Lernhilfe LA1/DIS1

Norman Koch, Lukas Malte Causse

2. Februar 2020

Inhaltsverzeichnis

1 Vorwort

Dieses Dokument stellt nach bestem Wissen und Gewissen mein Verständnis des im ersten Semester der Informatik an der TU Dresden in Linearer Algebra und Diskreten Strukturen dar. Ich erhebe weder Anspruch auf Vollständigkeit noch auf Richtigkeit meines Verständnisses noch der hier behandelten Themen.

Ich stelle dieses Dokument unter die WTFPL[1]. Jeder kann damit machen, was er oder sie möchte, und das völlig ohne Einschränkungen jedweder Art. Gleichzeitig bin ich aber für das, was Jemand mit diesem Dokument macht, nicht verantwortlich.

[1] Siehe dazu `http://www.wtfpl.net/`.

2 TODOs

Todo list

3 Allgemeine Tipps

3.1 Herleitung der Potenzgesetze

Das habe ich mir im Abi überlegt und das einmal gerafft zu haben (und nicht blind dogmatisch einfach angenommen zu haben) hat mir bisher immer ganz gut geholfen.

3.1.1 Warum ist $x^0 = 1$? Warum ist $x^{-1} = \frac{1}{x}$?

...

$$x \times x \times x = x^3 \qquad : \text{x}$$

$$\frac{x \times x \times x}{x} = x \times x = x^2 \qquad : \text{x}$$

$$\frac{x \times x \times x}{x \times x} = x = x^1 \qquad : \text{x}$$

$$\frac{x \times x \times x}{x \times x \times x} = 1 = x^0 \qquad : \text{x}$$

⚠: Wenn $x = 0$, dann hätte man $\frac{0}{0}$, daher $0^0 = \text{undef.}$

$$\frac{x \times x \times x}{x \times x \times x \times x} = \frac{\cancel{x \times x \times x} \to 1}{\cancel{x \times x \times x \times x} \to 1x} = \frac{1}{x} = x^{-1} \qquad : \text{x}$$

$$\frac{x \times x \times x}{x \times x \times x \times x} = \frac{\cancel{x \times x \times x} \to 1}{\cancel{x \times x \times x \times x} \to 1x \times x} = \frac{1}{x \times x} = x^{-2} \qquad : \text{x}$$

...

3.1.2 Warum ist $x^n \cdot x^m = x^{n+m}$?

Nehmen wir das Beispiel

$$x^3 \cdot x^5, \tag{1}$$

das bedeutet,

$$(x \cdot x \cdot x) \cdot (x \cdot x \cdot x \cdot x \cdot x), \tag{2}$$

was wegen der Assoziativität bedeutet:

$$x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x, \tag{3}$$

was das Gleiche ist wie

$$x^{3+5} = x^8. \tag{4}$$

Ich kann es nicht beweisen, aber es ist (für mich zumindest) ersichtlich, dass diese Regel aufgrund der Assoziativität der Multiplikation allgemeingültig ist.

Gleiches gilt übrigens für alle $x^r, r \in \mathbb{R}$, denn z. B.

$$x^3 \cdot x^{-2} = (x \cdot x \cdot x) \cdot (\frac{1}{x \cdot x}) = \frac{\cancel{x \cdot x} \to 1 \cdot x}{\cancel{x \cdot x} \to 1} = \frac{x}{1} = x^1 = x^{3-2}. \tag{5}$$

3.1.3 Warum ist $(x^n)^m = (x^m)^n = x^{n \cdot m}$?

Nehmen wir auch hier ein konkretes Beispiel:

$$\left(2^3\right)^2 = (2 \cdot 2 \cdot 2)^2 = (2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^6 = 2^{2 \cdot 3}. \tag{6}$$

Vertauschen wir m und n, dann erhalten wir:

$$\left(2^2\right)^3 = (2 \cdot 2)^3 = (2 \cdot 2) \cdot (2 \cdot 2) \cdot (2 \cdot 2) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^6 = 2^{3 \cdot 2}. \tag{7}$$

Auch hier kann ich es nicht allgemein *beweisen*, halte es aber, wenn man es im konkreten Fall sieht, für einleuchtend auch im Allgemeinen Fall.

3.1.4 Warum ist $x^{\frac{1}{n}} = \sqrt[n]{x}$?

Dadurch, dass $x^n \times x^m = x^{n+m}$ ist, können wir einsehen, dass

$$x^{\frac{1}{n}} \cdot x^{\frac{1}{n}} = x^{\frac{1}{n}+\frac{1}{n}} = x^{\frac{2}{n}}. \tag{8}$$

Daraus folgt im spezifischen Fall z. B. für $n = 2$:

$$x^{\frac{1}{2}} \cdot x^{\frac{1}{2}} = x^{\frac{2}{2}} = x^1. \tag{9}$$

Die Zahl, die mit sich selbst multipliziert n ergibt, nennen wir auch $\sqrt{n}$. Daher gilt:

$$x^{\frac{1}{2}} = \sqrt{n}. \tag{10}$$

Gleiches gilt z. b. für $x^{\frac{1}{3}}$, denn:

$$x^{\frac{1}{3}} \cdot x^{\frac{1}{3}} \cdot x^{\frac{1}{3}} = x^{\frac{1}{3}+\frac{1}{3}+\frac{1}{3}} = x^{\frac{3}{3}} = x^1, \tag{11}$$

weshalb $x^{\frac{1}{3}} = \sqrt[3]{x}$ ist und allgemein $x^{\frac{1}{n}} = \sqrt[n]{x}$.

3.1.5 Warum ist $x^{\frac{a}{n}} = \sqrt[n]{x^a}$?

Nehmen wir wieder ein konkretes Beispiel.

$$2^{\frac{3}{2}} \cdot 2^{\frac{3}{2}} = 2^{\frac{3}{2}+\frac{3}{2}} = \left(2^{\frac{1}{2}}\right)^3. \tag{12}$$

Aufgrund der Assoziativität der Multiplikation kann man hier die innere und die äußere Potenz beliebig tauschen. Wir erhalten:

$$\left(2^3\right)^{\frac{1}{2}} = \sqrt[2]{2^3}. \tag{13}$$

Ersetzt man die konkreten Zahlen durch Variablen und erhöhlt dementsprechend die Anzahl der Multiplikationen, ist deutlich, dass dies allgemein gilt.

3.2 Komplizierte Binominale relativ schnell ausrechnen

Um etwas wie $(a+b)^6$ schnell auszurechnen, nehmen wir das pascal'sche Dreieck bis zur sechsten Zeile:

$$\begin{array}{lccccccccccc}
n=0 & & & & & & 1 & & & & & \\
n=1 & & & & & 1 & & 1 & & & & \\
n=2 & & & & 1 & & 2 & & 1 & & & \\
n=3 & & & 1 & & 3 & & 3 & & 1 & & \\
n=4 & & 1 & & 4 & & 6 & & 4 & & 1 & \\
n=5 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
n=6 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 \quad 1
\end{array} \tag{14}$$

Dazu nehmen wir die 6. Zeile als Vorfaktor und lassen von links nach rechts für je a die Potenzen von 6 bis 0 laufen und für b von 0 bis 6. Wir erhalten:

$$\begin{aligned}
a^6 \cdot b^0 + 6a^5 \cdot b^1 + 15a^4 \cdot b^2 + 20a^3 \cdot b^3 + 15a^2 \cdot b^4 + 6a^1 \cdot b^5 + a^0 \cdot b^6 = \\
a^6 + 6a^5 \cdot b + 15a^4 \cdot b^2 + 20a^3 \cdot b^3 + 15a^2 \cdot b^4 + 6a \cdot b^5 + b^6
\end{aligned} \tag{15}$$

Das pascal'sche Dreieck bietet übrigens auch ›Shortcuts‹ zu einigen Binominalkoeffizienten, nämlich so:

$$\begin{array}{ccccccccccc}
 & & & & & & \binom{0}{0} & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} &
\end{array} \tag{16}$$

4 Gesetze der Logik und Algebra

4.1 Transitivität

$$x = y \land y = z \implies x = z, \tag{17}$$

$$x < y \land y < z \implies x < z. \tag{18}$$

4.2 Kommutativgesetz

$$a \circ b = b \circ a \tag{19}$$

4.3 Assoziativgesetz

$$(a \circ b) \circ c = b(\circ a \circ c) \tag{20}$$

4.4 Distributivgesetz

$$a \cdot (b \diamond c) = (a \cdot b) \diamond (a \cdot c) \tag{21}$$

5 Diskrete Strukturen

5.1 Logische Prinizpien

5.1.1 Darstellungssatz

Der Darstellungssatz besagt, dass jede einvariablige logische Präposition dargestellt werden kann als

$$\bigvee\bigwedge l, \tag{22}$$

wobei l ein Literal ist, d. h. entweder $\neg x$ oder x.

5.1.2 Äquivalenzen

Es gilt das sogenannte Zirkelschlussprinzip. Das besagt:

$$((x_1 \Rightarrow x_2) \wedge (x_2 \Rightarrow x_3) \wedge (x_3 \Rightarrow x_4) \wedge (x_4 \Rightarrow x_1)) \equiv \bigwedge_{i \in \{1,\ldots,n\}} (x_i \Leftrightarrow x_1) \tag{23}$$

Das heißt, dass von jedem Schluss auf jeden anderen (logisch) geschlossen werden kann.

5.2 Die Russellsche Antinomie

Sagen wir, wir definieren die Menge aller Mengen, die sich nicht selbst beinhalten:

$$M = \{x | x \notin x\} \tag{24}$$

Dann erhalten wir ein Paradox: beinhaltet die Menge sich selbst, dann darf sie sich nicht selbst beinhalten und darf nicht in die Liste (muss aber dafür vorher in der Liste gewesen sein). Beinhaltet sie sich nicht selbst, dann muss sie in Liste und darf dementsprechend wieder nicht in der Liste sein.

Dieses Problem lösen wir rein praktisch durch eine minimale Form der Typentheorie, nämlich so, dass man die Eingabemenge beschränkt. Mit:

$$M = \{x \in \mathbb{N} | x \notin x\} \tag{25}$$

entsteht dieses Paradox nicht, da in $\mathbb{N}$ keine Mengen sind, sondern konkrete einzelne Objekte.

5.3 Gödels Unvollständigkeitssätze

Gödels Unvollständigkeitssätze besagen, dass jedes formale System, aus dem Etwas wie natürliche Zahlen und die Multiplikation heraus definierbar sind, entweder

- Sätze beinhalten, die nicht bewiesen werden können, aber wahr sind, oder, wenn das System beweisen kann, dass es vollständig ist,

- dass das System dann notwendigerweise widersprüchlich sein muss.

Das heißt, man kann nie per Algorithmus alle wahren Aussagen aus einem ausreichend-komplexen formalen System auch beweisen.

Eine (sehr vereinfachte) Weise, sich solche Sätze vorzustellen, wäre z. B. ›dieser Satz ist nicht beweisbar‹. Wäre er beweisbar, wäre er wahr, also wäre er nicht beweisbar.

5.4 Die Potenzmenge

Die Potenzmenge einer Menge wird bezeichnet mit $\mathscr{P}(A)$ und beschreibt die Menge aller aus der Menge A bildbaren Untermengen.

Die Potenzmenge der leeren Menge ist die Menge mit dem Element der leeren Menge: $\mathscr{P}(\emptyset) = \{\emptyset\}$.

Die Kardinalität der Potenzmenge bei endlichen Mengen ist $|\mathscr{P}(A)| = 2^{|A|}$. Die Potenzmengen unendlicher Mengen sind strikt größer als die Ursprungsmengen.

5.5 Binominalkoeffizienten

Der Binominalkoeffizient gibt an, wie viele Möglichkeiten es gibt, aus n Elementen k auszuwählen, z. B. wie viele Möglichkeiten es gibt, beim Lotto $k = 6$ Zahlen aus $n = 49$ auszuwählen.

Das schreibt man so:

$$\binom{n}{k} = \binom{49}{6}. \tag{26}$$

Die konkrete Zahl bestimmt sich aus

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}. \tag{27}$$

Konkret für das Beispiel der Lottoziehung heißt das:

$$\begin{gathered}\binom{49}{6} = \frac{49!}{6! \cdot (49-6)!} = \frac{49!}{6! \cdot 43!} = \\ \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44 \cdot \cancel{43!}}{(6 \cdot 5 \cdot 4 \cdot 3 \cdot 2) \cdot \cancel{43!}} = \\ \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} = \frac{10068347520}{720} = 13983816\end{gathered} \tag{28}$$

Das heißt, dass die Wahrscheinlichkeit, die richtigen 6 Zahlen zu ziehen, $1 : 13983816$ ist (also etwa $0{,}00000715\%$).

Für ein einfacheres Beispiel, sagen wir, wir haben 5 Murmeln und ziehen daraus 3 heraus, heißt das, es gibt

$$\binom{5}{3} = \frac{5!}{3! \cdot (5-3)!} = \frac{5!}{3! \cdot 2!} = \frac{5 \cdot 4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 2} = \frac{120}{12} = 10 \tag{29}$$

→ 10 Kombination von Dreiermurmeln, wie wir aus den 5 Murmeln rausziehen können[2].

5.6 Permutationen

Eine Permutation ist eine bijektive Funktion, die A nach B eineindeutig abbildet.

Hat man z. B. die ersten drei natürlichen Zahlen und permutiert sie z. B. so, dass jede Zahl ›nach rechts verschoben‹ wird, dann ergibt sich folgende Permutation:

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \tag{30}$$

1 bildet hier auf 3 ab, 2 auf 1 und 3 auf 2.

Komponiert man Permutationen, fängt man im hintersten Element an und arbeitet sich dann Wert für Wert nach vorne. Das Komponieren von Permutationen ist **nicht** assoziativ, d. h. im allgemeinen Fall $p_1 \circ p_2 \neq p_2 \circ p_1$.

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tag{31}$$

$$P_1 \circ P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \tag{32}$$

Solange die Ordnung bewahrt bleibt, ist die Reihenfolge, in der die Werte aufgeschrieben werden, egal (das heißt: man muss quasi das Bild ›rotieren‹ können, als wäre es auf einem dreidimensionalen Zylinder angeordnet).

5.7 Boole'sche Funktionen

Boole'sche Funktionen haben als Eingabemenge $B^n = \{0,1\}^n$ und als Ausgabemenge die Menge $B = \{0,1\}$. Wir können diese Werte verstehen als ›0 = False‹ und ›1 = True‹.

5.8 Das DeMorgan'sche Gesetz

Kurz gesagt: $\neg(x \wedge y) = \neg x \vee \neg y$. Wenn nötig, Beweis durch Wahrheitstabelle.

5.9 Erfüllbarkeit

Eine Aussage P ist dann erfüllbar, wenn es eine Variablenbelegung gibt, für die P ein wahrer Ausdruck ist.

Beispiel:

$$P = (X \wedge Y) \vee (X \wedge \neg Y) \tag{33}$$

[2] Das lässt sich auch ausdrücken als $|M| = 5, |\{N | N \in \mathscr{P}(M) \wedge |N| = 3\}| = 10$.

P ist dann erfüllt, wenn X wahr ist. Der Wahrheitswert von Y spielt hier keine Rolle. P ist also erfüllbar, weil es eine Belegung gibt, für die P ein wahrer Satz ist.

5.10 Konjunktive/Disjunktive Normalform

Die konjunktive/disjunktive Normalform sieht beispielsweise folgendermaßen aus:

Konjunktive Normalform: $(A \vee B \vee \neg C) \wedge (D \vee E \neg F)$. Die Struktur ist, dass wir mindestens eine Klausel haben, die in der Klausel mit dem $\bigvee$ verbunden ist und die Klauseln als Ganzes sind mit dem $\bigwedge$ verbunden.

Disjunktive Normalform: $(A \wedge B \wedge \neg C) \vee (D \vee E \neg F)$. Die Struktur ist, dass wir mindestens eine Klausel haben, die in der Klausel mit dem $\bigwedge$ verbunden ist und die Klauseln als Ganzes sind mit dem $\bigvee$ verbunden.

Wir erhalten aus einer Wahrheitstabelle die KNF, in dem wir uns nur die falschen Werte ansehen und dann entsprechend negieren. Beispiel:

Nummer	A	B	C	F
1	0	0	0	1
2	0	0	1	1
3	0	1	0	1
4	0	1	1	1
5	1	0	0	0
6	1	0	1	1
7	1	1	0	0
8	1	1	1	1

Interessant sind hier die Zeilen mit der Nummer 5 und 7, denn diese sind 0. Um sie aus den Werten A, B und C zu generieren, müssen wir folgende Formeln annehmen:

$$P = (\neg A \vee B \vee C) \wedge (\neg A \vee \neg B \vee C) \tag{34}$$

und haben somit die KNF gefunden.

Bei der DNF schauen wir uns nur die wahren Zeilen an:

Nummer	A	B	C	F
1	0	0	0	0
2	0	0	1	0
3	0	1	0	0
4	0	1	1	0
5	1	0	0	1
6	1	0	1	0
7	1	1	0	1
8	1	1	1	0

(Wieder 5 und 7, nur diesmal exakt andersherum)

Wir schauen uns an, welche Werte negiert werden müssen, um in der Disjunktion zu diesen Falschheitswerten zu kommen und wenden das DeMorgan'sche Gesetz (vgl. ↗ *Das DeMorgan'sche Gesetz* (5.8)) an.

$$P = \neg(\neg A \wedge B \wedge C) \vee \neg(\neg A \wedge \neg B \wedge C) = \tag{35}$$
$$(A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C)$$

5.11 Horn-Satisfiability

Der Horn-Satisfiability-Algorithmus[3] (kurz: Horn-SAT) bietet eine Möglichkeit, die Erfüllbarkeit einiger Sätze, die in der H o r nschen Normalform (welche eine KNF ist, vgl. dazu ↗ *Konjunktive/Disjunktive Normalform* (5.10)) gegeben sind, relativ schnell zu überprüfen. Dafür müssen ›positive Klauseln‹ (Klauseln, die nicht negiert sind) herausgesucht werden und alle negierten Klauseln der selben Variable weggestrichen werden. Ein Ausdruck heißt ›Horn‹, wenn in jeder Klausel maximal ein positives Literal ist.

