Skript zur Vorlesung

Diskrete Mathematik

Wintersemester 2012/2013

Prof. Dr. Steffen Reith
Steffen.Reith@hs-rm.de

Hochschule RheinMain
Fachbereich Design Informatik Medien

Erstellt von:	Steffen Reith
Zuletzt überarbeitet von:	Steffen Reith
Email:	Steffen.Reith@hs-rm.de
Erste Version vollendet:	Juli 2007
Version:	1231
Date:	2013-02-10

Die ganzen Zahlen hat der liebe Gott
gemacht, alles andere ist Menschenwerk.

Leopold Kronecker

Die Mathematiker sind eine Art Franzosen: Redet man
zu ihnen, so übersetzen sie es in ihre Sprache,
und dann ist es alsbald etwas anderes.

Johann Wolfgang von Goethe

When you aim for perfection you will
discover it is a moving target.

Weisheit aus einem Glückskeks

Dieses Skript ist aus der Vorlesung „Diskrete Mathematik“ des Master-Studiengangs Informatik an der Fachhochschule Wiesbaden hervorgegangen. Ich danke allen Höreren dieser Vorlesung für konstruktive Anmerkungen und Verbesserungen. Besonders hervorzuheben sind hier Martin van Wickeren, Patrick Vogt, Michael Kranz, Carola Henzel, Fabio Campos, Thomas Frenken, Dan Marinescu und Alexandru Paler, die zahlreiche Verbesserungsvorschläge beigesteuert haben. Naturgemäß ist ein Skript nie fehlerfrei (alle Fehler wurden selbstverständlich nur aus didaktischen Gründen absichtlich eingebaut) und es ändert (mit Sicherheit!) sich im Laufe der Zeit (hoffentlich!). Deshalb bin ich auf weitere Verbesserungvorschläge meiner Studenten angewiesen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Algorithmenverzeichnis

1. Einleitung

Die Informatik ist die Wissenschaft der (systematischen) Verarbeitung von Informationen. Strebt man ein tieferes Verständnis über die Hintergründe von Soft- und Hardwareentwicklung und über das Design von Algorithmen an, so spielen

- mathematische Methoden (z.B. Induktion) und
- formale Beschreibungen und Modelle

eine wichtige Rolle. Alle diese Begriffe beschäftigen sich mit mathematischen Strukturen, die abzählbar unendlich oder endlich, also *diskret*, sind. Damit spielen die Begriffe der Analysis, wie Stetigkeit, Ableitung und Grenzwerte, in der „Mathematik für Informatiker“ oft keine oder nur eine sehr untergeordnete Rolle.
Häufig werden die folgenden Gebiete der diskreten Mathematik zugeordnet:

- Mathematische Logik
- Mengentheorie
- Graphentheorie
- Kombinatorik
- Zahlentheorie
- Kodierungstheorie
- Kryptographie

1.1. Zwei Beispiele

1.1.1. Die Türme von Hanoi

Die Türme von Hanoi wurden von Edouard Lucas[1] im Jahr 1883 bekannt gemacht. Dabei ist ein Turm von acht Scheiben und drei Stäben gegeben (siehe Abbildung 1). Es ist folgende Aufgabe zu lösen: Bewege die Scheiben von Stab A nach Stab C, wobei *nie* eine größere über einer kleineren Scheibe liegen darf. Zum Transport der Scheiben darf Stab B als „Zwischenlager“ verwendet werden. Zusammen mit diesem Spiel wurde die folgende Legende (sinngemäß) verbreitet:

> Es gibt einen Turm mit 64 Scheiben aus Gold, die auf Stäben aus Diamant ruhen. Priester bewegen jeden Tag eine Scheibe nach dem folgenden Schema:
>
> „Wenn Du den Turm der Höhe n von X über Y nach Z bewegen sollst, dann gibt Deinem ältesten Lehrling den Auftrag einen Turm der Höhe $n-1$ von X über Z nach Y zu bewegen, bewege dann selbst die letzte Scheibe von X nach Z. Sodann soll Dein Lehrling seinen Turm von Y über X nach Z bewegen.“
>
> Wenn die Arbeit getan ist, dann geht die Welt unter.

Es ist sicherlich interessant zu wissen, ob die Welt untergeht, bevor diese Vorlesung beendet werden kann. Sollte dies der Fall sein, so würde sich z.B. die Prüfungsvorbereitung wesentlich vereinfachen.
Um einen allgemeinen Zusammenhang zwischen der Turmhöhe und der Anzahl der Scheibenbewegungen zu finden, analysieren wir das Problem für eine beliebige Scheibenzahl und probieren einige (kleine) Turmhöhen von Hand aus. Enthält der Turm gar keine Scheiben ($n = 0$), so braucht man keine Bewegung, für $n = 1$ wird eine Bewegung

[1] Edouard Lucas wurde 1842 in Amiens geboren und starb 1891 in Paris. Er entwickelte einen sehr effizienten Test für Mersenneprimzahlen.

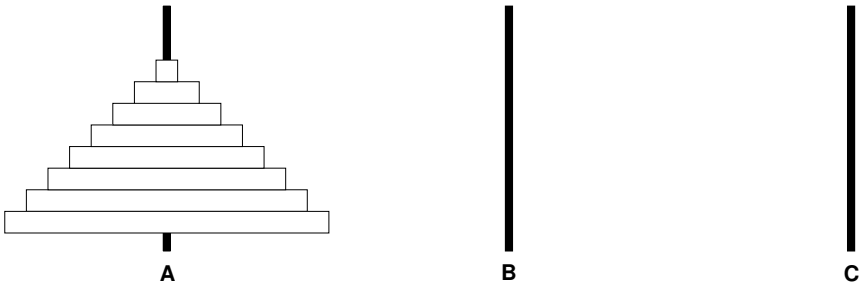


Abbildung 1: Die Türme von Hanoi

notwendig und für $n = 2$ werden maximal drei Schritte notwendig. Für den Fall $n = 3$ ist das Ausprobieren ein wenig schwieriger. Dazu legen wir erst die folgenden Abkürzungen fest: „M“ steht für „Meister“, „L1“ für „Lehrling der ersten Stufe“ und „L2“ für „Lehrling der zweiten Stufe“. Die Anweisung „Bewege n Scheiben von X über Y nach Z“ notieren wir mit $[n; X, Y, Z]$. Dann ergibt sich die folgende Lösung für $n = 3$:

M: [3;A,B,C]
L1: [2; A,C,B]
L2: [1;A,-,C]
L1: [1; A,-,B]
L2: [1;C,-,B]
M: [1;A,-,C]
L1: [2; B,A,C]
L2: [1;B,-,A]
L1: [1; B,-,C]
L2: [1;A,-,C]

Also werden für eine Turmhöhe von $n = 3$ maximal sieben Scheibenbewegungen benötigt.

Sei nun $T\colon \mathbb{N} \to \mathbb{N}$ die Funktion, die angibt, wieviele Bewegungen bei einer Turmhöhe von n notwendig sind. Wir wissen bereits $T(0) = 0$, $T(1) = 1$, $T(2) \leq 3$ und $T(3) \leq 7$. Mit Hilfe der „überlieferten“ Arbeitsbeschreibung ergibt sich mit $n > 0$:

$$T(n) \leq 2T(n-1) + 1$$

Nun ist noch unklar, ob $T(n) = 2T(n-1) + 1$ gilt, denn es könnte ja eine bessere Strategie geben. Folgende Überlegung zeigt aber, dass dies nicht der Fall ist. Auf jeden Fall muss der Meister eine Bewegung durchführen, um die letzte Scheibe zu bewegen, und der Lehrling muss mindestens zweimal einen Turm der Höhe $n-1$ bewegen (vor und nach seinem Meister), d.h. es sind jeweils mindestens $T(n-1)$ Bewegungen notwendig. Damit ergibt sich $T(n) \geq 2T(n-1) + 1$ und somit $T(n) = 2T(n-1) + 1$. In dieser Gleichung kommt das Funktionssymbol sowohl auf der linken als auch auf der rechten Seite vor. Solche Gleichungen nennt man *Rekurrenzgleichung*. Ein kurzer Test ergibt $T(3) = 2T(2)+1 = 2(2T(1)+1)+1 = 2(2(2T(0)+1)+1)+1 = 8T(0)+7 = 7$, d.h. diese Gleichung gibt die Anzahl der Scheibenbewegungen an. Nun soll die Rekurrenzgleichung in explizite Form gebracht werden:

Satz 1: *Um die Türme von Hanoi zu lösen, werden bei einer Turmhöhe von $n \in \mathbb{N}$, genau $T(n) = 2^n - 1$ Bewegungen von Scheiben benötigt.*

Beweis: Der Beweis wird mit Hilfe einer Induktion über n geführt:

(IA) Für $n = 0$ ergibt sich $T(0) = 0 = 2^0 - 1$.

