Vorlesung "Mathematische Strukturen"

Sommersemester 2015

Prof. Barbara König
Übungsleitung: Dennis Nolte

Das heutige Programm

- Organisatorisches
  - Vorstellung
  - Ablauf der Vorlesung und der Übungen
  - Prüfung
  - Literatur & Folien
- Einführung und Motivation
- Inhalt der weiteren Vorlesung
- Grundlagen: Mengen, Funktionen, Relationen, ...

Wer sind wir?

Dozentin: Prof. Barbara König

- Raum LF 264
- E-Mail: barbara_koenig@uni-due.de
- Sprechstunde: nach Vereinbarung

Übungsleitung: M.Sc. Dennis Nolte

- Raum LF 263
- E-Mail: dennis.nolte@uni-due.de

Web-Seite: www.ti.inf.uni-due.de/teaching/ss2015/mast/

Einordnung

Diese Vorlesung ist für

- KOMEDIA-Studierende im 2. Semester

gedacht.

Vorlesungstermine

Vorlesungs-Termin:

- Dienstag, 8:20–9:50 Uhr, im LB 107

Termine der Übungsgruppen/Tutorien

Übungsgruppen:

1. Di, 12-14 Uhr, LE 120
2. Di, 12-14 Uhr, LD 102
3. ~~Di, 16-18 Uhr, LF 125~~
4. Di, 16-18 Uhr, LC 026
5. Mi, 12-14 Uhr, LC 137
6. Do, 8-10 Uhr, LC 137
7. ~~Do, 8-10 Uhr, LE 120~~
8. Di, 12-14 Uhr, LC 026

Tutorium: Fr, 10-12 Uhr, LF 125

Hinweise zu den Übungen

- Bitte versuchen Sie, sich möglichst gleichmäßig auf die Übungen zu verteilen. Dazu werden wir nach der ersten Woche die Teilnehmerzahlen der einzelnen Übungen bekanntgeben.
- Besuchen Sie die Übungen und machen Sie die Hausaufgaben! Diesen Stoff kann man nur durch regelmäßiges Üben erlernen. Auswendiglernen hilft nicht besonders viel.
- Die Übungen beginnen in der dritten Semesterwoche am Dienstag, den 21. April.

Hinweise zu den Übungen

- Das Übungsblatt wird jeweils am Dienstag ins Netz gestellt.
  Das erste Übungsblatt wird am 14.4. bereitgestellt, das zweite am 21.4.
- Die schriftlichen Aufgaben müssen bis spätestens Dienstag, 12:00 Uhr, der darauffolgenden Woche abgegeben werden.
  D.h., das erste Blatt muss am 21.4. abgegeben werden.
  Die Abgaben werden innerhalb einer Woche korrigiert. Die Besprechung eines Übungsblattes findet in derselben Woche statt wie die Abgabe, das erste Blatt wird also ab 21.4. besprochen.
- Einwurf in den Briefkasten neben dem Raum LF259.
- Bitte geben Sie auf Ihrer Lösung *deutlich* die Vorlesung, Ihren Namen, Ihre Matrikelnumer *und* Ihre Gruppennnumer an.
- Sie dürfen in Zweier-Gruppen abgeben.

Hinweise zu den Übungen

Wir verwenden Moodle, um:

- die Aufgabenblätter zur Verfügung zu stellen *und*
- um Diskussionsforen bereitzustellen.

Eine elektronische Abgabe der Hausaufgaben über Moodle ist nicht vorgesehen.
Moodle2-Plattform an der Universität Duisburg-Essen:
`http://moodle2.uni-due.de/` (siehe auch Link auf der Webseite)

Bitte legen Sie dort einen Zugang an (falls noch nicht vorhanden) und tragen Sie sich in den Kurs "Mathematische Strukturen 2015" (Sommersemester 2015 $\rightarrow$ Ingenieurwissenschaften $\rightarrow$ Abteilung Informatik und Angewandte Kognitionswissenschaft) ein.

Zugangsschlüssel: ...

Klausur

Die Vorlesung wird durch eine Klausur am Ende des Semesters geprüft. Der derzeitige Planungsstand für den Klausurtermin ist der 18. August (mit Vorbehalt!).

Die Anmeldung erfolgt über das Prüfungsamt.

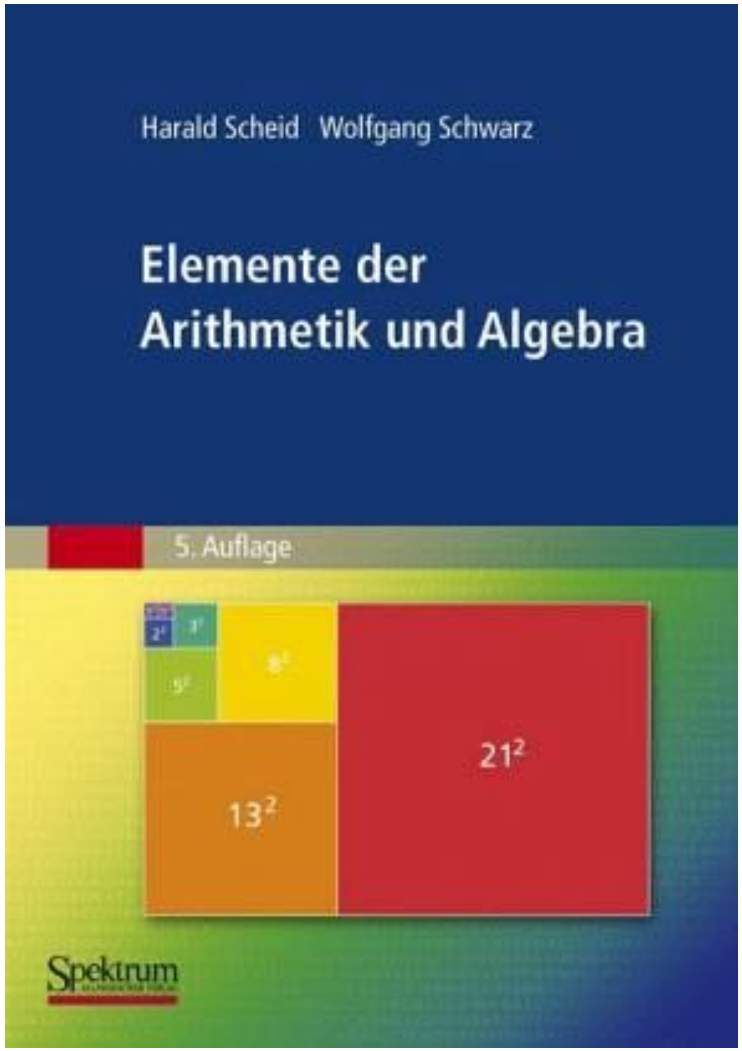
Klausur

Es gibt folgende Bonusregelung:

- Wenn Sie 50% der Punkte erzielt haben, so erhalten Sie einen Bonus für die Klausur.
- Auswirkung: Verbesserung um eine Notenstufe; z.B. von 2,3 auf 2,0

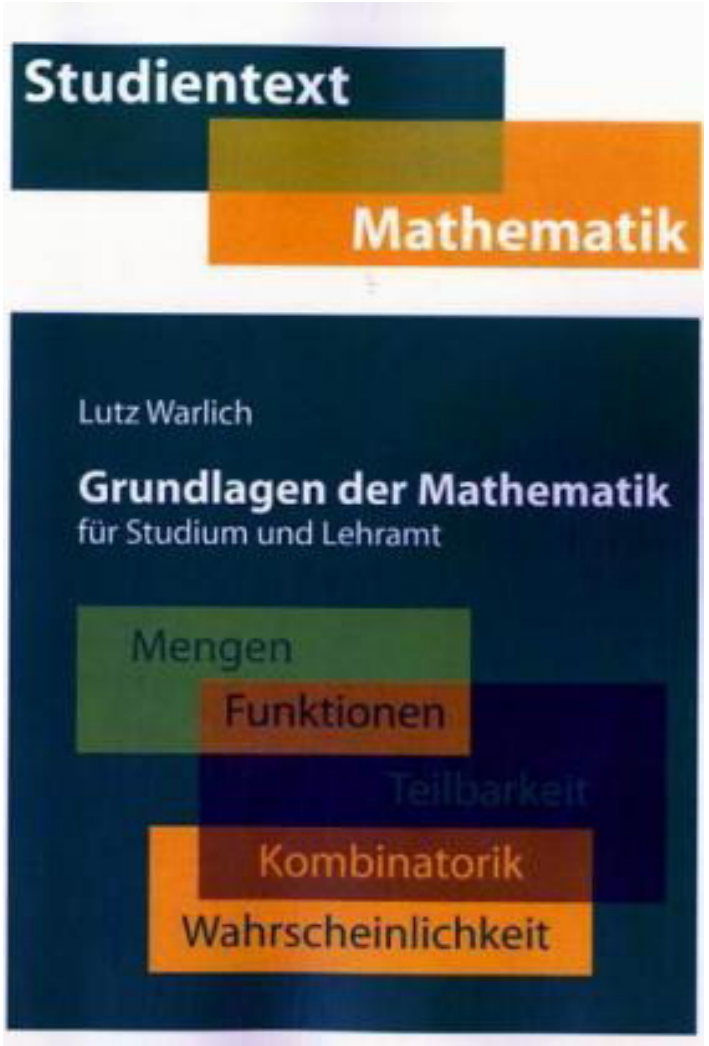
Literatur

Harald Scheid, Wolfgang Schwarz: Elemente der Arithmetik und Algebra. Spektrum 2008



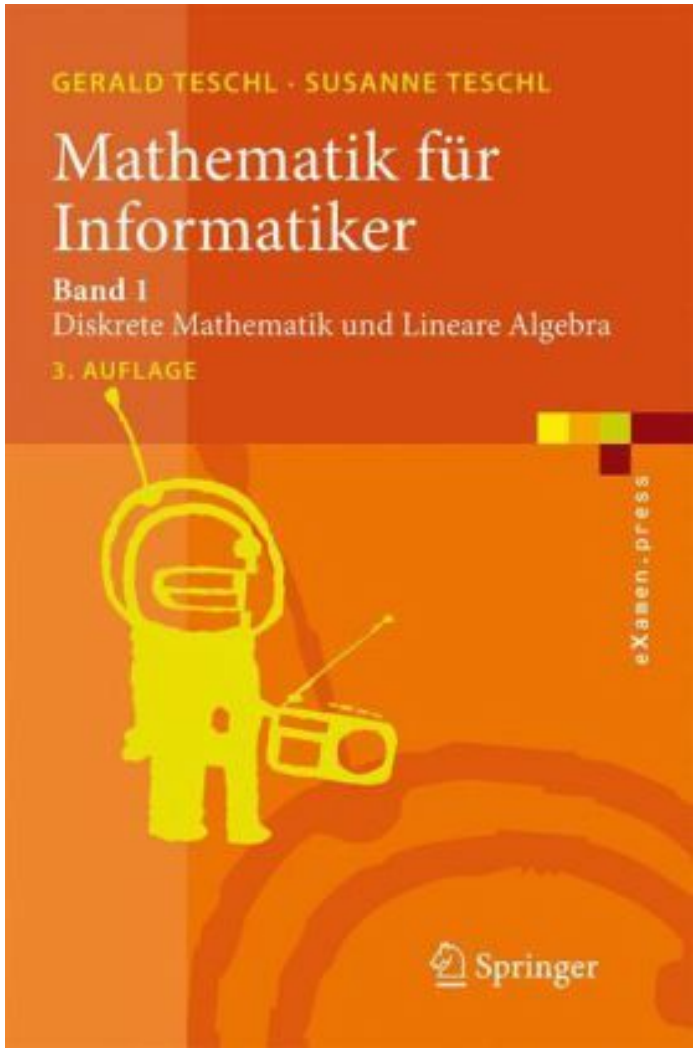
Literatur

Lutz Warlich: Grundlagen der Mathematik für Studium und Lehramt: Mengen, Funktionen, Teilbarkeit, Kombinatorik, Wahrscheinlichkeit.
Books on Demand, 1. Auflage (Juli 2006)



Literatur

Gerald Teschl, Susanne Teschl:
Mathematik für Informatiker, Diskrete Mathematik und Lineare Algebra, Bd.1, Springer, 2008



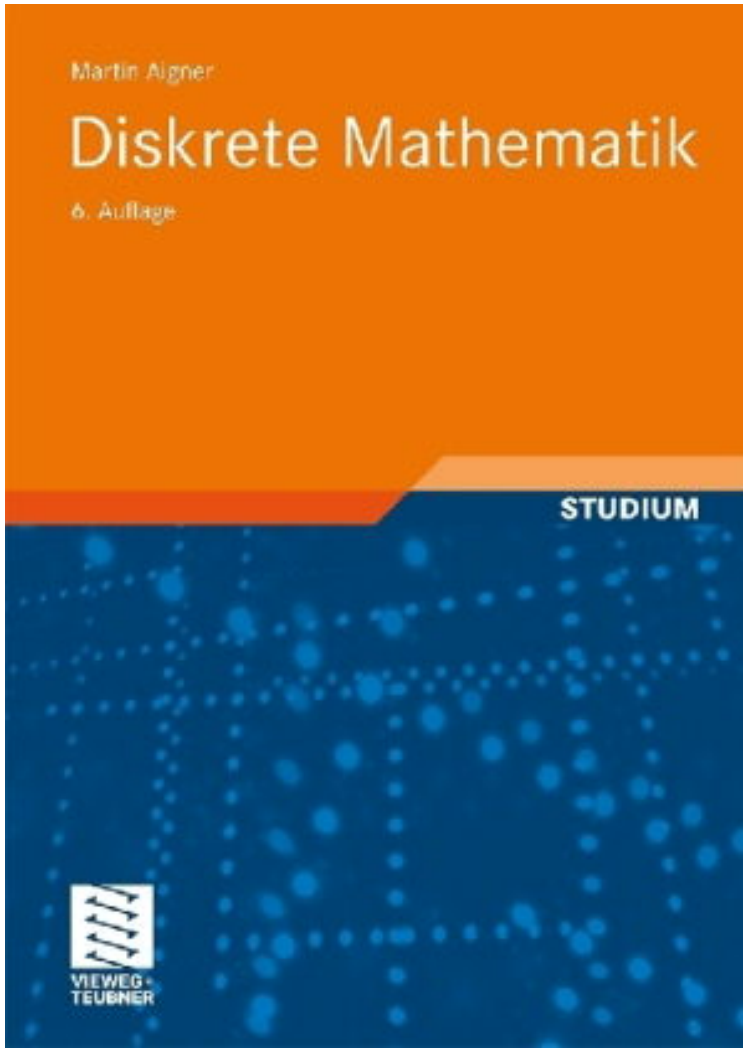
Literatur

Angelika Steger: Diskrete Strukturen 1. Kombinatorik, Graphentheorie, Algebra. Springer 2007

`http://www.springerlink.com/content/p18557/`
(zugreifbar über den Uni-Account)

Literatur

Martin Aigner: Diskrete Mathematik. Vieweg+Teubner, 2006.



Literatur

Dirk Hachenberger: Mathematik für Informatiker. Pearson, 2008.

Literatur

Hinweise:

- Die Bücher sind als Ergänzung gedacht, sie präsentieren den Stoff oft aus einem anderen Blickwinkel.
- Sehen Sie sich die Bücher erst an, bevor Sie sie kaufen. Nicht jede/r kommt mit jedem Buch zurecht.
- Die Bibliothek (LK) ist ein guter Platz um nach Büchern zu stöbern (Mathematik-Abteilung im 1. Stock, Lehrbuchsammlung im Keller)

Folien

Folien werden

- im Anschluss an die Vorlesung im Web als PDF bereitgestellt und
- regelmäßig aktualisiert.
- Große Teile der Folien werden im Wesentlichen gleich zu den Folien aus dem Sommersemester 2014 sein (erhältlich über die Webseite der letztjährigen Vorlesung).

Inhalt

- Grundlagen
  (Mengen, Relationen, Funktionen)
- Analysis, Kurvendiskussion, Ableitung
- Algebraische Strukturen
  (Gruppen, Körper, Vektorräume, Matrizen)
- Kombinatorik und Wahrscheinlichkeit

Inhalt

Diskrete Mathematik vs. Kontinuierliche Mathematik

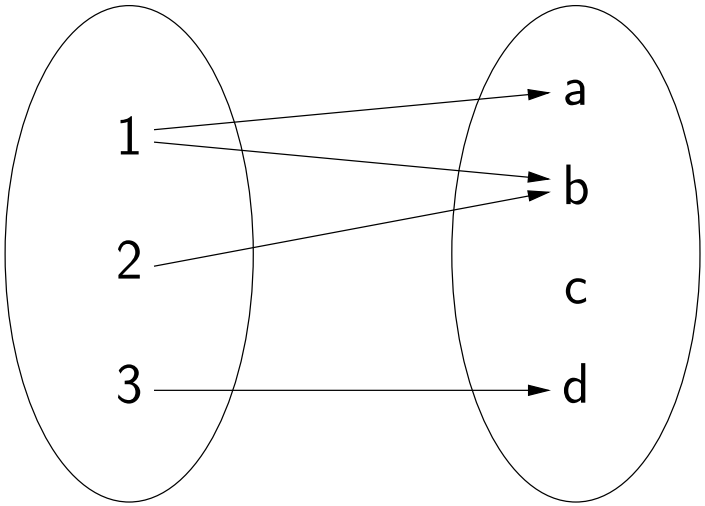
In dieser Vorlesung geht es schwerpunktmäßig um diskrete Mathematik, d.h., um das Arbeiten mit endlichen oder abzählbaren Mengen von Elementen.

Daneben gibt es noch die kontinuierliche Mathematik (Analysis, etc.), in der man mit reellen oder komplexen Zahlen arbeitet. (Ableitung, Integration von Funktionen, etc.)

Inhalt

Grundlagen (Mengen, Relationen, Funktionen)

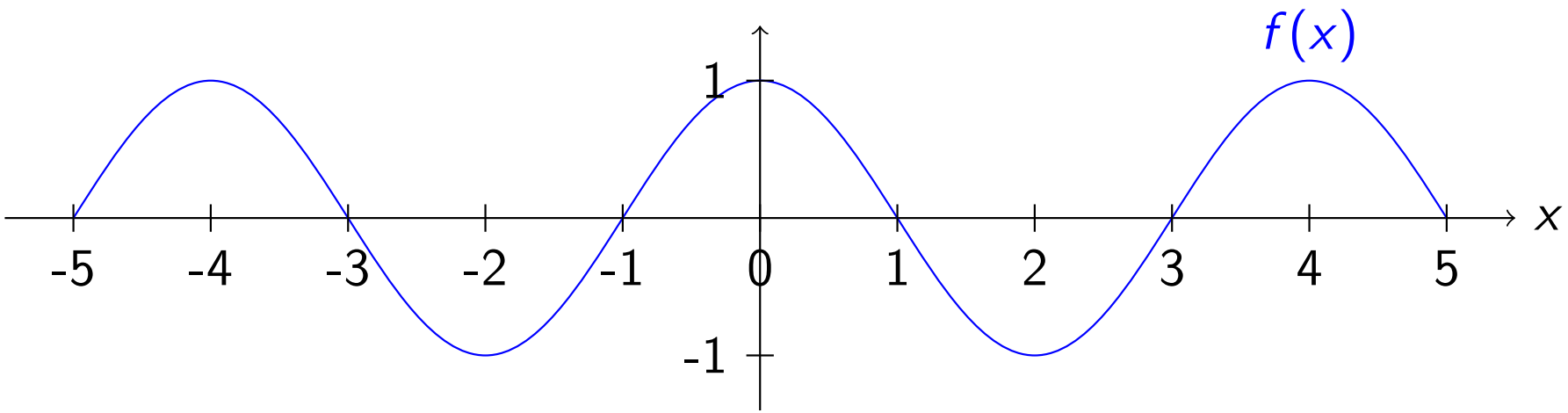
Wir besprechen/wiederholen grundlegende Konzepte der Mathematik.
Wie beschreibt man Ansammlungen von Elementen? $\rightsquigarrow$ Mengen
Wie beschreibt man Zusammenhänge zwischen Mengen? $\rightsquigarrow$ Relationen, Funktionen
Außerdem besprechen wir grundlegende Zahlentheorie (Primzahlen, etc.).



Inhalt

Analysis, Kurvendiskussion, Ableitbarkeit

Wir betrachten Funktionen auf reellen Zahlen und wiederholen Grundlagen der Kurvendiskussion. Dabei gehen wir vor allem auf das Ableiten (= Differenzieren) von Funktionen ein.

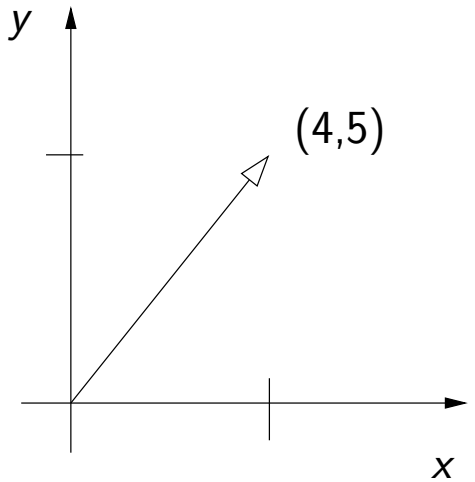


Inhalt

Algebraische Strukturen (Gruppen, Körper, Vektorräume, Matrizen)

Wir behandeln grundlegende Rechenstrukturen (Gruppen, Körper) und Anwendungen in der Kryptographie.
Anschließend: Vektorräume und Matrizen mit Anwendungen in der Darstellung von mehrdimensionalen Räumen. Lösen von Gleichungssystemen.

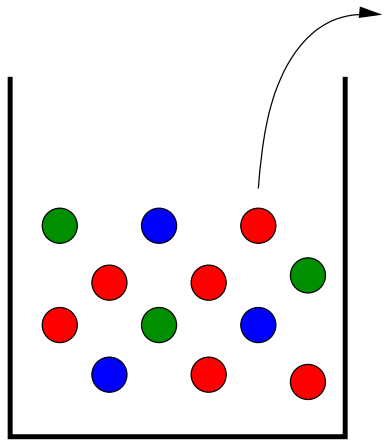
$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$



Inhalt

Kombinatorik und Wahrscheinlichkeit

Abzählen von Mengen: “Ziehen aus Urnen” und andere Modelle mit praktischen Beispielen.
Wahrscheinlichkeit des Auftretens bestimmter Ereignisse



Inhalt

Bemerkung:

- Der Inhalt änderte sich im Sommersemester 2013 gegenüber dem Vorjahr aufgrund von Wünschen und Vorschlägen aus der Studierendenschaft.
- Insbesondere wurden Teile des Stoffs ("Dreh- und Spiegelmatrizen" & "Graphen") durch ein Analysis-Kapitel ersetzt.

Mathematik im KOMEDIA-Studium

- Statistik (Inferenz-Statistik, Deskriptive Statistik) ($\rightsquigarrow$ Kombinatorik und Wahrscheinlichkeit)
- Informatik ($\rightsquigarrow$ u.a. Funktionen, Relationen, Graphen)
- Multimedia Engineering/Multimediasysteme ($\rightsquigarrow$ Vektorrechnung, z.B. für Grafiken)
- Modellierung ($\rightsquigarrow$ Grundlagen: Mengen, Relationen, Funktionen, Matrizenrechnung, Graphen)
- Mensch-Computer-Interaktion ($\rightsquigarrow$ Visualisierung und Navigation mit Graphen)
- Datenbanken ($\rightsquigarrow$ Relationen)
- Volkswirtschaftslehre ($\rightsquigarrow$ Kurvendiskussion, Ableitung)
- Kryptographische Verfahren (z.B. Gruppen, Körper)
- In Praxisprojekten, im Master-Studium

Mengen

Menge

Menge M von Elementen, wird beschrieben als Aufzählung

$$M = \{0, 2, 4, 6, 8, \dots\}$$

oder als Menge von Elementen mit einer bestimmten Eigenschaft

$$M = \{n \mid n \in \mathbb{N}_0 \text{ und } n \text{ gerade}\}.$$

Allgemeines Format:

$$M = \{x \mid P(x)\}$$

M ist Menge aller Elemente, die die Eigenschaft P erfüllen.

$$M = \{x \in X \mid P(x)\}$$

M ist Menge aller Elemente aus der Grundmenge X, die P erfüllen.

Mengen

Bemerkungen:

- Die Elemente einer Menge sind ungeordnet, d.h., ihre Ordnung spielt keine Rolle. Beispielsweise gilt:

$$\{1,2,3\} = \{1,3,2\} = \{2,1,3\} = \{2,3,1\} = \{3,1,2\} = \{3,2,1\}$$

- Ein Element kann nicht "mehrfach" in einer Menge auftreten. Es ist entweder in der Menge, oder es ist nicht in der Menge. Beispielsweise gilt:

$$\{1,2,3\} \neq \{1,2,3,4\} = \{1,2,3,4,4\}$$

Mengen

Element einer Menge

Wir schreiben $a \in M$, falls ein Element a in der Menge M enthalten ist.

Anzahl der Elemente einer Menge

Für eine Menge M gibt $|M|$ die Anzahl ihrer Elemente an.

Teilmengenbeziehung

Wir schreiben $A \subseteq B$, falls jedes Element von A auch in B enthalten ist. Die Beziehung $\subseteq$ heißt auch Inklusion.

Leere Menge

Mit $\emptyset$ oder $\{\}$ bezeichnet man die leere Menge. Sie enthält keine Elemente und ist Teilmenge jeder anderen Menge.

Mengen

Vereinigung

Die Vereinigung zweier Mengen A, A ist die Menge M, die die Elemente enthält, die in A oder B vorkommen. Man schreibt dafür $A \cup B$.

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$$

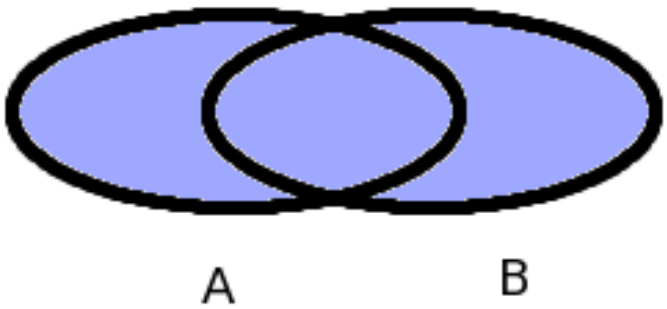
Schnitt

Der Schnitt zweier Mengen A, B ist die Menge M, die die Element enthält, die sowohl in A als auch in B vorkommen. Man schreibt dafür $A \cap B$.

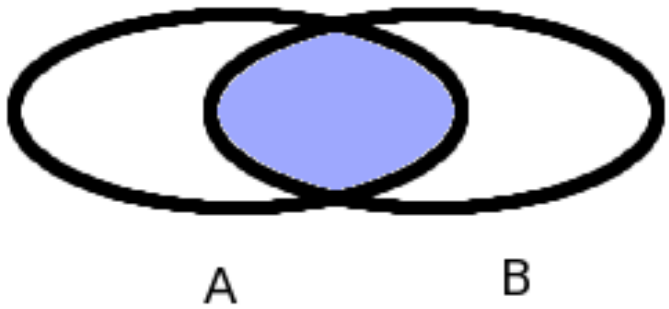
$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$$

Mengen

Veranschaulichung von Vereinigung und Schnitt durch Venn-Diagramme:



Blau eingefärbte Fläche entspricht der Vereinigung $A \cup B$



Blau eingefärbte Fläche entspricht dem Schnitt $A \cap B$

Mengen

Mengendifferenz

Seien A, B zwei Mengen. Dann bezeichnet $A \backslash B$ die Menge aller Elemente, die in A vorkommen und in B nicht vorkommen.

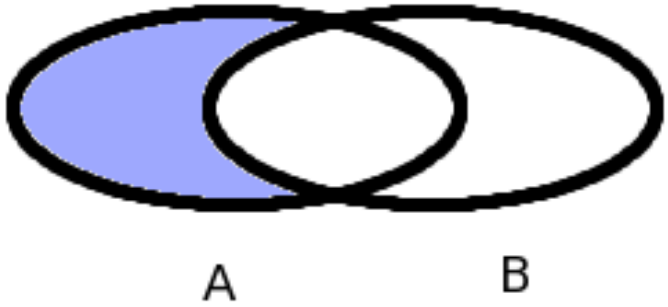
$$A \backslash B = \{x \mid x \in A \text{ und } x \notin B\}$$

Beispiele:

- $\{0, 1, 2, 3, 4, 5\} \backslash \{0\} = \{1, 2, 3, 4, 5\}$
- $\{a, b, c\} \backslash \{c, d\} = \{a, b\}$

Mengen

Veranschaulichung der Mengendifferenz durch ein Venn-Diagramm:



Blau eingefärbte Fläche entspricht der Mengendifferenz $A \setminus B$

Mengen

Potenzmenge

Sei M eine Menge. Die Menge $\mathcal{P}(M)$ ist die Menge aller Teilmengen von M.

$$\mathcal{P}(M) = \{A \mid A \subseteq M\}$$

Beispiel:

$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Es gilt: $|\mathcal{P}(M)| = 2^{|M|}$ (für eine endliche Menge M).

Mengen

Kreuzprodukt (kartesisches Produkt)

Seien A, B zwei Mengen. Die Menge $A \times B$ ist die Menge aller Paare (a, b), wobei die erste Komponente des Paars aus A, die zweite aus B kommt.

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

Beispiel:

$\{1, 2\} \times \{3, 4, 5\} = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$

Es gilt: $|A \times B| = |A| \cdot |B|$ (für endliche Menge A, B).

Mengen

Bemerkungen:

- Wir betrachten nicht nur Paare, sondern auch sogenannte Tupel, bestehend aus mehreren Komponenten. Ein Tupel $(a_1, \ldots, a_n)$ bestehend aus n Komponenten heißt auch n-Tupel.
- In einem Tupel sind die Komponenten geordnet! Es gilt z.B.:

$$(1, 2, 3) \neq (1, 3, 2) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \mathbb{N}_0$$

- Eine Komponente kann "mehrfach" in einem Tupel auftreten. Tupel unterschiedlicher Länge sind immer verschieden. Beispielsweise:

$$(1, 2, 3, 4) \neq (1, 2, 3, 4, 4)$$

Runde Klammern $(,)$ und geschweifte Klammern $\{,\}$ stehen für ganz verschiedene mathematische Objekte!

Relationen

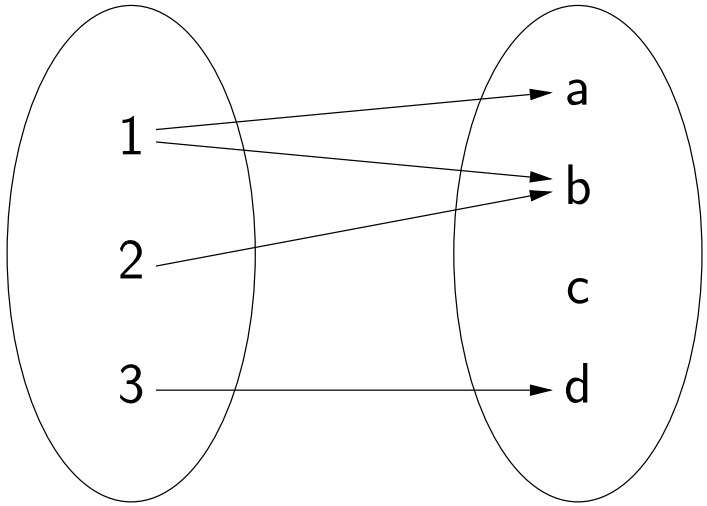
Relation zwischen der Menge A und der Menge B

Eine Teilmenge $R \subseteq A \times B$ des Kreuzprodukts von A und B heißt Relation zwischen A und B.

Beispiel:

$A = \{1, 2, 3\}$ $B = \{a, b, c, d\}$ $R = \{(1, a), (1, b), (2, b), (3, d)\}$

Relationen können auf folgende Weise graphisch dargestellt werden:



Relationen

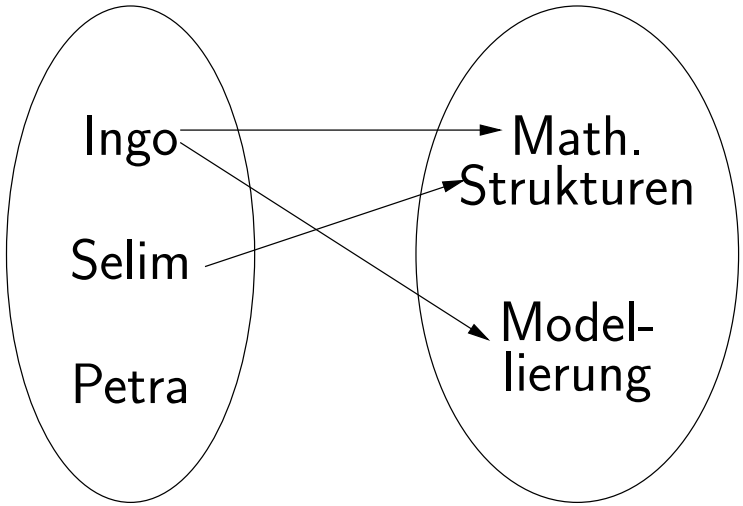
Schreibweise: wir notieren folgendermaßen, dass ein Paar in einer Relation liegt

- Standard-Schreibweise: $(2, b) \in R$
- Infix-Schreibweise: $2\, R\, b$

  Für Relationen wie $=$, $<$, $\leq$, $>$, $\geq$ wird fast immer die Infix-Schreibweise verwendet
  (Beispielsweise $2 < 5$, $7 \geq 3$)

Relationen

Weiteres Beispiel: Zuordnung von Studierenden zu Veranstaltungen



$$
\begin{aligned}
A &= \{\text{Ingo}, \text{Selim}, \text{Petra}\} \\
B &= \{\text{Math.Strukturen}, \text{Modellierung}\} \\
R &= \{(\text{Ingo}, \text{Math.Strukturen}), (\text{Ingo}, \text{Modellierung}), \\
&\quad\ (\text{Selim}, \text{Math.Strukturen})\}
\end{aligned}
$$

Relationen

Wir sehen uns nun einige besondere Arten von Relationen an:

- Funktionen
- Äquivalenzrelationen
- Ordnungen

Funktionen

Funktion von der Menge A in die Menge B

Eine Relation $f \subseteq A \times B$ heißt Funktion, wenn folgendes gilt:

- für jedes Element $a \in A$ gibt es genau ein Element $b \in B$ mit $(a, b) \in f$.

Anschaulich: jedes Element in der Menge A hat genau einen ausgehenden Pfeil. (Die vorherigen Beispiels-Relationen waren also keine Funktionen.)

Funktionen

Notation von Funktionen

$$\begin{aligned} f: A &\to B \\ a &\mapsto f(a) \end{aligned}$$

Die Funktion f bildet jedes Element $a \in A$ auf genau ein Element $f(a) \in B$ ab. Dabei ist A der Definitionsbereich und B der Wertebereich. Außerdem muss eine Zuordnungsvorschrift angegeben werden ($a \mapsto f(a)$).