Der Algorithmus lautet im Detail wiefolgt:

1. Suche nach Klauseln, die nur ein einziges positives Literal haben (z. B. $(X, \neg Y, \neg Z)$, hier: X).
2. Streiche in allen anderen Klauseln, in denen das Positive Literal negiert sind, dieses negierte Literal heraus.
3. Sollte eine Klausel leer werden, gebe ›unerfüllbar‹ zurück.
4. Gehe zur nächsten Klausel und beginne von vorn, bis keine Streichungen mehr möglich sind. Pro Klausel darf nur eine Variable gestrichen werden
5. Gebe ›erfüllbar‹ zurück.

Beispiel.

$$\underbrace{(Y \vee \neg Z \vee \neg U)}_{\text{Erste Klausel}} \wedge \underbrace{(\neg U \vee \neg Y)}_{\text{Zweite Klausel}} \tag{36}$$

In der ersten Klausel ist nur exakt ein nicht-negiertes Literal, nämlich Y. Streichen wir nun die Negation von Y aus der zweiten Klausel und wir erhalten:

$$(Y \vee \neg Z \vee \neg U) \wedge (\neg U) \tag{37}$$

Damit die neue zweite Klausel wahr wird, muss U falsch sein. Damit die erste Klausel wahr wird, muss U ebenfalls falsch sein, also streichen wir auch die zweite Klausel.

$$(Y \vee \neg Z \vee \neg U) \tag{38}$$

und haben damit die Belegung, die die Bedingung erfüllt: $Y = 1, Z = 0, U = 0$.

[3] Der Algorithmus ist auch bekannt als ›positive-1-Resolution‹.

5.12 Mengenlehre

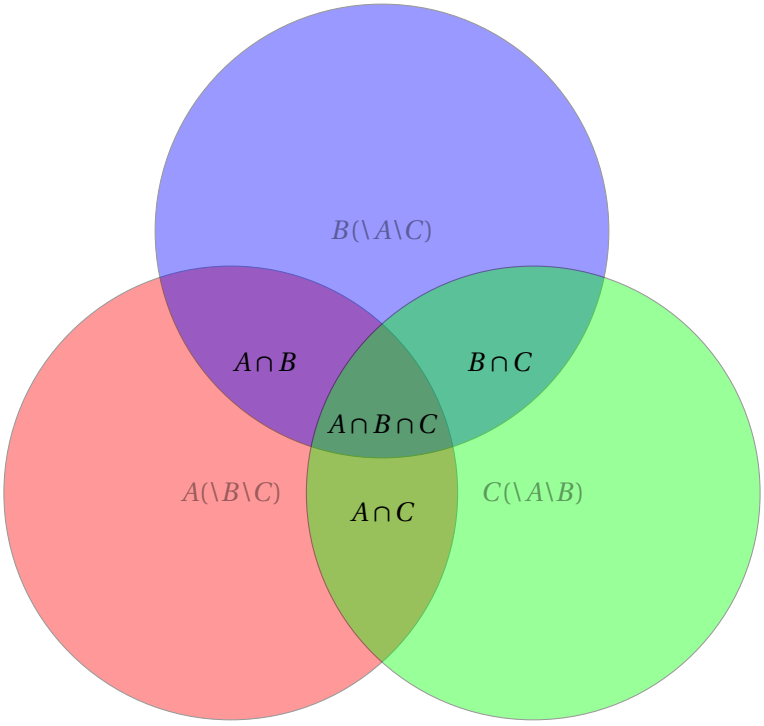


Abbildung 1: Die Mengenoperationen im Venn-Diagramm. Alle Mengen zusammen ergeben $A(\cup B \cup C)$

Eine Menge ist eine abstrakte Sammlung von verschiedenartigen Gegenständen. Mengen werden in Mengenklammern geschrieben:

$$\{a, b, c, \ldots\}. \tag{39}$$

In Mengen kommen keine Elemente doppelt vor. Die Menge ›verschluckt‹ alle gleichartigen Elemente.

Mengenoperationen sind die Vereinigung $(A \cup B)$, der Schnitt $(A \cap B)$ und die Differenz $(A \backslash B)$.

5.13 Die natürlichen Zahlen

In der Mengentheorie ist alles eine Menge, und so sind auch die natürlichen Zahlen $\mathbb{N}$ eine Menge. $0 = \{\emptyset\}, 1 = \{\emptyset, \{\emptyset\}\}, \ldots$.

Die natürlichen Zahlen sind wohlgeordnet, das heißt: in jeder beliebigen Menge aus $\mathbb{N}$ gibt es ein eindeutig-kleinstes Element (gleiches gilt für jede Untermenge aus dieser Menge, weshalb jede Zahl eine genaue Ordnung hat).

$\mathbb{C}$ ist dagegen z. b. nicht wohlgeordnet, denn es gibt kein eindeutig-kleinstes Element.

5.14 Funktionen

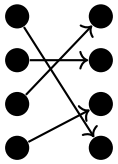
Funktionen bilden eine Menge auf eine andere anhand einer genau spezifizierten Regel ab.

Beispielsweise die Funktion $f(x) = x^2$. Die bessere Schreibweise wäre:

$$f : \mathbb{R} \to \mathbb{R} \longrightarrow x \to x^2, \tag{40}$$

denn dabei ist ersichtlich, welche Menge auf welche abgebildet wird (hier beide $\mathbb{R}$).

5.14.1 Eigenschaften von Funktionen



Surjektivität Eine Funktion ist surjektiv, wenn jedes Element in der Zielmenge mindestens ein mal getroffen wird

Die Surjektivität lässt sich zeigen, indem man schaut, ob jede Gleichung der Form $y = f(x)$ eine Lösung beinhaltet. Die Gleichung $y = \frac{1}{x}$ ist beispielsweise nicht surjektiv, weil für $x = 0$ keine Lösung existiert.

Injektivität Eine Funktion ist injektiv, wenn jedes Element der Zielmenge maximal einmal getroffen wird.

Das heißt, für einen Beweis z. B., dass für jede injektive Funktion gelten muss:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2. \tag{41}$$

Beispiel:

$$x_1, x_2 \in \mathbb{R}, \tag{42}$$

$$f : \mathbb{R} \to \mathbb{R} : x \longrightarrow e^x, \tag{43}$$

$$f(x_1) = f(x_2) \Rightarrow e^{x_1} = e^{x_2} \Rightarrow \ln(e^{x_1}) = \ln(e^{x_2}) \Rightarrow x^1 = x^2 \blacksquare. \tag{44}$$

Bijektivität Eine Funktion ist bijektiv, wenn sie sowohl surjektiv als auch injektiv ist (d. h. jedes Element wird exakt ein mal getroffen).

5.15 Operatoren

Verallgemeinert kann man Operatoren sehen als Funktion auf einer oder mehr Variablen. Der Operator $\neg x$ z. B. hat als Parameter nur eine einzige Variable, während $a + b$ zwei Variablen hat (und damit sowas wäre wie plus(a, b). Wenn es nicht um das konkrete Ausführen einer Funktion geht, schreibt man auch ›∘‹ statt dem Funktionsnamen.

5.16 Tupel

Tupel sind geordnete Zahlenpaare der Form $\langle a, b, c, \dots \rangle$. Das geordnete Paar $\langle 0, 1, 2 \rangle$ löst sich auf zur Menge $\{0, \{0, 1\}, \{0, 1, 2\}\}$. Die Kardinalität der jeweiligen Untermenge bestimmt ihre Position, während ihr im Vergleich zu allen niedrigerkardinalen Mengen neues Element das Element an der jeweiligen Position bestimmt.

5.17 Beweis durch vollständige Induktion

Bei einer vollständigen Induktion zeigt man, dass die These T für $n = 0$ (bzw. 1 bzw. das erste Element, für das sie gelten soll) gilt, dann, dass sie für n gilt und dann, dass sie auch für $n+1$ gilt.

Dabei ergibt sich dadurch, dass sie für n und den Nachfolger von n gilt, dass sie für alle n gilt.

Beispiel.

Wir wollen zeigen, dass $\forall n \in \mathbb{N}$ gilt:

$$\underbrace{\sum_{k=1}^{n} (2k-1)^2}_{\text{Linker Gleichungsteil}} = \underbrace{\frac{n \cdot (2n-1) \cdot (2n+1)}{3}}_{\text{Rechter Gleichungsteil}} \tag{45}$$

Dazu schauen wir erst, ob das für $n = 1$ gilt (Induktionsanfang), indem wir in beide Teilformeln $n = 1$ einsetzen:

$$\underbrace{\sum_{k=1}^{1} (2k-1)^2 = (2 \cdot 1 - 1)^2 = (2-1)^2 = 1^2 = 1}_{\text{Einsetzung von } n \to 1 \text{ in linke Teilgleichung}}. \tag{46}$$

$$\underbrace{\frac{1 \cdot (2 \cdot 1 - 1) \cdot (2 \cdot 1 + 1)}{3}}_{\text{Einsetzung von } n \to 1 \text{ in rechte Teilgleichung}} = \frac{1 \cdot (2-1) \cdot (2+1)}{3} = \frac{1 \cdot 1 \cdot 3}{3} = \frac{3}{3} = 1. \tag{47}$$

Die Ergebnisse beider Gleichungen sind identisch, daher ist der Induktionsanfang erfüllt. Sollten hier bereits unterschiedliche Ergebnisse herauskommen, dann hat man sich entweder verrechnet oder man kann den Beweis abbrechen (sofern man sich nicht verrechnet hat), weil dann die Gleichung nicht mehr allgemeingültig ist.

Sofern man weitermacht, ersetzt man nun n durch $n+1$ in beiden Gleichungen.

$$\sum_{k=1}^{n+1} (2 \cdot k - 1)^2 = \sum_{k=1}^{n} (2 \cdot k - 1)^2 + \sum_{k=n+1}^{n+1} (2 \cdot k - 1)^2 = \tag{48}$$

Dabei nutzt man in diesem Falle aus, dass die Summe aufteilbar ist in die Summe der vorherigen Glieder plus der Summe des neuen Gliedes für $n+1$. Nun benutzt man die Induktionsannahme, dass $\sum_{k=1}^{n} (2k-1)^2 = \frac{n \cdot (2n-1) \cdot (2n+1)}{3}$ ist, und ersetzt die Summe bis n durch die Gleichung in der Formel für $n+1$:

$$\sum_{k=1}^{n+1}(2\cdot k-1)^2=\frac{n\cdot(2n-1)\cdot(2n+1)}{3}+\sum_{k=n+1}^{n+1}(2\cdot k-1)^2. \tag{49}$$

Dann berechnet man die Summe für das Übriggebliebene Summenglied:

$$\sum_{k=1}^{n+1}(2\cdot k-1)^2=\frac{n\cdot(2n-1)\cdot(2n+1)}{3}+(2\cdot(n+1)-1)^2. \tag{50}$$

Um einen gemeinsamen Nenner zu bekommen, multiplizieren wir nun das zweite Glied mit 3 und dividieren es gleich wieder dadurch. Wir erhalten:

$$\sum_{k=1}^{n+1}(2\cdot k-1)^2=\frac{n\cdot(2n-1)\cdot(2n+1)}{3}+\frac{(2\cdot(n+1)-1)^2\cdot 3}{3}= \tag{51}$$

$$\frac{n\cdot(2n-1)\cdot(2n+1)+(2\cdot(n+1)-1)^2\cdot 3}{3}.$$

Multiplizieren wir diese Gleichung stückweise aus:

$$\frac{n\cdot(2n-1)\cdot(2n+1)+(2\cdot(n+1)-1)^2\cdot 3}{3}=\frac{n\cdot(4n^2-1)+(2\cdot(n+1)-1)^2\cdot 3}{3}= \tag{52}$$

$$\frac{4n^3-n+(2\cdot(n+1)-1)^2\cdot 3}{3}=\frac{4n^3-n+(2n+2-1)^2\cdot 3}{3}=\frac{4n^3-n+(4n^2+4n+1)\cdot 3}{3}=$$

$$\frac{4n^3-n+12n^2+12n+3}{3}=\underbrace{\frac{4n^3+12n^2+11n+3}{3}}_{\text{Vereinfachte Lösung für } n+1 \text{ aus dem linken Gleichungsteil}}.$$

Mit der Gleichung $\frac{4n^3+12n^2+11n+3}{3}$ haben wir die Formel für $\sum_{k=1}^{n+1}$ soweit es geht zusammengefasst.

Nun vergleichen wir, was passiert, wenn man die die Induktionsannahme $\frac{n\cdot(2n-1)\cdot(2n+1)}{3}$ statt n jetzt $n+1$ einsetzt. Wir erhalten:

$$\frac{(n+1)\cdot(2(n+1)-1)\cdot(2(n+1)+1)}{3}. \tag{53}$$

Diese Gleichung multiplizieren wir wieder aus:

$$\frac{(n+1)\cdot(2(n+1)-1)\cdot(2(n+1)+1)}{3}=\frac{(n+1)\cdot(2n+2-1)\cdot(2n+2+1)}{3}= \tag{54}$$

$$\frac{(n+1)\cdot(2n+1)\cdot(2n+3)}{3}=\frac{(n+1)\cdot(2n+1)\cdot(2n+3)}{3}=$$

$$\frac{(n+1)\cdot((4(n+1)^2-1))}{3}=\frac{(n+1)\cdot((4\cdot(n^2+2n+1)-1))}{3}=$$

$$\frac{(n+1)\cdot((4n^2+8n+4)-1)}{3}=\frac{(n+1)\cdot(4n^2+8n+3)}{3}=$$

$$\underbrace{\frac{4n^3+12n^2+11n+3}{3}}_{\text{Vereinfachte Lösung für } n+1 \text{ aus dem rechte Gleichungsteil}}.$$

Wir sehen, dass die beiden Ergebnisse für den linken Teil der Gleichung und den rechten Teil der Gleichung gleich sind. Das heißt, wir sind tatsächlich in der Induktionsannahme bestätigt, und das heißt:

$$\forall n \in \mathbb{N} : \sum_{k=1}^{n} (2k-1)^2 = \frac{n \cdot (2n-1) \cdot (2n+1)}{3}.$$

■

5.17.1 Kann man, wenn man in der vollständigen Induktion annehmen muss, dass das, was man beweisen ist, wahr ist nicht Beliebiges (auch Falsches) beweisen?

Diese Frage hab ich mir gestellt und dazu folgendes Beispiel gefunden:

Wir wollen per Induktion beweisen, dass $\forall n \in \mathbb{N} : n+1 < n$. Dieser Beweis scheitert, sobald wir den Induktionsanfang mit $n = 0$ machen wollen, denn: $(0+1 < 0) \equiv (1 < 0)$ ist eine falsche Aussage.

Es gibt aber auch Beweise, für die der Induktionsanfang funktioniert, die aber nicht für alle weiteren n gelten, z. B.:

$$\forall n \in \mathbb{N} : n^3 \leq n^2 \tag{55}$$

Setzen wir $n = 1$, erhalten wir:

$$(1^3 \leq 1^2) \equiv (1 \leq 1) \tag{56}$$

was eine wahre Aussage ist. Der Induktionsanfang ist also gegeben.

Nun setzen wir n auf $n+1$:

$$\begin{aligned}
(n+1)^3 \leq (n+1)^2 \equiv \qquad (57)\\
n^3+3n^2+3n+1 \leq n^2+2n+1 \equiv\\
3(n^2+n)+n^3+1 \leq 2n+n^2+1 \equiv\\
3(n^2+n)+n^3 \leq 2n+n^2 \equiv\\
3n^2+3n+n^3 \leq 2n+n^2 =\\
3n+3+n^2 \leq 2+n =\\
n^2+2n+3 \leq 2.
\end{aligned}$$

Durch Kürzen von auf beiden Seiten vorkommenden Variablen mit Vorfaktoren erhalten wir diese Ungleichung, aus der wir sehen, dass das für kein weiteres n eine wahre Aussage ergibt, solange $n^2+2n+3 \not\leq 2$ ist, d. h. die Gleichung nur für $n \in \{0,1\}$ gilt. Das heißt: der Beweis scheitert, weil wir eine falsche Induktionsannahme gemacht haben.

5.18 Primzahlen

Eine Primzahl ist eine Zahl, die nur zwei Teiler aus $\mathbb{N}$ hat, nämlich 1 und sich selbst.

Jede Zahl lässt sich eineindeutig in Primfaktoren zerlegen, so dass $n \in \mathbb{N} \Rightarrow n = p_1 \times p_2 \times \cdots \times p_n$.

Es gibt ›mehr als jede vorgelegte Anzahl an Primzahlen‹ (Euklid), d. h. unendlich viele.

Die Dichte der Primzahlen bis x entspricht $\approx \frac{x}{\ln(x)}$.

5.19 Schnelles Berechnen großer ganzzahliger Potenzen per binärer Exponentiation

Mit dieser Methode ist es möglich, die Anzahl an auszuführenden Multiplikationen bei großen Potenzen enorm zu verringern. Sie funktioniert folgendermaßen: man hat die Potenz a^n und schreibt sich zuerst n in Binär auf, beispielsweise bei 2^{10} ist die 1010 in Binär 1010_2.