(IV) $T(n) = 2^n - 1$

(IS) Es ergibt sich $T(n+1) = 2T(n)+1 \overset{\text{(IV)}}{=} 2\cdot(2^n-1)+1 = 2\cdot 2^n - 2 + 1 = 2^{n+1}-1$. #

Folgerung 2: *Die Welt geht in genau* $2^{64}-1$ *Tagen* $\approx 1.84\cdot 10^{19}$ *Tagen* $\approx 5.05\cdot 10^{16}$ *Jahren unter, nachdem die Priester ihr Werk begenonnen haben.*

Damit ist klar, dass uns noch genug Zeit für die Vorlesung bleibt.

2. Einige Grundlagen der elementaren Kombinatorik

2.1. Zählen

In diesem Abschnitt beschäftigen wir uns mit dem Zählen von Elementen in endlichen Mengen.

Beispiel 3: *In einem Fachbereich für Informatik einer hessischen Hochschule sind alle internen Telefonnummern zweistellig. Sei* $D = \{0,\dots,9\}$*, dann ist* $D\times D$ *die Menge der zulässigen Telefonnummern. Dann gilt:*

$$\begin{aligned}\#(D\times D) &= \#\{(0,0),\dots,(9,0),(0,1),\dots,(9,1),\dots,(0,9),\dots,(9,9)\}\\ &= 10\cdot 10\\ &= 100.\end{aligned}$$

Satz 4 (Multiplikationsregel): *Seien* A *und* B *endliche Mengen, dann gilt*

$$\#(A\times B) = \#A\cdot\#B$$

Beweis: Wir zeigen die Aussage via Induktion über die Anzahl der Elemente in B.
(IA) Sei $\#B = 0$, dann gilt $B = \emptyset$ und damit $A\times B = \emptyset$. Also ergibt sich $0 = \#(A\times B) = \#A\cdot\#B = \#A\cdot 0 = 0$.
(IV) Sei B eine beliebige Menge mit $\#B = n$, dann gilt $\#(A\times B) = \#A\cdot\#B$.
(IS) Sei $\#B = n+1$, $b\in B$ beliebig und $B' =_{\text{def}} B\setminus\{b\}$. Nun gilt $\#B' = n$ und mit der Induktionsvoraussetzung gilt dann $\#(A\times B') = \#A\cdot\#B'$. Zusätzlich zu den Elementen aus $A\times B'$ sind in $A\times B$ die Paare (a,b) mit $a\in A$ enthalten. Es gibt genau $\#A$ solche Paare. Zusammen ergibt sich also

$$\begin{aligned}\#(A\times B) &= \#(A\times B') + \#A\\ &\overset{\text{(IV)}}{=} \#A\cdot\#B' + \#A\\ &= \#A\cdot(\#B'+1)\\ &= \#A\cdot\#B,\end{aligned}$$

womit die Aussage gezeigt ist. #

Folgerung 5 (Produktregel): *Sei* $k\in\mathbb{N}\setminus\{0\}$ *und seien* $A_1,\dots,A_k$ *endliche Mengen, dann gilt:*

$$\#(A_1\times A_2\times\cdots\times A_k) = \prod_{i=1}^{k}\#A_i$$

Beweis: Übung #

Beispiel 6: *In der Informatik (z.B. in der Theorie der formale Sprachen) sind Wörter fester Länge über einem (endlichen) Alphabet von Bedeutung. Sei Σ ein Alphabet, dann entspricht ein Wort der Länge k einem Element aus $\Sigma^k = \underbrace{\Sigma \times \Sigma \times \cdots \times \Sigma}_{k-mal}$. Es gibt also genau $(\#\Sigma)^k$ solche Worte.*

Satz 7 (Additionsregel): *Seien A und B disjunkte endliche Mengen, dann gilt*

$$\#(A \cup B) = \#A + \#B.$$

Beweis: Wir zeigen die Aussage durch Induktion über $\#B$.
(IA) Sei $\#B = 0$, dann gilt $B = \emptyset$ und $\#(A \cup B) = \#A = \#A + 0 = \#A + \#B$.
(IV) Sei B eine beliebige Menge mit $\#B = n$, dann gilt $\#(A \cup B) = \#A + \#B$.
(IS) Sei nun $\#B = n + 1$, $b \in B$ beliebig und $B' =_{\text{def}} B \setminus \{b\}$. Dann gilt $\#B' = n$ und nach Induktionsvoraussetzung $\#(A \cup B') = \#A + \#B'$. Da $A \cap B = \emptyset$ ist, gilt $b \notin A$ und auch $b \notin B'$. Damit ergibt sich

$$\begin{aligned} \#(A \cup B) &= \#(A \cup B' \cup \{b\}) \\ &= \#(A \cup B') + 1 \\ &\overset{\text{(IV)}}{=} \#A + \#B' + 1 \\ &= \#A + \#B. \end{aligned}$$

Wodurch die Aussage des Satzes gezeigt ist. #

Folgerung 8 (Summenregel): *Sei $k \in \mathbb{N} \setminus \{0\}$ und seien $A_1, \ldots, A_k$ endliche und paarweise disjunkte Mengen, dann gilt:*

$$\#\bigcup_{i=1}^{k} A_i = \sum_{i=1}^{k} \#A_i$$

Beispiel 9: *In einer fiktiven Programmiersprache beginnt ein Variablenname mit einem Buchstaben, gefolgt von bis zu sieben weiteren Zeichen. Wieviele verschiedene Variablennamen gibt es?*

Zuerst legen wir $\Sigma = \{0, \ldots, 9, a, \ldots z\}$ (wir unterscheiden Groß- und Kleinschreibung nicht) fest und definieren die folgenden disjunkten Variablenmengen:

$$A_i =_{\text{def}} \{w \in \Sigma^* \mid \text{ } w \text{ ist ein Variablenname der Länge } i\}.$$

Damit ergibt sich $\#A_1 = 26$ und mit der Produktregel gilt $A_i = \#\{a, \ldots, z\} \cdot \#\Sigma^{i-1} = 26 \cdot 36^{i-1}$ für $2 \leq i \leq 8$. Mit der Additions- und Summenregel ergibt sich die Gesamtzahl der Variablennamen zu

$$\begin{aligned} 26 + \sum_{i=2}^{8} 26 \cdot 36^{i-1} &= 26 \cdot (1 + \sum_{i=2}^{8} 36^{i-1}) \\ &= 26 \cdot (1 + \sum_{i=1}^{7} 36^{i}) \\ &= 2\,095\,681\,645\,538 \end{aligned}$$

Bei der Additionsregel ist es wichtig, dass die Mengen A und B disjunkt sind, da sonst Elemente aus dem Schnitt von A und B doppelt gezählt werden. Der nächste Satz umgeht diese Einschränkung:

Satz 10: *Seien A und B endliche Mengen, dann gilt*

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

Anschaulich bedeutet dies, dass die doppelt gezählten Elemente aus der Schnittmenge $A \cap B$ wieder abgezogen werden.
Beweis: Wir führen eine Induktion über $\#B$ durch.
(IA) Sei $\#B = 0$, dann gilt auch $B = \emptyset$ und damit ist $\#(A \cup B) = \#A + 0 - 0 = \#A + \#B - \#(A \cap B)$.
(IV) Die Behauptung $\#(A \cup B) = \#A + \#B - \#(A \cap B)$ gilt für beliebige Mengen B mit n Elementen.
(IS) Sei $\#B = n + 1$, $b \in B$ beliebig und $B' =_{\text{def}} B \setminus \{b\}$ mit $\#B' = n$. Nach **(IV)** gilt $\#(A \cup B') = \#A + \#B' - \#(A \cap B')$.

