ein Widerspruch zur linearen Unabhängigkeit von $\vec{a}$ und $\vec{b}$. Damit folgt:

$$\nu \neq 0$$

$$\Rightarrow \quad \vec{c} = \left(-\frac{\lambda}{\nu}\right) \cdot \vec{a} + \left(-\frac{\mu}{\nu}\right) \cdot \vec{b}$$

$$\Rightarrow \quad \vec{c} \quad \text{wird durch Linearkombination von } \vec{a} \text{ und } \vec{b} \text{ dargestellt}$$

Da sich ein beliebiger Vektor $\vec{c}$ aus der Ebene so darstellen ließ, bilden $\vec{a}$ und $\vec{b}$ zusammen eine sogenannte **Basis** der Ebene.

Definition:
Sind Vektoren $\vec{a}_1, \ldots, \vec{a}_n$ mit

[15] Begründungen folgen

1. jeder Vektor $\vec{c}$ lässt sich als Linearkombination der $\vec{a}_i$ darstellen:

$$\vec{c} = \lambda_1 \cdot \vec{a}_1 + \lambda_2 \cdot \vec{a}_2 + \ldots + \lambda_n \cdot \vec{a}_n \tag{60}$$

2. die Vektoren $\vec{a}_i$ sind linear unabhängig,

gegeben, so heißen die $\vec{a}_1, \ldots, \vec{a}_n$ **Basis** des zugehörigen Vektorraums.

Frage: Warum ist die Darstellung (60) eines Vektors durch eine Basis eindeutig?
Antwort: Angenommen, man hat zwei Darstellungen von $\vec{c}$:

$$\vec{c} = \lambda_1 \cdot \vec{a}_1 + \lambda_2 \cdot \vec{a}_2 + \ldots + \lambda_n \cdot \vec{a}_n$$
$$\vec{c} = \mu_1 \cdot \vec{a}_1 + \mu_2 \cdot \vec{a}_2 + \ldots + \mu_n \cdot \vec{a}_n$$

Die Subtraktion beider Darstellungen voneinander liefert:

$$0 = (\lambda_1 - \mu_1) \cdot \vec{a}_1 + (\lambda_2 - \mu_2) \cdot \vec{a}_2 + \ldots + (\lambda_n - \mu_n) \cdot \vec{a}_n \tag{61}$$

Da die $\vec{a}_i$ eine Basis bilden, sind sie linear unabhängig. Die Koeffizienten in (61) sind daher Null:

$$(\lambda_i - \mu_i) = 0 \quad \Rightarrow \quad \lambda_i = \mu_i \quad \text{für} \quad i = 1, \ldots, n$$

Es handelt sich also beide Male um dieselbe Darstellung von $\vec{c}$ durch die Basis $(\vec{a}_1, \ldots, \vec{a}_n)$.

Bemerkung:

$$n = \text{Anzahl der Basisvektoren} = \begin{array}{l}\text{maximale Anzahl der linear}\\ \text{unabhängigen Vektoren}\end{array}$$

Beispiel:

- Ebene: Anzahl Basisvektoren=Dimension= 2.
- (Anschauungs-) Raum: Anzahl Basisvektoren=Dimension= 3.

Um dieses begründen zu können, benötigt man eine andere Sicht auf die Komponentendarstellung von Vektoren.

7.9.3 Basis und Komponentendarstellung

Um zu zeigen, dass die Dimension der Ebene tatsächlich zwei beträgt, gibt man eine Basis der Ebene der Länge zwei an. Eine solche Basis ist die **Standardbasis**, bestehend aus den beiden Einheitsvektoren

$$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Man zeigt leicht, dass diese beiden Vektoren linear unabhängig sind; außerdem stellen sie jeden beliebigen Vektor der Ebene dar:

$$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = a_1 \cdot \vec{e}_1 + a_2 \cdot \vec{e}_2$$

Auf die gleiche Art zeigt man, dass der Raum die Dimension drei besitzt. Auch hier bilden die drei Einheitsvektoren

$$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \vec{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \vec{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{62}$$

die Standardbasis. Einen beliebigen räumlichen Vektor stellt man damit durch

$$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = a_1 \cdot \vec{e}_1 + a_2 \cdot \vec{e}_2 + a_3 \cdot \vec{e}_3 \tag{63}$$

dar.

Bezeichnungen:

$$\begin{aligned} \text{Ebene/Zahlenebene} &= \text{2-dim. Anschauungsraum} \;\hat{=}\; \mathbb{R}^2 \\ \text{Raum/Zahlenraum} &= \text{3-dim. Anschauungsraum} \;\hat{=}\; \mathbb{R}^3 \end{aligned}$$

8 Matrizen

8.1 Der Begriff der Matrix

Wir kommen auf die linearen Gleichungssysteme zurück und verfolgen das Ziel, für diese eine geeignetere und auch kürzere Schreibweise zu finden.
Der wesentliche Bestandteil eines Gleichungssystems sind seine Koeffizienten, sie bestimmen Rang und Corang des Gleichungssystems. Man beginnt daher beim Aufstellen der neuen Schreibweise bei den Koeffizienten:
Die Koeffizienten eines linearen Gleichungssystems mit m Gleichungen und n Unbekannten

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

schreibt man in der Form einer sogenannten $m \times n$–Matrix

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

Eine $m \times n$–Matrix ist ein rechteckiges Zahlenschema mit m Zeilen und n Spalten. Man bezeichnet Matrizen meist mit großen Druckbuchstaben. Kurzschreibweisen für allgemeine Matrizen sind

$$\underline{\underline{A}} = ((a_{ij}),\, i = 1 \ldots m,\, j = 1 \ldots n)$$

oder, falls Zeilen- und Spaltenzahl bereits festliegen, auch nur einfach $\underline{\underline{A}} = ((a_{ij}))$. Die a_{ij} nennt man die Koeffizienten oder Einträge der Matrix.

Als Beispiel betrachten wir das lineare Gleichungssystem

$$\begin{array}{rcrcrcr} 2x_1 & + & 10x_2 & + & 6x_3 & = & 18 \\ -x_1 & + & 2x_2 & - & 3x_3 & = & 0 \\ 3x_1 & + & x_2 & + & 2x_3 & = & 9 \\ 4x_1 & + & 13x_2 & + & 5x_3 & = & 27 \end{array} \tag{64}$$

Dieses ist ein Gleichungssystem mit 4 Gleichungen und 3 Unbekannten, es besitzt als Koeffizientenmatrix die 4×3–Matrix

$$\underline{\underline{A}} = \begin{pmatrix} 2 & 10 & 6 \\ -1 & 2 & -3 \\ 3 & 1 & 2 \\ 4 & 13 & 5 \end{pmatrix} \tag{65}$$

Matrizen sind eine Verallgemeinerung der Spaltenvektoren, der Schreibweise, die man für die Lösung von Gleichungssystemen verwendet: Einen Spaltenvektor wie

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

kann man als $n \times 1$–Matrix auffassen, also als Matrix mit n Zeilen und nur einer Spalte. Umgekehrt ist es oft günstig, eine $m \times n$–Matrix als Zusammensetzung von n Spaltenvektoren mit jeweils m Komponenten zu betrachten:

$$\begin{aligned} \underline{\underline{A}} &= ((a_{ij}),\, i = 1, \ldots, m,\, j = 1, \ldots, n) \\ &= (\vec{a}_1, \ldots, \vec{a}_n) \end{aligned}$$

$$\text{mit} \quad \vec{a}_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \quad \text{für} \quad j = 1, \ldots, n$$

Der erste Index zählt hier die Komponente des Spaltenvektors, der zweite gibt an, dass es sich um den j-ten Spaltenvektor handelt.

Die Spaltenvektoren der Matrix (65) sind

$$\vec{a}_1 = \begin{pmatrix} 2 \\ -1 \\ 3 \\ 4 \end{pmatrix} \qquad \vec{a}_2 = \begin{pmatrix} 10 \\ 2 \\ 1 \\ 13 \end{pmatrix} \qquad \vec{a}_3 = \begin{pmatrix} 6 \\ -3 \\ 2 \\ 5 \end{pmatrix}$$

Die Menge der n–dimensionalen Spaltenvektoren wird mit $\mathbb{R}^n$ bezeichnet.

Für Matrizen trifft man entsprechend die
Definition:
Für $m, n \in \mathbb{N}$ ist

$$\mathrm{M}^{m,n}(\mathbb{R}) = \{\underline{\underline{A}} = (a_{ij})_{i=1\ldots m,\, j=1\ldots n)} \,|\, a_{ij} \in \mathbb{R}\}$$

die Menge aller (reellen) $m \times n$–Matrizen.

Die Matrix (65) ist demnach ein Element der Menge $\mathrm{M}^{4,3}(\mathbb{R})$.

Als wichtige Spezialfälle von $\mathrm{M}^{m,n}(\mathbb{R})$ hat man:

- $\mathrm{M}^{n,n}(\mathbb{R})$ ist die Menge der quadratischen Matrizen; Zeilen- und Spaltenzahl sind bei diesen gleich.
- $\mathrm{M}^{m,1}(\mathbb{R})$ ist – wie bereits erwähnt – die Menge der einspaltigen Matrizen, sie entspricht der Menge der m-dimensionalen Spaltenvektoren:

$$\mathrm{M}^{m,1}(\mathbb{R}) \mathrel{\tilde{=}} \mathbb{R}^m$$

- $\mathrm{M}^{1,n}(\mathbb{R})$ ist die Menge der einzeiligen Matrizen, sie entspricht der Menge der n-dimensionalen Zeilenvektoren:

$$\mathrm{M}^{1,n}(\mathbb{R}) \mathrel{\tilde{=}} \{(a_1, \ldots, a_n) \,|\, a_i \in \mathbb{R}\}$$

- $\mathrm{M}^{1,1}(\mathbb{R})$ ist die Menge der Matrizen mit nur einem einzigen Eintrag, sie entspricht der Menge der reellen Zahlen:

$$\mathrm{M}^{1,1}(\mathbb{R}) \mathrel{\tilde{=}} \mathbb{R}$$

Um mit Hilfe der Matrizen zu einer einfachen Schreibweise für lineare Gleichungssysteme zu gelangen, definiert man eine „Multiplikation“ zwischen einer $m \times n$–Matrix und einem n-dimensionalen Spaltenvektor:
Definition:
Seien

$$\underline{\underline{A}} = ((a_{i,j})) \in \mathrm{M}^{m,n}(\mathbb{R}) \qquad \text{und} \qquad \vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$$

eine $m \times n$–Matrix und ein n-dimensionaler Spaltenvektor, dann definiert man deren Produkt durch

$$\begin{aligned} \underline{\underline{A}} \cdot \vec{x} &= \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\ &= \begin{pmatrix} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n \\ \vdots & & \vdots & & & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n \end{pmatrix} \end{aligned} \tag{66}$$

Verknüpft wird hier immer jeweils eine Zeile der Matrix mit dem Spaltenvektor:

$$(a_{i1}, \dots, a_{in}) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longrightarrow a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n \in \mathbb{R}$$

Das Ergebnis hiervon ist eine reelle Zahl. Hat die Matrix m Zeilen, so liefert die gesamte Operation als Ergebnis m reelle Zahlen; diese bilden genau einen m–dimensionalen Spaltenvektor.
Der Wertebereich der Verknüpfung „$\cdot$“ zwischen einer $m \times n$–Matrix und einem n–dimensionalen Spaltenvektor ist somit der $\mathbb{R}^m$:

$$\cdot : \quad \mathrm{M}^{m,n}(\mathbb{R}) \times \mathbb{R}^n \longrightarrow \mathbb{R}^m$$

Jetzt braucht man nur die rechte Seite eines Gleichungssystems als m–dimensionalen Spaltenvektor darzustellen. Dann kann man statt

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

das Gleichungssystem in der einfacheren Form

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

aufschreiben, bzw. man kann die Kurzschreibweise

$$\underline{\underline{A}} \cdot \vec{x} = \vec{b}$$

verwenden. Der letzte Ausdruck ist die direkte Verallgemeinerung der Darstellung $ax = b$ einer einfachen Gleichung mit einer Unbekannten.

Die Matrix–Vektor–Multiplikation

$$\underline{\underline{A}} \cdot \vec{x} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}x_1 & + & \dots & + & a_{1n}x_n \\ \vdots & & & & \vdots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n \end{pmatrix}$$

ist dabei so gefasst worden, dass sie genau auf die linearen Gleichungssysteme passt!

Beispiel: Das Gleichungssystem (64) auf Seite 137 bekommt in Matrizenschreibweise die Gestalt

$$\begin{pmatrix} 2 & 10 & 6 \\ -1 & 2 & -3 \\ 3 & 1 & 2 \\ 4 & 13 & 5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 18 \\ 0 \\ 9 \\ 27 \end{pmatrix}$$

Beim Reduzieren des Gleichungssystems mit dem Gaußschen Verfahren schreibt man natürlich nur die Koeffizientenmatrix und den Spaltenvektor der rechten Seite auf:

1. Normierung der ersten Gleichung liefert

$$\left(\begin{array}{ccc|c} 1 & 5 & 3 & 9 \\ -1 & 2 & -3 & 0 \\ 3 & 1 & 2 & 9 \\ 4 & 13 & 5 & 27 \end{array}\right)$$

2. Geeignete Vielfache der ersten Zeile werden von den folgenden abgezogen oder zu diesen hinzuaddiert:

$$\left(\begin{array}{ccc|c} 1 & 5 & 3 & 9 \\ 0 & 7 & 0 & 9 \\ 0 & -14 & 7 & -18 \\ 0 & -7 & -7 & -9 \end{array}\right)$$

3. Die zweite Zeile wird normiert, anschließend werden geeignete Vielfache der zweiten Zeile von den folgenden abgezogen oder zu diesen hinzuaddiert:

$$\left(\begin{array}{ccc|c} 1 & 5 & 3 & 9 \\ 0 & 1 & 0 & \frac{9}{7} \\ 0 & 0 & 7 & 0 \\ 0 & 0 & -7 & 0 \end{array}\right)$$

4. Normiert man nun noch die dritte Gleichung und addiert man ihr Siebenfaches zur letzten Gleichung, so erhält man ein reduziertes Gleichungssystem, das in Matrizenschreibweise so aussieht:

$$\begin{pmatrix} 1 & 5 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 9 \\ \frac{9}{7} \\ 0 \\ 0 \end{pmatrix}$$

Nachdem wir hier die Matrizen über lineare Gleichungssysteme eingeführt haben, werden wir sie jedoch – so wie es üblich ist - weitestgehend losgelöst von den Gleichungssystemen behandelt. Wir werden sehen, dass man Matrizen formal gut handhaben kann und werden insbesondere die Matrizenrechnung kennenlernen.

Eine wichtige Kennzahl „erbt“ die Matrix vom zugehörigen linearen Gleichungssystem:
Definition:
Der Rang einer Matrix $\underline{\underline{M}}$, geschrieben $\mathrm{rg}\left(\underline{\underline{M}}\right)$, ist der Rang eines linearen Gleichungssystems mit Koeffizientenmatrix $\underline{\underline{M}}$.

Ein Gleichungssystem mit Koeffizientenmatrix $\underline{\underline{M}}$ hat die Gestalt $\underline{\underline{M}} \cdot \vec{x} = \vec{b}$ mit einem $\vec{b} \in \mathbb{R}^m$. Will man den Rang berechnen, so erfolgt das natürlich mit dem Gaußschen Verfahren. Ist man nur am Rang der Matrix interessiert und nicht an möglichen Lösungen des Gleichungssystems, so reicht es, die Umformungsschritte des Verfahrens nur auf die Matrix anzuwenden und dabei die rechte Seite $\vec{b}$ nicht zu beachten.