Statt nun 9 Multiplikationen der Form $\underbrace{2 \times 2 \times 2 \times 2 \times \cdots \times 2}_{9 \text{ Multiplikationsoperationen}}$ durchzuführen, nimmt man die Binärzahl als ›Rezept‹ und wandelt sie um: Aus einer 1 wird ein QM und aus einer 0 ein Q. Wir erhalten nun:

QM Q QM Q

Q steht für das Quadrieren, QM für Quadrieren und Multiplizieren.

Wir streichen nun das erste Element und erhalten:

Q QM Q

Das heißt: wir rechnen statt 2^{10} jetzt:

$$\left(\left(\left(2^2\right)^2\right) \cdot 2\right)^2 = ((16) \cdot 2)^2 = (32)^2 = 1024 \tag{58}$$

Wichtig: rechnet man in einem Restklassenring R, kann man nach Al-Kashi nach jeder Operation modulo nehmen, und so den Modulo des Gesamtproduktes berechnen, ohne in exorbitant große Zahlenbereiche zu kommen (vgl. dazu ↗ *Al-Kashi* (5.30)). So ist im Restklassenring $\mathbb{R}_{10}$ 2^{10}:

$$\left(\left(\left(\left(2^2\right)^2\right) \cdot 2\right)^2 \equiv (6 \cdot 2)^2 \equiv (2)^2 \equiv 4 \mod 10\right) = (1024 \equiv 4 \mod 10) \tag{59}$$

5.20 (Erweiterter) euklidischer Algorithmus

— Eine Herleitung von Lukas Malte Causse —

5.20.1 Tabellenform wählen

Bedeutungen:

i – Indexnummer

k_i – Wie oft geht r_{i+1} in r_i?

i	k_i	r_i	a_i	b_i
0				
1			a_1	
2				
3				
4				
5				

r_i – Restwert (beinhaltet auch Ausgangswerte, die ebenfalls als Rest behandelt werden)[4]

a_i, b_i – Bézout-Multiplikator zur betreffenden Zeile. Die Bézout-Multiplikatoren für den ggT sind die letzten a_i und b_i

5.20.2 Grundwerte eintragen

Für das Beispiel ggt(1001, 90) sind die beiden Eingabewerte als erstes in die r_i Spalten (für $i = \{0, 1\}$) einzutragen, wobei die größere der beiden Zahlen stets an die nullte Stelle kommt.

a_i und b_i können in den gleichen Zeilen auch immer bereits eingesetzt werden.

i	k_i	r_i	a_i	b_i
0		1001	1	0
1		90	0	1
2				
3				
4				
5				

Allgemeine Formeln:

$$k_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor \tag{60}$$

$$r_n = r_{n-2} - r_{n-1} 1 k_{n-1} \tag{61}$$

$$a_n = a_{n-2} - k_{n-1} a_{n-1} \tag{62}$$

$$b_n = b_{n-2} - k_{n-1} b_{n-1} \tag{63}$$

Mit konkreten Werten für dieses Beispiel:

$$k_1 = \left\lfloor \frac{r_0}{1} \right\rfloor = \left\lfloor \frac{1001}{90} \right\rfloor = \lfloor 11, 1\overline{2} \rfloor = 11 \tag{64}$$

[4] Die Idee ist wohl, dass jeder E-Eukl-Algorithmus Resultat eines ›höherwertigen‹ E-Eukl-Startwert-Algorithmus ist. D. h. die Tabelle in Richtung negativer Indexwerte unendlich ist.

$$r_2 = r_0 - r_1 k_1 = 1001 - 90 \times 11 = 1001 - 990 = 11 \tag{65}$$

$$a_2 = a_0 - k_1 a_1 = 1 - 11 \times 0 = 1 \tag{66}$$

$$b_2 = b_0 - k_1 b_1 = 0 - 11 \times 1 = -11 \tag{67}$$

i	k_i	r_i	a_i	b_i
0		1001	1	0
1	11	90	0	1
2		11	1	-11
3				
4				
5				

5.20.3 Weiterrechnen und »B. M.-Trick«

Es gelten allgemein die oben aufgestellten generalisierten Regeln. Aber es gibt einen Trick: um nicht jedes Mal die Formeln benutzen zu müssen, kann man sich merken: »oben, anfang, drunter«.

i	k_i	r_i	a_i	b_i
0		1001	1	0
1	11	90	0	1
2	8	11	1	-11
3		2	-8	89
4				
5				

Allgemeine Formel:

$$a_{i+2} = a_i - k_{i+1} \times a_{i+1} \tag{68}$$

Analoges gilt für b_{i+2}:

$$b_{i+2} = b_i - k_{i+1} \times b_{i+1} \tag{69}$$

5.20.4 Fertigrechnen und Überprüfungstrick

Hat man $r_i = 1$, muss nicht weitergemacht werden.o

Überprüfungstrick: die Vorzeichen zwischen a_i und b_i müssen in jeder Zeile wechseln, sonst hat man einen Rechenfehler gemacht.

i	k_i	r_i	a_i	b_i
0		1001	1	0
1	11	90	0	1
2	8	11	1	-11
3	5	2	-8	89
4	2	1	41	-456
5		0		

Man nehme die letzte Zeile (in der $r_i \neq 0$ ist und überprüfe:

$$\text{ggt}(1001,90) = 1 = 41 \times 1001 + (-456) \times 90 = 1 \tag{70}$$

5.21 Das Lemma von Bezout

Seien m und n Zahlen $\in \mathbb{N} \wedge m \neq 0 \wedge n \neq 0$, dann gibt es $a, b \in \mathbb{N}$, so dass $\text{ggT}(m,n) = am + bn$. a und b lassen sich mit dem erweitertem euklidischen Algorithmus (auch ›E-Eukl‹ genannt, vgl. dazu ↗ *(Erweiterter) euklidischer Algorithmus* (5.20)) ermitteln.

5.22 Körper

Körper sind abstrakte algebraische Objekte, die aus einer Menge und zwei Operationen (›+‹ und ›·‹) bestehen.

Einen Körper schreibt man so: $(G, \cdot, +)$.

Für Körper gelten die folgende Regeln:

- $(K, +)$ ist eine abelsche Gruppe (vgl. ↗ *Spezialfall: Abelsche Gruppen* (5.23.2))
- $(K, \cdot)$ ist eine abelsche Gruppe
- Es gelten die Distributivgesetze:

$$\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c \tag{71}$$

$$\forall a, b, c \in K : (a + b) \cdot c = a \cdot c + b \cdot c \tag{72}$$

5.23 Gruppen

Gruppen bestehen aus:

- Einer Grundmenge G
- Einer zweistelligen Operation $G\circ : G^2 \to G$ und der Umkehroperation $G\circ^{-1} : G \to G$
- Einem neutralen Element $e \in G$

Damit diese Dinge eine Gruppe ergeben, müssen für die Operation $\circ$ folgende Eigenschaften erfüllt sein:

- Assoziativität: $a \circ (b \circ c) = (a \circ b) \circ c$
- Das neutrale und inverse Element: $a \circ a^{-1} = a^{-1} \circ a = e$, $e \circ a = a \circ e = a$, das neutrale Element ist dabei das, für das gilt: $a \circ e = e \circ a = a$, das Inverse das, für das gilt $a \circ a^{-1} = e$.
- Gruppen müssen abgeschlossen sein, d. h. $a \circ b$ bzw. $b \circ a$ darf für kein a, b aus der Grundmenge der Gruppe herausführen

Schreibweise: $(G, \circ, e)$.

5.23.1 Halbgruppe

Ist nur die Assoziativität gegeben, spricht man auch von einer Halbgruppe. Halbgruppen sind abstraktere Strukturen als Gruppen (die noch neutrale Elemente für $+, \cdot$ beinhalten und abgeschlosssen sein müssen).

5.23.2 Spezialfall: Abelsche Gruppen

Abelsche Gruppen sind Gruppen (vgl. ↗ *Gruppen* (5.23)), für die die Kommutativität gilt, d. h.:

$$a \circ b = b \circ a$$

So sind $(\mathbb{N}, +)$ und $(\mathbb{N}, \cdot)$ abelsche Gruppen (denn $\forall a, b \in \mathbb{N} : a + b = b + 1 \land a \cdot b = b \cdot a$), aber $(\mathbb{N}, /)$ (Division) ist keine, denn $\neg \forall a, b \in \mathbb{N} : \frac{a}{b} = \frac{b}{a}$.

5.23.3 Spezialfall: Zyklische Gruppen

Eine zyklische Gruppe ist eine Gruppe modulo n, in der ein Element g existiert, das, wenn man es potenziert, alle anderen Elemente der Gruppe erreicht.

Beispiel: $\mathbb{N}_5$ enthält die Zahlen der Menge $M = \{x \in \mathbb{N} | 1 \leq x \leq 5 \land \text{ggT}(x, 5) = 1\}$, was de facto bedeutet: $M = \{1, 2, 3, 4\}$. Die Kardinalität der Menge M ist $\phi(5) = 4$.

a	b	$a^b \equiv \underline{c} \mod 5$
3	0	$3^0 \equiv \underline{1} \mod 5$
3	1	$3^1 \equiv \underline{3} \mod 5$
3	2	$3^2 \equiv \underline{4} \mod 5$
3	3	$3^3 \equiv \underline{2} \mod 5$
3	4	$3^4 \equiv \underline{1} \mod 5$
3	5	$3^5 \equiv \underline{3} \mod 5$
…	…	…

Das heißt, dass $\mathbb{N}_5$ in Bezug auf das Element $3 \in \mathbb{N}_5$ eine zyklische Gruppe ist, denn jedes Element der Menge M ist durch Potenzen von 3 erreichbar.

Allgemein lautet die Regel: Sei G eine Gruppe und $g \in G, n, \in \mathbb{N}$. Dann ist $g^0 = e$ (das neutrale Element), $g^1 = g$, $g^n = g \circ g^{n-1}$ für $n \geq 1$. Eine Gruppe heißt zyklisch, wenn gilt: $G = \{g^n | n \in \mathbb{Z}\}$.

5.24 Ring

Ein Ring besteht aus einer Menge R und zwei zweistelligen Operationen, + und ·, so dass $(R, +)$ eine abelsche Gruppe (vgl. ↗ *Spezialfall: Abelsche Gruppen* (5.23.2)) ist und $(R, \cdot)$ eine Halbgruppe (vgl. ↗ *Halbgruppe* (5.23.1)). Außerdem müssen die Distributivgesetze erfüllt sein, d. h.

$$\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c. \tag{73}$$

5.24.1 Restklassenring

Restklassenringe haben einen Maximalwert, so wie z. B. ein CPU mit einer Bitbreite von 16 nur `unsigned Integer` von 0 bis 65535 verarbeiten kann und in einen Overflow läuft, wird die Zahl größer. Bei $2^{16} = 65536$ Bits wird jede gespeicherte Zahl eigentlich erst Modulo 65536 genommen.

Beispiel. Nehmen wir den Restklassenring $\mathbb{N}_5$. Bleiben wir in unseren Rechnungen unterhalb der 5, dann ändert sich nichts an der gewohnten Weise, mit dem Restklassenring zu rechnen. Nehmen wir jedoch $a = 3, b = 3 \in \mathbb{N}_5$ und multiplizieren wir diese, erhalten wir:

$$3 \cdot 3 = 9, \tag{74}$$

$$9 \equiv \underline{4} \mod 5 \tag{75}$$

Das Ergebnis von $3 \cdot 3$ in $\mathbb{N}_5$ ist also 4.

Ähnlich verhält es sich mit dem Restklassenring $\mathbb{N}_2$, den wir im Unterricht als GF(2) hatten.

Dort ist $0 + 0 = 0, 1 + 0 = 1, 0 + 1 = 1,$ $\underbrace{1 + 1 = 0}_{\text{Wegen } 1+1=2,\ 2\equiv 0 \mod 2}$.

Damit wir rein praktisch nicht in riesige Zahlen laufen, können wir dank der Homomorphieregel nach jedem Rechenschritt einzeln modulo nehmen.

5.25 Einheiten

Eine Einheit ist ein Element a eines Ringes R, für das gilt: $a \circ a^{-1} = e$ (e = neutrales Element).

5.26 Nullteiler

Ein Nullteiler eines Ringes R_n ist eine von 0 verschiedene Zahl a, für die gilt: $a, b \in R_n : a \neq 0, b \neq 0 : a \cdot b = 0 \mod n$.

Ein Beispiel eines Nullteilers wäre z. B. im Ring $(\mathbb{Z}_6, +, \cdot)$ die Zahlen 2, 3, 4, denn:

$$2 \cdot 3 \equiv 4 \cdot 3 \equiv 0 \mod 6. \tag{76}$$

Ein Nullteiler ist nie eine Einheit (vgl. ↗ *Einheiten* (5.25)).

5.27 Die Komplexitätsklassen

Die Komplexitätsklassen beschreiben, wie effizient eine Aufgabe ausgeführt werden kann. Es gibt Aufgaben, die in polynominaler Zeit im Vergleich zur Inputgröße ausgeführt werden können (z. B. Addition), für andere sind keine Algorithmen bekannt, die in polynominaler Zeit ausgeführt werden können (z. B. die Faktorisierung von Zahlen in ihre Primzahlfaktorisierung.

Angegeben wird das für Algorithmen in der Landau-Notation: Bogosort hat z. B. im Worst-Case die nicht-polynominale Zeit $\mathcal{O}(n \cdot n!)$, d. h. für eine maximal-unsortierte (umgekehrt-sortierte) Liste mit n Einträgen braucht man $n \cdot n!$ Berechnungen.

5.27.1 Die Komplexitätsklasse P

Probleme, für die Algorithmen bekannt sind, die eine polynominale Laufzeit haben, gehören der Klasse ›P‹ an.

5.27.2 Die Komplexitätsklasse NP

Probleme, für die keine Algorithmen bekannt sind, die eine polynominale Laufzeit haben, gehören der Klasse ›P‹ an. Es ist nicht bekannt, ob $P = NP$, d. h. ob es für alle Probleme prinzipiell Algorithmen gibt, die diese in polynominaler Zeit lösen.

5.27.3 Die Komplexitätsklasse RP

›RP‹ steht für ›**R**andomized **P**olynomial‹, d. h.

1. die Laufzeit ist polynomiell.
2. falls die Antwort ›nein‹ lautet, muss der Algorithmus ›nein‹ ausgeben,
3. falls die Antwort ›ja‹ lautet, muss der Algorithmus mit mindestens einer $\frac{2}{3}$-Wahrscheinlichkeit ›ja‹ ausgeben.

5.28 Multiplikative Gruppe Modulo n

Die Menge $\mathbb{Z}_n$ beinhaltet die Zahlen $\{0, 1, 2, \ldots, n\}$. Aus dieser Menge lässt sich eine Gruppe definieren (vgl. ↗ *Gruppen* (5.23)).

Dazu definieren wir die Menge $\mathbb{Z}_n^*$, die alle Elemente beinhaltet, die teilerfremd zu n sind. Mathematisch ausgedrückt heißt das:

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n | \text{ggt}(k, n) = 1\} \tag{77}$$

Das heißt für das Beispiel $\mathbb{Z}_{10}$ wird $\mathbb{Z}_n^*$ zu $\{k \in \{0,1,2,3,4,5,6,7,8,9\} | \text{ggt}(k,10) = 1\}$, was inhaltlich bedeutet:

$$k = 0 \rightarrow \text{ggT}(10,0) = 10 X$$

$$k = 1 \rightarrow \text{ggT}(10,1) = 1 \checkmark$$

$$k = 2 \rightarrow \text{ggT}(10,2) = 2 X$$

$$k = 3 \rightarrow \text{ggT}(10,3) = 1 \checkmark$$

$$k = 4 \rightarrow \text{ggT}(10,4) = 2 X$$

$$k = 5 \rightarrow \text{ggT}(10,5) = 5 X$$

$$k = 6 \rightarrow \text{ggT}(10,6) = 2 X$$

$$k = 7 \rightarrow \text{ggT}(10,7) = 1 \checkmark$$

$$k = 8 \rightarrow \text{ggT}(10,8) = 2 X$$

$$k = 9 \rightarrow \text{ggT}(10,9) = 1 \checkmark$$

Das heißt, die Menge $\mathbb{Z}_n^*$ besteht aus $\{1,3,7,9\}$. (Die Kardinalität von $\mathbb{Z}_n^*$ kann mit der eulerschen ϕ-Funktion (vgl. ↗ *Die eulersche ϕ-Funktion* (5.28.1)) ermittelt werden.)

Das Multiplikativ-Inverse von $a \in \mathbb{Z}_n^*$ bedeutet, dass man das $a \circ a^{-1} = a^{-1} \circ a = e$ (mit e als neutralem Element, z. B. für $\circ \rightarrow \cdot \Rightarrow e = 1$).

Die Frage, welches a^{-1} für a ein Multiplikativ-Inverses in $\mathbb{Z}_n^*$ ist, lässt sich umschreiben als folgende Frage: Welche Zahl muss für b eingesetzt werden, damit $a, b \in \mathbb{Z}_n^* : (b \cdot a \equiv 1 \mod n)$?

Nehmen wir das Beispiel $\mathbb{Z}_{10}^*$, dessen Menge wir oben über den ggT definiert haben und das Beispielelement 3. Welches $b \in \mathbb{Z}_{10}^*$ müssen wir wählen, damit $b \cdot 3 \equiv 1 \mod 10$?