Fall $b \in A$**:** Dann gilt mit der Beobachtung $\#(A \cap B) = \#(A \cap B') + 1$:

$$\begin{array}{rcl} \#(A \cup B) & = & \#(A \cup B') \text{ (da } b \in A) \\ & \overset{\text{(IV)}}{=} & \#A + \#B' - \#(A \cap B') \\ & = & \#A + \#B - 1 - (\#(A \cap B) - 1) \\ & = & \#A + \#B - \#(A \cap B) \end{array}$$

Fall $b \notin A$**:** Nun gilt

$$\begin{array}{rcl} \#(A \cup B) & = & \#(A \cup B') + 1 \text{ (da } b \notin A) \\ & \overset{\text{(IV)}}{=} & \#A + \#B' - \#(A \cap B') + 1 \\ & = & \#A + \#B - 1 - \#(A \cap B) + 1 \text{ (da } b \notin A \cap B') \\ & = & \#A + \#B - \#(A \cap B) \end{array}$$

Damit ist die Aussage des Satzes gezeigt. #

Beispiel 11: *Sei* $L =_{\text{def}} \{w \in \{0,1\}^8 \mid w \text{ beginnt mit } 0 \text{ oder endet mit } 11\}$. *Damit werden die Sprachen* $A =_{\text{def}} \{w \in \{0,1\}^8 \mid w \text{ beginnt mit } 0\}$ *und* $B =_{\text{def}} \{w \in \{0,1\}^8 \mid w \text{ endet mit } 11\}$ *definiert und es gilt* $\#L = \#(A \cup B)$.
Mit der Produktregel ergibt sich sofort $\#A = 1 \cdot 2^7$, $\#B = 2^6 \cdot 1 \cdot 1$ *und* $\#(A \cap B) = \#\{w \in \{0,1\}^8 \mid w = 0w'11\} = 1 \cdot 2^5 \cdot 1 \cdot 1$. *Damit ergibt sich* $\#L = \#(A \cup B) = 2^7 + 2^6 - 2^5 = 160$.

Satz 10 kann auch auf drei (oder mehr) Mengen verallgemeinert werden (vgl. Abbildung 2):

Satz 12: *Seien A, B und C endliche Mengen, dann gilt*

$$\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C).$$

Beweis: Seien A, B und C beliebige endliche Mengen, dann

$$\begin{array}{rcl} \#(A \cup B \cup C) & = & \#(A \cup B) + \#C - \#((A \cup B) \cap C) \\ & = & \#A + \#B - \#(A \cap B) + \#C - \#((A \cup B) \cap C) \\ & = & \#A + \#B - \#(A \cap B) + \#C - \#((A \cap C) \cup (B \cap C)) \\ & = & \#A + \#B - \#(A \cap B) + \#C - (\#(A \cap C) + \#(B \cap C) \\ & & -\#((A \cap C) \cap (B \cap C))) \\ & = & \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) \\ & & +\#(A \cap B \cap C) \end{array}$$

Damit ist die Aussage des Satzes gezeigt. #

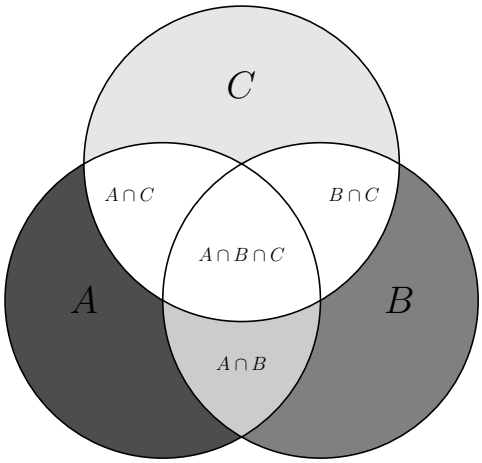


Abbildung 2: Eine graphische Darstellung des Schnitts dreier Mengen

2.2. Einige einfache Grundlagen der elementaren Kombinatorik

2.2.1. Permutationen

Definition 13: *Sei M eine (endliche) Menge und $\pi\colon M \to M$ eine bijektive Abbildung, dann nennt man π auch* Permutation.

Für unsere Zwecke sind besonders Permutationen von endlichen Mengen von Belang.

Beispiel 14: *Sei $M = \{1, 2, 3\}$, dann gibt es genau sechs verschiedene bijektive Abbildungen $\pi_i\colon M \to M$:*

i	$\pi_1(i)$	$\pi_2(i)$	$\pi_3(i)$	$\pi_4(i)$	$\pi_5(i)$	$\pi_6(i)$
1	1	1	2	2	3	3
2	2	3	1	3	1	2
3	3	2	3	1	2	1

Eine Permutation einer endlichen Menge kann man auch als *Anordnung* der Elemente dieser Menge auffassen. Sei $M = \{1, 2, 3\}$, dann gibt es sechs solche Anordnungen[2]: $\langle 1, 2, 3\rangle$, $\langle 1, 3, 2\rangle$, $\langle 2, 1, 3\rangle$, $\langle 2, 3, 1\rangle$, $\langle 3, 1, 2\rangle$ und $\langle 3, 2, 1\rangle$.

Satz 15: *Sei M eine endliche Menge mit $m = \#M$, dann gibt es $m!$ viele Permutationen von M.*

Beweis: Wir führen einen Induktion über $\#M$ durch:
(IA) Wenn $\#M = 1$, dann gibt es genau $1! = 1$ Permutation von M.
(IV) Sei $\#M = n$, dann gibt es $n!$ Permutationen von M.
(IS) Wenn $\#M = n + 1$, $a \in M$, $M' =_{\text{def}} M \setminus \{a\}$ und π' Permutation von M', dann ist

$$\pi(x) =_{\text{def}} \begin{cases} \pi'(x), & \text{falls } x \in M' \\ a, & \text{sonst} \end{cases}$$

eine Permutation von M. Nach **(IV)** gibt es $n!$ viele verschiedene Permutationen von M'. Weiterhin gibt es $n+1$ Möglichkeiten das Element a zu wählen, also gibt es $(n+1)\cdot n! = (n+1)!$ Permutationen von M, denn andere Permutationen von M existieren nicht.#

[2] Die Notation $\langle \ldots \rangle$ deutet an, dass die Reihenfolge der in den Klammern enthaltenen Objekte wichtig ist, ganz im Gegenteil zu der Notation für Mengen $\{\ldots\}$, bei denen die Reihenfolge der Elemente keine Bedeutung hat.

Bemerkung 16: *Oft schreibt man Permutationen auch als Matrix. Sei* $M = \{a, b, c\}$ *und* π *die Permutation von* M *mit* $\pi(a) = b$, $\pi(b) = c$ *und* $\pi(c) = a$. *Dann ist*

$$\pi = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

die Matrixschreibweise von π. *Diese Schreibweise kann natürlich auch für eine Permutation* π' *von* $M = \{a_1, \ldots, a_n\}$ *mit* $b_i = \pi'(a_i)$ *und* $1 \leq i \leq n$ *verallgemeinert werden:*

$$\pi' = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

2.2.2. Variationen

Definition 17: *Eine* k-Permutation *einer endlichen Menge* M *ist eine Permutation einer* k*-elementigen Teilmenge von* M

Beispiel 18: *Sei* $M = \{1, 2, 3\}$, *dann gibt es* 3 *Teilmengen mit* 2 *Elementen:* $\{1, 2\}$, $\{1, 3\}$ *und* $\{2, 3\}$ *und die* 2*-Permutationen* $\langle 1, 2\rangle$, $\langle 2, 1\rangle$, $\langle 1, 3\rangle$, $\langle 3, 1\rangle$, $\langle 2, 3\rangle$ *und* $\langle 3, 2\rangle$.

Definition 19: *Die Anzahl von* k*-Permutationen einer Menge mit* n *Elementen notieren wir mit* $\begin{bmatrix} n \\ k \end{bmatrix}$.

Satz 20: *Seien* $n, k \in \mathbb{N}$ *und* $n \geq k \geq 1$, *dann gilt für die Anzahl der* k*-Permutationen einer* n*-elementigen Menge*

$$\begin{bmatrix} n \\ k \end{bmatrix} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

Den Spezialfall $n = k$ kennen wir schon und es gilt $\begin{bmatrix} k \\ k \end{bmatrix} = k!$.