Beispiel: Für die Matrix (65) ergab die Rechnung ab Seite 140

$$\mathrm{rg} \begin{pmatrix} 2 & 10 & 6 \\ -1 & 2 & -3 \\ 3 & 1 & 2 \\ 4 & 13 & 5 \end{pmatrix} = 3$$

Eine wichtige Operation auf Matrizen ist die Transposition:
Definition:
Sei $\underline{\underline{A}} \in \mathrm{M}^{m,n}(\mathbb{R})$ ein $m \times n$–Matrix. Dann ist

$$\underline{\underline{A}}^t \qquad \text{oder in Worten: “}A\text{ transponiert“}$$

diejenige Matrix $n \times m$–Matrix, die man erhält, wenn man A an der Hauptdiagonalen[16] spiegelt. Die Spalten von $\underline{\underline{A}}^t$ sind dann genau die Zeilen von $\underline{\underline{A}}$:

$$\underline{\underline{A}} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad \Rightarrow \quad \underline{\underline{A}}^t = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}$$

Beispiel:

$$\begin{pmatrix} 2 & 10 & 6 \\ -1 & 2 & -3 \\ 3 & 1 & 2 \\ 4 & 13 & 5 \end{pmatrix}^t = \begin{pmatrix} 2 & -1 & 3 & 4 \\ 10 & 2 & 1 & 13 \\ 6 & -3 & 2 & 5 \end{pmatrix}$$

Bemerkung: Bei nicht quadratischen Matrizen werden beim Transponieren Zeilen- und Spaltenzahl vertauscht, d. h.

$$\underline{\underline{A}} \in \mathrm{M}^{m,n}(\mathbb{R}) \quad \Rightarrow \quad \underline{\underline{A}}^t \in \mathrm{M}^{n,m}(\mathbb{R})$$

Für $n \neq m$ liegt insbesondere die transponierte Matrix in einer anderen Matrizenmenge, nämlich $\mathrm{M}^{n,m}(\mathbb{R})$, als die ursprüngliche.
Nicht so bei quadratischen Matrizen, dort gilt:

$$\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R}) \quad \Rightarrow \quad \underline{\underline{A}}^t \in \mathrm{M}^{n,n}(\mathbb{R})$$

Da doppeltes Spiegeln zum Ursprünglichen zurückführt, gilt der
Satz:
$\underline{\underline{A}} \in \mathrm{M}^{m,n}(\mathbb{R}) \quad \Rightarrow \quad (\underline{\underline{A}}^t)^t = \underline{\underline{A}}$.

Die zweimal transponierte Matrix ist also gleich der ursprünglichen!

Definition:
Eine quadratische Matrix $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ heißt symmetrisch, falls sie gleich ihrer Transponierten ist:

$$\underline{\underline{A}} = \underline{\underline{A}}^t$$

Eine $n \times n$–Matrix $\underline{\underline{A}} = ((a_{ij}))$ ist genau dann symmetrisch, wenn ihre Einträge die Gleichungen

$$a_{ij} = a_{ji} \qquad \text{für alle} \quad i, j = 1 \dots n$$

erfüllen.

[16] Die Hauptdiagonale ist die Diagonale mit den Elementen $a_{11}, a_{22}, \dots$.

Beispiel:

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix} \quad \text{ist symmetrisch,}$$

$$\underline{\underline{B}} = \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix} \quad \text{dagegen nicht.}$$

Zwei interessante Spezialfälle beim Transponieren sind Zeilen- und Spaltenvektoren: Ein Spaltenvektor geht in einen Zeilenvektor über und umgekehrt.

$$\vec{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \Leftrightarrow \quad \vec{a}^t = (a_1, \ldots, a_n)$$

Dieses hat u. a. Bedeutung für die Schreibweise:
Für Zeilenvektoren gewinnt eine Schreibweise dadurch, dass man sie als transponierte Spaltenvektoren schreibt. Dieses führt auf Bezeichnungen wie $\vec{a}^t$, $\vec{b}^t$ oder $\vec{c}^t$ für Zeilenvektoren. Ist nämlich

$$\vec{c}^t = (c_1, \ldots, c_n) \tag{67}$$

ein Zeilenvektor, so ist $\vec{c}$ der zugehörige Spaltenvektor; dieses erkennt man, indem man beide Seiten der Gleichung (67) transponiert:

$$\vec{c}^{tt} = (c_1, \ldots, c_n)^t = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

und $\vec{c}^{tt} = \vec{c}$ verwendet. Ebenso verwendet man für Spaltenvektoren mitunter die bequemere Schreibweise „$\vec{a} = (a_1, \ldots, a_n)^t$“, es ist nämlich

$$\vec{a} = (a_1, \ldots, a_n)^t = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

Es folgt ein wichtiger Satz, der später noch plausibilisiert werden wird:
Satz:
Die transponierte Matrix besitzt denselben Rang wie die ursprüngliche Matrix:

$$\operatorname{rg}\left(\underline{\underline{A}}\right) = \operatorname{rg}\left(\underline{\underline{A}}^t\right)$$

8.2 Rechnen mit Matrizen, das Matrizenprodukt

Zunächst lassen sich zwei Matrizen derselben Dimension addieren; das Ergebnis der Addition ist wieder eine Matrix derselben Dimension:

$$+ : \mathrm{M}^{m,n}(\mathbb{R}) \times \mathrm{M}^{m,n}(\mathbb{R}) \longrightarrow \mathrm{M}^{m,n}(\mathbb{R})$$

Die Addition erfolgt komponentenweise:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

Ein neutrales Element der Addition ist vorhanden, die **Nullmatrix**, die man üblicherweise einfach durch „$\underline{\underline{0}}$“ bezeichnet:

$$\underline{\underline{0}} = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

Ebenso gibt es zu jeder Matrix $\underline{\underline{A}} = ((a_{ij}))$ die negative:

$$\underline{\underline{-A}} = \begin{pmatrix} -a_{11} & \dots & -a_{1n} \\ \vdots & & \vdots \\ -a_{m1} & \dots & -a_{mn} \end{pmatrix}$$

Damit ist $\underline{\underline{A}} + (\underline{\underline{-A}}) = 0$. Zu beachten ist, dass man zwei Matrizen nur dann addieren oder voneinander abziehen kann, wenn sie Elemente derselben Matrizenmenge $\mathrm{M}^{m,n}(\mathbb{R})$ sind. Es ist $\underline{\underline{-A}} = -\underline{\underline{A}}$.

Weiterhin kann man eine Matrix mit einer reellen Zahl $\lambda \in \mathbb{R}$ multiplizieren; diese Multiplikation erfolgt ebenfalls komponentenweise:

$$\lambda \cdot \underline{\underline{A}} = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1n} \\ \vdots & & \vdots \\ \lambda a_{m1} & \dots & \lambda a_{mn} \end{pmatrix}$$

Die bedeutsamste Rechenoperation für Matrizen ist das **Matrizenprodukt**, das zwischen Matrizen passender Dimension erfüllt ist:

Ist $\underline{\underline{A}} \in \mathrm{M}^{l,m}(\mathbb{R})$ und $\underline{\underline{B}} \in \mathrm{M}^{m,n}(\mathbb{R})$, so lässt sich mit diesen Matrizen die Matrizenmultiplikation ausführen:

$$\underline{\underline{A}} \cdot \underline{\underline{B}} = \underline{\underline{C}}$$

Das Ergebnis ist eine Matrix $\underline{\underline{C}} \in \mathrm{M}^{l,n}(\mathbb{R})$.

Notwendige Bedingung für die Existenz des Matrizenprodukts ist also:

Spaltenanzahl von $\underline{\underline{A}}$ = Zeilenanzahl von $\underline{\underline{B}}$

Die **Ergebnismatrix** $\underline{\underline{C}} \in \mathrm{M}^{l,n}(\mathbb{R})$ der Multiplikation **erbt** dann die **Zeilenanzahl** vom ersten Faktor $\underline{\underline{A}} \in \mathrm{M}^{l,m}(\mathbb{R})$ und die **Spaltenanzahl** vom zweiten Faktor $\underline{\underline{B}} \in \mathrm{M}^{m,n}(\mathbb{R})$.

Zur Bezeichnung der Matrizenmultiplikation wird auch der Malpunkt "$\cdot$" verwendet.

Zur Herleitung der genauen Definition des Matrizenproduktes kehren wir zur Multiplikation von Matrizen mit Spaltenvektoren zurück:

Wir betrachten dazu den zweiten Faktor $\underline{\underline{B}}$ wieder als aus n Spaltenvektoren zusammengesetzt:

$$\underline{\underline{B}} \;=\; (\vec{b}_1, \ldots, \vec{b}_n) \qquad \text{mit} \quad \vec{b}_j \;=\; \begin{pmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{pmatrix} \quad \text{für} \quad j = 1 \ldots n$$

Dann erhalten wir $\underline{\underline{A}} \cdot \underline{\underline{B}}$ durch Multiplikation von jedem dieser Spaltenvektoren $\vec{b_j}$ $j = 1 \ldots n$ mit der Matrix $\underline{\underline{A}}$!

Definition:
Sei $\underline{\underline{A}} = ((a_{ki})) \in \mathrm{M}^{l,m}(\mathbb{R})$ eine $l \times m$–Matrix und $\underline{\underline{B}} = ((b_{ij})) \in \mathrm{M}^{m,n}(\mathbb{R})$ eine $m \times n$–Matrix. Dann ist deren Produktmatrix

$$\underline{\underline{C}} \;=\; \underline{\underline{A}} \cdot \underline{\underline{B}} \;=\; (\underline{\underline{A}} \cdot \vec{b}_1, \ldots, \underline{\underline{A}} \cdot \vec{b}_n).$$

Die Produktmatrix $\underline{\underline{C}}$ ist die $l \times n$–Matrix $\underline{\underline{C}} = ((c_{kj})) \in \mathrm{M}^{l,n}(\mathbb{R})$ mit den Koeffizienten

$$c_{kj} \;=\; (\underline{\underline{A}} \cdot \vec{b}_j)_k \;=\; \sum_{i=1}^{m} a_{ki} b_{ij} \qquad \text{für} \quad \begin{matrix} k &=& 1 \ldots l \\ j &=& 1 \ldots n \end{matrix} \tag{68}$$

Man beachte, dass der zweite Index der Einträge von $\underline{\underline{A}}$ und der erste Index der Einträge von $\underline{\underline{B}}$ denselben Wertebereich durchlaufen; dieses ist auch genau der Bereich des Summationsindex' in (68).

Wir wollen jetzt das Matrizenprodukt $\underline{\underline{A}} \cdot \underline{\underline{B}} = \underline{\underline{C}}$ noch etwas genauer betrachten und dabei zwei weitere wichtige Schreibweisen für dieses gewinnen. Zunächst erkennt man, dass bei der Berechnung der Koeffizienten c_{kj} von $\underline{\underline{C}}$, also in

$$c_{kj} \;=\; \sum_{i=1}^{m} a_{ki} b_{ij} \;=\; a_{k1} b_{1j} + \ldots + a_{km} b_{mj} \tag{69}$$

die k-te Zeile $(a_{k1}, \ldots, a_{km})$ von $\underline{\underline{A}}$ mit der j-ten Spalte $(b_{1j}, \ldots, b_{mj})^t$ von $\underline{\underline{B}}$ miteinander verknüpft werden:

$$\begin{pmatrix} b_{11} & \dots & \boxed{b_{1j}} & \dots & b_{1n} \\ \vdots & & \vdots & & \vdots \\ b_{m1} & \dots & b_{mj} & \dots & b_{mn} \end{pmatrix}$$
$$\downarrow$$
$$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ \boxed{a_{k1} \quad \dots \quad a_{km}} \\ \vdots & & \vdots \\ a_{l1} & \dots & a_{lm} \end{pmatrix} \rightarrow \qquad c_{kj}$$

Beispiel:

$$\begin{pmatrix} 1 & 2 & 4 \\ 9 & 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 3 & 4 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 0+2\cdot 3+4\cdot 1 & 1\cdot 2+2\cdot 4+4\cdot 1 \\ 9\cdot 0+8\cdot 3+1\cdot 1 & 9\cdot 2+8\cdot 4+1\cdot 1 \end{pmatrix}$$
$$= \begin{pmatrix} 10 & 14 \\ 25 & 51 \end{pmatrix}$$

Nochmals die wichtige Bemerkung: Die Multiplikation zweier Matrizen kann nur dann ausgeführt werden, wenn die Dimensionen passend sind: Die Spaltenzahl des linken Faktors muss gleich der Zeilenzahl des rechten Faktors sein; also

$$\begin{array}{ccccc} \mathrm{M}^{l,m}(\mathbb{R}) & \times & \mathrm{M}^{m,n}(\mathbb{R}) & \longrightarrow & \mathrm{M}^{l,n}(\mathbb{R}) \\ \underline{\underline{A}} & \cdot & \underline{\underline{B}} & = & \underline{\underline{C}} \end{array} \tag{70}$$

Die Produktmatrix „erbt“ die Zeilenzahl vom linken und die Spaltenzahl vom rechten Faktor.

Satz[17]:
Sei $\underline{\underline{A}} \in \mathrm{M}^{l,m}(\mathbb{R})$ und $\underline{\underline{B}} \in \mathrm{M}^{m,n}(\mathbb{R})$. Dann ist $\underline{\underline{A}} \cdot \underline{\underline{B}}$ definiert, und es gilt

$$(\underline{\underline{A}} \cdot \underline{\underline{B}})^t = \underline{\underline{B}}^t \cdot \underline{\underline{A}}^t \tag{71}$$

(Man beachte, dass wegen $\underline{\underline{B}}^t \in \mathrm{M}^{n,m}(\mathbb{R})$ und $\underline{\underline{A}}^t \in \mathrm{M}^{m,l}(\mathbb{R})$ auch das Produkt $\underline{\underline{B}}^t \cdot \underline{\underline{A}}^t$ definiert ist.)

Die folgenden **Rechenregeln für das Matrizenprodukt** werden ohne Beweise[18] gebracht. Sehr wichtig ist darunter insbesondere die erste Aussage, das Assoziativgesetz:

[17] Ohne Beweis!
[18] Diese Beweise erfolgen durch Nachrechnen.