Probieren wir einige Zahlen durch.

n	a	b	$a \cdot b = m$	$m \equiv n \mod 10$
10	3	1	$3 \cdot 1 = 3$	$3 \equiv \underline{3} \mod 10$ X
10	3	2	$3 \cdot 2 = 6$	$6 \equiv \underline{6} \mod 10$ X
10	3	3	$3 \cdot 3 = 9$	$9 \equiv \underline{9} \mod 10$ X
10	3	4	$3 \cdot 4 = 12$	$12 \equiv \underline{2} \mod 10$ X
10	3	5	$3 \cdot 5 = 15$	$15 \equiv \underline{5} \mod 10$ X
10	3	6	$3 \cdot 6 = 18$	$18 \equiv \underline{8} \mod 10$ X
10	3	7	$3 \cdot 7 = 21$	$21 \equiv \underline{1} \mod 10$ ✓
10	3	8	$3 \cdot 8 = 24$	$24 \equiv \underline{4} \mod 10$ X
10	3	9	$3 \cdot 9 = 27$	$27 \equiv \underline{7} \mod 10$ X
10	3	10	$3 \cdot 10 = 30$	$30 \equiv \underline{0} \mod 10$ X
10	3	11	$3 \cdot 11 = 33$	$33 \equiv \underline{3} \mod 10$ X
10	3	12	$3 \cdot 12 = 36$	$36 \equiv \underline{6} \mod 10$ X
10	3	13	$3 \cdot 13 = 39$	$39 \equiv \underline{9} \mod 10$ X
10	3	14	$3 \cdot 14 = 42$	$42 \equiv \underline{2} \mod 10$ X
10	3	15	$3 \cdot 15 = 45$	$45 \equiv \underline{5} \mod 10$ X
10	3	16	$3 \cdot 16 = 48$	$48 \equiv \underline{8} \mod 10$ X
10	3	17	$3 \cdot 17 = 51$	$51 \equiv \underline{1} \mod 10$ ✓
…	…	…	…	…
10	3	27	$3 \cdot 27 = 81$	$81 \equiv \underline{1} \mod 10$ ✓
…	…	…	…	…
10	3	37	$3 \cdot 27 = 111$	$111 \equiv \underline{1} \mod 10$ ✓

Wir sehen, dass das eine zyklische Gruppe ist, denn es gibt mehrere multiplikative Inverse für $a = 3$ (nämlich $R = \{7, 17, 27, 37, \ldots, (k \cdot n) + 7\}$), für die gilt: $a \in \mathbb{Z}_n^*, b \in R : a \cdot b = 1$.

Wir können das generalisieren zu $kn + 7$ mit $k \in \mathbb{N}$, da $7 \cdot 3 = 21$ und kn durch das Modulo n jeweils ›wegfällt‹. Auch die 21 fällt jeweils weg und wird zu einer 1, denn $21 \equiv 1 \mod 10$. Daher sind alle Zahlen $kn + 7$ multiplikative Inverse von 3 in $\mathbb{Z}_{10}^*$.

5.28.1 Die eulersche ϕ-Funktion

Die eulersche ϕ-Funktion gibt für jedes $n \in \mathbb{N}$ an, wie viele teilerfremde natürliche Zahlen kleiner n es gibt. Ihre Definition lautet:

$$\phi(n) := \left| \{ a \in \mathbb{N} \mid (1 \leq a \leq n) \wedge \mathrm{ggT}(a, n) = 1 \} \right|. \tag{78}$$

Beispiel. $n = 10$.

a	ggT$(10,a)$	Ist in Menge?
0	10	X
1	1	✓
2	2	X
3	1	✓
4	2	X
5	5	X
6	2	X
7	1	✓
8	2	X
9	1	✓
10	10	X

Die Menge der Zahlen kleiner $n = 10$, die den ggT$(n,a) = 1$ haben und kleiner sind als n beinhaltet also: $\{1,3,7,9\}$. Ihre Kardinalität ist 4. Das heißt $\phi(10) = 4$.

Für Primzahlen p gilt[5]:

$$\phi(p) = p - 1. \tag{79}$$

Daher kann man von jeder Zahl auch ihre Primfaktorzerlegung eingeben, so dass:

$$\phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1). \tag{80}$$

5.29 Homomorphieregel

Die Homomorphieregel besagt:

$$\forall a, b, c \in \mathbb{N}: \tag{81}$$

$$a + b \mod c = (a \mod n) + (b \mod n), \tag{82}$$

$$(a \cdot b) \mod n = (a \mod n) \cdot (b \mod n). \tag{83}$$

5.30 Al-Kashi

Das Theorem von Al-Kashi erlaubt die Modulo-Rechnung in einem Restklassenring erheblich zu beschleunigen, indem man die Quadrieren-und-Multiplizieren-Methode (vgl. ↗ *Schnelles Berechnen großer ganzzahliger Potenzen per binärer Exponentiation* (5.19)) anwendet und nach jedem Zwischenschritt wieder Modulo nimmt. Damit explodieren die Zahlengrößen nicht ins unermessliche.

Das Gesetz, das erlaubt, nach jeder Zwischenrechnung Modulo zu nehmen, heißt ›Homomorphieregel‹ (vgl. ↗ *Homomorphieregel* (5.29)).

[5] Das gilt, weil alle Elemente, die in $\mathbb{N}_p$ sind, keinen gemeinsamen Teiler mit p haben, d. h. $\forall k \in \{1,2,3,\ldots,p-1\}$: ggT$(p,k) = 1$ und sie sind damit Element der Gruppenmenge $\mathbb{N}_p$, woraus folgt, dass $|\mathbb{N}_p| = \phi(p) = p - 1$.

5.31 Chinesischer Restsatz

⚠!!!TODO!!!⚠ Chinesischer Restsatz

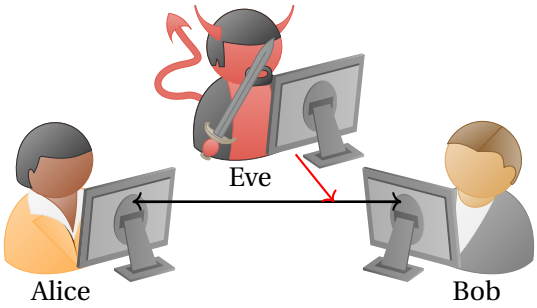
5.32 Verschlüsselung

Verschlüsselungssysteme bieten eine Möglichkeit, Informationen geheimzuhalten und trotzdem gleichzeitig über öffentliche Netze zu übertragen, so dass jeder die übertragenen Daten mitlesen, aber nur die gewünschten Personen diese Daten entschlüsseln können.

5.32.1 Diffie-Hellman

Mit Diffie-Hellman kann man über einen öffentlichen Kanal einen privaten Schlüssel austauschen, ohne dass andere als Sender und Empfänger die Möglichkeit haben, diesen Schlüssel abzugreifen.

Stellen wir uns die Situation vor, dass Alice Bob ein Geheimnis mitteilen will, während Eve jede Kommunikation zwischen Beiden mithören kann.



Dazu einigen Alice und Bob sich zuerst öffentlich auf eine große Primzahl p und eine Zahl $g \in \mathbb{N}$, für die gilt: $g < p$. g ist dabei ein Erzeuger der zyklischen Gruppe $\mathbb{Z}_p$ (vgl. ↗ *Spezialfall: Zyklische Gruppen* (5.23.3)).

Dann erzeugen Alice und Bob je eine zufällige Zahl zwischen 1 und $p-1$, die sie für sich behalten. Alice behält die Zahl a für sich und Bob die Zahl b.

Nun berechnet Alice mit ihrer geheimen Zahl einen öffentlichen Schlüssel:

$$A = g^a \mod p. \tag{84}$$

Sie schickt nun dieses A über den unsicheren Kommunikationskanal an Bob. Bob berechnet mit seiner geheimen Zahl auch einen öffentlichen Schlüssel:

$$B = g^b \mod p, \tag{85}$$

und schickt diesen an Alice.

Nun kennen Alice und Bob jeweils A und B. Mit dem privaten Schlüssel a berechnet Alice nun $K_1 = B^a \mod p$. Bob berechnet widerrum $K_2 = A^b \mod p$. Dabei gilt: $K_1 = K_2$. Dieses K ist für Eve nicht berechenbar, denn Eve kennt die geheimen Schlüssel der Beiden nicht. Nun können Alice und Bob K als gemeinsamen Schlüssel für einen verschlüsselten Kommunikationskanal verwenden, an den Even nicht herankommt.

5.32.2 RSA

RSA ist ein assymetrisches Verschlüsselungssystem, das heißt, es benutzt einen öffentlichen und einen privaten Schlüssel.

Zuerst generiert man einen Schlüssel.

1. Wähle zwei zufällige Primzahlen p, q, so dass $p \neq q$. p und q müssen geheim bleiben.
2. Berechne $N = pq$.
3. Berechne die eulersche ϕ-Funktion von N: $\phi(N) = (p-1) \cdot (q-1)$ (vgl. dazu die ↗ *Die eulersche ϕ-Funktion* (5.28.1))
4. Wähle eine Zahl e, die teilerfremd zu $\phi(N)$ ist und für die gilt, dass $1 < e < \phi(N)$.
5. Berechne d, so dass $e \cdot d \equiv 1 \mod \phi(N)$.
6. Der berechnete Schlüssel ist das Zahlenpaar (e, d, N).

Um nun damit Nachrichten zu verschlüsseln, berechnet man

$$c \equiv m^e \mod N. \tag{86}$$

c ist nun die verschlüsselte Nachricht. Um c wieder zu entschlüsseln berechnet man

$$m \equiv c^d \mod N \tag{87}$$

und erhält die Ursprungsnachricht zurück.

5.33 Graphentheorie

Graphen sind eine sehr praktische Möglichkeit, eine sehr große Menge an Sachverhalten zu modellieren. Als Beispiele kann man Abhängigkeiten in Modulsystemen anführen oder Navigationssysteme.

Ein Graph besteht aus Knoten (Edges) und Kanten (Vertices). Eine Knote kann z. B. ein Ort sein, eine Kante die Straße, die zu ihm führt.

Mathematisch lässt sich dieser Graph darstellen durch zwei Mengen, die Menge der Knoten $V = \{1,2,3,4,5\}$ und die Menge der Kanten, die sich je durch eine Menge definieren, die bestimmt, welche Kanten verbunden sind: $E = \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,1\}\}$.

Für die Notation der Kanten wurde dieser Formalismus eingeführt: $\binom{V}{2}$ verweist auf die zweielementigen Mengen der Potenzmenge von V. Zweielementig, weil immer zwischen

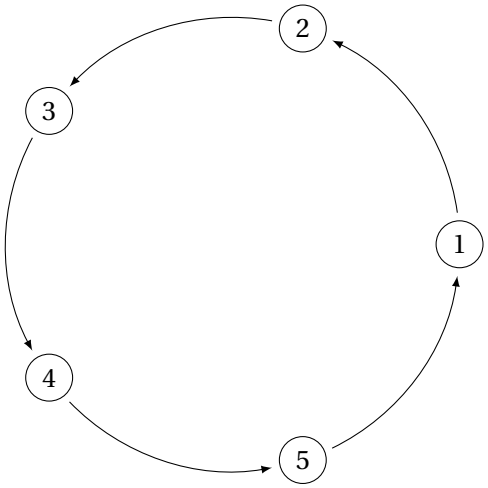


Abbildung 2: Ein einfacher gerichteter zyklischer Graph (Kreis) mit 5 Knoten und 4 Kanten.

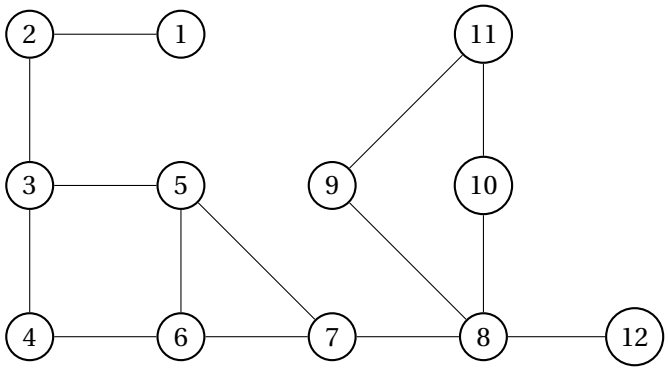


Abbildung 3: Ein komplexerer Beispielgraph

exakt zwei Knoten eine Kante geschlossen wird. Für vollständig-verbundene Graphen gilt: $E = \binom{V}{2}$, denn dort sind alle Knoten mit allen anderen verbunden. Für nicht-vollständig-verbundene Graphen gilt, dass $E \subset \binom{V}{2}$ ist.

5.33.1 Grad eines Knoten

Der Grad eines Knoten bestimmt sich durch die ein- und ausgehenden Kanten, die an diesem Knoten anliegen.

5.33.2 Subgraphen

Ein Subgraph H eines Graphen G ist ein Graph, so dass gilt, dass alle Elemente von H_E und H_V je Elemente von G_E respektive G_V sind.

Ein induzierter Subgraph entsteht, wenn man aus G Knoten löscht, oder formal:

$$\underbrace{V(H) \subseteq V(G)}_{\substack{\text{Die Knoten von } H \\ \text{sind eine Untermenge} \\ \text{der Knoten von } G}} \quad \wedge \quad \underbrace{E(H) = E(G) \cap \binom{V(H)}{2}}_{\substack{\text{Die Kanten von } H \\ \text{sind die Kanten von } G \\ \text{abzüglich der zweielementigen} \\ \text{Untermengen der Kanten von } H}} \quad . \tag{88}$$

Das heißt, man nimmt die Knoten des Originalgraphen und kann einige entfernen (muss aber nicht). Aus der formalen Definition folgt, dass in H keine neuen Knoten oder Kanten existieren dürfen, die nicht bereits in G sind.

5.33.3 Homomorphismus und Isomorphismus

Seien G und H zwei Graphen.

Homomorphismus Als Homomorphismus bezeichnet man eine Abbildung ϕ von $E(G)$ nach $E(H)$ und $V(G)$ nach $V(H)$, so dass

$$\forall \{x, y\} \in E(G) : \forall \{a, b\} \in E(H) : \left(\{\phi_V(x, y)\} = \{\phi_V(a, b)\}\right) \in E(H) \tag{89}$$

gilt.

Isomorphismus Wenn die Abbildungen

$$\forall x \in G : \forall y \in H : \phi(x) = \phi(y) \tag{90}$$

und

$$\forall \{x, y\} \in E(G) : \forall \{a, b\} \in E(H) : \phi_V\left(\{x, y\}\right) \wedge \phi_V\left(\{x, y\}\right) \tag{91}$$

bijektiv sind (d. h. eine 1:1-Korrespondenz zwischen Kanten und Knoten erstellt werden kann), dann sind G isomorph. Das heißt im Praktischen: G und H sehen, trotz unterschiedlicher Benennung, ›gleich aus‹. Wir schreiben: $G \cong H$.

5.33.4 Bäume

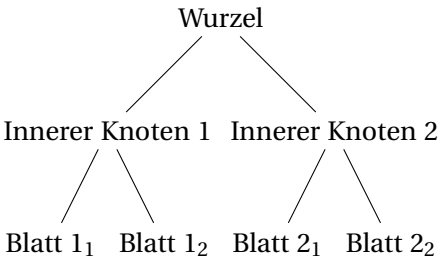


Abbildung 4: Ein Baum.

Bäume sind zusammenhängende Graphen, die nach Löschen einer Kante nicht mehr zusammenhängend sind. Daraus folgt, dass Bäume keine geschlossenen Pfade haben.

Eine Ansammlung von nicht-zusammenhängenden Bäumen heißt Wald.

5.33.5 Kreise

Kreise sind Graphen der Form $G = (V, E)$, so, dass $E \subset \binom{V}{2}$ und eine fortlaufende Verbindung zwischen den Kanten möglich ist, d. h. z. B.: $E = \{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}, \{v_n, v_1\}\}$. Löscht man aus einem Kreis einen beliebigen Knoten entsteht ein Baum.

5.33.6 Zusammenhang

Ein Graph ist dann zusammenhängend, wenn man von jedem Knoten über die Kanten zu jedem beliebigen anderen Knoten gelangen kann.

5.33.7 k-Zusammenhang

Ein Graph ist dann k-zusammenhängend, wenn man aus ihm beliebige $k-1$ einzelnen Knoten streichen und trotzdem über die gegebenen Kanten noch zu allen anderen Knoten des Graphen kommen kann. Wenn man dadurch den Zusammenhang zerstört, ist der Graph nur zusammenhängend, aber nicht k-zusammenhängend.

5.33.8 Satz von Menger

Der Satz von Menger ist eine Generalisierung, denn er nimmt nicht nur Pfade zwischen zwei Punkten $v, w \in E$, sondern er beschreibt Pfade zwischen zwei Zielregionen $A, B \in V$, die je aus mehreren (nicht notwendigerweise disjunkten) Punkten bestehen.

Die minimale Menge an Knoten, die auf den Pfaden von A nach B liegt, heißt $\kappa(A, B)$. Der Graph ist genau dann k-zusammenhängend, wenn es für jedes Knotenpaar in A mindestens k disjunkte Pfade zu den Knotenelementen in B gibt.

5.33.9 Disjunkte und unabhängige Pfade

Pfade heißen disjunkt, wenn sie keine gleichen Knoten ansteuern, d. h. wenn $P_1 = \{\{v_n, v_{n+1}\}, \ldots, \{v_{n+i}, v_{n+i+1}\}\}$ und $P_2 = \{\{v_a, v_{a+1}\}, \ldots, \{v_{a+j}, v_{a+j+1}\}\}$ und $P_1 \cup P_2 = \emptyset$.

Pfade heißen unabhängig, wenn

$$P_1 = \{\{v_1, v_2\}, \ldots, \{v_{n-1}, v_n\}\} \tag{92}$$

und

$$P_1 = \{\{u_1, u_2\}, \ldots, \{u_{m-1}, v_m\}\} \tag{93}$$

mit

$$a = v_1 = u_1 \tag{94}$$

und

$$b = v_n = u_m \tag{95}$$

(gleicher Start- und Endpunkt), wenn $P_1 \cap P_2 = \{a, b\}$.