Beweis: Eine k-Permutation ist die Anordnung einer k-elementigen Menge, wobei die Elemente aus M stammen.

Sei nun $M' = \{a'_1, \ldots, a'_k\} \subseteq M$. Für eine Anordnung $\langle a'_1, \ldots, a'_k\rangle$ gibt es n Möglichkeiten um a'_1 zu wählen, $n-1$ Möglichkeiten für a'_2, $\ldots$, $n-k+2$ Möglichkeiten für a'_{k-1} und $n-k+1$ Möglichkeiten zur Wahl von a'_k. Also gibt es $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ verschiedene k-Permutationen von M. #

Folgerung 21: *Seien* $n, k \in \mathbb{N}$ *und* $n \geq k \geq 1$, *dann gilt*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{n!}{(n-k)!}$$

Beispiel 22: *Bei einer Lottoziehung werden* 6 *Kugeln aus einer Urne mit* 49 *Kugeln gezogen. Wieviele mögliche Ziehungsverläufe gibt es?*

Jede Ziehung entspricht genau einer 6*-Permutation einer Menge mit* 49 *Elementen, d.h. es gibt*

$$\begin{bmatrix} 49 \\ 6 \end{bmatrix} = \frac{49!}{(49-6)!} = 10\,068\,347\,520$$

verschiedene Ziehungsverläufe.

2.2.3. Kombinationen

Bei einer Lottoziehung kommt es aber nicht auf die Reihenfolge der Elemente an. Eine Ziehung von beispielsweise $3, 43, 6, 17, 22, 11$ ist zu $22, 6, 43, 3, 11, 17$ gleichwertig, d.h. die 6-Permutationen werden wieder als Menge betrachtet. Da es 6! gleichwertige Anordungen dieser Menge gibt, existieren

$$\frac{\begin{bmatrix}49\\6\end{bmatrix}}{6!} = 13\,983\,816$$

mögliche verschiedene Ergebnisse einer Lottoziehung. Dies führt zu der folgenden Definition:

Definition 23: *Seien $n, k \in \mathbb{N}$ und $n \geq k \geq 1$, dann definieren wir mit*

$$\binom{n}{k} =_{\text{def}} \frac{\begin{bmatrix}n\\k\end{bmatrix}}{\begin{bmatrix}k\\k\end{bmatrix}}$$

die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge (Sprechweise: n über k). Der Wert $\binom{n}{k}$ wird auch der Binominialkoeffizient genannt.

Satz 24: *Seien $n, k \in \mathbb{N}$ und $k \leq n$, dann gilt:*

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

Beweis: Es gilt

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

#

Schreibt man die Binominialkoeffizienten geordnet auf, so erhält man das bekannte *Pascal'sche Dreieck*:

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Satz 25: *Für alle $n, k \in \mathbb{N}$ mit $1 \leq k \leq n$ gilt*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Beweis: Für $n, k \in \mathbb{N}$ mit $1 \leq k \leq n$ ergibt sich

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

#

Folgerung 26: *Die Binominialkoeffizienten können aufgrund von Satz 25 rekursiv berechnet bzw. induktiv definiert werden:*
(IA)

- *Wenn $n \in \mathbb{N}$ und $n \geq 1$, dann $\binom{n}{0} = 1$.*
- *Wenn $n, k \in \mathbb{N}$ und $n < k$, dann $\binom{n}{k} = 0$.*

(IS) *Sei $n, k \in \mathbb{N}$ und $1 \leq k \leq n$, dann*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Satz 27 (Binomischer Satz): *Für alle $n \in \mathbb{N}, n \geq 1$ gilt*

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

Beweis: Es gilt $(x+y)^n = \underbrace{(x+y)\cdot(x+y)\cdot\ldots\cdot(x+y)}_{n\text{-mal}}$, d.h. jeder Summand, der beim Ausmultiplizieren entsteht, hat die Form $x^i y^j$ mit $i+j=n$ und es wurde i-mal x und j-mal y gewählt. Damit ergeben sich die folgenden Gleichungen:

$$\begin{aligned}
(x+y)^n &= \sum_{A\subseteq\{1,\ldots,n\}} \Big(\prod_{i\in\{1,\ldots,n\}\setminus A} x \cdot \prod_{i\in A} y \Big) \\
&= \sum_{A\subseteq\{1,\ldots,n\}} (x^{n-j}\cdot y^j) \\
&= \sum_{j=0}^{n} \sum_{\substack{A\subseteq\{1,\ldots,n\} \\ \#A=j}} (x^{n-j}\cdot y^j) \\
&= \sum_{j=0}^{n} \binom{n}{j} x^{n-j}\cdot y^j
\end{aligned}$$

Der letzte Schritt ergibt sich, weil es genau $\binom{n}{j}$ Teilmengen mit j Elementen der Grundmenge mit n Elementen gibt. #

Beispiel 28: *Nach dem Binomischen Satz gilt* $(x+y)^5 = 1\cdot x^5 + 5\cdot x^4 y + 10\cdot x^3 y^2 + 10\cdot x^2 y^3 + 5\cdot x y^4 + 1\cdot y^5$.

Folgerung 29 (Alternierende Summe): *Sei $n \in \mathbb{N}, n \geq 1$, dann*

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$$

Beweis:

$$0 = ((-1)+1)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i}(1)^i = \sum_{i=0}^{n} \binom{n}{i} (-1)^i$$

#

Folgerung 30: *Sei $n \in \mathbb{N}$ und $n \geq 1$, dann*

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Beweis: Übung #

Es gilt die folgende Näherung für $n!$:

Satz 31 (Stirling'sche Formel): *Sei $n \in \mathbb{N}$, dann gilt*

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2\pi n}\left(\frac{n}{e}\right)^{n+\frac{1}{12n}}$$

Folgerung 32: *Für $n, k \in \mathbb{N}$ gilt*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{e \cdot n}{k}\right)^k.$$

Beweis: Sei $0 \leq a < k \leq n$, dann gilt

$$\frac{n}{k} \leq \frac{n-a}{k-a}.$$

Dies kann leicht durch ausmultiplizieren der Ungleichung gezeigt werden. Damit ergibt sich

$$\begin{aligned} \binom{n}{k} &= \tfrac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{1\cdot 2\cdot\ldots\cdot k} \\ &= \tfrac{n}{k} \cdot \tfrac{n-1}{k-1} \cdot \tfrac{n-2}{k-2} \cdot \ldots \cdot \tfrac{n-(k-1)}{k-(k-1)} \\ &\geq \tfrac{n}{k} \cdot \tfrac{n}{k} \cdot \tfrac{n}{k} \cdot \ldots \cdot \tfrac{n}{k} \\ &= \left(\tfrac{n}{k}\right)^k \end{aligned}$$

Dies zeigt den linken Teil der Folgerung. Mit der Stirling'schen Formel gilt

$$\left(\frac{k}{e}\right)^k \leq k! \text{ und somit } \left(\frac{e}{k}\right)^k \geq \frac{1}{k!}.$$

Damit ergibt sich

$$\begin{aligned} \binom{n}{k} &= \tfrac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!} \\ &\leq \tfrac{n^k}{k!} \\ &\leq n^k \cdot \left(\tfrac{e}{k}\right)^k \\ &= \left(\tfrac{e\cdot n}{k}\right)^k, \end{aligned}$$

was den zweiten Teil der Aussage zeigt. #

3. Algebraische Grundlagen

3.1. Algebraische Strukturen

Definition 33: *Sei $n \in \mathbb{N}$, dann heißt eine Abbildung $f\colon A^n \to A$ n-stellige* Operation auf A. *Wir definieren*

- $\mathrm{Op}_n(A) =_{\mathrm{def}} \{f \mid f \text{ ist } n\text{-stellige Operation auf } A\}$ *und*
- $\mathrm{Op}(A) =_{\mathrm{def}} \bigcup_{i\in\mathbb{N}} \mathrm{Op}_i(A)$ *(„Menge aller endlichstelligen Operationen“).*

Die Stelligkeit einer Operation wird auch Arität *genannt.*

Operationen der Arität 0 haben keine Argumente, d.h. sie sind Konstanten.