Satz:
Die folgenden Matrizen seien gegeben

$$\underline{\underline{A}},\ \underline{\underline{A_1}},\ \underline{\underline{A_2}} \in \mathrm{M}^{l,m}(\mathbb{R}), \quad \underline{\underline{B}},\ \underline{\underline{B_1}},\ \underline{\underline{B_2}} \in \mathrm{M}^{m,n}(\mathbb{R}), \quad \text{und} \quad \underline{\underline{C}} \in \mathrm{M}^{n,p}(\mathbb{R})$$

Dann gilt:

1. Das Assoziativgesetz:
$$(\underline{\underline{A}} \cdot \underline{\underline{B}}) \cdot \underline{\underline{C}} = \underline{\underline{A}} \cdot (\underline{\underline{B}} \cdot \underline{\underline{C}})$$
2. Das 1. Distributivgesetz:
$$(\underline{\underline{A_1}} + \underline{\underline{A_2}}) \cdot \underline{\underline{B}} = \underline{\underline{A_1}} \cdot \underline{\underline{B}} + \underline{\underline{A_2}} \cdot \underline{\underline{B}}$$
3. Das 2. Distributivgesetz:
$$\underline{\underline{A}} \cdot (\underline{\underline{B_1}} + \underline{\underline{B_2}}) = \underline{\underline{A}} \cdot \underline{\underline{B_1}} + \underline{\underline{A}} \cdot \underline{\underline{B_2}}$$
4. Für $\lambda \in \mathbb{R}$ ist
$$\lambda \cdot (\underline{\underline{A}} \cdot \underline{\underline{B}}) = (\lambda \cdot \underline{\underline{A}}) \cdot \underline{\underline{B}} = \underline{\underline{A}} \cdot (\lambda \cdot \underline{\underline{B}})$$

Achtung: Das Matrizenprodukt ist nicht kommutativ , d.h. in der Regel gilt

$$\underline{\underline{A}} \cdot \underline{\underline{B}} \neq \underline{\underline{B}} \cdot \underline{\underline{A}}.$$

Beispiel:

$$\begin{pmatrix} 1 & 2 & 4 \\ 9 & 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 3 & 4 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 0+2\cdot 3+4\cdot 1 & 1\cdot 2+2\cdot 4+4\cdot 1 \\ 9\cdot 0+8\cdot 3+1\cdot 1 & 9\cdot 2+8\cdot 4+1\cdot 1 \end{pmatrix}$$

$$= \begin{pmatrix} 10 & 14 \\ 25 & 51 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 \\ 3 & 4 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 4 \\ 9 & 8 & 1 \end{pmatrix} = \begin{pmatrix} 0\cdot 1+2\cdot 9 & 0\cdot 2+2\cdot 8 & 0\cdot 4+2\cdot 1 \\ 3\cdot 1+4\cdot 9 & 3\cdot 2+4\cdot 8 & 3\cdot 4+4\cdot 1 \\ 1\cdot 1+1\cdot 9 & 1\cdot 2+1\cdot 8 & 1\cdot 4+1\cdot 1 \end{pmatrix} \quad (72)$$

$$= \begin{pmatrix} 18 & 16 & 2 \\ 37 & 38 & 16 \\ 10 & 10 & 5 \end{pmatrix} \quad (73)$$

Zum Schluss dieses Abschnitts noch ein weiteres Beispiel zur Anwendung des Matrizenproduktes. Wir betrachten die Matrix A mit

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

und berechnen deren Quadrat

$$\underline{\underline{A}}^2 = \underline{\underline{A}} \cdot \underline{\underline{A}} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

8.3 Quadratische Matrizen und die Umkehrmatrix (inverse Matrix)

Multipliziert man zwei Matrizen passender Dimension miteinander so hat im allgemeinen die Produktmatrix eine andere Dimension als die beiden Faktoren (siehe (70) auf Seite 146), d. h. sie liegt in einer anderen Matrizenmenge $\mathrm{M}^{l,n}(\mathbb{R})$.
Anders (besser!) verhält es sich bei quadratischen Matrizen:
Sind zwei quadratische Matrizen $\underline{\underline{A}}$ und $\underline{\underline{B}}$ derselben Dimension gegeben, so sind beide Matrizenprodukte $\underline{\underline{A}} \cdot \underline{\underline{B}}$ und $\underline{\underline{B}} \cdot \underline{\underline{A}}$ definiert, und die Ergebnisse sind wieder quadratische Matrizen derselben Dimension (siehe dazu (70) mit $l = m = n$):

$$\underline{\underline{A}}, \underline{\underline{B}} \in \mathrm{M}^{n,n}(\mathbb{R}) \quad \Rightarrow \quad \underline{\underline{A}} \cdot \underline{\underline{B}}, \underline{\underline{B}} \cdot \underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$$

Damit wird die Matrizenmultiplikation zu einer inneren Verknüpfung der Menge $\mathrm{M}^{n,n}(\mathbb{R})$: Sie ist für alle Elemente aus $\mathrm{M}^{n,n}(\mathbb{R})$ definiert, und $\mathrm{M}^{n,n}(\mathbb{R})$ ist abgeschlossen bezüglich „$\cdot$“.
Zum Vergleich sei daran erinnert, dass die übliche Multiplikation eine innere Verknüpfung der Menge der reellen Zahlen ist.

Betrachtet man $\mathrm{M}^{n,n}(\mathbb{R})$ zusammen mit den beiden inneren Verknüpfungen „$+$“ (der komponentenweisen Addition) und „$\cdot$“, so spricht man vom Matrizenring und schreibt

$$(\mathrm{M}^{n,n}(\mathbb{R}), +, \cdot)$$

Bezüglich der Addition wird das auf der Seite 144 ausgeführt; insgesamt gilt: Zusammen mit „$+$“ ist $\mathrm{M}^{n,n}(\mathbb{R})$ eine kommutative Gruppe mit der Nullmatrix als neutralem Element;

das negative Element einer Matrix erhält man dadurch, dass man jeden ihrer Einträge durch dessen Negatives ersetzt.

Wir wollen uns jetzt der anderen inneren Verknüpfung „$\cdot$“ zuwenden. Zunächst gilt auch hier der Satz auf Seite 147:

- $\cdot$ ist assoziativ, d. h.

$$\underline{\underline{A}}, \underline{\underline{B}}, \underline{\underline{C}} \in \mathrm{M}^{n,n}(\mathbb{R}) \quad \Rightarrow \quad (\underline{\underline{A}} \cdot \underline{\underline{B}}) \cdot \underline{\underline{C}} = \underline{\underline{A}} \cdot (\underline{\underline{B}} \cdot \underline{\underline{C}})$$

- Zusammen mit der Addition gelten die Distributivgesetze:

$$\begin{array}{rcl} (\underline{\underline{A}} + \underline{\underline{B}}) \cdot \underline{\underline{C}} & = & \underline{\underline{A}} \cdot \underline{\underline{C}} + \underline{\underline{B}} \cdot \underline{\underline{C}} \\ \underline{\underline{A}} \cdot (\underline{\underline{B}} + \underline{\underline{C}}) & = & \underline{\underline{A}} \cdot \underline{\underline{B}} + \underline{\underline{A}} \cdot \underline{\underline{C}} \end{array} \quad \underline{\underline{A}}, \underline{\underline{B}}, \underline{\underline{C}} \in \mathrm{M}^{n,n}(\mathbb{R}) \quad \Rightarrow$$

Wie steht es bei der Matrizenmultiplikation bezüglich

- Kommutativität
- neutralem Element
- Inversenbildung

aus?

Wir gehen nacheinander diese Punkte durch. Dazu setzen wir fortan $n > 1$ voraus. Für $n = 1$ entspricht $\mathrm{M}^{n,n}(\mathbb{R})$ der Menge der reellen Zahlen (Aufgaben: Machen Sie sich dieses klar!):

$$(\mathrm{M}^{1,1}(\mathbb{R}), +, \cdot) \tilde{=} (\mathbb{R}, +, \cdot)$$

Zunächst muss man nochmals feststellen, dass die Matrizenmultiplikation **nicht kommutativ** ist, d. h. es gibt Matrizen $\underline{\underline{A}}, \underline{\underline{B}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit $\underline{\underline{A}} \cdot \underline{\underline{B}} \neq \underline{\underline{B}} \cdot \underline{\underline{A}}$.

Beispiel:

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

$$\neq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Ein **neutrales Element zur Matrizenmultiplikation** ist vorhanden; dieses ist die sogenannte **Einheitsmatrix**, bezeichnet mit „$\underline{\underline{E}}$“:

$$\underline{\underline{E}} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Die Einheitsmatrix ist die Matrix, deren Einträge auf der Hauptdiagonalen alle gleich 1 und sonst gleich 0 sind. Die Einträge von $\underline{\underline{E}}$ bezeichnet man üblicherweise mit δ_{ij}:

$$\underline{\underline{E}} = \begin{pmatrix} \delta_{11} & \dots & \delta_{1n} \\ \vdots & & \vdots \\ \delta_{n1} & \dots & \delta_{nn} \end{pmatrix} \quad \text{mit} \quad \delta_{ij} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$$

Die δ_{ij} heißen Kroneckersymbole.

Eine weitere Schreibweise für die Einheitsmatrix ist die Darstellung durch Spaltenvektoren:

$$\underline{\underline{E}} = (\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n)$$

$$\text{mit} \quad \vec{e}_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \longleftarrow j\text{-te Stelle}$$

Die $\vec{e}_1, \dots, \vec{e}_n$ bezeichnet man als die n-dimensionalen Einheitsvektoren; die Einheitsvektoren enthalten genau eine Eins und sonst Nullen. Für $n = 3$ hat man beispielsweise

$$\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{und} \quad \vec{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Zusammen ergeben diese die dreidimensionale Einheitsmatrix:

$$\underline{\underline{E}} = (\vec{e}_1, \vec{e}_2, \vec{e}_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Um zu zeigen, dass $\underline{\underline{E}}$ wirklich neutrales Element ist, bedarf es zweier Sätze:

Satz:
Für alle $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ ist

$$\underline{\underline{E}} \cdot \underline{\underline{A}} = \underline{\underline{A}}.$$

Beweis: Sei $\vec{a} = (a_1, \ldots, a_n)^t \in \mathbb{R}^n$; wir zeigen im ersten Schritt $\underline{\underline{E}} \cdot \vec{a} = \vec{a}$:

$$\underline{\underline{E}} \cdot \vec{a} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \circ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

$$= \begin{pmatrix} 1 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n \\ 0 \cdot a_1 + 1 \cdot a_2 + \cdots + 0 \cdot a_n \\ \vdots \\ 0 \cdot a_1 + 0 \cdot a_2 + \cdots + 1 \cdot a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \vec{a}$$

Stellt man jetzt $\underline{\underline{A}}$ in Spaltenschreibweise dar, so folgt im zweiten Schritt

$$\begin{aligned} \underline{\underline{E}} \cdot \underline{\underline{A}} = \underline{\underline{E}} \cdot (\vec{a}_1, \ldots, \vec{a}_n) &= (\underline{\underline{E}} \cdot \vec{a}_1, \ldots, \underline{\underline{E}} \cdot \vec{a}_n) \\ &= (\vec{a}_1, \ldots, \vec{a}_n) = \underline{\underline{A}} \end{aligned}$$

Denn, wie eben gezeigt, ist stets $\underline{\underline{E}} \cdot \vec{a}_j = \vec{a}_j$. qed.

Bis jetzt wurde nur gezeigt, dass für alle $A \in \mathrm{M}^{n,n}(\mathbb{R})$ die Gleichung

$$\underline{\underline{E}} \cdot \underline{\underline{A}} = \underline{\underline{A}}$$

gilt, d. h. es wurde nur gezeigt, dass $\underline{\underline{E}}$ ein sogenanntes linksneutrales Element ist. Man kann daraus **nicht** unmittelbar folgern, dass auch

$$\underline{\underline{A}} \cdot \underline{\underline{E}} = \underline{\underline{A}} \tag{74}$$

gilt, denn die Matrizenmultiplikation ist **nicht** kommutativ!
Die Gleichung (74) wird im nächsten Satz gezeigt; dabei wird verwendet, dass die Einheitsmatrix symmetrisch ist

$$\underline{\underline{E}}^t = \underline{\underline{E}}$$

Satz:
Für alle $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ gilt

$$\underline{\underline{A}} \cdot \underline{\underline{E}} = \underline{\underline{A}}$$

Beweis: Im vorangegangenen Satz wurde gezeigt, dass für alle $\underline{\underline{B}} \in \mathrm{M}^{n,n}(\mathbb{R})$ gilt

$$\underline{\underline{B}} = \underline{\underline{E}} \cdot \underline{\underline{B}}$$

Dieses wenden wir auf die Matrix $\underline{\underline{A}}^t$ (der Transponierten unserer gegebenen Matrix $\underline{\underline{A}}$) an:

$$\underline{\underline{A}}^t = \underline{\underline{E}} \cdot \underline{\underline{A}}^t$$

und transponieren beide Seiten dieser Gleichung

$$\underline{\underline{A}}^{tt} = (\underline{\underline{E}} \cdot \underline{\underline{A}}^t)^t$$

Wegen $\underline{\underline{A}}^{tt} = \underline{\underline{A}}$ und $\underline{\underline{E}}^t = \underline{\underline{E}}$ folgt daraus nach Gleichung (71) auf Seite 146

$$\underline{\underline{A}} = (\underline{\underline{E}} \cdot \underline{\underline{A}}^t)^t = \underline{\underline{A}}^{tt} \cdot \underline{\underline{E}}^t = \underline{\underline{A}} \cdot \underline{\underline{E}}$$

qed.

Die Einheitsmatrix $\underline{\underline{E}}$ ist ein **links- und rechtsneutrales Element**.

Ist ein solches neutrales Element vorhanden, so stellt sich sofort die Frage nach **inversen Elementen**:
Zu $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$, $\underline{\underline{A}} \neq \underline{\underline{0}}$ ist ein $\underline{\underline{D}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit

$$\underline{\underline{A}} \cdot \underline{\underline{D}} = \underline{\underline{E}}$$

gesucht.

Man muss jedoch sogleich feststellen, dass es – im Gegensatz zu den reellen Zahlen – nicht zu jedem von Null verschiedenen Element ein Inverses gibt.

Als Beispiel betrachten wir

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$$

Setzt man hilfsweise

$$\underline{\underline{C}} = \begin{pmatrix} 3 & -1 \\ 3 & -1 \end{pmatrix}$$

so rechnet man nach:

$$\underline{\underline{C}} \cdot \underline{\underline{A}} = \underline{\underline{0}} \tag{75}$$

Angenommen, $\underline{\underline{A}}$ besitzt ein Inverses, d. h. es gibt eine Matrix $\underline{\underline{D}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit $\underline{\underline{A}} \cdot \underline{\underline{D}} = \underline{\underline{E}}$. Multipliziert man beide Seiten der Gleichung (75) von rechts mit dieser Matrix $\underline{\underline{D}}$, so folgt

$$\underline{\underline{C}} \cdot \underbrace{\underline{\underline{A}} \cdot \underline{\underline{D}}}_{=\underline{\underline{E}}} = \underbrace{\underline{\underline{0}} \cdot \underline{\underline{D}}}_{=\underline{\underline{0}}}$$

$$\Rightarrow \qquad \underline{\underline{C}} \cdot \underline{\underline{E}} = \underline{\underline{C}} = \underline{\underline{0}}$$

Widerspruch, denn nach Definition ist $\underline{\underline{C}} \neq \underline{\underline{0}}$.

Der folgende Satz gibt an, wann eine Matrix invertierbar ist; der zweite Teil seines Beweises weist darüber hinaus einen Weg, um zu einer gegebenen Matrix deren Inverse zu berechnen.

Satz:
Sei $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$. Zu $\underline{\underline{A}}$ gibt es genau dann eine Matrix $\underline{\underline{D}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit

$$\underline{\underline{A}} \cdot \underline{\underline{D}} = \underline{\underline{E}}$$

wenn $\mathrm{rg}\left(\underline{\underline{A}}\right) = n$ ist, d. h. genau dann, wenn $\underline{\underline{A}}$ vollen Rang hat.

Beweis: Zwei Richtungen sind zu zeigen.

1. Es sei eine Matrix $\underline{\underline{D}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit $\underline{\underline{A}} \cdot \underline{\underline{D}} = \underline{\underline{E}}$ vorhanden. Zu zeigen: Dann folgt $\mathrm{rg}\left(\underline{\underline{A}}\right) = n$.

