Peter Hartmann

Mathematik für Informatiker

7. Auflage

Lösungsskizzen zu Teil 1: Diskrete Mathematik und lineare Algebra

1 Mengen und Abbildungen

Verständnisfragen

1. Was ist der Unterschied zwischen $=$ und $:=$?

= steht für die Gleichheit der rechten und linken Seite, := für die Definition des links stehenden Ausdrucks.

2. Was ist die Potenzmenge der leeren Menge $P(\varnothing)$?

$\{\varnothing\}$.

3. Gibt es Mengen A, B mit $A \subset B$, $A \neq B$, aber $|A| = |B|$?

Ja, z.B. $\mathbb{N}$ und $\mathbb{Z}$.

4. Was ist $\bigcup_{n\in\mathbb{N}}^{n} \{x \in \mathbb{R} \mid -n < x < n\}$.

$\mathbb{R}$.

5. Kann eine Ordnungsrelation gleichzeitig eine Äquivalenzrelation sein?

In einer Ordnungsrelation folgt aus $a \leq b$ und aus $b \leq a$ immer $a = b$. Wenn die Ordnungsrelation symmetrisch wäre, muss also für alle Elemente $a = b$ gelten. Nur auf einelementigen Mengen ist also die = Relation auch eine (ziemlich langweilige) Ordnungsrelation.

6. Eine Äquivalenzrelation teilt eine Menge M in disjunkte Äquivalenzklassen ein. Sei umgekehrt eine Einteilung von M in disjunkte Teilmengen gegeben, deren Vereinigung gerade M ergibt. Gibt es eine Äquivalenzrelation, deren Äquivalenzklassen genau diese Teilmengen sind?

Ja, die Relation kann definiert werden durch $a \approx b$ genau dann, wenn a und b in einer dieser Teilmengen liegen.

7. Was ist der Unterschied zwischen einer partiellen Ordnung und einer linearen Ordnung?

In einer linearen Ordnung sind je zwei Elemente vergleichbar, in der partiellen Ordnung nicht.

8. Seien $f : M \to N$ und $g : N \to M$ Abbildungen mit der Eigenschaft, dass $g \circ f : M \to M$ die identische Abbildung auf M ist. Ist dann auch $f \circ g : N \to N$ die identische Abbildung auf N?

Nein! Beispiel: $f : \mathbb{R}^+ \to \mathbb{R}, x \mapsto x, g : \mathbb{R} \to \mathbb{R}^+, x \mapsto |x|$. Es ist $g \circ f$ die identische Abbildung, $f \circ g$ bildet x auf $|x|$ ab.

9. Gibt es eine injektive Abbildung von $\mathbb{R}$ nach $\mathbb{N}$?

Nein, denn die Mächtigkeit von $\mathbb{R}$ ist größer als die von $\mathbb{N}$.

Übungsaufgaben

1. Beweisen Sie die Formel $S \cup (M \cap N) = (S \cup M) \cap (S \cup N)$

   „⊂„ 1. Fall: $x \in S \Rightarrow x \in S \cup M$ und $x \in S \cup N \Rightarrow x \in (S \cup M) \cap (S \cup N)$

   2. Fall: $x \in M \cap N \Rightarrow x \in M$
   $x \in N \Rightarrow x \in S \cup M$ und $x \in S \cup N \Rightarrow x \in (S \cup M) \cap (S \cup N)$.

   „⊃„ 1. Fall: $x \in S \Rightarrow x \in S \cup (M \cap N)$

   2. Fall: $x \notin S \Rightarrow$ (wegen $x \in S \cup M$ und $x \in S \cup N$) $x \in M$ und $x \in N$
   $\Rightarrow x \in M \cap N \Rightarrow x \in S \cup (M \cap N)$

2. Beweisen Sie die Formel $\overline{M \cup N} = \overline{M} \cap \overline{N}$.

   $x \in \overline{M \cup N} \Leftrightarrow x \notin M \cup N \Leftrightarrow x \notin M$ und $x \notin N \Leftrightarrow x \in \overline{M}$ und $x \in \overline{N} \Leftrightarrow x \in \overline{M} \cap \overline{N}$

3. Untersuchen Sie die Relationen $\subset$ und $\not\subset$ auf Reflexivität, Symmetrie und Transitivität.

   Das Ergebnis: $\subset$ ist transitiv und reflexiv, $\not\subset$ ist gar nichts.

4. Sei $R = \{(m, n) \in \mathbb{Z} \mid m - n$ ist durch 5 teilbar$\}$ und $r \in \{0,1,2,3,4\}$. Wir wissen schon, dass R eine Äquivalenzrelation ist. Zeigen Sie, dass $[r]$, die Äquivalenzklasse von r genau die Menge der Zahlen ist, die Rest r bei Division durch 5 lassen.

   m hat Rest *r* bei Division durch *q* genau dann, wenn es ein $k \in \mathbb{Z}$ gibt mit $m = qk+r$.

   Zu zeigen ist, dass die Mengen $M = \{x \mid xRr\} = \{x \mid$ Es gibt ein $k \in \mathbb{Z}$ mit $x - r = 5k\}$ und $N = \{x \mid x$ lässt Rest r bei Division durch 5$\} = \{x \mid$ Es gibt ein $k \in \mathbb{Z}$ mit $x = 5k + r\}$ übereinstimmen. Es gilt: $x \in M \Leftrightarrow x - r = 5k \Leftrightarrow x = 5k + r \Leftrightarrow x \in N$.

5. Es seien folgende Mengen von natürlichen Zahlen gegeben:

   M = $\{x \mid 4$ teilt $x\}$
   N = $\{x \mid 100$ teilt $x\}$
   T = $\{x \mid 400$ teilt $x\}$
   S = $\{x \mid x$ ist ein Schaltjahr$\}$

   Formulieren Sie die Menge S mit Hilfe der Mengenoperationen $\cup$, $\cap$ und \ aus den Mengen M, N, T. Eliminieren Sie in dieser Darstellung das \ Zeichen durch Komplementbildung.

   Schaltjahre sind Jahre die durch 4 teilbar sind, außer den Jahren die durch 100, nicht aber durch 400 teilbar sind. (1900 war kein Schaltjahr, 2000 war ein Schaltjahr und 2100 wird wieder kein Schaltjahr sein!)

   Es gibt verschiedene Möglichkeiten. Zum Beispiel:

   $S = M \setminus (N \setminus T) = M \setminus (N \cap \overline{T}) = M \cap (\overline{N \cap \overline{T}}) = M \cap (\overline{N} \cup T)$ oder

   $S = T \cup M \setminus N = T \cup (M \cap \overline{N}) = (T \cup M) \cap (T \cup \overline{N}) = M \cap (T \cup \overline{N})$.

6. Überprüfen Sie, ob die folgenden Abbildungen surjektiv beziehungsweise injektiv sind:

   a) $f:\mathbb{R}^3 \to \mathbb{R}^2, (x,y,z) \mapsto (x+y, y+z)$

   b) $f:\mathbb{R}^2 \to \mathbb{R}^3, (x,y) \mapsto (x, x+y, y)$

   a) ist surjektiv: (x,z) hat zum Beispiel das Urbild $(x,0,z)$.
   ist nicht injektiv: denn (0,1,0) und (1,0,1) haben Bild (1,1).

   b) ist injektiv: $(x_1,y_1) \neq (x_2,y_2) \Rightarrow (x_1, x_1+y_1, y_1) \neq (x_2, x_2+y_2, y_2)$.
   ist nicht surjektiv: denn zum Beispiel hat (1,1,1) kein Urbild.

7. Ist $f:M \to N$ eine Abbildung, so werden dadurch zwei Abbildungen zwischen den Potenzmengen erzeugt:

$$F:P(M) \to P(N), \qquad G:P(N) \to P(M),$$
$$U \mapsto f(U) \qquad\qquad V \mapsto f^{-1}(V)$$

   Sind dies wirklich Abbildungen? (Überprüfen Sie die Definition.) Überlegen Sie mit einem einfachen Beispiel für *f*, dass *F* und *G* nicht invers zueinander sind.

   Die Vorschriften ordnen jeder Menge aus $P(M)$ (bzw. $P(N)$) genau eine Bildmenge aus $P(N)$ bzw. $P(M)$ zu, sie sind also Abbildungen. Das Beispiel $M = \{1,2\}$, $N = \{a, b\}$ $f(1) = f(2) = a$ zeigt, dass F nicht injektiv ist, denn z.B. $F(\{1\}) = F(\{2\}) = \{a\}$. Damit sind sie auch nicht invers zueinander.

8. Zeigen Sie: Sind *f* und *g* Abbildungen, und ist die Verknüpfung $f \circ g$ möglich, so gilt: Sind *f* und *g* surjektiv beziehungsweise injektiv, so ist auch $f \circ g$ surjektiv beziehungsweise injektiv.

   $f \circ g$ ist surjektiv: Seien $g:M \to N, f:N \to S$ surjektiv. Sei $z \in S$. Dann gibt es $y \in N$ mit $f(y) = z$ und weiter ein $x \in M$ mit $g(x) = y$. Dann ist $f \circ g(x) = f(g(x)) = f(y) = z$, also x Urbild von z unter $f \circ g$.

   $f \circ g$ ist injektiv: sei $x \neq y$. Dann ist $g(x) \neq g(y)$ und da auch f injektiv ist folgt auch $f(g(x)) \neq f(g(y))$.

2 Logik

Verständnisfragen

1. Kann man von einer Aussage immer entscheiden, ob sie richtig oder falsch ist?

Nein, siehe z.B. die Kontinuumshypothese.

2. Erläutern Sie den Unterschied zwischen $\leftrightarrow$ und $\Leftrightarrow$.

$\leftrightarrow$ ist ein Symbol der Sprache der Aussagenlogik (der Syntax), $\Leftrightarrow$ ist ein Symbol der Semantik.

3. Und was ist der Unterschied zwischen $\rightarrow$ und $\Rightarrow$.

Das Gleiche: $\rightarrow$ ist ein Symbol der Syntax (wenn – dann), $\Rightarrow$ ist ein Symbol der Semantik

4. Aus einem einstelligen Prädikat kann man mit zwei Methoden eine Aussage machen. Welche sind das?

Quantifizieren oder Einsetzen eines Wertes für die Variable.

5. Woraus besteht eine formale Sprache?

Aus Alphabet, Syntax und Semantik.

6. Gibt es Aussagen, die keine Prädikate sind?

Nein. Aussagen sind 0-stellige Prädikate.

7. Gibt es einen Unterschied zwischen einer Tautologie (die immer wahr ist) und dem Wahrheitswert „wahr“?

Eine Tautologie ist eine Aussage, „wahr“ der Wahrheitswert, der einer Aussage oder Aussagenformel zugeordnet werden kann, spricht über die Bedeutung einer Aussage.

Übungsaufgaben

1. Überprüfen Sie, ob die folgenden Sätze Aussagen sind, und ob sie wahr oder falsch sind:

   a) Entweder ist $5 < 3$ oder aus $2+3 = 5$ folgt $3 \cdot 4 = 12$.

   b) Wenn ich groß bin, dann bin ich klein.

   c) Dieser Satz ist keine Aussage.

   Zu a): Entweder A oder $(B \rightarrow C)$. Dies ist wahr, da A falsch und $B \rightarrow C$ wahr ist.

   Zu b): $A \rightarrow B$ ist wahr, wenn A falsch und B wahr, $A \rightarrow B$ ist falsch wenn A wahr und B falsch. Also ist $A \rightarrow \neg A$ wahr, wenn A falsch ist (ich bin klein) und falsch, wenn A wahr ist (ich bin groß).

   Zu c): Dies ist eine falsche Aussage.

2. Stellen Sie für die Bindewörter „weder ... noch“, „entweder ... oder“ und „zwar ... jedoch nicht“ Wahrheitstafeln auf und versuchen Sie diese Verbindungen mit $\wedge$, $\vee$, $\neg$ auszudrücken.

   Als Beispiel: zwar ... jedoch nicht (die anderen Verknüpfungen gehen ähnlich)

A	B	zwar A jedoch nicht B	$A \wedge \neg B$
w	w	f	f
w	f	w	w
f	w	f	f
f	f	f	f

3. Bilden Sie die Negation von

   a) Das Dreieck ist rechtwinklig und gleichschenklig.

   b) Boris kann russisch oder deutsch sprechen.

   Zu a): Das Dreieck ist nicht rechtwinklig oder nicht gleichschenklig.

   Zu b): Boris kann nicht russisch und nicht deutsch sprechen.

4. Beweisen Sie ein Distributiv- und ein Assoziativgesetz für die Verknüpfungen $\wedge$, $\vee$.

   Für das Distributivgesetz:

A	B	C	$A \vee B$	$\boldsymbol{(A \vee B) \wedge C}$	$A \wedge C$	$B \wedge C$	$\boldsymbol{(A \wedge C) \vee (B \wedge C)}$
w	w	w	w	$\boldsymbol{w}$	w	w	$\boldsymbol{w}$
w	w	f	w	$\boldsymbol{f}$	f	f	$\boldsymbol{f}$
w	f	w	w	$\boldsymbol{w}$	w	f	$\boldsymbol{w}$

   usw. usw (insgesamt 8 Fälle). Auch für das Assoziativgesetz muss so eine Tabelle aufgestellt werden.

5. Zeigen Sie, dass $(\neg B \to B) \to B$ eine Tautologie ist. (Wenn man aus dem Gegenteil einer Annahme die Annahme herleiten kann, dann ist die Annahme wahr). Ist auch $(\neg B \to B) \leftrightarrow B$ eine Tautologie?

B	$\neg B$	$\neg B \to B$	$(\neg B \to B) \to B$	$(\neg B \to B) \leftrightarrow B$
w	f	w	w	w
f	w	f	w	w

Bei beiden Aussagen handelt es sich also um Tautologien.

6. Für jede natürliche Zahl n sei a_n eine reelle Zahl. Im zweiten Teil des Buches werden wir sehen, dass die Folge a_n genau dann gegen Null konvergiert, wenn die folgende logische Aussage erfüllt ist:

$$\forall t \exists m \forall n \quad (n > m \to |a_n| < \frac{1}{t}), \quad m, n, t \in \mathbb{N}.$$

Bilden Sie die Negation dieser Aussage.

Die Negation lautet: $\exists t \forall m \exists n \quad \neg(n > m \to |a_n| < \frac{1}{t})$. Rechnen Sie noch aus, dass $\neg(A \to B) \leftrightarrow (A \wedge \neg B)$ einen Tautologie ist, so erhalten Sie die äquivalente Form:

$$\exists t \forall m \exists n \quad (n > m \ \wedge \ |a_n| \geq \frac{1}{t}).$$

7. Aus Satz 2.11 folgt nicht, dass das Produkt der ersten n Primzahlen + 1 eine Primzahl ist. Finden Sie das kleinste n mit der Eigenschaft, dass $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ nicht prim ist.