Definition 34: *Eine* Algebra $\mathcal{A}$ *ist ein geordnetes Paar*

$$\mathcal{A} = (A, F),$$

wobei $A \neq \emptyset$ und $F \subseteq \mathrm{Op}(A)$. A heißt auch Universum *der Algebra $\mathcal{A}$ und F wird als die Menge der* fundamentalen Operationen *bezeichnet. Eine Algebra $\mathcal{A} = (A, F)$ heißt* endlich, *wenn A eine endliche Menge ist.*

Definition 35: *Sei $\mathcal{A} = (A, F)$ eine Algebra mit $F = \{f_1, \ldots, f_r\}$ und $f_i \in \mathrm{Op}_{n_i}(A)$ für $1 \leq i \leq r$ (d.h. f_1 hat Stelligkeit n_1, f_2 hat Stelligkeit n_2,...,f_r hat Stelligkeit n_r), dann nennt man $\mathcal{A}$ eine Algebra vom* Typ $(n_1, \ldots, n_r)$.

Beispiel 36:

- *Eine Algebra $(A, \{\circ\})$ vom Typ (2) heißt* Gruppoid *(oder* Magma*), d.h. ein Gruppoid besteht aus einer nicht leeren Menge und einer binären Operation.*
- *Ein Gruppoid $(A, \{\circ\})$ mit der zusätzlichen Eigenschaft, dass für alle $a, b, c \in A$ die Beziehung $a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziativität) gilt, heißt* Halbgruppe.
- *Eine Algebra $\mathcal{M} = (M, \{\circ, e\})$ vom Typ $(2, 0)$ heißt* Monoid, *wenn $(M, \{\circ\})$ eine Halbgruppe ist und zusätzlich für alle $a \in M$*

  $$a \circ e = e \circ a = a$$

  gilt. Die Konstante $e \in M$ heißt auch neutrales Element *des Monoids $\mathcal{M}$.*
- *Eine Algebra $\mathcal{G} = (G, \{\circ, ^{-1}, e\})$ vom Typ $(2, 1, 0)$ heißt* Gruppe, *wenn $(G, \{\circ, e\})$ ein Monoid ist und für alle $g \in G$*

  $$g \circ g^{-1} = g^{-1} \circ g = e$$

  gilt. Dabei wird g^{-1} als das inverses Element *(von g) bezeichnet. Gilt zusätzlich noch für alle $a, b \in G$*

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

  dann heißt G kommutativ *oder* abelsch[3]*.*

[3] Diese Bezeichnung leitet sich von dem Namen des norwegischen Mathematikers Niels Abel ab, der 1802 in Frindoe geboren wurde und 1829 in Froland starb.

- *Eine Algebra $\mathcal{V} = (V, \{\sqcap, \sqcup\})$ vom Typ $(2,2)$ heißt* Verband*, wenn die folgenden Gleichungen für alle $x, y, z \in V$ erfüllt sind*

$$\left.\begin{array}{rcl} x \sqcup y & = & y \sqcup x \\ x \sqcap y & = & y \sqcap x \end{array}\right\} \quad \textit{Kommutativitätsgesetze}$$

$$\left.\begin{array}{rcl} x \sqcup (y \sqcup z) & = & (x \sqcup y) \sqcup z \\ x \sqcap (y \sqcap z) & = & (x \sqcap y) \sqcap z \end{array}\right\} \quad \textit{Assoziativitätsgesetze}$$

$$\left.\begin{array}{rcl} x \sqcup x & = & x \\ x \sqcap x & = & x \end{array}\right\} \quad \textit{Idempotenz}$$

$$\left.\begin{array}{rcl} x \sqcup (x \sqcap y) & = & x \\ x \sqcap (x \sqcup y) & = & x \end{array}\right\} \quad \textit{Absorptionsgesetze}$$

Der Verband $\mathcal{V}$ heißt distributiv*, wenn zusätzlich zu den beschriebenen Verbandseigenschaften für alle $x, y, z \in V$ sowohl $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ als auch $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$ gelten.*

Oft vereinfacht man die Notation einer Algebra und schreibt statt $(A, \{f_1, \ldots, f_r\})$ auch $(A, f_1, \ldots, f_r)$. Weiterhin führt man 0-stellige Operationen, also besondere Konstanten, nicht in der Liste der Operationen auf. Sind die Operationen einer Algebra aus dem Kontext klar, notiert man die Algebra oft nur durch ihr Universum.

3.2. Monoide

Definition 37 (alternative Definition): *Eine Algebra $(M, \circ)$ heißt* Monoid*, falls*

- *für alle $a, b, c \in M$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$ („Assoziativität“) und*
- *es gibt ein ausgezeichnetes $e \in M$, so dass für alle $m \in M$ die Beziehung $e \circ m = m = m \circ e$ gilt.*

Ein Monoid $(M, \circ)$ heißt kommutativ *bzw.* abelsch*, wenn zusätzlich für alle $a, b \in M$ auch $a \circ b = b \circ a$ gilt.*

Für das Verknüpfungssymbol „$\circ$“ eines Monoids verwendet man aus Bequemlichkeitsgründen oft „$\cdot$“ (bzw. „$+$“). Dies wird dann als *multiplikative Schreibweise* (bzw. *additive Schreibweise*) des Monoids bezeichnet. Das neutrale Element wird dann als die „*Eins*“ (bzw. „*Null*“) des Monoids bezeichnet.
In diesem Zusammenhang sind dann die abkürzenden Schreibweisen

$$\begin{array}{rcl} a^n & =_{\text{def}} & \underbrace{a \cdot \ldots \cdot a}_{n\text{-mal}} \text{ und} \\ n \cdot a & =_{\text{def}} & \underbrace{a + \ldots + a}_{n\text{-mal}} \end{array}$$

gebräuchlich.

Proposition 38: *Sei $(M, \cdot)$ ein Monoid und seien $n, m \in \mathbb{N}\backslash\{0\}$, dann gilt für $a, b \in M$ (in multiplikativer Schreibweise)*

$$(a^n)^m = a^{n \cdot m} \text{ und } a^n \cdot a^m = a^{n+m}$$

Für kommutative Monoide gilt zusätzlich

$$(ab)^n = a^n b^n$$

Definition 39: *Seien $(M_1, \oplus)$ und $(M_2, \odot)$ Monoide mit den neutralen Elementen $e_1 \in M_1$ und $e_2 \in M_2$. Dann heißt eine Abbildung $\eta\colon M_1 \to M_2$* Monoidhomomorphismus*, wenn*

$$\eta(a \oplus b) = \eta(a) \odot \eta(b)$$

für alle $a, b \in M_1$ und

$$\eta(e_1) = e_2$$

gilt. Ist η bijektiv, dann heißt η auch Monoidisomorphismus*.*

Beispiel 40:

- *Die Algebren $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{C}, +)$ sind kommutative Monoide.*
- *Sei $X^X =_{\text{def}} \{f \mid f\colon X \to X\}$, dann ist X^X mit der Komposition von Abbildungen ein Monoid.*
- *Sei M ein Monoid und*

  $$M^M =_{\text{def}} \{\eta \mid \eta\colon M \to M \text{ ist Monoidhomomorphismusvon } M\},$$

  dann ist M^M mit der Komposition wieder ein Monoid.

Beispiel 41: *Sei Σ ein beliebiges (endliches) Alphabet, dann definieren wir die Menge von Worten über Σ als $\Sigma^* =_{\text{def}} \{w \mid w \text{ ist ein Wort über } \Sigma\}$. Sei $w_1 = a_1 \dots a_n \in \Sigma^*$ und $w_2 = b_1 \dots b_m \in \Sigma^*$. Wir definieren*

$$w_1 \circ w_2 =_{\text{def}} a_1 \dots a_n b_1 \dots b_m \text{ („Konkatenation“).}$$

*Dann ist $(\Sigma^*, \circ)$ ein Monoid mit dem neutralen Element ϵ (das „*leere Wort*“), das aus keinem Buchstaben besteht. Das Monoid $(\Sigma^*, \circ)$ wird auch als das* freie Monoid *(über Σ) bezeichnet.*