Beispiel (Quadratfunktion):

$$f: \mathbb{Z} \to \mathbb{N}_0, \quad f(n) = n^2$$

$$\ldots, -3 \mapsto 9, -2 \mapsto 4, -1 \mapsto 1, 0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 4, 3 \mapsto 9, \ldots$$

Dabei ist $\mathbb{N}_0$ die Menge der natürlichen Zahlen (mit der Null) und $\mathbb{Z}$ die Menge der ganzen Zahlen.

Funktionen

Bild und Urbild einer Menge

Sei $f : A \to B$ eine Funktion und $A' \subseteq A$. Dann nennt man die Menge

$$f(A') = \{f(a) \mid a \in A'\}$$

das Bild von A' unter der Funktion f.

Sei nun $B' \subseteq B$. Die Menge

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

heißt das Urbild von B' unter der Funktion f.

Funktionen

Injektive Funktion

Eine Funktion $f : A \to B$ heißt injektiv, falls es keine Elemente $a_1, a_2 \in A$ gibt mit $a_1 \neq a_2$ und $f(a_1) = f(a_2)$.
Alternativ: Eine Funktion f ist injektiv, falls für alle Elemente $a_1, a_2 \in A$ aus $f(a_1) = f(a_2)$ immer $a_1 = a_2$ folgt.

Anschaulich: auf kein Element im Wertebereich zeigt mehr als ein Pfeil.

Surjektive Funktion

Eine Funktion $f : A \to B$ heißt surjektiv, falls es für jedes $b \in B$ (mindestens) ein $a \in A$ gibt mit $f(a) = b$.

Anschaulich: auf jedes Element im Wertebereich zeigt (mindestens) ein Pfeil.

Funktionen

Bijektive Funktion

Eine Funktion $f : A \to B$ heißt bijektiv, falls sie injektiv und surjektiv ist.

Anschaulich: auf jedes Element im Wertebereich zeigt genau ein Pfeil. D.h., es gibt eine eins-zu-eins-Zuordnung zwischen den Elementen des Definitionsbereichs und des Wertebereichs

Funktionen

Bemerkung: Die bijektiven Funktionen sind genau die invertierbaren Funktionen. Zu einer bijektiven Funktion $f : A \to B$ gibt es eine Umkehrfunktion $f^{-1} : B \to A$ mit folgenden Eigenschaften:

- $f^{-1}(f(a)) = a$ für alle $a \in A$
- $f(f^{-1}(b)) = b$ für alle $b \in B$

Beispiel: Die Funktion

$$f : \mathbb{Z} \to \mathbb{Z} \qquad z \mapsto z - 1$$

hat als Umkehrfunktion

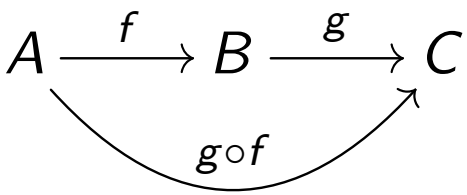
$$f^{-1} : \mathbb{Z} \to \mathbb{Z} \qquad z \mapsto z + 1$$

Funktionen

Verknüpfung von Funktionen

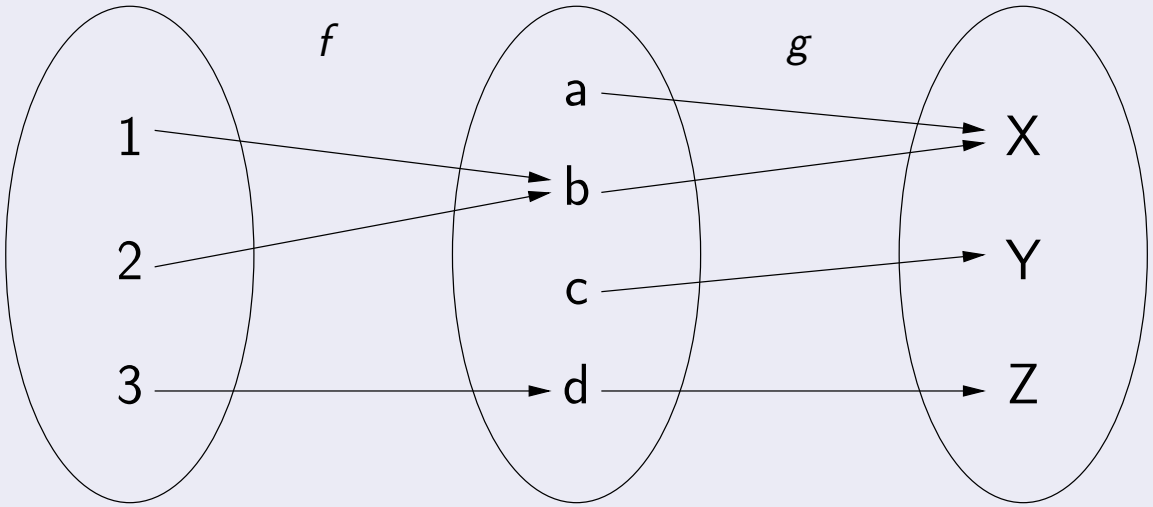
Gegeben seien zwei Funktionen $f: A \to B$ und $g: B \to C$. Mit $g \circ f$ bezeichnen wir die Verknüpfung oder Hintereinanderausführung von f und g. Diese Funktion ist wie folgt definiert:

$$\begin{aligned} g \circ f: A &\to C \\ a &\mapsto g(f(a)) \end{aligned}$$



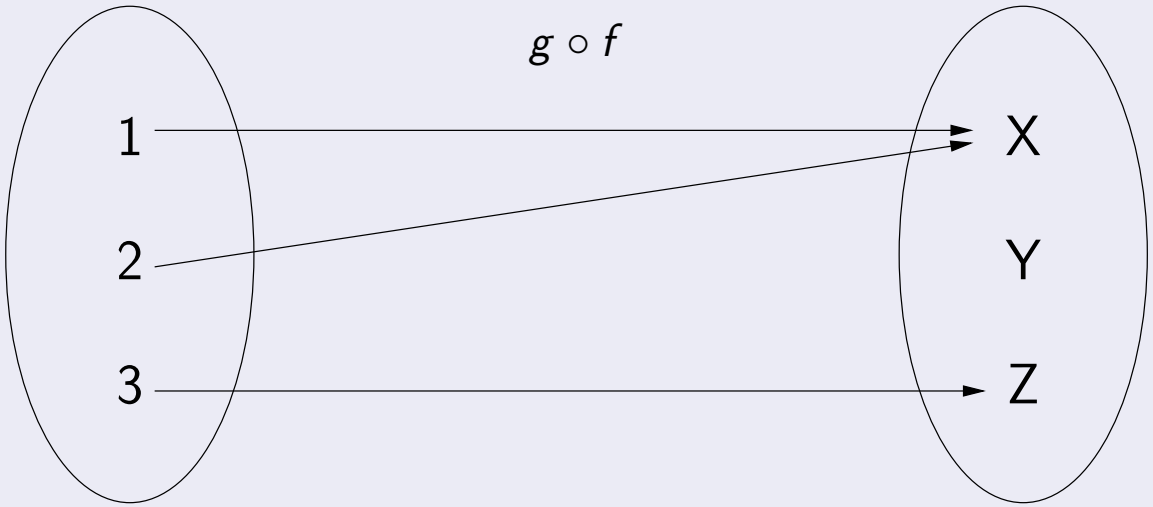
Funktionen

Beispiel: Funktionsverknüpfung



Funktionen

Beispiel: Funktionsverknüpfung



Relationen

Wir betrachten nun spezielle Relationen, die nur auf einer Menge A definiert sind.

Äquivalenzrelation

Eine Relation $R \subseteq A \times A$ heißt Äquivalenzrelation, falls folgendes gilt:

- Reflexivität: für alle $a \in A$ gilt $(a, a) \in R$.
- Transitivität: falls für beliebige $a, b, c \in A$, $(a, b) \in R$ und $(b, c) \in R$ gilt, so muss auch $(a, c) \in R$ gelten.
- Symmetrie: falls für beliebige $a, b \in A$, $(a, b) \in R$ gilt, so muss auch $(b, a) \in R$ gelten.

Relationen

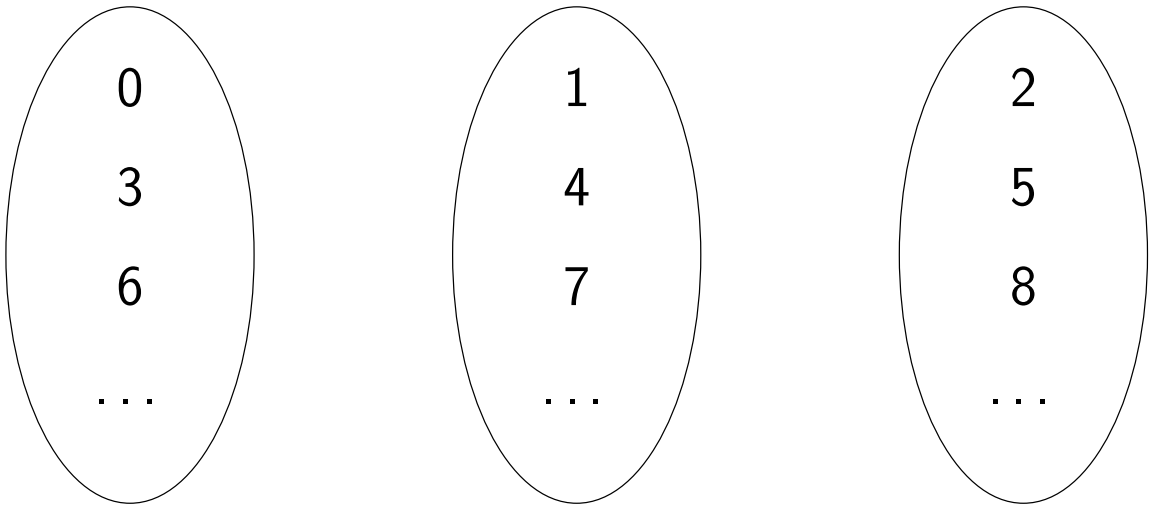
Beispiel für eine Äquivalenzrelation:

$$R = \{(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid x, y \text{ haben denselben Divisionsrest bei ganzzahliger Division durch } 3\}$$

Relationen

Bemerkung:

- Durch eine Äquivalenzrelation $R \subseteq A \times A$ zerfällt die Menge A in sogenannte Äquivalenzklassen.
- Graphische Darstellung von Äquivalenzklassen für das vorherige Beispiel:



Relationen

Äquivalenzklassen

Sei $R \subseteq A \times A$ eine Äquivalenzrelation und $a \in A$. Die Äquivalenzklasse von a ist

$$[a]_R = \{a' \in A \mid a \, R \, a'\}$$

Für zwei Element $a, b \in A$ gilt entweder $[a]_R = [b]_R$ oder $[a]_R \cap [b]_R = \emptyset$.

Relationen

(Partielle) Ordnung

Eine Relation $R \subseteq A \times A$ heißt (partielle) Ordnung, falls folgendes gilt:

- Reflexivität: für alle $a \in A$ gilt $(a, a) \in R$.
- Transitivität: falls für beliebige $a, b, c \in A$, $(a, b) \in R$ und $(b, c) \in R$ gilt, so muss auch $(a, c) \in R$ gelten.
- Antisymmetrie: falls für beliebige $a, b \in A$, $(a, b) \in R$ und $(b, a) \in R$ gilt, so muss $a = b$ gelten, d.h., a und b müssen dann gleich sein.

Relationen

Bei der Definition einer Ordnung hat sich gegenüber der Definition einer Äquivalenzrelation nur die letzte Eigenschaft geändert (Antisymmetrie versus Symmetrie).

Achtung: Antisymmetrie ist nicht das Gegenteil von Symmetrie! Jede Gleichheitsrelation erfüllt beide Eigenschaften.

Relationen

Beispiel für eine Ordnung:

Wir betrachten die Potenzmenge $\mathcal{P}(M)$ einer festen Menge M und die Mengeninklusion $\subseteq$.

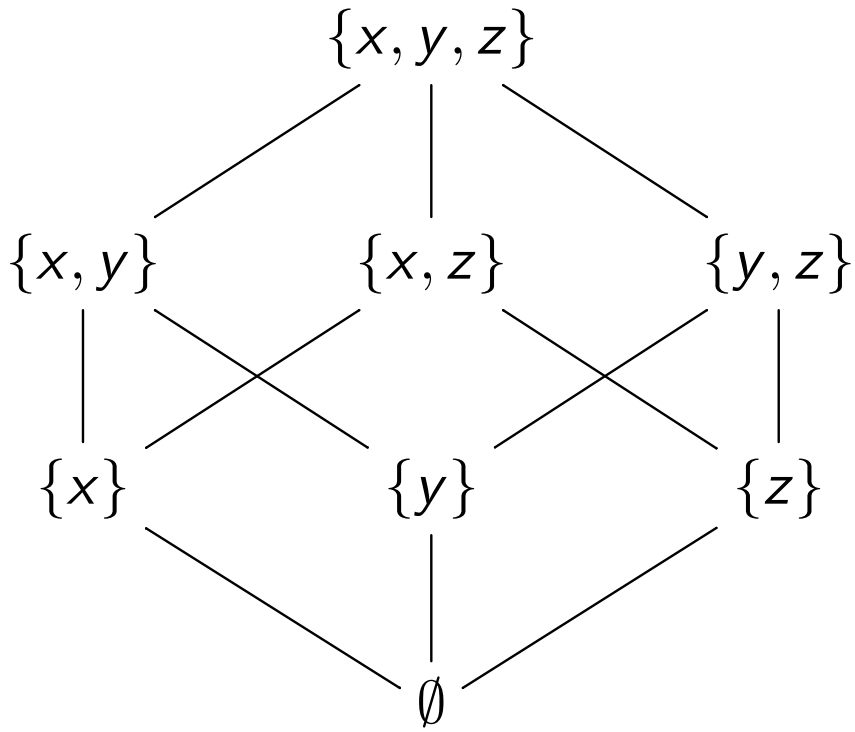
Relationen

Ordnungen werden graphisch als sogenannte Hasse-Diagramme dargestellt:

Beispiel: $\mathcal{P}(\{x, y, z\})$ und Inklusion $\subseteq$

Falls $a\,R\,b$ (und $a \neq b$) gilt, dann:

- liegt a unterhalb von b *und*
- wenn keine Elemente "zwischen" a und b liegen (bezüglich R), dann werden beide mit einer Linie verbunden.



Zahlen

Wir betrachten folgende spezielle Mengen von Zahlen:

Natürliche Zahlen mit 0

$\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \dots\}$

Ganze Zahlen

$\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$

Zahlen

Rationale Zahlen

$\mathbb{Q}$: die Menge aller Brüche (= Menge aller Kommazahlen mit endlicher oder periodischer Dezimaldarstellung)

$$2 \quad -4 \quad \frac{1}{2} \quad \frac{27}{7} \quad 0,75 \quad 32,333417 \quad \frac{1}{3} = 0,3333\ldots = 0,\overline{3}$$

Reelle Zahlen

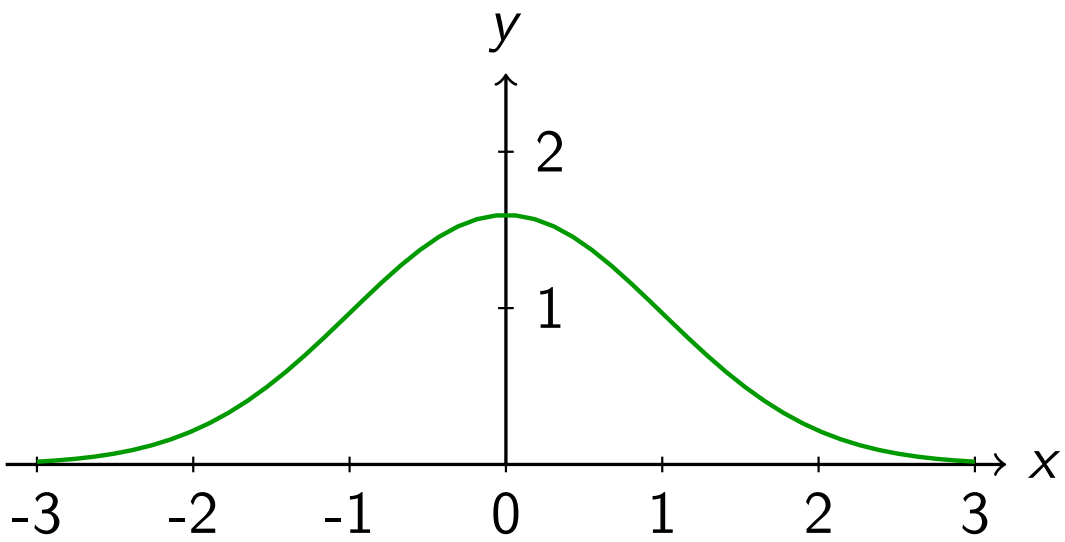
$\mathbb{R}$: die Menge aller reellen Zahlen (= Menge aller Kommazahlen mit beliebiger – auch unendlicher, nicht-periodischer – Dezimaldarstellung)

$$2 \quad -4 \quad \frac{1}{2} \quad \sqrt{2} = 1,41421\ldots \quad \pi = 3,14159\ldots$$
$$e = 2,718281\ldots$$

Analysis

Analysis, Kurvendiskussion, Ableitbarkeit

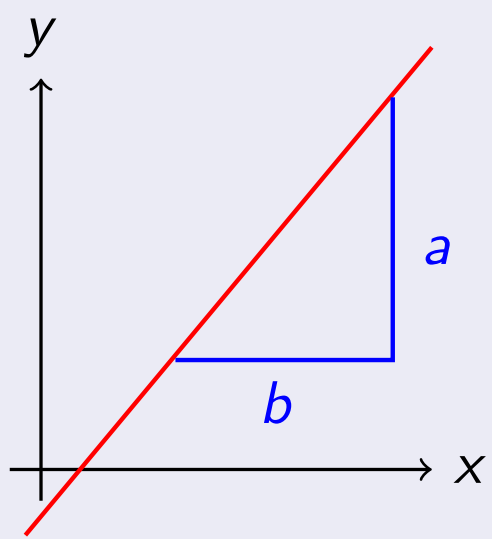
Wir betrachten Funktionen auf reellen Zahlen und wiederholen Grundlagen der Kurvendiskussion. Dabei gehen wir vor allem auf das Ableiten (= Differenzieren) von Funktionen ein.



Motivation

Die Steigung einer Funktion an einer bestimmten Stelle ist anschaulich ein Maß für die Steilheit bzw. den Grad des Wachstums.

Steigung einer Geraden



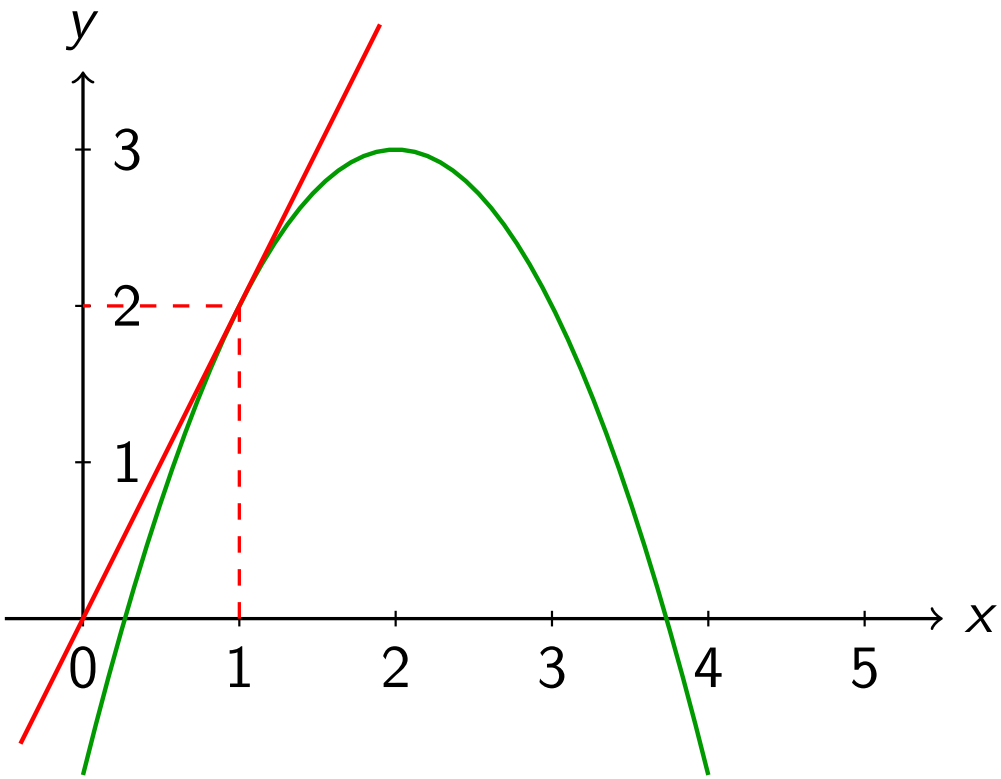
Für ein rechtwinkliges Dreieck (mit Katheten parallel zur x- und y-Achse) unterhalb der Geraden bestimmt man die Länge der Katheten: a, b

Steigung der Geraden: $\frac{a}{b}$

Dabei ist es unerheblich, wo das Dreieck liegt und wie groß es ist. Man erhält immer denselben Wert.

Motivation

Um die Steigung einer Kurve in einem Punkt zu bestimmen, bestimmen wir die Tangente an diesem Punkt, d.h. eine Gerade, die die Kurve in diesem Punkt berührt. Die Steigung der Tangente ist dann die Steigung der Kurve.



Motivation

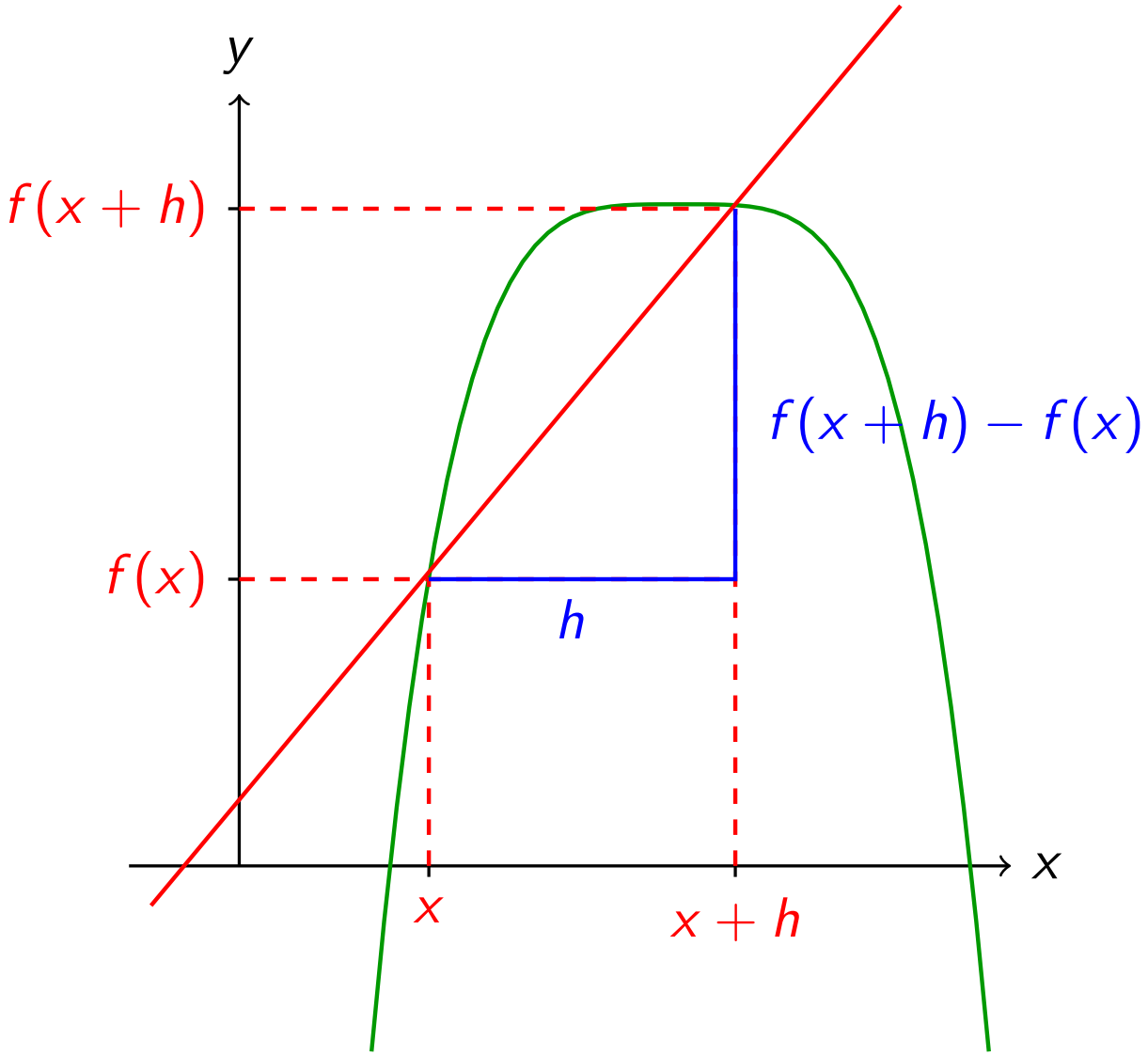
Es ist jedoch nicht offensichtlich, wie die Steigung der Tangente berechnet werden soll.

Wir nehmen an, dass die Kurve der Graph einer reellwertigen Funktion $f : \mathbb{R} \to \mathbb{R}$ ist. Wir wollen die Steigung in x bestimmen, d.h. eine Tangente durch den Punkt $(x, f(x))$ legen.

Vorgehen:

- Bestimme (für beliebiges $h \in \mathbb{R}$) einen weiteren Punkt $(x + h, f(x + h))$ und lege eine Gerade durch diese beiden Punkte.
  Die Steigung der Gerade ist: $\frac{f(x+h)-f(x)}{(x+h)-x} = \frac{f(x+h)-f(x)}{h}$
- Lasse h gegen 0 gehen (d.h. h wird immer kleiner). Dann nähert sich die Steigung der Geraden immer mehr der Steigung der Tangenten an.

Motivation



Grenzwerte

Um dies genauer beschreiben zu können und um konkrete Steigungen berechnen zu können, benötigen wir den Begriff des Grenzwerts oder Limes.

Beispiel:

Die Funktion

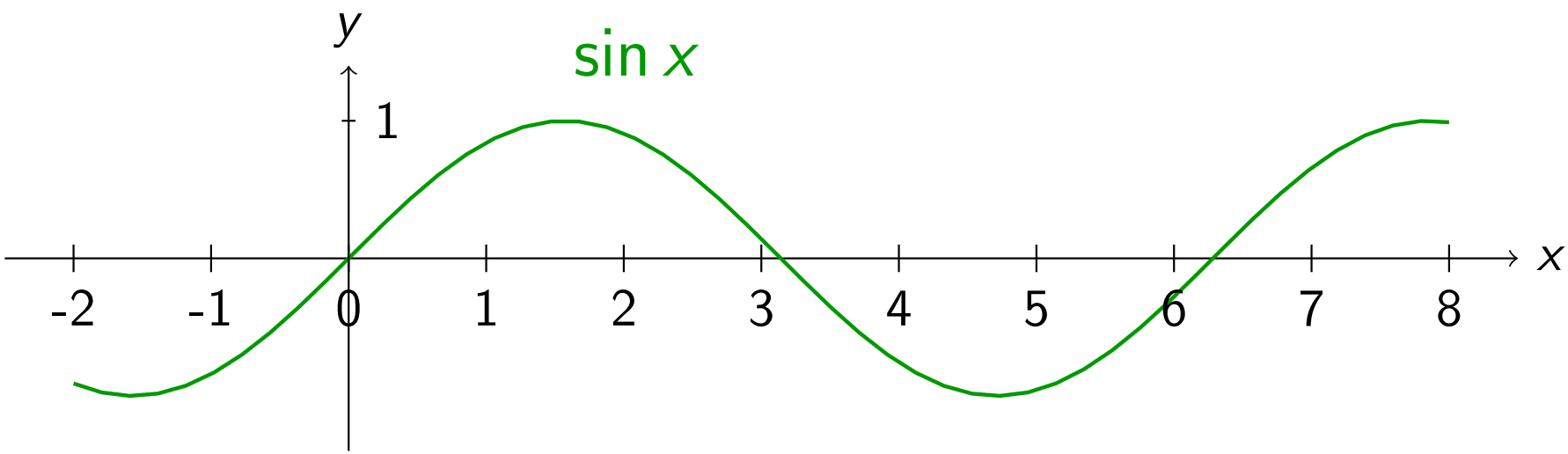
$$f : \mathbb{R}\backslash\{0\} \to \mathbb{R}, \quad f(x) = \frac{\sin x}{x}$$

ist nicht für Null definiert. (Es ist auch nicht möglich, den Definitionsbereich zu erweitern, da durch 0 dividiert wird.)

Bei Betrachtung des Funktionsgraphen scheint sich jedoch der Funktionswert von f für x gegen 0 beliebig der 1 zu nähern.

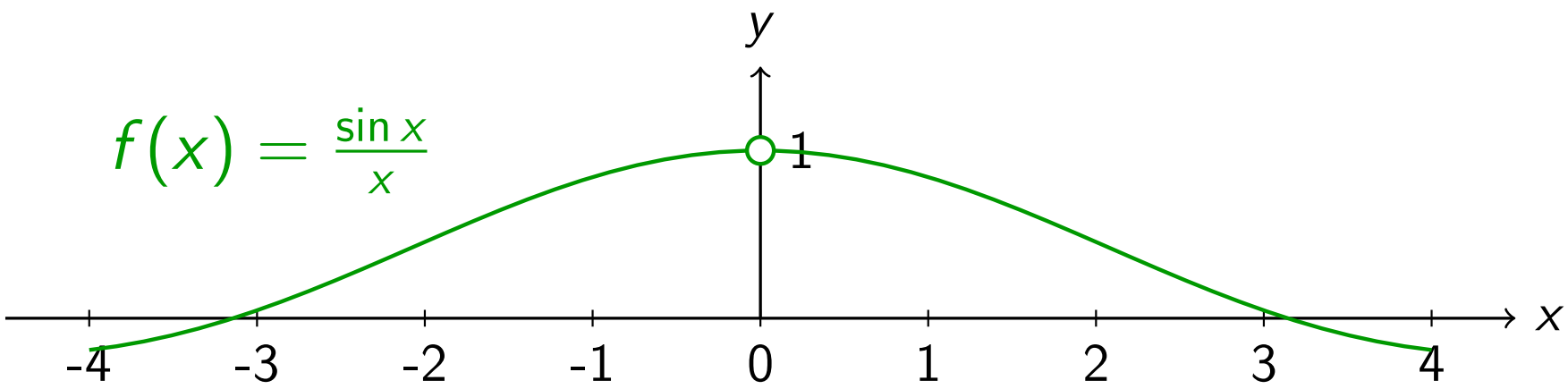
Grenzwerte

Zur Erinnerung: Graph der Sinusfunktion



Grenzwerte

Graph der Funktion $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$, $f(x) = \frac{\sin x}{x}$



Wir wollen ausdrücken können, dass der Grenzwert von f für x gegen 0 gleich 1 ist.

Grenzwerte

Grenzwert einer Funktion

Sei $f : X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}$ eine Funktion und seien $x_0, a \in \mathbb{R}$. Angenommen, es gibt für jedes $\varepsilon > 0$ ein $\delta > 0$, so dass für jedes $x \in X$ mit $|x_0 - x| < \delta$ folgt, dass $|a - f(x)| < \varepsilon$.

Dann ist a der Grenzwert (oder Limes) von f für x gegen x_0 und man schreibt:

$$\lim_{x \to x_0} f(x) = a.$$

Bemerkungen:

- Die Werte ε, δ sind reelle Zahlen.
- $|z|$ bezeichnet den Absolutwert der Zahl $z \in \mathbb{R}$:

$$|z| = \begin{cases} z & \text{falls } z \geq 0 \\ -z & \text{sonst} \end{cases}$$

Beispielsweise: $|7| = 7$, $|0| = 0$, $|-3| = 3$

Grenzwerte

Bemerkungen:

- Anschaulich sagt die Grenzwert-Definition: der Abstand zwischen $f(x)$ und a wird beliebig klein (beschrieben durch ε), wenn x nur nahe genug bei x_0 liegt (beschrieben durch δ).
- Für eine Funktion f und ein gegebenes x_0 muss nicht notwendigerweise ein Grenzwert existieren. (Gegenbeispiel später.)

Grenzwerte

Um zu zeigen, dass $\lim_{x\to 0} \frac{\sin x}{x} = 1$ gilt, benötigen wir noch folgende Abschätzung (ohne Beweis): für alle $x \in \mathbb{R}$ gilt

$$|x - \sin x| \leq \frac{|x|^3}{6}.$$

Daraus folgt für $x \neq 0$:

$$\left|1 - \frac{\sin x}{x}\right| = \frac{|x - \sin x|}{|x|} \leq \frac{|x|^2}{6}.$$

Das heißt, wenn wir für ein $\varepsilon \leq 6$ erreichen wollen, dass $|1 - \frac{\sin x}{x}| < \varepsilon$ gilt, dann reicht es, $\delta = \varepsilon$ zu setzen. Denn für ein x mit $|0 - x| = |x| < \delta$ gilt:

$$\left|1 - \frac{\sin x}{x}\right| \leq \frac{|x|^2}{6} < \frac{\delta^2}{6} \leq \delta = \varepsilon.$$

(Für $\varepsilon > 6$ kann man $\delta = 6$ setzen.)

Grenzwerte

Der Begriff des Grenzwerts macht nur Sinn für sogenannte Häufungspunkte von X.

Häufungspunkt

Sei $X \subseteq \mathbb{R}$. Eine reelle Zahl $x_0 \in \mathbb{R}$ ist ein Häufungspunkt von X, wenn es für jedes $\varepsilon > 0$ ein $x \in X$ gibt mit $x \neq x_0$ und $|x_0 - x| < \varepsilon$.

D.h. ein Häufungspunkt von X ist eine Zahl, in deren Umgebung unendlich viele Elemente von X sind, die beliebig nahe an x_0 liegen.

Ist x_0 kein Häufungspunkt von x, dann gibt es keine Möglichkeit, x_0 beliebig nahe zu kommen und die Grenzwert-Definition macht keinen Sinn.

Beispiel: Die Zahl $x_0 = 0$ ist ein Häufungspunkt von $X = \mathbb{R}\backslash\{0\}$.