In dem Mathematiktool `sage` berechnen die beiden folgenden Zeilen die Faktorzerlegung der ersten n Primzahlen + 1:

```
L = [Primes().unrank(i) for i in range(0,6)]
factor(prod(L)+1)
```

Ergebnis: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ ist $59 \cdot 509$.

3 Natürliche Zahlen, vollständige Induktion, Rekursion

Verständnisfragen

1. Kann man ein Axiom beweisen?

Nein!

2. Kann ein Beweis einer Aussage richtig sein, wenn im Induktionsschluss die Induktionsannahme nicht verwendet wird?

Kann sein, dann hat man die Aussage direkt bewiesen, aber keine vollständige Induktion durchgeführt.

3. Warum ist das Hexadezimalsystem für Informatiker so wichtig?

Ein Byte lässt sich genau durch 2 Hexadezimalziffern darstellen (4 Bit für jede Ziffer)

4. Kann bei der Darstellung einer natürlichen Zahl im b-adischen System auch eine negative Basis verwendet werden?

Nein, das klappt nicht, denn dann treten auch negative Zahlen auf!

5. Bei der Berechnung der b-adischen Darstellung einer Zahl wird eine fortgesetzte Division mit Rest durchgeführt. Kann man wirklich sicher sein, dass dieses Verfahren immer endet?

Ja, denn da man mindestens durch 2 dividiert wird der Quotient in jedem Schritt kleiner, irgendwann muss dann 0 rauskommen und das Verfahren ist zu Ende.

6. Ein Integer in gängigen Programmiersprachen hat eine definierte Größe, zum Beispiel 4 Byte. Wie könnten Sie vorgehen, wenn Sie eine Klasse implementieren wollen, die beliebig große Integer enthält?

Ein Array definieren, die Elemente des Arrays enthalten die Ziffern der Zahl.

7. Worauf muss man bei der Implementierung rekursiver Programme achten?

Ist die Abbruchbedingung vorhanden und wird sie erreicht? Hat der rekursive Aufruf ein kleineres Argument als die Funktion selbst?

Übungsaufgaben

1. Zeigen Sie, dass für $n \geq 3$ gilt: $2n+1 \leq 2^n$.

   Induktionsanfang: $n = 3$: $2 \cdot 3+1 \leq 2^3$ ist richtig.
   Induktionsannahme: Sei $2n+1 \leq 2^n$ richtig.
   Induktionsschluss: $2(n+1)+1 = 2n+3 \leq 2^n + 3 \leq 2^n+2^n = 2 \cdot 2^n = 2^{n+1}$.
   ↖ $n \geq 3$!

2. Für welche natürlichen Zahlen gilt $n^2 \leq 2^n$?

   Ausprobieren: Die Aussage stimmt für 1,2,4, für 3 ist sie falsch. Der Rest folgt mit Induktion:

   Induktionsanfang: $n = 4$: $4^2 \leq 2^4$ ist richtig.
   Induktionsannahme: Sei $n^2 \leq 2^n$ richtig.
   Induktionsschluss: $(n+1)^2 = n^2 + 2n + 1 \leq 2^n+2^n = 2^{n+1}$.
   ↖ Aufgabe 1 und Induktionsannahme

3. Zeigen Sie mit vollständiger Induktion: $n \in \mathbb{N}, x \in \mathbb{R}, x \geq -1 \Rightarrow (1+x)^n \geq 1+nx$.

   Induktionsanfang: $(1 + x)^1 \geq 1+1x$ ist richtig.
   Induktionsannahme: Sei $(1 + x)^n \geq 1 + nx$ richtig .
   Induktionsschluss: $(1 + x)^{n+1} = (1 + x)^n (1 + x) \geq (1 + nx)(1 + x) = 1 + nx + x + nx^2 \geq 1 + (n + 1) x.$
   ↖ da $1+x \geq 0$

4. Zeigen Sie mit vollständiger Induktion: $\sum_{k=1}^{n} (2k-1) = n^2$.

   Induktionsanfang: $n = 1$: $2 \cdot 1 - 1 = 1^2$ ist richtig.

   Induktionsannahme: Sei $\sum_{k=1}^{n} (2k-1) = n^2$ richtig.

   Induktionsschluss: $\sum_{k=1}^{n+1} (2k-1) = \sum_{k=1}^{n} (2k-1) + 2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2$.

5. Zeigen Sie mit vollständiger Induktion: $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

   Dahinter steckt die Tatsache, dass bei der Darstellung von Zahlen im Binärsystem gilt: $\underbrace{111\cdots111}_{n} + 1 = 1\underbrace{000\cdots000}_{n}$. Formulieren Sie entsprechende Aussagen für andere Basen.

   Induktionsanfang: $n = 0$: $2^0 = 2^1 - 1$ oder $n = 1$: $1 + 2^1 = 2^2 - 1$.
   Induktionsannahme: Sei $1 + 2 + 2^2 + 2^3 + ... + 2^n = 2^{n+1} - 1$.
   Induktionsschluss: $1+2+2^2+ 2^3 +...+ 2^n + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2(2^{n+1}) - 1 = 2^{n+2} - 1$.

6. Zeigen Sie mit vollständiger Induktion: Jede nicht-leere Teilmenge der natürlichen Zahlen hat ein kleinstes Element.

   Sei M eine nicht-leere Teilmenge von $\mathbb{N}$. Wir nehmen an, dass M kein kleinstes Element hat. Sei K die Menge der natürlichen Zahlen die kleiner sind als alle Elemente von M:

   $$K := \{n \in \mathbb{N} \mid n < m \text{ für alle } m \in M\}$$

K ist eine Teilmenge des Komplements von M. Mit vollständiger Induktion zeigen wir jetzt, dass $K = \mathbb{N}$ ist und damit natürlich $M = \varnothing$ im Widerspruch zur Annahme.

Induktionsanfang: $1 \in K$, denn 1 ist die kleinste natürliche Zahl und kann nicht in M sein, sonst wäre 1 das kleinste Element in M.

Induktionsannahme: Zeige: ist $n \in K$, dann auch $n+1 \in K$.

Induktionsschluss: Sei $n \in K$. Alle Elemente von M sind größer als n. Wäre $n+1 \in M$, dann wäre $n+1$ das kleinste Element von M, da $n \notin M$ ist. Also sind sogar alle Elemente von M größer als $n+1$ und damit $n+1 \in K$.

7. Überprüfen Sie die Richtigkeit des folgenden Induktionsbeweises:

Behauptung:	Alle Pferde haben die gleiche Farbe.
Induktionsanfang:	ein Pferd hat offensichtlich die gleiche Farbe.
Induktionsannahme:	je n Pferde haben die gleiche Farbe.
Induktionsschluss:	Seien $n+1$ Pferde gegeben. Nimmt man ein Pferd heraus, so haben die restlichen n Pferde nach Induktionsannahme die gleiche Farbe. Fügt man das $n+1$. Pferd wieder hinzu und entfernt ein anderes Pferd, so haben die übrigen Pferde n wieder die gleiche Farbe. Da mindestens ein Pferd in beiden n-elementigen Pferdemengen enthalten ist, haben alle Pferde der n-elementigen Mengen die gleiche Farbe und damit auch alle $n+1$ Pferde.

Der Induktionsanfang ist richtig, auch wenn er komisch klingt, und auch der Induktionsschluss, allerdings nur für $n \geq 2$. Der Induktionsschluss von 1 auf 2 klappt nicht. Machen Sie eine Skizze dazu!

8. Darstellung von Zahlen in verschiedenen Zahlsystemen:

   Stellen Sie die Zahl $(10000)_{10}$ im 4er, 5er und 8er System dar.
   Stellen Sie $(FB97B7FE)_{16}$ im 2er System dar.
   Stellen Sie $(3614)_7$ im 11er System dar.

$(10000)_{10} = (2130100)_4 = (310000)_5 = (23420)_8$.

Bei fortgesetzter Division mit Rest ergeben die Reste die Zahldarstellung (z.B. im 8 er System):

10000:8	= 1250	Rest 0
1250:8	= 156	Rest 2
156:8	= 19	Rest 4
19:8	= 2	Rest 3
2:8	= 0	Rest 2

$(FB97B7FE)_{16} = (1111\ 1011\ 1001\ 0111\ 1011\ 0111\ 1111\ 1110)_2$.(1 Hexzeichen = 4 Bit)

$(3614)_7 = (1003)_{11}$. Das bekommen Sie am schnellsten raus, wenn Sie zunächst $(3614)_7$ ins Dezimalsystem umwandeln: $(3614)_7 = 3 \cdot 7^3 + 6 \cdot 7^2 + 1 \cdot 7^1 + 4 = 1334$, und dann ins 11 er System.

9. Untersuchen Sie den folgenden rekursiven Algorithmus:

$$x^n = \begin{cases} 1 & \text{falls } n = 0 \\ x^{\frac{n}{2}} \cdot x^{\frac{n}{2}} & \text{falls } n \text{ gerade} \\ x^{n-1} \cdot x & \text{sonst} \end{cases}$$

Berechnen Sie die Laufzeit dieses Algorithmus in Abhängigkeit von n in den Spezialfällen $n = 2^m$ und $n = 2^m–1$. Überlegen Sie, dass dies der beste beziehungsweise der schlechteste Fall ist (das heißt die reale Laufzeit liegt dazwischen).

Implementieren Sie den Algorithmus und überprüfen Sie ihre Berechnung, indem Sie bei der Ausführung die Anzahl der durchgeführten Rekursionsaufrufe zählen.

Eine Multiplikation soll die Zeit c brauchen. Der beste Fall liegt vor, wenn immer Alternative 1 gewählt werden kann, dann schrumpft n am schnellsten. Das ist der Fall, wenn $n = 2^m$. In diesem Fall ist die Laufzeit $f(n)$:

$$f(n) = f(2^m) = c + f(2^{m-1}) = 2c + f(2^{m-2}) = \ldots = mc + f(1) + d\,,$$

das heißt wegen $n = \log_2 m$: $f(n) = \log_2 n \cdot c + d$.

Was ist der schlimmste Fall? Da nach Eintreten der Alternative 3 immer n wieder gerade ist, geht n am langsamsten gegen 0, wenn abwechselnd Alternative 2 und 3 gewählt werden muss. Dies ist für die Zahlen der Form $n = 2^m – 1$ der Fall:

$$f(n) = f(2^m - 1) = c + f(2^m - 2) = c + f(2 \cdot (2^{m-1} - 1)) = 2c + f(2^{m-1} - 1) =$$
$$= 2mc + f(2^0 - 1) = 2mc + e$$

Wegen $m = \log_2(n+1)$: $f(n) = \log_2(n+1) \cdot 2c + e$.

In beiden Fällen ist der Algorithmus etwa proportional zu $\log_2 n$. (Er ist O(log n), siehe dazu *Die O-Notation* im Abschnitt 13.1 des Buches).

Hier eine Implementierung in `sage`:

```
def potenz(x,n):
    global aufrufe
    aufrufe += 1
    if (n  == 1):
        return x
    if (n%2 == 0):
        return potenz(x,n/2)^2
    return potenz(x,n-1)*x
```

```
aufrufe = 0
print(potenz(.9,31))
print(aufrufe)
```

```
0.0381520424476946
9
```

4 Etwas Zahlentheorie

Verständnisfragen

1. Wenn Sie die Berechnung des Binomialkoeffizienten mit Hilfe von Satz 4.4 in einem Programm durchführen wollen, stoßen Sie schnell auf ein Problem. Welches? Haben Sie eine Lösung dafür?

Wegen der doppelten Rekursion explodiert die Anzahl der Aufrufe. Man kann aber einmal berechnete Werte in einem Array zwischenspeichern.

2. Warum führt der Euklid'sche Algorithmus immer zu einem Ergebnis?

Der Rest wird immer kleiner, daher irgendwann zu 0.

3. Der größte gemeinsame Teiler zweier Zahlen a,b sei eine Primzahl. Kann es sein, dass a,b weitere gemeinsame Teiler haben?

Nein, dieser müsste sonst ein Teiler der Primzahl sein.

4. Wie viele gerade Primzahlen gibt es?

Nur die Zahl 2!

5. Wie wird der Rest einer Division a/b in der Mathematik berechnet, wie in gängigen Programmiersprachen (Java oder C++)?

Mathe: Das eindeutige r mit $0 \leq r < b$ mit $a = bq + r$ (immer positiv!)
Java: Berechne $q = |a|/|b|$, ist a oder b negativ dann $q_2 = -q$ und r kommt aus $a = bq_2 + r$

6. Wird als Hashfunktion die modulo Abbildung modulo einer Primzahl verwendet, so kann man bei linearer Kollisionsauflösung alle Primzahlen verwenden, bei quadratischer Kollisionsauflösung nicht. Warum?

Da nicht alle Zahlen der Hashtabelle durchlaufen werden, wenn $p \not\equiv 3 \bmod 4$ ist.

7. In $\mathbb{N}$ gilt immer $n! \neq 0$. Kann $n! = 0$ werden in $\mathbb{Z} / m\mathbb{Z}$?

Ja, sobald $m \leq n$ ist.

Übungsaufgaben

1. Zeigen Sie: sind a, b ganze Zahlen mit $a \mid b$ und $b \mid a$, so gilt $a = b$ oder $a = -b$.

   $a|b \Rightarrow b = q_1 \cdot a$, $b|a \Rightarrow a = q_2 \cdot b$. Eingesetzt: $a = q_2 \cdot (q_1 \cdot a) \Rightarrow a = q_1 q_2 \cdot a \Rightarrow q_1 q_2 = 1$. Dies ist nur möglich wenn $q_1 = q_2 = 1$ oder $q_1 = q_2 = -1$. Also ist $a = \pm b$.

2. Zeigen Sie: gilt für ganze Zahlen $a_1 \mid b_1$ und $a_2 \mid b_2$, so gilt auch $a_1\, a_2 \mid b_1\, b_2$.

   $a_1|b_1 \Rightarrow b_1 = q_1 \cdot a_1$, $a_2|b_2 \Rightarrow b_2 = q_2 \cdot a_2$. Damit $b_1\, b_2 = q_1 a_1 \cdot q_2 a_2 = q_1 q_2 \cdot a_1 a_2$, also $a_1 a_2 | b_1 b_2$.