5.33.10 Ohrendekomposition

Bei der Ohrendekomposition hängt man an zwei verschiedene Kanten eines Graphen einen Pfad an, der die beiden Kanten verbindet. Dieser Pfad ergibt ein angehängtes ›Ohr‹.

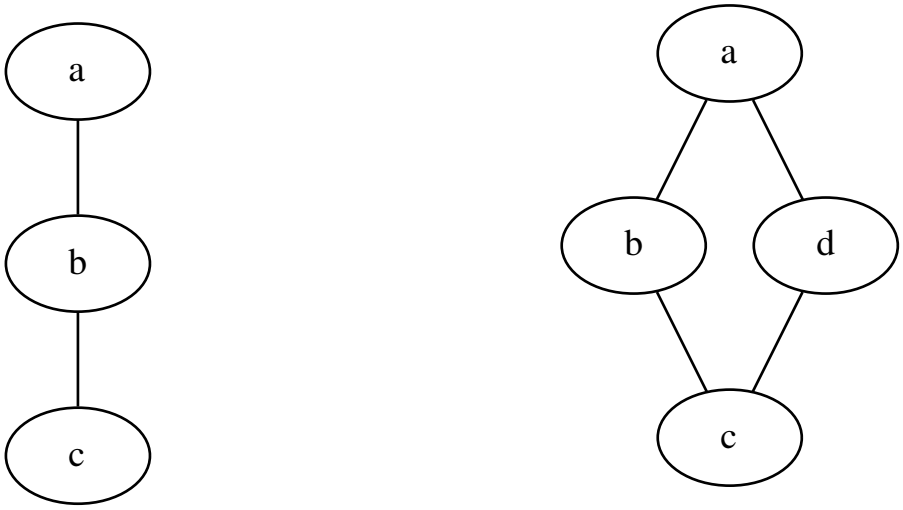


Abbildung 5: Links: Der Graph $G = (\{a,b,c\},\{\{a,b\},\{b,c\}\})$. Rechts: Der Graph $G = (\{a,b,c\},\{\{a,b\},\{b,c\},\{a,d\},\{d,c\}\})$.

Durch das Anfügen solcher ›Ohren‹ kann man einen n-zusammenhängenden Graphen $n+1$-zusammenhängend machen, denn es werden weitere Verbindungen angehängt, die man erst wieder entfernen müsste, um den Graphen in seine Komponenten zerlegen zu können.

5.33.11 Eulersche Graphen

Ein Graph heißt Eulergraph, wenn es möglich ist, jeden Knoten ihn ihm abzuschreiten, ohne einen einzigen Knoten mehrfach zu betreten. Der beschrittene Weg heißt ›Eulerzug‹. Ein Eulerzug heißt offener Eulerzug, wenn man nicht wieder zum Anfangsknoten zurückkehren kann und geschlossen, wenn man das kann (d. h. geschlossen ist er, wenn $E = \{\{v_1,v_2\},\{v_2,v_3\},\ldots,\{v_{n-1},v_n\},\{v_n,v_1\}\}$).

Ein Graph G hat genau dann einen Eulerzug, wenn er

(a) G zusammenhängend ist und

(b) jeder Knoten einen geraden Grad hat, d. h. es eine gerade Anzahl an eingehenden Kanten für jeden Knoten gibt.

5.33.12 Maximale Blöcke

Maximal-zusammenhängende Blöcke sind maximal-große Subgraphen, die zweizusammenhängend sind und keine Gelenkpunkte haben.

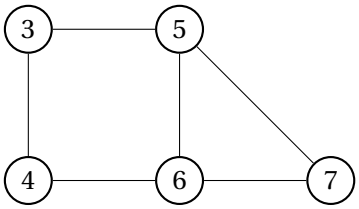
Hier alle Blöcke aus dem Graphen 3:

$E = \{1\}, V = \emptyset$

$E = \{1,2\}, V = \{\{1,2\}\}$

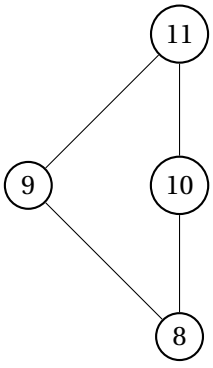
$E = \{2,3\}$

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



$E = \{3,4,5,6,7\}$

$V = \{\{3,4\},\{3,5\},\{5,6\},\{5,7\},\{4,6\},\{6,7\}\}$



$E = \{8,9,10,11\}$

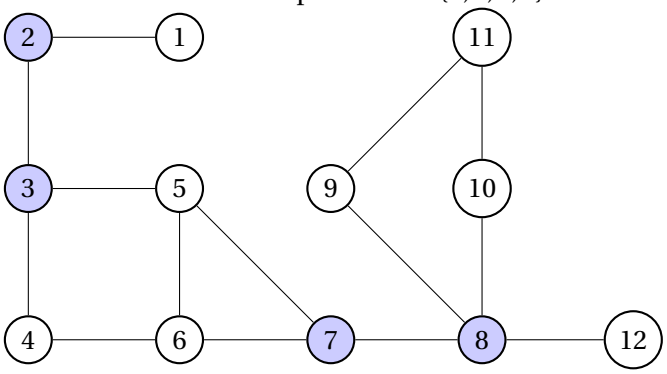
$V = \{\{8,9\},\{8,10\},\{9,11\},\{10,11\}\}$

Aus allen diesen Subgraphen könnte man einen beliebigen Knoten entfernen und trotz-

dem noch all seine Knoten über die Kantenpfade erreichen.

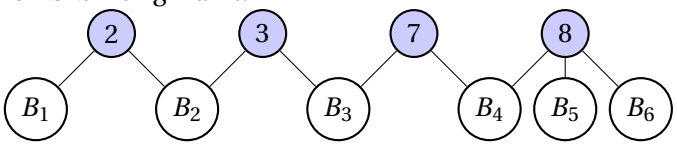
5.33.13 Gelenkpunkte

Ein Gelenkpunkt ist derjenige Punkt, an dem ein Block endet und ein neuer anfängt. In der Grafik 3 sind diese Gelenkpunkte $G = \{2, 3, 7, 8\}$.



5.33.14 Blockgraphen

Zur Erstellung eines Blockgraphen nimmt man die (eingefärbten) Gelenkpunkte und verkürzt die Darstellung insofern, als dass man für alle Untergraphen, die Blöcke bilden, nur ihre Abkürzung wählt.



$$V = \left\{ \underbrace{2,3,7,8}_{\text{Gelenkpunkte}} , \underbrace{B_1, B_2, B_3, B_4, B_5, B_6}_{\text{Blöcke von } G} \right\} \tag{96}$$

$$E = \{\{2, B_1\}, \{2, B_2\}, \{3, B_2\}, \{3, B_3\}, \{7, B_3\}, \{7, B_4\}, \{8, B_4\}, \{8, B_5\}, \{8, B_6\}\} \tag{97}$$

Wenn ein Graph zusammenhängend ist, dann ist auch sein Blockgraph zusammenhängend.

5.33.15 Wege

Wege von einem Knoten über einen anderen können dargestellt werden als Tupel $(v_1, v_2, \ldots, v_{n-1}, v_n)$. Das ist im Prinzip eine Kurzform für: $\{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}\}$.

5.33.16 Zusammenhangskomponente

Die Zusammenhangskomponente bezeichnet einen maximal-großen zusammenhängenden ↗ *Subgraphen* (5.33.2).

5.33.17 Brücken

Eine Brücke ist eine Kante zwischen zwei Blöcken insofern, als dass, wenn man diese Kante streicht, diese Blöcke nicht mehr zusammenhängend sind. Wenn man eine Brücke entfernt, wird die ↗ *Zusammenhangskomponente* (5.33.16) erhöht.

5.33.18 Kantengraphen

Ein Kantengraph $L(G)$ von G entsteht durch das Vertauschen von Knoten und Kanten.

Sei $G = (V, E)$ ein Graph. Dann besteht der Kantengraph G' von G aus den Knoten $V' = E(G)$ und den Kanten $E' = \{\{e_1, e_2\} | e_1 \cap e_2 \neq \emptyset\}$ (mit $e_1, e_2 \in V$). Das heißt, zwischen den neuen Knoten (die aus einer Kante bestehen) existiert dann eine Verbindung, wenn die beiden Kanten vorher einen gemeinsamen Knoten hatten.

Beispiel.

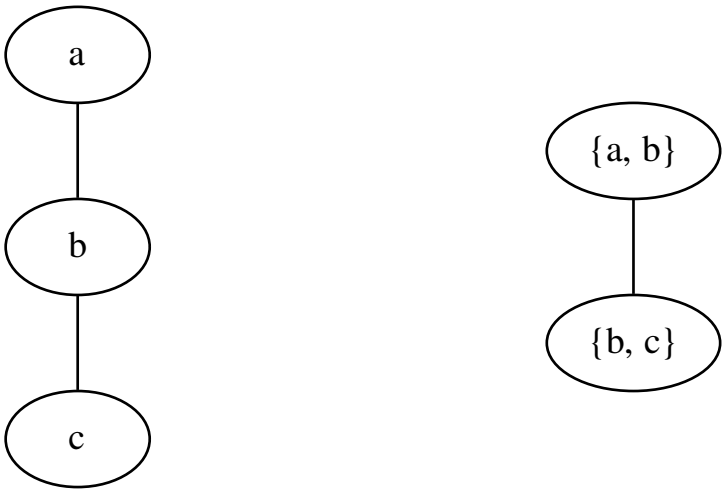
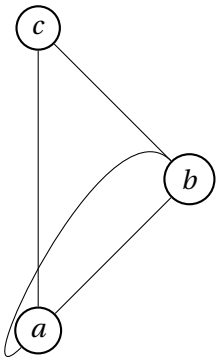


Abbildung 6: Links: Der Graph $G = (\{a, b, c\}, \{\{a, b\}, \{b, c\}\})$. Rechts: Der Kantengraph von G: $G' = (\{\{a, b\}, \{b, c\}\}, \{\{\{a, b\}, \{b, c\}\}\})$.

5.33.19 Multigraphen

Multigraphen sind Graphen, in denen zwischen zwei Punkten mehrere Kanten bestehen können.
Ein beispielhafter Multigraph ist der links angebildete. In diesem sind zwischen a und b zwei Verbindungen.



5.33.20 Kantenkontraktion

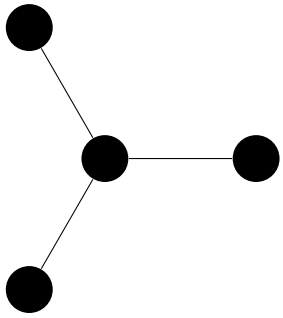
Bei einer Kantenkontraktion wird eine Kante zwischen zwei Knoten entfernt und die beiden Knoten zu einem Knoten zusammengefasst.

Als Notation wurde eingeführt: G/e, wobei e eine Kante ist, die zwei Knoten $a, b \in E(G)$ verbindet ($e = (a,b), e \in V(G)$).

5.33.21 Gradmatrix

Die Gradmatrix eines Graphen besteht aus Einträgen in der Hauptdiagonale, die je den Grad des Knoten bestimmen. Betrachten wir dazu den Stern S_4 auf der linken Seite.
Dieser besitzt die Gradmatrix:

$$G = \begin{array}{c|c} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \hline \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \tag{98}$$



S_3

Knoten 1 ist das Zentrum des Sterns.

5.33.22 Adjazenzmatrix

Die Adjazenzmatrix ist eine Möglichkeit, lineare Algebra und Graphentheorie zu verbinden. In einer solchen Adjazenzmatrix stellt man eine Tabelle auf, die alle Knoten $V(G)$ beinhaltet

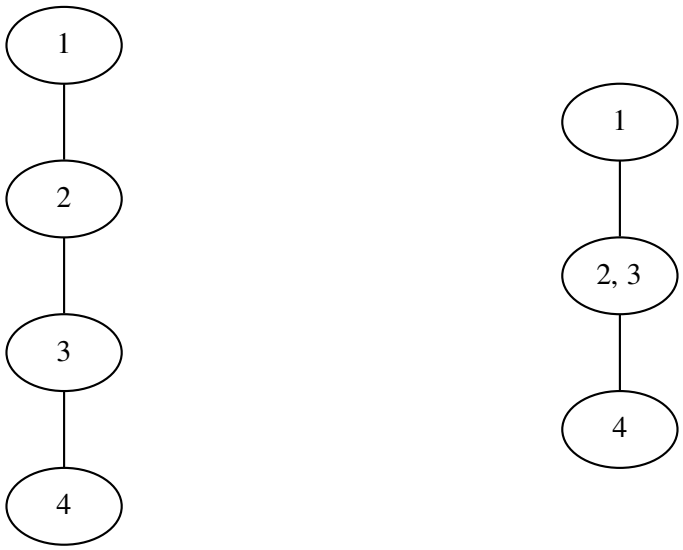


Abbildung 7: Links: Der Graph $G = (\{1,2,3,4\},\{\{\{1,2\}\},\{\{2,3\}\},\{\{3,4\}\}\})$. Rechts der kantenkontraktierte Graph $G' = (\{1,\rangle 2,3\langle,4\}\,\{\{\{1,\rangle 2,3\langle\}\},\{\{\rangle 2,3\langle,4\}\}\})$.

und setzt den Wert an der (x,y)-Spalte auf 1, wenn die Knoten eine gemeinsame Kante $(((x_1,x_2) \in V(G)) \wedge ((x_1,x_2) \in E(G) \longrightarrow 1))$ haben und auf 0, wenn nicht.

$$\begin{array}{c|c} & \begin{array}{ccc} a & b & c \end{array} \\ \hline \begin{array}{c} a \\ b \\ c \end{array} & \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array} \tag{99}$$

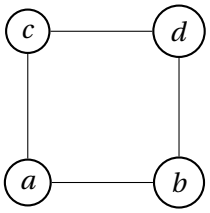
5.33.23 Cliquen

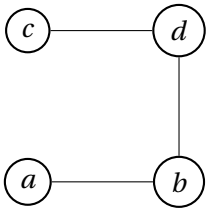
Sei $G = (V,E)$ ein Graph. Dann ist U eine Clique, wenn U eine Untermenge von V ist und alle Kanten von U untereinander verbunden sind. Eine Clique heißt dann *maximale Clique*, wenn man keine weiteren Kanten zu ihr hinzufügen kann und es trotzdem eine Clique bleibt.

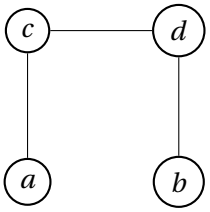
5.33.24 Spannbäume

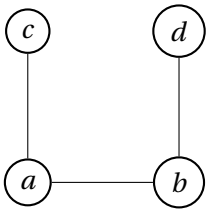
Spannbäume — auch: Gerüst — sind Subgraphen, die ein Baum sind und alle Knoten des Graphen enthalten (d. h. es werden nur Kanten entfernt).

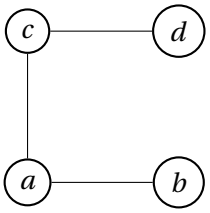
Spannbäume von $G = \{\{a,b,c,d\},\{\{a,c\},\{b,a\},\{c,d\},\{d,b\}\}\}$.







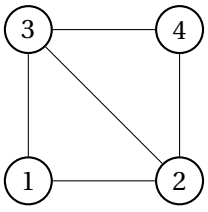




5.33.25 Satz von Kirchhoff

Die Anzahl der Spannbäume eines Graphen kann mit dem Satz von Kirchhoff bestimmt werden über die Determinante der *Adjazenzmatrix* (5.33.22) des Graphen.

Nehmen wir den Graphen $G = (\{1,2,3,4\}, \{\{1,2\}, \{1,3\}, \{3,4\}, \{2,3\}, \{2,4\}\})$ als Beispiel.



Erzeugen wir als erstes die Adjazenzmatrix

$$A = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 & 1 \\ 3 & 1 & 1 & 0 & 1 \\ 4 & 0 & 1 & 1 & 0 \end{array}. \tag{100}$$

Nun bestimmen wir die *Gradmatrix* (5.33.21):

$$B = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 2 & 0 & 0 & 0 \\ 2 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 \\ 4 & 0 & 0 & 0 & 2 \end{array}. \tag{101}$$

Daraus lässt sich die sogenannte Laplace-Matrix berechnen:

$$L = B - A \tag{102}$$

$$L = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}. \tag{103}$$

Aus dieser Matrix lassen sich nun je eine beliebige Zeile und Spalte löschen, z. B.

$$L* = \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 2 \end{pmatrix}. \tag{104}$$

Von dieser Matrix können wir nun die ↗ *Determinante* (6.2.5) bilden:

$$\det \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 2 \end{pmatrix} = 8. \tag{105}$$

Wir erhalten 8, und 8 ist die Anzahl der Spannbäume des Graphen G.

5.33.26 Satz von Cayley

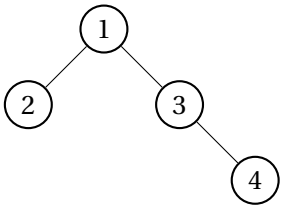
Der Satz von Cayley besagt, dass es n^{n-2} verschiedene bezeichnete Bäume mit n Knoten gibt. Dies kann unter Anderem bewiesen werden durch die ↗ *Prüfer-Codes* (5.33.27).

5.33.27 Prüfer-Codes

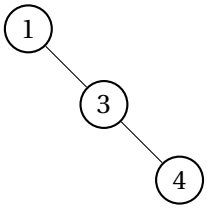
Prüfer-Codes sind eine Methode, einen Baum eineindeutig mit einer Ziffernfolge zu beschreiben. Das heißt, dass jeder Baum einen spezifischen Prüfer-Code hat und aus jedem Prüfer-Code ein spezifischer Baum wiederhergestellt werden kann. Der Prüfer-Code eines Baumes mit n Knoten hat $n-2$ Zeichen, was den ↗ *Satz von Cayley* (5.33.26) beweist.