Grenzwerte

Rechnen mit Grenzwerten

Gegeben seien zwei Funktionen $f, g\colon X \to \mathbb{R}$, wobei $X \subseteq \mathbb{R}$. Wir nehmen an, dass beide Funktionen einen Grenzwert in $x_0 \in \mathbb{R}$ haben:

$$\lim_{x \to x_0} f(x) = a \qquad \lim_{x \to x_0} g(x) = b$$

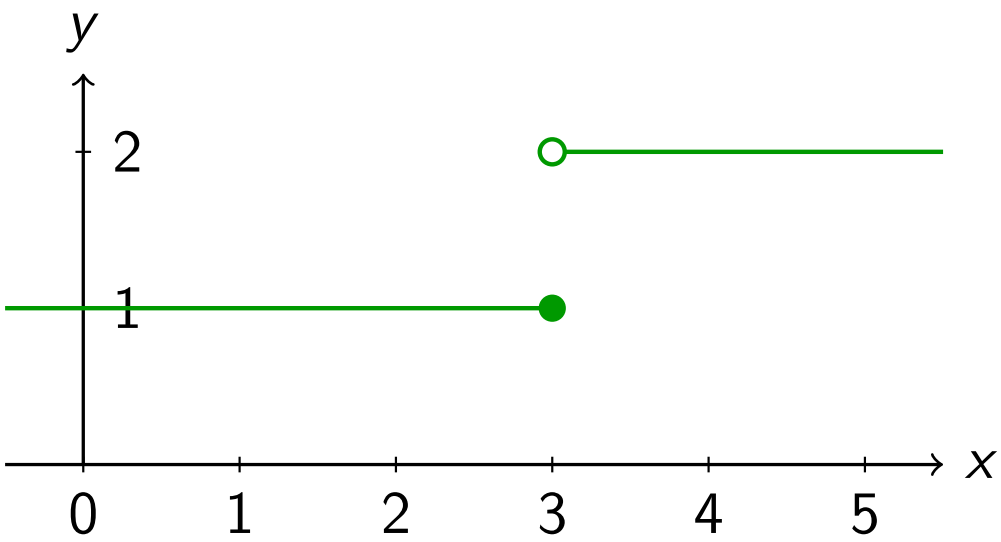
Außerdem sei $c \in \mathbb{R}$. Dann gilt:

$$\begin{aligned}
\lim_{x \to x_0} (c \cdot f(x)) &= c \cdot \lim_{x \to x_0} f(x) = c \cdot a \\
\lim_{x \to x_0} (f(x) + g(x)) &= \lim_{x \to x_0} f(x) + \lim_{x \to x_0} g(x) = a + b \\
\lim_{x \to x_0} (f(x) - g(x)) &= \lim_{x \to x_0} f(x) - \lim_{x \to x_0} g(x) = a - b \\
\lim_{x \to x_0} (f(x) \cdot g(x)) &= \lim_{x \to x_0} f(x) \cdot \lim_{x \to x_0} g(x) = a \cdot b
\end{aligned}$$

Stetigkeit

Manche Funktionen machen "Sprünge", beispielsweise folgende Funktion g:

$$g\colon \mathbb{R} \to \mathbb{R}, \quad g(x) = \begin{cases} 1 & \text{falls } x \leq 3 \\ 2 & \text{falls } x > 3 \end{cases}$$



Anschaulich bezeichnen wir eine Funktion als stetig, wenn sie keine solchen Sprungstellen besitzen.

Stetigkeit

Stetigkeit

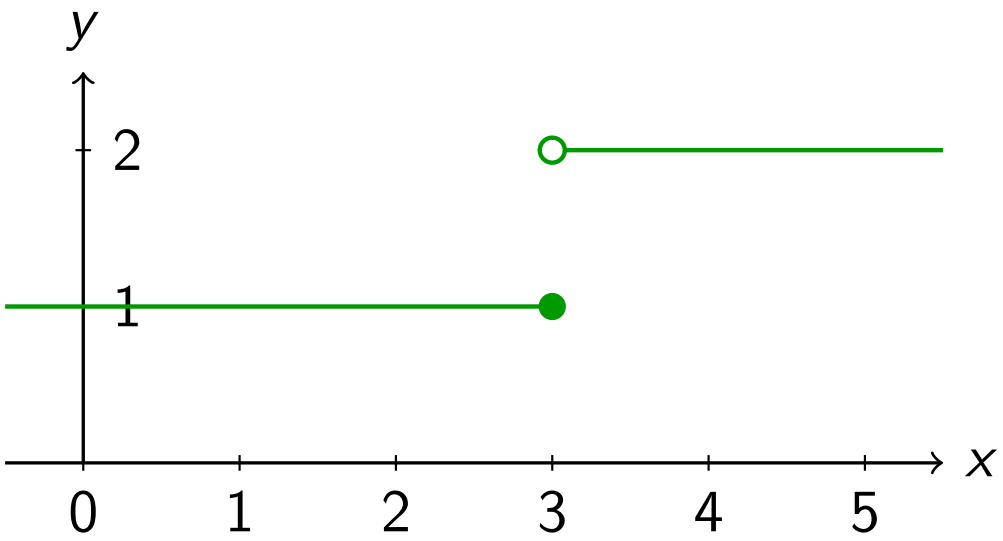
Eine Funktion $f : X \to \mathbb{R}$ heißt stetig an der Stelle $x_0 \in X$, wenn der Grenzwert $\lim_{x \to x_0} f(x)$ definiert ist und außerdem gleich $f(x_0)$ ist ($\lim_{x \to x_0} f(x) = f(x_0)$). Die Funktion f heißt stetig, wenn sie für jedes $x_0 \in X$ stetig ist.

Anschaulich: wenn man sich dem Wert x_0 (von links oder rechts nähert) und Funktionswerte bildet, so erhält man im Grenzwert genau den Wert $f(x_0)$.

Für stetige Funktion gilt also immer: $\lim_{x \to x_0} f(x) = f(x_0)$, d.h., man erhält den Grenzwert einfach durch Einsetzen in die Funktion.

Stetigkeit

Beispiel: sei $x_0 = 3$. Wenn man sich von rechts x_0 nähert, dann nähert man sich *nicht* dem Funktionswert $g(x_0) = 1$.



Genauer: für $\varepsilon < 1$ gibt es kein δ, so dass aus $|x_0 - x| = |3 - x| < \delta$ auch $|g(x_0) - g(x)| = |1 - g(x)| < \varepsilon$ folgt. Beispielsweise gilt für $x = 3 + \frac{\delta}{2}$ immer $g(x) = 2$ und damit $|1 - g(x)| = 1 > \varepsilon$.

Damit existiert kein Grenzwert $\lim_{x \to 3} g(x)$.

Stetigkeit

Weiteres Beispiel:

Man kann die Funktion

$$f : \mathbb{R}\backslash\{0\} \to \mathbb{R}, \quad f(x) = \frac{\sin x}{x}$$

stetig fortsetzen, d.h., eine Funktion $\overline{f} : \mathbb{R} \to \mathbb{R}$ konstruieren, die

- auf allen reellen Zahlen definiert ist,
- auf $\mathbb{R}\backslash\{0\}$ mit f übereinstimmt *und*
- stetig ist.

Dabei ist $\overline{f}$ wie folgt definiert:

$$\overline{f}(x) = \begin{cases} \frac{\sin x}{x} & \text{falls } x \neq 0 \\ 1 & \text{falls } x = 0 \end{cases}$$

Diese Funktion ist stetig, denn $\lim_{x \to 0} \frac{\sin x}{x} = 1$.

Bestimmung der Ableitung

Mit Hilfe des Grenzwert-Begriffs kann man nun die Steigung einer Funktion f definieren. Die entstehende Funktion f', die zu jedem x-Wert die Steigung an der jeweiligen Stelle angibt, heißt Ableitung. Die Bestimmung von f' bezeichnet man auch als Ableiten bzw. Differenzieren.

Ableitung

Eine Funktion $f : X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}$ heißt differenzierbar (oder ableitbar) an der Stelle $x \in X$, wenn der Grenzwert

$$\lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

existiert. Dieser wird mit $f'(x)$ bezeichnet.

Eine Funktion heißt differenzierbar, wenn sie für alle $x \in X$ differenzierbar ist. Die dabei entstehende Funktion $f' : X \to \mathbb{R}$ wird als Ableitung bezeichnet.

Bestimmung der Ableitung

Bemerkungen:

- Statt $f'(x)$ schreibt man manchmal auch $\frac{d}{dx}f(x)$, $\frac{df(x)}{dx}$ oder $\frac{df}{dx}(x)$.

  Dabei steht dx für die Distanz zwischen Werten auf der x-Achse und $df(x)$ für die Distanz zwischen Funktionswerten.
- Jede differenzierbare Funktion ist auch stetig.

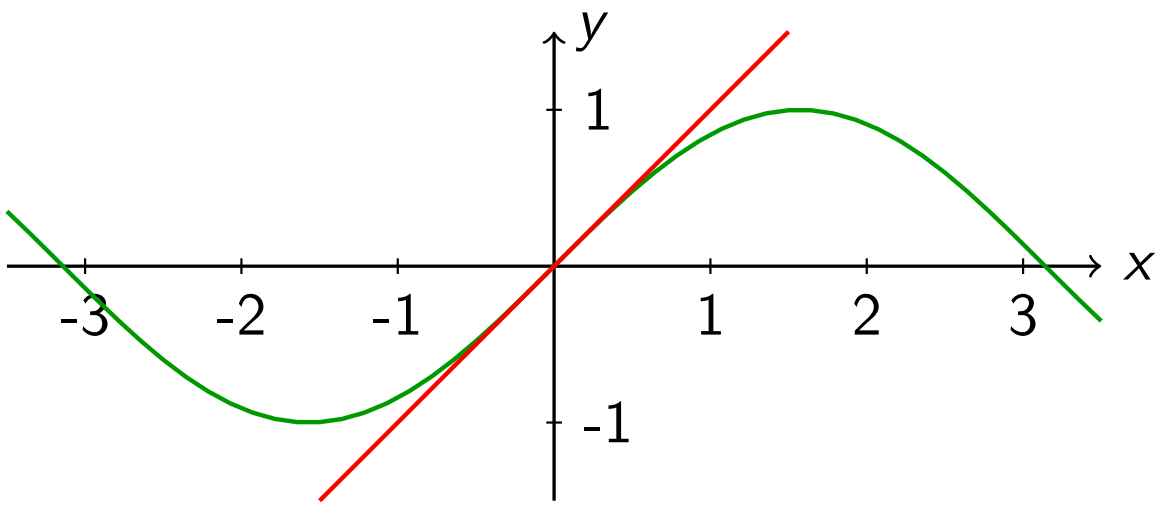
Bestimmung der Ableitung

Beispiel:

Wir bestimmen die Ableitung der Sinusfunktion an der Stelle $x = 0$.

$$\sin' 0 = \lim_{h \to 0} \frac{\sin(0+h) - \sin 0}{h} = \lim_{h \to 0} \frac{\sin h - \sin 0}{h} = \lim_{h \to 0} \frac{\sin h}{h} = 1$$

Folgende Abbildung stellt die Tangente an der Sinuskurve an der Stelle 0 dar. Diese Tangente hat Steigung 1.



Bestimmung der Ableitung

Ableitung einer konstanten Funktion

Sei $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = c$, wobei $c \in \mathbb{R}$ eine Konstante ist.

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \to 0} \frac{c - c}{h} = \lim_{h \to 0} 0 = 0$$

Ableitung der Identitätsfunkion

Sei $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x$.

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \to 0} \frac{(x+h) - x}{h} = \lim_{h \to 0} 1 = 1$$

Bestimmung der Ableitung

Ableitung einer (Normal-)Parabel

Sei $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$.

$$\begin{aligned} f'(x) &= \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \to 0} \frac{(x+h)^2 - x^2}{h} \\ &= \lim_{h \to 0} \frac{2xh + h^2}{h} = \lim_{h \to 0} (2x + h) = 2x \end{aligned}$$

Bestimmung der Ableitung

Ableitung von $f(x) = x^n$

Sei $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^n$ für ein festes $n \in \mathbb{N}_0$.

$$\begin{aligned} f'(x) &= \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \to 0} \frac{\sum_{k=0}^{n} \binom{n}{k} x^{n-k} h^k - x^n}{h} \\ &= \lim_{h \to 0} \sum_{k=1}^{n} \binom{n}{k} x^{n-k} h^{k-1} = \binom{n}{1} x^{n-1} = n \cdot x^{n-1} \end{aligned}$$

Die Berechnung basiert auf folgenden zwei Beobachtungen:

- der binomischen Formel für $(x+h)^n$ mit Binomialkoeffizienten $\binom{n}{k}$ (siehe Kombinatorik ▸ Binomische Formel);
- das vorletzte Gleichheitszeichen gilt, da nur der Summand für $k = 1$ keinen Faktor h enthält. Alle anderen Summanden enthalten ein h und werden zu 0, wenn h gegen 0 geht.

Bestimmung der Ableitung

Bemerkung:

Auch für $f(x) = x^c$, wobei $c \in \mathbb{R}$ eine beliebige reelle Zahl ist, gilt $f'(x) = c \cdot x^{c-1}$.

D.h. für $f : \mathbb{R}_0^+ \to \mathbb{R}$, $f(x) = \sqrt{x} = x^{\frac{1}{2}}$ gilt:

$$f'(x) = \frac{1}{2} x^{-\frac{1}{2}} = \frac{1}{2\sqrt{x}}$$

Ableitungen bekannter Funktionen

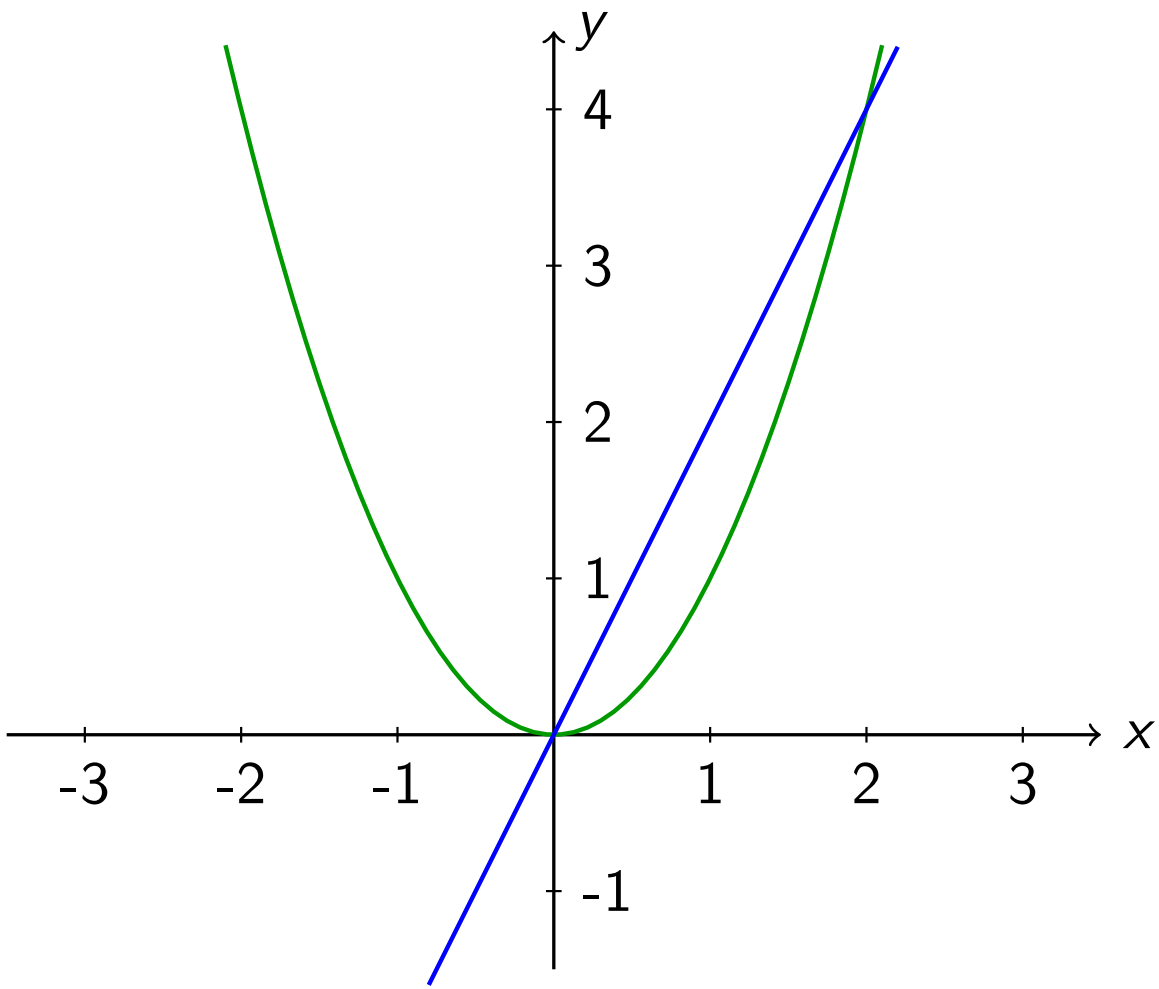
Folgende Tabelle enthält die Ableitungen weiterer bekannter Funktionen. Dabei ist $a \in \mathbb{R}$.

$f(x)$	$f'(x)$
e^x	e^x
a^x	$\ln(a) \cdot a^x$
$\ln x$	$\frac{1}{x}$
$\log_a(x)$	$\frac{1}{\ln(a) \cdot x}$
$\sin x$	$\cos x$
$\cos x$	$-\sin x$

- e: Eulersche Zahl ($\approx 2,718281\ldots$)
- $\ln x$: Logarithmus naturalis (Logarithmus zur Basis e)
- $\log_a x$: Logarithmus zur Basis a (bezeichnet die eindeutig bestimmte Zahl $y \in \mathbb{R}$ für die gilt $a^y = x$)

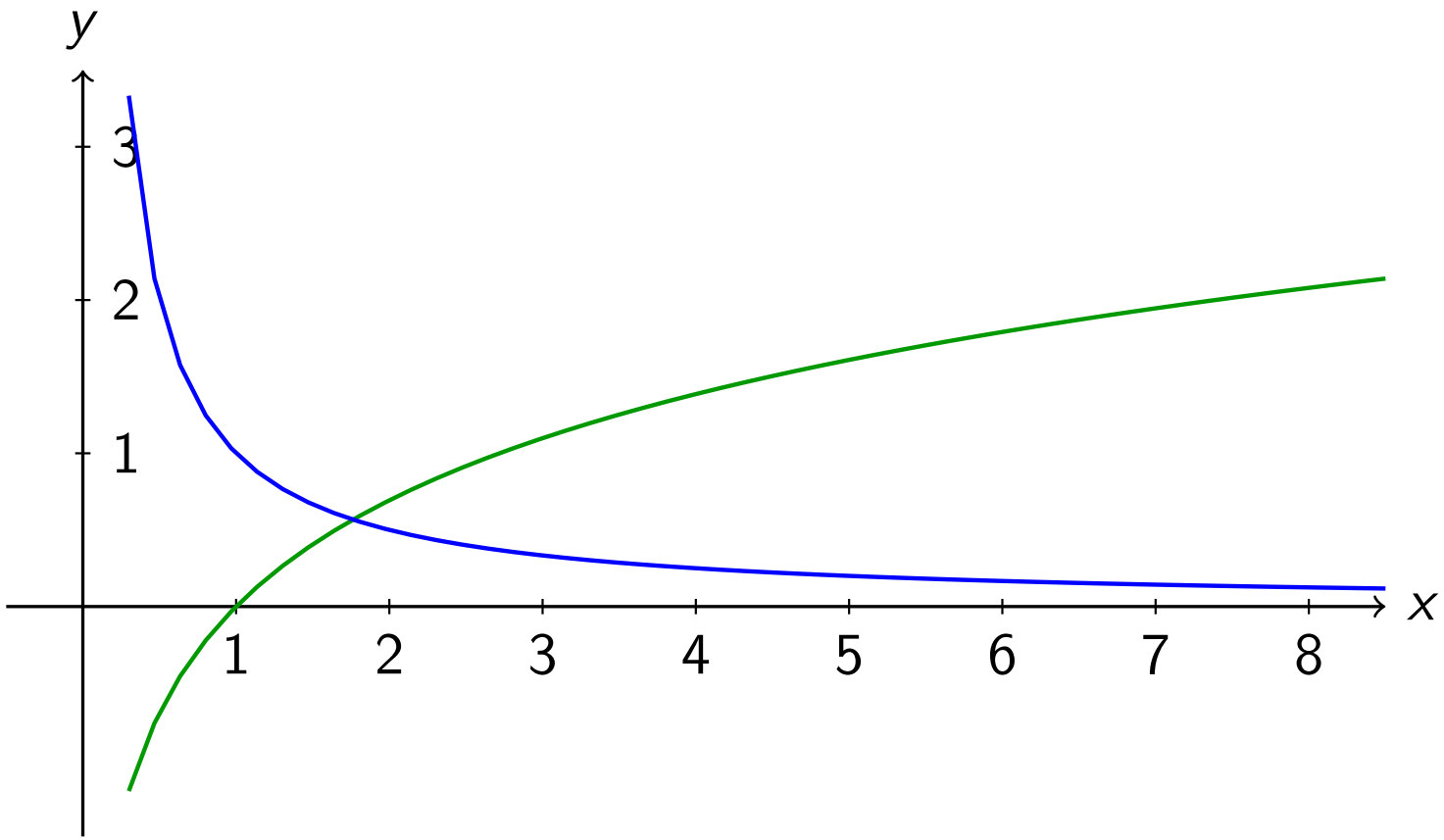
Ableitungen bekannter Funktionen

Beispiel 1: Graph der Parabel ($f(x) = x^2$) und ihre Ableitung ($f'(x) = 2x$).



Ableitungen bekannter Funktionen

Beispiel 2: Graph des Logarithmus naturalis ($f(x) = \ln x$) und seiner Ableitung ($f'(x) = \frac{1}{x}$) (auf den positiven reellen Zahlen).



Ableitungsregeln

Wenn man die Ableitungen bestimmter Funktionen kennt, kann man daraus – nach einer Art Baukastenprinzip – weitere Ableitungen konstruieren. Dafür gelten die unten aufgeführten Regeln.

Faktorregel

Sei $f : X \to \mathbb{R}$ eine differenzierbare Funktion mit Ableitung f' und sei $g : X \to \mathbb{R}$ definiert als $g(x) = c \cdot f(x)$ für $c \in \mathbb{R}$. Dann gilt:

$$g'(x) = (c \cdot f)'(x) = c \cdot f'(x)$$

Ableitungsregeln

Beweis der Faktorregel:

$$\begin{aligned}\lim_{h\to 0}\frac{g(x+h)-g(x)}{h} &= \lim_{h\to 0}\frac{c\cdot f(x+h)-c\cdot f(x)}{h}\\ &= c\cdot\lim_{h\to 0}\frac{f(x+h)-f(x)}{h} = c\cdot f'(x)\end{aligned}$$

Für das vorletzte Gleichheitszeichen siehe ▸ Rechnen mit Grenzwerten.

Ableitungsregeln

Bemerkung:

Wir verwenden im Weiteren häufiger Abkürzungen wie $c \cdot f$ (Produkt einer Funktion mit einer Konstante c).

Ebenso schreiben wir $f + g$ und $f \cdot g$ für die punktweise Addition und Multiplikation von zwei Funktionen. Dabei gilt $(f + g)(x) = f(x) + g(x)$ und $(f \cdot g)(x) = f(x) \cdot g(x)$.

Bereits eingeführt wurde die Notation $f \circ g$ (Verknüpfung von Funktionen ▸ Verknüpfung).

Ableitungsregeln

Summenregel

Seien $f, g : X \to \mathbb{R}$ differenzierbare Funktionen mit Ableitungen f', g' und sei $k : X \to \mathbb{R}$ definiert als $k(x) = f(x) + g(x)$. Dann gilt:

$$k'(x) = (f+g)'(x) = f'(x) + g'(x)$$

Beweis:

$$\lim_{h\to 0} \frac{k(x+h) - k(x)}{h} = \lim_{h\to 0} \frac{f(x+h) + g(x+h) - f(x) - g(x)}{h}$$

$$= \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} + \lim_{h\to 0} \frac{g(x+h) - g(x)}{h} = f'(x) + g'(x)$$

Für das vorletzte Gleichheitszeichen siehe wieder .

Ableitungsregeln

Produktregel

Seien $f, g\colon X \to \mathbb{R}$ differenzierbare Funktionen mit Ableitungen f', g' und sei $k\colon X \to \mathbb{R}$ definiert als $k(x) = f(x) \cdot g(x)$. Dann gilt:

$$k'(x) = (f \cdot g)'(x) = f'(x) \cdot g(x) + f(x) \cdot g'(x)$$

Auch zum Beweis der Produktregel benötigt man die Rechenregeln für Grenzwerte ▸ Rechnen mit Grenzwerten:

Ableitungsregeln

Beweis der Produktregel:

$$\lim_{h\to 0}\frac{k(x+h)-k(x)}{h} = \lim_{h\to 0}\frac{f(x+h)\cdot g(x+h)-f(x)\cdot g(x)}{h}$$

$$= \lim_{h\to 0}\left(\frac{f(x+h)\cdot g(x)-f(x)\cdot g(x)}{h} + \frac{f(x+h)\cdot g(x+h)-f(x+h)\cdot g(x)}{h}\right)$$

$$= \lim_{h\to 0}\left(\frac{f(x+h)-f(x)}{h}\cdot g(x) + f(x+h)\cdot\frac{g(x+h)-g(x)}{h}\right)$$

$$= \left(\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}\right)\cdot g(x) + \left(\lim_{h\to 0} f(x+h)\right)\cdot\left(\lim_{h\to 0}\frac{g(x+h)-g(x)}{h}\right)$$

$$= f'(x)\cdot g(x) + f(x)\cdot g'(x)$$

Ableitungsregeln

Wir betrachten nun Anwendungen der bisher eingeführten Ableitungsregeln für Funktionen $f : \mathbb{R} \to \mathbb{R}$. Für die Ableitung eines Polynoms verwendet man die Faktor- und die Summenregel.

Ableiten eines Polynoms

Sei $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ mit $a_i \in \mathbb{R}$, $n \in \mathbb{N}_0$.

Dann gilt:

$f'(x) = n \cdot a_n \cdot x^{n-1} + (n-1) \cdot a_{n-1} \cdot x^{n-2} + \cdots + a_1$

Beispiel:

Die Ableitung von $f(x) = x^5 - 2x^3$ ist $f'(x) = 5x^4 - 6x^2$.

Ableitungsregeln

Beispiel für die Anwendung der Produktregel:

Die Ableitung von $f(x) = x^2 \cdot 2^x$ ist

$$f'(x) = 2x \cdot 2^x + x^2 \cdot \ln(2) \cdot 2^x = (2x + \ln(2) \cdot x^2) \cdot 2^x.$$

Ableitungsregeln

Kettenregel

Seien $f : \mathbb{R} \to \mathbb{R}$, $g : X \to \mathbb{R}$ differenzierbare Funktionen mit Ableitungen f', g' und sei $k : X \to \mathbb{R}$ definiert als $k(x) = f(g(x)) = (f \circ g)(x)$. Dann gilt:

$$k'(x) = (f \circ g)'(x) = f'(g(x)) \cdot g'(x)$$

(Ohne Beweis)

Ableitungsregeln

Beispiel für die Anwendung der Kettenregel:

Die Ableitung von $f(x) = 2^{x^2}$ ist

$$f'(x) = \ln(2) \cdot 2^{x^2} \cdot 2x = 2 \cdot \ln(2) \cdot x \cdot 2^{x^2}$$

Bemerkung:

Die Multiplikation mit dem Faktor $g'(x)$ bei der Kettenregel bezeichnet man manchmal auch als "Nachdifferenzieren".

Ableitungsregeln

Durch die Kombination der Kettenregel und der Beziehung $\frac{d}{dx}x^c = c \cdot x^{c-1}$ ergibt sich die Kehrwertregel.

Kehrwertregel

Sei $g\colon X \to \mathbb{R}$ eine differenzierbare Funktionen mit Ableitung g' und sei $k\colon X \to \mathbb{R}$ definiert als $k(x) = \frac{1}{g(x)}$. Dann gilt:

$$k'(x) = -\frac{g'(x)}{g(x)^2},$$

falls $g(x) \neq 0$.

Beweis:

$$k'(x) = \frac{d}{dx}g(x)^{-1} = (-1) \cdot g(x)^{-2} \cdot g'(x) = -\frac{g'(x)}{g(x)^2}$$

Ableitungsregeln

Wenn man nun die Kehrwertregel mit der Produktregel kombiniert, erhält man die Quotientenregel.

Quotientenregel

Seien $f: X \to \mathbb{R}$, $g: X \to \mathbb{R}$ differenzierbare Funktionen mit Ableitungen f', g' und sei $k: X \to \mathbb{R}$ definiert als $k(x) = \frac{f(x)}{g(x)}$.
Dann gilt:

$$k'(x) = \frac{f'(x) \cdot g(x) - f(x) \cdot g'(x)}{g(x)^2},$$

falls $g(x) \neq 0$.

Ableitungsregeln

Beweis der Quotientenregel:

$$\begin{aligned} k'(x) &= \frac{d}{dx}\left(f(x) \cdot \frac{1}{g(x)}\right) \\ &= f'(x) \cdot \frac{1}{g(x)} + f(x) \cdot \left(-\frac{g'(x)}{g(x)^2}\right) \\ &= \frac{f'(x) \cdot g(x) - f(x) \cdot g'(x)}{g(x)^2} \end{aligned}$$

Ableitungsregeln

Beispiel:

Die Ableitung von $f(x) = \frac{\sin x}{x}$ ist

$$f'(x) = \frac{(\cos x) \cdot x - (\sin x) \cdot 1}{x^2} = \frac{(\cos x) \cdot x - (\sin x)}{x^2}$$

für $x \neq 0$.

Mehrfache Ableitungen

Man kann Ableitungen nochmal differenzieren und erhält dann die zweite Ableitung, dritte Ableitung, ...

n-te Ableitungen

Für eine differenzierbare Funktion $f: X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}$ definieren wir Funktionen $f^{(n)}: X \to \mathbb{R}$ mit:

$$f^{(0)}(x) = f(x) \qquad f^{(n+1)}(x) = (f^{(n)})'(x)$$

Dabei wird gefordert, dass jede Funktion $f^{(n)}$ wiederum differenzierbar ist.

Für das Polynom $p: \mathbb{R} \to \mathbb{R}$ mit $p(x) = x^2 + 3x - 2$ gilt:
0-te Ableitung: die Funktion p selbst, d.h. $p^{(0)} = p$
1-te Ableitung: $p^{(1)}(x) = p'(x) = 2x + 3$
2-te Ableitung: $p^{(2)}(x) = p''(x) = 2$
3-te und weitere Ableitungen: $p^{(3)}(x) = p^{(4)}(x) = \cdots = 0$

Kurvendiskussion

Da die Ableitung einer Funktion f deren Steigung beschreibt, kann man aus ihr Schlüsse über die Funktion ziehen:

Schlüsse aus der ersten Ableitung

- $f'(x) > 0$: Funktion f steigt an der Stelle x
- $f'(x) < 0$: Funktion f fällt an der Stelle x

Schlüsse aus der zweiten Ableitung

- $f''(x) > 0$: Ableitung f' steigt an der Stelle x, d.h., f ist an der Stelle x linksgekrümmt
- $f''(x) < 0$: Ableitung f' fällt an der Stelle x, d.h., f ist an der Stelle x rechtsgekrümmt

Kurvendiskussion

Mit Hilfe der Ableitungen kann man auch Aussagen über die Extrema, d.h. Minima und Maxima, einer Funktion machen.

Lokale Extrema

Eine Funktion $f : X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}$ hat an der Stelle x_0 ein lokales Minimum, wenn es ein $\varepsilon > 0$ gibt mit $f(x_0) \leq f(x)$ für alle x mit $|x_0 - x| < \varepsilon$.

Eine Funktion $f : X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}$ hat an der Stelle x_0 ein lokales Maximum, wenn es ein $\varepsilon > 0$ gibt mit $f(x_0) \geq f(x)$ für alle y mit $|x_0 - x| < \varepsilon$.

Lokale Minima und Maxima heißen auch lokale Extrema.

Ein lokales Minimum (Maximum) ist nicht notwendigerweise auch ein globales Minimum (Maximum) der Funktion.

Kurvendiskussion

Lokale Extrema und erste Ableitungen

Hat eine differenzierbare Funktion $f : X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}$ an der Stelle x_0 ein lokales Extremum, so muss an dieser Stelle $f'(x_0) = 0$ gelten.

Anschauliche Begründung: bei einem Extremum wechselt die Steigung einer Funktion von negativ nach positiv (oder umgekehrt) und muss daher an dieser Stelle den Wert 0 einnehmen.

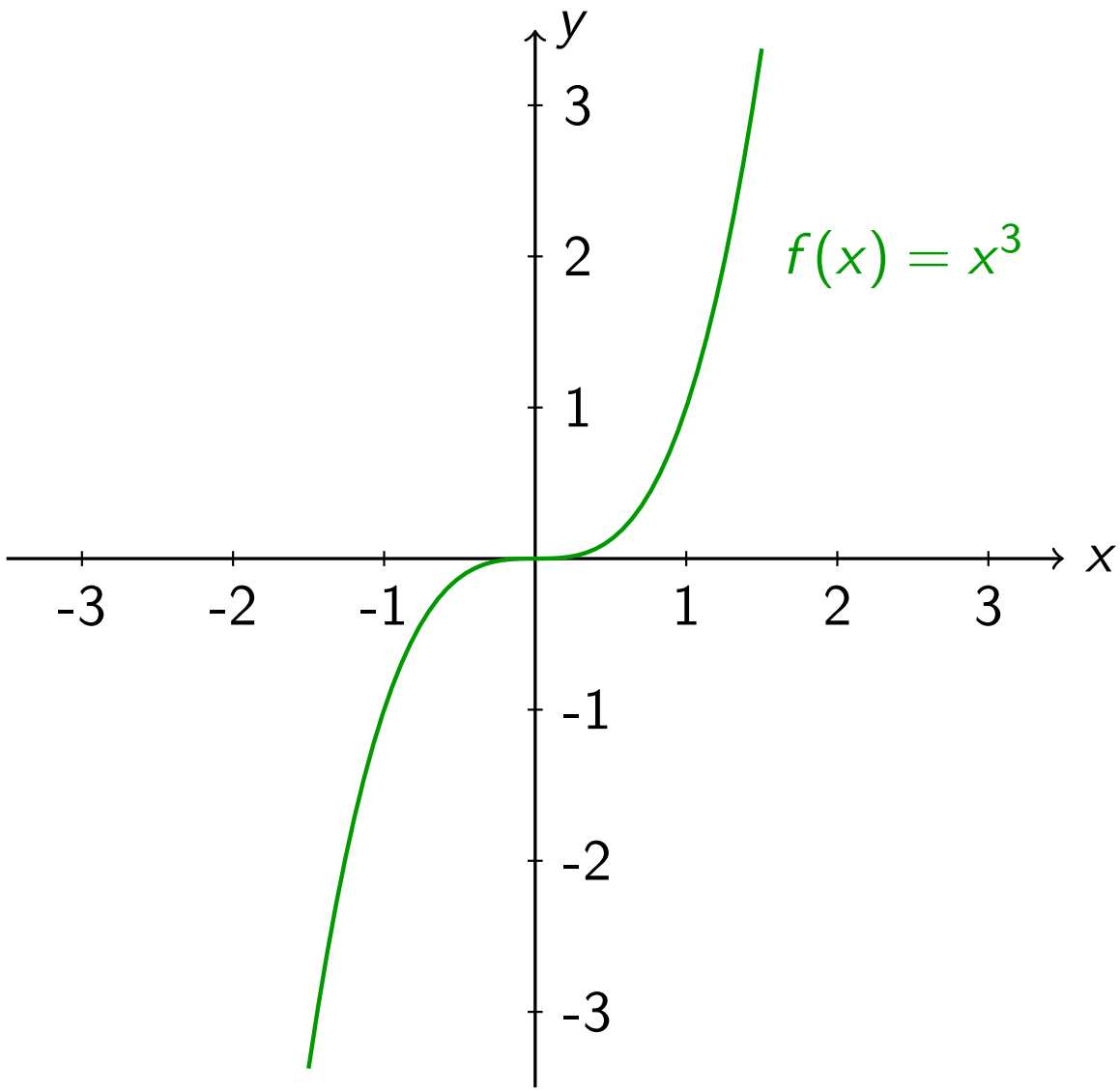
Kurvendiskussion

Bemerkung:

Allerdings gibt es Nullstellen der ersten Ableitung, an denen die Funktion kein Extremum einnimmt, sondern einen sogenannten Sattelpunkt (eine Stelle mit Steigung 0, an der aber kein Extremum vorliegt).