3. Zeigen Sie, dass die Teilbarkeitsrelation | (Definition 4.9) auf den natürlichen Zahlen eine partielle Ordnung darstellt.

   Es ist Definition 1.12 nachzuprüfen. Wegen 4.10a) gilt $a|b$ und $b|c \Rightarrow a|c$.
   Natürlich gilt $a|a$ und wegen 4.10d) gilt auch $a|b$ und $b|a \Rightarrow a = b$.
   (Die Aufgabe war auf die natürlichen Zahlen beschränkt, daher kann nicht $a = -b$ sein.)

4. Schreiben Sie ein rekursives Programm zur Berechnung von $\binom{n}{k}$. Verwenden Sie dazu die Formel $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

   Eine Lösung in `sage`:

```
def nueberk(n,k):
    if k == n or k == 0:
        return 1
    return nueberk(n-1,k) + nueberk(n-1,k-1)
```

```
%%time
nueberk(49,6)
```

```
CPU times: user 11.8 s, sys: 1.69 s, total: 13.5 s
Wall time: 13.5 s
13983816
```

   Dieses Programm hat eine lange Laufzeit, da viele Koeffizienten mehrfach berechnet werden. Wenn man die schon berechneten Werte in ein Array schreibt und die Rekursion nur ausführt, wenn ein Element noch nicht berechnet ist, geht es viel schneller:

```
a = []
def nueberk1(n,k):
    global a
    if a == []:
        for i in range(1,n+1):
            a.append([0 for j in range(1,i+1)])

    if k == n or k == 0:
        a[n][k]=1
        return 1
    if a[n-1][k] == 0:
        a[n-1][k] = nueberk1(n-1,k)
    if a[n-1][k-1] == 0:
        a[n-1][k-1] = nueberk1(n-1,k-1)
    return a[n-1][k] + a[n-1][k-1]
```

```
%%time
nueberk1(49,6)
```

```
CPU times: user 0 ns, sys: 0 ns, total: 0 ns
Wall time: 15 µs
13983816
```

5. Eine etwas kniffligere Induktionsaufgabe: Zeigen Sie, dass zur rekursiven Berechnung von $\binom{n}{k}$ (nach Aufgabe 4) genau $2\cdot\binom{n}{k}-1$ Funktionsaufrufe nötig sind.

Induktionsanfang: $\binom{0}{0}=1 \Rightarrow$ ein Funktionsaufruf.

Induktionsannahme: Sei die Behauptung richtig für $n\in\mathbb{N}$ und $0 \le k \le n$.

Induktionsschluss: Sei $0 \le k < n+1$. Der 1. Aufruf lautet: `nueberk(n+1,k);` In dieser Funktion wird `nueberk(n,k)` und `nueberk(n,k-1)` berechnet, also zusätzlich nach Induktionsannahme $2\binom{n}{k}-1+2\binom{n}{k-1}-1=2\binom{n+1}{k}-2$ Aufrufe. Also haben wir insgesamt $2\cdot\binom{n+1}{k}-1$ Aufrufe. Für den Fall $k = n+1$ haben wir genau einen Aufruf und es ist ja auch $2\cdot\binom{n+1}{n+1}-1=1$.

Sie können das auch ausprobieren, indem Sie in Ihrer Implementierung einen Zähler integrieren, der die Anzahl der Funktionsaufrufe zählt. In dieser Form ist der Algorithmus also für praktische Zwecke ungeeignet. Wenn Sie die Berechnung eines Binomialkoeffizienten genau analysieren werden Sie feststellen, dass in der Rekursion viele Koeffizienten mehrfach berechnet werden. Durch einen kleinen Trick können Sie das vermeiden und den Algorithmus so aufbohren, dass er doch noch sehr schnell wird.

6. Berechnen Sie die Wahrscheinlichkeit 6 Richtige im Lotto zu haben, wenn man 8 Zahlen aus 49 auswählen kann.

$\binom{49}{6}$ = Anzahl möglicher 6 er. $\binom{8}{6}$ = Anzahl der möglichen 6er in 8 Zahlen. Die Wahrscheinlichkeit ist (1/Anzahl der möglichen 6er)·(Anzahl der möglichen 6er in 8 Zahlen) $\approx 2\cdot10^{-6}$.

7. Zeigen Sie mit vollständiger Induktion, dass für alle $n \in \mathbb{N}$ gilt:
a) $n^2 + n$ ist durch 2 teilbar, b) $n^3 - n$ ist durch 6 teilbar.

Zu a): Induktionsanfang: $1^2 + 1$ ist durch 2 teilbar.
Induktionsannahme: Es sei $n^2 + n$ durch 2 teilbar, also $n^2 + n = 2k$.
Induktionsschluss: $(n+1)^2+(n+1)=n^2+2n+1+n+1=(n^2+n)+2n+2=2k+2(n+1)$, das ist durch 2 teilbar.
Zu b): Induktionsanfang: $1^3 - 1 = 0$ ist durch 6 teilbar.
Induktionsannahme: Es sei $n^3 - n$ durch 6 teilbar, also $n^3 - n = 6k$.
Induktionsschluss: $(n+1)^3-(n+1)=n^3+3n^2+3n+1-n-1=(n^3-n)+3(n^2+n)$
$=6k+3\cdot 2l$, das ist durch 6 teilbar.

8. Berechnen Sie den größten gemeinsamen Teiler d von 456 und 269 mit Hilfe des Euklid'schen Algorithmus. Bestimmen Sie Zahlen α, β mit $\alpha \cdot 269 + \beta \cdot 456 = d$.

456	=	1·269	+	187	⇒	187	=				1·456	+ –1· 269
269	=	1·187	+	82	⇒	82	=	–1·187	+	1·269	=	–1·456 + 2· 269
187	=	2·82	+	23	⇒	23	=	–2·82	+	1·187	=	3·456 + –5· 269
82	=	3·23	+	13	⇒	13	=	–3·23	+	1·82	=	–10·456 + 17· 269
23	=	1·13	+	10	⇒	10	=	–1·13	+	1·23	=	13·456 + –22· 269
13	=	1·10	+	3	⇒	3	=	–1·10	+	1·13	=	–23·456 + 39· 269
10	=	3·3	+	1	⇒	1	=	–3·3	+	1·10	=	82·456 + –139· 269
3	=	3·1	+	0								

9. Schreiben Sie in C++ oder Java einen Modulo-Operator, der auch für negative Zahlen mathematisch korrekt arbeitet.

Sei $p > 0$ und $n < 0$. Es ist $\big(n + (-n)\big) \bmod p \equiv n \bmod p + (-n) \bmod p \equiv 0$. Da $n \bmod p$ und $(-n) \bmod p$ beides Reste modulo p sind, muss $n \bmod p = p - \big((-n) \bmod p\big)$ sein. Damit lautet eine mögliche Implementierung in C++:

```
long mod(long n, unsigned long p){
   if (n >= 0)
      return n%p;
   else
      return p - (-n)%p;
}
```

10. Schreiben Sie für $\mathbb{Z}/7\mathbb{Z}$ und $\mathbb{Z}/8\mathbb{Z}$ die Multiplikationstabellen auf. Schauen Sie sich die Zeilen und Spalten in den beiden Tabellen genau an. Was fällt Ihnen dabei auf?

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

In jeder Zeile und in jeder Spalte von $\mathbb{Z}/7\mathbb{Z}$ kommt jede Zahl genau einmal vor, bei $\mathbb{Z}/8\mathbb{Z}$ nicht. Woran das liegt lernen Sie im nächsten Kapitel

11. Zeigen Sie: Ist $a \equiv a' \bmod m$ und $b \equiv b' \bmod m$, so gilt $a+b \equiv a'+b' \bmod m$.

$a \equiv a' \bmod m \Rightarrow a - a' = q_1 m$, und $b \equiv b' \bmod m \Rightarrow b - b' = q_2 m$. Daraus folgt:
$(a - a') + (b - b') = (q_1 + q_2)m \Rightarrow (a + b) - (a' + b') = (q_1 + q_2)m$,
also $a + b \equiv a' + b' \bmod m$.

12. Beim Rechnen mit Resten kann man die Operationen +,· mit der modulo Operation vertauschen. Genauso geht man beim Potenzieren vor: Um $a^2 \bmod n$ zu berechnen, ist es einfacher $[(a \bmod n)(a \bmod n)] \bmod n$ zu berechnen (warum eigentlich? Probieren Sie ein paar Beispiele aus). Ähnlich geht man bei der Berechnung von $a^m \bmod n$ vor. Mit diesem Wissen können Sie mit Hilfe des in Aufgabe 8 von Kapitel 3 angegebenen Algorithmus zur Berechnung von x^n einen rekursiven Algorithmus zur Berechnung von $a^m \bmod n$ formulieren.

$$a^m \bmod n = \begin{cases} a \bmod n, & \text{falls } m = 1 \\ (a^{m/2} \bmod n)(a^{m/2} \bmod n) \bmod n, & \text{falls } m \text{ gerade} \\ (a \bmod n)(a^{m-1} \bmod n) \bmod n, & \text{falls } m \text{ ungerade} \end{cases}$$

13. Implementieren Sie den Euklid'schen Algorithmus; einmal iterativ und einmal rekursiv.

Zunächst rekursiv (in sage):

```
def ggt(a,b):
    r = a%b
    if r == 0:
        return b
    return ggt(b,r)
```

Und jetzt iterativ, gleichzeitig werden α und β berechnet mit $\alpha \cdot a + \beta \cdot b = \text{ggt}(a, b)$:

```
a = 456
b = 269

r  = a;                 # Initialisierung
r1 = b;
b0 = 0;
a0 = 1;
b1 = 1;
a1 = 0;
r2 = 1

while (r2 != 0):        # Abbruchbedingung
    q  = r//r1;         # Schleifenrumpf
    r2 = r%r1;

    a2 = a0 - q*a1;
    b2 = b0 - q*b1;

    r  = r1;            # Umspeichern von Variablen
    r1 = r2;
    a0 = a1;
    a1 = a2;
    b0 = b1;
    b1 = b2;

s = str(a0)+'*'+str(a)+' + '+str(b0)+'*'+str(b)+' = '+str(r)
print(s)
```

```
82*456 + -139*269 = 1
```

5 Algebraische Strukturen

Verständnisfragen

1. Ein Ring muss nicht unbedingt ein 1-Element besitzen. Schauen Sie sich noch einmal die Beispiele in Abschnitt 5.2. an. Finden Sie einen Ring ohne 1?

$(m\mathbb{Z},+,\cdot)$ ist ein Beispiel.

2. Wie lautet in $\mathbb{C}$ die $\sqrt{-25}$?

5i.

3. Gilt in $\mathbb{C}: x \cdot \overline{x} = 0 \Leftrightarrow x = 0$?

Ja, denn $x \cdot \overline{x} = x^2$

4. Warum gilt im Körper $\mathbb{Z}/p\mathbb{Z}$ immer $(p-1)(p-1) = 1$?

weil $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \bmod p$

5. Ist ein Ring-Homomorphismus von *R* nach *S* automatisch auch ein Homomorphismus der additiven Gruppen von *R* nach *S*?

Ja.

6. Wenn Sie Schlüssel für einen kryptographischen Algorithmus erzeugen wollen, brauchen Sie einen Zufallszahlengenerator. Warum sind die standardmäßig in Programmiersprachen enthaltenen Zufallszahlengeneratoren nicht dafür geeignet?

Die erzeugten Zufallszahlen sind oft 32 Bit lang, der Schlüsselraum ist daher zu klein.

7. Worin liegt die große Bedeutung der elliptischen Kurven in der Kryptographie?

Bei vergleichbarer Sicherheit sind die Schlüssellängen kleiner und die Performance besser als bei anderen public key Algorithmen.

8. Welche beiden ungelösten mathematischen Probleme liegen den meisten public key Algorithmen zu Grunde?

Das Faktorisierungsproblem für große Zahlen und das Problem des diskreten Logarithmus.

Übungsaufgaben

1. Stellen Sie eine Additions- und Multiplikationstabelle für $\mathbb{Z}/6\mathbb{Z}$ auf. Zeigen Sie, dass $\mathbb{Z}/6\mathbb{Z} \setminus \{0\}$ mit der Multiplikation keine Gruppe bildet.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dies ist keine Gruppe, da z.B. 2, 3 und 4 kein multiplikatives Inverses haben.

2. Ordnen Sie den Elementen der Verknüpfungstafel der S_3 die Elemente der S_3 zu.

   a, b und d sind gegeben. Berechnen Sie zuerst $b^2 = (1\ 2\ 3)^2 = (1\ 3\ 2)$, also ist $c = (1\ 3\ 2)$. Dann $cd = (1\ 3\ 2)(2\ 3) = (1\ 3)$. Daraus folgt $f = (1\ 3)$ und für e bleibt dann nur noch $(1\ 2)$ übrig.

   Die Gruppe S_3 hat einige Untergruppen, kommutative und nicht kommutative. Finden Sie diese?

3. Zeigen Sie, dass $(\mathbb{R}^+,\cdot)$ eine Gruppe bildet.

   $x,y \in \mathbb{R}^+ \Rightarrow x \cdot y \in \mathbb{R}^+$, also ist dies eine Verknüpfung in $\mathbb{R}^+$. Für $x \in \mathbb{R}^+$ ist auch $x^{-1} \in \mathbb{R}^+$ und 1 ist das neutrale Element. Als Teilmenge von $\mathbb{R}$ ist $\mathbb{R}^+$ auch assoziativ.

4. Zeigen Sie, dass im Körper $\mathbb{C}$ gilt: $z \cdot \bar{z} = |z|^2$, $z^{-1} = \dfrac{\bar{z}}{|z|^2}$.

$$z \cdot \bar{z} = (x+iy)(x-iy) = x^2 + y^2 + i(xy - yx) = x^2 + y^2,$$

$$z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{\bar{z}}{|z|^2}.$$

5. Sei $z = 4 + 3i$, $w = 6 + 5i$. Berechnen Sie z^{-1} und $\dfrac{w}{z}$ in der Form $a+bi$.

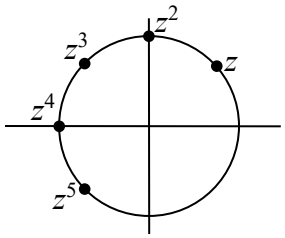
$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{4-3i}{25} = \frac{4}{25} - \frac{3}{25}i, \qquad \frac{w}{z} = \frac{6+5i}{4+3i} = \frac{(6+5i)(4-3i)}{(4+3i)(4-3i)} = \frac{39+2i}{25}.$$

6. Stellen Sie $\frac{1+i}{2-i}$ in der Form $a+bi$ dar.

$$\frac{1+i}{2-i}=\frac{(1+i)(2+i)}{(2-i)(2+i)}=\frac{1}{5}+\frac{3}{5}i$$

7. Im Körper $\mathbb{C}$ der komplexen Zahlen sei $z=\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$. Berechnen Sie und zeichnen Sie in der Gauß'schen Zahlenebene z, z^2, z^3, z^4, z^5.

$$z^2=0+i, z^3=\frac{-\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i, z^4=-1, z^5=\frac{-\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i.$$



Die Zahlen liegen alle auf dem Einheitskreis. Den Grund dafür erfahren Sie am Ende von Kapitel 14 des Buches.