Zum Erstellen des Prüfer-Codes wählt man sich einen beliebigen Baum und schaut sich die einzelnen Blätter an. Es wird das Blatt entfernt, das den geringsten Wert in der Beschriftung hat und in den Code der Wert des Knoten, an dem das Blatt hängt, geschrieben. Dies wird iterativ fortgeführt, bis nur noch zwei Knoten übrig sind.

Beispiel.

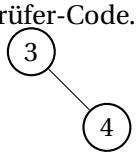


Die Blätter dieses Baumes sind 2,4. Das Blatt mit der geringsten Beschriftung ist die 2. Also entfernen wir die 2 und schreiben die 1, an der die 2 hängt, in den Prüfercode.



Prüfer-Code: 2.

Das nächstgeringste Blatt ist die 1, also entfernen wir die 1 und schreiben die 3 in den Prüfer-Code.



Prüfer-Code: 2,3.

Nun sind nur noch die Knoten 3,4 übrig. Das heißt, der Algorithmus terminiert hier und an den Prüfer-Code wird das leere Wort ϵ angehangen: $2,3,\epsilon$.

Zur Rekonstruktion braucht man nun die Knotenmenge, $E(G) = \{1,2,3,4\}$, und den Prüfer-Code.

⚠!!!TODO!!!⚠ Prüfer-Codes

5.33.28 Planare Graphen

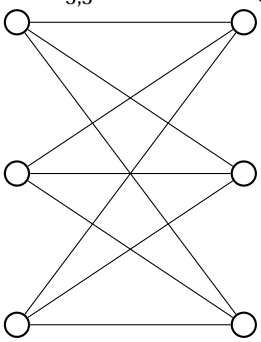
Ein planarer Graph ist ein Graph, der sich auf einer Ebene zeichnen lässt, ohne dass sich Kanten überschneiden. Ein Beispiel dafür ist (vereinfacht) das Straßennetz, solange Brücken und Tunnel nicht vorhanden sind. Ein anderes Beispiel wäre der Graph von Flüssen, wenn soetwas wie das Wasserstraßenkreuz Minden nicht berücksichtigt wird.

5.33.29 Minoren

Ein Graph H heißt Minor, wenn er aus dem Graphen G durch *Kantenkontraktion* (5.33.20) oder durch Weglassen von Kanten oder Knoten entsteht. Die Benennung von Kanten spielt hier keine Rolle, so dass H auch dann ein Minor von G ist, wenn die Kantenmengen beider Graphen disjunkt sind, sie sich aber isomorph verhalten.

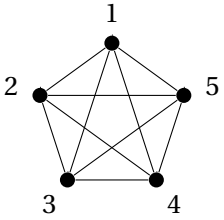
5.33.30 Satz von Kuratowski

Der Satz von Kuratowski besagt, dass ein Graph exakt dann planar ist, wenn er weder K_5 noch $K_{3,3}$ als Minoren (vgl. ↗ *Minoren* (5.33.29)) enthält



Der bipartite Graph (vgl. ↗ *Bipartite Graphen* (5.33.32)) $K_{3,3}$. Wenn durch Wegstreichung und Kantenkontraktion aus einem Graphen auf irgendeine Weise $K_{3,3}$ erzeugt werden kann, ist der Graph nicht planar.

Genauso verhält es sich mit dem Graphen K_5. Ist dieser irgendwie durch Kantenkontraktion oder Wegstreichung von Kanten oder Knoten aus einem Graphen G erzeugbar ist, dann ist G nicht planar.

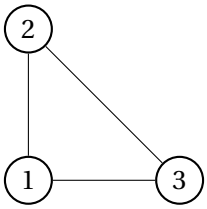


5.33.31 Eulerscher Polyedersatz

Der eulersche Polyedersatz besagt, dass bei zusammenhängenden planaren Graphen folgende Formel gilt:

$$|E(G)| - |V(G)| + f = 2 \tag{106}$$

Dabei beschreibt $|E(G)|$ die Anzahl der Knoten, $|V(G)|$ die Anzahl der Kanten und f die Anzahl der Fläche, die im Graph (inklusive der einheitlichen Fläche außerhalb des Graphen) entstehen.

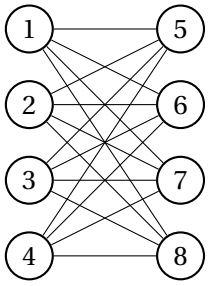


Es gibt in diesem Graph 3 Knoten ($|V(G) = 3$), 3 Kanten ($E(G) = 3$) und zwei Flächen ($f = 2$). Es gilt also:

$$\underbrace{\underbrace{3}_{|E(G)|} - \underbrace{3}_{|V(G)|}}_{=0} + \underbrace{2}_{f} = 2. \tag{107}$$

5.33.32 Bipartite Graphen

Ein Graph heißt ›bipartit‹, falls sich seine Knotenmengen aufteilen lassen in Partitionsklassen, so, dass zwischen den Knoten in den Partitionsklassen keine Verbindungen bestehen.



Im links gezeigten Graph entstehen zwei Partitionsklassen, nämlich $\{1,2,3,4\}$ und $\{5,6,7,8\}$, denn innerhalb dieser Partitionsklassen befinden sich keine Verbindungen.

5.34 Partitionen

Partitionierung einer Menge M bedeutet, dass man alle möglichen Untermengen bildet, die in-sich disjunkt sind (anders als die Potenzmengen, die nicht disjunkt sein müssen).

Gegeben sei die Menge $M = \{a, b, c\}$. Von dieser lassen sich nun $|M|$ Arten von Partitionen bilden.

- 1-Partitionen: $\{\{a, b, c\}\}$
- 2-Partitionen: $\{\{a\}, \{b, c\}\}$, $\{\{a, b\}, \{c\}\}$, $\{\{a, c\}, \{b\}\}$
- 3-Partitionen: $\{\{a, b, c\}\}$.

Graphisch kann man sich die Partitionierung vorstellen als Möglichkeit, eine Menge von n Elementen in verschiedene (einander nicht überlappende) Gruppen einzuordnen.

Die Anzahl an möglichen Partitionen einer Menge lässt sich über die bell'schen Zahlen bestimmen. Die bell'sche Zahl lässt sich rekursiv berechnen über

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k. \tag{108}$$

5.35 Relationen

Eine zweistellige Relation ist eine Menge R, die Untermenge des kartesischen Produktes von $A \times B$ ist. Das kartesische Produkt ist die Verbindung aller Elemente einer Menge mit den Elementen einer Anderen. Beispiel:

$$A = \{1,2,3\}, B = \{a,b,c\} \tag{109}$$

$$A \times B = \{\{a,1\},\{a,2\},\{a,3\},\{b,1\},\{b,2\},\{b,3\},\{c,1\},\{c,2\},\{c,3\}\} \tag{110}$$

R könnte z. B. in diesem Beispiel sein: $R = \{\{a,1\},\{b,2\},\{c,3\}\}$. Das würde bedeuten, dass a in Relation zu 1 steht, b in Relation zu 2 und c in Relation zu 3.

5.35.1 Äquivalenzrelationen

Eine Äquivalenzrelation besitzt drei Eigenschaften:

- Reflexivität
- Transitivität
- Symmetrie.

5.35.2 Eigenschaften von Relationen

Reflexivität Eine Relation R ist reflexiv, wenn gilt, dass $\forall x : xRx$. Gilt dies nicht, ist die Relation entweder irreflexiv (wenn $\forall x : \neg xRx$), oder besitzt keine Reflexivitätseigenschaften (wenn für einige Elemente xRx gilt, aber für andere nicht). Ein Beispiel für Reflexivität ist die Relation kleiner-gleich, denn $\vdash \forall n \in \mathbb{M} : n \leq n$.

Transitivität Eine Relation R ist transitiv, wenn gilt: $xRy \wedge yRz \implies xRz$. Das Gleichheitszeichen z. B. ist transitiv, denn es gilt: $x = y \wedge y = z \implies x = z$. Das Gegenteil von Transitivität ist die Intransitivität, diese findet man z. B. beim Schnick-Schnack-Schnuck-Spiel, denn a schlägt b (aRb), b schlägt c (bRc), aber a schlägt c nicht ($\not\vdash aRc$).

Symmetrie Eine Relation R ist symmetrisch, wenn $\forall x, y : xRy \longrightarrow yRx$. Beispiel für eine symmetrische Relation ist die Addition im Ring $(\mathbb{N}, \cdot, +)$: dort gilt $a + b = b + a$ ($aRb \Leftrightarrow bRa$).

5.35.3 Beispiel von Wikipedia

Die Wikipedia liefert ein gutes Beispiel für eine Äquivalenzrelation. Stellen wir uns eine Menge T vor, die Tiere auf einem Bauernhof beinhaltet. Wir definieren, dass $a, b, c \in T$ genau dann äquivalent sein sollen, wenn a und b derselben Tierart angehören. Sind jetzt a eine Kuh und b ein Bulle, dann sind a und b in einer Äquivalenzrelation, aber c — ein Hahn — ist es nicht. Es gilt:
$a \sim b \wedge a \not\sim c$.
Hier sind alle drei Eigenschaften erfüllt:

- Reflexivität: jedes Tier gehört zur selben Spezies wie es selbst

- Symmetrie: Seien x, y, z Tiere aus T, dann gilt: wenn $x \sim y$ und $y \sim z$, dann ist auch $x \sim z$[6]
- Transitivität: wenn $a, b \in T : a \sim b$ (a und b gehören zur selben Spezies) und $c \in T : a \sim c$, dann gilt auch, dass a und c in der selben Spezies sind.

Die Äquivalenzklassen bestehen in diesem Beispiel aus den Tieren je einer Art. Z. B. gehören Kuh und Bulle zur selben Äquivalenzklasse, Hahn und Huhn auch, aber Hahn und Huhn und Kuh und Bulle sind nicht die gleichen Äquivalenzklassen.

5.36 Ordnungen

5.36.1 Halbordnungen

Eine Halbordnung besteht auf einer Menge M, wenn für alle Elemente $x, y \in M$ gilt:

- xRx (Reflexivität),
- $xRy \wedge yRx \implies x = y$ (Antisymmetrie),
- $xRy \wedge yRz \implies xRz$ (Transitivität).

Beispiel für eine Halbordnung ist der Teilerverband einer Zahl. In diesem werden alle Teiler einer Zahl untereinander in Relation gesetzt. So sind die Teiler von $\mathcal{T}(60) = \{1, 2, 3, 4, 5, 6, 10, 15, 30, 20, 12, 60\}$ ein Teilerverband und eine Halbordnung, da für alle $x, y \in \mathcal{T}$ gilt:

- x ist Teiler von x (Reflexivität, jede natürliche Zahl teilt sich selbst),
- Wenn x y teilt und y x teilt, dann ist $x = y$ (Antisymmetrie)
- Wenn x y teilt und y z teilt, dann teilt auch x z (Transitivität)

5.36.2 Hasse-Diagramme

Hasse-Diagramme sind eine Möglichkeit, Halbordnungen mithilfe eines gerichteten Graphen darzustellen.

Das Hasse-Diagramm vom Teilerverband der Teiler von 70 (mit $\mathcal{T}(70) = \{1, 2, 5, 7, 10, 14, 35, 70\}$) sich darstellen als Graph (siehe dazu Abbildung 8).

Dabei werden zwei Knoten $a, b \in M$ verbunden, wenn gilt: aRb (d., h. wenn gilt, dass a, b transitiv, reflexiv und antisymmetrisch sind).

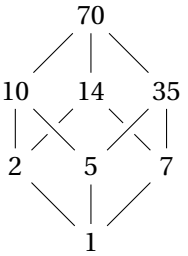


Abbildung 8: Hasse-Diagramm des Teilerverbandes von 70

[6] Biologisch sind z. B. Ringspezies hiervon ausgeschlossen, aber wir gehen davon aus, dass der Baum noch nicht genügend Zeit hatte, um ausreichend große evolutionäre Änderungen einzuführen.

In der Darstellung des Hasse-Diagramms werden die Schleifen, die sich aus der Reflexivität (aRa bzw. in der Teilbarkeitsrelation a teilt a, was für alle $a \in \mathbb{N}$ gilt) ergeben, weggelassen.

5.36.3 Quasiordnungen

Quasiordnungen sind reflexive und transitive Ordnungen, die aber nicht symmetrisch sein müssen (d. h. entweder symmetrisch, antisymmetrisch oder asymmetrisch). Jede Äquivalenzrelation ist eine Quasiordnung mit Symmetrie.

Für eine Quasiordnung von M gilt daher für alle $a, b, c \in M$:

- aRa (jedes Element steht mit sich selbst in der Relation R, Reflexivität)
- $aRb \wedge bRc \implies aRc$ (Transitivität)

Ein Beispiel für eine Quasiordnung ist die Relation der Teilbarkeit auf der Menge der natürlichen Zahlen, denn:

- Jede natürliche Zahl ist durch sich selbst teilbar (Reflexivität)
- Wenn eine natürliche Zahl a durch b teilbar ist, und b durch c, dann ist auch a durch c teilbar

6 Lineare Algebra

6.1 Komplexe Zahlen

Komplexe Zahlen ($\mathbb{C}$) erweitern die reellen Zahlen um die Möglichkeit, Gleichungen der Struktur $x^2 + 1 = 0$ zu lösen, indem sie definieren, dass $i = \sqrt{-1}$ und folglich $i^2 = -1$ zulässige Zahlen sind.

6.1.1 Division komplexer Zahlen

Für die Division durch komplexe Zahlen kann man einen Trick anwenden:

$$\frac{a}{1+i} = \frac{a}{1+i} \cdot \frac{1-i}{1-i} = \frac{a \cdot (1+i)}{(1-i)(1-i)} = \frac{a \cdot (1-i)}{2}. \tag{111}$$

Dabei bildet man die komplex-konjugierte komplexe Zahl (Vorzeichenwechsel beim Imaginäranteil) und multipliziert sie sowohl im Zähler als auch im Nenner an die Zahl. Das geht, weil sich dadurch die Relation nicht verändert (sie könnten ja jederzeit wieder rausgestrichen werden). Der Vorteil ist, dass man die imaginäre Zahl damit aus dem Nenner herauskriegen kann.

6.1.2 Addition in den komplexen Zahlen

Die Addition in $\mathbb{C}$ geschieht komponentenweise, d. h.

$$(a + bi) + (c + di) = (a + c) + ((b + d)i). \tag{112}$$

6.1.3 Gaußsche Zahlenebene

Anstatt sich – wie bei allen Zahlenklassen bis einschließlich $\mathbb{R}$ – die Zahlen als geordnet in einer Linie vorzustellen, bestimmen sich komplexe Zahlen durch ihre Position auf einer zweidimensionalen Fläche, der gauß'schen Zahlenebene.

Zahlen können hier über drei Schreibweise exakt verortet werden.

1. $a + bi$, als cartesische Koordinaten
2. $r \cdot e^{\phi}$, als Winkel ϕ, der sich gegen den Uhrzeigersinn von der Reellen Achse abhebt und einen Abstand von r hat,
3. Als Sinus-Cosinusdarstellung: $r(\cos(\phi) + i \cdot \sin(\phi)$

Wichtig zu merken ist für die letzten beiden Arten der Darstellung, dass π eine halbe Umdrehung ist, so dass 2π eine ganze ist und $\frac{\pi}{2}$ eine Viertelumdrehung. Darüber kann man oft optisch gut abschätzen, wo sich die Zahl befindet.

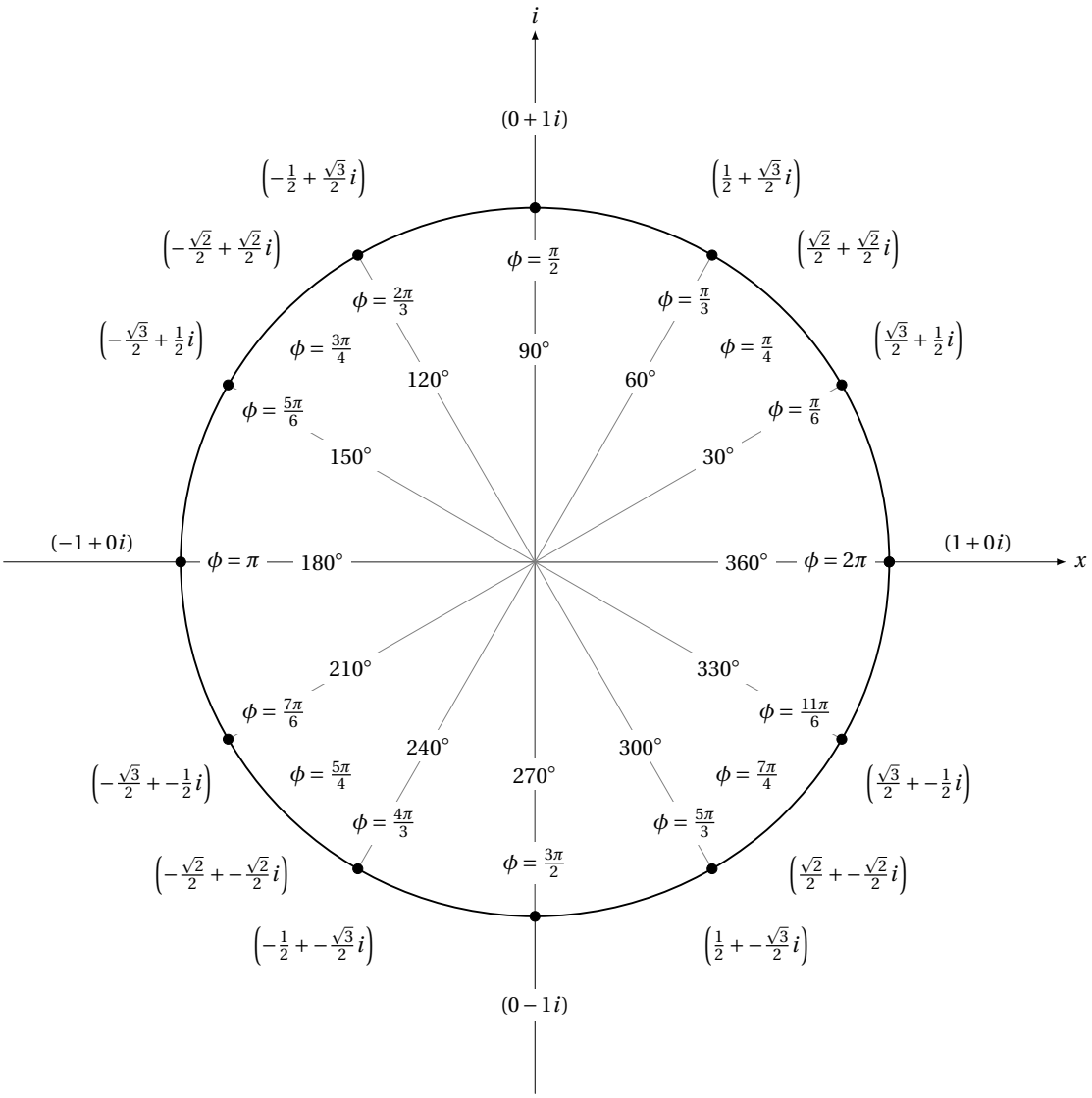


Abbildung 9: Der Einheitskreis und einige komplexe Zahlen auf ihm.