Für $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^3$ gilt $f'(x) = 3x^2$ und es gilt $f'(0) = 0$. Jedoch gibt es an der Stelle $x_0 = 0$ weder ein lokales Minimum noch ein lokales Maximum (siehe Abbildung).

Kurvendiskussion



Kurvendiskussion

Die allgemeine Regel für die Bestimmung von lokalen Minima und Maxima lautet wie folgt:

Lokale Extrema und n-te Ableitungen

Sei $f : X \to \mathbb{R}$ eine Funktion und $f^{(n)} : X \to \mathbb{R}$, $n \in \mathbb{N}_0$ ihre n-ten Ableitungen. Für $x_0 \in X$ gilt $f'(x_0) = 0$ und $n \in \mathbb{N}_0 \setminus \{0\}$ ist die kleinste Zahl, für die $f^{(n)}(x_0) \neq 0$ gilt. Wir unterscheiden nun folgende Fälle:

- n ist gerade:
  - $f^{(n)}(x_0) < 0 \rightsquigarrow$ lokales Maximum an der Stelle x_0
  - $f^{(n)}(x_0) > 0 \rightsquigarrow$ lokales Minimum an der Stelle x_0
- n ist ungerade $\rightsquigarrow$ Sattelpunkt an der Stelle x_0

Kurvendiskussion

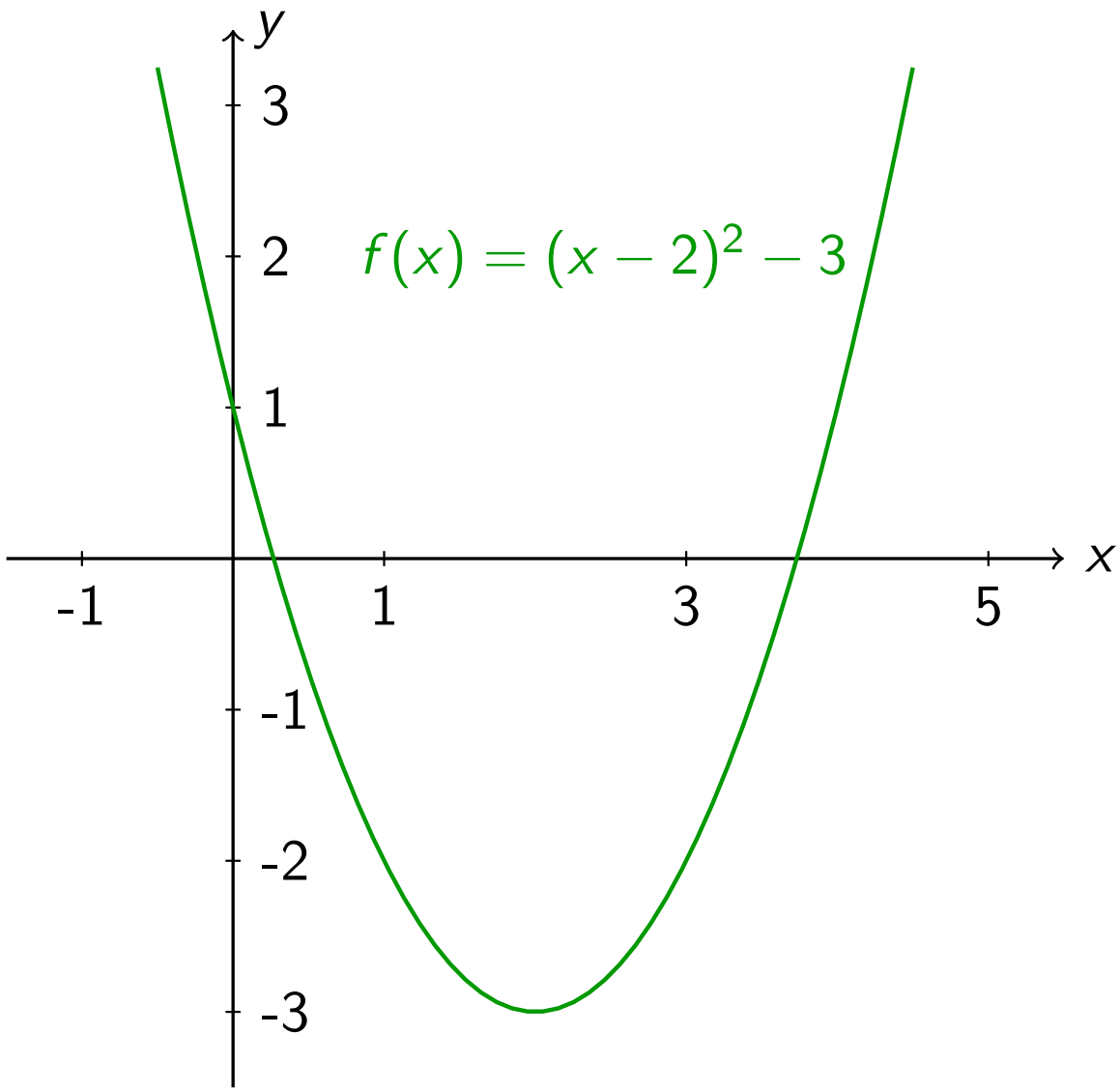
Beispiel 1: $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = (x-2)^2 - 3$

1-te Ableitung: $f'(x) = 2 \cdot (x-2) = 2x - 4$, Nullstelle bei $x = 2$

2-te Ableitung: $f''(x) = 2$, $f''(2) = 2 > 0$

D.h., es gibt ein (lokales) Minimum an der Stelle $x = 2$ mit Funktionswert $f(2) = -3$.

Kurvendiskussion



Kurvendiskussion

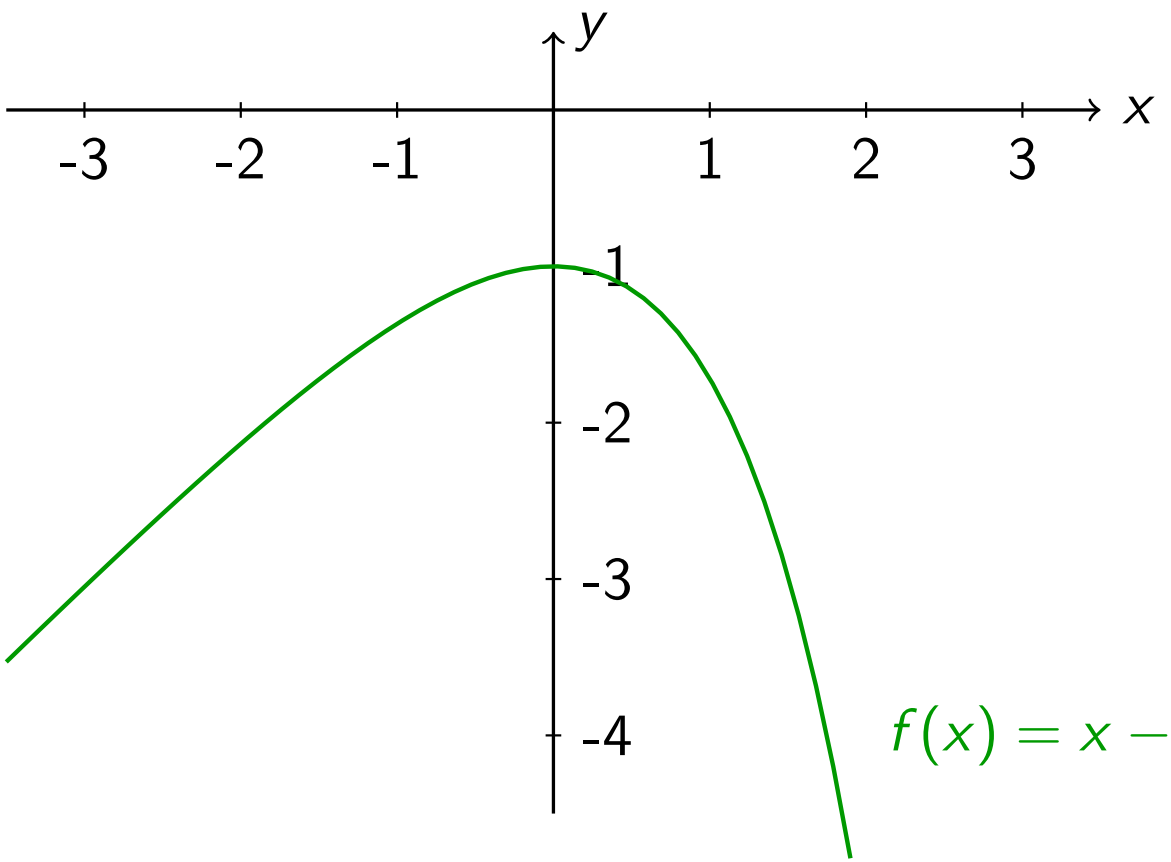
Beispiel 2: $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x - e^x$

1-te Ableitung: $f'(x) = 1 - e^x$, Nullstelle bei $x = 0$

2-te Ableitung: $f''(x) = -e^x$, $f''(0) = -1 < 0$

D.h., es gibt ein (lokales) Maximum an der Stelle $x = 0$ mit Funktionswert $f(0) = -1$.

Kurvendiskussion



$f(x) = x - e^x$

Kurvendiskussion

Beispiel 3: $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^5 - 2x^3$

1-te Ableitung: $f'(x) = 5x^4 - 6x^2 = 5x^2(x^2 - \frac{6}{5})$, Nullstellen bei

$$x = 0,\ x = -\sqrt{\tfrac{6}{5}} \text{ und } x = \sqrt{\tfrac{6}{5}} \quad \left(\sqrt{\tfrac{6}{5}} \approx 1,095\ldots\right)$$

2-te Ableitung: $f''(x) = 20x^3 - 12x$, es gilt

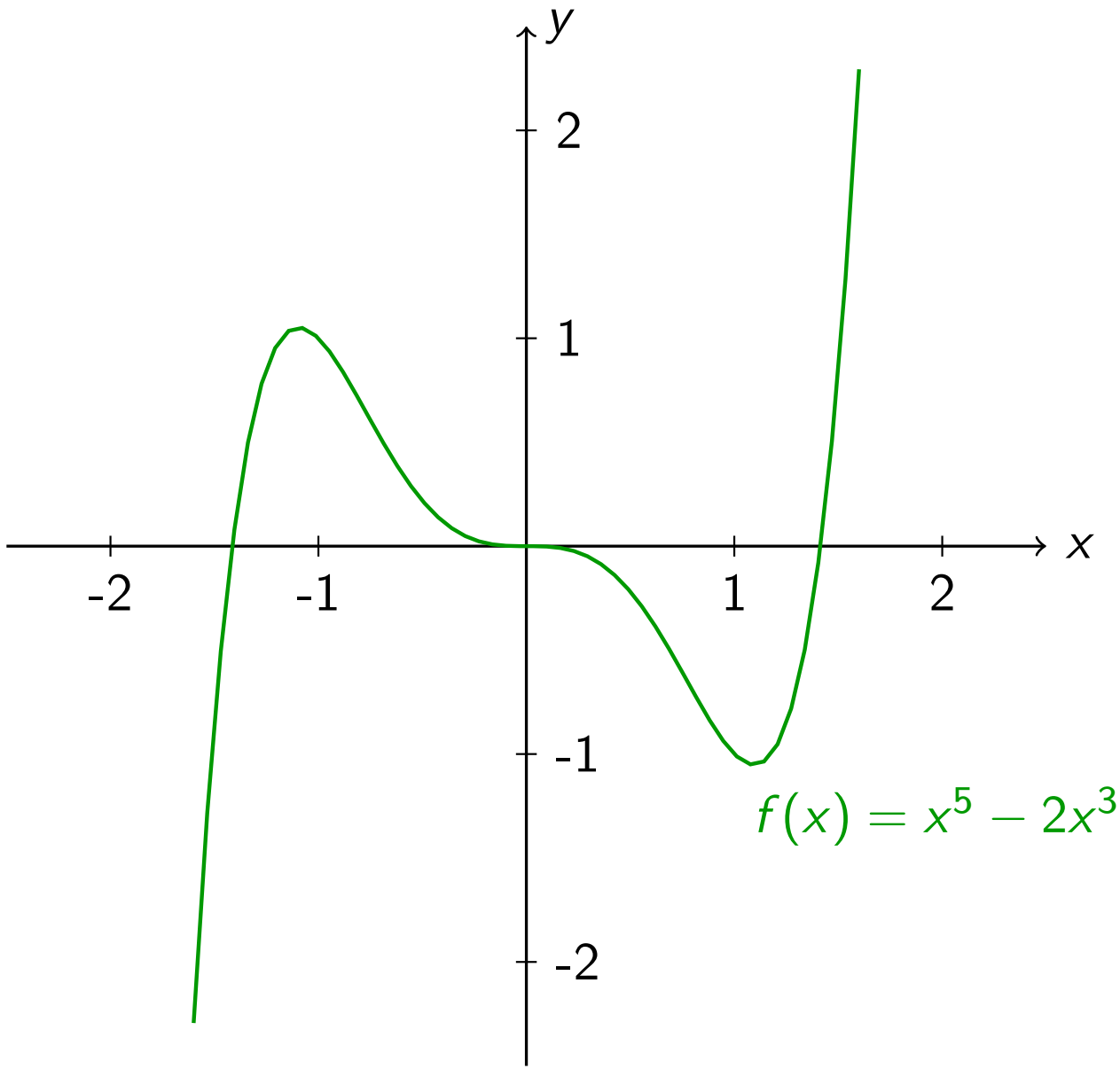
$$f''\left(-\sqrt{\tfrac{6}{5}}\right) \approx -13,145\cdots < 0,$$

$$f''\left(\sqrt{\tfrac{6}{5}}\right) \approx 13,145\cdots > 0,\ f''(0) = 0$$

3-te Ableitung: $f'''(x) = 60x^2 - 12,\ f'''(0) = -12$

D.h., es gibt ein lokales Maximum an der Stelle $x = -\sqrt{\frac{6}{5}}$, ein lokales Minimum an der Stelle $x = \sqrt{\frac{6}{5}}$ und einen Sattelpunkt an der Stelle $x = 0$.
Die lokalen Extrema sind hier keine globalen Extrema.

Kurvendiskussion



Kurvendiskussion

Wendepunkte

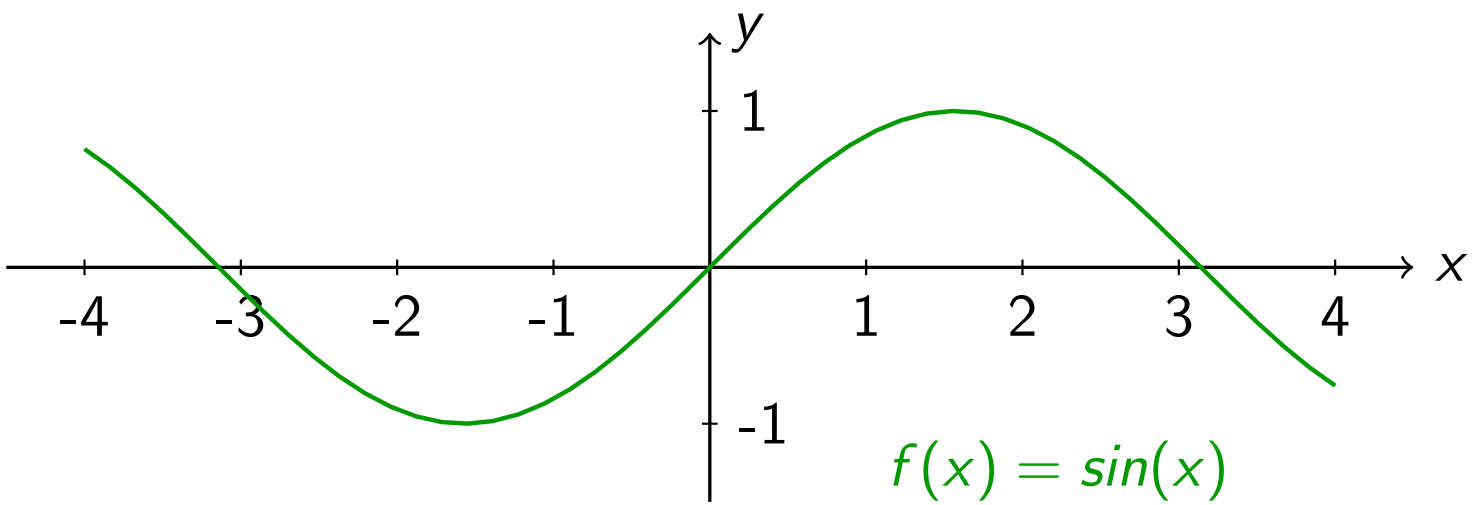
Sei $f : X \to \mathbb{R}$ eine differenzierbare Funktion mit $f''(x_0) = 0$ und $f'''(x_0) \neq 0$ für ein $x_0 \in X$, d.h., die zweite Ableitung ist gleich null und die dritte Ableitung ungleich Null.

Dann gibt es an dieser Stelle einen Wendepunkt, bei dem die Kurve ihre Krümmung ändert (von links- auf rechtsgekrümmt oder umgekehrt).

Kurvendiskussion

Beispiel 1:

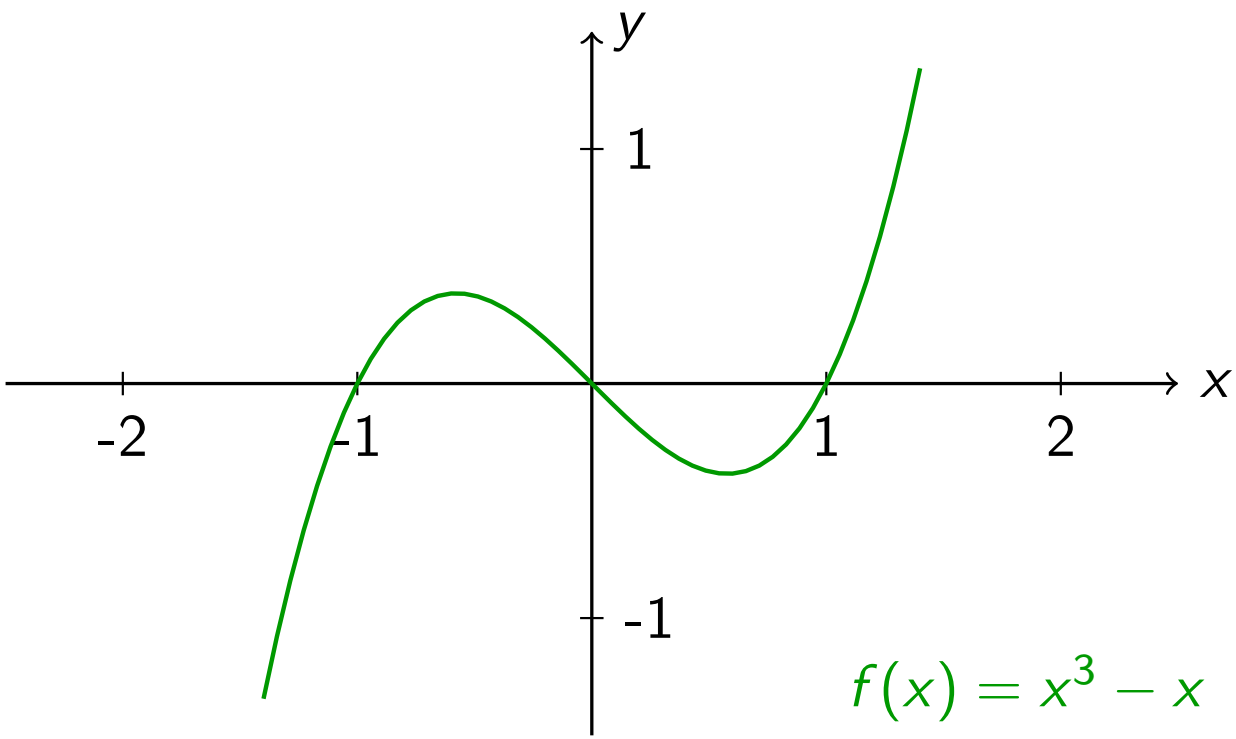
Die Sinuskurve hat (unter anderem) einen Wendepunkt an der Stelle $x_0 = 0$.



Kurvendiskussion

Beispiel 2:

Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = (x-1) \cdot x \cdot (x+1) = x^3 - x$ hat (genau) einen Wendepunkt, und zwar an der Stelle $x_0 = 0$.



Zahlen

Division mit Rest

Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen mit $a \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $z, r \in \mathbb{Z}$ mit $0 \leq r < |a|$ und

$$z \cdot a + r = b$$

- z heißt Ergebnis der ganzzahligen Division von b durch a und man schreibt $z = b$ div a.
- r heißt Rest der ganzzahligen Division von b durch a und man schreibt $r = b$ mod a.

Dabei ist $|a|$ der Absolutwert von a, beispielsweise ist $|-7| = 7$.
Im Folgenden wird a aber immer eine positive ganze Zahl sein.

Zahlen

Konkret (z.B. bei Verwendung eines Taschenrechners) lassen sich (b div a) und (b mod a) folgendermaßen berechnen (für den Fall, dass $a > 0$):

$$b \text{ div } a = \left\lfloor \frac{b}{a} \right\rfloor \qquad b \text{ mod } a = b - a \cdot \left\lfloor \frac{b}{a} \right\rfloor$$

Dabei steht $\lfloor q \rfloor$ mit $q \in \mathbb{R}$ für die Abrundung von q nach unten. D.h., $\lfloor q \rfloor$ ist die größte ganze Zahl, die kleiner gleich q ist.

Beispiele: $\lfloor 3 \rfloor = 3$, $\lfloor 5,17 \rfloor = 5$, $\lfloor \pi \rfloor = 3$, $\lfloor -1 \rfloor = -1$, $\lfloor -0,7 \rfloor = -1$

Zahlen

Ein Spezialfall der Division mit Rest ist die Teilbarkeit:

Teilbarkeit

Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen. Man sagt, a teilt b, wenn es ein $z \in \mathbb{Z}$ gibt mit $a \cdot z = b$.
Wir schreiben auch $a \mid b$ und nennen a Teiler von b.

Bemerkung: Hier wird auch $a = 0$ erlaubt.

Die Relation $\mid$ (Teilbarkeit) ist eine partielle Ordnung, wenn man sie auf die natürlichen Zahlen einschränkt.

Zahlen

Gelten folgende Beziehungen?

$2 \mid 18$	(Ja, $z = 9$)
$-7 \mid 14$	(Ja, $z = -2$)
$3 \mid 10$	(Nein)
$0 \mid 0$	(Ja, z beliebig)
$0 \mid 7$	(Nein)
$7 \mid 0$	(Ja, $z = 0$)

Zahlen

Primzahl

Eine Zahl $p \in \mathbb{N}_0$ heißt Primzahl, wenn folgendes gilt:

- $p \neq 0$ und $p \neq 1$
- die einzigen Teiler von p in den natürlichen Zahlen sind 1 und p selbst.

Primzahlen: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$

Es gibt unendlich viele Primzahlen.

Zahlen

Eindeutigkeit der Primfaktorzerlegung

Sei $n \in \mathbb{N}_0$ mit $n \neq 0$ eine natürliche Zahl. Ein Produkt $p_1 \cdot \dots \cdot p_m = n$ von Primzahlen heißt Primfaktorzerlegung von n.

Jede Zahl $n \neq 0$ besitzt eine solche Primfaktorzerlegung.
Wenn man zudem verlangt, dass die Primfaktoren in aufsteigender Reihenfolge angeordnet sind ($p_i \leq p_j$ für $i < j$), so ist die Primfaktorzerlegung einer Zahl eindeutig.

Bemerkungen:

- Die Primfaktorzerlegung von 1 ist das leere Produkt.
- Wenn wir auch die 1 als Primzahl einführen würden, so würden wir die die Eindeutigkeit der Primfaktorzerlegung verlieren. ($7 = 1 \cdot 7 = 1 \cdot 1 \cdot 7 = \dots$).

Zahlen

Größter gemeinsamer Teiler

Seien $a, b \in \mathbb{N}_0$ (wobei mindestens eine der beiden Zahlen verschieden von 0 ist). Eine Zahl $d \in \mathbb{N}_0$ heißt größter gemeinsamer Teiler von a und b ($d = ggT(a, b)$), falls folgendes gilt:

- $d \mid a$ und $d \mid b$, d.h., d teilt sowohl a als auch b.
- für jede andere natürliche Zahl d', die a und b teilt, gilt: $d' \leq d$.

Zahlen

Kleinstes gemeinsames Vielfaches

Seien $a, b \in \mathbb{N}_0$. Eine Zahl $m \in \mathbb{N}_0$ mit $m \neq 0$ heißt kleinstes gemeinsames Vielfaches von a und b ($m = kgV(a, b)$), falls folgendes gilt:

- $a \mid m$ und $b \mid m$, d.h., sowohl a als auch b teilen m.
- für jede andere natürliche Zahl m', die von a und b geteilt wird, gilt: $m \leq m'$.

Zahlen

Wie bestimmt man den größten gemeinsamen Teiler?

Bestimmung von $d = ggT(a, b)$ – Methode 1

- Bestimme die Primfaktorzerlegungen von a und b
- Betrachte alle Primfaktoren p, die in beiden Zerlegungen vorkommen: angenommen p kommt in a k-mal und in b ℓ-mal vor. Dann kommt p in d genau $\min(k, \ell)$-mal vor.

Beispiel: $ggT(12, 30)$

- $12 = 2 \cdot 2 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$
- $ggT(12, 30) = 2 \cdot 3 = 6$.

Zahlen

Bestimmung von $d = ggT(a, b)$ – Methode 2 (Euklidischer Algorithmus)

- $ggT(0, a) = a$
- $ggT(a, b) = ggT(b, a)$
- $ggT(a, b) = ggT(a - b, b)$, falls $b \leq a$

Wende diese Regeln zur ggT-Berechnung so lange an, bis ein Ausdruck der Form $ggT(0, a)$ erreicht wird.

$$ggT(12, 30) = ggT(30, 12) = ggT(18, 12) = ggT(6, 12)$$
$$= ggT(12, 6) = ggT(6, 6) = ggT(0, 6) = 6$$

Zahlen

Bemerkung:

Die Methode 2 ist bei weitem effizienter, insbesondere, wenn man die dritte Regel durch

$$ggT(a, b) = ggT(a \bmod b, b) \quad \text{falls } b \leq a$$

ersetzt.

Zahlen

Der ggT und die ggT-Berechnung sind ein wichtiges Werkzeug für das Lösen bestimmter Gleichungen.

Lösen diophantischer Gleichungen

Gegeben seien $a, b, c \in \mathbb{N}_0$ (wobei mindestens eine der beiden Zahlen a, b verschieden von 0 ist). Wir suchen Lösungen $x, y \in \mathbb{Z}$ der Gleichung

$$a \cdot x + b \cdot y = c$$

Es gilt:

- Diese Gleichung hat genau dann eine Lösung, wenn $ggT(a, b) \mid c$.

Zahlen

Für Gleichungen der Form $a \cdot x + b \cdot y = ggT(a, b)$ kann man x, y dadurch bestimmen, dass man die ggT-Berechnung "rückwärts" nachvollzieht.

Beispiel: Lösen von $30 \cdot x + 12 \cdot y = 6$.

$$\begin{aligned} ggT(12, 30) = ggT(12, 18) = ggT(6, 12) = ggT(6, 6) \\ = ggT(6, 0) = ggT(0, 6) = 6 \end{aligned}$$

Dabei wurden die Zahlen folgendermaßen ermittelt:
$18 = 30 - 12$, $6 = 18 - 12$.

Damit kann man einsetzen:

$$6 = 18 - 12 = (30 - 12) - 12 = 30 \cdot 1 + 12 \cdot (-2)$$

Und damit hat man eine Lösung $x = 1$, $y = -2$.

Zahlen

Gleichungen der Form $a \cdot x + b \cdot y = c$ mit $c \neq ggT(a, b)$ (aber $ggT(a, b) \mid c$) kann man folgendermaßen lösen:

- Zunächst die Gleichung $a \cdot x' + b \cdot y' = ggT(a, b)$ lösen.
- Dann die Lösungen x', y' mit $c/ggT(a, b)$ multiplizieren, das ergibt die Lösungen x, y.

Beispiel: Lösen von $30 \cdot x + 12 \cdot y = 24$

$\rightsquigarrow$ Lösen von $30 \cdot x' + 12 \cdot y' = 6$ ergibt $x' = 1$, $y' = -2$.

$\rightsquigarrow$ mit $24/6 = 4$ multiplizieren ergibt $x = 4$, $y = -8$.

Zahlen

Teilerfremdheit

Zwei Zahlen $a, b \in \mathbb{N}_0$ heißen teilerfremd, falls $ggT(a, b) = 1$.

Eulersche φ-Funktion

Die Eulersche φ-Funktion $\varphi\colon \mathbb{N}_0 \to \mathbb{N}_0$ ist folgendermaßen definiert:

- $\varphi(n)$ mit $n \in \mathbb{N}_0$ ist die Anzahl der Zahlen zwischen 1 und n, die zu n teilerfremd sind.

$$\varphi(n) = |\{m \in \mathbb{N}_0 \mid 1 \leq m \leq n \text{ und } ggT(m, n) = 1\}|$$

Zahlen

Beispiele (Eulersche φ-Funktion):

n	$\varphi(n)$	n	$\varphi(n)$
0	0	7	6
1	1	8	4
2	1	9	6
3	2	10	4
4	2	11	10
5	4	12	4
6	2	13	12

Für eine Primzahl p gilt $\varphi(p) = p - 1$.

Außerdem gilt:

- $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, falls m, n teilerfremd sind.
- $\varphi(p^k) = p^k - p^{k-1}$, falls p eine Primzahl ist.

Monoide, Gruppen, Körper

Wir betrachten nun grundlegende "Rechenstrukturen". Das sind Strukturen, mit denen man rechnen kann wie mit (natürlichen/rationalen/reellen) Zahlen, die aber möglicherweise andere Elemente enthalten.

Dabei beantworten u.a. wir folgende Fragen:

- Welche (gemeinsamen) Eigenschaften haben Addition und Multiplikation?
- Wie unterscheiden sich $\mathbb{N}_0$ und $\mathbb{Z}$?
- Kann man auch mit endlichen Mengen von Objekten rechnen?
- Was sind mögliche Anwendungen in der Kryptographie?

Monoide, Gruppen, Körper

Monoid

Gegen sei eine Menge M und eine zweistellige Abbildung $\circ\colon M \times M \to M$. Wir benutzen meist die Infix-Schreibweise: $\circ((m_1, m_2)) = m_1 \circ m_2$ und bezeichnen $\circ$ als zweistelligen Operator.

$(M, \circ)$ heißt Monoid, falls folgendes gilt:

- $\circ$ ist assoziativ, d.h., es gilt $m_1 \circ (m_2 \circ m_3) = (m_1 \circ m_2) \circ m_3$ für alle $m_1, m_2, m_3 \in M$.
- Es gibt ein neutrales Element $e \in M$, für das gilt: $e \circ m = m \circ e = m$ für alle $m \in M$.

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Monoide

- $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind Monoide
  (neutrales Element: 0)
- $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ sind Monoide
  (neutrales Element: 1)
- $(\mathbb{Z}, -)$ ist kein Monoid
  (fehlende Assoziativität)

Monoide, Gruppen, Körper

Modulo-Rechnen

Wir definieren $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ mit folgender Addition $+_n$ und Multiplikation $\cdot_n$. Seien $k, \ell \in \mathbb{Z}_n$, dann gilt:

$$k +_n \ell = (k + \ell) \bmod n \qquad k \cdot_n \ell = (k \cdot \ell) \bmod n$$

$(\mathbb{Z}_n, +_n)$ und $(\mathbb{Z}_n, \cdot_n)$ sind Monoide
(mit neutralen Elementen 0 bzw. 1)

Sie spielen eine große Rolle u.a. in der Kryptographie und Kodierungstheorie.

Monoide, Gruppen, Körper

Bemerkungen:

Bei Modulo-Rechnungen kann man Addition/Multiplikation und Modulo-Rechnung beliebig tauschen. Es gilt nämlich:

Modulo-Gesetze

- $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
- $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$
- $a^k \bmod n = (a \bmod n)^k \bmod n$

Statt $(x \bmod n) = (a \bmod n)$ schreibt man oft auch:

$$x \equiv a \pmod{n}.$$

Monoide, Gruppen, Körper

Additions-/Multiplikationstabellen für $\mathbb{Z}_5$:

$+_n$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_n$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Monoide, Gruppen, Körper

In vielen Fällen (z.B. zum Lösen von Gleichungssystemen) benötigt man beim Rechnen etwas mehr Struktur: man braucht sogenannte Inverse.

Gruppe

Ein Monoid $(G, \circ)$ mit neutralem Element e heißt Gruppe, wenn zusätzlich zu den Monoid-Eigenschaften noch folgendes gilt:

- für jedes $g \in G$ gibt es ein $g^{-1} \in G$ mit $g \circ g^{-1} = e$.

Dabei heißt g^{-1} das Inverse von g.

$(G, \circ)$ heißt kommutative Gruppe (oder abelsche Gruppe), falls außerdem $g_1 \circ g_2 = g_2 \circ g_1$ für alle $g_1, g_2 \in G$ gilt.

Bemerkung: In jeder Gruppe gilt nicht nur $g \circ g^{-1} = e$, sondern auch $g^{-1} \circ g = e$ für alle $g \in G$.

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Gruppen

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind Gruppen
  (Inverses zu x ist $-x$)
- $(\mathbb{N}_0, +)$ ist keine Gruppe
  (fehlende Inverse)
- $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$ sind Gruppen
  (Inverses zu x ist $\frac{1}{x}$)
- $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ sind keine Gruppen
  (0 hat kein Inverses)
- $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}\backslash\{0\}, \cdot)$ sind keine Gruppen
  (fehlende Inverse)

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Gruppen (Fortsetzung)

- $(\mathbb{Z}_n, +_n)$ ist eine Gruppe
- $(\mathbb{Z}_n, \cdot_n)$ ist keine Gruppe
  (0 hat kein Inverses)
- $(\mathbb{Z}_n \backslash \{0\}, \cdot_n)$ ist genau dann eine Gruppe, wenn n eine Primzahl ist.
  (Ein Element $m \in \mathbb{Z}_n$ hat genau dann ein Inverses, wenn m, n teilerfremd sind.)

Monoide, Gruppen, Körper

Am Beispiel $\mathbb{Z}_4$ ($n = 4$):

Es gilt $n = 4 = 2 \cdot 2$, d.h., 4 ist keine Primzahl.

$m = 2$ hat kein multiplikatives Inverses in $\mathbb{Z}_4$, denn $ggT(2, 4) = 2 \neq 1$.