8. Führen Sie bei folgenden Polynomen Division mit Rest durch:

a) in $\mathbb{Z}/2\mathbb{Z}[x]$: $(x^8 + x^6 + x^2 + x)/(x^2 + x)$,
b) in $\mathbb{Z}/2\mathbb{Z}[x]$: $(x^5 + x^4 + x^3 + x + 1)/(x^3 + x^2 + 1)$,
c) in $\mathbb{Z}/5\mathbb{Z}[x]$: $(4x^3 + 2x^2 + 1)/(2x^2 + 3x)$,

und machen Sie jeweils anschließend die Probe.

Ausführlich gerechnet Nummer c): Es hilft, wenn Sie sich die Additions- und Multiplikationstabellen für $\mathbb{Z}/5\mathbb{Z}$ aufschreiben:

$$\begin{array}{l} (4x^3 + 2x^2 + 1)/(2x^2 + 3x) = 2x + 3 \\ \underline{4x^3 + x^2} \\ \quad x^2 + 1 \\ \quad \underline{x^2 + 4x} \\ \quad\quad x + 1 \qquad\qquad = \text{Rest} \end{array}$$

Probe: $(2x^2 + 3x)(2x + 3) + x + 1 = 4x^3 + x^2 + x^2 + 4x + (x+1) = 4x^3 + 2x^2 + 1$

Das Ergebnis von a) lautet $x^6 + x^5 + 1$, das Ergebnis von b) lautet: $x^2 + 1$ Rest x.

9. Zeigen Sie, dass es in $\mathbb{Z}/n\mathbb{Z}[x]$, n keine Primzahl, Polynome vom Grad zwei mit mehr als zwei verschiedenen Nullstellen gibt.

Diese verblüffende Tatsache hängt damit zusammen, dass es in $\mathbb{Z}/n\mathbb{Z}$ von 0 verschiedene Elemente gibt, deren Produkt 0 ist. Ein Beispiel genügt: in $\mathbb{Z}/6\mathbb{Z}$ ist zum Beispiel $2\cdot 3 = 0$. Das quadratische Polynom $(x-2)(x-3)=x^2-2x-3x+2\cdot 3=x^2+x$ in $\mathbb{Z}/6\mathbb{Z}[x]$ hat dann die Nullstellen 2, 3 und 0.

10. Zeigen Sie, dass für $n \in \mathbb{N}$ die Menge $(\mathbb{R}^n, +)$ mit der folgenden Addition eine Gruppe bildet: $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$.

    Das Nullelement ist (0,0,...,0), das Inverse zu $(a_1, a_2, \ldots, a_n)$ ist $(-a_1, -a_2, \ldots, -a_n)$.

    Die Menge ist assoziativ, denn $((a_1,\ldots, a_n) + (b_1,\ldots, b_n)) + (c_1,\ldots, c_n) =$
    $= (a_1 + b_1 + c_1,\ldots, a_n + b_n + c_n) = (a_1,\ldots, a_n) + ((b_1,\ldots, b_n) + (c_1,\ldots, c_n))$.

11. Zeigen Sie, dass die Abbildungen

    a) $f : \mathbb{R}^3 \to \mathbb{R}^2, (x, y, z) \mapsto (x + y, y + z)$

    b) $g : \mathbb{R}^2 \to \mathbb{R}^3, (x, y) \mapsto (x, x + y, y)$

    Homomorphismen sind. $\mathbb{R}^2$ beziehungsweise $\mathbb{R}^3$ sind dabei die Gruppen aus der letzten Aufgabe. Berechnen Sie Ker *f* und Ker *g*.

    Die Homomorphieeigenschaft zum Beispiel für *f*:

    $$f(x_1, y_1, z_1) + f(x_2, y_2, z_2) = (x_1 + y_1, y_1 + z_1) + (x_2 + y_2, y_2 + z_2) =$$
    $$(x_1 + x_2 + y_1 + y_2, y_1 + y_2 + z_1 + z_2) = f(x_1 + x_2, y_1 + y_2, z_1 + z_2).$$

    $\ker f = \{(x, y, z) \mid f(x, y, z) = 0\}$. $f(x, y, z) = 0$ heißt $x + y = 0, y + z = 0$

    $\Rightarrow x = -y, z = -y, \Rightarrow$ Ker $f = \{a(1, -1, 1) \mid a \in \mathbb{R}\}$.

    Ähnlich folgt: Ker $g = \{(0,0)\}$.

12. Zeigen Sie, dass man in der Definition 5.2, Axiom (G2) auf die Forderung der Eindeutigkeit verzichten kann: In einer Gruppe ist das Inverse a^{-1} zu einem Element *a* eindeutig bestimmt.

    Angenommen es gilt $ab = ac$, also *b* und *c* seien Inverse zu *a*. Dann ist $a^{-1}(ab) = a^{-1}(ac)$, wegen des Assoziativgesetzes also auch $(a^{-1}a)b = (a^{-1}a)c$ und damit $b = c$.

13. Zeigen Sie, dass in einer ISBN-Nummer jeder einzelne Ziffernfehler und auch das Vertauschen der Prüfziffer mit einer der vorderen Ziffern entdeckt werden können.

    Einzelner Ziffernfehler:

    Hat die Ziffer an der Stelle *i* richtig den Wert *a* und den falschen Wert *b*, so ergibt die Differenz der Prüfziffern (gerechnet in GF(11)): $ai - bi = (a - b)i \neq 0$, da $a - b \neq 0$ ist.

    Vertauschung der Prüfziffer mit der Ziffer an der Stelle i

    Die richtige Prüfziffer lautet: $1a_1 \cdots + ia_i + \cdots 9a_9 = p$

    Sind a_i und *p* verschieden und wird die Vertauschung von a_i mit *p* nicht erkannt, so müsste gelten: $1a_1 \cdots + ip + \cdots 9a_9 = a_i$.

Die Differenz der beiden Zeilen ergibt: $i(a_i - p) = p - a_i$. Da $a_i - p \neq 0$ ist folgt daraus $i = -1$, also $i = p - 1 = 10$ in GF(11). Der maximale Wert für *i* ist aber 9.

14. In $\mathbb{R}^2$ bildet die Menge der (*x*,*y*) mit $y = mx + t$ eine Gerade. Dabei ist *m* der Anstieg und *t* der *y*-Abschnitt. Untersuchen Sie jetzt Geraden über dem Körper GF(*p*), also in GF(*p*)^2:

a) Zeigen Sie, dass jede Gerade in GF(*p*)^2 genau *p* Punkte enthält.

b) Verwenden Sie ein Mathematikwerkzeug um für einige Primzahlen und für einige *m*, *t* die Punkte der Geraden zu zeichnen. Nehmen Sie zum Beispiel *p* = 31, $m = 1, 2, 13, 16(=\frac{1}{2}), 29(=-2)$ und *t* = 0, 5. Vergleichen Sie die Zeichnungen mit den entsprechenden Geraden in $\mathbb{R}^2$.

Zu a):
Ist $x_1 \neq x_2$, so ist auch $mx_1 + t \neq mx_2 + t$ und umgekehrt. Die Gerade hat also genauso viele Punkte wie GF(*p*).

Zu b):
Der folgende sage Code zeichnet die Gerade 2*x* +5

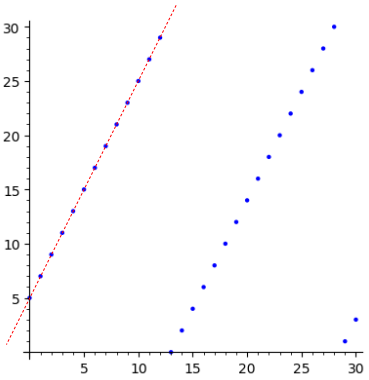
```
def gerade(m,t,p):    # Gerade mx+t in GF(p)
    GFp = IntegerModRing(p)
    m = GFp(m)
    t = GFp(t)
    points = []

    for x1 in GFp:
        points.append([x1,m*x1+t])

    return list_plot(points, aspect_ratio = 1)

show(gerade(2,5,31))
```

Das Bild sieht so aus:



Die Gerade 2*x*+5 über den reellen Zahlen ist darin rot gestrichelt eingezeichnet.

6 Vektorräume

Verständnisfragen

1. Ist eine Gerade im $\mathbb{R}^3$, welche nicht durch den Ursprung geht, ein Vektorraum?

Nein, Der Ursprung muss in jedem Vektorraum enthalten sein.

2. Gibt es einen Vektorraum der echter Unterraum des $\mathbb{R}^2$ ist und der die x-Achse echt umfasst?

Nein, nur Dimension 1 (x-Achse) oder Dimension 2 ($\mathbb{R}^2$) sind möglich.

3. Ist der $\mathbb{Q}^3$ ein Untervektorraum des $\mathbb{R}^3$?

Nein, die Räume sind nicht vergleichbar, da verschiedene Skalarenkörper!

4. Sind $\mathbb{R}^4$ und $\mathbb{C}^2$ als Vektorräume isomorph? Kann es eine lineare Abbildung zwischen $\mathbb{R}^4$ und $\mathbb{C}^2$ geben?

Auch wenn die Versuchung groß ist, die Komponenten aufeinander abzubilden: da die Skalarenkörper verschieden sind, ist dies keine lineare Abbildung und damit auch kein Isomorphismus.

5. Gibt es Vektorräume mit Basen, die verschieden viele Elemente haben?

Nein, je zwei Basen haben gleich viele Elemente.

6. Richtig oder falsch: Wählt man aus einem unendlich-dimensionalen Vektorraum V endlich viele Elemente aus, so bildet der Span dieser Elemente einen endlich dimensionalen Teilraum von V.

Der Span einer Menge von Vektoren ist immer ein Vektorraum, und die Dimension kann nicht größer sein als die erzeugende Menge. Also: ja.

7. Lässt sich eine surjektive lineare Abbildung vom $\mathbb{R}^n$ auf den $\mathbb{R}^n$ immer invertieren?

Ja, denn wegen dim Im + dim Ker = n ist der Kern 0 und die Abbildung daher auch injektiv.

Übungsaufgaben

1. Zeigen Sie, dass die Abbildungen

   a) $f:\mathbb{R}^3 \to \mathbb{R}^2, (x,y,z) \mapsto (x+y, y+z)$

   b) $g:\mathbb{R}^2 \to \mathbb{R}^3, (x,y) \mapsto (x, x+y, y)$

   linear sind. Berechnen Sie Ker *f* und Ker *g*.

   Diese Aufgabe habe ich schon im Kapitel 5 gestellt: Dort wurde berechnet, dass die beiden Abbildungen Gruppenhomomorphismen sind. Zur Linearität fehlt noch:

   $f(\lambda(x,y,z)) = f(\lambda x, \lambda y, \lambda z) = \big(\lambda(x+y), \lambda(y+z)\big) = \lambda(x+y, y+z) = \lambda f(x,y,z)$, bzw.
   $g(\lambda(x,y)) = g(\lambda x, \lambda y) = \big(\lambda x, \lambda(x+y), \lambda y\big) = \lambda(x, x+y, y) = \lambda g(x,y)$.

2. Die Gleichung $y = 3x+4$ lässt sich als Gerade im $\mathbb{R}^2$ interpretieren:
   $g = \{(x,y) \mid y = 3x+4\}$, $a, b \in \mathbb{R}^2$. Suchen Sie Vektoren a, b in $\mathbb{R}^2$ mit $g = \{a + \lambda b \mid \lambda \in \mathbb{R}\}$.

   Wähle für a einen Punkt auf der Geraden, für b die Differenz zweier Punkte der Geraden,

   zum Beispiel: $g = \begin{pmatrix} 0 \\ 4 \end{pmatrix} + \lambda \left(\begin{pmatrix} 0 \\ 4 \end{pmatrix} - \begin{pmatrix} -4/3 \\ 0 \end{pmatrix} \right)$.

3. Jeder Graph einer Geraden $y = mx+c$ hat eine Darstellung in der Form $g = \{a + \lambda b \mid \lambda \in \mathbb{R}\}$. Bestimmen Sie für diese Darstellung Vektoren a, b. Gibt es umgekehrt zu jeder Geraden g im $\mathbb{R}^2$ eine Darstellung als Graph einer Geraden $y = mx+c$?

   Die Punkte $(0, c)$ und $(1, m+c)$ liegen auf der Geraden. Darum ist zum Beispiel $g = \{(0, c) + \lambda(1, m)\}$.

   Der Richtungsvektor der Geraden kann nie in y-Richtung zeigen, dies wäre m = unendlich.

4. Prüfen Sie die Vektorraumbedingungen (V1) bis (V4) für $\mathbb{R}^3$ nach.

   Das lässt sich komponentenweise leicht nachrechnen, ähnlich wie in Aufgabe 9 aus Kapitel 5.

5. Überlegen Sie, ob $\mathbb{R}^2$ mit der üblichen Addition und mit der Skalarmultiplikation $\lambda \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ y \end{pmatrix}$ ein Vektorraum ist.

   Nein: Ein Gegenbeispiel genügt. z.B. ist $(1+1)\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \neq 1\begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$.

6. Suchen Sie eine lineare Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$ für die gilt Ker f = Im f.

   z.B. $(x, y) \to (y, 0)$: Ker f = Im f = x-Achse. Zu jeder Geraden durch den Ursprung können Sie eine lineare Abbildung finden, so dass diese Gerade Kern und Bild ist.

7. Was sagen Sie zu der Aufgabe 6, wenn ich $\mathbb{R}^2$ jeweils durch $\mathbb{R}^5$ ersetze?

   Eine solche Abbildung kann nicht existieren, da dim Ker + dim Im = 5 nicht möglich ist, wenn Kern und Bild gleich sind.

8. Die Vektoren $\begin{pmatrix} 3 \\ 5 \end{pmatrix}$ und $\begin{pmatrix} 2 \\ 4 \end{pmatrix}$ bilden eine Basis B des $\mathbb{R}^2$. Sei $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$.

   Berechnen Sie die Koordinaten von $\begin{pmatrix} x \\ y \end{pmatrix}$ in der Basis B.