   Dieses wird gezeigt, indem man nachrechnet, dass ein lineares Gleichungssystem mit Koeffizentenmatrix $\underline{\underline{A}}$ den Rang n besitzt.

   Ein quadratisches Gleichungssystem mit n Unbekannten hat genau dann den vollen Rang n, wenn es für jede rechte Seite lösbar ist (siehe auch Seite 95). Zu zeigen bleibt also, dass für jedes $\vec{b} \in \mathbb{R}^n$ eine Lösung von

   $$\underline{\underline{A}} \cdot \vec{x} = \vec{b} \tag{76}$$

   vorhanden ist. Mit Hilfe der Matrix $\underline{\underline{D}}$ kann man die Lösung sofort angeben: Diese lautet:

   $$\vec{x} = \underline{\underline{D}} \cdot \vec{b} \tag{77}$$

   Dann ist nämlich, wenn man dieses in Gleichung (76) einsetzt:

   $$\begin{aligned} \underline{\underline{A}} \cdot \vec{x} &= \underbrace{\underline{\underline{A}} \cdot \underline{\underline{D}}}_{=\underline{\underline{E}}} \cdot \vec{b} \\ &= \underline{\underline{E}} \cdot \vec{b} = \vec{b} \end{aligned}$$

   In der Tat hat man so eine Lösung von (76) für eine beliebige rechte Seite $\vec{b}$ gefunden. $\underline{\underline{A}}$ hat folglich den Rang n.

2. Jetzt werde umgekehrt vorausgesetzt, dass $\mathrm{rg}\left(\underline{\underline{A}}\right) = n$ ist; zu zeigen ist nun: es gibt ein $\underline{\underline{D}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit $\underline{\underline{A}} \cdot \underline{\underline{D}} = \underline{\underline{E}}$.

   Da $\mathrm{rg}A = n$ ist, hat ein quadratischen Gleichungssystem mit Koeffizientenmatrix $\underline{\underline{A}}$, also

   $$\underline{\underline{A}} \cdot \vec{x} = \vec{b}$$

   den Rang n und ist für jede rechte Seite $\vec{b}$ lösbar. Insbesondere lassen sich Lösungen finden, wenn man für $\vec{b}$ die n Spalten der Einheitsmatrix $\underline{\underline{E}} = (\vec{e}_1, \ldots, \vec{e}_n)$ einsetzt; dieses liefert die n Gleichungssysteme

   $$\underline{\underline{A}} \cdot \vec{x} = \vec{e}_j \qquad \text{für} \quad j = 1 \ldots n \tag{78}$$

Sei $\vec{d_j} \in \mathbb{R}^n$ jeweils die Lösung hiervon. Dann kann man schreiben

$$\underline{\underline{A}} \cdot \vec{d_j} = \vec{e_j} \qquad \text{für} \quad j = 1 \ldots n$$

Definiert man nun die Matrix $D \in \mathrm{M}^{n,n}(\mathbb{R})$ durch

$$\underline{\underline{D}} = (\vec{d_1}, \ldots, \vec{d_n})$$

so ist

$$\begin{aligned} \underline{\underline{A}} \cdot \underline{\underline{D}} &= \underline{\underline{A}} \cdot (\vec{d_1}, \ldots, \vec{d_n}) \\ &= (\underline{\underline{A}} \cdot \vec{d_1}, \ldots, \underline{\underline{A}} \cdot \vec{d_n}) \\ &= (\vec{e_1}, \ldots, \vec{e_n}) \\ &= \underline{\underline{E}} \end{aligned}$$

$\underline{\underline{D}}$ ist die gesuchte inverse Matrix zu $\underline{\underline{A}}$. qed.

Im zweiten Teil des Beweises wurde die inverse Matrix mit Hilfe linearer Gleichungssysteme gefunden. Wir kommen darauf zurück, wenn wir die Inverse einer gegebenen Matrix explizit berechnen wollen.

Ist zu $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ ein $\underline{\underline{D}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit $\underline{\underline{A}} \cdot \underline{\underline{D}} = \underline{\underline{E}}$ vorhanden, so schreibt man für $\underline{\underline{D}}$ $\underline{\underline{A}}^{-1}$ und nennt $\underline{\underline{A}}^{-1}$ die **Umkehrmatrix/inverse Matrix** zu $\underline{\underline{A}}$.

Existiert $\underline{\underline{A}}^{-1}$, so nennt man $\underline{\underline{A}}$ **umkehrbar oder invertierbar**.

Wegen der fehlenden Kommutativität der Matrizenmultiplikation taucht hier wieder ein Problem auf: Es ist zwar

$$\underline{\underline{A}} \cdot \underline{\underline{A}}^{-1} = \underline{\underline{E}}$$

Daraus folgt aber noch nicht, dass auch $\underline{\underline{A}}^{-1} \cdot \underline{\underline{A}} = \underline{\underline{E}}$ ist. Wir wissen eben bis jetzt nur, $\underline{\underline{A}}^{-1}$ ein Rechtsinverses zu $\underline{\underline{A}}$; dass $\underline{\underline{A}}^{-1}$ auch Linksinverses ist, ist eine der Aussagen des folgenden Satzes.

Satz:
Die Matrix $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ sei umkehrbar mit Umkehrmatrix $\underline{\underline{A}}^{-1}$. Dann gilt

1. Die Matrix $\underline{\underline{A}}^{-1}$ ist ebenfalls umkehrbar.
2. Ist $(\underline{\underline{A}}^{-1})^{-1}$ die (rechtsinverse) Umkehrmatrix von $\underline{\underline{A}}^{-1}$, so ist
$$(\underline{\underline{A}}^{-1})^{-1} = \underline{\underline{A}}$$
3. Es ist
$$\underline{\underline{A}}^{-1} \cdot \underline{\underline{A}} = \underline{\underline{E}}$$

Nun wissen wir, dass $\underline{\underline{A}}^{-1}$ sowohl Links- als auch Rechtsinverses zu $\underline{\underline{A}}$ ist:

$$\underline{\underline{A}}^{-1} \cdot \underline{\underline{A}} \;=\; \underline{\underline{A}} \cdot \underline{\underline{A}}^{-1} \;=\; \underline{\underline{E}}$$

Wir wollen jetzt ein **Verfahren** kennenlernen, zu $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ mit $\mathrm{rg}\left(\underline{\underline{A}}\right) = n$ die **Umkehrmatrix** $\underline{\underline{A}}^{-1}$ zu **berechnen**.
In dem Beweis des Satzes auf Seite 153 wurde das Verfahren bereits beschrieben:

Man muss die Gleichungssysteme

$$\underline{\underline{A}} \cdot \vec{x} \;=\; \vec{e}_j \tag{79}$$

für $j = 1 \ldots n$ lösen.
Dabei sind $\vec{e}_1, \ldots, \vec{e}_n$ die Spalten der Einheitsmatrix $\underline{\underline{E}} = (\vec{e}_1, \ldots, \vec{e}_n)$. Sind $\vec{d}_1, \ldots, \vec{d}_n$ die Lösungen der Gleichung (79), so ist – wie gezeigt -

$$\underline{\underline{A}}^{-1} \;=\; (\vec{d}_1, \ldots, \vec{d}_n)$$

Da sich die n Gleichungssysteme (79) nur um die rechten Seiten unterscheiden, lassen sie sich mit Hilfe des Gaußschen Verfahrens **simultan** lösen.
Man schreibt dazu die gemeinsame Koeffizientenmatrix $\underline{\underline{A}}$ und die rechten Seiten nebeneinander auf:

$$\underline{\underline{A}} \;\big|\; \vec{e}_1 \;\big|\; \vec{e}_2 \;\big|\; \cdots \;\big|\; \vec{e}_n$$

bzw. ausführlicher

$$\left(\begin{array}{ccc} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{array}\right) \left|\; \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right| \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \left|\; \cdots \;\right| \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Anschließend beginnt man mit dem Umformen nach dem Gaußschen Verfahren. Die Umformungsschritte wendet man hier nicht nur auf die eine rechte Seite, sondern auf die n rechten Seiten an. Dieses liefert die reduzierte Form der n Gleichungssysteme; sie bekommen damit die Gestalt

$$\left(\begin{array}{cccccc} 1 & \alpha_{12} & \alpha_{13} & \ldots & \alpha_{1n-1} & \alpha_{1n} \\ 0 & 1 & \alpha_{23} & \ldots & \alpha_{2n-1} & \alpha_{2n} \\ 0 & 0 & 1 & \ldots & \alpha_{3n-1} & \alpha_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & \alpha_{n-1n} \\ 0 & 0 & 0 & \vdots & 0 & 1 \end{array}\right) \;\big|\; \vec{e}_1^{\,(1)} \;\big|\; \vec{e}_2^{\,(1)} \;\big|\; \cdots \;\big|\; \vec{e}_n^{\,(1)}$$

Die $\vec{e}_1^{\,(1)}, \ldots, \vec{e}_n^{\,(1)}$ sind die umgeformten rechten Seiten. Auf der gesamten Diagonalen der reduzierten Koeffizientenmatrix müssen Einsen stehen, da ja $\left(\mathrm{rg}\underline{\underline{A}}\right) = n$ vorausgesetzt ist.

Stieße man hier auf Nullgleichungen, so wäre $\operatorname{rg}\left(\underline{\underline{A}}\right) < n$, und man könnte die Rechnung abbrechen, da $\underline{\underline{A}}$ nicht invertierbar wäre.
Wegen der Einsen auf der Diagonalen kann man die weitere Rechnung dadurch beschleunigen, dass man die Gleichungssysteme noch weiter reduziert. Die Fortsetzung des Reduktionsvorganges soll dazu führen, dass auch oberhalb der Diagonalen nur Nullen stehen. Die Vorgehensweise dabei lautet:

Als erstes zieht man für $i = 1 \ldots n-1$ das α_{in}–Fache der letzten Zeile von der i-ten Zeile ab; dieses liefert

$$\left(\begin{array}{cccccc} 1 & \alpha_{12} & \alpha_{13} & \ldots & \alpha_{1n-1} & 0 \\ 0 & 1 & \alpha_{23} & \ldots & \alpha_{2n-1} & 0 \\ 0 & 0 & 1 & \ldots & \alpha_{3n-1} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \vdots & 0 & 1 \end{array}\right) \left| \vec{e}_1^{\,(2)} \right| \vec{e}_2^{\,(2)} \left| \cdots \right| \vec{e}_n^{\,(2)}$$

Jetzt sind die Elemente der letzten Spalte außerhalb der Diagonalen alle Null. Die rechten Seiten haben sich aufgrund der Zeilensubtraktionen auch weiter verändert.

Man verfährt jetzt so weiter, indem man – von hinten beginnend – für $j = n-1 \ldots 2$ und bei festem j jeweils für $i = 1 \ldots j-1$ das α_{ij}–Fache der j-ten Zeile von der i-ten Zeile abzieht; dieses liefert die vollständig reduzierte Form

$$\left(\begin{array}{cccccc} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \vdots & 0 & 1 \end{array}\right) \left| \vec{f}_1 \right| \vec{f}_2 \left| \cdots \right| \vec{f}_n$$

Dabei sind die $\vec{f}_1, \ldots, \vec{f}_n$ die endgültig umgeformten rechten Seiten. Die Koeffizientenmatrix ist in die Einheitsmatrix verwandelt worden. Damit kann man die vollständig reduzierten Gleichungssysteme schreiben als

$$\underline{\underline{E}} \cdot \vec{x} \;=\; \vec{f}_j \qquad \text{für} \quad j = 1 \ldots n \tag{80}$$

Wegen

$$\underline{\underline{E}} \cdot \vec{f}_j \;=\; \vec{f}_j$$

sind die Lösungen von (80) und damit auch die Lösungen von (79) genau die n Spaltenvektoren $\vec{f}_1, \ldots, \vec{f}_n$. Die aus deren Zusammensetzung gebildete Matrix

$$\underline{\underline{D}} \;=\; (\vec{f}_1, \ldots, \vec{f}_n)$$

ist gerade die Umkehrmatrix von A, also

$$\underline{\underline{A}}^{-1} \;=\; (\vec{f}_1, \ldots, \vec{f}_n)$$

Im **nachfolgenden Beispiel** werden wir zunächst Schrittweise dieses gerade beschriebene Vorgehen nachvollziehen.

Beipiel: Wir wollen die Umkehrmatrix (inverse Matrix) der 3×3–Matrix

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 11 & 22 \\ 3 & 10 & 38 \end{pmatrix}$$

berechnen und schreiben dazu

$$\underline{\underline{A}} \mid \vec{e}_1 \mid \vec{e}_2 \mid \vec{e}_3$$

Ausgeschrieben lautet dies

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 3 & 1 & 0 & 0 \\ 5 & 11 & 22 & 0 & 1 & 0 \\ 3 & 10 & 38 & 0 & 0 & 1 \end{array}\right)$$

Geeignete Vielfache der ersten Zeile werden von den folgenden Zeilen abgezogen:

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 7 & -5 & 1 & 0 \\ 0 & 4 & 29 & -3 & 0 & 1 \end{array}\right)$$

Das Vierfache der zweiten wird von der letzen Zeile abgezogen:

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 7 & -5 & 1 & 0 \\ 0 & 0 & 1 & 17 & -4 & 1 \end{array}\right)$$

Jetzt setzt man die Reduzierung fort; dabei wird das 7–Fache der letzten von der zweiten und das 3–Fache der letzten von der ersten Zeile abgezogen:

$$\left(\begin{array}{ccc|c|c|c} 1 & 2 & 0 & -50 & 12 & -3 \\ 0 & 1 & 0 & -124 & 29 & -7 \\ 0 & 0 & 1 & 17 & -4 & 1 \end{array}\right)$$

Zum Schluss wird das Zweifache der zweiten Zeile von der ersten abgezogen:

$$\left(\begin{array}{ccc|c|c|c} 1 & 0 & 0 & 198 & -46 & 11 \\ 0 & 1 & 0 & -124 & 29 & -7 \\ 0 & 0 & 1 & 17 & -4 & 1 \end{array}\right)$$

Damit haben wir als Ergebnis unserer Berechnung erhalten:

$$\underline{\underline{A}}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 11 & 22 \\ 3 & 10 & 38 \end{pmatrix}^{-1} = \begin{pmatrix} 198 & -46 & 11 \\ -124 & 29 & -7 \\ 17 & -4 & 1 \end{pmatrix}$$

Jetzt werden wir das **erweiterte Gauß-Schema** zur stärkeren Formalisierung dieser Rechenschritte in Erweiterung des **Gauß-Schemas**(vergl. Seite 93) an Hand eines Beispiels einführen.

Beispiel (erweitertes Gauß-Schema):

Gegeben ist eine Matrix $\underline{\underline{A}}$ mit $rg\left(\underline{\underline{A}}\right) = n$, nämlich

$$\underline{\underline{A}} = \begin{pmatrix} -2 & -1 & 3 \\ 2 & 2 & 3 \\ 4 & 1 & -3 \end{pmatrix}$$

Das **erweiterte Gauß-Schema** ist eine Tabelle mit zwei Spalten (linke Spalte und rechte Spalte), die jeweils links und rechts eine Matrix enthält. Jede elementare Umformung der Vorwärtselimination, die simultan in der linken und rechten Spalte durchgeführt wird, erzeugt eine neue Spalte diesen Typs. Man startet in der ersten Zeile mit der Matrix $\underline{\underline{A}}$ in der linken Spalte und der Einheitsmatrix $\underline{\underline{E}}$ in der rechten Spalte (vereinfacht ohne Klammern geschrieben). Am Ende der Vorwärtselimination hat man in der linken Spalte eine Matrix in Dreiecksform (ohne Nullzeilen wegen $rg\left(\underline{\underline{A}}\right) = n$) und in der rechten Spalte eine entsprechend der Rechenoperationen der Vorwärtselimination aus der Einheitsmatrix $\underline{\underline{E}}$ entstandene Matrix $\underline{\underline{\tilde{E}}}$. (Man kann jetzt auch die Determinante $\det\left(\underline{\underline{A}}\right)$ berechnen, siehe nachfolgender Abschnitt 8.4!).