Insbesondere hat die Gleichung $2 \cdot_4 x = (2 \cdot x) \bmod 4 = 1$ keine Lösung: $2 \cdot x$ ist für alle $x \in \mathbb{Z}$ eine gerade Zahl und $(2 \cdot x) \bmod 4$ ist daher ebenfalls eine gerade Zahl. D.h., man kann niemals das Ergebnis 1 erhalten.

Die Zahlen 1 und 3 sind allerdings teilerfremd zu n und besitzen multiplikative Inverse in $\mathbb{Z}_4$.

Monoide, Gruppen, Körper

Inversenbildung in $(\mathbb{Z}_n, +_n)$

Das Inverse zu $m \in \mathbb{Z}_n$ bezüglich der Addition $+_n$ ist $-_n m = (-m) \bmod n = (n - m) \bmod n$. Es gilt:

$$m +_n (-_n m) = (m + (-m)) \bmod n = 0 \bmod n = 0$$

Monoide, Gruppen, Körper

Für die Bildung von multiplikativen Inversen in $\mathbb{Z}_n$ benötigen wir folgenden Satz:

Satz von Euler-Fermat

Für teilerfremde Zahlen $m, n \in \mathbb{N}_0$ mit $n > 1$ gilt:

$$m^{\varphi(n)} \bmod n = 1$$

▸ Eulersche φ-Funktion

Monoide, Gruppen, Körper

Inversenbildung in $(\mathbb{Z}_n, \cdot_n)$ (Methode 1)

Mit dem Satz von Euler-Fermat:

$$m^{-1} = m^{\varphi(n)-1} \bmod n$$

Denn es gilt

$$m \cdot_n m^{-1} = (m \cdot m^{\varphi(n)-1}) \bmod n = m^{\varphi(n)} \bmod n = 1$$

Bemerkung: Inversenbildung funktioniert nur dann, wenn m, n teilerfremd sind. (Ansonsten hat m kein multiplikatives Inverses.) Diese Bedingung ist immer erfüllt, falls $m \neq 0$ und n eine Primzahl ist.

Monoide, Gruppen, Körper

Beispiel: Wir berechnen das multiplikative Inverse von 3 in $\mathbb{Z}_5$.

$3^{-1} = 3^{\varphi(5)-1} \bmod 5 = 3^3 \bmod 5 = 27 \bmod 5 = 2$

Test: $3 \cdot_5 2 = (3 \cdot 2) \bmod 5 = 6 \bmod 5 = 1$.

Monoide, Gruppen, Körper

Inversenbildung in $(\mathbb{Z}_n, \cdot_n)$ (Methode 2)

Das Inverse zu $m \in \mathbb{Z}_n$ bezüglich der Multiplikation $\cdot_n$ kann auch folgendermaßen bestimmt werden:

- Diophantische Gleichung $m \cdot x + n \cdot y = 1$ lösen.
- Bestimme Inverses $m^{-1} = x \bmod n$.

Denn es gilt:

$$m \cdot_n m^{-1} = m \cdot_n (x \bmod n) = (m \cdot x) \bmod n = (1 - n \cdot y) \bmod n = 1$$

Diese Methode funktioniert auch dann, wenn der Wert $\varphi(n)$ nicht einfach berechnet werden kann (z.B. wenn n sehr groß ist).

Monoide, Gruppen, Körper

Beispiel: Wir berechnen wieder das multiplikative Inverses von 3 in $\mathbb{Z}_5$.

Löse $3 \cdot x + 5 \cdot y = 1$:

$$ggT(3,5) = ggT(5,3) = ggT(2,3) = ggT(3,2) = ggT(1,2)$$
$$= ggT(2,1) = ggT(1,1) = ggT(0,1) = 1$$

Rückwärts einsetzen: $1 = 3 - 2 = 3 - (5 - 3) = 3 \cdot 2 + 5 \cdot (-1)$

Wir erhalten die Lösungen $x = 2$, $y = -1$

Bestimme $m^{-1} = x \bmod n = 2 \bmod 5 = 2$.

Monoide, Gruppen, Körper

Tabelle der Inversen in $(\mathbb{Z}_5 \setminus \{0\}, \cdot_5)$:

m	1	2	3	4
m^{-1}	1	3	2	4

Monoide, Gruppen, Körper

Nun betrachten wir noch eine Rechenstruktur, die zwei (miteinander kompatible) Operationen (normalerweise $+$ und $\cdot$) vereint.

Körper

Sei $(K, +, \cdot)$ ein Tupel, das aus einer Menge K und zwei zweistelligen Operationen $+$ und $\cdot$ auf K besteht.

$(K, +, \cdot)$ heißt Körper, falls folgendes gilt:

- $(K, +)$ ist eine kommutative Gruppe mit neutralem Element 0.
- $(K \backslash \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1.
- Das Distributivgesetz gilt: das heißt, für alle $a, b, c \in K$ gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Monoide, Gruppen, Körper

Körperaxiome (Zusammenfassung, Teil 1)

Für einen Körper $(K, +, \cdot)$ muss gelten:

- $+ : K \times K \to K$ und $\cdot : K \times K \to K$ sind zweistellige Operationen auf K.
- $+$ und $\cdot$ sind assoziativ, d.h., es gilt für alle $x, y, z \in K$:

$$(x + y) + z = x + (y + z) \quad \text{und} \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

- $+$ hat ein neutrales Element, welches mit 0 bezeichnet wird und $\cdot$ hat ein neutrales Element, welches mit 1 bezeichnet wird.

Monoide, Gruppen, Körper

Körperaxiome (Zusammenfassung, Teil 2)

- Jedes Element hat ein additives Inverses und jedes Element, außer 0, hat ein multiplikatives Inverses.
- $+$ und $\cdot$ sind kommutativ, d.h., es gilt für alle $x, y \in K$:

$$x + y = y + x \qquad \text{und} \qquad x \cdot y = y \cdot x$$

- Es gilt das Distributivgesetz, d.h., für alle $x, y, z \in K$ gilt

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

(Das zweite Distributivgesetz folgt aus dem ersten aufgrund der Kommutativität von $\cdot$.)

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Körper

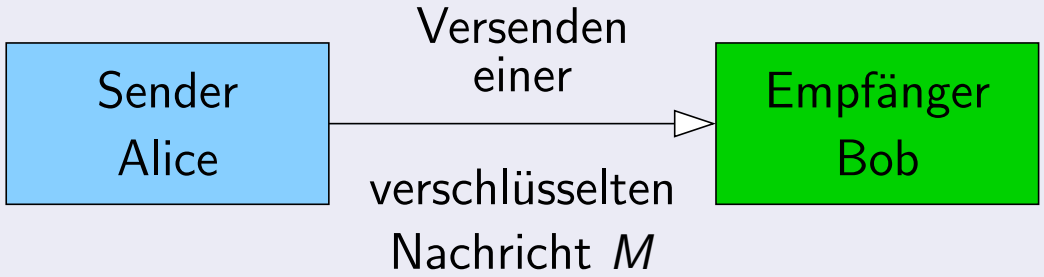
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper
- $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper, falls n eine Primzahl ist

Weitere Beispiele für Körper (auf die wir nicht mehr weiter eingehen): komplexe Zahlen, endliche Körper (mit $4, 8, 9, \ldots$ Elementen), ...

Anwendungsbeispiel: RSA

Wir betrachten eine Anwendung im Bereich der asymmetrischen Verschlüsselung (public-key cryptography).

Das sogenannte RSA-Verfahren (benannt nach Rivest, Shamir, Adleman) ist die Grundlage von wichtigen Kommunikationsprotokollen im Internet. Außerdem bildet es die Basis von elektronischen Signaturen.



- Alice will eine Nachricht M an Bob verschicken.
- Alice verwendet den öffentlichen Schlüssel von Bob zum Verschlüsseln.
- Bob verwendet seinen privaten Schlüssel zum Entschlüsseln.

Anwendungsbeispiel: RSA

1. Schritt: Schlüsselerzeugung

- Bob generiert zwei große Primzahlen p, q mit $p \neq q$ und setzt $n = p \cdot q$.
- Bob bestimmt $\varphi(n)$
  (in diesem Fall gilt $\varphi(n) = (p-1) \cdot (q-1)$).
- Bob bestimmt d, e mit $(d \cdot e) \bmod \varphi(n) = 1$
  (d.h., d, e sind in $\mathbb{Z}_{\varphi(n)}$ zueinander multiplikativ invers)
- (e, n) ist der öffentliche Schlüssel, den Bob bekanntgibt.
- (d, n) ist der private Schlüssel, den Bob geheimhält.

Anwendungsbeispiel: RSA

2. Schritt: Verschlüsselung

- Alice will eine Nachricht M an Bob verschlüsseln. Sie kodiert diese Nachricht als eine Zahl $m \in \mathbb{Z}_n$ (z.B. durch Binärkodierung).
- Alice rechnet $c = m^e \bmod n$ und schickt c an Bob.

Hier wird also in $\mathbb{Z}_n$ gerechnet.

3. Schritt: Entschlüsselung

- Bob empfängt c.
- Er rechnet $m = c^d \bmod n$ und erhält damit wieder die ursprüngliche Nachricht.

Wie bei der Verschlüsselung wird hier wieder in $\mathbb{Z}_n$ gerechnet.

Anwendungsbeispiel: RSA

Rechenbeispiel RSA

- $p = 5$, $q = 11$, $n = 5 \cdot 11 = 55$
- $\varphi(n) = (p-1) \cdot (q-1) = 4 \cdot 10 = 40$
- Wähle $e = 3$ und berechne das Inverse (Methode 2):
  - Löse $3 \cdot x + 40 \cdot y = 1$, ergibt Lösungen $x = -13$, $y = 1$
  - Setze $d = x \bmod 40 = (-13) \bmod 40 = 27$
- Nachricht $m = 9$ soll übertragen werden. Alice berechnet die Kodierung $c = 9^3 \bmod 55 = 729 \bmod 55 = 14$.
- Code $c = 14$ kommt an. Bob rechnet

$$
\begin{aligned}
14^{27} \bmod 55 &= (14^3 \bmod 55)^9 \bmod 55 \\
&= (2744 \bmod 55)^9 \bmod 55 = 49^9 \bmod 55 \\
&= (49^3 \bmod 55)^3 \bmod 55 = (117649 \bmod 55)^3 \bmod 55 \\
&= 4^3 \bmod 55 = 64 \bmod 55 = 9 = m
\end{aligned}
$$

Anwendungsbeispiel: RSA

Warum funktioniert RSA?

Korrektheit: Warum erhält Bob wieder die ursprüngliche Nachricht?

Das kann mit dem Satz von Euler-Fermat nachgewiesen werden.

Es gilt $(e \cdot d \bmod \varphi(n)) = 1$ und damit gibt es eine Zahl z mit $e \cdot d = z \cdot \varphi(n) + 1$. Also entsteht beim Verschlüsseln und anschließenden Entschlüsseln:

$$(m^e \bmod n)^d \bmod n = m^{e \cdot d} \bmod n = m^{z \cdot \varphi(n)+1} \bmod n$$
$$= (m \cdot (m^{\varphi(n)})^z) \bmod n = m \cdot 1^z \bmod n = m \bmod n = m$$

Diese Argumentation funktioniert nicht, falls m, n nicht teilerfremd sind. In diesem Fall kann man aber anders nachweisen, dass man trotzdem das richtige Ergebnis erhält.

Anwendungsbeispiel: RSA

Warum funktioniert RSA? (Fortsetzung)

Sicherheit: Warum ist es für andere Teilnehmer (außer Bob) schwierig, die Nachricht zu entschlüsseln?

Das liegt daran, dass man d nur dann leicht aus e berechnen kann, wenn man $\varphi(n)$ kennt. Um $\varphi(n)$ zu berechnen, müsste man die Primfaktorzerlegung von großen Zahlen n (ca. 1024–2048 Bits) bestimmen, was sehr schwer ist.

Vektorräume und Matrizen

Wir betrachten nun Vektoren, die Tupel von Elementen eines Körpers sind. Mengen von Vektoren bilden einen sogenannten Vektorraum.

Vektoren sind wichtig für die Darstellung geometrischer Objekte. Matrizen werden dazu verwendet, um (lineare) Funktionen in Vektorräumen zu beschreiben. Sie spielen auch eine wichtige Rolle beim Lösen von Gleichungssystemen.

Vektorräume und Matrizen

Vektor

Sei $n \in \mathbb{N}_0$ eine natürliche Zahl und $(K, +, \cdot)$ ein Körper. Ein Vektor $\vec{u}$ der Dimension n über K besteht aus n Elementen $u_1, \ldots, u_n \in K$ des Körpers.

Ein Vektor wird im allgemeinen folgendermaßen dargestellt und heißt daher auch Spaltenvektor.

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

Vektorräume und Matrizen

Vektorraum

Die Menge aller Vektoren der Dimension n über K heißt n-dimensionaler Vektorraum über K und wird mit K^n bezeichnet.

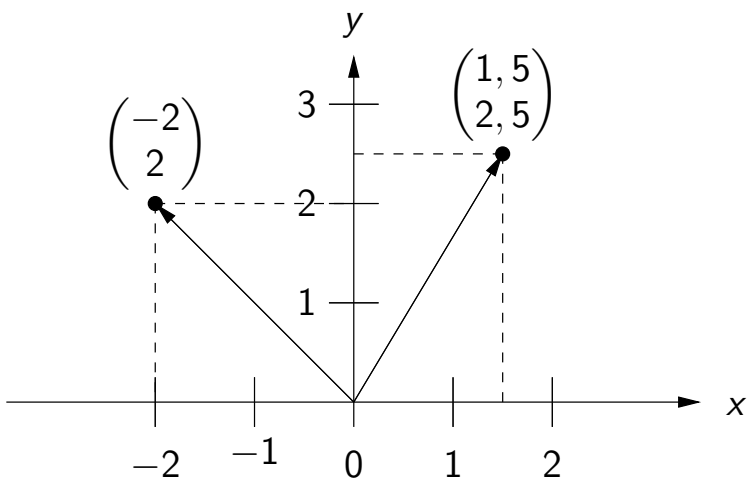
Hinweis: es gibt noch allgemeinere Definitionen eines Vektorraums (ähnlich zu den Definitionen von Monoid, Gruppe, Körper), die wir hier aber nicht betrachten.

Die Operationen auf einem Vektorraum sind Addition von Vektoren und Skalarmultiplikation, die im Folgenden betrachtet werden.

Vektorräume und Matrizen

Klassisches Beispiel: Sei $n = 2$ und $K = \mathbb{R}$, d.h., wir betrachten den Vektorraum $\mathbb{R}^2$.

Dann handelt es sich bei den Vektoren um Punkte im zweidimensionalen Raum. Diese werden auch durch Pfeile – ausgehend vom Ursprung des Koordinatensystems – dargestellt.



Die erste Koordinate bezeichnet man dabei – wie üblich – als x-Koordinate, die zweite als y-Koordinate.

Vektorräume und Matrizen

In Vektorräumen sind verschiedene Operationen definiert:

Addition von Vektoren

Die Addition auf Vektoren ist eine zweistelligen Operation $+ : K^n \times K^n \to K^n$, die folgendermaßen definiert ist:

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix}$$

Dabei werden die einzelnen Körperelemente mit Hilfe der $+$-Operation des Körpers verknüpft.

Vektorräume und Matrizen

Vektorraum als Gruppe

Ein Vektorraum mit der Addition ist eine kommutative Gruppe. Das neutrale Element ist der Nullvektor $\vec{0}$ und das additive Inverse zu $\vec{u}$ wird mit $-\vec{u}$ bezeichnet:

$$\vec{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{Falls } \vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \text{ dann ist } -\vec{u} = \begin{pmatrix} -u_1 \\ \vdots \\ -u_n \end{pmatrix}.$$

Dabei sind $-u_1, \ldots, -u_n$ die additiven Inversen im Körper.

Vektorräume und Matrizen

Multiplikation mit einem Skalar

Ein Vektor $\vec{u} \in K^n$ kann mit einem einzelnen Körperelement $k \in K$ multipliziert werden. Das Element k nennt man dann auch Skalar.

$$k \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} k \cdot u_1 \\ \vdots \\ k \cdot u_n \end{pmatrix}$$

Dabei entstehen $k \cdot u_1, \ldots, k \cdot u_n$ durch die Multiplikationsoperation im Körper.

Vektorräume und Matrizen

Eigenschaften der Multiplikation mit einem Skalar

Seien $\vec{u}, \vec{v} \in K^n$ Vektoren und $k, \ell \in K$ Skalare. Dann gilt:

$$\begin{aligned} k \cdot (\ell \cdot \vec{u}) &= (k \cdot \ell) \cdot \vec{u} \\ k \cdot (\vec{u} + \vec{v}) &= k \cdot \vec{u} + k \cdot \vec{v} \\ (k + \ell) \cdot \vec{u} &= k \cdot \vec{u} + \ell \cdot \vec{u} \\ 1 \cdot \vec{u} &= \vec{u} \end{aligned}$$

Dabei ist 1 das neutrale Element der Multiplikation im Körper.

Vektorräume und Matrizen

Wir betrachten nun bestimmte Abbildungen auf Vektorräumen: sogenannte lineare Abbildungen.

Lineare Abbildung

Seien K^n, K^m zwei Vektorräume. Eine Funktion $\psi\colon K^n \to K^m$ heißt lineare Abbildung, falls folgendes gilt:

$$\psi(\vec{u}+\vec{v}) = \psi(\vec{u}) + \psi(\vec{v}) \qquad \text{für alle } \vec{u}, \vec{v} \in K^n$$
$$\psi(k \cdot \vec{u}) = k \cdot \psi(\vec{u}) \qquad \text{für alle } \vec{u} \in K^n, k \in K$$

Die Multiplikation mit einem Skalar ist eine lineare Abbildung.

Auch viele der interessanten Abbildungen in der Geometrie sind linear (z.B. Drehungen, Spiegelungen).

Vektorräume und Matrizen

Wir betrachten nun Matrizen, mit denen solche linearen Abbildungen beschrieben werden können:

Matrix

Seien $m, n \in \mathbb{N}_0$ und K ein Körper. Eine $m \times n$-Matrix A über K besteht aus $m \cdot n$ Einträgen

$$A_{i,j} \in K \qquad \text{für } i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}$$

Sie wird folgendermaßen dargestellt:

$$A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix}$$

Vektorräume und Matrizen

Bemerkungen:

Eine $m \times n$-Matrix besteht also aus m Zeilen der Länge n, oder – anders ausgedrückt – aus n Spalten der Länge m.

Dabei heißt m Zeilendimension und n Spaltendimension der Matrix.

Bei einem Eintrag $A_{i,j}$ bezeichnet der erste Index i die Zeile, der zweite Index j die Spalte.

Eine Matrix, für die $m = n$ gilt, heißt quadratisch.

Vektorräume und Matrizen

Matrizen können mit Vektoren muliplizierт werden.

Multiplikation einer Matrix mit einem Vektor

Sei A eine $m \times n$-Matrix und $\vec{u} \in K^n$ ein Vektor der Dimension n. Dann ist $A \cdot \vec{u}$ folgender Vektor aus K^m:

$$A \cdot \vec{u} = \begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix} \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} A_{1,1} \cdot u_1 + \cdots + A_{1,n} \cdot u_n \\ \cdots \\ A_{m,1} \cdot u_1 + \cdots + A_{m,n} \cdot u_n \end{pmatrix}$$

Das heißt, in der i-ten Zeile des Spaltenvektors steht der Eintrag

$$\sum_{j=1}^{n} A_{i,j} \cdot u_j$$

Vektorräume und Matrizen

Bemerkung:

Wir verwenden das Summenzeichen Σ als abkürzende Schreibweise:

$$\sum_{j=1}^{n} a_j = a_1 + a_2 + \cdots + a_n$$

Rechenregeln für Summen

$$\sum_{j=1}^{n} (a_j + b_j) = \sum_{j=1}^{n} a_j + \sum_{j=1}^{n} b_j$$

$$\sum_{j=1}^{n} (k \cdot a_j) = k \cdot \sum_{j=1}^{n} a_j$$

Vektorräume und Matrizen

Beispiel: Multiplikation von Matrix und Vektor in $\mathbb{R}$

Multiplikation einer 2×3-Matrix mit einem Vektor der Dimension 3:

$$\begin{pmatrix} 3 & 4 & -1 \\ -2 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0,5 \\ -2 \end{pmatrix} = \begin{pmatrix} 3+2+2 \\ -2+1+6 \end{pmatrix} = \begin{pmatrix} 7 \\ 5 \end{pmatrix}$$

Vektorräume und Matrizen

Merkregel:

- Die Multiplikation einer $m \times n$-Matrix mit einem Vektor der Dimension n ergibt einen Vektor der Dimension m.
- Multipliziere die Zeilen der Matrix nacheinander mit der Spalte des Vektors (und addiere jeweils die Multiplikationsergebnisse auf).

Vektorräume und Matrizen

Matrix als lineare Abbildung

Eine $m \times n$-Matrix A über K beschreibt eine lineare Abbildung $\psi_A \colon K^n \to K^m$ wie folgt:

$$\psi_A(\vec{u}) = A \cdot \vec{u}$$

Durch Nachrechnen stellt man fest, dass tatsächlich die Eigenschaften einer linearen Abbildung erfüllt sind. Insbesondere gilt für eine Matrix A, Vektoren $\vec{u}, \vec{v}$ und einen Skalar k:

$$A \cdot (\vec{u} + \vec{v}) = A \cdot \vec{u} + A \cdot \vec{v} \qquad A \cdot (k \cdot \vec{u}) = k \cdot (A \cdot \vec{u})$$

Außerdem gibt es zu jeder linearen Abbildung $\psi \colon K^n \to K^m$ eine Matrix A mit $\psi = \psi_A$.

Vektorräume und Matrizen

Beispiel: wir betrachten folgende 2×2-Matrix als lineare Abbildung:

$$A = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}$$

Es gilt:

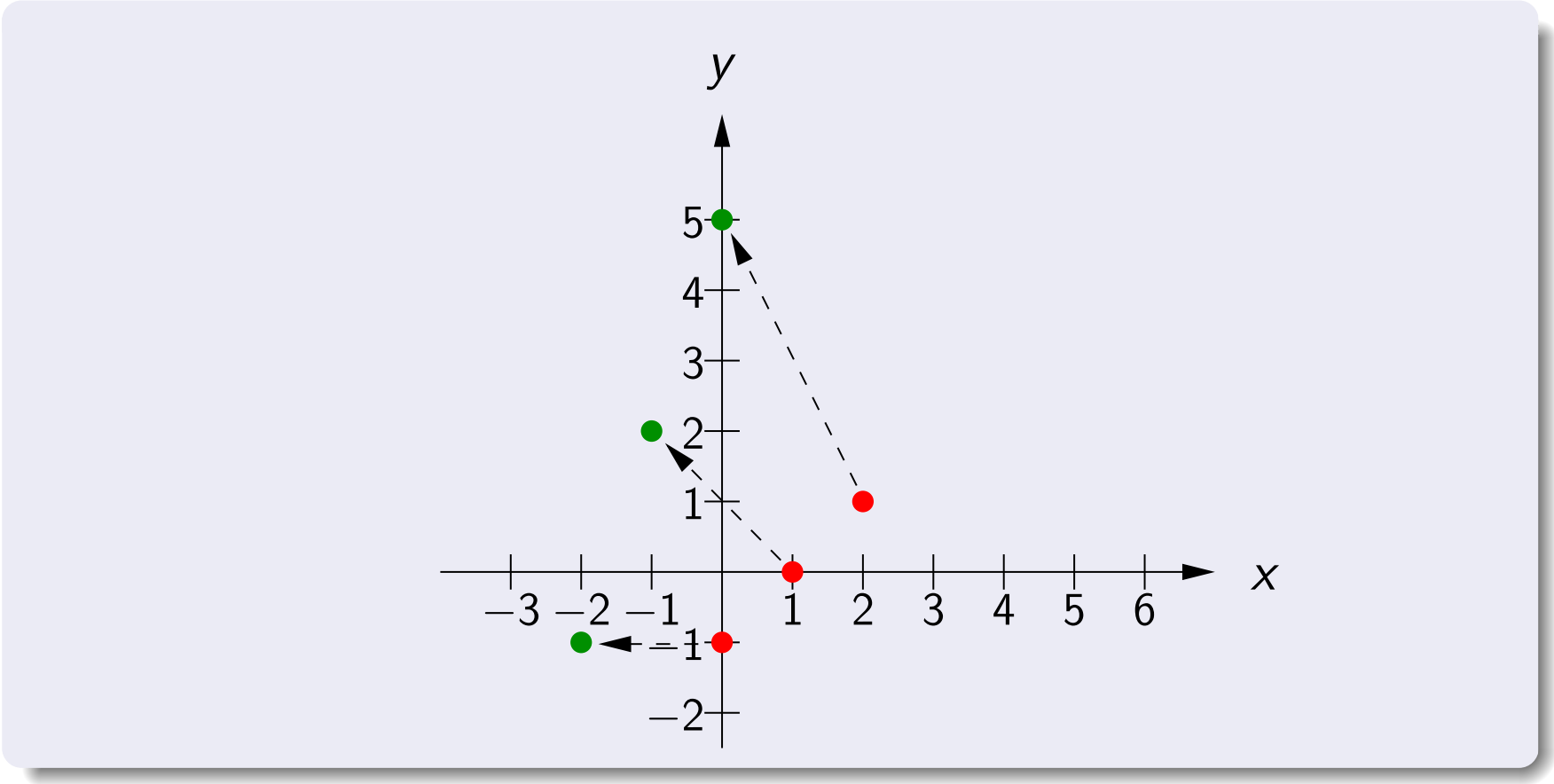
$$A \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \text{ d.h. } \psi_A(\begin{pmatrix} 0 \\ -1 \end{pmatrix}) = \begin{pmatrix} -2 \\ -1 \end{pmatrix}$$

$$A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \text{ d.h. } \psi_A(\begin{pmatrix} 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

$$A \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \text{ d.h. } \psi_A(\begin{pmatrix} 2 \\ 1 \end{pmatrix}) = \begin{pmatrix} 0 \\ 5 \end{pmatrix}$$

Vektorräume und Matrizen

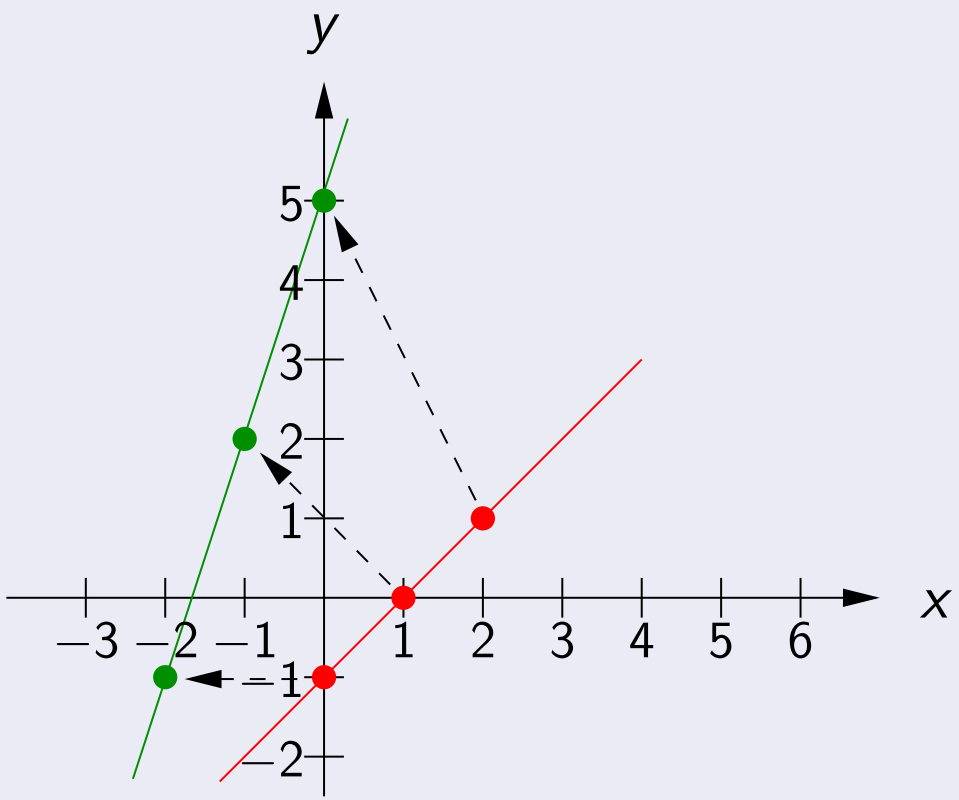
Graphische Darstellung:



Rote Punkte/Vektoren werden auf grüne Punkte/Vektoren abgebildet. Darstellung der Abbildungsvorschrift durch gestrichelte Pfeile.

Vektorräume und Matrizen

Graphische Darstellung:



Lineare Abbildungen bilden Geraden auf Geraden ab. Linien werden also erhalten. Daher stammt der Name!

Vektorräume und Matrizen

Zwei Matrizen gleicher Zeilen- und Spaltendimension können addiert werden:

Addition von Matrizen

Seien A, B $m \times n$-Matrizen. Dann hat $C = A + B$ folgendes Aussehen:

$$\begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix} + \begin{pmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{pmatrix} = \begin{pmatrix} C_{1,1} & \dots & C_{1,n} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,n} \end{pmatrix}$$

mit $C_{i,j} = A_{i,j} + B_{i,j}$.
Die Addition erfolgt komponentenweise.

Vektorräume und Matrizen

Matrizen als additive Gruppe

Die Menge aller $m \times n$-Matrizen über einem Körper K bildet eine kommutative Gruppe bezüglich der Addition.
Dabei ist die Nullmatrix N das neutrale Element und das additive Inverse zu A ist $-A$:

$$N = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \qquad -A = \begin{pmatrix} -A_{1,1} & \dots & -A_{1,n} \\ \vdots & \ddots & \vdots \\ -A_{m,1} & \dots & -A_{m,n} \end{pmatrix}$$

Vektorräume und Matrizen

Matrizen können auch miteinander multipliziert werden.

Multiplikation von Matrizen

Sei A eine $m \times n$-Matrix und B eine $n \times r$-Matrix. Dann ist $C = A \cdot B$ eine $m \times r$-Matrix und hat folgendes Aussehen:

$$\begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix} \cdot \begin{pmatrix} B_{1,1} & \dots & B_{1,r} \\ \vdots & \ddots & \vdots \\ B_{n,1} & \dots & B_{n,r} \end{pmatrix} = \begin{pmatrix} C_{1,1} & \dots & C_{1,r} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,r} \end{pmatrix}$$

mit

$$C_{i,j} = \sum_{\ell=1}^{n} A_{i,\ell} \cdot B_{\ell,j}$$

Vektorräume und Matrizen

Merkregel:

- Multipliziere die Zeilen der ersten Matrix (A) mit den Spalten der zweiten Matrix (B).
- Um in der Ergebnismatrix C den Eintrag $C_{i,j}$ zu erhalten, multipliziere die i-te Zeile der ersten Matrix (A) mit der j-ten Spalte der zweiten Matrix (B) und addiere jeweils die Multiplikationsergebnisse auf.

Vektorräume und Matrizen

Alternative Beschreibung: teile B in r (Spalten-)Vektoren auf

$$B = \begin{pmatrix} \vec{b}_1 & \dots & \vec{b}_r \end{pmatrix}$$

Multipliziere diese Spaltenvektoren dann einzeln. Die entstehenden Spaltenvektoren werden dabei von links nach rechts nebeneinandergeschrieben.

$$A \cdot B = A \cdot \begin{pmatrix} \vec{b}_1 & \dots & \vec{b}_r \end{pmatrix} = \begin{pmatrix} A \cdot \vec{b}_1 & \dots & A \cdot \vec{b}_r \end{pmatrix}$$

Multiplikation einer Matrix mit einem Vektor ist daher ein Spezialfall der Matrizenmultiplikation.

Vektorräume und Matrizen

Beispiel: Matrixmultiplikation in $\mathbb{R}$

Multiplikation einer 2×3-Matrix mit einer 3×2-Matrix:

$$\begin{pmatrix} 3 & 4 & -1 \\ -2 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0,5 & -3 \\ -2 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 3+2+2 & 0-12+1 \\ -2+1+6 & 0-6+3 \end{pmatrix} = \begin{pmatrix} 7 & -11 \\ 5 & -3 \end{pmatrix}$$

Vektorräume und Matrizen

Merkregel Falk-Schema: Folgende "Eselsbrücke" hilft bei der Matrizenmultiplikation $A \cdot B = C$

- Die zweite Matrix B wird nach oben verschoben.
- In dem Feld rechts von der ersten Matrix A und unterhalb der zweiten Matrix B entsteht dann die neue Matrix C.
- Ein Eintrag von C entsteht dadurch, dass die entsprechende Zeile von A und Spalte von B miteinander multipliziert werden.

$$\begin{pmatrix} 3 & 4 & -1 \\ -2 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0,5 & -3 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} 7 & -11 \\ 5 & -3 \end{pmatrix}$$

			1	0
			0,5	-3
			-2	-1
3	4	-1	7	-11
-2	2	-3	5	-3

Vektorräume und Matrizen

Assoziativität der Matrizenmultiplikation

Matrixmultiplikation ist assoziativ. D.h., falls A eine $m \times n$-Matrix, B eine $n \times r$-Matrix und C eine $r \times s$-Matrix ist, dann gilt:

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

Es macht keinen Sinn zu fragen, ob die Menge aller Matrizen beliebiger Dimension ein Monoid oder eine Gruppe bezüglich der Multiplikation ist. Es läßt sich nicht jede Matrix mit jeder Matrix verknüpfen, da die Dimensionen übereinstimmen müssen.

Diese Frage macht nur Sinn für quadratische Matrizen fester Dimension.

Vektorräume und Matrizen

Eigenschaften quadratischer Matrizen (I)

- Die Menge aller quadratischen $n \times n$-Matrizen bildet ein Monoid mit der Multiplikationsoperation.
- Insbesondere gibt es ein neutrales Element der Multiplikation, die sogenannte Einheitsmatrix E_n:

$$E_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

Diese Matrix hat Einsen in der Diagonale von links oben nach rechts unten und besteht ansonsten nur aus Nullen.

Vektorräume und Matrizen

Eigenschaften quadratischer Matrizen (II)

- Nicht jede quadratische Matrix A hat ein multiplikatives Inverses A^{-1}. Matrizen, die kein multiplikatives Inverses haben, heißen singulär.
- Matrizenmultiplikation ist außerdem nicht kommutativ.

Vektorräume und Matrizen

Beispiel 1: Multiplikation mit der Einheitsmatrix

$$E_3 \cdot \begin{pmatrix} -2 & 3 & 1 \\ 0,5 & 7 & -3 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 3 & 1 \\ 0,5 & 7 & -3 \\ 1 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} -2+0+0 & 3+0+0 & 1+0+0 \\ 0+0,5+0 & 0+7+0 & 0+(-3)+0 \\ 0+0+1 & 0+0+1 & 0+0+0 \end{pmatrix} = \begin{pmatrix} -2 & 3 & 1 \\ 0,5 & 7 & -3 \\ 1 & 1 & 0 \end{pmatrix}$$

Für jede $n \times n$-Matrix A gilt sowohl $E_n \cdot A = A$, als auch $A \cdot E_n = A$.