   Es muss λ, μ berechnet werden, so dass gilt: $\begin{pmatrix} x \\ y \end{pmatrix} = \lambda \begin{pmatrix} 3 \\ 5 \end{pmatrix} + \mu \begin{pmatrix} 2 \\ 4 \end{pmatrix}$. Dazu ist das lineare Gleichungssystem $3\lambda + 2\mu = x$ und $5\lambda + 4\mu = y$ zu nach λ und μ aufzulösen.

   Das Ergebnis lautet : $\lambda = 2x - y$, $\mu = -5/2\, x + 3/2\, y$.

9. Zeigen Sie: Sind u, v linear unabhängige Vektoren in V, so sind auch $u + v$ und $u - v$ linear unabhängig (machen Sie eine Skizze im $\mathbb{R}^2$!)

   Sei $\lambda(u + v) + \mu(u - v) = 0$. Ausmultiplizieren ergibt: $(\lambda+\mu)u + (\lambda-\mu)v = 0$. Daraus folgt wegen der linearen Unabhängigkeit von u und v: $\lambda+\mu = \lambda-\mu = 0$, also $\lambda = \mu = 0$. Damit sind $u + v$ und $u - v$ linear unabhängig.

7 Matrizen

Verständnisfragen

1. Richtig oder falsch: Sind A und B beliebige Matrizen, dann ist die Multiplikation zwar nicht kommutativ, aber die Produkte $A \cdot B$ und $B \cdot A$ können immer berechnet werden.

Falsch, die Matrizen müssen von der Größe zusammenpassen.

2. Werden die n Basisvektoren im $\mathbb{R}^n$ um verschiedene Faktoren gestreckt, ist dann die dadurch erzeugte Abbildung eine lineare Abbildung?

Ja, die Bilder der Basisvektoren bestimmen die Abbildung.

3. Warum lässt sich eine einfache Verschiebung um einen festen Vektor im $\mathbb{R}^3$ nicht durch eine lineare Abbildung beschreiben?

Da hierbei der Ursprung verschoben wird. Der bleibt aber bei linearen Abbildungen fest.

4. Kann man zwei nicht quadratische Matrizen so multiplizieren, dass eine (quadratische) Einheitsmatrix herauskommt? Wenn ja: Was bedeutet das für die zu den Matrizen gehörigen linearen Abbildungen?

Ja das geht (ist als Verständnisfrage vielleicht etwas dick geraten). Ein Beispiel finden Sie, wenn Sie an die Einheitsmatrix links bzw. oben noch Nullspalten bzw. Nullzeilen hinhängen. Die erste Abbildung (zur zweiten Matrix) ist injektiv, die zweite Abbildung surjektiv, die zusammengesetzte Abbildung ist die Identität. Vergleiche dazu Satz 1.17 b)

5. Gibt es einen Unterschied zwischen der Multiplikation <Matrix>·<Vektor> und <Matrix>·<einspaltige Matrix>?

Nein, kein Unterschied.

6. Warum ist die Matrixmultiplikation assoziativ?

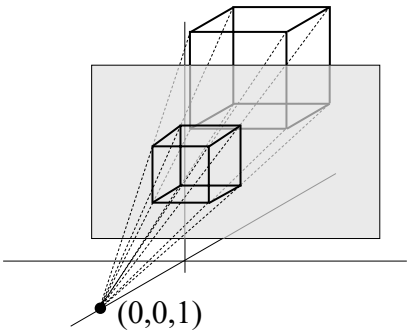
Weil sie als Hintereinanderausführung von Abbildungen interpretiert werden kann.

7. Ist die Menge der gleich großen quadratischen Matrizen mit der Multiplikation eine Gruppe? Ist die Menge der gleich großen quadratischen Matrizen mit der Addition eine Gruppe?

Mit der Multiplikation nicht, da nicht jede Matrix invertierbar ist. Mit der Addition schon, die Menge $\mathbb{R}^{n \times n}$ mit der Addition ist nichts anderes als die additive Gruppe $\mathbb{R}^{n \cdot n}$.

Übungsaufgaben

1. Im folgenden Bild sehen Sie eine Zentralprojektion skizziert, mit deren Hilfe Objekte des Raumes in den $\mathbb{R}^2$ abgebildet werden können. Die Punkte des $\mathbb{R}^3$, die projiziert werden sollen, werden mit dem Projektionszentrum verbunden, das sich im Punkt $(0, 0, 1)$ befindet. Die Projektionsebene ist die x-y-Ebene. Der Schnittpunkt der Verbindungsgeraden mit der Projektionsebene ergibt den darzustellenden Punkt. Berechnen Sie, wohin der Punkt (x, y, z) bei dieser Projektion abgebildet wird. Ist diese Abbildung für alle Punkte des $\mathbb{R}^3$ definiert? Ist sie eine lineare Abbildung?



Die Gerade durch (0,0,1) und (x,y,z) hat die Form $\begin{pmatrix}0\\0\\1\end{pmatrix}+\lambda\left(\begin{pmatrix}0\\0\\1\end{pmatrix}-\begin{pmatrix}x\\y\\z\end{pmatrix}\right)$. Um den Schnittpunkt $(x_0, y_0, 0)$ mit der x-y-Ebene zu bestimmen muss das λ berechnet werden mit

$$\begin{pmatrix}x_0\\y_0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\end{pmatrix}+\lambda\begin{pmatrix}x\\y\\z-1\end{pmatrix}.$$

Aus der dritten Zeile folgt $0=1+\lambda(z-1)$, also $\lambda=\frac{1}{1-z}$. Damit ergibt sich: $x_0=\frac{x}{1-z}, y_0=\frac{y}{1-z}$.

In der Ebene parallel zur x-y-Ebene durch (0,0,1), (die Ebene $z = 1$) ist die Abbildung nicht definiert. Daher kann sie auch keine lineare Abbildung sein.

2. Die Vektoren $\begin{pmatrix}3\\5\end{pmatrix}$ und $\begin{pmatrix}2\\4\end{pmatrix}$ bilden eine Basis B des $\mathbb{R}^2$. Sei $\begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2$. Berechnen Sie die Koordinaten von $\begin{pmatrix}x\\y\end{pmatrix}$ bezüglich der Basis B.

Diese Aufgabe habe ich schon im letzten Kapitel gestellt: Die Lösung $\lambda = 2x - y$, $\mu = -5/2\ x + 3/2\ y$ ist im Zusammenhang mit der nächsten Aufgabe wieder interessant:

3. Bestimmen Sie die Matrix der Abbildung, die $\begin{pmatrix}1\\0\end{pmatrix}$ in $\begin{pmatrix}3\\5\end{pmatrix}$ und $\begin{pmatrix}0\\1\end{pmatrix}$ in $\begin{pmatrix}2\\4\end{pmatrix}$ abbildet und berechnen Sie die Inverse dieser Matrix.

Die Matrix lautet $\begin{pmatrix}3 & 2\\5 & 4\end{pmatrix}$, suchen Sie dann $\begin{pmatrix}x_i\\y_i\end{pmatrix}$ mit $\begin{pmatrix}3 & 2\\5 & 4\end{pmatrix}\begin{pmatrix}x_1\\y_1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$, bzw. mit $\begin{pmatrix}3 & 2\\5 & 4\end{pmatrix}\begin{pmatrix}x_2\\y_2\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$. $\begin{pmatrix}x_i\\y_i\end{pmatrix}$ sind die Bilder der Basis der Umkehrabbildung und daher die Spalten der Matrix. Es ergibt sich: $\begin{pmatrix}2 & -1\\-5/2 & 3/2\end{pmatrix}$.

4. Bestimmen Sie die Matrizen der Abbildungen
   a) $f:\mathbb{R}^3\to\mathbb{R}^2,(x,y,z)\mapsto(x+y,y+z)$
   b) $g:\mathbb{R}^2\to\mathbb{R}^3,(x,y)\mapsto(x,x+y,y)$

a) $A=\begin{pmatrix}1 & 1 & 0\\0 & 1 & 1\end{pmatrix}$, b) $A=\begin{pmatrix}1 & 0\\1 & 1\\0 & 1\end{pmatrix}$. Die Spalten sind die Bilder der Basis.

5. Führen Sie die folgenden Matrixmultiplikationen durch:

a) $\begin{pmatrix}-2 & 3 & 1\\6 & -9 & -3\\4 & -6 & -2\end{pmatrix}\cdot\begin{pmatrix}3 & 1 & 1\\2 & 0 & 1\\0 & 2 & -1\end{pmatrix}=\begin{pmatrix}0 & 0 & 0\\0 & 0 & 0\\0 & 0 & 0\end{pmatrix}$ b) $\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\4 & 0 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\4 & 0 & 0\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\0 & 1 & 0\\4 & 0 & 0\end{pmatrix}$

c) $\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 2\\0 & 4\end{pmatrix}=\begin{pmatrix}1 & 6\\1 & 6\end{pmatrix}$ d) $\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}\cdot\begin{pmatrix}0 & 3\\1 & 3\end{pmatrix}=\begin{pmatrix}1 & 6\\1 & 6\end{pmatrix}$

6. Bestimmen Sie zu den folgenden linearen Abbildungen die dazugehörigen Matrizen und ihren Rang.

a) $f:\mathbb{R}^2\to\mathbb{R}^2,\begin{pmatrix}x_1\\x_2\end{pmatrix}\mapsto\begin{pmatrix}x_1-2x_2\\0\end{pmatrix}$

b) $f:\mathbb{R}^3\to\mathbb{R}^2,\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\mapsto\begin{pmatrix}x_1-x_2+x_3\\2x_1-2x_2+2x_3\end{pmatrix}$

a) $\begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix}$, Rang ist 1 b) $\begin{pmatrix} 1 & -1 & 1 \\ 2 & -2 & 2 \end{pmatrix}$, Rang ist 1.

7. Zeigen Sie, dass für Matrizen $A, B \in K^{n\times m}$ und $C \in K^{m\times r}$ gilt: $(A + B)C = AC + BC$.

Sei $D = (A + B)C$ und $F = AC + BC =$ Ich verwende die Multiplikationsregel (7.5) $d_{ij} = \sum_{k=1}^{m} b_{ik} a_{kj}$ um das Element d_{ij} zu berechnen:

$$d_{ij} = \sum_{k=1}^{m} (a_{ik} + b_{ik}) c_{kj} = \sum_{k=1}^{m} \left(a_{ik} c_{kj} + b_{ik} c_{kj} \right) = \sum_{k=1}^{m} a_{ik} c_{kj} + \sum_{k=1}^{m} b_{ik} c_{kj} = (AC)_{ij} + (BC)_{ij} = f_{ij} .$$

8 Gauß'scher Algorithmus und lineare Gleichungssysteme

Verständnisfragen

1. Welches sind die elementaren Zeilenoperationen in einer Matrix?

Vertauschen, multiplizieren mit einem Skalar und Addition des λ-fachen einer Zeile zu einer anderen.

2. Das Vertauschen zweier Zeilen ändert den Rang einer Matrix nicht. Kann das Vertauschen zweier Spalten den Rang ändern?

Nein, denn der Rang ist die Dimension des Spaltenraums, der ändert sich bei dem Vertauschen der Spalten nicht.

3. Kann bei der Durchführung elementarer Zeilenumformungen eine invertierbare Matrix zu einer nicht-invertierbaren Matrix werden?

Nein, denn der Rang der Matrix ändert sich nicht.

4. Was ist das Pivotelement im Gauß'schen Algorithmus?

Das Element unter dem alles zu 0 gemacht werden soll.

5. Ein lineares Gleichungssystem sei durch die Matrix A und den Ergebnisvektor b bestimmt. Wie können Sie aus der Matrix A die Anzahl der Unbekannten und die Anzahl der Gleichungen ablesen?

Die Anzahl der Unbekannten ist die Spaltenzahl, die Anzahl der Gleichungen die Zeilenzahl.

6. Sei $Ax = 0$ ein homogenes lineares Gleichungssystem. Wie können Sie aus dem Rang von A und der Anzahl der Unbekannten die Dimension des Lösungsraums bestimmen?

Siehe Satz 8.7: Die Dimension ist Anzahl der Unbekannten – Rang A.

7. Die Lösungsmenge eines homogenen linearen Gleichungssystems ist immer ein Vektorraum. Was ist die Lösung eines inhomogenen linearen Gleichungssystems?

Ein aus dem Ursprung verschobener Vektorraum.

8. Die Lösungsmenge einer linearen Gleichung im $\mathbb{R}^3$ beschreibt eine Ebene im $\mathbb{R}^3$. Warum? Welche geometrische Form hat die Lösungsmenge zweier linearer Gleichungen im $\mathbb{R}^3$? Erklären Sie den Zusammenhang zu den Ebenen, welche durch die beiden einzelnen Gleichungen bestimmt werden.

$Ax = 0$ heißt hier Rang 1 (die Matrix hat eine Zeile). Es gibt drei Unbekannte, also ist die Dimension des Lösungsraums 2 (eine Ebene durch den Ursprung), und die Lösung des inhomogenen Systems ist eine aus dem Ursprung verschobene Ebene.