6.1.4 Umrechnen in andere Darstellungsformen

Für einige Operationen eignen sich andere Darstellungsformen einer komplexen Zahl besser als Andere. Daher kurz die Umrechnungsregeln:

Variablenname	Bedeutung
$\Im(z)$	Imaginäranteil von z (bei $z = 4 + 6i$ ist $\Im(z) = 6$)
$\Re(z)$	Realanteil von z (bei $z = 4 + 6i$ ist $\Re(z) = 4$)
r	Der Abstand zum Nullpunkt auf kürzestem Wege
ϕ	Der Winkel zur Achse der reellen Zahlen

$$r = |z| = \sqrt{a^2 + b^2} \tag{113}$$

$$\sin(\phi) = \frac{y}{r}, \cos(\phi) = \frac{x}{r} \tag{114}$$

Mithilfe des Arcus-Sinus oder Arcus-Cosinus können wir dann die Werte für ϕ bestimmen. Jedoch ist es sehr hilfreich, das geometrisch zu verstehen, denn häufig sind ϕ-Werte gebrochen-rationale oder ganzzahlige Vielfache von π (einer halben Drehung).

6.1.5 Multiplikation komplexer Zahlen

Wenn man zwei komplexe Zahlen multiplizieren will, z. B. $z_1 = 1 + 0i$ und $z_2 = 0 + 1i$, dann ist es einfacher, sie in die e-Funktionsschreibweise zu bringen.

$$z_1 = 1 + 0i = 1 \cdot e^{0 \cdot \phi \cdot i} = 1 \cdot e^{0 \cdot i} = 1 \tag{115}$$

$$z_2 = 0 + 1i = 1 \cdot e^{1 \cdot \frac{1}{2}\pi \cdot i} = e^{\frac{1}{2}\pi \cdot i} \tag{116}$$

Wir erhalten dann:

$$e^{0 \cdot i} \cdot e^{\frac{1}{2}\pi \cdot i} = e^{(0 \cdot i) + (\frac{1}{2}\pi \cdot i)} = e^{\frac{1}{2}\pi \cdot i} \tag{117}$$

Durch das $\frac{1}{2}\pi$ kriegen wir eine Viertelkreisdrehung und landen exakt auf i, ohne Stauchung oder Streckung durch Vorfaktoren. Daher ist $z_1 \cdot z_2 = i$.

6.1.6 Komplexe Potenzen

$$\begin{aligned} z &= re^{i\phi}, \\ z^n &= \left(re^{i\phi}\right)^n, \end{aligned} \tag{118}$$

dank ↗ *Warum ist* $(x^n)^m = (x^m)^n = x^{n \cdot m}$*?* (3.1.3) können wir schlussfolgern:

$$z^n = r^n \cdot e^{n \cdot i\phi}.$$

6.1.7 Komplexe Wurzeln

Komplexe Zahlen haben, im Gegensatz zu reellen, keine eineindeutige Wurzel mehr.

Wollen wir herausfinden, welche z eingesetzt werden können, damit $z^5 = 1$ ist (d. h. wir wollen wir fünfte Wurzel ziehen), dann müssen wir z erst in die eulersche Form umwandeln, i. e. $z = r \cdot e^{\phi \cdot i}$.

Für z^n sind die Wurzeln: $\sqrt[n]{r_0} \cdot e^{i \cdot \frac{\phi}{n} + \frac{2\pi}{n} \cdot k}$ für $k \in \{0, 1, 2, \ldots, n-1\}$.

6.2 Matrixrechnung

6.2.1 Standardskalarprodukt

Das Standardskalarprodukt von zwei Vektoren bestimmt sich aus der Summe der jeweiligen Zeilen, die multipliziert werden. Man kann schreiben:

$$A^{1\times m} \cdot B^{1\times m} = \sum_{i=1}^{m} A_i \cdot B_i. \tag{119}$$

Ein Beispiel:

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \cdot \begin{pmatrix} d \\ e \\ f \end{pmatrix} = ab + be + cf. \tag{120}$$

6.2.2 Skalarmultiplikation

Matrizen werden skalar multipliziert, indem der Vorfaktor (hier a) an jeden einzelnen Wert heranmultipliziert wird:

$$a \cdot \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix} = \begin{pmatrix} ax_1 & ay_1 & az_1 \\ ax_2 & ay_2 & az_2 \end{pmatrix}. \tag{121}$$

Diese Relation lässt sich auch umkehren, um Matrizen zu vereinfachen, indem man gemeinsame Vorfaktoren herauszieht.

6.2.3 Matrixmultiplikation

Matrixmultiplikation funktioniert nur bei einigen Matrizen. Dabei kann nur eine $n \times m$-Matrix mit einer $m \times n$-Matrix multipliziert werden. Die Matrixmultiplikation ist **nicht** kommutativ, d. h. im allgemeinen Fall: $A \times B \neq B \times A$.

Matrizen werden multipliziert durch einen ›Trick‹. Man stelle sich vor, man nehme sich die a-te Spalte aus der zweiten Matrix, kippe sie nach links zur Seite und lege sie über die b-te Spalte der ersten Matrix. Multipliziert man diese nun miteinander und komponiert sie per Addition, dann ergibt sich der Wert an Position (a, b) in der Ergebnismatrix.

Beispiel.

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \cdot \begin{pmatrix} h & i \\ j & k \\ l & m \end{pmatrix} = \begin{pmatrix} ah + bj + cl & ai + bk + cm \\ dh + ej + fl & di + ek + fm \end{pmatrix}. \tag{122}$$

6.2.4 Matrixaddition

Bei einer Matrixaddition werden einfach alle komponenten an den Positionen $\langle a, b\rangle$ in beiden Matrizen addiert. Dabei müssen die beiden Matrizen gleichen Types sein, d. h. $A^{n\times n} \wedge B^{n\times n}$.

Beispiel:

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} + \begin{pmatrix} h & i & j \\ k & l & m \end{pmatrix} = \begin{pmatrix} a+h & b+i & c+j \\ d+k & e+l & f+m \end{pmatrix} \tag{123}$$

6.2.5 Determinante

Die Determinante einer Matrix bestimmt im Zusammenhang mit der linearen Algebra die Flächen- bzw. Volumenveränderung einer Struktur, wenn man sie anhand dieser Matrix manipuliert.

Die Determinante der Matrix

$$A \in K^{2\times 2} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{124}$$

bestimmt sich als $ad - bc$.

Für quadratische Matrizen bis 3×3 lässt sich die Determinante durch die Regel von Sarrus bestimmen, in der man (wie in der Abbildung) pfeilweise multipliziert und dann die Produkte addiert bzw. subtrahiert.

$$\det(A) = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \left(\begin{array}{ccccc} a & b & c & a & b \\ d & e & f & d & e \\ g & h & i & g & h \\ & & + & + & + \end{array} \right) = aei + bfg + cdh - gec - hfa - idb. \tag{125}$$

Wenn die Determinante einer Matrix ungleich 0 ist, dann ist die Matrix invertierbar (vgl. ↗ *Invertieren einer Matrix* (6.2.10)).

Für größere quadratische Matrizen lässt sich die Determinante über den sogenannten ›Laplace'schen Entwicklungssatz‹ entwickeln.

Wir wählen dazu eine beliebige Zeile aus (im einfachsten Fall eine, in der möglichst viele Nullen vorkommen) und gehen sie elementweise durch. Die Zeile und Spalte, in der sie sich befindet, blenden wir in Gedanken aus, und berechnen aus den übriggebliebenen Spalten und Zeilen die Determinante. Diese multiplizieren wir nun mit dem Wert aus der ausgeblendeten Spalte und addieren sie alternierend (beginnend mit +). Das Ergebnis ist die Determinante der Matrix.

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \tag{126}$$

$$a \cdot \det \begin{pmatrix} \star & \star & \star \\ \star & e & f \\ \star & h & i \end{pmatrix} - b \cdot \det \begin{pmatrix} \star & \star & \star \\ d & \star & f \\ g & \star & i \end{pmatrix} + c \cdot \det \begin{pmatrix} \star & \star & \star \\ d & e & \star \\ g & h & \star \end{pmatrix} = \tag{127}$$

$$a \cdot \det\begin{pmatrix} e & f \\ h & i \end{pmatrix} - b \cdot \det\begin{pmatrix} d & f \\ g & i \end{pmatrix} + c \cdot \det\begin{pmatrix} d & e \\ g & h \end{pmatrix} = \tag{128}$$

$$a(ei - hf) - b(di - gf) + c(dh - ge) = aei - ahf - bdi + bgf + cdh - cge \tag{129}$$

Matrizen der Form $\mathbb{K}^{n \times n}$ können hiermit in Matrizen der Form $\mathbb{K}^{n-1 \times n-1}$ ›heruntergebrochen‹ werden. Damit lassen sich prinzipiell rekursiv alle quadratischen Matrizen determinieren, wenn man dieses Verfahren dann auf die $n-1 \times n-1$-Matrix anwendet, bis man viele kleine 2×2-Matrizen hat, die über die Formel $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - cb$ berechnet werden können.

6.2.6 Die Zeilenstufenform

Jede Matrix kann durch Operationen auf sie in die Zeilenstufenform überführt werden. Dazu sind zwei Begriffe relevant:

Begriff	Erklärung
Nullzeile	Eine Zeile, in der nur Nullen stehen
Zeilenführer	Erste Zahl in einer Zeile, die nicht 0 ist

Die Zeilenführer habe ich in dieser Beispielmatrix grün eingefärbt, die Nullzeilen rot.

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \tag{130}$$

Ziel ist es, dass der Zeilenführer von oben nach unten betrachtet von links nach rechts wandert und eine ›Treppe‹ entsteht[7]. Bei der Beispielmatrix erreicht man das mit

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\underline{\text{II}} \to \underline{\text{II}} - 2 \cdot \underline{\text{I}}} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \tag{131}$$

Legale Operationen sind dabei die Multiplikation mit Skalaren aus $\mathbb{R}$ und die Addition und Subtraktion von Zeilen aus der Matrix selbst miteinander (z. B. die Zweite Zeile von der ersten abziehen oder addieren, d. h. Komponente-für-Komponente durchgehen und voneinander abziehen oder addieren). Außerdem kann man die Zeilen beliebig vertauschen.

6.2.7 Lösung linearer Gleichungssysteme mit Matrizen

Ein lineares Gleichungssystem der Form

$$3x + 5y + z = 6 \tag{132}$$

$$12x + 5z - 7z = 5 \tag{133}$$

[7] Mir hat es geholfen zu erkennen, dass die Treppe von Rechts nach Links geht und nicht von Links nach Rechts.

$$-x+y-2z=-1 \tag{134}$$

kann mit einer erweiterten Koeffizientenmatrix dargestellt werden als:

$$\left(\begin{array}{ccc|c} 3 & 5 & 1 & 6 \\ 12 & 5 & -6 & 5 \\ -1 & 1 & -2 & -1 \end{array}\right)\begin{pmatrix} x \\ y \\ z \end{pmatrix}. \tag{135}$$

Dadurch, dass man die Zeilenvektoren miteinander multipliziert und addiert und skalar multipliziert, kann man, wenn das Gleichungssystem lösbar ist, eine Einsermatrix der Form

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \end{array}\right). \tag{136}$$

Dann steht dort quasi $x=a, y=b$ und $z=c$.

6.2.8 Matrixtransponierung

Beim Transponieren einer Matrix wird die erste Zeile zur ersten Spalte, die zweite Spalte zur zweiten Zeile usw.

Beispiel:

$$A^T=\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}^T=\begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}. \tag{137}$$

Allgemeine Rechenregeln:

$$(A^T)^T=A$$

$$A^T+B^T=(A+B)^T$$

$$(A\cdot B)^T=B^T\cdot A^T$$

6.2.9 Spur

Die Spur einer Matrix $K^{n\times n}$ ist die Summe ihrer Hauptdiagonalelemente.

Beispiel:

$$\text{Spur}\begin{pmatrix} a & b & c & d \\ e & f & h & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}=a+f+k+p. \tag{138}$$

Wenn die Spur einer Matrix 0 ist, dann gilt die Matrix als spurfrei.

Allgemein gilt:

- Die Spur einer Matrix ist gleich der Summe ihrer Eigenwerte.
- $\text{Spur}(A) = \text{Spur}(A^T)$

6.2.10 Invertieren einer Matrix

Eine Matrix multipliziert mit ihrem Inversen ergibt die Einheitsmatrix. Beispiel:

$$M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}, \tag{139}$$

$$M \cdot M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{140}$$

Die Methode dafür ist, die Matrix, in unserem Fall $M = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$, mit der Einheitsmatrix als Koeffizientenmatrix aufzuschreiben. Wir haben dann also:

$$M = \left(\begin{array}{cc|cc} 2 & 5 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{array}\right). \tag{141}$$

Nun stellen wir so lange um, bis wir links die Einheitsmatrix erhalten.
Zuerst schicken wir II auf $2 \cdot$ II.

$$M = \left(\begin{array}{cc|cc} 2 & 5 & 1 & 0 \\ 2 & 6 & 0 & 2 \end{array}\right). \tag{142}$$

Dann schicken wir II auf II $-$ I:

$$M = \left(\begin{array}{cc|cc} 2 & 5 & 1 & 0 \\ 0 & 1 & -1 & 2 \end{array}\right). \tag{143}$$

Dann schicken wir I auf I $-5 \cdot$ I:

$$M = \left(\begin{array}{cc|cc} 2 & 0 & 6 & -10 \\ 0 & 1 & -1 & 2 \end{array}\right). \tag{144}$$

Dann schicken wir I auf $\frac{\text{I}}{2}$:

$$M = \left(\begin{array}{cc|cc} 1 & 0 & 3 & -5 \\ 0 & 1 & -1 & 2 \end{array}\right). \tag{145}$$

Im rechten Teil der Matrix können wir nun die invertierte Matrix ablesen.

Aus diesem Verfahren ist offensichtlich, dass sich nicht alle Matrizen invertieren lassen, denn hat man z. B. die Nullmatrix, dann kann man die Zeilen so oft und viel miteinander verrechnen wie man will und man kommt nie zum Ende. Wenn alle Zeilen linear abhängig sind, dann ist die Matrix nicht invertierbar, genauso, wenn die Determinante gleich 0 ist.

6.2.11 Die Dimension einer Matrix

Die Dimension einer Matrix bestimmt sich aus der Anzahl der linear unabhängigen Spalten der Matrix. Die Dimension einer Matrix bestimmt, in wie vielen räumlichen Dimensionen sich ein Vektor, der ein Vielfaches der Matrix ist, ausbreiten kann.

Beispiel:

$$U = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 2 & -1 \\ 2 & 4 & 10 \end{pmatrix} = \left\{ \left(\left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + 2 \times \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 10 \end{pmatrix} \right) \right) \right\}. \tag{146}$$

Da der erste und zweite Vektor linear abhängig sind, fällt einer der beiden bei der Dimensionsbetrachtung weg. Daher gilt: $\mathrm{Dim}\,(U) = 2$. Wenn die Spaltenvektoren keien Vielfachen sind, dann müssen auch noch die Zeilenvektoren überprüft werden.

6.2.12 Der Rang einer Matrix

Der Rang bezeichnet die Anzahl der unabhängigen Zeilen- und Spaltenvektoren einer Matrix.