Vektorräume und Matrizen

Beispiel 2: Nicht-Existenz von Inversen

Die Nullmatrix, aber auch viele andere Matrizen haben kein Inverses. Wir betrachten folgende Matrix A:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Es gibt keine 3×3-Matrix B, so dass $A \cdot B$ die Einheitsmatrix ist:

$$A \cdot B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} B_{1,1} & B_{1,2} & B_{1,3} \\ B_{2,1} & B_{2,3} & B_{2,3} \\ B_{3,1} & B_{3,2} & B_{3,3} \end{pmatrix}$$

$$= \begin{pmatrix} B_{1,1} & B_{1,2} & B_{1,3} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_3$$

Vektorräume und Matrizen

Beispiel 3: Nicht-Kommutativität der Matrizenmultiplikation

$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 2 \\ 0 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 3 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

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

Vektorräume und Matrizen

Die Multiplikation von zwei Matrizen entspricht der Verknüpfung der dazugehörigen linearen Abbildungen.

Matrixmultiplikation und Verknüpfung linearer Abbildungen

Sei A eine $m \times n$-Matrix über und $\psi_A \colon K^n \to K^m$ die dazugehörige lineare Abbildung mit $\psi_A(\vec{u}) = A \cdot \vec{u}$. Analog sei B eine $n \times r$-Matrix und $\psi_B \colon K^r \to K^n$ die dazugehörige lineare Abbildung.

Dann beschreibt die Matrix $C = A \cdot B$ folgende lineare Abbildung $\psi_C \colon K^r \to K^m$ mit

$$\psi_C(\vec{u}) = (A \cdot B) \cdot \vec{u} = A \cdot (B \cdot \vec{u}) = A \cdot \psi_B(\vec{u}) = \psi_A(\psi_B(\vec{u}))$$

und damit gilt $\psi_C = \psi_{A \cdot B} = \psi_A \circ \psi_B$.

Das beruht im wesentlichen auf der Assoziativität der Matrixmultiplikation.

Erzeugendensysteme und Basen

Wir betrachten nun Konzepte, mit denen man einen Vektorraum aus einigen wenigen Vektoren, sogenannten Basisvektoren erzeugen kann.

Das hat auch Beziehungen zur Berechnung von multiplikativen Inversen einer Matrix und zum Lösen von Gleichungssystemen.

Erzeugendensysteme und Basen

Erzeugendensystem

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K. Eine Menge $S = \{\vec{v}_1, \ldots, \vec{v}_m\}$ von Vektoren heißt Erzeugendensystem des Vektorraums, falls sich jeder Vektor $\vec{u} \in K^n$ als Linearkombination von Vektoren aus S darstellen läßt. D.h., für jeden Vektor $\vec{u}$ gibt es Skalare $k_1, \ldots, k_m \in K$, so dass gilt:

$$\vec{u} = k_1 \cdot \vec{v}_1 + \cdots + k_m \cdot \vec{v}_m$$

Erzeugendensysteme und Basen

Beispiel 1: die Menge

$$S = \{\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\}$$

ist ein Erzeugendensystem für den Vektorraum $\mathbb{R}^2$. Ein Vektor $\vec{u}$ läßt sich immer folgendermaßen darstellen:

$$\vec{u} = \begin{pmatrix}u_1\\u_2\end{pmatrix} = \frac{u_1}{2} \cdot \begin{pmatrix}2\\0\end{pmatrix} + u_2 \cdot \begin{pmatrix}0\\1\end{pmatrix} + 0 \cdot \begin{pmatrix}1\\1\end{pmatrix}$$

Erzeugendensysteme und Basen

Bemerkung: Die Beziehung

$$\vec{u} = k_1 \cdot \vec{v}_1 + \cdots + k_m \cdot \vec{v}_m$$

kann auch dargestellt werden als

$$\vec{u} = \underbrace{\begin{pmatrix} \vec{v}_1 & \dots & \vec{v}_m \end{pmatrix}}_{V} \cdot \begin{pmatrix} k_1 \\ \vdots \\ k_m \end{pmatrix}$$

wobei $V = \begin{pmatrix} \vec{v}_1 & \dots & \vec{v}_m \end{pmatrix}$ eine Matrix ist, die aus den Spaltenvektoren $\vec{v}_1, \dots, \vec{v}_m$ zusammengesetzt ist.

D.h., eine Multiplikation einer Matrix mit einem Vektor ergibt eine Linearkombination der Spalten der Matrix.

Erzeugendensysteme und Basen

Die Menge S im vorherigen Beispiel enthält überflüssige Elemente, mindestens ein Vektor ist redundant. Beispielsweise kann der dritte Vektor durch die beiden ersten dargestellt werden.

Linear unabhängige Menge

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K. Eine Menge $S = \{\vec{v}_1, \ldots, \vec{v}_m\}$ von Vektoren heißt linear unabhängig, falls sich kein Vektor $\vec{v}$ aus S als Linearkombination der anderen Vektoren darstellen läßt.

Erzeugendensysteme und Basen

Beispiel 2: die Menge

$$S = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \}$$

ist linear unabhängig im $\mathbb{R}^3$, sie ist jedoch kein Erzeugendensystem.

Erzeugendensysteme und Basen

Alternative Definition für linear unabhängig:

Eine Menge $S = \{\vec{v}_1, \ldots, \vec{v}_m\}$ von Vektoren ist linear unabhängig, wenn für beliebige Skalare $k_1, \ldots, k_m \in K$ aus

$$k_1 \cdot \vec{v}_1 + \cdots + k_m \cdot \vec{v}_m = \vec{0}$$

immer $k_1 = \cdots = k_m = 0$ folgt.

Das heißt, man kann den Nullvektor nur auf eine Weise als Linearkombination von linear unabhängigen Vektoren darstellen: indem man alle Skalare mit 0 belegt.

In Kombination mit Lösungsverfahren für Gleichungssysteme ($\rightsquigarrow$ Gaußsches Eliminationsverfahren, wird im Anschluss behandelt), erhält man dadurch eine Methode, um zu überprüfen, ob eine Menge von Vektoren linear unabhängig ist.

Erzeugendensysteme und Basen

Basis

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K. Eine Menge $B = \{\vec{b}_1, \ldots, \vec{b}_m\}$ von Vektoren heißt Basis, falls sie gleichzeitig ein Erzeugendensystem und linear unabhängig ist.

Erzeugendensysteme und Basen

Beispiel 3: die Mengen

$$B_1 = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \}$$

und

$$B_2 = \{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix} \}$$

sind beides Basen des $\mathbb{R}^3$.

Für B_1 ist dies relativ offensichtlich. Aus B_2 kann man einfach die Elemente von B_1 (die sogenannten Einheitsvektoren) bestimmen und außerdem sind die drei Vektoren linear unabhängig.

Erzeugendensysteme und Basen

Beispiel 3: die Menge

$$B_3 = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} \}$$

ist keine Basis des $\mathbb{R}^3$, denn ihre Vektoren sind nicht linear unabhängig. Insbesondere kann man den dritten Vektor durch Linearkombination der anderen beiden Vektoren darstellen:

$$\begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} = (-2) \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

Erzeugendensysteme und Basen

Einheitsvektoren

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K und sei $i \in \{1, \ldots, n\}$. Der i-te Einheitsvektor $\vec{e_i}$ ist der Vektor, der an der i-ten Stelle eine 1 hat und sonst nur aus Nullen besteht.

$$\vec{e_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \ldots \quad \vec{e_n} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Erzeugendensysteme und Basen

Bemerkungen:

- Wenn B eine Basis des K^n ist, dann gibt es für jeden Vektor des K^n genau eine Möglichkeit, diesen als Linearkombination von Vektoren aus B darzustellen.
- Die Einheitsvektoren bilden immer eine Basis des K^n. Für jeden Vektor $\vec{u}$ gilt:

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = u_1 \cdot \vec{e}_1 + \cdots + u_n \cdot \vec{e}_n$$

- Die Einheitsvektoren sind jedoch nicht die einzige Basis.

Erzeugendensysteme und Basen

Weitere Bemerkungen:

- Ein Erzeugendensystem des K^n besteht immer aus mindestens n Vektoren. Eine Menge, die weniger als n Vektoren enthält, kann also kein Erzeugendensystem sein.
- Eine linear unabhängige Menge im K^n besteht immer aus höchstens n Vektoren. Eine Menge, die mehr als n Vektoren enthält, ist also immer linear abhängig.

Erzeugendensysteme und Basen

Weitere Bemerkungen:

- Eine Basis des K^n besteht immer aus genau n Vektoren.
- Eine linear unabhängige Menge mit n Vektoren ist immer eine Basis des K^n.
- Ein Erzeugendensystem mit n Vektoren ist auch immer eine Basis des K^n.

Erzeugendensysteme und Basen

Aus den letzten beiden Bemerkungen ergeben sich zwei einfache Verfahren, um festzustellen, ob eine Menge $B \subseteq K^n$ von Vektoren eine Basis des K^n ist oder nicht:

- Man überprüft, ob B genau n Vektoren enthält und ob diese Vektoren ein Erzeugendensystem sind.
- *Oder:* Man überprüft, ob B genau n Vektoren enthält und ob diese Vektoren linear unabhängig sind.

Insbesondere kann eine Menge von Vektoren, die mehr oder weniger als n Vektoren enthält, niemals eine Basis sein.

Erzeugendensysteme und Basen

Wir können nun die Frage beantworten, wann eine quadratische Matrix A invertierbar ist.

Angenommen die Matrix A ist invertierbar, d.h., es gibt ein multiplikatives Inverses A^{-1} mit $A \cdot A^{-1} = E_n$. Wir betrachten A^{-1} als aufgebaut aus einzelnen Spaltenvektoren $\vec{a}_1, \ldots, \vec{a}_n$, d.h. $A^{-1} = \begin{pmatrix} \vec{a}_1 & \ldots & \vec{a}_n \end{pmatrix}$. Dann gilt:

$$A \cdot A^{-1} = A \cdot \begin{pmatrix} \vec{a}_1 & \ldots & \vec{a}_n \end{pmatrix} = \begin{pmatrix} A \cdot \vec{a}_1 & \ldots & A \cdot \vec{a}_n \end{pmatrix} = \begin{pmatrix} \vec{e}_1 & \ldots & \vec{e}_n \end{pmatrix}$$

Es gilt also $A \cdot \vec{a}_i = \vec{e}_i$ für $i \in \{1, \ldots, n\}$. Das bedeutet, dass man aus den Spalten von A durch Linearkombination jeden Einheitsvektor (und damit auch jeden anderen Vektor) erhalten kann.

Erzeugendensysteme und Basen

Die Menge der Spaltenvektoren von A ist damit ein Erzeugendensystem und – da sie aus genau n Vektoren besteht – eine Basis.

Umgekehrt gilt auch, dass es zu einer Matrix, deren Spaltenvektoren eine Basis bilden, Vektoren $\vec{a}_1, \ldots, \vec{a}_n$ gibt, die die obigen Eigenschaften haben und aus denen man eine inverse Matrix konstruieren kann. (Wie man diese Vektoren berechnen kann, besprechen wir später.)

Erzeugendensysteme und Basen

Zusammenfassend gilt also:

Invertierbare Matrizen und Basen

Eine $n \times n$-Matrix A über einem Körper K ist invertierbar, genau dann, wenn die Spalten von A eine Basis des K^n bilden.

Man sagt dann auch, die Matrix hat den vollen Rang.

Gaußsches Eliminationsverfahren

Wir betrachten nun ein Verfahren zum Lösen von Gleichungssystemen.

Gegeben sei eine $m \times n$-Matrix A und ein m-dimensionaler Vektor $\vec{b}$. Gesucht ist ein n-dimensionaler Vektor $\vec{x}$, der folgende Gleichung erfüllt:

$$A \cdot \vec{x} = \vec{b}$$

Wenn A quadratisch ($m = n$) und zudem noch invertierbar ist, dann kann man zeigen, dass es genau eine Lösung $\vec{x}$ gibt: man multipliziert die obige Gleichung auf beiden Seiten mit A^{-1}:

$A^{-1} \cdot A \cdot \vec{x} = A^{-1} \cdot \vec{b}$ und daraus folgt wegen $A^{-1} \cdot A \cdot \vec{x} = E_n \cdot \vec{x} = \vec{x}$, dass $\vec{x} = A^{-1} \cdot \vec{b}$.

Gaußsches Eliminationsverfahren

Trotzdem bleiben noch viele offene Fragen:

- Wie berechnet man $\vec{x}$? (Wir haben ja noch kein Verfahren, um das multiplikative Inverse einer Matrix zu bestimmen.)
- Was passiert, wenn A nicht quadratisch oder nicht invertierbar ist?
- Kann eine Gleichung evtl. mehrere Lösungen haben?
- Kann eine Gleichung evtl. keine Lösung haben?

Gaußsches Eliminationsverfahren

Wir betrachten eine Gleichung in "ausgeschriebener" Form:

$$A \cdot \vec{x} = \vec{b}$$

wird geschrieben als

$$\begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

und das ist gleichbedeutend damit, dass das folgende Gleichungssystem eine Lösung hat:

$$\begin{aligned} A_{1,1} \cdot x_1 + \cdots + A_{1,n} \cdot x_n &= b_1 \\ &\vdots \\ A_{m,1} \cdot x_1 + \cdots + A_{m,n} \cdot x_n &= b_m \end{aligned}$$

Gaußsches Eliminationsverfahren

In den folgenden Beispielen arbeiten wir im Körper $\mathbb{R}$.

Beispiel 1: Gleichungssystem mit einer Lösung

$$\begin{aligned} 3 \cdot x_1 + 4 \cdot x_2 &= 2 \\ x_1 - 3 \cdot x_2 &= 5 \end{aligned}$$

Man kann dieses Gleichungssystem durch "geschicktes" Einsetzen lösen: zweite Gleichung wird umgeformt in $x_1 = 5 + 3 \cdot x_2$, eingesetzt in die erste Gleichung ergibt

$$3 \cdot (5 + 3 \cdot x_2) + 4 \cdot x_2 = 15 + 13 \cdot x_2 = 2$$

und daraus folgt $x_2 = -1$. Daher: $x_1 = 5 + 3 \cdot x_2 = 5 + 3 \cdot (-1) = 2$.

Die (einzige) Lösung ist damit $x_1 = 2$, $x_2 = -1$.

Gaußsches Eliminationsverfahren

Für dieses Beispiel gilt:

$$A = \begin{pmatrix} 3 & 4 \\ 1 & -3 \end{pmatrix} \qquad \vec{b} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

und A hat das multiplikative Inverse

$$A^{-1} = \begin{pmatrix} \frac{3}{13} & \frac{4}{13} \\ \frac{1}{13} & -\frac{3}{13} \end{pmatrix}$$

(Wir werden noch sehen, wie man solche Inverse tatsächlich berechnen kann.)

Test:

$$\vec{x} = A^{-1} \cdot \vec{b} = \begin{pmatrix} \frac{3}{13} & \frac{4}{13} \\ \frac{1}{13} & -\frac{3}{13} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} \frac{26}{13} \\ -\frac{13}{13} \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$$

Gaußsches Eliminationsverfahren

Beispiel 2: Gleichungssystem ohne Lösung

$$\begin{aligned} x_1 + 2 \cdot x_2 &= 3 \\ -2 \cdot x_1 - 4 \cdot x_2 &= 1 \end{aligned}$$

Man sieht, dass man $-2 \cdot x_1 - 4 \cdot x_2$ erhält, indem man $x_1 + 2 \cdot x_2$ mit -2 multipliziert. Also müsste auch das Ergebnis rechts unten ($= 1$) ein entsprechendes Vielfaches des Ergebnisses rechts oben ($= 3$) sein. Das ist aber nicht der Fall.
Daher hat das Gleichungssystem keine Lösung.

Hier sieht man, dass die Matrix

$$A = \begin{pmatrix} 1 & 2 \\ -2 & -4 \end{pmatrix}$$

aus linear abhängigen Spaltenvektoren besteht und nicht den vollen Rang hat. Sie ist also nicht invertierbar.

Gaußsches Eliminationsverfahren

Beispiel 3: Gleichungssystem mit mehreren Lösungen

$$\begin{aligned} x_1 + 2 \cdot x_2 &= 3 \\ -2 \cdot x_1 - 4 \cdot x_2 &= -6 \end{aligned}$$

Die untere Gleichung ist ein Vielfaches der oberen Gleichung (Faktor -2). Also ist die untere Gleichung redundant und wir müssen alle Lösungen der oberen Gleichung bestimmen. Es gilt $x_1 = 3 - 2 \cdot x_2$, also hat die Lösung $\vec{x}$ die Form:

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 - 2 \cdot x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

Dabei kann $x_2 \in \mathbb{R}$ beliebig gewählt werden und wir haben unendlich viele Lösungen.

Wie in Beispiel 2 ist die Matrix nicht invertierbar.

Gaußsches Eliminationsverfahren

Wir betrachten nun ein allgemeines Verfahren, um solche Gleichungssystem zu lösen: das Gaußsche Eliminationsverfahren. Der Einfachheit halber stellen wir ein Gleichungssystem folgendermaßen dar:

$$\begin{aligned} A_{1,1} \cdot x_1 + \cdots + A_{1,n} \cdot x_n &= b_1 \\ &\vdots \\ A_{m,1} \cdot x_1 + \cdots + A_{m,n} \cdot x_n &= b_m \end{aligned}$$

entspricht

$$\left(\begin{array}{ccc|c} A_{1,1} & \cdots & A_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ A_{m,1} & \cdots & A_{m,n} & b_m \end{array}\right)$$

Gaußsches Eliminationsverfahren

Das Gaußsche Eliminationsverfahren basiert auf folgenden Beobachtungen:

- Wenn man zwei Zeilen vertauscht, so ändern sich dadurch die Lösungen nicht.
- Wenn man eine Zeile mit einem Wert ungleich 0 multipliziert, so ändern sich dadurch die Lösungen nicht.
- Wenn man das Vielfache einer Zeile zu einer anderen Zeile addiert (von einer anderen Zeile subtrahiert), so ändern sich dadurch die Lösungen nicht.
- Wenn man zwei Spalten i, j vertauscht, so ändert sich dadurch die Reihenfolge der Variablen (Wert von x_i wird mit Wert von x_j vertauscht). Das kann man sich merken und am Ende wieder in Ordnung bringen.

Gaußsches Eliminationsverfahren

Ziel: wir bringen das Gleichungssystem durch die oben beschriebenen Umformungen auf folgende Form (obere Dreiecksform):

$$\left(\begin{array}{cccccc|c} A_{1,1} & A_{1,2} & \dots & A_{1,k} & \dots & A_{1,n} & b_1 \\ 0 & A_{2,2} & \dots & A_{2,k} & \dots & A_{2,n} & b_2 \\ \vdots & \ddots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & A_{k,k} & \dots & A_{k,n} & b_k \\ 0 & & & \dots & & 0 & b_{k+1} \\ \vdots & & & \ddots & & \vdots & \vdots \\ 0 & & & \dots & & 0 & b_m \end{array}\right)$$

wobei $A_{1,1} = 1, A_{2,2} = 1, \dots, A_{k,k} = 1$

Gaußsches Eliminationsverfahren

Bemerkung:

Es handelt sich dabei um eine Matrix mit Einsen auf der (nicht notwendigerweise durchgehenden) Diagonale, bei der unterhalb der Diagonale nur Nullen stehen.

Außerdem kommen ab der $k+1$-sten Zeile nur noch Nullen vor. Dieser Block von Nullen kann auch vollkommen fehlen.

Aus obiger Form kann man dann relativ einfach alle Lösungen ablesen.

Gaußsches Eliminationsverfahren

Bei einer $m \times n$-Matrix A läuft das Gaußsche Eliminationsverfahren in n Schritten ab. In jedem Schritt wird eine weitere Spalte in die gewünschte Form gebracht.

Gaußsches Eliminationsverfahren (i-ter Schritt)

Angenommen die Spalten $1, \ldots, i-1$ sind schon in der gewünschten Form. Dann sieht die Matrix folgendermaßen aus:

$$\left(\begin{array}{ccccccc|c}
1 & A_{1,2} & \ldots & & A_{1,i} & \ldots & A_{1,n} & b_1 \\
0 & 1 & \ldots & & A_{2,i} & \ldots & A_{2,n} & b_2 \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \vdots & \vdots \\
0 & \ldots & 0 & & A_{i,i} & \ldots & A_{i,n} & b_i \\
0 & \ldots & 0 & & A_{i+1,i} & \ldots & A_{i+1,n} & b_{i+1} \\
\vdots & \ddots & \vdots & & \vdots & \ddots & \vdots & \vdots \\
0 & \ldots & 0 & & A_{m,i} & \ldots & A_{m,n} & b_m
\end{array}\right)$$

Gaußsches Eliminationsverfahren

Wir betrachten nun $A_{i,i}$, das sogenannte Pivotelement.

Pivotelement $A_{i,i} \neq 0$

In diesem Fall hat $A_{i,i}$ ein multiplikatives Inverses $A_{i,i}^{-1}$ (wir arbeiten in einem Körper!).

Wir multiplizieren die i-te Zeile mit $A_{i,i}^{-1}$, wodurch das Pivotelement nun den Wert 1 hat. Wir haben folgende Situation:

$$\left(\begin{array}{ccccccc|c}
1 & A_{1,2} & \dots & 0 & A_{1,i} & \dots & A_{1,n} & b_1 \\
0 & 1 & \dots & 0 & A_{2,i} & \dots & A_{2,n} & b_2 \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \dots & 0 & 1 & 1 & \dots & A_{i,n} & b_i \\
0 & \dots & 0 & 0 & A_{i+1,i} & \dots & A_{i+1,n} & b_{i+1} \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \dots & 0 & 0 & A_{m,i} & \dots & A_{m,n} & b_m
\end{array}\right)$$

Gaußsches Eliminationsverfahren

Pivotelement $A_{i,i} \neq 0$ (Fortsetzung)

Wir behandeln nun jede Zeile j (mit $j > i$): wir multiplizieren die i-te Zeile mit $A_{j,i}$ und ziehen sie von der j-ten Zeile ab.

Dadurch ergibt sich folgende Zeile:

$$0 \quad \dots \quad 0 \quad (A_{j,i} - A_{j,i} \cdot 1) \quad \dots \quad (A_{j,n} - A_{j,i} \cdot A_{i,n}) \mid (b_j - A_{j,i} \cdot b_i)$$

und es gilt $A_{j,i} - A_{j,i} \cdot 1 = 0$.

Damit ist die i-te Spalte jetzt in der richtigen Form.

Gaußsches Eliminationsverfahren

Falls das Pivotelement $A_{i,i}$ den Wert 0 hat, so hat es kein multiplikatives Inverses und wir können das vorherige Verfahren nicht anwenden. Wir unterscheiden zwei Fälle:

Pivotelement $A_{i,i} = 0$ (Fall 1)

Angenommen es gibt ein Element $A_{j,i}$ (mit $j > i$) unterhalb von $A_{i,i}$ mit $A_{j,i} \neq 0$.

Dann vertausche die i-te und die j-te Zeile und fange mit dem i-ten Schritt wieder von vorne an.
(Achtung: die Elemente b_i, b_j in der rechten Spalte müssen auch getauscht werden.)

Gaußsches Eliminationsverfahren

Pivotelement $A_{i,i} = 0$ (Fall 2)

Angenommen es gibt kein Element $A_{j,i}$ (mit $j > i$) unterhalb von $A_{i,i}$ mit $A_{j,i} \neq 0$. D.h., alle Elemente in dieser Spalte, angefangen mit $A_{i,i}$, sind gleich Null.

Dann betrachten wir das Rechteck rechts unten in der Matrix:

$$\left(\begin{array}{ccc|c} A_{i,i} & \dots & A_{i,n} & b_i \\ A_{i+1,i} & \dots & A_{i+1,n} & b_{i+1} \\ \vdots & \ddots & \vdots & \vdots \\ A_{m,i} & \dots & A_{m,n} & b_m \end{array}\right)$$

Falls alle Elemente $A_{j,\ell}$ (mit $j \geq i$ und $\ell \geq i$) gleich Null sind, dann hält das Verfahren an.

Gaußsches Eliminationsverfahren

Pivotelement $A_{i,i} = 0$ (Fall 2) (Fortsetzung)

Ansonsten finde eine Spalte ℓ, in der es einen Wert $A_{j,\ell} \neq 0$ gibt (mit $j \geq i$, $\ell \geq i$) und vertausche die Spalte i und die Spalte ℓ.

Diese Vertauschung muss gemerkt und später wieder rückgängig gemacht werden!

Beginne mit dem i-ten Schritt wieder von vorne.

Gaußsches Eliminationsverfahren

Ablesen der Lösung: ▸ Umgeformtes Gleichungssystem

Keine Lösung

Wir betrachten zunächst den unteren Block, in dem nur Nullen stehen. Falls eines der Elemente $b_{k+1}, \ldots, b_m$ ungleich Null ist, so hat das Gleichungssystem keine Lösung.

Gaußsches Eliminationsverfahren

▸ Umgeformtes Gleichungssystem

Lösung bestimmen

Ansonsten betrachte den oberen Block mit
$A_{1,1} = 1, A_{2,2} = 1, \ldots, A_{k,k} = 1$

$$\left(\begin{array}{ccccccc|c} A_{1,1} & A_{1,2} & \ldots & A_{1,k} & \ldots & A_{1,n} & b_1 \\ 0 & A_{2,2} & \ldots & A_{2,k} & \ldots & A_{2,n} & b_2 \\ \vdots & \ddots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & A_{k,k} & \ldots & A_{k,n} & b_k \end{array}\right)$$

und behandle die Zeilen von unten nach oben wie im Folgenden beschrieben.

Gaußsches Eliminationsverfahren

▸ Umgeformtes Gleichungssystem

Lösung bestimmen (Fortsetzung)

Die j-te Zeile entspricht folgender Gleichung:

$$x_j + A_{j,j+1} \cdot x_{j+1} + \cdots + A_{j,n} \cdot x_n = b_j$$

Es gilt

$$x_j = b_j - A_{j,j+1} \cdot x_{j+1} - \cdots - A_{j,n} \cdot x_n$$

Setze dabei für $x_{j+1}, \ldots, x_n$ möglicherweise bereits berechneten Werte ein.

Gaußsches Eliminationsverfahren

Nachbehandlung

Zuletzt mache noch die gemerkten Vertauschungen rückgängig.

Dadurch erhält man die Werte von $x_1, \ldots, x_n$, wobei gegebenenfalls Variablen x_j in der Darstellung übrigbleiben. Diese bleiben stehen und repräsentieren beliebige Körperelemente.
Dies passiert immer dann, wenn der obere Block nicht quadratisch ist und die Diagonale daher nicht ganz durchgeht.

Insgesamt erhält man eine Menge von Lösungsvektoren $\vec{x}$, die wie folgt dargestellt werden können:

$$\vec{x} \in \{\vec{u} + x_{j_1} \cdot \vec{v}_1 + \cdots + x_{j_r} \cdot \vec{v}_r \mid x_{j_k} \in \mathbb{R}\}$$

Falls $\vec{u} = \vec{0}$ (das passiert, falls $\vec{b} = \vec{0}$), dann ist die Lösungsmenge ein Vektorraum und $\vec{v}_1, \ldots, \vec{v}_r$ eine Basis dieses Vektorraums.

Gaußsches Eliminationsverfahren

Bemerkungen:

Beim Zeilen- bzw. Spaltentausch hat man meist mehrere Möglichkeiten. In diesem Fall tauscht man mit der Zeile, die das günstigste Pivotelement liefert.

Ein Pivotelement ist günstig, wenn es ein einfach zu handhabendes multiplikatives Inverses hat. Am besten ist natürlich die Eins als Pivotelement.

Gaußsches Eliminationsverfahren

Beispiel 4:

Wir lösen folgendes Gleichungssystem in $\mathbb{R}$:

$$\begin{array}{llll} & & +3 \cdot x_3 & +x_4 & = 3 \\ 3 \cdot x_1 & +4 \cdot x_2 & -2 \cdot x_3 & +3 \cdot x_4 & = 4 \\ 6 \cdot x_1 & +8 \cdot x_2 & +x_3 & -x_4 & = -13 \end{array}$$

In Matrixschreibweise:

$$\begin{pmatrix} 0 & 0 & 3 & 1 \\ 3 & 4 & -2 & 3 \\ 6 & 8 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ -13 \end{pmatrix}$$

Gaußsches Eliminationsverfahren

Anfangssituation:

$$\left(\begin{array}{cccc|c} 0 & 0 & 3 & 1 & 3 \\ 3 & 4 & -2 & 3 & 4 \\ 6 & 8 & 1 & -1 & -13 \end{array}\right)$$

Schritt 1(a): Zeile 1 und Zeile 2 vertauschen, um Pivotelement ungleich 0 zu erhalten

$$\left(\begin{array}{cccc|c} 3 & 4 & -2 & 3 & 4 \\ 0 & 0 & 3 & 1 & 3 \\ 6 & 8 & 1 & -1 & -13 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 1(b): Zeile 1 mit $\frac{1}{3}$ multiplizieren, um Pivotelement zu eins zu machen

$$\left(\begin{array}{cccc|c} 1 & \frac{4}{3} & -\frac{2}{3} & 1 & \frac{4}{3} \\ 0 & 0 & 3 & 1 & 3 \\ 6 & 8 & 1 & -1 & -13 \end{array}\right)$$

Schritt 1(c): Rechne "(Zeile 2) $-$ 0$\cdot$ (Zeile 1)" und "(Zeile 3) $-$ 6$\cdot$ (Zeile 1)"

$$\left(\begin{array}{cccc|c} 1 & \frac{4}{3} & -\frac{2}{3} & 1 & \frac{4}{3} \\ 0 & 0 & 3 & 1 & 3 \\ 0 & 0 & 5 & -7 & -21 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 2(a): Spalte 2 und Spalte 4 vertauschen, um Pivotelement ungleich 0 zu erhalten. (Spaltenvertauschung merken!)

$$\left(\begin{array}{cccc|c} 1 & 1 & -\frac{2}{3} & \frac{4}{3} & \frac{4}{3} \\ 0 & 1 & 3 & 0 & 3 \\ 0 & -7 & 5 & 0 & -21 \end{array}\right)$$

Das Pivotelement ist bereits 1.

Schritt 2(b): Rechne "(Zeile 3) $-$ $(-7)\cdot$ (Zeile 2)"

$$\left(\begin{array}{cccc|c} 1 & 1 & -\frac{2}{3} & \frac{4}{3} & \frac{4}{3} \\ 0 & 1 & 3 & 0 & 3 \\ 0 & 0 & 26 & 0 & 0 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 2(c): Zeile 3 mit $\frac{1}{26}$ multiplizieren, um Pivotelement zu eins zu machen

$$\left(\begin{array}{cccc|c} 1 & 1 & -\frac{2}{3} & \frac{4}{3} & \frac{4}{3} \\ 0 & 1 & 3 & 0 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

Damit ist das Gleichungssystem in der gewünschten Form.

Existenz der Lösung: es gibt keinen Block von Nullen, daher existiert eine Lösung.

Gaußsches Eliminationsverfahren

Bestimmung der Lösung:

Zeile 3: $x_3 = 0$
Zeile 2: $x_2 + 3 \cdot x_3 = 3$, also $x_2 = 3 - 3 \cdot x_3 = 3 - 0 = 3$
Zeile 1: $x_1 + x_2 - \frac{2}{3} \cdot x_3 + \frac{4}{3} \cdot x_4 = \frac{4}{3}$,
also $x_1 = \frac{4}{3} - x_2 + \frac{2}{3} \cdot x_3 - \frac{4}{3} \cdot x_4 = \frac{4}{3} - 3 + 0 - \frac{4}{3} \cdot x_4 = -\frac{5}{3} - \frac{4}{3} \cdot x_4$.

Vertauschungen rückgängig machen: wir müssen noch x_2 und x_4 zurücktauschen, es ergibt sich damit

$$x_1 = -\frac{5}{3} - \frac{4}{3} \cdot x_2 \qquad x_2 \text{ beliebig} \qquad x_3 = 0 \qquad x_4 = 3$$

Gaußsches Eliminationsverfahren

Vektorschreibweise:

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -\frac{5}{3} - \frac{4}{3} \cdot x_2 \\ x_2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} -\frac{5}{3} \\ 0 \\ 0 \\ 3 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -\frac{4}{3} \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Dieses Gleichungssystem hat unendlich viele Lösungen, eine für jede Belegung von x_2 mit einer reellen Zahl.

Gaußsches Eliminationsverfahren

Beispiel 2 (noch einmal):

$$\begin{aligned} x_1 + 2 \cdot x_2 &= 3 \\ -2 \cdot x_1 - 4 \cdot x_2 &= 1 \end{aligned}$$

Anfangssituation:

$$\left(\begin{array}{cc|c} 1 & 2 & 3 \\ -2 & -4 & 1 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 1: Rechne "(Zeile 2) − (−2)·(Zeile 1)"

$$\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 0 & 7 \end{array}$$

Existenz der Lösung: Im unteren Block der Nullen ist das Element in der rechten Spalte ungleich Null (7). Daher existiert keine Lösung.

Gaußsches Eliminationsverfahren

Bemerkung:

Das Gaußsche Eliminationsverfahren kann *nicht* dazu benutzt werden, um diophantische Gleichungen zu lösen.

Dort sucht man nach Lösungen in den ganzen Zahlen $\mathbb{Z}$. Die ganzen Zahlen mit der Addition und Multiplikation bilden jedoch keinen Körper (fehlende multiplikative Inverse!).

Das Gaußsche Eliminationsverfahren ist jedoch für jeden beliebigen Körper (z.B. $(\mathbb{Z}_p, +_p, \cdot_p)$, p Primzahl) anwendbar.

Multiplikatives Inverses einer Matrix

Mit Hilfe des Gaußschen Eliminationsverfahrens kann man nun das multiplikative Inverse einer Matrix bestimmen.

Gegeben sei eine quadratische Matrix

$$A = \begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{n,1} & \dots & A_{n,n} \end{pmatrix}$$

Man stellt sich vor, dass das multiplikative Inverse A^{-1} aus Spaltenvektoren $\vec{a}_1, \dots, \vec{a}_n$ zusammengesetzt ist und schreibt $A^{-1} = \begin{pmatrix} \vec{a}_1 & \dots & \vec{a}_n \end{pmatrix}$.

(Siehe auch den Abschnitt über Erzeugendensysteme und Basen ▸ Invertierbare Matrizen und Basen.)

Multiplikatives Inverses einer Matrix

Damit A^{-1} das Inverse von A ist, muss gelten:

$$A \cdot A^{-1} = A \cdot \begin{pmatrix} \vec{a}_1 & \dots & \vec{a}_n \end{pmatrix} = \begin{pmatrix} A \cdot \vec{a}_1 & \dots & A \cdot \vec{a}_n \end{pmatrix}$$

$$= E_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} \vec{e}_1 & \dots & \vec{e}_n \end{pmatrix}$$

Also gilt für jedes $i \in \{1, \dots, n\}$: $A \cdot \vec{a}_i = \vec{e}_i$

Dabei ist $\vec{e}_i$ der i-te Einheitsvektor.

Man muss also n Gleichungssysteme mit jeweils n Gleichungen lösen. Existieren für alle Gleichungssysteme Lösungen, so erhält man die Inverse A^{-1}. Anderenfalls gibt es keine Inverse.