Übungsaufgaben

1. Bestimmen Sie jeweils den Rang der folgenden Matrizen:

$$\begin{pmatrix} 1 & 3 & -2 & 5 & 4 \\ 1 & 4 & 1 & 3 & 5 \\ 1 & 4 & 2 & 4 & 3 \\ 2 & 7 & -3 & 6 & 13 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & -3 & -2 & -3 \\ 1 & 3 & -2 & 0 & -4 \\ 3 & 8 & -7 & -2 & -11 \\ 2 & 1 & -9 & -10 & -3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 2 \\ 4 & 5 & 5 \\ 5 & 8 & 1 \\ -1 & -2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 3 & -7 \\ -6 & 1 \\ 5 & -8 \end{pmatrix}.$$

Die Ränge der Matrizen sind der Reihe nach: 3, 2, 3, 2. z.B. für die erste Matrix:

$$\begin{pmatrix} 1 & 3 & -2 & 5 & 4 \\ 1 & 4 & 1 & 3 & 5 \\ 1 & 4 & 2 & 4 & 3 \\ 2 & 7 & -3 & 6 & 13 \end{pmatrix} \begin{matrix} \\ II-I \\ III-I \\ IV-2I \end{matrix} \rightarrow \begin{pmatrix} 1 & 3 & -2 & 5 & 4 \\ 0 & 1 & 3 & -2 & 1 \\ 0 & 1 & 4 & -1 & -1 \\ 0 & 1 & 1 & -4 & 5 \end{pmatrix} \begin{matrix} \\ \\ III-II \\ IV-II \end{matrix} \rightarrow \begin{pmatrix} 1 & 3 & -2 & 5 & 4 \\ 0 & 1 & 3 & -2 & 1 \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & -2 & -2 & 4 \end{pmatrix} \begin{matrix} \\ \\ \\ IV+2III \end{matrix} \rightarrow \begin{pmatrix} 1 & 3 & -2 & 5 & 4 \\ 0 & 1 & 3 & -2 & 1 \\ 0 & 0 & 1 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Für die zweite Matrix:

$$\begin{pmatrix} 1 & 2 & -3 & -2 & -3 \\ 1 & 3 & -2 & 0 & -4 \\ 3 & 8 & -7 & -2 & -11 \\ 2 & 1 & -9 & -10 & -3 \end{pmatrix} \begin{matrix} \\ II-I \\ III-3I \\ IV-2I \end{matrix} \rightarrow \begin{pmatrix} 1 & 2 & -3 & -2 & -3 \\ 0 & 1 & 1 & 2 & -1 \\ 0 & 2 & 2 & 4 & -2 \\ 0 & -3 & -3 & -6 & 3 \end{pmatrix} \begin{matrix} \\ \\ III-2II \\ IV+3II \end{matrix} \rightarrow \begin{pmatrix} 1 & 3 & -2 & 5 & 4 \\ 0 & 1 & 3 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2. Welche Unterräume des $\mathbb{R}^3$ werden durch die Lösungen der folgenden linearen homogenen Gleichungssysteme bestimmt?

a) $2x_1 - 2x_2 + x_3 = 0$

b) $\begin{aligned} 2x_1 - 2x_2 + x_3 &= 0 \\ x_2 + 3x_3 &= 0 \end{aligned}$

c) $\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 + x_3 &= 0 \\ 2x_1 + x_2 + 2x_3 &= 0 \end{aligned}$

Es sei jeweils A die zugehörige Koeffizientenmatrix uns L der Lösungsraum. Dann gilt:

a) Rang $A = 1 \Rightarrow \dim L = 2$. Eine Basis ist zum Beispiel (0,1,2), (1,1,0).

b) Rang $A = 2 \Rightarrow \dim L = 1$. Die Umwandlung mit dem Gauß'schen Algorithmus liefert die Matrix: $\begin{pmatrix} 1 & 0 & 3{,}5 \\ 0 & 1 & 3 \end{pmatrix}$ und damit als Basisvektor zum Beispiel (–3.5, –3, 1).

c) Rang $A = 2, \Rightarrow \dim L = 1$. Ein Basisvektor ist zum Beispiel (1,0,–1).

3. Bestimmen Sie die Inversen der folgenden Matrizen, falls sie existieren:

$$\begin{pmatrix} 3 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 3 & 0 & 1 \\ 6 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 5 & 0 & 0 \\ -1 & 2 & 0 \\ 4 & 1 & 3 \end{pmatrix}.$$

$A^{-1} = \begin{pmatrix} 1/2 & -1/2 & 0 \\ 0 & 0 & 1 \\ -1/2 & 3/2 & 0 \end{pmatrix}$, B^{-1} existiert nicht (Rang $B = 2$), $C^{-1} = \begin{pmatrix} 2/10 & 0 & 0 \\ 1/10 & 1/2 & 0 \\ -3/10 & -1/6 & 1/3 \end{pmatrix}$

4. Stellen Sie fest, ob das folgende lineare Gleichungssystem lösbar ist und bestimmen Sie gegebenenfalls die Lösungsmenge:

$$\begin{aligned} x_1 &+ 2x_2 &+ 3x_3 &= 1 \\ 4x_1 &+ 5x_2 &+ 6x_3 &= 2 \\ 7x_1 &+ 8x_2 &+ 9x_3 &= 3 \\ 5x_1 &+ 7x_2 &+ 9x_3 &= 4 \end{aligned}$$

Das System hat keine Lösung, da der Gauß'sche Algorithmus liefert: $\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 2/3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$,

d.h. Rang (A,b) > Rang A.

5. Lösen Sie das folgende lineare Gleichungssystem:

$$\begin{aligned} 2x_1 &+ x_2 &+ x_3 &= a_1 \\ 5x_1 &+ 4x_2 &- 5x_3 &= a_2 \\ 3x_1 &+ 2x_2 &- x_3 &= a_3 \end{aligned}$$

wobei einmal $a_1 = 5$, $a_2 = -1$, $a_3 = 3$, und einmal $a_1 = 1$, $a_2 = -1$, $a_3 = 1$ zu wählen sind.

Der Gauß'sche Algorithmus ergibt $\left(\begin{array}{ccc|c} 2 & 1 & 1 & 5 \\ 0 & 1.5 & -7.5 & -13.5 \\ 0 & 0 & 0 & 0 \end{array}\right)$, bzw. $\left(\begin{array}{ccc|c} 2 & 1 & 1 & 5 \\ 0 & 1.5 & -7.5 & -3.5 \\ 0 & 0 & 0 & 2/3 \end{array}\right)$.

Damit existiert im zweiten Fall keine Lösung, im ersten Fall lautet die Gauß-Jordan-Form:
$\left(\begin{array}{ccc|c} 1 & 0 & 3 & 7 \\ 0 & 1 & -5 & -9 \\ 0 & 0 & 0 & 0 \end{array}\right)$, woraus sich als Lösung für das homogene System ergibt:
$\{\lambda \begin{pmatrix} -3 \\ 5 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R}\}$. Eine spezielle Lösung lautet $\begin{pmatrix} 7 \\ -9 \\ 0 \end{pmatrix}$.

6. Welche Ordnung hat der Gauß'sche Algorithmus , wenn Sie das folgende Gleichungssystem auflösen:

$$\begin{pmatrix} a_{11} & a_{12} & 0 & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & a_{23} & 0 & 0 & \cdots & 0 \\ 0 & a_{32} & a_{33} & a_{34} & 0 & \cdots & 0 \\ 0 & 0 & a_{43} & a_{44} & a_{45} & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & a_{n-1,n-2} & a_{n-1,n-1} & a_{n-1,n} \\ 0 & 0 & 0 & 0 & 0 & a_{n,n-1} & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \\ \\ \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \\ \\ \\ b_n \end{pmatrix}$$

Zeigen Sie, dass dieses System immer eindeutig lösbar ist falls für alle i gilt $|a_{ii}| > |a_{i-1,i}| + |a_{i+1,i}|$. Eine solche Matrix heißt "spaltendiagonaldominant".

Dann kann man nämlich die folgenden Umformungen vornehmen, ohne dass irgendwann die 0 im Nenner auftritt (warum?).

Beginnen Sie mit der zweiten Zeile und ziehen Sie für $k = 2$ bis $k = n$ jeweils von der k-ten Zeile das $\frac{a_{k,k-1}}{a_{k-1,k-1}}$ – fache der (k–1)-ten Zeile ab. Danach hat die erweiterte Matrix die Form:

$$\left(\begin{array}{ccccccc|c} a_{11} & a_{12} & 0 & 0 & 0 & \cdots & 0 & b_1 \\ 0 & a_{22} & a_{23} & 0 & 0 & \cdots & 0 & b_2 \\ 0 & 0 & a_{33} & a_{34} & 0 & \cdots & 0 & b_3 \\ 0 & 0 & 0 & 0 & a_{45} & \ddots & \vdots & \\ 0 & 0 & 0 & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & \vdots & \vdots & \ddots & 0 & a_{n-1,n-1} & a_{n-1,n} & \\ 0 & 0 & 0 & 0 & 0 & 0 & a_{nn} & b_n \end{array}\right).$$

Dabei wurden n – 1 elementare Zeilenoperationen durchgeführt. In der zweiten Runde müssen Sie von $k = n$ bis $k = 2$ von der (k–1)-ten Zeile das $\frac{a_{k-1,k}}{a_{k,k}}$ – fache der k-ten Zeile abziehen. Das Ergebnis ist die Gauß-Jordan Form.

Eine elementare Zeilenoperation besteht in dieser einfachen Matrix aus höchstens 1 Division, 3 Multiplikationen und 3 Subtraktionen, hat also konstante Laufzeit. 2(n – 1) solche Operationen ergeben eine lineare Laufzeit: die Ordnung des Algorithmus ist n.

9 Eigenwerte, Eigenvektoren und Basistransformationen

Verständnisfragen

1. Welche geometrische Bedeutung hat die Determinante einer Matrix?

Bis auf das Vorzeichen stellt sie das Volumen des von den Zeilenvektoren aufgespannten Körpers dar.

2. Erläutern Sie den Zusammenhang zwischen der Determinante einer Matrix, dem Rang der Matrix und dem Kern der dazugehörigen linearen Abbildung.

Wenn die Determinante $\neq 0$ ist, hat die Matrix den maximalen Rang und der Kern der linearen Abbildung ist $\{0\}$. Siehe Satz 9.4.

3. Bei einer Drehspiegelung im $\mathbb{R}^3$ wird zunächst an einer Ebene gespiegelt und anschließend um die Achse senkrecht zu dieser Ebene gedreht. Wie viele Eigenvektoren hat eine Drehspiegelung. Welches sind die dazugehörigen Eigenwerte? Gibt es Sonderfälle?

Normalerweise hat die Drehspiegelung genau einen Eigenvektor, die Drehachse. Sonderfälle sind Drehungen um 180° und 360°. Dann ist die Ebene senkrecht zur Drehachse Eigenraum.

4. Ist $\vec{0}$ Eigenvektor zu jedem Eigenwert?

Ja.

5. Ist u ein Eigenvektor zu dem Eigenwert λ und v ein Eigenvektor zu dem Eigenwert μ ($\lambda \neq \mu$), ist dann auch $u + v$ ein Eigenvektor?

Nein, denn dann müsste $f(u + v) = \lambda u + \mu v = k(u + v)$ für ein k sein. Das geht nicht, wenn $\lambda \neq \mu$ ist.

6. Wenn eine Matrix aus dem $\mathbb{R}^{4\times4}$ drei Eigenwerte hat und die Dimension des Eigenraums zum ersten Eigenwert 2 ist, gibt es dann eine Basis aus Eigenvektoren zu der Matrix?

Ja, denn jeder Eigenraum hat mindestens Dimension 1.

7. Richtig oder falsch: Wenn ein Eigenwert der Matrix aus dem $\mathbb{R}^{3\times3}$ einen Eigenraum mit der Dimension 2 hat, so hat die Matrix genau einen weiteren Eigenwert.

Falsch, die Matrix kann auch nur einen einzigen Eigenwert haben.

8. Ist λ Eigenwert einer Matrix A aus $\mathbb{R}^{2\times2}$, kann dann $\operatorname{rang}(A-\lambda E) = 2$ sein?

Nein, $\operatorname{rang}(A-\lambda E)$ ist immer echt kleiner als die Matrixgröße.

9. Ist A eine Matrix aus $\mathbb{R}^{n\times n}$ und $T \in \mathbb{R}^{n\times n}$ eine invertierbare Matrix, hat dann $T^{-1}AT$ die gleichen Eigenwerte wie A?

Ja, da die Matrizen ähnlich sind.

Übungsaufgaben

1. Zeigen Sie: Die Determinante einer 2×2 Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ist genau die Fläche des Parallelogramms, das durch die beiden Zeilenvektoren bestimmt wird.

   Aus der Zeichnung ergeben sich die folgenden Flächen:

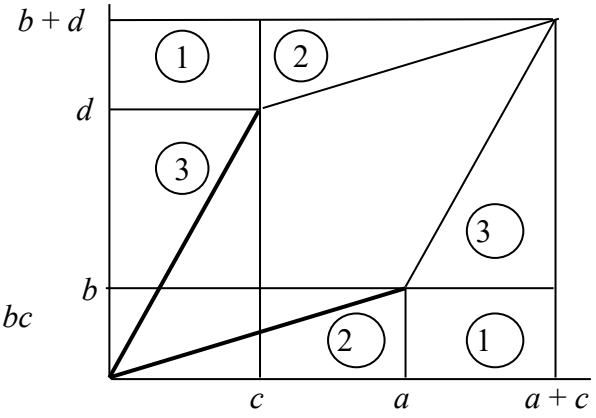
   $1 = bc$

   $2 = ½(ab)$

   $3 = ½(cd)$

   Die Gesamtfläche des großen Rechtecks beträgt $= (a+c)(b+d)$

   Die Parallelogrammfläche ist die Gesamtfläche minus die Einzelflächen $= ad - bc$



2. Berechnen Sie die Determinanten der folgenden Matrizen:

$$\begin{pmatrix} 2 & -6 & 4 & 0 \\ 4 & -12 & -1 & 2 \\ 1 & 7 & 2 & 1 \\ 0 & 10 & 3 & 9 \end{pmatrix}, \quad \begin{pmatrix} 3 & -4 & 0 & 2 \\ 0 & 7 & 6 & 3 \\ 2 & -6 & 0 & 1 \\ 5 & 3 & 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -1 & 2 \\ 2 & 1 & 0 & 1 \\ -3 & 1 & 0 & 1 \\ 2 & 2 & 0 & -1 \end{pmatrix}.$$

   Die beiden ersten Determinanten berechnet man mit dem Gauß'schen Algorithmus. Die Ergebnisse lauten 1560 beziehungsweise –401. Die dritte Determinante erhält man durch Entwicklung nach der dritten Spalte:

$$\begin{vmatrix} 1 & 0 & -1 & 2 \\ 2 & 1 & 0 & 1 \\ -3 & 1 & 0 & 1 \\ 2 & 2 & 0 & -1 \end{vmatrix} = -1 \cdot \begin{vmatrix} 2 & 1 & 1 \\ -3 & 1 & 1 \\ 2 & 2 & -1 \end{vmatrix} = -1 \cdot (-15) = 15 .$$

3. a) Berechnen Sie die Eigenwerte der Matrizen $\begin{pmatrix} 5 & -1 & 2 \\ -1 & 5 & 2 \\ 2 & 2 & 2 \end{pmatrix}$ und $\begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}$.

   b) Geben Sie zu jedem Eigenwert eine Basis des dazugehörigen Eigenraums an. Sind die Matrizen diagonalisierbar? Wenn ja geben Sie die zugehörige Basistransformationsmatrix an.