Die Matrix

$$A = \begin{pmatrix} 1 & 3 & -1 \\ 2 & 6 & -2 \\ 5 & 23 & 0 \end{pmatrix}, A \in \mathbb{N}^{3\times 3} \tag{147}$$

hat die Zeilenvektoren

$$\begin{pmatrix} 1 & 3 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 6 & -2 \end{pmatrix}, \begin{pmatrix} 5 & 23 & 0 \end{pmatrix} \tag{148}$$

und die Spaltenvektoren

$$\begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \\ 23 \end{pmatrix}, \begin{pmatrix} -1 \\ -2 \\ 0 \end{pmatrix}. \tag{149}$$

Als erstes müssen wir versuchen, die Matrix in die Zeilenstufenform zu bringen (vgl. ↗ *Die Zeilenstufenform* (6.2.6).

$$\begin{pmatrix} 1 & 3 & -1 \\ 2 & 6 & -2 \\ 5 & 23 & 0 \end{pmatrix} \xrightarrow{\underline{\underline{\mathrm{II}}} \to 2 \cdot \underline{\mathrm{I}}} \begin{pmatrix} 1 & 3 & -1 \\ 0 & 0 & 0 \\ 5 & 23 & 0 \end{pmatrix} \xrightarrow{\underline{\underline{\mathrm{II}}} \leftrightarrow \underline{\underline{\mathrm{III}}}} \begin{pmatrix} 1 & 3 & -1 \\ 5 & 23 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{150}$$

Um die Zeilenstufenform zu vollenden, müssen wir nun nur noch den Zeilenführer der zweiten Zeile verschieben:

$$\begin{pmatrix} 1 & 3 & -1 \\ 5 & 23 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\underline{\underline{\mathrm{II}}} \to \underline{\underline{\mathrm{II}}} - 5 \cdot I} \begin{pmatrix} 1 & 3 & -1 \\ 0 & 8 & 5 \\ 0 & 0 & 0 \end{pmatrix} \tag{151}$$

und wir haben die Zeilenstufenform. Der Rang der Matrix ist die Anzahl von Zeilen, die nicht ausschließlich aus 0 bestehen. Das heißt: $\mathrm{rang}(A) = 2$, weil von den drei Zeilen zwei nicht 0 sind.

6.2.13 Der Kern einer Matrix

Der Kern einer Matrix ist dadurch bestimmt, dass die Matrix multipliziert mit ihrem Kern zum Nullvektor wird. Das heißt abstrakt: $\mathrm{Ker}(A^{n\times m}) = \left\{x \in \mathbb{R}^{n\times 1} \middle| Ax = \vec{0}\right\}$.

Oder im konkreten Beispiel:

$$U = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 2 & 1 & 10 \end{pmatrix}, \tag{152}$$

$$\mathrm{Ker}\,(U) \Rightarrow \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 2 & 1 & 10 \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \tag{153}$$

Das impliziert die Gleichungssysteme:

$$x_1 + 2x_2 + x_3 = 0 \tag{154}$$

$$x_1 + \quad - x_3 = 0 \tag{155}$$

$$2x_1 + x_2 + 10x_3 = 0 \tag{156}$$

Daraus ergibt sich, dass $x_1 = x_2 = x_3 = 0$. Das heißt, $\mathrm{Ker}(U) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. (Es ist der Nullvektor, weil alle Zeilen voneinander unabhängig waren; bei abhängigen Zeilen gäbe es etwas Anderes als den Nullvektor.)

Die Dimension (vgl. ↗ *Die Dimension einer Matrix* (6.2.11)) des Kerns bestimmt sich durch die Anzahl linear unabhängiger Werte in ihr, d. h. für dieses Beispiel $\dim(\mathrm{Ker}\,(U)) = 1$, da alle Werte 0 sind und damit linear abhängig voneinander.

6.2.14 Multilinearität von Matrizen

Gegeben sei die Matrix $M \in \mathbb{K}^{n\times n}$ mit:

$$\begin{pmatrix} a & b & c \\ xd & xe & xf \\ h & i & j \end{pmatrix} \tag{157}$$

und die Matrix M' ohne den Vorfaktor x:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ h & i & j \end{pmatrix} \tag{158}$$

Dann ist die Determinante $\det(M) = x\det(M')$.

Gleiches gilt für Spalten. So ist

$$\det\begin{pmatrix} a & xb & c \\ d & xe & f \\ h & xi & j \end{pmatrix} = x\det\begin{pmatrix} a & b & c \\ d & e & f \\ h & i & j \end{pmatrix}. \tag{159}$$

Ist ein Vorfaktor in jeder Zeile, wie z. B. ein ›-‹, dann kann man ihn auch ›herausziehen‹:

$$\det(-M) = \det\begin{pmatrix} -a & -b & -c \\ -d & -e & -f \\ -h & -i & -j \end{pmatrix} = (-1)^3\det\begin{pmatrix} a & b & c \\ d & e & f \\ h & i & j \end{pmatrix}. \tag{160}$$

6.2.15 Schnell Potenzen von Matrizen berechnen

⚠!!!TODO!!!⚠ Schnell Potenzen von Matrizen berechnen

$$A = SDS^{-1} \tag{161}$$

6.3 Vektorräume und Untervektorräume

Allgemeine Definition. Sei K ein Körper, dann ist $(V, +, \langle k|k \in K\rangle)$ ein K-Vektorraum. Dieser besteht aus:

- Einer Menge V, die ungleich der leeren Menge ist.
- Einer Addition: $+ : V \times V \to V$.
- Einer Skalarmultiplikation $(k|k \in K) : K \times V \to V$.

Beispiele für Vektorräume sind der allgemeine K-VR oder mit spezifischen Körpern der $\mathbb{R}$-Vr oder $\mathbb{C}$-VR.

6.3.1 Vektorraumaxiome

1. $\forall v_1, v_2 \in V$ ist $v_1 \times v_2$ ein eindeutig bestimmtes Element von V.
2. $v_1, v_2, v_3 \in V : v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ (Assoziativ)
3. $v_1, v_2 \in V : v_1 + v_2 = v_2 + v_1$ (Kommutativ)
4. $\forall v \in V : \exists \vec{0} \in V : v = \vec{0} + v = v + \vec{0}$ (Nullvektor als neutrales Element der Addition)
5. $\forall v \in V : \exists -v \in V : v + (-v) = (-v) + v = \vec{0}$ (Jedes Element hat ein additives Inverses)
6. $\forall k \in K : \forall v \in V : \exists kv \in V$
7. $\forall v \in V : \vec{1} \cdot v = v$ (Einsvektor als neutrales Element der Multiplikation)
8. $\forall k_1, k_2 \in K : \forall v \in V : (k_1 k_2)v = k_2(k_1 v)$ (Assoziativität der Multiplikation)

9. $\forall k \in K : \forall v_1, v_2 \in V : (k_1 + k_2) \times v = vk_1 + vk_2$
10. $\forall k \in K : \forall v_1, v_2 \in V : k(v_1 + v_2) = kv_1 + kv_2$

6.3.2 Bestimmen, ob U ein Untervektorraum von V ist

Um zu bestimmen, ob U ein Untervektorraum von V ist, muss man schauen, ob der Nullvektor in diesem Vektorraum ist. Das heißt, das Gleichungssystem

$$U \times \vec{x} = \vec{0} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \tag{162}$$

muss Lösungen haben. Hat es keine, ist es kein Untervektorraum.

Hat es welche, muss weiterhin überprüft werden, ob man durch Addition oder Multiplikation aus dem Vektorraum herauskommt. Sollte z. B. die Beschränkung sein, dass $a_n \leq 1 \wedge b_n \leq 1$, dann käme man mit einer Multiplikation, die a oder b größer 1 machen würde, aus dem Vektorraum hinaus und U wäre kein Untervektorraum.

Jeder Untervektorraum ist selbst wieder ein Vektorraum. Die anderen Axiome (z. B. die Assoziativität der Multiplikation) müssen nicht überprüft werden. Diese werden vom Übervektorraum ›geerbt‹.

6.3.3 Lineare Abhängigkeit

Zwei Vektoren sind linear abhängig, wenn der eine ein Vielfaches des Anderen ist. So ist z. B.

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \frac{1}{2} \times \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix}. \tag{163}$$

Damit sind diese beiden Vektoren Vielfache voneinander und linear abhängig.

Die Vektoren $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ können beispielsweise nicht linear abhängig sein, denn die 0 lässt sich durch keine Multiplikation zu einer 1 machen.

Ein effizienter Algorithmus zum Herausfinden, ob eine Menge von Vektoren Vielfache voneinander sind, wäre es, die einzelnen Vektoren $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ zu ordnen und anzufangen mit $\vec{v}_1$ und diesen mit jedem $\vec{v}_2, \ldots, \vec{v}_n$ zu vergleichen. Ist er ein Vielfaches von irgendeinem dieser Vektoren, streichen wir ihn und brechen die Betrachtung für den ersten Vektor ab. Dann ›verschieben‹ wir das Raster und fangen mit $\vec{v}_2$ an und vergleichen ihn mit $\vec{v}_3, \ldots, \vec{v}_n$, streichen ihn raus, wenn er ein Vielfaches von einem dieser Vektoren ist und wiederholen dies, bis wir alle Vektoren einmal miteinander verglichen haben.

Die nun nicht-durchgestrichenen Vektoren sind keine Vielfache voneinander.

6.3.4 Span bestimmen

Gegeben sei

$$U = \left\{ \begin{pmatrix} a+3b-8c \\ a-b+4c \\ 2a-b+5c \end{pmatrix} \middle| a,b,c \in \mathbb{R} \right\}. \tag{164}$$

Diese lässt sich umschreiben zu:

$$U = \left\{ \begin{pmatrix} a \\ a \\ 2a \end{pmatrix} + \begin{pmatrix} 3b \\ -b \\ -b \end{pmatrix} + \begin{pmatrix} -8c \\ 4c \\ 5c \end{pmatrix} \middle| a,b,c \in \mathbb{R} \right\}. \tag{165}$$

Nun klammern wir die Parameter aus:

$$U = \left\{ a \times \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + b \times \begin{pmatrix} 3 \\ -1 \\ -1 \end{pmatrix} + c \times \begin{pmatrix} -8 \\ 4 \\ 5 \end{pmatrix} \middle| a,b,c \in \mathbb{R} \right\}. \tag{166}$$

Lassen wir nun die Parameter weg, erhalten wir fast den Span:

$$\mathrm{Span}_{\mathbb{R}}(U) = \mathrm{Span}_{\mathbb{R}} \left(\left\{ \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -8 \\ 4 \\ 5 \end{pmatrix} \right\} \right). \tag{167}$$

Der einzige Schritt, den wir jetzt noch checken müssen ist, ob die Parameter linear abhängig sind oder nicht (vgl. auch ↗ *Lineare Abhängigkeit* (6.3.3)). Aus der Menge der untereinander linear abhängigen Parameter muss dann noch einer ausgewählt werden (welcher ist egal, denn sie sind alle ›inhaltlich‹ gleich) und die anderen im Span verworfen werden.

6.4 Eigenwerte und Eigenvektoren

Der Eigenwert λ bestimmt sich dadurch, dass eine Matrix A mal einem Vektor x gleich ist mit dem skalaren $\lambda \cdot x$, oder in Formeln:

$$A \cdot x = \lambda \cdot x. \tag{168}$$

Das ist gleichbedeutend mit $A \cdot x = \lambda E \cdot x$, wobei E die Einheitsmatrix ist. Da links und rechts der Gleichung zwei verschiedene Ringe (vgl. ↗ *Ring* (5.24)) sind, stellt man die Gleichung in die Form mit der Einheitsmatrix um (damit sowohl links als auch Rechts der Ring $(\mathbb{K}^{n\times n}, \cdot, +)$ benutzt wird).

Nun stellt man die Gleichung so um, dass auf einer Seite vom Gleichheitszeichen die 0 steht:

$$A \cdot x = \lambda E \cdot x \Leftrightarrow A \cdot x - \lambda x = 0 \Leftrightarrow (A - \lambda E)x = 0 \tag{169}$$

Die Determinante $\det(A - \lambda E)$ heißt *charakteristisches Polynon* der Matrix A.

Das charakteristische Polynon bestimmt sich folgendermaßen:

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}, x = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, E^{3\times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{170}$$

Wir können nun bei Matrizen bis 3×3 die Regel von Sarrus nehmen (alternativ den Laplace'schen Entwicklungssatz bei größeren Matrizen) und die Determinante bestimmen.

$$\det(A - \lambda E) = \det \begin{pmatrix} a-\lambda & b & c \\ d & e-\lambda & f \\ g & h & i-\lambda \end{pmatrix} = \tag{171}$$

$$(a-\lambda)(-\lambda(e+i) + ei - fh + \lambda^2) + b(-di + d\lambda + fg) + c(dh - eg + g\lambda) = 0. \tag{172}$$

Hiervon bestimmen wir nun die Nullstellen, um die Eigenwerte zu bestimmen. Ein praktisches Beispiel:

Bestimmen wir dies nun für die Beispielmatrix $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 7 \\ 1 & 0 & 2 \end{pmatrix}$ und $x = \begin{pmatrix} 1 \\ 5 \\ 6 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 7 \\ 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ 6 \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ 5 \\ 6 \end{pmatrix} \Leftrightarrow \tag{173}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 7 \\ 1 & 0 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \tag{174}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 7 \\ 1 & 0 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1-\lambda & 2 & 3 \\ 3 & 4-\lambda & 7 \\ 1 & 0 & 2-\lambda \end{pmatrix}. \tag{175}$$

Nun bestimmen wir die Determinante (bzw. das charakteristische Polynon) dieser Matrix.

$$\det \begin{pmatrix} 1-\lambda & 2 & 3 \\ 3 & 4-\lambda & 7 \\ 1 & 0 & 2-\lambda \end{pmatrix} = (1-\lambda)(4-\lambda)(2-\lambda) - 10 + 9\lambda. \tag{176}$$

Nun versuchen wir, die Nullstellen dieses charakteristischen Polynoms zu finden. Dazu formen wir es ein wenig um.

$$-2 + 5\lambda + 7\lambda^2 - \lambda^3 = 0. \tag{177}$$

Da ich die Ausgangsmatrix schlecht gewählt habe, erhalten wir häßliche reelle Zahlen als Lösungen: $\lambda_1 \approx -0,28, \lambda_2 \approx 1,15, \lambda_3 \approx 6,13$.

Der weitere Weg ist, die λ-Werte einzusetzen in die Matrix und den Kern der Matrix zu berechnen (d. h. $Av = 0$). Für jedes λ ist v ist dann ein Eigenvektor der Matrix.

Ein besseres Beispiel ist das Folgende, denn dort kommen ›schönere‹ Eigenwerte raus:

$$\begin{pmatrix} 3 & -1 & 0 \\ 2 & 0 & 0 \\ -2 & 2 & -1 \end{pmatrix} \cdot v = \lambda v \Leftrightarrow \det\left(\begin{pmatrix} 3 & -1 & 0 \\ 2 & 0 & 0 \\ -2 & 2 & -1 \end{pmatrix} - \lambda E^{3\times 3}\right) \Leftrightarrow \tag{178}$$

$$\det\begin{pmatrix} 3-\lambda & -1 & 0 \\ 2 & 0-\lambda & 0 \\ -2 & 2 & -1-\lambda \end{pmatrix} = -2+\lambda+2\lambda^2-\lambda^3. \tag{179}$$

Nun suchen wir die Nullstellen von $-2+\lambda+2\lambda^2-\lambda^3=0$. Wir erraten die erste Nullstelle, $\lambda_1=1$, und lösen dann die restliche Gleichung via PQ-Formel.

Wir erhalten die Eigenwerte $\lambda \in \{-1,1,2\}$.

Wir setzen nun diese Werte für λ ein und erhalten folgende Matrizen:

$$M_{-1} = \begin{pmatrix} 4 & -1 & 0 \\ 2 & 1 & 0 \\ -2 & 2 & 0 \end{pmatrix}, M_1 = \begin{pmatrix} 2 & -1 & 0 \\ 2 & -1 & 0 \\ -2 & 2 & -2 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 2 & 0 \\ -2 & 2 & 1 \end{pmatrix}. \tag{180}$$

Für diese berechnen wir nun den Kern, d. h. z. B. für M_2:

$$\begin{pmatrix} 1 & -1 & 0 \\ 2 & 2 & 0 \\ -2 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \tag{181}$$

Daraus ergibt sich das Gleichungssystem:

$$x - y = 0, \tag{182}$$

$$2x + 2y = 0, \tag{183}$$

$$-2x + 2y + z = 0, \tag{184}$$

woraus sich der Kern bestimmt als:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{185}$$

6.5 Orthogonalräume

⚠!!!TODO!!!⚠ Orthogonalräume

6.5.1 Orthonormalbasis

⚠!!!TODO!!!⚠ Orthonormalbasis

6.5.2 Orthogonale Projektion

⚠!!!TODO!!!⚠ Orthogonale Projektion

6.6 Projektion

⚠!!!TODO!!!⚠ Projektion

6.7 Gram-Schmidt-Verfahren

⚠!!!TODO!!!⚠ Gram-Schmidt-Verfahren

6.8 Basiswechselsatz

⚠!!!TODO!!!⚠ Basiswechselsatz

6.9 Norm

Die Norm eines Vektors ist in R^2 bzw. R^3 vergleichbar mit der Länge eines Vektors. Sie wird berechnet über

$$||v||_2 := \sqrt{v_1^2 + v_2^2 + \cdots + v_n^2} = \sqrt{\sum_{i=1}^{n} v_i^2} \tag{186}$$

Diese Formel ergibt sich aus einer Abstraktion des Satzes von Pythagoras.

6.10 Bestapproximation

Sei $Ax = b$ ein lineares Gleichungssystem ohne Lösung (z. B. durch Messungen gewonnene Punkkte), die nicht exakt auf eine Linie fallen. Dann kann man mit einer Bestapproximation ein lineares Gleichungssystem finden, das sich dem ursprünglichen unlösbaren LGS möglichst nah annähert. Das heißt, dass zwischen den einzelnen gemessenen Punkten eine möglichst kleine Distanz zu den Punkten in der Funktion befindet.

Dafür gilt:

$$\forall u \in U : ||v - \hat{v}|| = ||v - u||, \tag{187}$$

$$\hat{v} = \text{proj}_u v \tag{188}$$

⚠!!!TODO!!!⚠ Bestapproximation