Multiplikatives Inverses einer Matrix

Beispiel: wir bestimmen das multiplikative Inverse folgender Matrix

$$A = \begin{pmatrix} 3 & 4 \\ 1 & -3 \end{pmatrix}$$

Wir setzen zunächst $\vec{a_1} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ und lösen das Gleichungssystem $A \cdot \vec{a_1} = \vec{e_1}$:

$$\begin{aligned} 3 \cdot x_1 + 4 \cdot x_2 &= 1 \\ x_1 - 3 \cdot x_2 &= 0 \end{aligned}$$

Das ergibt die Lösungen $x_1 = \frac{3}{13}$ und $x_2 = \frac{1}{13}$.

Multiplikatives Inverses einer Matrix

Wir setzen nun $\vec{a}_2 = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ und lösen das Gleichungssystem $A \cdot \vec{a}_2 = \vec{e}_2$:

$$\begin{aligned} 3 \cdot y_1 + 4 \cdot y_2 &= 0 \\ y_1 - 3 \cdot y_2 &= 1 \end{aligned}$$

Das ergibt die Lösungen $y_1 = \frac{4}{13}$ und $y_2 = -\frac{3}{13}$.

Insgesamt erhält man folgende Matrix A^{-1}:

$$A^{-1} = \begin{pmatrix} \vec{a}_1 & \vec{a}_2 \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \begin{pmatrix} \frac{3}{13} & \frac{4}{13} \\ \frac{1}{13} & -\frac{3}{13} \end{pmatrix}$$

Multiplikatives Inverses einer Matrix

Bemerkung (Gauß-Jordan-Verfahren):

Es gibt eine effizientere Methode um das Inverse einer Matrix zu bestimmen. Man kann insbesondere alle n Gleichungssysteme "gleichzeitig" lösen.

Dabei schreibt man die zu invertierende Matrix und die Einheitsmatrix wie folgt nebeneinander:

$$\left(\begin{array}{rr|rr} 3 & 4 & 1 & 0 \\ 1 & -3 & 0 & 1 \end{array}\right)$$

Dann formt man die linke Matrix durch Zeilentausch (nicht Spaltentausch!), indem man Zeilen mit einem Wert (ungleich 0) multipliziert und indem man Vielfache von Zeilen zu anderen Zeilen addiert, zur Einheitsmatrix um.
Die Matrix, die dabei rechts entsteht, ist dann die Inverse.

Schlussbemerkungen

Es gibt noch viele andere wichtige Gebiete im Zusammenhang mit algebraischen Strukturen, Vektorräumen und Matrizen:

- Ringe (Strukturen, die ähnlich zu Körpern sind, in denen aber weniger Gesetze gelten)
- Eigenvektoren und Eigenwerte
- Determinanten
- ...

Kombinatorik: Einführung

Es folgt eine Einführung in die Kombinatorik.

Dabei geht es darum, die Elemente einer Menge zu zählen. Dabei ist die Größe der Menge nicht fest (sonst wäre das ja einfach!), sondern abhängig von bestimmten Parametern.

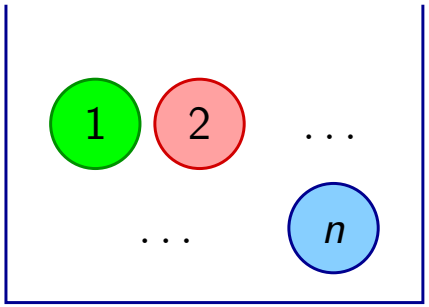
Anwendungsbeispiele:

- Anzahl der Zustände bzw. Anzahl der Abläufe in einem System zählen. (Wichtig für Systeme der Informatik, in denen die Anzahl der Systemzustände sehr groß werden kann.)
- Wahrscheinlichkeiten für das Eintreten eines Ereignisses berechnen. (Wichtig für Statistik.)

Ziehen aus Urnen

Angenommen, wir haben eine Urne (einen großen Behälter), in der n durchnumerierte (und daher unterscheidbare) Kugeln liegen. Aus dieser Urne werden k Kugeln gezogen.

Die Frage ist: wieviele verschiedene Möglichkeiten gibt es, Kugeln zu ziehen?



Mit Hilfe dieser Metapher lassen sich viele Zählprobleme erfassen.

Ziehen aus Urnen

Die Antwort: das hängt davon ab ...

Es hängt insbesondere davon ab, wie die Regeln festgelegt werden:

- Werden die Kugeln nach dem Ziehen wieder in die Urne gelegt? (Ziehen mit/ohne Zurücklegen)
- Wird die Reihenfolge des Ziehens gewertet? (mit/ohne Beachtung der Reihenfolge)

  Beispiel: Ist die Sequenz $1, 5, 7$ gleichbedeutend mit $7, 1, 5$?

Ziehen aus Urnen

Beispiel 1: Lottozahlen

Bei der Ziehung der Lottozahlen werden die Kugeln nicht zurückgelegt und die Reihenfolge nicht beachtet. Es ist egal, ob eine Zahl vor oder nach einer anderen Zahl gezogen wird.

Die Parameter sind $n = 49$ und $k = 6$ (6 aus 49).

Beispiel 2: Würfeln mit drei (identischen) Würfeln

Das kann man als das Ziehen von $k = 3$ Kugeln aus einer Urne mit $n = 6$ Kugeln interpretieren. Hierbei werden die Kugeln zurückgelegt und die Reihenfolge ebenfalls nicht betrachtet.

Beim Ziehen mit Zurücklegen kann eine Zahl durchaus auch mehrfach auftreten. Dieses mehrfache Auftreten spielt (im Unterschied zu Mengen) eine Rolle. Das Würfelergebnis $3, 3, 6$ ist verschieden von $3, 6, 6$.

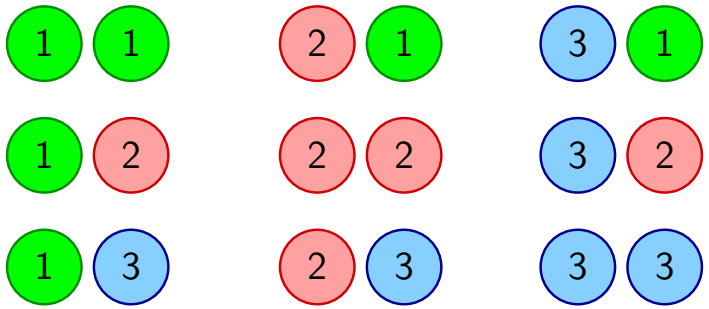
Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Wir beginnen mit folgendem Fall:

Ziehe k Kugeln aus einer Urne mit n Kugeln, mit Zurücklegen und unter Beachtung der Reihenfolge.

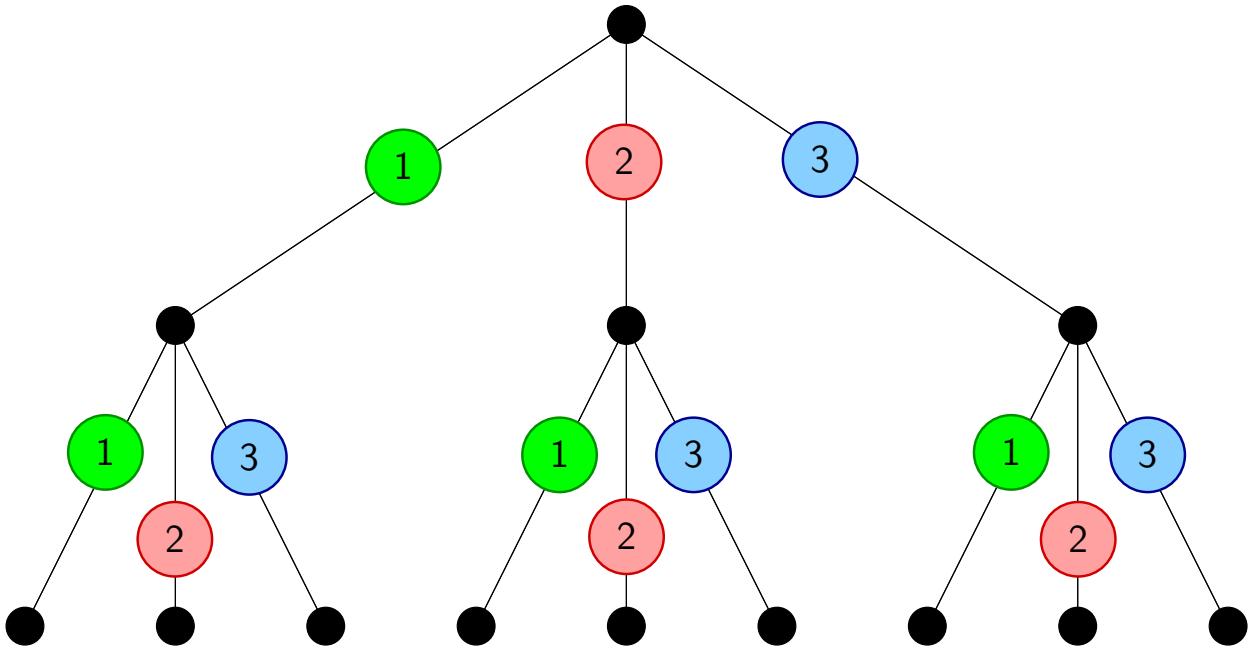
Angenommen, die Urne enthält $n = 3$ drei Kugeln: 

Dann gibt es folgende neun Möglichkeiten, $k = 2$ Kugeln aus der Urne zu ziehen:



Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Diese neun Möglichkeiten kann man auch als Entscheidungsbaum darstellen:

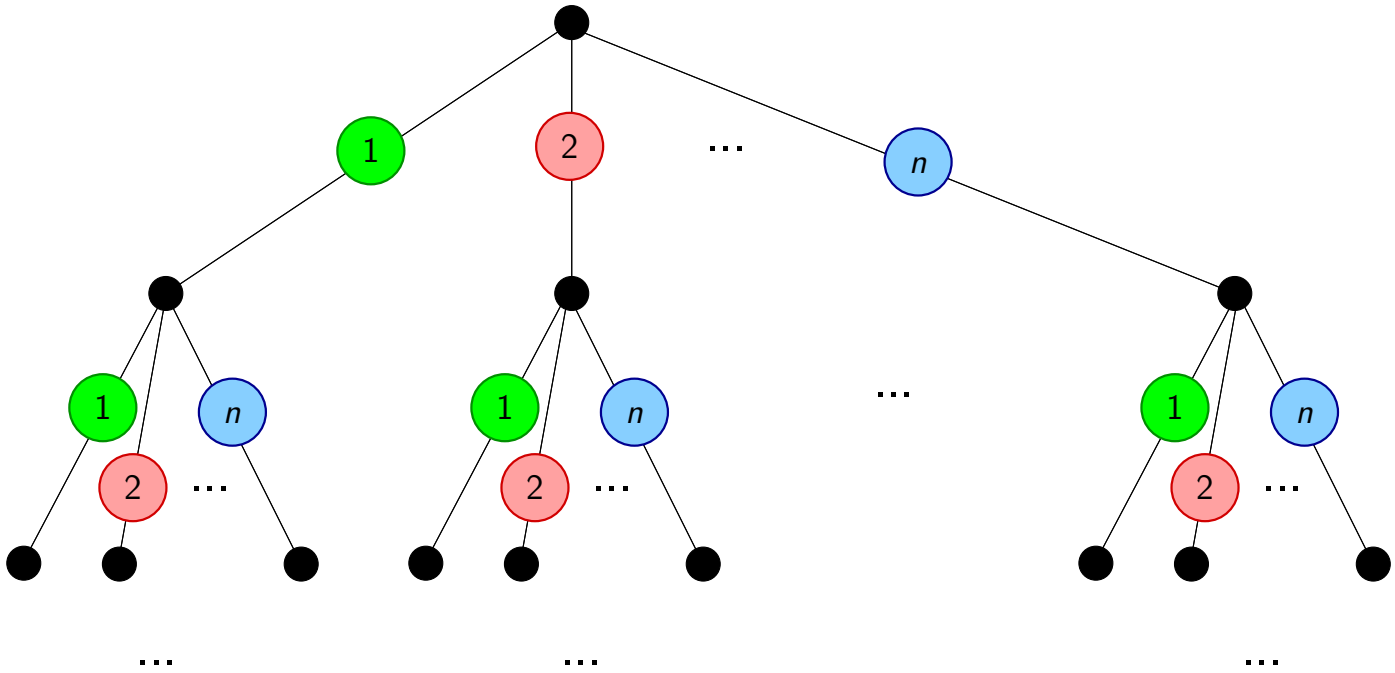


3 Entscheidungsmöglichkeiten auf der ersten Ebene, ergibt dreimal 3 Entscheidungsmöglichkeiten auf der zweiten Ebene.

Damit hat man insgesamt $3 \cdot 3 = 3^2 = 9$ Fälle.

Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Im allgemeinen Fall:



Auf der ersten Ebene: n Entscheidungsmöglichkeiten
Auf der zweiten Ebene: $n \cdot n$ Entscheidungsmöglichkeiten
...
Auf der k-ten Ebene: $\underbrace{n \cdot n \cdot \ldots \cdot n}_{k\text{-mal}} = n^k$ Möglichkeiten

Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Ziehen mit Zurücklegen und unter Beachtung der Reihenfolge

Für das Ziehen aus einer Urne mit Zurücklegen und unter Beachtung der Reihenfolge ergeben sich

$$n^k \text{ Möglichkeiten,}$$

falls sich n (verschiedene) Kugeln in der Urne befinden und k Kugeln gezogen werden.

Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Anwendungen:

Gegeben seien zwei endliche Mengen A, B. Wieviele Funktionen zwischen A und B gibt es?

Beispiel: sei A eine Menge von Personen und B eine Menge von Räumen. Wieviele Möglichkeiten gibt, jeder Person einen Raum zuzuordnen? (Dabei müssen nicht notwendigerweise alle Räume verwendet werden und mehreren Personen kann der gleiche Raum zugeteilt werden.)

Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Wieviele Funktionen zwischen A und B gibt es? (Fortsetzung)

Wir nehmen an, dass $A = \{a_1, \ldots, a_k\}$ mit $k = |A|$ und $n = |B|$. Wir können B als Urne betrachten, aus der nacheinander k Elemente gezogen werden (mit Zurücklegen, unter Beachtung der Reihenfolge).

D.h., zunächst wird ein Element aus B gezogen, das a_1 zugeordnet wird, dann wird ein weiteres Element gezogen, das a_2 zugeordnet wird, etc.

Insgesamt erhält man n^k Funktionen zwischen den Mengen A und B.

Ziehen aus Urnen (mit Zurücklegen, mit Reihenfolge)

Bemerkung: Beim Zählen von Möglichkeiten erhält man leicht sehr große Zahlen (sogenannte Zustandsexplosion).

Beispiel: eine Bedienoberfläche enthält 10 Elemente (Widgets, wie beispielsweise Radio Buttons, Drop-down-lists, ...), von denen sich jedes in 5 verschiedenen Zuständen befinden kann, die unabhängig voneinander einstellbar sind.

In wievielen Zuständen kann sich die Oberfläche insgesamt befinden?

Antwort: Ziehen von 10 Kugeln aus einer Urne mit 5 Kugeln (mit Zurücklegen, unter Beachtung der Reihenfolge).

Insgesamt erhält man $5^{10} = 9.765.625$ Möglichkeiten.

Es ist sehr schwierig, diese fast 10 Millionen Zustände alle durchzuprobieren, um festzustellen, dass sich die unter der Benutzeroberfläche liegende Software immer korrekt verhält.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

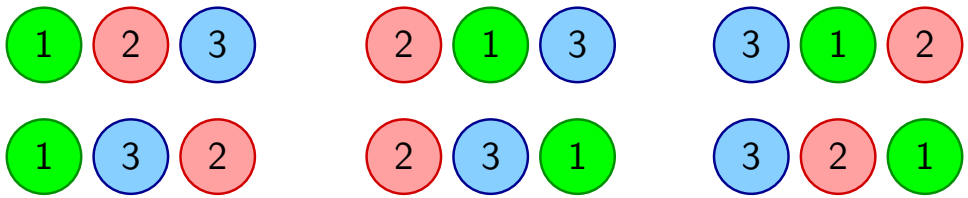
Wir betrachten nun folgenden Fall:

Ziehe k Kugeln aus einer Urne mit n Kugeln, ohne Zurücklegen und unter Beachtung der Reihenfolge.

Dieser Fall macht nur Sinn, falls $k \leq n$.

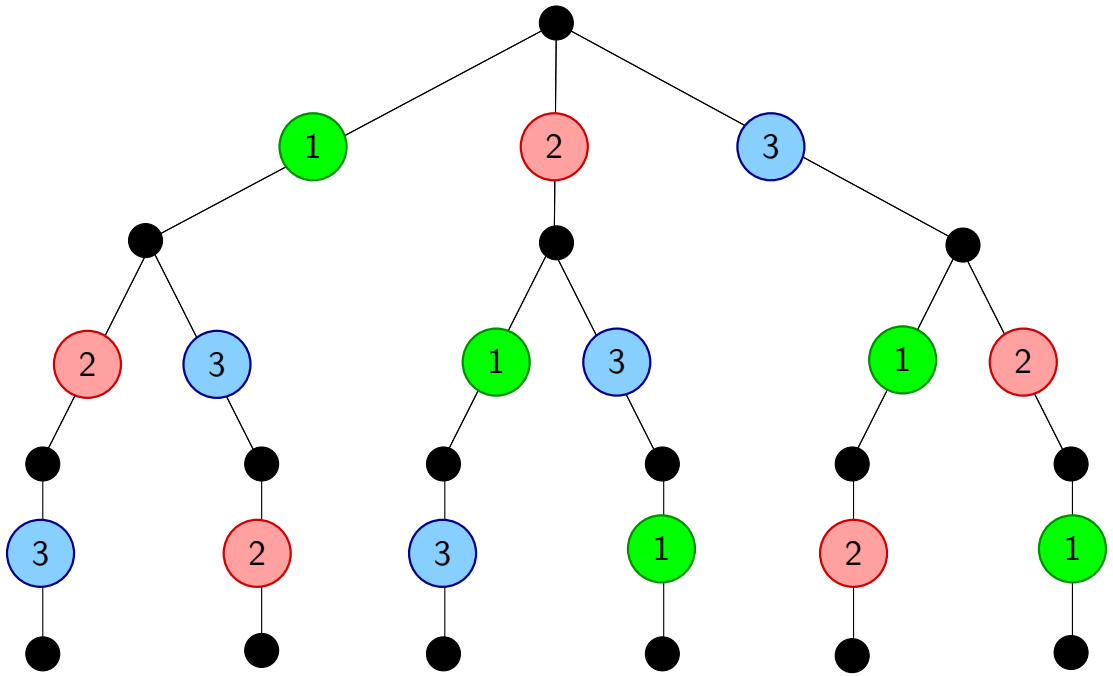
Angenommen, die Urne enthält $n = 3$ drei Kugeln: 

Dann gibt es folgende sechs Möglichkeiten, $k = 3$ Kugeln aus der Urne zu ziehen:



Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Diese sechs Möglichkeiten kann man auch als Entscheidungsbaum darstellen:

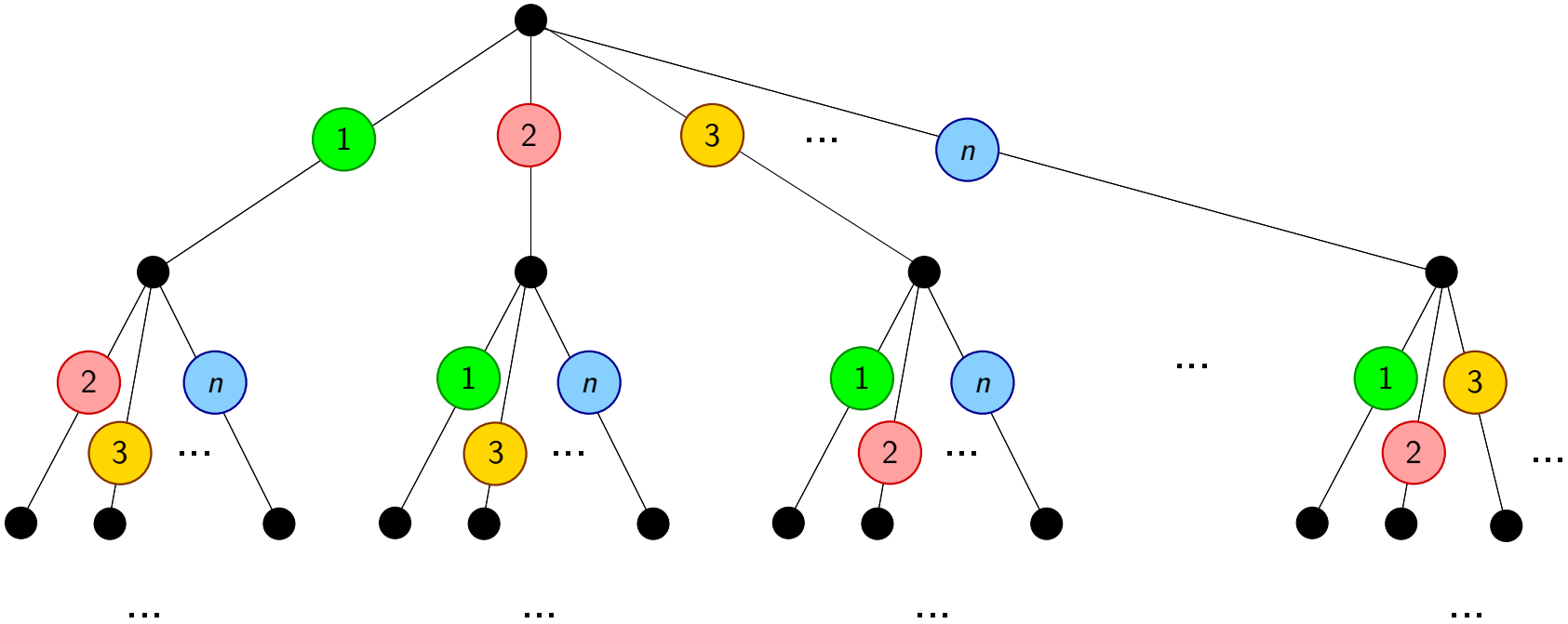


3 Entscheidungsmöglichkeiten auf der ersten Ebene, ergibt:
$3 \cdot 2$ Entscheidungsmöglichkeiten auf der zweiten Ebene *und*
$3 \cdot 2 \cdot 1$ Entscheidungsmöglichkeiten auf der dritten Ebene.

Damit hat man insgesamt $3 \cdot 2 \cdot 1 = 6$ Fälle.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Wir betrachten den allgemeinen Fall, zunächst für $n = k$:



Auf der ersten Ebene: n Entscheidungsmöglichkeiten
Auf der zweiten Ebene: $n \cdot (n-1)$ Entscheidungsmöglichkeiten
...
Auf der k-ten Ebene: $n \cdot (n-1) \cdot \ldots \cdot 1 = n!$ Möglichkeiten

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Fakultätsfunktion

Die Funktion, die $n \in \mathbb{N}_0$ auf

$$n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$$

abbildet, wird als Fakultätsfunktion bezeichnet. Man schreibt:

$$n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$$

Für $n = 0$ wird $0! = 1$ festgelegt.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

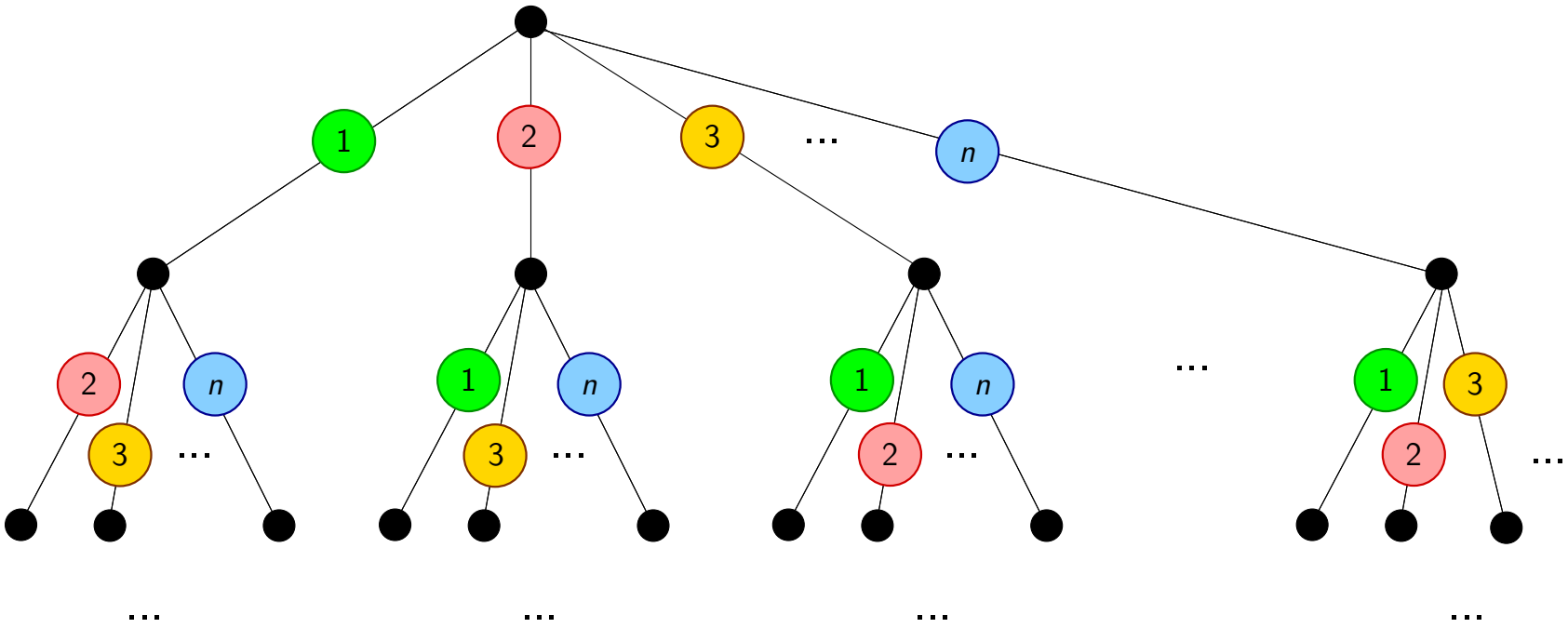
Wertetabelle:

n	$n!$	n	$n!$
0	1	5	120
1	1	6	720
2	2	7	5040
3	6	8	40320
4	24	9	362880

Man sieht, dass die Fakultätsfunktion ungeheuer schnell wächst.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Im allgemeinen Fall hat man beim letzten Ziehen noch $n - k + 1$ Kugeln übrig:



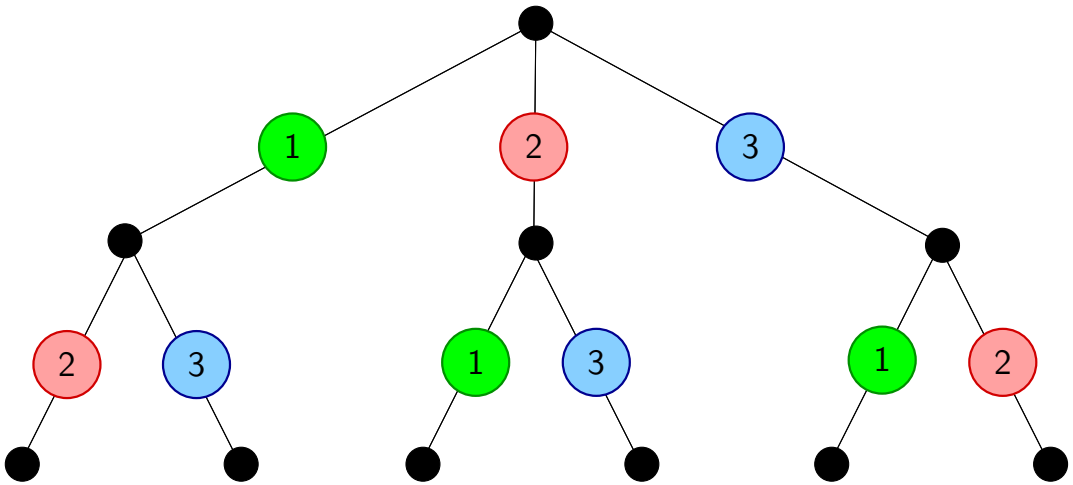
Auf der ersten Ebene: n Entscheidungsmöglichkeiten

...

Auf der k-ten Ebene: $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ Möglichkeiten

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Beispiel: es sind $n = 3$ Kugeln in der Urne, von denen $k = 2$ gezogen werden:



Im letzten Schritt sind noch $2 = n - k + 1$ Kugeln übrig.

Warum? $\rightsquigarrow$ Zum Schluss sind $n - k$ Kugeln übrig, wir befinden uns einen Schritt vorher.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

n hoch k fallend

Seien $k, n \in \mathbb{N}_0$ mit $k \leq n$. Der Ausdruck

$$n^{\underline{k}} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

wird *n hoch k fallend* gelesen.

Für den Fall $k = 0$ setzt man $n^{\underline{0}} = 1$. (Das gilt auch, falls $n = 0$.)

Es gilt:

$$\begin{aligned} \frac{n!}{(n-k)!} &= \frac{n \cdot \ldots \cdot (n-k+1) \cdot (n-k) \cdot \ldots \cdot 1}{(n-k) \cdot \ldots \cdot 1} \\ &= n \cdot \ldots \cdot (n-k+1) \\ &= n^{\underline{k}} \end{aligned}$$

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Ziehen ohne Zurücklegen und unter Beachtung der Reihenfolge

Für das Ziehen aus einer Urne ohne Zurücklegen und unter Beachtung der Reihenfolge ergeben sich

$$n^{\underline{k}} = \frac{n!}{(n-k)!} \text{ Möglichkeiten,}$$

falls sich n (verschiedene) Kugeln in der Urne befinden und $k \leq n$ Kugeln gezogen werden.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Anwendungen:

Gegeben seien zwei endliche Mengen A, B. Wieviele injektive Funktionen zwischen A und B gibt es?

Beispiel: sei A eine Menge von Personen und B eine Menge von Räumen. Wieviele Möglichkeiten gibt, jeder Person einen Raum zuzuordnen, so dass sich in einem Raum höchstens eine Person befindet?

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Wieviele injektive Funktionen zwischen A und B gibt es?
(Fortsetzung)

Wir nehmen an, dass $k = |A|$ mit $A = \{a_1, \ldots, a_k\}$ und $n = |B|$.
Wir können B als Urne betrachten, aus der nacheinander k Elemente gezogen werden, ohne dass Elemente zurückgelegt werden (jedoch mit Beachtung der Reihenfolge).
(Kein Element im Wertebereich darf mehr als einem Element im Definitionsbereich zugeordnet werden!)

Insgesamt erhält man $n^{\underline{k}}$ injektive Funktionen zwischen den Mengen A und B.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Beispiel: gegebenen seien n Städte, die alle der Reihe nach besucht werden sollen (Problem des Handlungsreisenden). Wieviele Möglichkeiten gibt es, die Städte zu besuchen?

Wir legen n mit den Namen Städte beschriftete Kugeln in eine Urne und ziehen nacheinander n Kugeln.

Insgesamt hat man $n^{\underline{n}} = n!$ Möglichkeiten.

Ziehen aus Urnen (ohne Zurücklegen, mit Reihenfolge)

Beispiel (Fortsetzung):

Nehmen wir an, die Städte wären Duisburg (DU), Essen (E), Bochum (BO), Dortmund (DO). Dann gibt es $4! = 24$ Möglichkeiten:

DU E BO DO	E DU BO DO	BO DU E DO	DO DU E BO
DU E DO BO	E DU DO BO	BO DU DO E	DO DU BO E
DU BO E DO	E BO DU DO	BO E DU DO	DO E DU BO
DU BO DO E	E BO DO DU	BO E DO DU	DO E BO DU
DU DO E BO	E DO DU BO	BO DO DU E	DO BO DU E
DU DO BO E	E DO BO DU	BO DO E DU	DO BO E DU

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

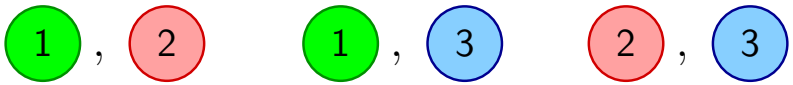
Wir betrachten nun folgenden Fall:

Ziehe k Kugeln aus einer Urne mit n Kugeln, ohne Zurücklegen und ohne Beachtung der Reihenfolge.

Dieser Fall macht wiederum nur Sinn, falls $k \leq n$.

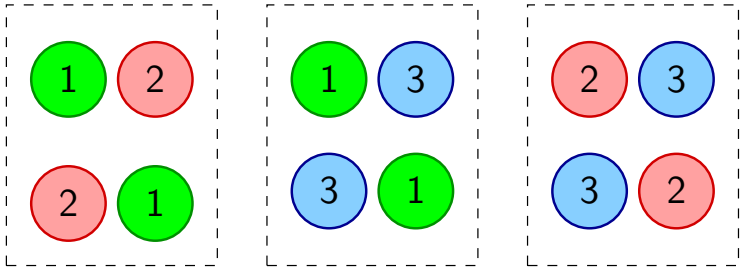
Angenommen, die Urne enthält $n = 3$ Kugeln: 

Dann gibt es folgende drei Möglichkeiten, $k = 2$ Kugeln aus der Urne zu ziehen:



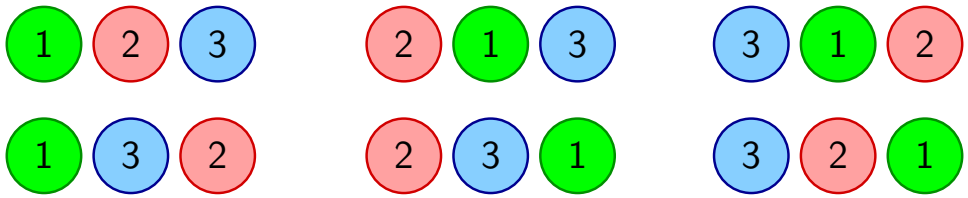
Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Diese drei Möglichkeiten entstehen dadurch, dass von den sechs Möglichkeiten beim Ziehen mit Reihenfolge (ohne Zurücklegen) jeweils immer zwei zusammenfallen.



Im Fall, dass k Kugeln gezogen werden, fallen jeweils $k!$ Kombinationen zusammen. Das ist die Anzahl der Möglichkeiten, k verschiedene Kugeln beliebig anzuordnen.

Fall $k = 3$: Es gibt $3! = 6$ verschiedene Anordnungen.



Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Wenn man mit Beachtung der Reihenfolge zieht, so erhält man

$$n^{\underline{k}} \text{ Möglichkeiten.}$$

Damit hat man jedoch die Möglichkeiten ohne Beachtung der Reihenfolge um den Faktor $k!$ überschätzt. Durch diesen Faktor muss noch geteilt werden.

Insgesamt ergeben sich damit

$$\frac{n^{\underline{k}}}{k!} = \frac{n!}{(n-k)! \cdot k!}$$

Möglichkeiten.

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Binomialkoeffizient

Seien $k, n \in \mathbb{N}_0$ mit $k \leq n$. Der Ausdruck

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

wird Binomialkoeffizient genannt. Er ist immer eine natürliche Zahl.