Beispiel 42: *Sei $L \subseteq \Sigma^*$ eine beliebige (formale) Sprache über Σ, dann definieren wir die folgende Relation $\sim_L$:*
Seien $x, y \in \Sigma^*$, dann gilt $x \sim_L y$ genau dann, wenn für alle $z \in \Sigma^*$ gilt:

$$x \circ z \in L \text{ gdw. } y \circ z \in L$$

Die Relation $\sim_L$ ist eine Äquivalenzrelation, da sie

- *reflexiv, denn $x \sim_L x$, weil für alle $z \in \Sigma^*$ sicherlich $x \circ z \in L$ gdw. $x \circ z \in L$ gilt,*
- *symmetrisch, denn wenn $x \sim_L y$, dann ist immer auch $y \sim_L x$, da für alle $z \in \Sigma^*$ gilt, dass aus $x \circ z \in L$ gdw. $y \circ z \in L$ auch $y \circ z \in L$ gdw. $x \circ z \in L$ folgt und*
- *transitiv ist, denn wenn $x \sim_L y$ und $y \sim_L z$, dann gilt für alle $w, w_1, w_2 \in \Sigma^*$ sowohl $x \circ w_1 \in L$ gdw. $y \circ w_1 \in L$ als auch $y \circ w_2 \in L$ gdw. $z \circ w_2 \in L$. Zusammen ergibt sich damit für alle $z \in \Sigma^*$ $x \circ w \in L$ gdw. $z \circ w \in L$, d.h. $x \sim_L z$.*

Sei nun $a \in \Sigma^*$, $[a] =_{\text{def}} \{b \in \Sigma^* \mid a \sim_L b\}$ und $M(L) =_{\text{def}} \{[a] \mid a \in \Sigma^*\}$. Es gilt, dass $(M(L), \cdot)$ ein Monoid ist, wenn wir die Monoidverknüpfung wie folgt definieren

$$[a] \cdot [b] =_{\text{def}} [a \circ b].$$

Offensichtlich gilt, dass „$\cdot$“ eine Operation aus $\text{Op}_2(M(L))$ ist, aber wir müssen noch überprüfen, ob die Abbildung auch wohldefiniert *ist, d.h. ob für zwei Äquivalenzklassen*

A_1 und A_2 mit $[a_1] = A_1 = [a_1']$ und $[a_2] = A_2 = [a_2']$ auch gilt $[a_1] \cdot [a_2] = [a_1'] \cdot [a_2']$. Anschaulich bedeutet dies, dass die Monoidverknüpfung unabhängig von der Wahl des Repräsentanten der jeweiligen Äquivalenzklassen ist. Da $[a_1] = [a_1']$ gilt für alle $z \in \Sigma^*$ $a_1 \circ z \in L$ gdw. $a_1' \circ z \in L$ und wegen $[a_2] = [a_2']$ gilt für alle $z \in \Sigma^*$ $a_2 \circ z \in L$ gdw. $a_2' \circ z \in L$. Also ist

$$\begin{aligned}
[a_1 \circ a_2] &= \{b \in \Sigma^* \mid \textit{für alle } z \in \Sigma^* \textit{ gilt } b \circ z \in L \textit{ gdw. } (a_1 \circ a_2) \circ z \in L\} \\
&= \{b \in \Sigma^* \mid \textit{für alle } z \in \Sigma^* \textit{ gilt } b \circ z \in L \textit{ gdw. } a_1 \circ (a_2 \circ z) \in L\} \\
&= \{b \in \Sigma^* \mid \textit{für alle } z \in \Sigma^* \textit{ gilt } b \circ z \in L \textit{ gdw. } a_1 \circ (a_2' \circ z) \in L\} \\
&= \{b \in \Sigma^* \mid \textit{für alle } z \in \Sigma^* \textit{ gilt } b \circ z \in L \textit{ gdw. } a_1' \circ (a_2' \circ z) \in L\} \\
&= \{b \in \Sigma^* \mid \textit{für alle } z \in \Sigma^* \textit{ gilt } b \circ z \in L \textit{ gdw. } (a_1' \circ a_2') \circ z \in L\} \\
&= [a_1' \circ a_2']
\end{aligned}$$

D.h. die Verknüpfung „$\cdot$“ ist wohldefiniert und $[\epsilon]$ ist ein neutrales Element. Die Assoziativität überträgt sich durch die ursprüngliche Verknüpfung „$\circ$“, was zeigt, dass $(M(L), \cdot)$ ein Monoid ist. Es gilt der folgende wichtige Satz aus der Theorie der formalen Sprachen:

Satz 43 (Myhill-Nerode): *Eine Sprache L ist genau dann regulär (d.h. vom Chomsky-Typ 3), wenn das Monoid $(M(L), \cdot)$ endlich ist.*

Treibt man diese Überlegungen weiter, so läßt sich der bekannte Minimisierungsalgorithmus für endliche Automaten ableiten.

3.3. Elementare Gruppentheorie

In diesem Abschnitt sollen besonders endliche Gruppen (von Permutationen) untersucht werden. Endliche Gruppen sind für Informatiker von besonderem Interesse, da z.B. die Gruppenverknüpfung besonders einfach durch eine *Gruppentafel/ Verknüpfungstafel* implementiert werden kann und weil sie viele Anwendungen, z.B. in der Kryptographie, haben. Sei $\mathcal{G} = (\{a_1, \ldots, a_n\}, \circ)$, dann kann die Verknüpfung „$\circ$“ wie folgt repräsentiert werden:

$\circ$	a_1	a_2	$\ldots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\ldots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\ldots$	$a_2 \circ a_n$
a_3	$a_3 \circ a_1$	$a_3 \circ a_2$	$\ldots$	$a_3 \circ a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\ldots$	$a_n \circ a_n$

Definition 44: *Seien $\mathcal{G}_1 = (G_1, \oplus)$ und $\mathcal{G}_2 = (G_2, \odot)$ Gruppen und $\eta\colon G_1 \to G_2$. Gilt für alle $g, g' \in G_1$ die Gleichung*

$$\eta(g \oplus g') = \eta(g) \odot \eta(g'),$$

dann nennt man η einen Gruppenhomomorphismus. *Ist η zusätzlich noch bijektiv, dann heißt η* Gruppenisomorphismus *(Symbol: $G_1 \cong G_2$).*

Anschaulich bedeutet die Isomorphie zwischen Gruppen $\mathcal{G}_1$ und $\mathcal{G}_2$, dass sie die gleiche Struktur aufweisen, lediglich die Gruppenelemente werden anders „benannt“. Homomorphismen und insbesondere Isomorphismen sind also *strukturerhaltende Abbildungen*.

Definition 45: *Sei $\mathcal{G} = (G, \circ)$ eine Gruppe. Die Mächtigkeit $\#G$ heißt auch* Ordnung *(von $\mathcal{G}$).*

Mit Hilfe der Gruppenaxiome ergeben sich direkt die folgenden Rechenregeln in Gruppen:

Satz 46 (Kürzungsregeln): *Sei $\mathcal{G} = (G, \cdot)$ eine Gruppe, dann gilt für alle $a, b, c \in G$:*

i) Wenn $ac = bc$, dann $a = b$

ii) Wenn $ca = cb$, dann $a = b$.

Beweis: Sei $e \in G$ das neutrale Element von $\mathcal{G}$, dann gilt $a = ae = a \cdot (cc^{-1}) = (ac) \cdot c^{-1} = (bc)c^{-1} = b \cdot (cc^{-1}) = b$. Die andere Regel ergibt sich analog. #

Satz 47: *Sei M eine endliche Menge und $S(M) =_{\text{def}} \{\pi \mid \pi \colon M \to M$ ist bijektiv$\}$, dann bildet $S(M)$ zusammen mit der Komposition von Funktionen eine Gruppe. Diese Gruppe heißt die* symmetrische Gruppe[4] *von M.*

Beweis: Seien $\pi_1, \pi_2, \pi_3 \in S(M)$, dann gilt

$$\begin{aligned}(\pi_1 \circ \pi_2) \circ \pi_3(x) &= (\pi_1 \circ \pi_2)(\pi_3(x)) \\ &= \pi_1(\pi_2(\pi_3(x))) \\ &= \pi_1(\pi_2 \circ \pi_3(x)) \\ &= \pi_1 \circ (\pi_2 \circ \pi_3)(x).\end{aligned}$$

Deshalb ist die Komposition von Funktionen assoziativ und weiterhin existiert ein neutrales Element $\mathrm{id}(x) =_{\text{def}} x$, denn offensichtlich ist $\mathrm{id}(x) \in S(M)$. Für jede Funktion $\pi \in S(M)$ existiert die Umkehrfunktion π^{-1} mit $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \mathrm{id}$, wie man leicht mit der Matrixdarstellung von Permutationen einsehen kann. Damit ist gezeigt, dass $(S(M), \circ)$ eine Gruppe ist. #