Zur ersten Matrix:

Das charakteristische Polynom lautet $-\lambda^3+12\lambda^2-36\lambda=(-\lambda)(\lambda^2-12\lambda+36)$. Es hat die Nullstellen $\lambda_1 = 0$ und $\lambda_{2/3} = 6$, also zwei Eigenwerte. Zu diesen gehören die linearen Gleichungssysteme

$$\begin{pmatrix} 5-\lambda & -1 & 2 \\ -1 & 5-\lambda & 2 \\ 2 & 2 & 2-\lambda \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \text{ das heißt:}$$

$$\begin{pmatrix} 5 & -1 & 2 \\ -1 & 5 & 2 \\ 2 & 2 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ und } \begin{pmatrix} -1 & -1 & 2 \\ -1 & -1 & 2 \\ 2 & 2 & -4 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Aus dem ersten System erhält man mit dem Gauß'schen Algorithmus (Rang 2) die Lösung (1,1,–2), das zweite System (Rang 1) hat z.B. die Lösungen (1,–1,0) und (0,2,–1). Die Matrix ist diagonalisierbar, da sie eine Basis aus Eigenvektoren besitzt, die Transformationsmatrix enthält als Spalten gerade die Basisvektoren:

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

Zur zweiten Matrix:

Das charakteristische Polynom lautet $-\lambda^3+12\lambda+16$. Durch Ausprobieren findet man die Nullstelle –2. Polynomdivision durch λ+2 ergibt $:\lambda^2-2\lambda-8$. Diese Gleichung hat die Nullstellen –2 und 4, also gibt es insgesamt zwei Eigenwerte. Zu lösen sind die linearen Gleichungssysteme (für $\lambda = -2$ bzw. $\lambda = 4$):

$$\begin{pmatrix} 3 & -3 & 3 \\ 3 & -3 & 3 \\ 6 & -6 & 6 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \text{bzw.} \begin{pmatrix} -3 & -3 & 3 \\ 3 & -9 & 3 \\ 6 & -6 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

mit Rang 1 (2-dimensionaler Eigenraum) bzw. Rang 2 (1-dimensionaler Eigenraum). Eine Basis des Eigenraums zu –2 ist {(1,1,0), (0,1,1)}, die zweite Matrix wird mit dem Gauß'schen Algorithmus umgeformt zu $\begin{pmatrix} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix}$, woraus sich als Basis des Eigenraums zu 4 ergibt: (1/2,1/2,1). Die Matrix ist diagonalisierbar, da sie eine Basis aus Eigenvektoren besitzt, die Transformationsmatrix lautet: $T=\begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 1 & 1 & \frac{1}{2} \\ 0 & 1 & 1 \end{pmatrix}$

4. Zeigen Sie, dass sich bei der Hintereinanderausführung zweier Basistransformationen die Transformationsmatrizen multiplizieren: ist T die Transformationsmatrix von B_1 nach B_2, und S die von B_2 nach B_3, so ist TS die Transformationsmatrix von B_1 nach B_3.

$$\text{Sei } v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}_{B_1}, v = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}_{B_2} \quad v = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}_{B_3} . \text{ Dann gilt}$$

$$\text{Sei} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}_{B_1} = T \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}_{B_2}, \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}_{B_2} = S \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}_{B_3} \Rightarrow \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}_{B_1} = TS \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}_{B_3} .$$

und damit TS die gesuchte Transformationsmatrix.

5. Zeigen Sie, dass, die Äquivalenzrelation "gleich orientiert" die Menge der Basen des $\mathbb{R}^n$ in genau zwei Äquivalenzklassen einteilt.

   Seien A und B verschieden orientiert und A und C verschieden orientiert. Zu zeigen ist dann, dass B und C gleich orientiert sind. Ist T die Transformationsmatrix von A nach B und U die Transformationsmatrix von A nach C so haben beide die Determinante –1. Ist noch S die Transformationsmatrix von B nach C so gilt nach Aufgabe 4: $TS = U$, also $\det T \cdot \det S = \det U$, das heißt $-1 \cdot \det S = -1$, damit $\det S = 1$, das heißt B und C sind gleich orientiert.

6. Warum vertauscht ein Spiegel links und rechts, nicht aber oben und unten?

   Ein Spiegel vertauscht rechts und links genauso wenig wie oben und unten, er vertauscht nur vorne und hinten. Das können Sie überprüfen, indem Sie zwei Gegenstände im Spiegel anschauen, die verschieden weit vom Spiegel entfernt sind. Das Vertauschen von vorne und hinten ändert aber die Blickrichtung meines Spiegelbildes, es schaut mir gerade ins Gesicht. Da links und rechts aber subjektive Begriffe sind (im Gegensatz zu oben und unten), die von der Blickrichtung des Subjekts abhängen, ist das Rechts meines Spiegelbildes genau anders herum als meines.

   Können Sie mir jetzt erklären, warum der Spiegel aus normaler Schrift Spiegelschrift macht?

10 Skalarprodukt und orthogonale Abbildungen

Verständnisfragen

1. Bildet ein Vektorraum mit der Addition und mit einem Skalarprodukt als Multiplikation einen Ring?

Nein, denn die Skalarmultiplikation liefert keinen Vektor.

2. Warum kann ein Skalarprodukt nur für reelle Vektorräume sinnvoll erklärt werden?

Weil eine Anordnung auf dem Skalarenkörper notwendig ist.

3. Erklären Sie den Zusammenhang zwischen Skalarprodukt und Norm.

Jedes Skalarprodukt liefert eine Norm durch die Vorschrift $\|u\| = \sqrt{< u, u >}$.

4. Wenn eine lineare Abbildung im $\mathbb{R}^3$ die Winkel zwischen allen Vektoren erhält, so erhält sie auch die Länge der Vektoren und ist somit eine orthogonale Abbildung.

Nein. Ein Gegenbeispiel ist die Streckung.

5. Welche Typen von orthogonalen Abbildungen gibt es im $\mathbb{R}^3$.

Drehungen um eine Achse, Spiegelungen an einer Ebene und die Kombination davon: Drehspiegelungen.

6. Die Drehung im $\mathbb{R}^2$ hat die Matrix $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$, die Spiegelung die Matrix $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$. Und welche Abbildungen werden durch $\begin{pmatrix} -\cos\alpha & \sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ bzw. durch $\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$ beschrieben?

Die erste hat Determinante -1 ist also eine Spiegelung, die zweite hat Determinante 1, ist also eine Drehung. Wenn Sie anschauen wohin dabei (1,0) jeweils abgebildet wird (vergleiche das Bild 7.3) finden Sie auch Spiegelachse bzw. Drehwinkel.

7. Die Translation ist zwar keine lineare Abbildung. Aber ist sie eine „orthogonale“ Abbildung in dem Sinn, dass sie Längen von Vektoren und Winkel zwischen Vektoren erhält?

Längen werden erhalten, aber Winkel nicht.

8. Warum ist es manchmal sinnvoll mit homogenen Koordinaten zu rechnen?

Wenn man Translationen durch Matrizen beschreiben will.

Übungsaufgaben

1. Bestimmen Sie eine lineare Gleichung, deren Lösungsmenge die Ebene beschreibt, die durch die Punkte (1,0,1), (2,1,2) und (1,1,3) im $\mathbb{R}^3$ bestimmt ist.

   Die Ebene steht senkrecht zu (2,1,2) – (1,0,1) = (1,1,1) und zu (1,1,3) – (1,0,1) = (0,1,2) . Eine gemeinsame Senkrechte zu diesen beiden Vektoren stellt den Normalenvektor dar. Am leichtesten berechnet man diese mit dem so genannten Kreuzprodukt, das ich Ihnen aber vorenthalten habe. Daher müssen Sie die beiden Gleichungen $\langle (1,1,1),(x_1,x_2,x_3)\rangle = 0$ und $\langle (0,1,2),(x_1,x_2,x_3)\rangle = 0$ auflösen und erhalten als eine Lösung zum Beispiel u = (1, –2, 1). Die gegebene Ebene steht senkrecht zu u und geht durch v = (1,0,1), die beschreibende Gleichung hat also die Form (vergleichen Sie die Bemerkungen nach dem Beweis von Satz 10.5):

   $$E = \{x \in \mathbb{R}^3 \mid \langle u,x\rangle - \langle u,v\rangle = 0\} = E = \{x \in \mathbb{R}^3 \mid x_1 - 2x_2 + x_3 - 2 = 0\}.$$

2. Bestimmen Sie den Winkel zwischen den Vektoren (2,1,-1) und (1,2,1).

   Wegen $\langle u,v\rangle = \|u\|\|u\| \cdot \cos\alpha$ gilt $5 = \sqrt{6} \cdot \sqrt{6} \cdot \cos\alpha$, also $\alpha = \cos^{-1}(5/6) = 33.56°$.

3. Bestimmen Sie den Winkel zwischen der Diagonale eines Würfels und einer an die Diagonale angrenzenden Kante.

   Zu berechnen ist also zum Beispiel der Winkel zwischen (1,1,1) und (0,0,1). Genau wie in der letzten Aufgabe erhalten wir $1 = \sqrt{3}\cos\alpha$ und daraus $\alpha = 54.74°$.

4. Ergänzen Sie den Vektor $\left(1/2, 1/2, 1/\sqrt{2}\right)$ zu einer Orthonormalbasis des $\mathbb{R}^3$.

   Die Ebene senkrecht dazu hat die Form $\frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{\sqrt{2}}x_3 = 0$. Darin liegt zum Beispiel (1,–1,0). Ein Vektor dieser Ebene, der auch noch senkrecht zu (1,–1,0) ist, muss also auch noch die Gleichung $1x_1 - 1x_2 = 0$ erfüllen. Eine Lösung lautet $\left(1,1,-\sqrt{2}\right)$. Damit sind $\left(\frac{1}{2},\frac{1}{2},\frac{1}{\sqrt{2}}\right)$, (1,–1,0), $\left(1,1,-\sqrt{2}\right)$ paarweise orthogonal. Sie müssen noch normalisiert werden, indem man sie durch ihren Betrag dividiert. Der erste Vektor hat bereits Länge 1, der Betrag des zweiten ist $\sqrt{2}$, der des dritten 2 . Damit hat die Orthonormalbasis die Gestalt: $\left(\frac{1}{2},\frac{1}{2},\frac{1}{\sqrt{2}}\right),\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right),\left(\frac{1}{2},\frac{1}{2},\frac{-1}{\sqrt{2}}\right)$.

5. Beweisen Sie: sind die Vektoren $v_1, v_2, ..., v_n$ paarweise orthogonal, so sind sie auch linear unabhängig.

   Es sollte noch die Bedingung dazu: $v_1, v_2, ..., v_n$ alle ungleich 0. Angenommen die v_i sind doch linear abhängig. Ohne Einschränkung kann dann angenommen werden, dass gilt: $v_1 = \lambda_2 v_2 + \lambda_3 v_3 + ... + \lambda_n v_n$. Auf Grund der Linearitätseigenschaften des Skalarprodukts und der Orthogonalität folgt dann:

   $$\langle v_1, v_1 \rangle = \langle v_1, \lambda_2 v_2 + \lambda_3 v_3 + ... + \lambda_n v_n \rangle = \lambda_2 \langle v_1, v_2 \rangle + ... + \lambda_n \langle v_1, v_n \rangle = 0$$

   also $v_1 = 0$, im Widerspruch zur Annahme.

6. Welchen Typ von Abbildung erhält man im $\mathbb{R}^3$, wenn man nacheinander eine Drehung, 2 Spiegelungen, 2 Drehungen und noch 4 Spiegelungen ausführt?

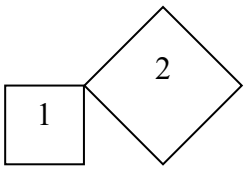
   Nur die Determinante ist interessant, und diese multiplizieren sich. Die Determinante der Abbildung ist $1 \cdot (-1)^2 \cdot 1^2 \cdot (-1)^4 = 1$. Es handelt sich also um eine Abbildung vom Typ A, eine Drehung.

7. Welche der folgenden Matrizen sind orthogonal?

   a) $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{\sqrt{2}} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{\sqrt{2}} \end{pmatrix}$ b) $\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ c) $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{5}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{2} & \frac{1}{6} & \frac{1}{6} & -\frac{5}{6} \\ \frac{1}{2} & \frac{1}{6} & -\frac{5}{6} & \frac{1}{6} \end{pmatrix}$

   Sie müssen nur überprüfen, ob $AA^T = E$ ist. Dies ist bei der zweiten und dritten Matrix der Fall.

8. Bestimmen Sie die homogene Matrix der Abbildung, welche das Quadrat 1 mit der Kantenlänge 1 und Ursprung links unten in das Quadrat 2 abbildet.

   Zunächst wird um 45° gedreht, dann um den Faktor $\sqrt{2}$ gestreckt und schließlich eine Translation nach $(\sqrt{2}, \sqrt{2})$ durchgeführt. Das cos 45° = sin 45° = $1/\sqrt{2}$, hat die Dreh-Streckungsmatrix (in gewöhnlichen Koordinaten) die Form $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ und daher die homogene Matrix die Form:

$$\begin{bmatrix} 1 & -1 & \sqrt{2} \\ 1 & 1 & \sqrt{2} \\ 0 & 0 & 1 \end{bmatrix}.$$

9. Leiten Sie für die Norm $\|u\| := \sqrt{\langle u,u \rangle}$ aus der Cauchy-Schwarz'schen Ungleichung $|\langle u,v \rangle| \le \|u\| \cdot \|v\|$ die Dreiecksungleichung $\|u+v\| \le \|u\| + \|v\|$ her.

   Wir untersuchen das Quadrat der Dreiecksungleichung und erhalten:

   $$\|u+v\|^2 = \langle u+v, u+v \rangle = \langle u,u \rangle + \langle v,v \rangle + \langle u,v \rangle + \langle v,u \rangle \le \|u\|^2 + \|v\|^2 + 2\|u\|\|v\| = \left(\|u\| + \|v\|\right)^2.$$

10. Ist A eine symmetrische Matrix, das heißt $A = A^T$, so sind Eigenvektoren zu verschiedenen reellen Eigenwerten orthogonal.

    Es ist

    $$\lambda_1 \langle v_1, v_2 \rangle = \langle \lambda_1 v_1, v_2 \rangle = \langle Av_1, v_2 \rangle = v_1^T A^T v_2,$$
    $$\lambda_2 \langle v_1, v_2 \rangle = \langle v_1, \lambda_2 v_2 \rangle = \langle v_1, Av_2 \rangle = v_1^T A v_2,$$

    und wegen $A = A^T$ ist das das Gleiche.

11 Graphentheorie

Verständnisfragen

1. Ein zusammenhängender Graph ist ein Baum, wenn er einen Knoten mehr hat als Kanten. Warum ist in diesem Satz der Zusammenhang wichtig?

Einfaches Gegenbeispiel: Drei Punkte in einem Dreieck und ein weiterer Punkt.