Sprechweise: "n über k", "k aus n"

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{(n-k)! \cdot k!} = \frac{n!}{k! \cdot (n-k)!} \\ &= \frac{n!}{(n-(n-k))! \cdot (n-k)!} = \binom{n}{n-k}\end{aligned}$$

Es gilt also für alle $n, k \in \mathbb{N}_0$, $k \leq n$:

$$\binom{n}{k} = \binom{n}{n-k}$$

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Binomialkoeffizienten als Pascalsches Dreieck:

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} &
\end{array}$$

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 5 & & 10 & & 10 & & 5 & & 1 &
\end{array}$$

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Bemerkung: die Werte im unteren und oberen Dreieck entsprechen einander, es sind nur verschiedene Darstellungen angegeben. Einmal der Binomialkoeffizient, einmal der berechnete Wert des Binomialkoeffizienten.

Beispiele:

$$\binom{5}{3} = \frac{5!}{(5-3)! \cdot 3!} = \frac{5!}{2! \cdot 3!} = \frac{120}{2 \cdot 6} = 10$$

$$\binom{5}{0} = \frac{5!}{(5-0)! \cdot 0!} = \frac{5!}{5! \cdot 0!} = \frac{120}{120 \cdot 1} = 1$$

Im letzten Fall zieht man 0 Kugeln (aus einer Urne mit 5 Kugeln). Dabei kann es nur eine mögliche enstehende Sequenz von Kugeln geben: die leere Sequenz.

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Ziehen ohne Zurücklegen und ohne Beachtung der Reihenfolge

Für das Ziehen aus einer Urne ohne Zurücklegen und ohne Beachtung der Reihenfolge ergeben sich

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \text{ Möglichkeiten,}$$

falls sich n (verschiedene) Kugeln in der Urne befinden und $k \leq n$ Kugeln gezogen werden.

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Beispiel: Lottozahlen

Beim Lottospielen werden $k = 6$ Kugeln aus $n = 49$ gezogen, die Kugeln werden nicht zurückgelegt, die Reihenfolge wird nicht beachtet.

Daher gibt es insgesamt

$$\binom{49}{6} = 13.983.816$$

mögliche Ziehungsergebnisse.

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Beispiel: Fussballpaarung

Aus einem Topf mit Kugeln, die mit $n = 18$ Fussball-Mannschaften beschriftet sind, werden zwei Kugeln gezogen, um eine Paarung zu ermitteln.

Es gibt dabei

$$\binom{18}{2} = 153$$

mögliche Ziehungsergebnisse. (Das ist genau die Anzahl der Spiele in einer Bundesliga-Hinrunde.)

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Anwendungen: allgemeine binomische Formel.

Der Ausdruck $(x+y)^n$ soll (in einem Körper) mit Hilfe des Distributivgesetzes ausmultipliziert werden. Was erhält man?

$$(x+y)^n = (x+y)\cdot(x+y)\cdot\ldots\cdot(x+y)$$

- Wenn man diesen Ausdruck ausmultipliziert, wählt man aus jedem der Faktoren entweder ein x oder ein y.
- Wenn man k-mal ein y wählt, dann wählt man $(n-k)$-mal ein x. Man erhält den Summanden $x^{n-k}\cdot y^k$.
- Wieviele Möglichkeiten gibt es, k-mal ein y zu wählen? $\rightsquigarrow \binom{n}{k}$

Zusammenfassung: Der Summand $x^{n-k}\cdot y^k$ kommt $\binom{n}{k}$-mal vor. Der Index k kann einen der Werte von 0 bis n einnehmen.

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Formel:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Spezialfall $n = 2$:

$$\begin{aligned}(x+y)^2 &= (x+y)\cdot(x+y) = x\cdot x + x\cdot y + y\cdot x + y\cdot y \\ &= x^2 + 2xy + y^2 = \binom{2}{0}\cdot x^2 y^0 + \binom{2}{1}\cdot xy + \binom{2}{2} x^0 y^2\end{aligned}$$

Ziehen aus Urnen (ohne Zurücklegen, ohne Reihenfolge)

Spezialfall $n = 3$:

$$\begin{aligned}
(x+y)^3 &= (x+y)\cdot(x+y)\cdot(x+y) \\
&= x\cdot x\cdot x + x\cdot x\cdot y + x\cdot y\cdot x + x\cdot y\cdot y \\
&\quad + y\cdot x\cdot x + y\cdot x\cdot y + y\cdot y\cdot x + y\cdot y\cdot y \\
&= x^3 + 3x^2y + 3xy^2 + y^3 \\
&= \binom{3}{0}\cdot x^3y^0 + \binom{3}{1}\cdot x^2y + \binom{3}{2}xy^2 + \binom{3}{3}x^0y^3
\end{aligned}$$

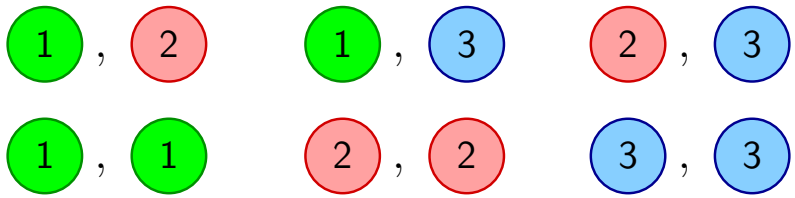
Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

Wir betrachten nun noch den letzten Fall:

Ziehe k Kugeln aus einer Urne mit n Kugeln, mit Zurücklegen und ohne Beachtung der Reihenfolge.

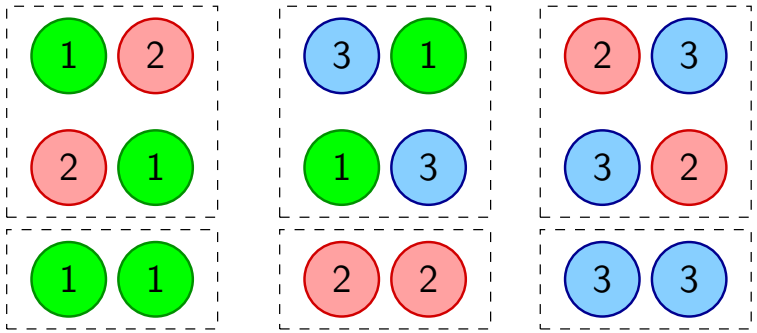
Angenommen, die Urne enthält $n = 3$ Kugeln: 

Dann gibt es folgende sechs Möglichkeiten, $k = 2$ Kugeln aus der Urne zu ziehen:



Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

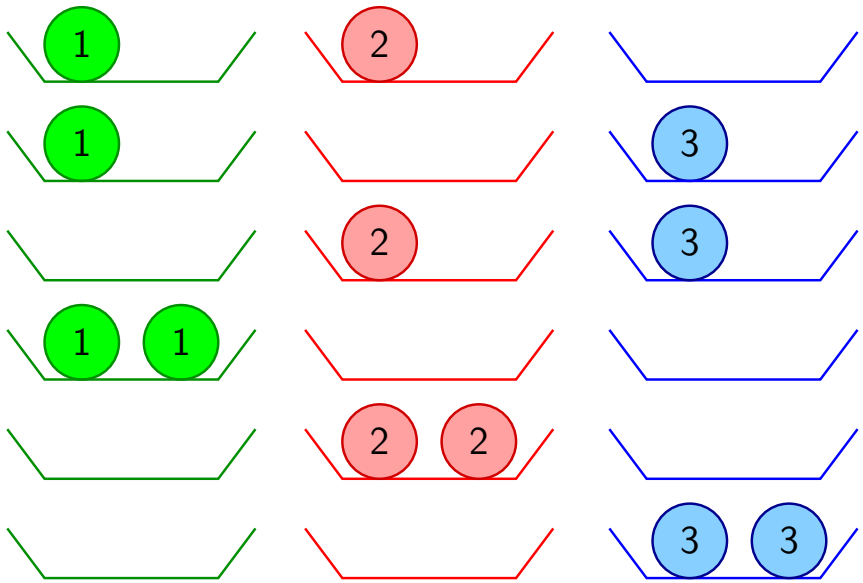
Hier braucht man eine gute Idee, um die Anzahl der Möglichkeiten zu zählen. Sie entstehen anscheinend nicht dadurch, dass die neun Möglichkeiten des Ziehens mit Reihenfolge (mit Zurücklegen) in gleich große Blöcke zusammengefasst werden.



?

Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

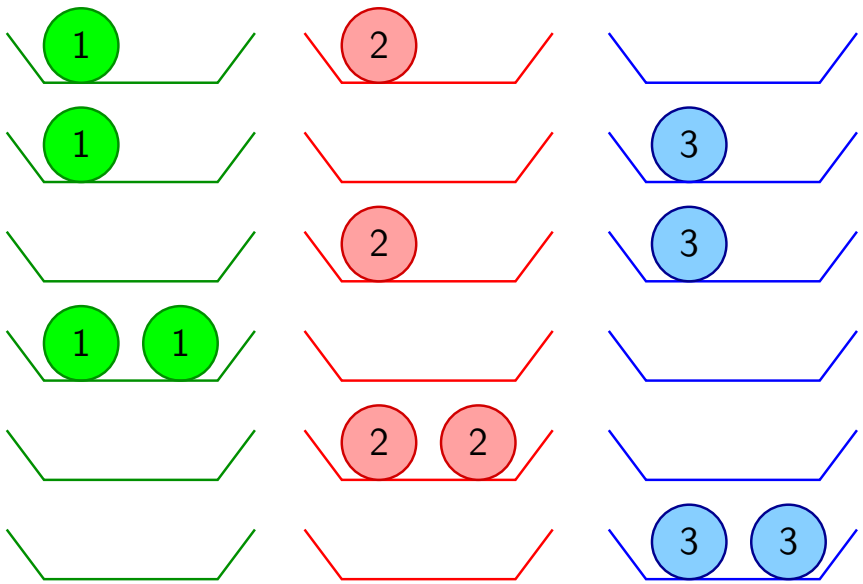
Die sechs Möglichkeiten kann man dadurch darstellen, dass man drei Fächer (eines für jede Farbe) einrichtet. Die Anzahl der Möglichkeiten ist die Anzahl der Möglichkeiten, zwei Kugeln auf diese drei Fächer zu verteilen.



Dabei bestimmt die Farbe des Fachs die Farbe der Kugeln.

Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

Die Farben kann man weglassen und nur noch zwischen erstem, zweitem und dritten Fach unterscheiden.
Wir benutzen eine Notation, in der die Kugeln durch kleine Kreise und die Trennwände zwischen den Fächern als Striche dargestellt werden (siehe rechte Spalte).



Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

Wir müssen also in einer vierelementigen Zeichenfolge darüber entscheiden, wo die beiden Striche und wo die beiden Kreise platziert werden.

Man kann entweder die zwei Striche wählen: $\binom{4}{2} = 6$ Möglichkeiten oder die zwei Kreise wählen: ebenfalls $\binom{4}{2} = 6$ Möglichkeiten

Bemerkung: aufgrund der Beziehung $\binom{n}{k} = \binom{n}{n-k}$ erhält man auch dann in beiden Fällen das gleiche Ergebnis, wenn die Anzahl der Striche und der Kreise unterschiedlich ist.

Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

Allgemeiner Fall:

Wir ziehen k Kugeln $\rightsquigarrow$ die Anzahl der Kreise ist k

Wir haben n Kugeln in der Urne $\rightsquigarrow$ die Anzahl der Farben bzw. Fächer ist n. Damit ist die Anzahl der Trennstriche $n-1$.

Die Länge der Zeichenfolge ist die Summe beider Zahlen: $n+k-1$

Insgesamt ergeben sich damit

$$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Möglichkeiten.

Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

Ziehen mit Zurücklegen und ohne Beachtung der Reihenfolge

Für das Ziehen aus einer Urne mit Zurücklegen und ohne Beachtung der Reihenfolge ergeben sich

$$\binom{n+k-1}{k} = \binom{n+k-1}{n-1} \text{ Möglichkeiten,}$$

falls sich n (verschiedene) Kugeln in der Urne befinden und k Kugeln gezogen werden.

Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

Beispiel: Würfeln

Falls mit drei identischen Würfeln gewürfelt wird, so entspricht das dem Ziehen von $k = 3$ Kugeln aus einer Urne mit $n = 6$ Kugeln, mit Zurücklegen und ohne Beachtung der Reichenfolge.

Insgesamt haben wir

$$\binom{n+k-1}{k} = \binom{8}{3} = \frac{8!}{5! \cdot 3!} = 56$$

verschiedene Würfelergebnisse.

Es folgt die Aufzählung aller 56 Möglichkeiten ...

Ziehen aus Urnen (mit Zurücklegen, ohne Reihenfolge)

1,1,1	1,1,2	1,1,3	1,1,4	1,1,5	1,1,6
1,2,2	1,2,3	1,2,4	1,2,5	1,2,6	
1,3,3	1,3,4	1,3,5	1,3,6		
1,4,4	1,4,5	1,4,6			
1,5,5	1,5,6				
1,6,6					
2,2,2	2,2,3	2,2,4	2,2,5	2,2,6	
2,3,3	2,3,4	2,3,5	2,3,6		
2,4,4	2,4,5	2,4,6			
2,5,5	2,5,6				
2,6,6					
3,3,3	3,3,4	3,3,5	3,3,6		
3,4,4	3,4,5	3,4,6			
3,5,5	3,5,6				
3,6,6					
4,4,4	4,4,5	4,4,6			
4,5,5	4,5,6				
4,6,6					
5,5,5	5,5,6				
5,6,6					
6,6,6					

Ziehen aus Urnen

Zusammenfassung der vier Fälle:

Ziehen	mit Zurücklegen	ohne Zurücklegen
mit Reihenfolge	n^k	$n^{\underline{k}} = \frac{n!}{(n-k)!}$
ohne Reihenfolge	$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$	$\binom{n}{k} = \frac{n!}{(n-k)!\cdot k!}$

Dabei werden k Kugeln aus einer Urne mit n Kugeln gezogen.

Wahrscheinlichkeit

Um das Kapitel "Kombinatorik" abzuschließen, machen wir noch einige Überlegungen zur Wahrscheinlichkeit von Ereignissen.

Motivation: Wahrscheinlichkeit, im Lotto zu gewinnen

Bei einer Ziehung der Lottozahlen gibt es insgesamt $\binom{49}{6}$ Möglichkeiten (sogenannte Elementarereignisse).

Diese Elementarereignisse sind alle gleich wahrscheinlich. (Warum das so ist, überlegen wir uns im Folgenden.)

Also ist die Wahrscheinlichkeit dafür, dass die eigene Kombination gezogen wird:

$$\frac{1}{\binom{49}{6}} = \frac{1}{13.983.816} = 0,000000072\ldots$$

Dabei ist 1 die Wahrscheinlichkeit dafür, dass das betrachtete Ereignis auf jeden Fall eintritt (entspricht 100%).

Wahrscheinlichkeit

Elementarereignisse und ihre Wahrscheinlichkeiten werden in einem Wahrscheinlichkeitsraum zusammengefasst.

Wahrscheinlichkeitsraum

Ein Wahrscheinlichkeitsraum besteht aus

- einer Ergebnismenge Ω, bestehend aus den Elementarereignissen, und
- einer Funktion $P\colon \Omega \to \mathbb{R}$, die jedem Elementarereignis eine Wahrscheinlichkeit zuordnet.

Dabei muss gelten:

- Für jedes $x \in \Omega$ gilt $0 \leq P(x) \leq 1$. (Die Wahrscheinlichkeit für ein Ereignis liegt zwischen 0 und 1.)
- $\sum_{x \in \Omega} P(x) = 1$. (Die Summe aller Wahrscheinlichkeiten ist 1.)

Wahrscheinlichkeit

Bemerkungen:

- Die Formel $\sum_{x \in \Omega} P(x)$ bedeutet: summiere die Werte $P(x)$ für alle $x \in \Omega$ auf. Falls $\Omega = \{x_1, \ldots, x_n\}$, so kann man dies auch folgendermaßen schreiben:

$$\sum_{x \in \Omega} P(x) = \sum_{i=1}^{n} P(x_i) = P(x_1) + \cdots + P(x_n)$$

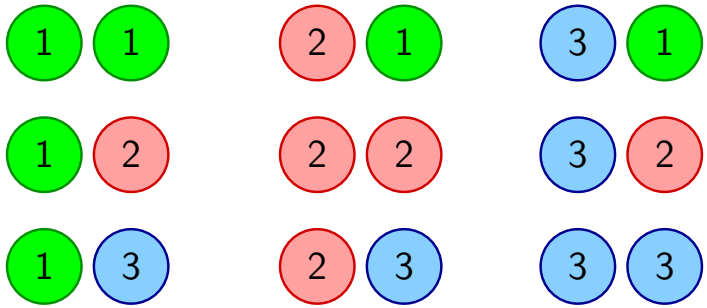
- Die Elementarereignisse müssen alle Möglichkeiten abdecken und dürfen sich nicht überlappen. Es tritt also immer genau ein Elementarereignis ein.
- Im Folgenden ist Ω eine endliche Menge. Es macht jedoch auch Sinn, unendliche Ergebnismengen zu betrachten.

Wahrscheinlichkeit

Beim Ziehen aus Urnen besteht die Ergebnismenge aus allen möglichen Kombinationen, die beim Ziehen entstehen können.

Beispiel:

Beim Ziehen von $k = 2$ Kugeln aus einer Urne mit $n = 3$ Kugeln (mit Zurücklegen, mit Beachtung der Reihenfolge) erhält man folgende neun Elementarereignisse:



Wahrscheinlichkeit

Falls alle Elementarereignisse in Ω gleich wahrscheinlich sind, so gilt

$$P(x) = \frac{1}{|\Omega|} \qquad \text{für jedes } x \in \Omega$$

Beim Ziehen mit Beachtung der Reihenfolge ist jedes Ereignis gleich wahrscheinlich, unter der Voraussetzung, dass bei einem Zug keine der vorhandenen Kugeln bevorzugt wird. Dann hat jede Verzweigung im Entscheidungsbaum die gleiche Wahrscheinlichkeit. (Das gilt mit und ohne Zurücklegen.)

- Entscheidungsbaum (Ziehen mit Zurücklegen, mit Reihenfolge)
- Entscheidungsbaum (Ziehen ohne Zurücklegen, mit Reihenfolge)

Wahrscheinlichkeit

Also gilt:

Beim Ziehen von k aus n Kugeln (mit Zurücklegen, mit Beachtung der Reihenfolge) hat jede Kombination die Wahrscheinlichkeit

$$\frac{1}{n^k}$$

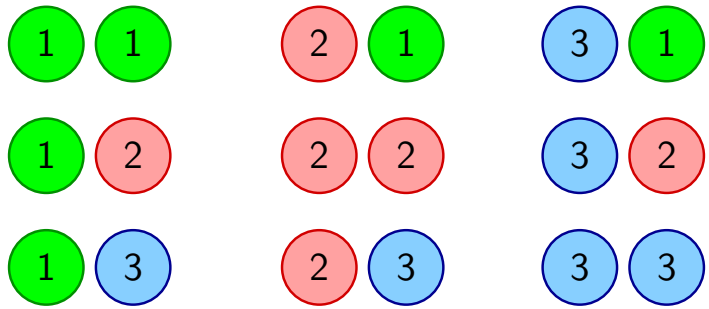
Beim Ziehen von k aus n Kugeln (ohne Zurücklegen, mit Beachtung der Reihenfolge) hat jede Kombination die Wahrscheinlichkeit

$$\frac{1}{n^{\underline{k}}}$$

Wahrscheinlichkeit

Beispiel:

Beim Ziehen von $k = 2$ Kugeln aus einer Urne mit $n = 3$ Kugeln (mit Zurücklegen, mit Beachtung der Reihenfolge) hat jedes der unten aufgeführten Elementarereignisse x die Wahrscheinlichkeit $P(x) = \frac{1}{3^2} = \frac{1}{9}$.



Wahrscheinlichkeit

Noch ein Beispiel:

Wir betrachten einen gezinkten Würfel, bei dem die Sechs wahrscheinlicher ist als die anderen Zahlen.

Die Ergebnismenge ist bei einem sechsseitigen Würfel wie folgt: $\Omega = \{1, 2, 3, 4, 5, 6\}$

Wir betrachten folgende Zurdnung von Wahrscheinlichkeiten: $P(6) = \frac{1}{2}$, $P(x) = \frac{1}{10}$ falls $x \in \{1, 2, 3, 4, 5\}$.

Test: Ergibt die Summe der Wahrscheinlichkeiten Eins?

$$\sum_{x \in \Omega} P(x) = P(1)+P(2)+P(3)+P(4)+P(5)+P(6) = 5 \cdot \frac{1}{10} + \frac{1}{2} = 1$$

Wahrscheinlichkeit

Frage: was ist die Wahrscheinlichkeit dafür, dass entweder eine 1 oder eine 6 gewürfelt wird?

Antwort: man muss nur die Wahrscheinlichkeiten der entsprechenden Elementarereignisse aufaddieren.

$\rightsquigarrow P(1) + P(6) = \frac{1}{10} + \frac{1}{2} = \frac{6}{10} = \frac{3}{5}$.

Wahrscheinlichkeit

Das Würfeln einer 1 oder 6 bezeichnet man als (zusammengesetztes) Ereignis, im Unterschied zu Elementarereignissen.

Ereignis, Wahrscheinlichkeit eines Ereignisses

Wir betrachten einen Wahrscheinlichkeitsraum, bestehend aus Ω und $P\colon \Omega \to \mathbb{R}$.

Eine Menge $E \subseteq \Omega$ heißt Ereignis. Die Wahrscheinlichkeit des Ereignisses E wird folgendermaßen berechnet:

$$P(E) = \sum_{x \in E} P(x)$$

Beispiel mit dem gezinkten Würfel: Ereignis $E = \{1, 6\}$ mit

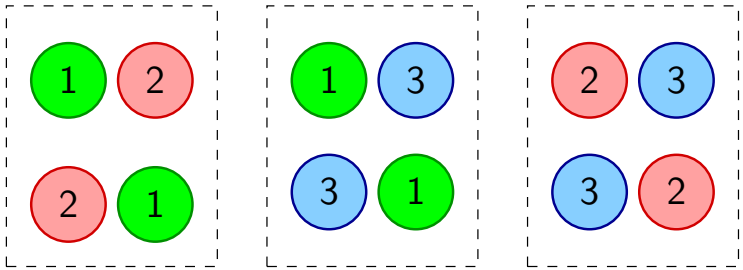
$$P(E) = P(\{1, 6\}) = P(1) + P(6) = \frac{3}{5}$$

Wahrscheinlichkeit

Für Ziehen ohne Zurücklegen, ohne Beachtung der Reihenfolge kann man den Wahrscheinlichkeitsraum des Ziehens ohne Zurücklegen, mit Beachtung der Reihenfolge betrachten.

Beispiel:

Beim Ziehen von $k = 2$ aus einer Urne mit $n = 3$ Kugeln (ohne Zurücklegen) gibt es folgende sechs Elementarereignisse, jeweils mit Wahrscheinlichkeit $\frac{1}{6}$.



Diese kann man zu drei Ereignissen zusammenfassen, die jeweils die gleichen Kombinationen (ohne Beachtung der Reihenfolge) enthalten. Jedes dieser drei Ereignisse hat die Wahrscheinlichkeit $\frac{1}{6} + \frac{1}{6} = 2 \cdot \frac{1}{6} = \frac{1}{3}$.

Wahrscheinlichkeit

Im allgemeinen Fall fasst man $k!$ Möglichkeiten zu einem Ereignis zusammen.

Beim Ziehen von k aus n Kugeln (ohne Zurücklegen, ohne Beachtung der Reihenfolge) hat jede Kombination die Wahrscheinlichkeit

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

Also hat auch in diesem Fall jede Kombination die gleiche Wahrscheinlichkeit.

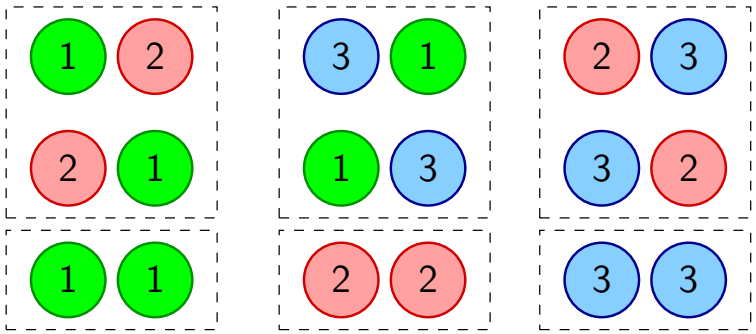
Bemerkung: Aufgrund dieser Beziehung war die Berechnung der Wahrscheinlichkeit für einen Lottogewinn korrekt.

Wahrscheinlichkeit

Wir betrachten nun noch das Ziehen mit Zurücklegen, ohne Beachtung der Reihenfolge basierend auf dem Wahrscheinlichkeitsraum des Ziehens mit Zurücklegen, mit Beachtung der Reihenfolge.

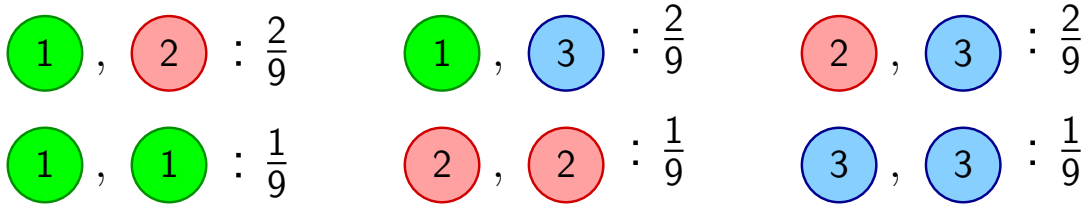
Beispiel:

Beim Ziehen von $k = 2$ Kugeln aus einer Urne mit $n = 3$ Kugeln (mit Zurücklegen) gibt es folgende neun Elementarereignisse, jeweils mit Wahrscheinlichkeit $\frac{1}{9}$.



Wahrscheinlichkeit

Diese kann man zu sechs Ereignissen zusammenfassen, die aber *nicht* alle die gleiche Wahrscheinlichkeit haben. Es ergeben sich folgende Wahrscheinlichkeiten:



Mit Summe $\frac{2}{9} + \frac{2}{9} + \frac{2}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9} = 1$

Vorsicht! Beim Ziehen von k aus n Kugeln (mit Zurücklegen, ohne Beachtung der Reihenfolge) hat nicht jede Kombination dieselbe Wahrscheinlichkeit.

Wahrscheinlichkeit

Weiteres Beispiel:

Beim Würfeln mit zwei (fairen und ununterscheidbaren) Würfeln haben nicht alle Ergebnisse dieselbe Wahrscheinlichkeit:

- Die Kombination $1, 2$ kann aus den Folgen $1\,2$ und $2\,1$ entstehen. Jede der beiden Folgen hat die Wahrscheinlichkeit $\frac{1}{6^2} = \frac{1}{36}$.
  Also hat das Würfelergebnis $1, 2$ die Wahrscheinlichkeit $2 \cdot \frac{1}{36} = \frac{1}{18}$.
- Der Sechserpasch $6, 6$ kann nur aus der Folge $6\,6$ entstehen.
  Er hat die Wahrscheinlichkeit $\frac{1}{6^2} = \frac{1}{36}$.

Wahrscheinlichkeitsrechnung

Rechnen mit Wahrscheinlichkeiten

Sei Ω ein Wahrscheinlichkeitsraum und seien $A, B \subseteq \Omega$ Ereignisse:

$$P(\Omega \backslash A) = 1 - P(A)$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(\emptyset) = 0$$

Insbesondere folgt daraus $P(A \cup B) = P(A) + P(B)$, falls $A \cap B = \emptyset$, d.h., falls A und B disjunkte Ereignisse sind.

Wahrscheinlichkeitsrechnung

Unabhängigkeit von Ereignissen (Definition)

Zwei Ereignisse $A, B \subseteq \Omega$ heißen unabhängig, falls gilt:

$$P(A \cap B) = P(A) \cdot P(B)$$

Beispiel Würfel:

- Die Ereignisse $A = \{1, 3, 5\}$ (Ergebnis ist ungerade) und $B = \{2, 4, 6\}$ (Ergebnis ist gerade) sind nicht unabhängig. Es gilt:

$$P(A \cap B) = P(\emptyset) = 0 \neq \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2} = P(A) \cdot P(B)$$

- Die Ereignisse $\{1, 3, 5\}$ (Ergebnis ist ungerade) und $\{1, 2, 3, 4\}$ (Ergebnis ist kleiner gleich vier) sind unabhängig. Es gilt:

$$P(A \cap B) = P(\{1, 3\}) = \frac{1}{3} = \frac{1}{2} \cdot \frac{2}{3} = P(A) \cdot P(B)$$

Wahrscheinlichkeitsrechnung

Bedingte Wahrscheinlichkeit (Definition)

Die bedingte Wahrscheinlichkeit ist definiert durch

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)},$$

falls $P(B) \neq 0$.

Die Wahrscheinlichkeit $P(A \mid B)$ ist intuitiv die Wahrscheinlichkeit, dass das Ereignis A eintritt, unter der Bedingung, dass man bereits weiß, dass das Ereignis B eintritt.

Sprechweise: Wahrscheinlichkeit von A, vorausgesetzt B.

Wahrscheinlichkeitsrechnung

Beispiel Würfel: $A = \{1, 3, 5\}$ (Ergebnis ist ungerade) und $B = \{1, 2, 3\}$ (Ergebnis ist kleiner gleich drei).

Dann gilt:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{P(\{1, 3\})}{P(\{1, 2, 3\})} = \frac{2}{3}$$

Unabhängigkeit und bedingte Wahrscheinlichkeit

Zwei (nicht-leere) Ereignisse A, B sind unabhängig genau dann, wenn:

$$P(A \mid B) = P(A) \quad \text{und} \quad P(B \mid A) = P(B)$$

D.h., die Kenntnis, dass das Ereignis B eintreten wird, ändert die Wahrscheinlichkeit von A nicht.

Zusammenfassung

Themen der Vorlesung

- Grundlagen: Mengenlehre, Relationen und Zahlentheorie
- Analysis, Ableitung, Kurvendiskussion
- Algebraische Strukturen: Monoide/Gruppen/Körper, Vektorräume und Matrizen, Gaußsches Eliminationsverfahren
- Kombinatorik: Ziehen aus Urnen, Wahrscheinlichkeit

Stichwortsammlung: Grundlagen

Mengenlehre:

- Menge M
- Element einer Menge $a \in M$
- Teilmenge $M' \subseteq M$
- Schnitt/Vereinigung $\cup$, $\cap$
- Potenzmenge $\mathcal{P}(M)$
- Kreuzprodukt $M_1 \times M_2$
- Relationen: Partielle Ordnung, Äquivalenzrelation (Symmetrie, Antisymmetrie, Reflexivität, Transitivität)
- Funktionen: Surjektivität, Injektivität, Bijektivität, Funktionsverkettung, Bild/Urbild einer Menge, Definitions- und Wertebereich
- Mengen von Zahlen: $\mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$

Stichwortsammlung: Analysis

Grenzwert, Stetigkeit:

- Steigung von Geraden und Tangenten
- Berechnung der Steigung mit Hilfe eines Grenzwertes
- Grenzwert
- Häufungspunkt
- Stetigkeit von Funktionen

Stichwortsammlung: Analysis

Ableitung, Kurvendiskussion:

- Definition der Ableitung (basierend auf Grenzwerten)
- Bestimmung der Ableitung bei konkreten Funktionen
- Ableitungen bekannter Funktionen
- Ableitungsregeln (Faktorregel, Summenregel, Produktregel, Kettenregel, Quotientenregel)
- n-te Ableitungen
- Kurvendiskussion (Minima, Maxima, Sattelpunkte, Wendepunkte)

Stichwortsammlung: Grundlagen

Zahlentheorie:

- Division mit Rest
- Modulo-Rechnung
- Teilbarkeit
- Primzahlen
- Primfaktorzerlegung
- Teilerfremdheit
- Größter gemeinsamer Teiler ggT & kleinstes gemeinsames Vielfaches kgV
- Euklidischer Algorithmus
- Diophantische Gleichungen
- Die Eulersche φ-Funktion
- Satz von Euler-Fermat

Stichwortsammlung: Algebraische Strukturen

Monoide/Gruppen/Körper:

- Zweistellige Operatoren
- Neutrale Elemente $0, 1$
- Inverse $-a, a^{-1}$
- Assoziativität
- Kommutativität
- Distributivität
- Der Körper $(\mathbb{Z}_n, +_n, \cdot_n)$, falls n eine Primzahl ist

Stichwortsammlung: Algebraische Strukturen

RSA-Algorithmus:

- Schlüsselerzeugung
- Privater Schlüssel
- Öffentlicher Schlüssel
- Verschlüsselung einer Nachricht
- Entschlüsselung einer Nachricht

Stichwortsammlung: Algebraische Strukturen

Vektorräume und Matrizen (Lineare Algebra):

- Vektor $\vec{v}$
- Vektorraum
- Skalar
- Anwendungsgebiet "Geometrie" (Punkte auf der Ebene und im Raum)
- Vektor-Addition $\vec{v} + \vec{u}$
- Vektorraum als Gruppe
- Multiplikation mit einem Skalar $k \cdot \vec{v}$
- Matrizen/Lineare Abbildungen A, ψ_A

Stichwortsammlung: Algebraische Strukturen

Matrizen:

- Matrizen
- Zeilendimension/Spaltendimension
- Multiplikation einer Matrix mit einem Vektor $A \cdot \vec{v}$
- Addition von zwei Matrizen $A + B$
- Die additive Gruppe der Matrizen
- Matrixmultiplikation $A \cdot B$
- Einheitsmatrix E_n
- Inverse Matrix A^{-1}

Stichwortsammlung: Algebraische Strukturen

Basen, Gaußsches Eliminationsverfahren und inverse Matrizen:

- Erzeugendensystem
- Lineare Unabhängigkeit
- Basis
- Lineare Gleichungssysteme
- Gaußsches Eliminationsverfahren
- Anzahl der möglichen Lösungen
- Inverse Matrix bestimmen

Stichwortsammlung: Kombinatorik

Ziehen aus Urnen (k Kugeln aus einer Urne mit n Kugeln):

- Mit Reihenfolge, mit Zurücklegen (n^k Möglichkeiten)
- Mit Reihenfolge, ohne Zurücklegen ($n^{\underline{k}}$ Möglichkeiten)
- Ohne Reihenfolge, mit Zurücklegen ($\binom{n+k-1}{k}$ Möglichkeiten)
- Ohne Reihenfolge, ohne Zurücklegen ($\binom{n}{k}$ Möglichkeiten)

Stichwortsammlung: Kombinatorik

Ziehen aus Urnen mit Anwendungen:

- Anzahl der Funktionen zwischen zwei Mengen
- Anzahl der injektiven Funktionen zwischen zwei Mengen
- Fakultätsfunktion
- Binomialkoeffizienten
- Allgemeine binomische Formel

Stichwortsammlung: Kombinatorik

Wahrscheinlichkeiten:

- Elementarereignisse/Ergebnismenge Ω
- Wahrscheinlichkeitsraum
- Wahrscheinlichkeiten in der Urnen-Metapher
- Rechnen mit Wahrscheinlichkeiten
- Unabhängige Ereignisse und bedingte Wahrscheinlichkeiten