Bemerkung 48: *Für den Spezialfall der symmetrischen Gruppe von $M = \{1, \ldots, n\}$ schreiben wir statt $S(\{1, \ldots, n\})$ einfach S_n.*

Folgerung 49: *Die Ordnung von S_n beträgt $n!$.*

Beispiel 50: *Sei $n = 6$,*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix} \in S_6 \text{ und } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} \in S_6,$$

dann ergibt sich

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 5 & 3 & 1 \end{pmatrix} \in S_6.$$

Weiterhin gilt

$$(\alpha \circ \beta)^{-1} = \begin{pmatrix} 6 & 4 & 2 & 5 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 2 & 4 & 1 \end{pmatrix} \in S_6.$$

Der folgende Satz zeigt uns, dass es ausreicht lediglich die symmetrische Gruppe S_n zu betrachten:

Satz 51: *Seien $A, B \neq \emptyset$ endliche Mengen mit $\#A = \#B$, dann sind die symmetrischen Gruppen $S(A)$ und $S(B)$ isomorph.*

[4] Der Name *symmetrische Gruppe* leitet sich von den so genannten *symmetrischen Funktionen* ab. Eine beliebige Funktion $f(x_1, \ldots, x_n)$ heißt symmetrisch, wenn für alle Permutationen $\pi \in S_n$ gilt, dass das Vertauschen der Variablen mit π die Funktion f nicht verändert.

Beweis: Da $\#A = \#B$ gilt, gibt es eine bijektive Abbildung $f\colon A \to B$. Sei $\eta\colon S(A) \to S(B)$, wobei $\eta(g) = f \circ g \circ f^{-1}$. Offensichtlich ist η bijektiv und $\eta(g_1 \circ g_2) = f \circ (g_1 \circ g_2) \circ f^{-1} = f \circ (g_1 \circ f^{-1} \circ f \circ g_2) \circ f^{-1} = (f \circ g_1 \circ f^{-1}) \circ (f \circ g_2 \circ f^{-1}) = \eta(g_1) \circ \eta(g_2)$.#

Folgerung 52: *Sei $n \in \mathbb{N}$, $n > 1$ und M eine Menge mit n Elementen, dann gilt $S_n \cong S(M)$.*

Aufgrund der letzten Folgerung können wir uns bei der weiteren Untersuchung der symmetrischen Gruppen auf die S_n beschränken, denn die S_n hat die gleiche Struktur wie $S(M)$ falls $\#M = n$.

Will man die S_n weiter untersuchen, dann ist die Matrixschreibweise der Permutationen recht schwerfällig. Die folgende Notation hilft hier. Die Permutation

$$\pi = \begin{pmatrix} 2 & 5 & 7 & 8 \\ 5 & 7 & 8 & 2 \end{pmatrix}$$

kann auch wie folgt aufgefasst werden. Das Element 2 geht in 5 über, die 5 wird zur 7, 7 zu 8, 8 zu 2 und 2 geht wieder in 5 über (kurz: $2 \to 5 \to 7 \to 8 \to 2$).

Diese Auffassung einer Permutation einer beliebigen n-elementigen Menge führt dann zu folgender Definition:

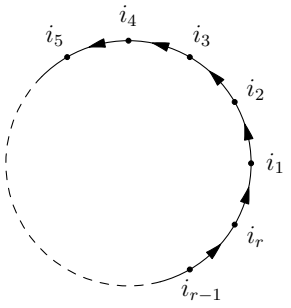
Definition 53: *Eine Permutation $\pi \in S_n$ heißt r-*Zykel*, wenn es eine Teilmenge $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$ gibt mit*

i) $\pi(i_k) = i_{k+1}$ *für* $1 \leq k < r$,

ii) $\pi(i_r) = i_1$ *und*

iii) $\pi(x) = x$, *für alle* $x \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$.

Abkürzend schreiben wir $\pi = (i_1, i_2, \ldots, i_r)$. Ein 2-Zykel wird auch Transposition *genannt.*



Mit dieser Definition gilt $\pi = (i_1, i_2, \ldots, i_r) = (i_1, \pi(i_1), \ldots \pi^{r-1}(i_1))$, wenn $\pi^k =_{\text{def}} \underbrace{\pi \circ \cdots \circ \pi}_{k\text{-mal}}$.

Beispiel 54: *Wir betrachten beliebige Permutationen, dann*

- *ist die Identität der einzige 1-Zykel,*
- $(1,2), (1,3), \ldots, (1,n)$ *sind Transpositionen aus S_n und*
- $S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

Weiterhin ergeben sich folgende Rechenregeln für Zykeln:

Satz 55: *Für beliebige Zykeln gelten die folgenden Rechenregeln:*

i) $(i_1, i_2, \ldots, i_r) = (i_2, \ldots, i_r, i_1) = (i_3, \ldots i_r, i_1, i_2) = (i_r, i_1, \ldots, i_{r-1})$, *d.h. die zyklische Vertauschung ändert einen Zykel nicht.*

ii) $(i_1, \ldots, i_r) = (i_1, \ldots, i_j)(i_j, \ldots, i_r)$, *für* $2 \leq j \leq r-1$.

iii) $(i_1, \ldots i_r) = (i_1, i_2)(i_2, i_3) \ldots (i_{r-1} i_r)$

iv) $(i_1, i_2, \ldots, i_r)^{-1} = (i_r, i_{r-1}, \ldots i_1)$

v) $\pi(i_1, i_2, \ldots, i_r)\pi^{-1} = (\pi(i_1), \ldots, \pi(i_r))$ *für alle* $\pi \in S_n$.

Beweis: Die einzelnen Punkte lassen sich wie folgt zeigen:

i) ergibt sich direkt aus der Definition

ii) Sei $\pi_1 = (i_1, \ldots i_j)$ und $\pi_2 = (i_j, \ldots i_r)$, dann ergibt $\pi_1 \circ \pi_2 = (i_1, \ldots, i_r)$, wenn man beachtet, dass der *rechte* Faktor zuerst angewendet werden muss.

iii) ergibt sich aus *ii)* mit dem Sonderfall $j = 2$.

iv) Sei $(i_1, \ldots, i_r) \in S_n$, dann folgt

$$(i_1, \ldots, i_r)^m = \begin{pmatrix} i_1 & \ldots & i_r \\ i_{s_m(1)} & \ldots & i_{s_m(r)} \end{pmatrix},$$

wobei

$$s(k) =_{\text{def}} \begin{cases} k+1, & \text{falls } k \leq r-1 \\ 1, & \text{sonst} \end{cases}$$

und $s_m(k) =_{\text{def}} \underbrace{s \circ s \circ \cdots \circ s}_{m\text{-mal}}$. Daraus ergibt sich dann

$$(i_1, \ldots, i_r)^{-1} = (i_1, \ldots, i_r)^{r-1} = \begin{pmatrix} i_1 & \ldots & i_r \\ i_{s_{r-1}(1)} & \ldots & i_{s_{r-1}(r)} \end{pmatrix} = (i_r, i_{r-1}, \ldots, i_1).$$

v) Da $\pi(i_1, \ldots, i_r)\pi^{-1} = \pi(i_1, \ldots, i_j)\pi^{-1}\pi(i_j, \ldots, i_r)\pi^{-1}$ für $2 \leq j \leq r-1$ reicht es die Aussage für Transposition zu zeigen. Sei $(i, j) \in S_n$ eine beliebige Transposition und $\pi \in S_n$, dann ist

$$\begin{aligned} (\pi(i,j)\pi^{-1})(m) &= \begin{cases} m, & \text{falls, } \pi^{-1}(m) \notin \{i, j\} \\ \pi(i), & \text{falls, } \pi^{-1}(m) = j \\ \pi(j), & \text{falls, } \pi^{-1}(m) = i \end{cases} \\ &= \begin{cases} m, & \text{falls, } \pi(i) \neq \pi(j) \neq m \\ \pi(i), & \text{falls, } m = \pi(j) \\ \pi(j), & \text{falls, } m = \pi(i) \end{cases} \end{aligned}$$