2. Wenn Sie in einem Wurzelbaum einen anderen Knoten zur Wurzel erklären, erhalten Sie wieder einen Wurzelbaum. Kann es sein, dass die beiden Wurzelbäume eine unterschiedliche Anzahl von Blättern haben?

Ja. Zum Beispiel Knoten a,b,c, Kanten $[a,b]$,$[b,c]$.

3. Jede Kantenfolge k von x nach y in einem Graphen enthält einen Weg w von x nach y. Natürlich ist w kürzer oder höchstens gleich lang wie k. Kann es einen Weg von x nach y geben, der länger ist als w?

Ja.

4. Wird ein gerichteter Graph automatisch zu einem Graphen, wenn man die Pfeile an den Kanten weglässt?

Nein, es könnten dann zwei Knoten durch zwei Kanten verbunden sein.

5. Wird ein Graph automatisch zu einem gerichteten Graphen, wenn man jeder Kante eine Richtung zuordnet?

Ja.

6. Kann man eine partielle Ordnung auf einer endlichen Menge durch einen Graphen oder durch einen gerichteten Graphen darstellen?

Ja, durch einen gerichteten Graphen: Die Knoten sind die Elemente der Menge, $[x,y]$ ist eine gerichtete Kante genau dann wenn $x < y$.

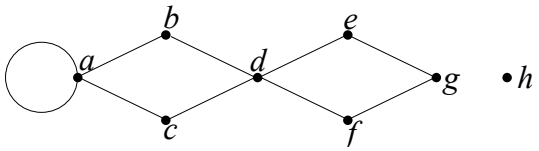
7. In einem gerichteten Graphen kann es zwei gerichtete Kanten zwischen den Knoten x und y geben. Kann es auch zwei gerichtete Kanten zwischen x und x geben?

Nein!

Übungsaufgaben

1. Schreiben Sie für den folgenden Graphen *G* den Grad jedes Knotens auf. Wie viele gerade und ungerade Knoten (= Knoten geraden beziehungsweise ungeraden Grades) enthält *G*?

   Stellen Sie die Adjazenzmatrix für *G* auf.



   Es ist $d(a,d)=4, d(b,c,e,f,g)=2, d(h)=0$. Die Adjazenzmatrix lautet (nur die obere Hälfte, sie ist symmetrisch):

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*
a	1	1	1	0	0	0	0	0
b		0	0	1	0	0	0	0
c			0	1	0	0	0	0
d				0	1	1	0	0
e					0	0	1	0
f						0	1	0
g							0	0
h								0

2. Ist es möglich, dass sich auf einer Party 9 Personen befinden, von denen jede genau fünf andere kennt?

   Nein: Sind in einem Graphen die Personen die Knoten und die Kenntnis die Kanten, so hat der Graph 9 Knoten und jeder Knoten hätte Grad 5. Die Anzahl der Knoten ungeraden Grades in einem Graphen ist aber immer gerade.

3. *G* sei ein Graph mit *n* Knoten und $n-1$ Kanten. Zeigen Sie, dass *G* mindestens einen Endknoten oder einen isolierten Knoten (ein Knoten vom Grad 0) enthält.

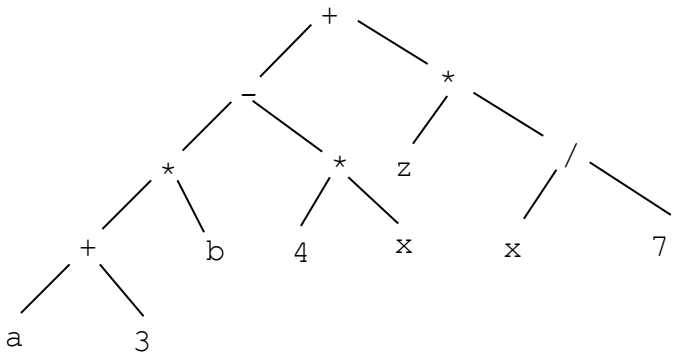
   Angenommen das ist nicht der Fall, dann ist $d(x) \geq 2$ für alle Knoten *x* und daher $\sum d(x) \geq 2n$. Es gilt aber $\sum d(x) = 2(\text{Anzahl der Kanten}) = 2(n-1)$, ein Widerspruch.

4. Zeichnen Sie den Syntaxbaum für den folgenden Ausdruck auf:

```
c = (a+3)*b - 4*x + z*x/7;
```

   Besuchen Sie die Knoten des Baumes mit den drei Verfahren Inorder, Preorder und Postorder.

   Preorder:
   `+-*+a3b*4x*z/x7`
   Inorder:
   `a+3*b-4*x+z*x/7`
   Postorder:
   `a3+b*4x*-zx7/*+`



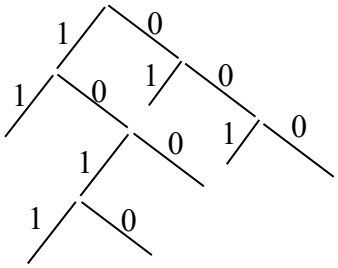
5. Überprüfen Sie, ob die Codes, die aus den folgenden Worten bestehen, Präfixcodes sind und zeichnen Sie gegebenenfalls den zugehörigen binären Baum.:

   a) 11, 1010, 1011, 100, 01, 001, 000

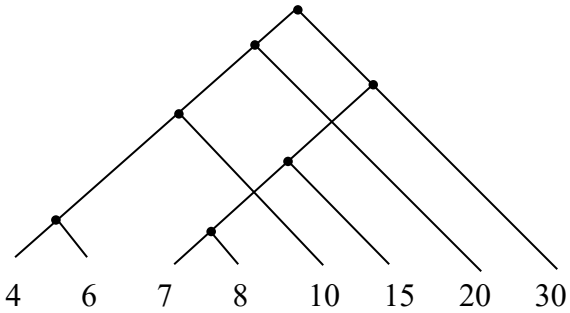
   b) 00, 010, 011, 10, 110, 111, 0110, 0111

   b) ist kein Präfixcode, denn 011 ist Anfang von 0110.

   Der Baum zum Präfixcode a) sieht wie folgt aus:



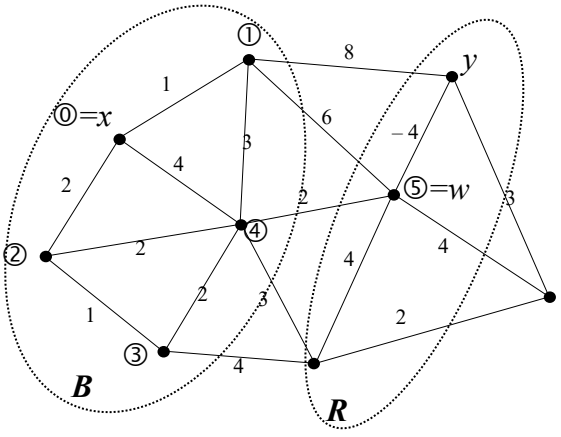
6. Konstruieren Sie einen Präfixcode für das Alphabet {*a*, *b*, *c*, *d*, *e*, *f*, *g*, *h*} bei der folgenden Häufigkeitsverteilung {4, 6, 7, 8, 10, 15, 20, 30} (*a* = 4%, *b* = 6%, ... , *h* = 30%).



   Präfixcode: a = 0000, b = 0001, c = 1000, d = 1001, e = 001, f = 101, g = 01, h = 11

7. Der Algorithmus von Dijkstra zum Finden kürzester Wege in bewerteten Graphen setzt voraus, dass die Entfernung zwischen zwei Knoten nicht negativ ist. Warum ist das so? Geben Sie ein Beispiel eines bewerteten Graphen an, in dem diese Bedingung nicht erfüllt ist, und in dem daher der Algorithmus versagt.

   Ist eine Entfernung negativ, so kann ein Weg zu einem Knoten *w* im Rand *R* für den $l_R(w)$ minimal ist, durch einen Umweg möglicherweise noch verkürzt werden, *w* kann also nicht zu *B* hinzugenommen werden. Als Beispiel die Abbildung zu dem Dijkstra Algorithmus aus dem Buch, wobei eine Entfernung negativ gewählt wurde. Nach dem Algorithmus wird *w* zu *B* dazu genommen, der kürzeste Weg zu *w* geht aber über *y*, und dieser Weg ist noch nicht bekannt.

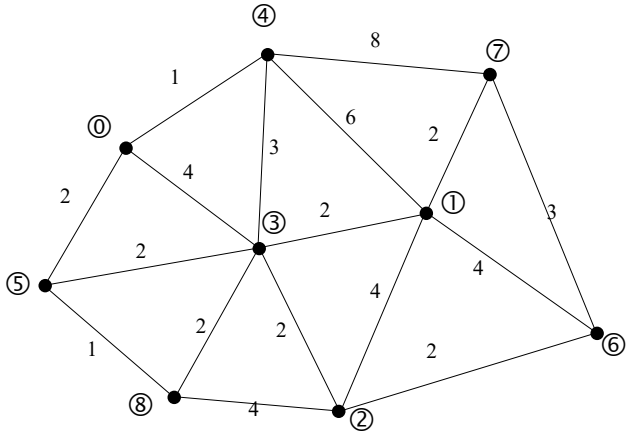


8. Gegeben ist die folgende Adjazenzmatrix eines bewerteten Graphen:

$$\begin{pmatrix} 0 & 0 & 0 & 4 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 2 & 6 & 0 & 4 & 2 & 0 \\ 0 & 4 & 0 & 2 & 0 & 0 & 2 & 0 & 4 \\ 4 & 2 & 2 & 0 & 3 & 2 & 0 & 0 & 2 \\ 1 & 6 & 0 & 3 & 0 & 0 & 0 & 8 & 0 \\ 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 4 & 2 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 0 & 8 & 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 2 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

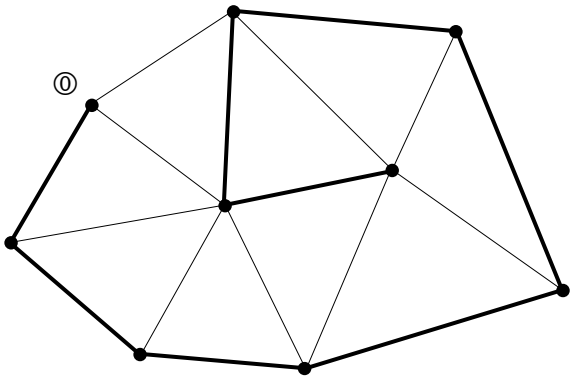
Der Matrixeintrag a_{ij} enthält gerade die Länge des Weges vom Knoten i zum Knoten j. Versuchen Sie ein überschneidungsfreies Bild des Graphen zu zeichnen. Bestimmen Sie ausgehend vom ersten Knoten die kürzesten Wege zu den anderen Knoten. Zeichnen Sie in den Graphen spannende Bäume ein, die entstehen, wenn man ausgehend vom ersten Knoten Breitensuche beziehungsweise Tiefensuche durchführt.

Haben Sie lange dazu gebraucht? Es ist natürlich viel leichter von einem gegebenen Graphen die Adjazenzmatrix aufzustellen als umgekehrt. Dies ist der gleiche Graph wie in der Aufgabe 7, die Punkte sind etwas anders nummeriert:

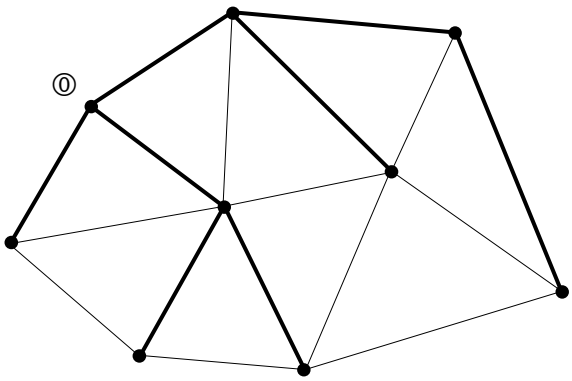


Beispiele für spannende Bäume (beginnend beim Knoten 0) in diesem Graphen bei

Tiefensuche:



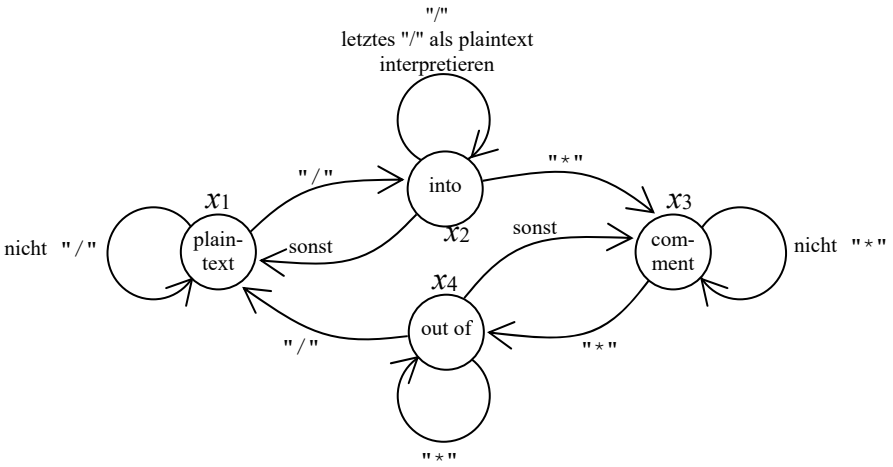
Breitensuche:



9. Der Automat aus Abbildung 11.19 ist noch nicht ganz perfekt. Wenn jemand auf die Idee kommt folgenden Text zu schreiben:

```
a//* das ist eine Division */b
```

dann versagt er. Vervollständigen Sie den Automaten, so dass er auch damit zurecht kommt!



An den Knoten into und out of müssen noch zwei Bögen angebracht werden. Bei der Implementierung muss man darauf achten, dass beim mehrfachen Lesen von "/" jeweils das letzte noch zum Plaintext gerechnet werden muss.

10. Zeigen Sie: Ein azyklischer bewerteter Graph, der genau eine Quelle und eine Senke hat ist schwach zusammenhängend.

Angenommen, der Graph ist nicht schwach zusammenhängend. Dann besteht er aus mindestens zwei Komponenten. Jede dieser Komponenten ist azyklisch, und daher hat jede dieser Komponenten eine Quelle und eine Senke. Damit gibt es mindestens 2 Quellen und zwei Senken.

http://www.springer.com/978-3-658-26523-6

Mathematik für Informatiker
Ein praxisbezogenes Lehrbuch
Hartmann, P.
2019, XII, 643 S. 186 Abb., Softcover
ISBN: 978-3-658-26523-6