$\begin{matrix} -2 & -1 & 3 \\ 2 & 2 & 3 \\ 4 & 1 & -3 \end{matrix}$	$\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$	**Vorwärtselimination** von **oben nach unten**
$\begin{matrix} -2 & -1 & 3 \\ 0 & 1 & 6 \\ 0 & -1 & 3 \end{matrix}$	$\begin{matrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{matrix}$	II+I und III+2· I
$\begin{matrix} -2 & -1 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 9 \end{matrix}$	$\begin{matrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 3 & 1 & 1 \end{matrix}$	III+II $\underline{\underline{\tilde{E}}}$ det (A)=(-2) · 1· 9=-18, weiter im selben Schema:
$\begin{matrix} -6 & -3 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{matrix}$	$\begin{matrix} 0 & -1 & -1 \\ -3 & 1 & -2 \\ 3 & 1 & 1 \end{matrix}$	**Rücksubstitution** von **unten nach oben**
$\begin{matrix} -6 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{matrix}$	$\begin{matrix} -3 & 0 & -3 \\ -3 & 1 & -2 \\ 3 & 1 & 1 \end{matrix}$	(-2)· III+3 · II und -III+3· I
$\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$	$\begin{matrix} \frac{1}{2} & 0 & \frac{1}{2} \\ -1 & \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{9} & \frac{1}{9} \end{matrix}$	II+I „Normierung“ $\underline{\underline{A}}^{-1}$

Im zweiten Teil, der **Rücksubstitution** von **unten nach oben** haben wir von unten (mit der dritten Zeile beginnend) nach oben analog zur Vorwärtselimination die Einträge der linken Seite oberhalb der Hauptdiagonalen eliminiert („genullt“).

Abschließend wird „zeilenweise“ in beiden Spalten „normiert“, indem man jeweils durch das Hauptdiagonalelement der linken Spalte teilt.

Es ist also $\underline{\underline{A}}^{-1} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ -1 & \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{9} & \frac{1}{9} \end{pmatrix}$

Die Probe ergibt

$$\underline{\underline{A}} \cdot \underline{\underline{A}}^{-1} = \begin{pmatrix} -2 & -1 & 3 \\ 2 & 2 & 3 \\ 4 & 1 & -3 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ -1 & \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{9} & \frac{1}{9} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Mit Hilfe der Umkehrmatrix (inversen Matrix) lässt sich das Gleichungssystem

$$\underline{\underline{A}} \cdot \vec{x} = \vec{b}$$

sofort lösen. Multipliziert man beide Seiten dieser (Matrizen-) Gleichung von links mit $\underline{\underline{A}}^{-1}$:

$$\underbrace{\underline{\underline{A}}^{-1} \cdot \underline{\underline{A}}}_{=\underline{\underline{E}}} \cdot \vec{x} = \underline{\underline{A}}^{-1} \cdot \vec{b}$$

so folgt daraus sofort die eindeutige Lösung

$$\boxed{\vec{x} = \underline{\underline{A}}^{-1} \cdot \vec{b}}$$

Beispiel: Die eindeutige Lösung von

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & 11 & 22 \\ 3 & 10 & 38 \end{pmatrix} \cdot \vec{x} = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

ist

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & 11 & 22 \\ 3 & 10 & 38 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 198 & -46 & 11 \\ -124 & 29 & -7 \\ 17 & -4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 513 \\ -321 \\ 44 \end{pmatrix}$$

Die Berechnung der Umkehrmatrix ist immer dann angezeigt, wenn ein quadratisches Gleichungssystem mit vollem Rang mehrmals mit unterschiedlichen rechten Seiten zu lösen ist. Hat man die Umkehrmatrix vorliegen, dann beschränkt sich der Aufwand beim Berechnen einer Lösung auf eine einfache Multiplikation einer Matrix mit einem Vektor.

Aufgabe: Eine Diagonalmatrix ist eine $n \times n$–Matrix, deren Einträge außerhalb der Hauptdiagonalen alle gleich Null sind:

$$\underline{\underline{D}} = \begin{pmatrix} \lambda_1 & 0 & & & \\ 0 & \lambda_2 & 0 & & \\ & 0 & \ddots & 0 & \\ & & 0 & \lambda_{n-1} & 0 \\ & & & 0 & \lambda_n \end{pmatrix} \qquad \text{mit} \quad \lambda_1, \ldots, \lambda_n \in \mathbb{R}$$

Zeigen Sie: D ist genau dann umkehrbar, wenn $\lambda_j \neq 0$ für $j = 1 \ldots n$ ist, und dass in diesem Falle die Umkehrmatrix durch

$$\underline{\underline{D}}^{-1} = \begin{pmatrix} \lambda_1^{-1} & 0 & & & \\ 0 & \lambda_2^{-1} & 0 & & \\ & 0 & \ddots & 0 & \\ & & 0 & \lambda_{n-1}^{-1} & 0 \\ & & & 0 & \lambda_n^{-1} \end{pmatrix}$$

gegeben ist!

Es folgen zwei nützliche Formeln im Zusammenhang mit den Einheitsvektoren. Zu deren Herleitung schreiben wir die $n \times n$–Matrix $\underline{\underline{A}}$ und anschließend auch die Einheitsmatrix in Spaltenschreibweise:

$$\begin{aligned} \underline{\underline{A}} &= (\vec{a}_1, \ldots, \vec{a}_n) && \text{Spaltenschreibweise} \\ &= \underline{\underline{A}} \cdot \underline{\underline{E}} \\ &= \underline{\underline{A}} \cdot (\vec{e}_1, \ldots, \vec{e}_n) && \text{Spaltenschreibeise für die Einheitsmatrix} \\ &= (\underline{\underline{A}} \cdot \vec{e}_1, \ldots, \underline{\underline{A}} \cdot \vec{e}_n) \end{aligned}$$

also:

$$(\vec{a}_1, \ldots, \vec{a}_n) = (\underline{\underline{A}} \cdot \vec{e}_1, \ldots, \underline{\underline{A}} \cdot \vec{e}_n)$$

Die letzte Gleichung gibt die Gleichheit zweier Matrizen an; da zwei Matrizen genau dann gleich sich, wenn ihre entsprechenden Spalten gleich sind, liefert dieses

$$\underline{\underline{A}} \cdot \vec{e}_j = \vec{a}_j \qquad \text{für} \quad j = 1 \ldots n \tag{81}$$

Diese Gleichung besagt: die Multiplikation einer Matrix mit dem j-ten Einheitsvektor liefert die j-te Spalte der Matrix.

Jetzt werde vorausgesetzt, dass die Matrix $\underline{\underline{A}}$ umkehrbar ist. Multipliziert man die Gleichung (81) von links mit $\underline{\underline{A}}^{-1}$, so erhält man

$$\begin{aligned} \underline{\underline{A}}^{-1} \cdot \underline{\underline{A}} \cdot \vec{e}_j &= \underline{\underline{A}}^{-1} \cdot \vec{a}_j \\ \Rightarrow \qquad \vec{e}_j &= \underline{\underline{A}}^{-1} \cdot \vec{a}_j \qquad \text{für} \quad j = 1 \ldots n \end{aligned} \tag{82}$$

Der nächste Satz beschreibt den Zusammenhang zwischen Matrizenmultiplikation und Inversenbildung.

Satz:
Sind $\underline{\underline{A}}, \underline{\underline{B}} \in \mathrm{M}^{n,n}(\mathbb{R})$ zwei umkehrbare Matrizen, so ist auch ihr Produkt umkehrbar, und die Umkehrmatrix des Produktes erhält man durch

$$(\underline{\underline{A}} \cdot \underline{\underline{B}})^{-1} = \underline{\underline{B}}^{-1} \cdot \underline{\underline{A}}^{-1} \tag{83}$$

Beweis: Man zeigt, dass $\underline{\underline{B}}^{-1} \cdot \underline{\underline{A}}^{-1}$ die Umkehrmatrix von $\underline{\underline{A}} \cdot \underline{\underline{B}}$ ist, indem man ganz einfach nachrechnet, dass diese beiden Matrizen miteinander multipliziert die Einheitsmatrix ergeben:

$$\begin{aligned} (\underline{\underline{A}} \cdot \underline{\underline{B}}) \cdot (\underline{\underline{B}}^{-1} \cdot \underline{\underline{A}}^{-1}) &= (\underline{\underline{A}} \cdot \underline{\underline{B}}) \cdot (\underline{\underline{B}}^{-1} \cdot \underline{\underline{A}}^{-1}) \\ &= \underline{\underline{A}} \cdot (\underline{\underline{B}} \cdot \underline{\underline{B}}^{-1}) \cdot \underline{\underline{A}}^{-1} \\ &= \underline{\underline{A}} \cdot \underline{\underline{E}} \cdot \underline{\underline{A}}^{-1} \\ &= \underline{\underline{A}} \cdot \underline{\underline{A}}^{-1} \\ &= \underline{\underline{E}} \end{aligned}$$

qed.

Es fehlt noch der Zusammenhang zwischen Inversenbildung und Transponieren; den herzuleiten, stellen wir als
Aufgabe: Zeigen Sie mit Hilfe der Gleichung (71) auf Seite 146: Die Transponierte einer umkehrbaren Matrix ist ebenfalls umkehrbar. Die Inverse der Transponierten erhält durch

$$(\underline{\underline{A}}^t)^{-1} = (\underline{\underline{A}}^{-1})^t$$

In Worten lautet diese Gleichung: Die Inverse der Transponierten ist die Transponierte der Inversen.

8.4 Die Determinante

8.4.1 Einführung und Definition

Das Ziel dieses Abschnittes besteht darin, eine Funktionen von der Menge der **quadratischen n–reihigen Matrizen**[19] in die Menge der reellen Zahlen, d. h. eine Funktion

$$det: \ \mathrm{M}^{n,n}(\mathbb{R}) \ \mapsto \ \mathbb{R}$$

zu finden, die „gute rechnerische Eigenschaften“ besitzt und für die gilt

$$det(\underline{\underline{A}}) \begin{cases} \neq 0 & \text{falls } \underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R}) \text{ umkehrbar ist} \\ = 0 & \text{sonst} \end{cases}$$

Diese Funktion ist dann die sogenannte Determinante.

Beispiel: Wir betrachten die 2×2–Matrix

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

und dazu das Gleichungssystem

$$A \cdot \vec{x} \ = \ \vec{b}$$

mit der rechten Seite $\vec{b} = (b_1, b_2)^t$. Ausgeschrieben lautet dieses Gleichungssystem

$$\begin{aligned} a_{11}x_1 \ + \ a_{12}x_2 \ &= \ b_1 \\ a_{21}x_1 \ + \ a_{22}x_2 \ &= \ b_2 \end{aligned}$$

Wir versuchen dieses Gleichungssystem zu lösen, indem wir hier die erste Gleichung mit a_{21} und die zweite Gleichung mit a_{11} multiplizieren:

$$\begin{aligned} a_{11}a_{21}x_1 \ + \ a_{12}a_{21}x_2 \ &= \ b_1a_{21} \\ a_{11}a_{21}x_1 \ + \ a_{11}a_{22}x_2 \ &= \ b_2a_{11} \end{aligned}$$

und anschließend die erste Gleichung von der zweiten abziehen:

$$\begin{aligned} a_{11}a_{21}x_1 \ + \ a_{12}a_{21}x_2 \ &= \ b_1a_{21} \\ \underbrace{(a_{11}a_{22} - \ a_{12}a_{21})}_{d} x_2 \ &= \ b_2a_{11} - b_1a_{21} \end{aligned}$$

Man sieht leicht, dass das Gleichungssystem genau dann für jede Wahl von $\vec{b} = (b_1, b_2)^t$ lösbar ist und folglich den vollen Rang $r = 2$ besitzt, wenn $d \neq 0$ ist. Man setzt daher für 2×2–Matrix A:

$$det\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) \ = \ \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \ = \ a_{11}a_{22} - \ a_{12}a_{21} = d$$

[19] **Merke: Determinanten sind nur für quadratische Matrizen definiert !!**

Wir machen zunächst folgende

Definition: (**Determinante einer** 1×1–**Matrix bzw. einer** 2×2–**Matrix** A)

1. Für $\underline{\underline{A}} = (a) \in \mathrm{M}^{1,1}(\mathbb{R}) = \mathbb{R}$ ist $det(\underline{\underline{A}}) = a$
2. Für $\underline{\underline{A}} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{M}^{2,2}(\mathbb{R})$ ist $det(\underline{\underline{A}}) = a_{11}a_{22} - a_{12}a_{21}$

Diese Definition der Determinanten soll nun auf $\mathrm{M}^{n,n}(\mathbb{R})$ für beliebiges $n \in \mathbb{N}$ verallgemeinert werden [20]. Dabei hilft folgende

Definition:[21]
Sei $\underline{\underline{A}}$ eine $n \times n$–Matrix. Dann setzt man für $1 \leq i, j \leq n$

$$\begin{array}{lcl} \underline{\underline{A_{ij}}} & : & \text{die } (n-1) \times (n-1)\text{-Matrix, die entsteht,} \\ & & \text{wenn man bei der } n \times n\text{–Matrix } \underline{\underline{A}} \text{ die } i\text{-te} \\ & & \text{Spalte und die } j\text{-te Zeile streicht.} \\ U_{ij} & = & \det \underline{\underline{A_{ij}}} \end{array} \tag{84}$$

Beispiel: Für $\underline{\underline{A}} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{M}^{2,2}(\mathbb{R})$ ist

$\underline{\underline{A_{11}}} = (a_{22})$ und damit $U_{11} = det(\underline{\underline{A_{11}}}) = a_{22}$

$\underline{\underline{A_{12}}} = (a_{12})$ und damit $U_{12} = det(\underline{\underline{A_{12}}}) = a_{12}$

$\underline{\underline{A_{21}}} = a_{21}$ und damit $U_{21} = det(\underline{\underline{A_{21}}}) = a_{21}$

$\underline{\underline{A_{22}}} = a_{11}$ und damit $U_{22} = det(\underline{\underline{A_{22}}}) = a_{11}$

Damit erhält man folgende Darstellung der Determinante einer 2×2–Matrix $\underline{\underline{A}}$:

$$det(\underline{\underline{A}}) = a_{11}a_{22} - a_{12}a_{21} = +a_{11} \cdot U_{11} - a_{12} \cdot U_{21}$$

Dies ist eine **alternierende Summe**, d.h. aufeinander folgende Summanden haben **„wechselndes Vorzeichen“**. Dabei richtet sich das Vorzeichen, d.h. der **Faktor +1 oder -1** nach der Summe der Indizes von A_{ij}: Das „Vorzeichen“ entspricht $(-1)^{i+j}$ also

[20] Dabei wird auf die exakte mathematische Herleitung verzichtet zu Gunsten einer pragmatischen (heuristischen) Herangehensweise!

[21] Man beachte, dass hier der erste Index i die Spalte und der zweite Index j die Zeile zählt!

$det(\underline{\underline{A}}) = a_{11}a_{22} - a_{12}a_{21} = +a_{11} \cdot U_{11} - a_{12} \cdot U_{21} = (-1)^{1+1} \cdot a_{11} \cdot U_{11} + (-1)^{1+2} \cdot a_{12} \cdot U_{21} = \sum_{j=1}^{2} (-1)^{1+j} \cdot a_{1j} \cdot U_{j1}$

Damit haben wir alles bereitgestellt, um (allgemein) die Determinante einer $n \times n$–Matrix A zu definieren:

Definition: (**Determinante einer** $n \times n$**–Matrix** A)

$$\det\left(\underline{\underline{A}}\right) = \sum_{j=1}^{n} (-1)^{1+j} \cdot a_{1j} \cdot U_{j1}$$

Diese Definition ist eine **Entwicklung (nach der ersten Zeile)** in eine Summe von Unterdeterminanten!

Bemerkung: Diese Definition ermöglicht das **rekursive Berechnen** der Determinante einer $n \times n$–Matrix $\underline{\underline{A}}$: Im ersten Schritt erhält man eine Summe mit n Summanden. Jeder Summand enthält eine Determinante U_{1j} einer $n-1 \times n-1$–Matrix $\underline{\underline{\underline{\underline{A}}}}_{1j}$. Jede dieser n Determinanten U_{1j} liefert dann eine Summe mit n-1 Summanden, die jeweils eine Determinante einer $n-2 \times n-2$–Matrix enthalten. Dieser Prozess wird fortgeführt, bis nach n-2 Schritten nur noch Summanden mit Determinanten einer 2×2–Matrix übrig bleiben. Diese Determinanten werden dann explizit berechnet! Zur praktischen Berechnung der Determinanten wird die obige Darstellung nur bei 2×2–Matrizen verwendet. Für $n \times n$–Matrizen mit $n \geq 2$ sind zur Determinantenberechnung geeignetere Verfahren vorhanden (siehe später).

Beispiel:
Die folgende Determinante wird mit dem Verfahren der Entwicklung nach der ersten Zeile berechnet:

$$\begin{aligned}
&\det \begin{pmatrix} -4 & 2 & -1 \\ 3 & 1 & 2 \\ 4 & 2 & 0 \end{pmatrix} \\
&= +(-4) \cdot \det \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} - 2 \cdot \det \begin{pmatrix} 3 & 2 \\ 4 & 0 \end{pmatrix} + (-1) \cdot \det \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} \\
&= -4 \cdot (1 \cdot 0 - 2 \cdot 2) - 2 \cdot (3 \cdot 0 - 2 \cdot 4) - 1 \cdot (3 \cdot 2 - 1 \cdot 4) \\
&= (-4) \cdot (-4) - 2 \cdot (-8) - 2 \\
&= 30
\end{aligned}$$

Dass zur Entwicklung der Determinante die erste Zeile als Entwicklungszeile verwendet wurde, ist nicht zwingend. Man kann jede andere (besonders "günstige") Zeile oder Spalte dafür auswählen! Dies regelt der folgende

Satz[22] (**Entwicklungssatz**)
Sei $\underline{\underline{A}}$ eine $n \times n$–Matrix. Dann gilt:

- Entwicklung nach der i**-ten Spalte**:

$$\det\left(\underline{\underline{A}}\right) = \sum_{j=1}^{n}(-1)^{j+i}a_{ji}U_{ij} \tag{85}$$

- Entwicklung nach der j**-ten Zeile**:

$$\det\left(\underline{\underline{A}}\right) = \sum_{i=1}^{n}(-1)^{j+i}a_{ji}U_{ij} \tag{86}$$

Beispiel:
Die folgende Determinante wird mit dem Entwicklungssatz berechnet. **Da die zweite Spalte eine Null enthält, wird nach dieser entwickelt**:

$$\begin{aligned}
&\det\begin{pmatrix}3&1&2\\7&0&2\\1&2&0\end{pmatrix}\\
&= -1\cdot\det\begin{pmatrix}7&2\\1&0\end{pmatrix} + 0\cdot\det\begin{pmatrix}3&2\\1&0\end{pmatrix} - 2\cdot\det\begin{pmatrix}3&2\\7&2\end{pmatrix}\\
&= -1\cdot(7\cdot 0-2\cdot 1) + 0 - 2\cdot(3\cdot 2-7\cdot 2)\\
&= 18
\end{aligned}$$

Im Folgenden erweist es sich wieder als vorteilhaft, eine $n \times n$–Matrix in Spaltenschreibweise darzustellen:

$$\underline{\underline{A}} = (\vec{a}_1,\ldots,\vec{a}_n) \qquad \text{mit Spaltenvektoren} \quad \vec{a}_i \in \mathbb{R}^n \quad \text{für} \quad i=1,\ldots,n$$

und die Determinante als Funktion der n Spaltenvektoren aufzufassen:

$$\det\left(\underline{\underline{A}}\right) = \det(\vec{a}_1,\ldots,\vec{a}_n)$$

[22] Ohne Beweis

Man erhält damit folgenden
Satz: (Eigenschaften der Determinante)[23]

1. Für die **Determinante der Einheitsmatrix** ist
$$\det\left(\underline{\underline{E}}\right) = 1$$
2. **Multipliziert man eine der Spalten** $\vec{a}_j$ mit einem **reellen Faktor**, so kann man diesen Faktor aus der Determinanten herausziehen:
Für $\lambda \in \mathbb{R}$ und $1 \leq j \leq n$ gilt:
$$\det(\vec{a}_1, \ldots, \lambda \cdot \vec{a}_j, \ldots, \vec{a}_n) = \lambda \cdot \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_n)$$
3. Ist eine der **Spalten eine Summe**, so kann man „die Addition aus der Determinanten herausziehen“: Hat die j-te Spalte die Gestalt $\vec{a}_j = \vec{u}_j + \vec{v}_j$, so gilt
$$\det(\vec{a}_1, \ldots, \vec{u}_j + \vec{v}_j, \ldots, \vec{a}_n) =$$
$$\det(\vec{a}_1, \ldots, \vec{u}_j, \ldots, \vec{a}_n) + \det(\vec{a}_1, \ldots, \vec{v}_j, \ldots, \vec{a}_n)$$
4. Sind **zwei Spalten der Matrix gleich**, so ist der Wert ihrer Determinanten Null; steht etwa die j-te Spalte auch an der i-ten Stelle mit $i \neq j$, so hat man:
$$\det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \underbrace{\vec{a}_j}_{i\text{-te Stelle}}, \ldots, \vec{a}_n) = 0$$
5. **Vertauscht man zwei Spalten**, so ändert der Wert der Determinanten sein Vorzeichen: für $i \neq j$ ist
$$\det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_i, \ldots, \vec{a}_n) = -\det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_n)$$
6. **Transponieren** verändert die Determinante nicht $\det\left(\underline{\underline{A}}^t\right) = \det\left(\underline{\underline{A}}\right)$
7. Die **Determinante des Produkts zweier Matrizen** ist das **Produkt der Determinanten** der beiden Matrizen $\det\left(\underline{\underline{A}} \cdot \underline{\underline{B}}\right) = \det\left(\underline{\underline{A}}\right) \cdot \det\left(\underline{\underline{B}}\right)$

Bemerkungen:

- Die erste Eigenschaft ist die sogenannte **Normierung**.
- Eigenschaft 2) und 3) zusammen werden als **Linearität in den Spalten** bezeichnet.
Aus Eigenschaft zwei folgt insbesondere für einen reellen Faktor λ, der bei allen n Spalten steht:
$$\det(\lambda \cdot \vec{a}_1, \ldots, \lambda \cdot \vec{a}_j, \ldots, \lambda \cdot \vec{a}_n) = \lambda^n \cdot \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_n)$$

[23] Ohne Beweis! Für 2×2–Matrix sind die Eigenschaften elementar nachzurechnen!

- Man kann zeigen, dass die beiden Eigenschaften 4) und 5) äquivalent sind; man bezeichnet sie als **Alternierend in den Spalten**.

Es folgt aus den fünf Eigenschaften sofort, dass eine Matrix $\underline{\underline{A}}$, von deren Spalten eine nur Nullen enthält, die Determinante Null besitzt: Gilt etwa für die j-te Spalte $\vec{a}_j = \vec{0}$, so ändert sich nichts, wenn man diese mit 0 multipliziert: $0 \cdot \vec{a}_j = \vec{0} = \vec{a}_j$, und man kann schließen:

$$\begin{aligned} \det\left(\underline{\underline{A}}\right) &= \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_n) \\ &= \det(\vec{a}_1, \ldots, 0 \cdot \vec{a}_j, \ldots, \vec{a}_n) \\ &= 0 \cdot \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_n) \\ &= 0 \cdot \det A \;=\; 0 \end{aligned}$$

Hierbei wurde verwendet, dass man den Faktor 0 nach Eigenschaft 2) herausziehen kann. Aus den Eigenschaften 2), 3) und 4) folgt gemeinsam **die wichtige Regel, dass sich der Wert der Determinanten nicht ändert, wenn man von einer Spalte das Vielfache einer anderen abzieht**; es gilt nämlich für $i \neq j$

$$\begin{aligned} &\det(\vec{a}_1, \ldots, \vec{a}_i - \lambda\vec{a}_j, \ldots, \vec{a}_j, \ldots, \vec{a}_n) \\ &\quad= \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_n) + \det(\vec{a}_1, \ldots, -\lambda\vec{a}_j, \ldots, \vec{a}_j, \ldots, \vec{a}_n) \\ &\quad= \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_n) - \lambda \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_j, \ldots, \vec{a}_n) \\ &\quad= \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_n) \end{aligned} \tag{87}$$

Hier wurde als erstes die Determinante nach Eigenschaft 3) auseinandergezogen; anschließend wurde mit Eigenschaft 2) der Faktor $-\lambda$ aus dem zweiten Summanden herausgezogen; in der letzten Zeile hat die zweite Determinante wegen der doppelt vorkommenden Spalte $\vec{a}_j$ nach Eigenschaft 4) den Wert Null.

8.4.2 Berechnung der Determinante mit dem Gauß-Algorithmus

Selbstverständlich könnte man die Determinante mit Hilfe der Darstellung aus der Definition oder mit Hilfe des Entwicklungssatzes berechnen. Aus praktischen Gründen und hinsichtlich des Rechenaufwandes ist aber häufig eine Berechnung beruhend auf dem Gaußschen Eliminationsverfahren vorzuziehen.

Zunächst erhalten wir aus dem Entwicklungssatz folgende Regeln:

Satz:
Sei $\underline{\underline{A}} \in \mathrm{M}^{n,n}(\mathbb{R})$ eine Matrix, die in der ersten Spalte ab dem zweiten Eintrag nur Nullen enthält. Eine solche Matrix $\underline{\underline{A}}$ hat die Gestalt

$$\underline{\underline{A}} = \left(\begin{array}{c|ccc} a_{11} & a_{12} & \ldots & a_{1n} \\ \hline 0 & & & \\ \vdots & & \underline{\underline{A_1}} & \\ 0 & & & \end{array}\right)$$

mit der $(n-1) \times (n-1)$-Matrix

$$\underline{\underline{A_1}} = \begin{pmatrix} a_{22} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Dann gilt für die Determinante von A:

$$\det\left(\underline{\underline{A}}\right) = a_{11} \cdot \det\left(\underline{\underline{A_1}}\right)$$

Satz:
Sei A eine **obere Dreiecksmatrix:** Eine obere Dreiecksmatrix ist eine Matrix, die unterhalb der Hauptdiagonalen nur Nullen besitzt.

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

Für eine solche Matrix A gilt:

$$\det\left(\underline{\underline{A}}\right) = a_{11} \cdot a_{22} \cdots a_{nn}$$

$\det\left(\underline{\underline{A}}\right)$ ist gerade das **Produkt der Diagonalelemente**.

Folgerung: Sei $\underline{\underline{A}}$ eine untere Dreiecksmatrix:

$$\underline{\underline{A}} = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Für eine solche Matrix gilt ebenfalls:

$$\det\left(\underline{\underline{A}}\right) = a_{11} \cdot a_{22} \cdots a_{nn}$$

Beweis: Folgt sofort wegen $\det\left(\underline{\underline{A}}^t\right) = \det\left(\underline{\underline{A}}\right)$.

Damit erhalten wir den folgenden **Zusammenhang zwischen der Existenz einer inversen Matrix und der Determinante der Matrix**:

Satz:
Eine $n \times n$–Matrix ist genau dann umkehrbar, wenn ihre Determinante ungleich Null ist.

Beweis: Die Bezeichnungen von eben werden verwendet:

$\underline{\underline{A}}$ ist umkehrbar $\Leftrightarrow$ Der Rang von $\underline{\underline{A}}$ beträgt n.
$\Leftrightarrow$ Die Stufen in der reduzierten Form verlaufen auf der Hauptdiagonalen
$\Leftrightarrow$ $a_{ii} \neq 0$ für $i = 1, \ldots, n$
$\Leftrightarrow$ $\det\left(\underline{\underline{A}}\right) = \pm a_{11} \cdot a_{22} \cdots a_{nn} \neq 0$

qed.

Beispiel: Wir wollen mit dem Gaußschen Verfahren die Determinante der 3×3–Matrix

$$\underline{\underline{A}} = \begin{pmatrix} 0 & 2 & 7 \\ 1 & 2 & 3 \\ 2 & 0 & 1 \end{pmatrix}$$

berechnen:

$$\det \begin{pmatrix} 0 & 2 & 7 \\ 1 & 2 & 3 \\ 2 & 0 & 1 \end{pmatrix}$$
Die ersten beiden Zeilen vertauschen.

$$= -\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 7 \\ 2 & 0 & 1 \end{pmatrix}$$
Das Zweifache der ersten Gleichung von der letzten abziehen.

$$= -\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 7 \\ 0 & -4 & -5 \end{pmatrix}$$
Das Zweifache der zweiten Gleichung zu der letzten hinzuzählen.

$$= -\det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 7 \\ 0 & 0 & 9 \end{pmatrix}$$
Jetzt kann das Produkt der Diagonalelemente genommen werden.

$$= -1 \cdot 2 \cdot 9 = -18$$

Zum Abschluss dieses Abschnitts folgen einige Bemerkungen zu den Verfahren zur Determinantenberechnung:

Entwicklungssatz: Der Nachteil besteht darin, dass ungefähr $n!$ Multiplikationen notwendig sind. Man nimmt den Entwicklungssatz nur bei kleinen Dimensionen (bis Dimension 3) oder bei Matrizen, die sehr viele Nullen enthalten. Man entwickelt dann stets nach der Zeile oder Spalte, die die meisten Nullen enthält.

Gaußsches Verfahren: Diese Methode bietet sich immer an. Da die Anzahl der notwendigen Multiplikationen – wie man zeigen kann – von der Größenordnung n^2 ist,

ist für größere n das Gaußsche Verfahren von erheblich geringerem Aufwand als der Entwicklungssatz.

Mitunter empfiehlt sich auch eine Verbindung von Entwicklungssatz und Gaußschem Verfahren: Enthält bei größerem n eine Zeile oder eine Spalte viele Nullen, so entwickelt man zunächst nach dieser Spalte bzw. Zeile und wendet dann das Gaußsche Verfahren auf die Unterdeterminanten U_{ij} an.

Sarrus-Regel [24] Für 3×3-Matrizen gibt es noch ein Verfahren, das zwar bezüglich der Multiplikationen noch etwas aufwendiger als der Entwicklungssatz ist, das aber wegen seines leicht zu merkenden Schemas oft genommen wird. Man schreibt dazu die ersten beiden Spalten der Determinanten noch einmal hinter die dritte Spalte und bildet die Summe bzw. Differenz aus den Produkten, die aus drei auf einer Schrägen liegenden Einträgen bestehen:

$$\begin{array}{ccc|cc} + & + & + & & \\ a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \\ - & - & - & & \end{array}$$

$$\begin{aligned} \text{damit ist} \quad \det\left(\underline{\underline{A}}\right) \quad = \quad & + a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ & - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12} \end{aligned}$$

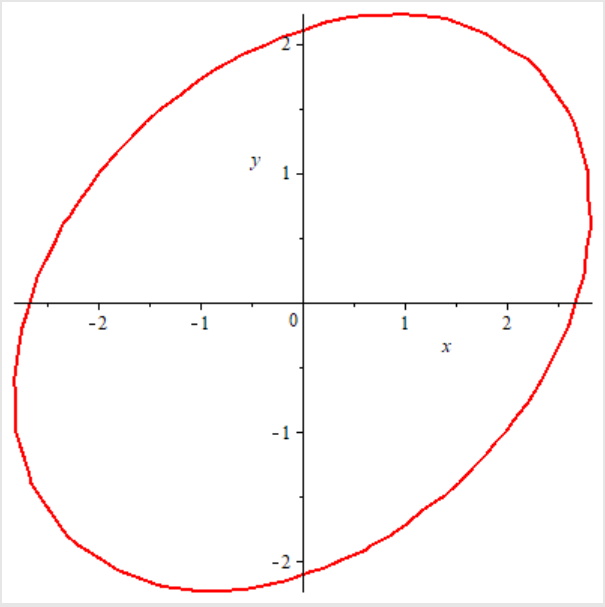
8.5 Eigenwerte und Eigenvektoren

Wir betrachten im Folgenden immer **quadratische Matrizen**, also $\underline{\underline{A}} \in M^{n,n}(\mathbb{R})$ für $n \in \mathbb{N}, n \geq 2$.

8.5.1 Einführung

Beispiel:
Die Menge $E = \{(x, y) \in \mathbb{R}^2 \mid 5x^2 - 4xy + 8y^2 - 36 = 0\}$ ist eine **Ellipse** im $\mathbb{R}^2$.

[24] **Gilt nur für 3×3–Matrix !!**



In welche Richtung zeigen die beiden Hauptachsen dieser Ellipse? Was hat das mit Matrizen zu tun?

Wir definieren die Matrix $\underline{\underline{A}} = \begin{pmatrix} 5 & -2 \\ -2 & 8 \end{pmatrix}$ und den Vektor $\vec{x} = \begin{pmatrix} x \\ y \end{pmatrix}$, dann gilt:

$$< \vec{x}, \underline{\underline{A}} \cdot \vec{x} > -36 = \vec{x} \cdot (\underline{\underline{A}} \cdot \vec{x}) - 36 = \underbrace{5x^2 - 4xy + 8y^2}_{=<\vec{x}, \underline{\underline{A}} \cdot \vec{x}>} - 36 = 0$$

8.5.2 Definitionen und Eigenwertberechnung

Gegeben ist $\underline{\underline{A}} \in M^{n,n}(\mathbb{R})$ und die Einheitsmatrix $\underline{\underline{E}} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ in $M^{n,n}$.

Definition:

Für die Matrix $\underline{\underline{A}} \in M^{n,n}(\mathbb{R})$ ist definiert:

1) Eine Zahl $\lambda \in \mathbb{R}$ heißt **Eigenwert der Matrix $\underline{\underline{A}}$** falls gilt:
   $\exists \vec{v} \in \mathbb{R}^n$, $\vec{v} \neq \vec{0}$ mit $\underline{\underline{A}} \cdot \vec{v} = \lambda \cdot \vec{v}$.

2) Jeder Vektor $\vec{v} \in \mathbb{R}^n$, $\vec{v} \neq \vec{0}$ mit $\underline{\underline{A}} \cdot \vec{v} = \lambda \cdot \vec{v}$ heißt **Eigenvektor der Matrix $\underline{\underline{A}}$ zum Eigenwert λ**

3) Das Polynom $p(\lambda) = det(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}})$ heißt **charakteristisches Polynom** der Matrix $\underline{\underline{A}}$.

Was liefert das charakteristische Polynom?

$\vec{v} \neq \vec{0}$ ist Eigenvektor zum Eigenwert λ, wenn $\vec{v}$ gilt

$\underline{\underline{A}} \cdot \vec{v} = \lambda \cdot \vec{v} \Leftrightarrow (\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}) \cdot \vec{v} = \vec{0}$,

d.h. $\vec{v}$ löst das **homogene lineare Gleichungssystem** $(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}) \cdot \vec{v} = \vec{0}$.

Dieses homogene lineare Gleichungssystem hat nur dann **Lösungen** $\vec{v} \neq \vec{0}$, wenn gilt: $p(\lambda) = det(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}) = 0$,d.h.

Die Nullstellen des charakteristischen Polynoms einer Matrix sind Eigenwerte der Matrix.

Beispiel:

Für die Matrix $\underline{\underline{A}} = \begin{pmatrix} 5 & -2 \\ -2 & 8 \end{pmatrix}$ erhält man mit $\underline{\underline{E}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ das charakteristische Polynom $p(\lambda) = det(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}) = det \begin{pmatrix} 5-\lambda & -2 \\ -2 & 8-\lambda \end{pmatrix} = (5-\lambda) \cdot (8-\lambda) - (-2) \cdot (-2) = 40 - 5 \cdot \lambda - 8 \cdot \lambda + \lambda^2 - 4 = \lambda^2 - 13 \cdot \lambda + 36$
Kandidaten für Eigenwerte liefern also die Lösungen der Gleichung $p(\lambda) = 0 \Leftrightarrow \lambda^2 - 13 \cdot \lambda + 36 = 0$ mit den Lösungen $\lambda_{1,2} = \frac{13}{2} \pm \sqrt{\left(\frac{13}{2}\right)^2 - 36} = \frac{13}{2} \pm \sqrt{\left(\frac{169}{4}\right) - \frac{144}{4}} = \frac{13}{2} \pm \sqrt{\frac{25}{4}} = \frac{13}{2} \pm \frac{5}{2} \Leftrightarrow \lambda_1 = 4 \vee \lambda_2 = 9$.

Eigenwerte der Matrix $\underline{\underline{A}}$ sind also $\lambda_1 = 4$ und $\lambda_2 = 9$.

8.5.3 Berechnung der Eigenvektoren

Zur Berechnung der Eigenvektoren zum Eigenwert λ muss man das **homogene lineare Gleichungssystem** $(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}) \cdot \vec{v} = \vec{0}$ lösen.
Jede Lösung $\vec{v} \neq \vec{0}$ ist ein Eigenvektor der Matrix $\underline{\underline{A}}$ zum Eigenwert λ.

Beispiel:

Für die Matrix $\underline{\underline{A}} = \begin{pmatrix} 5 & -2 \\ -2 & 8 \end{pmatrix}$ erhält man mit $\underline{\underline{E}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$:

a) Zum Eigenwert $\lambda_1 = 4$:
$(\underline{\underline{A}} - 4 \cdot \underline{\underline{E}}) \cdot \vec{v} = \vec{0} \Leftrightarrow \begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
Mit $v_2 = t, t \in \mathbb{R}$ erhält man $v_1 = 2 \cdot t$ und damit $\vec{v} = \begin{pmatrix} 2t \\ t \end{pmatrix} = t \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix}$

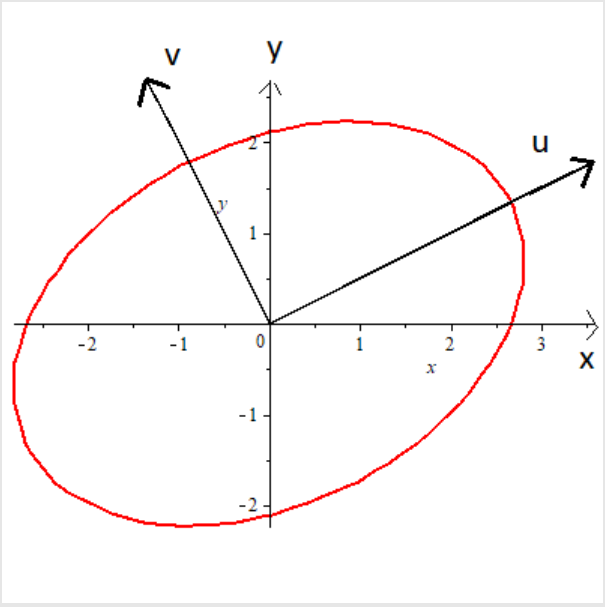
Die **Menge der Eigenvektoren** zum Eigenwert $\lambda_1 = 4$ ist damit
$E_1 = \{t \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} \mid t \in \mathbb{R}, t \neq 0\}$.

b) Zum Eigenwert $\lambda_2 = 9$:
$(\underline{\underline{A}} - 9 \cdot \underline{\underline{E}}) \cdot \vec{v} = \vec{0} \Leftrightarrow \begin{pmatrix} -4 & -2 \\ -2 & -1 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} -4 & -2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
Mit $v_2 = t, t \in \mathbb{R}$ erhält man $v_1 = -\frac{1}{2} \cdot t$ und damit $\vec{v} = \begin{pmatrix} -\frac{1}{2} \cdot t \\ t \end{pmatrix} = t \cdot \begin{pmatrix} -\frac{1}{2} \\ 1 \end{pmatrix}$
Die **Menge der Eigenvektoren** zum Eigenwert $\lambda_2 = 9$ ist damit
$E_1 = \{t \cdot \begin{pmatrix} -\frac{1}{2} \\ 1 \end{pmatrix} \mid t \in \mathbb{R}, t \neq 0\}$.

In der Menge der Eigenvektoren zeichnet man besondere Vektoren aus:

Definition:
Ein **normierter Eigenvektor** $\vec{v}$ zum Eigenwert λ der Matrix $\underline{\underline{A}}$ ist jeder Eigenvektor mit Betrag 1, also $\vec{v} \in \mathbb{R}^n$ mit $\underline{\underline{A}} \cdot \vec{v} = \lambda \cdot \vec{v}$ und $|\vec{v}| = 1$.

Beispiel:
Für die Matrix $\underline{\underline{A}} = \begin{pmatrix} 5 & -2 \\ -2 & 8 \end{pmatrix}$ erhält man für den Eigenwert $\lambda_1 = 4$:
$\vec{v} = \begin{pmatrix} 2t \\ t \end{pmatrix} \Rightarrow 1 = |\vec{v}| = 4t^2 + t^2 = 5t^2 \Rightarrow t = \frac{1}{\sqrt{5}}$
Ein normierter Eigenvektor ist also $\vec{v}_1 = \begin{pmatrix} \frac{2}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} \end{pmatrix}$
Zum Eigenwert $\lambda_2 = 9$ erhält man:
$\vec{v} = \begin{pmatrix} -\frac{1}{2} \cdot t \\ t \end{pmatrix} \Rightarrow 1 = |\vec{v}| = \frac{1}{4}t^2 + t^2 = \frac{5}{4}t^2 \Rightarrow t = \frac{2}{\sqrt{5}}$.
Ein normierter Eigenvektor ist also $\vec{v}_2 = \begin{pmatrix} -\frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{pmatrix}$
Das folgende Bild zeigt die Ellipse aus der Einführung mit zwei Strecken in Richtung der beiden normierten Eigenvektoren;
man erkennt, dass diese Strecken in **Richtung der Hauptachsen der Ellipse** liegen.



Beispiel:

Eigenwerte und Eigenvektoren einer Matrix $A \in M^{3,3}$:

Gegeben ist die Matrix $\underline{\underline{A}} = \begin{pmatrix} 0 & -1 & 3 \\ 2 & 3 & 3 \\ 2 & 1 & 1 \end{pmatrix}$.

Berechnen Sie die **Eigenwerte** und **Eigenvektoren** von $\underline{\underline{A}}$.

$$\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}} = \begin{pmatrix} 0 & -1 & 3 \\ 2 & 3 & 3 \\ 2 & 1 & 1 \end{pmatrix} - \lambda \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -\lambda & -1 & 3 \\ 2 & 3-\lambda & 3 \\ 2 & 1 & 1-\lambda \end{pmatrix} \Rightarrow$$

$$\det\left(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}\right) = -\lambda \cdot \begin{vmatrix} 3-\lambda & 3 \\ 1 & 1-\lambda \end{vmatrix} - (-1) \cdot \begin{vmatrix} 2 & 3 \\ 2 & 1-\lambda \end{vmatrix} + 3 \cdot \begin{vmatrix} 2 & 3-\lambda \\ 2 & 1 \end{vmatrix}$$
$$= -\lambda \cdot ((3-\lambda) \cdot (1-\lambda) - 3) + (2 \cdot (1-\lambda) - 6) + 3 \cdot (2 - 2 \cdot (3-\lambda))$$
$$= -\lambda \cdot (3 - 4\lambda + \lambda^2 - 3) - 2\lambda - 4 + 3 \cdot (-4 + 2\lambda)$$
$$= -\lambda^3 + 4\lambda^2 + 4\lambda - 16 = -\lambda^3 + 4\lambda + 4\lambda^2 - 16$$
$$= -\lambda \cdot (\lambda^2 - 4) + 4 \cdot (\lambda^2 - 4) = (\lambda^2 - 4) \cdot (4 - \lambda) \Rightarrow$$
$$\det\left(\underline{\underline{A}} - \lambda \cdot \underline{\underline{E}}\right) = 0 \text{ für } \lambda_1 = -2,\ \lambda_2 = 2,\ \lambda_3 = 4$$

Die Eigenwerte von $\underline{\underline{A}}$ sind also $\lambda_1 = -2,\ \lambda_2 = 2,\ \lambda_3 = 4$.
Zum Eigenwert $\lambda_1 = -2$ gehören die Lösungen des lin. Gleichungssystems

$\left(\underline{\underline{A}} - (-2) \cdot \underline{\underline{E}}\right) \cdot \vec{x} = \vec{0} \Leftrightarrow \begin{pmatrix} 2 & -1 & 3 \\ 2 & 5 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ als Eigenvektoren.

$\lambda_1 = -2$

2	−1	3	0
2	5	3	0
2	1	3	0
2	−1	3	0
0	6	0	0
0	2	0	0

damit folgt: $x_2 = 0,\ x_3 = s,\ x_1 = -\frac{3}{2}s$.

Die Lösungsmenge (Menge der Eigenvektoren) ist $E_1 = \left\{ s \cdot \begin{pmatrix} -3/2 \\ 0 \\ 1 \end{pmatrix} \middle| \quad s \in \mathbb{R}\backslash\{0\} \right\}$

Zum Eigenwert $\lambda_2 = 2$ gehören die Lösungen des lin. Gleichungssystems

$\left(\underline{\underline{A}} - 2 \cdot \underline{\underline{E}}\right) \cdot \vec{x} = \vec{0} \Leftrightarrow \begin{pmatrix} -2 & -1 & 3 \\ 2 & 1 & 3 \\ 2 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ als Eigenvektoren.

$\lambda_2 = 2$

−2	−1	3	0
2	1	3	0
2	1	−1	0
−2	−1	3	0
0	0	6	0
0	0	2	0

damit folgt: $x_3 = 0,\ x_2 = t,\ x_1 = -\frac{1}{2}t$.

Die Lösungsmenge (Menge der Eigenvektoren) ist

$E_2 = \left\{ t \cdot \begin{pmatrix} -1/2 \\ 1 \\ 0 \end{pmatrix} \middle| \quad t \in \mathbb{R}\backslash\{0\} \right\}$

Zum Eigenwert $\lambda_3 = 4$ gehören die Lösungen des lin. Gleichungssystems

$\left(\underline{\underline{A}} - 4 \cdot \underline{\underline{E}}\right) \cdot \vec{x} = \vec{0} \Leftrightarrow \begin{pmatrix} -4 & -1 & 3 \\ 2 & -1 & 3 \\ 2 & 1 & -3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ als Eigenvektoren.

$\lambda_3 = 4$

-4	-1	3	0
2	-1	3	0
2	1	-3	0
-4	-1	3	0
0	-3	9	0
0	1	-3	0
-4	-1	3	0
0	-3	9	0
0	0	0	0

damit folgt: $x_3 = r,\ x_2 = 3r,\ x_1 = 0.$

Die Lösungsmenge (Menge der Eigenvektoren) ist $E_3 = \left\{ r \cdot \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix} \middle| \quad r \in \mathbb{R}\backslash\{0\} \right\}$

8.6 Diagonalisierbarkeit von Matrizen

Definition:

Eine **Diagonalmatrix** ist eine $n \times n$–Matrix, deren Einträge außerhalb der Hauptdiagonalen alle gleich Null sind:

$$\underline{\underline{D}} = \begin{pmatrix} d_1 & 0 & & & \\ 0 & d_2 & 0 & & \\ & 0 & \ddots & 0 & \\ & & 0 & d_{n-1} & 0 \\ & & & 0 & d_n \end{pmatrix} \qquad \text{mit} \quad d_1, \ldots, d_n \in \mathbb{R}$$

Durch einfaches Nachrechnen erhält man:

1) Die Diagonalmatrix $\underline{\underline{D}}$ ist **invertierbar**, falls gilt: $d_i \neq 0$ für $1 \leq i \leq n$.
Es ist dann

$$\underline{\underline{D}}^{-1} = \begin{pmatrix} d_1^{-1} & 0 & & & \\ 0 & d_2^{-1} & 0 & & \\ & 0 & \ddots & 0 & \\ & & 0 & d_{n-1}^{-1} & 0 \\ & & & 0 & d_n^{-1} \end{pmatrix}$$

2) Für die **k-te Potenz** $\underline{\underline{D}}^k = \underbrace{\underline{\underline{D}} \cdot \underline{\underline{D}} \cdot \underline{\underline{D}} \cdot \ldots \cdot \underline{\underline{D}}}_{k-mal}, k \in \mathbb{N}$ gilt

$$\underline{\underline{D}}^k = \begin{pmatrix} d_1^k & 0 & & & \\ 0 & d_2^k & 0 & & \\ & 0 & \ddots & 0 & \\ & & 0 & d_{n-1}^k & 0 \\ & & & 0 & d_n^k \end{pmatrix}$$

Definition:
Eine Matrix $\underline{\underline{A}} \in M^{n,n}$ heißt **diagonalisierbar**, wenn es eine **invertierbare Matrix** $\underline{\underline{S}} \in M^{n,n}$ und eine **Diagonalmatrix** $\underline{\underline{D}}$ gibt mit $\underline{\underline{S}}^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}} = \underline{\underline{D}}$.

Es stellen sich folgende Fragen:
Wann ist eine Matrix $\underline{\underline{A}} \in M^{n,n}$ diagonalisierbar und was kann man damit machen?

Es gilt folgender

Satz:
Gegeben ist die Matrix $\underline{\underline{A}} \in M^{n,n}$.

1) Wenn $\underline{\underline{A}}$ n verschiedene Eigenwerte $\lambda_i \in \mathbb{R}$, $1 \leq i \leq n$, hat, ist $\underline{\underline{A}}$ diagonalisierbar.
2) Die Matrix $\underline{\underline{S}} \in M^{n,n}$ hat als Spalten(vektoren) die Eigenvektoren $\vec{v}_i$ der Matrix $\underline{\underline{A}}$ zu den Eigenwerten $\lambda_i \in \mathbb{R}$, $1 \leq i \leq n$; also $\underline{\underline{S}} = (\vec{v}_1 \vec{v}_2 \dots \vec{v}_n)$.
3) Die zugehörige Diagonalmatrix ist dann

$$\underline{\underline{D}} = \underline{\underline{S}}^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}} = \begin{pmatrix} \lambda_1 & 0 & & & \\ 0 & \lambda_2 & 0 & & \\ & 0 & \ddots & 0 & \\ & & 0 & \lambda_{n-1} & 0 \\ & & & 0 & \lambda_n \end{pmatrix}$$

.

Beispiel:

Gegeben ist die Matrix aus dem Beispiel Seite 174 $\underline{\underline{A}} = \begin{pmatrix} 0 & -1 & 3 \\ 2 & 3 & 3 \\ 2 & 1 & 1 \end{pmatrix}$.
Die Eigenwerte von $\underline{\underline{A}}$ sind $\lambda_1 = -2,\ \lambda_2 = 2,\ \lambda_3 = 4$.

Zugehörige **Eigenvektoren** sind (siehe vorheriges Beispiel):

Zu $\lambda_1 = -2$: $\vec{v_1} = \begin{pmatrix} -\frac{3}{2} \\ 0 \\ 1 \end{pmatrix}$, zu $\lambda_2 = 2$: $\vec{v_2} = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix}$, zu $\lambda_3 = 4$: $\vec{v_3} = \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix}$

Damit erhält man

$$\underline{\underline{S}} = \begin{pmatrix} -\frac{3}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix}$$

Berechnung von $\underline{\underline{S}}^{-1}$ im **erweiterten Gauß-Schema**:

$-\frac{3}{2}\quad -\frac{1}{2}\quad 0$ $0\quad 1\quad 3$ $1\quad 0\quad 1$	$1\quad 0\quad 0$ $0\quad 1\quad 0$ $0\quad 0\quad 1$
$1\quad 0\quad 1$ $0\quad 1\quad 3$ $-\frac{3}{2}\quad -\frac{1}{2}\quad 0$	$0\quad 0\quad 1$ $0\quad 1\quad 0$ $1\quad 0\quad 0$
$1\quad 0\quad 1$ $0\quad 1\quad 3$ $0\quad -\frac{1}{2}\quad \frac{3}{2}$	$0\quad 0\quad 1$ $0\quad 1\quad 0$ $1\quad 0\quad \frac{3}{2}$
$1\quad 0\quad 1$ $0\quad 1\quad 3$ $0\quad 0\quad 3$	$0\quad 0\quad 1$ $0\quad 1\quad 0$ $1\quad \frac{1}{2}\quad \frac{3}{2}$
$3\quad 0\quad 0$ $0\quad 1\quad 0$ $0\quad 0\quad 3$	$-1\quad -\frac{1}{2}\quad \frac{3}{2}$ $-1\quad \frac{1}{2}\quad -\frac{3}{2}$ $1\quad \frac{1}{2}\quad \frac{3}{2}$
$1\quad 0\quad 0$ $0\quad 1\quad 0$ $0\quad 0\quad 1$	$-\frac{1}{3}\quad -\frac{1}{6}\quad \frac{1}{2}$ $-1\quad \frac{1}{2}\quad -\frac{3}{2}$ $\frac{1}{3}\quad \frac{1}{6}\quad \frac{1}{2}$

Damit folgt $\underline{\underline{S}}^{-1} = \begin{pmatrix} -\frac{1}{3} & -\frac{1}{6} & \frac{1}{2} \\ -1 & \frac{1}{2} & -\frac{3}{2} \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{pmatrix}$ und

$\underline{\underline{D}} = \underline{\underline{S}}^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}} =$

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

Als „Anwendung“ berechnen wir Potenzen diagonalisierbarer Matrizen.

Satz:
Gegeben ist die diagonalisierbare Matrix $\underline{\underline{A}}$ mit der Diagonalmatrix $\underline{\underline{D}} = \underline{\underline{S}}^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}}$.
Dann gilt $\forall n \in \mathbb{N} : \underline{\underline{A}}^n = \underline{\underline{S}} \cdot \underline{\underline{D}}^n \cdot \underline{\underline{S}}^{-1}$.

Beweis (durch vollständige Induktion):
Induktionsanfang $n = 1$: $\underline{\underline{D}} = \underline{\underline{S}}^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}} \Rightarrow \underline{\underline{A}} = \underline{\underline{S}} \cdot \underline{\underline{D}} \cdot \underline{\underline{S}}^{-1}$ also $\underline{\underline{A}}^1 = \underline{\underline{S}} \cdot \underline{\underline{D}}^1 \cdot \underline{\underline{S}}^{-1}$.
Induktionsvoraussetzung: Für $n = k$ gilt $\underline{\underline{A}}^k = \underline{\underline{S}} \cdot \underline{\underline{D}}^k \cdot \underline{\underline{S}}^{-1}$
Induktionsbehauptung: Für $n = k + 1$ gilt $\underline{\underline{A}}^{k+1} = \underline{\underline{S}} \cdot \underline{\underline{D}}^{k+1} \cdot \underline{\underline{S}}^{-1}$

Beweis: $\underline{\underline{A}}^{k+1} = \underline{\underline{A}} \cdot \underline{\underline{A}}^k = \underbrace{\underline{\underline{A}}}_{=\underline{\underline{S}}\cdot\underline{\underline{D}}\cdot\underline{\underline{S}}^{-1}} \cdot \underline{\underline{S}} \cdot \underline{\underline{D}}^k \cdot \underline{\underline{S}}^{-1} = \underline{\underline{S}} \cdot \underline{\underline{D}} \cdot \underbrace{\underline{\underline{S}}^{-1} \cdot \underline{\underline{S}}}_{=\underline{\underline{E}}} \cdot \underline{\underline{D}}^k \cdot \underline{\underline{S}}^{-1} = \underline{\underline{S}} \cdot \underline{\underline{D}}^{k+1} \cdot \underline{\underline{S}}^{-1}$

Beispiel:

Wir nehmen die Matrix aus dem Beispiel Seite 177 $\underline{\underline{A}} = \begin{pmatrix} 0 & -1 & 3 \\ 2 & 3 & 3 \\ 2 & 1 & 1 \end{pmatrix}$.

Gesucht ist die Matrix A^5. Der gerade bewiesene Satz sagt $A^5 = S \cdot D^5 \cdot S^{-1}$ mit

$\underline{\underline{S}} = \begin{pmatrix} -\frac{3}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix}$, $\underline{\underline{S}}^{-1} = \begin{pmatrix} -\frac{1}{3} & -\frac{1}{6} & \frac{1}{2} \\ -1 & \frac{1}{2} & -\frac{3}{2} \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{pmatrix}$ und $\underline{\underline{D}} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$

Dann gilt $\underline{\underline{A}}^5 = \begin{pmatrix} -\frac{3}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}^5 \cdot \begin{pmatrix} -\frac{1}{3} & -\frac{1}{6} & \frac{1}{2} \\ -1 & \frac{1}{2} & -\frac{3}{2} \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{pmatrix}$

Dabei ist $\underline{\underline{D}}^5 = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}^5 = \begin{pmatrix} (-2)^5 & 0 & 0 \\ 0 & 2^5 & 0 \\ 0 & 0 & 4^5 \end{pmatrix} = \begin{pmatrix} -32 & 0 & 0 \\ 0 & 32 & 0 \\ 0 & 0 & 1024 \end{pmatrix}$ und damit

$\begin{pmatrix} -2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}^5 \cdot \begin{pmatrix} -\frac{1}{3} & -\frac{1}{6} & \frac{1}{2} \\ -1 & \frac{1}{2} & -\frac{3}{2} \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} -32 & 0 & 0 \\ 0 & 32 & 0 \\ 0 & 0 & 1024 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{3} & -\frac{1}{6} & \frac{1}{2} \\ -1 & \frac{1}{2} & -\frac{3}{2} \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{32}{3} & \frac{32}{6} & -16 \\ -32 & 16 & -48 \\ \frac{1024}{3} & \frac{512}{3} & 512 \end{pmatrix}$ und schließlich

$\underline{\underline{A}}^5 = \begin{pmatrix} -\frac{3}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{32}{3} & \frac{32}{6} & -16 \\ -32 & 16 & -48 \\ \frac{1024}{3} & \frac{512}{3} & 512 \end{pmatrix} = \begin{pmatrix} 0 & -16 & 48 \\ 992 & 528 & 1488 \\ 352 & 176 & 496 \end{pmatrix}$

Wir betrachten jetzt das Beispiel von Seite179

Beispiel:

Für die Matrix $\underline{\underline{A}} = \begin{pmatrix} 5 & -2 \\ -2 & 8 \end{pmatrix}$ erhält man für den Eigenwert $\lambda_1 = 4$ den normierten Eigenvektor $\vec{v}_1 = \begin{pmatrix} \frac{2}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} \end{pmatrix}$

Zum Eigenwert $\lambda_2 = 9$ erhält man den normierten Eigenvektor $\vec{v}_2 = \begin{pmatrix} -\frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{pmatrix}$

Diese normierten Eigenvektoren liefern die Matrizen

$$\underline{\underline{S}} = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix} \text{ und } \underline{\underline{S}}^{-1} = \underline{\underline{S}}^t = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix}$$

mit $\underline{\underline{S}}^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}} = \underline{\underline{D}} = \begin{pmatrix} 4 & 0 \\ 0 & 9 \end{pmatrix}$.

Die Ellipse aus der Einführung hat die Gleichung

$$< \vec{x}, \underline{\underline{A}} \cdot \vec{x} > -36 = \vec{x} \cdot (\underline{\underline{A}} \cdot \vec{x}) - 36 = \underbrace{5x^2 - 4xy + 8y^2}_{=<\vec{x}, \underline{\underline{A}} \cdot \vec{x}>} - 36 = 0$$

Setzt man $\underline{\underline{S}}^{-1} \cdot \vec{x} = \vec{z} = \begin{pmatrix} u \\ v \end{pmatrix}$ also $\vec{x} = \underline{\underline{S}} \cdot \vec{z}$ erhält man

$$0 =< \vec{x}, \underline{\underline{A}} \cdot \vec{x} > -36 =< \underline{\underline{S}} \cdot \vec{z}, \underline{\underline{A}} \cdot \underline{\underline{S}} \cdot \vec{z} > -36 =< \vec{z}, S^{-1} \cdot \underline{\underline{A}} \cdot \underline{\underline{S}} \cdot \vec{z} > -36 \Leftrightarrow$$
$$0 =< \vec{z}, \underline{\underline{D}} \cdot \vec{z} > -36 =$$

Wegen $\vec{z} = \begin{pmatrix} u \\ v \end{pmatrix}$ liefert das: $0 =< \vec{z}, \underline{\underline{D}} \cdot \vec{z} > -36 = 4u^2 + 9v^2 - 36 \Leftrightarrow \frac{u^2}{9} + \frac{v^2}{4} = 1.$

Das folgende Bild zeigt diese Ellipse mit zwei Halbgeraden in Richtung der beiden normierten Eigenvektoren; man erkennt, dass diese Halbgeraden in **Richtung der Hauptachsen der Ellipse** liegen und die Koordinatenachsen des neuen (u,v)-Koordinatensystems bilden.