Damit gilt $\pi(i, j)\pi^{-1} = (\pi(i), \pi(j))$. #

Folgerung 56: *Jede Permutation* π *ist das Produkt von Transpositionen.*

Beweis: Jede Permutation lässt sich als Produkt von r-Zyklen schreiben, wobei $r \geq 2$. Jeder r-Zyklus mit $r > 2$ lässt sich mit Satz 55 in ein Produkt von Transpositionen zerlegen. #

Definition 57: *Eine Permutation heißt* gerade*, wenn sie als Produkt einer geraden Anzahl von Transpositionen darstellbar ist.*

Definition 58: *Sei* $\mathcal{G} = (G, \circ)$ *eine Gruppe mit neutralen Element* e *und* $U \subseteq G$*. Die Algebra* $\mathcal{U} = (U, \circ)$ *heißt* Untergruppe *(von* $\mathcal{G}$*) gdw. für alle* $a, b \in U$ *auch* $a \circ b \in U$ *gilt (d.h. U ist abgeschlossen unter der Gruppenoperation „*$\circ$*“) und für alle* $a \in U$ *ist auch* $a^{-1} \in U$ *(d.h die Untergruppe ist abgeschlossen gegen die Inversenbildung) (kurz:* $\mathcal{U} \subseteq \mathcal{G}$*).*

Die Untergruppen $(\{e\}, \circ)$ *und* $(G, \circ)$ *heißen die* trivialen Untergruppen *(von* $\mathcal{G}$*).*

Beispiel 59:

- *Die endliche Gruppe* $\mathcal{K}_4 = (\{0, 1, a, b\}, \odot)$ *ist durch die folgendende Gruppentafel gegeben:*

$\odot$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

und

$\odot$	0	1
0	0	1
1	1	0

ist eine Untergruppe von $\mathcal{K}_4$*. Die Gruppe* $\mathcal{K}_4$ *ist auch als die „Kleinsche Vierergruppe“ bekannt*[5]*.*

- *Sei* $k\mathbb{Z} =_{\text{def}} \{g \in \mathbb{Z} \mid k \text{ teilt } g\} = \{g \in \mathbb{Z} \mid \text{es gibt ein } g' \in \mathbb{Z} \text{ mit } g = k \cdot g'\}$*, dann ist* $(k\mathbb{Z}, +)$ *eine Untergruppe von* $(\mathbb{Z}, +)$*.*
- $(\mathbb{R} \setminus \{0\}, \cdot)$ *ist eine Untergruppe von* $(\mathbb{C} \setminus \{0\}, \cdot)$*.*

Der folgende Satz von Cayley[6] zeigt, dass *alle* endlichen Gruppen in mindestens einer symmetrischen Gruppe eingebettet sind. Dies unterstreicht die Wichtigkeit der symmetrischen Gruppen.

Satz 60 (Cayley): *Jede endliche Gruppe der Ordnung* n *ist isomorph zu einer Untergruppe der* S_n*.*

Beweis: Sei $\mathcal{G} = (G, \cdot)$ eine beliebige endliche Gruppe mit neutralen Element e und der Ordnung $n = \#G$. Wir definieren die Familie von Abbildungen $\pi_a \colon G \to G$ mit $\pi_a(x) = a \cdot x$, wobei $a \in G$.

Jede Abbildung π_a ist bijektiv und total, denn aus $\pi_a(x) = \pi_a(x')$ folgt $a \cdot x = a \cdot x'$ und mit den Kürzungsregeln (siehe Satz 46) gilt dann $x = x'$, also ist π_a injektiv. Sei nun $g \in G$, dann gilt $\pi_a(a^{-1}g) = a \cdot a^{-1} \cdot g = g$, was die Surjektivität von π_a zeigt. Die Totalität der Funktionen π_a ist offensichtlich.

Die Algebra $\Pi^G =_{\text{def}} (\{\pi_a \mid a \in G\}, \circ)$ bildet eine Gruppe, da

i) „$\circ$“ assoziativ ist.

ii) Für π_e und $a \in G$ gilt $\pi_a \circ \pi_e = \pi_a = \pi_e \circ \pi_a$, d.h. π_e ist das neutrale Element von Π^G.

iii) Seien $\pi_a, \pi_b \in \Pi^G$, dann gilt $\pi_a \circ \pi_b = \pi_a(bx) = abx = \pi_{ab}(x)$, d.h. „$\circ$“ ist abgeschlossen.

iv) Sei $a \in G$, dann gilt $\pi_a \circ \pi_{a^{-1}} = \pi_e = \pi_{a^{-1}} \circ \pi_a$, d.h. zu jedem Element $\pi_a \in \Pi^G$ existiert ein inverses Element.

Wir definieren $\eta \colon G \to \{\pi_a \mid a \in G\}$ durch $\eta(a) = \pi_a$. Nach Definition ist η surjektiv und total. Weiterhin ist η injektiv, denn wenn $\eta(a) = \eta(b)$, dann gilt $\pi_a = \pi_b$, $ax = bx$ und damit $a = b$. Weiterhin gilt $\eta(a \cdot b) = \pi_{ab}(x) = (ab)x = a(bx) = a \cdot \pi_b(x) = \pi_a(\pi_b(x)) = \pi_a \circ \pi_b$, d.h. η ist ein Homomorphismus.

Damit gilt $G \cong \Pi^G$. Die Menge Π^G besteht nur aus Permutationen der n-elementigen Menge G, d.h. $\Pi^G \subseteq S(G)$ und damit ist $\mathcal{G}$ isomorph zu einer Untergruppe der S_n. #

[5] Der deutsche Mathematiker Felix Klein wurde 1849 in Düsseldorf geboren und starb 1925 in Göttingen.

[6] Der englische Mathematiker Arthur Cayley wurde 1821 in Richmond (England) geboren und starb 1895 in Cambridge (England).

Definition 61: *Sei $\mathcal{G} = (G, \cdot)$ eine Gruppe und $\mathcal{U} = (U, \cdot)$ eine Untergruppe von $\mathcal{G}$. Für jedes $a \in G$ heißt*

$$aU =_{\text{def}} \{a \cdot x \mid x \in U\}$$

Linksnebenklasse *und*

$$Ua =_{\text{def}} \{x \cdot a \mid x \in U\}$$

Rechtsnebenklasse *von $\mathcal{U}$.*

Beispiel 62: *Die Untergruppe $(5\mathbb{Z}, +)$ von $(\mathbb{Z}, +)$ besitzt die folgenden fünf Nebenklassen:*

- $5\mathbb{Z} = \{x \mid x = 5y, y \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$,
- $5\mathbb{Z} + 1 = \{x \mid x = 5y + 1, y \in \mathbb{Z}\} = \{1, -4, 6, -9, 11, -14, 16, \ldots\}$,
- $5\mathbb{Z} + 2 = \{x \mid x = 5y + 2, y \in \mathbb{Z}\} = \{2, -3, 7, -8, 12, -13, 17, \ldots\}$,
- $5\mathbb{Z} + 3 = \{x \mid x = 5y + 3, y \in \mathbb{Z}\} = \{3, -2, 8, -7, 13, -12, 18, \ldots\}$ *und*
- $5\mathbb{Z} + 4 = \{x \mid x = 5y + 4, y \in \mathbb{Z}\} = \{4, -1, 9, -6, 14, -11, 19, \ldots\}$.

Beispiel 63: *Die Untergruppe $\{1, -1\}$ der Gruppe $(\mathbb{Q} \setminus \{0\}, \cdot)$ besitzt unendlich viele Nebenklassen $\{x, -x\}$ für alle $x \in \mathbb{Q} \setminus \{0\}$.*

Der folgende Satz macht eine Aussage über die Mächtigkeit von Untergruppen einer endlichen Gruppe und wird dem Mathematiker Joseph-Louis Lagrange[7] zugeschrieben.

Satz 64 (Lagrange): *Sei $\mathcal{G} = (G, \cdot)$ eine endliche Gruppe und $\mathcal{U} = (U, \cdot)$ eine Untergruppe von $\mathcal{G}$. Dann gilt $\#G$ ist ein Vielfaches von $\#U$.*

Beweis: Wir legen eine Relation „$\sim$“ wie folgt fest: für $a, b \in U$ gilt $a \sim b$ gdw. $ba^{-1} \in U$. Die Relation $\sim\colon G \times G$ ist eine Äquivalenzrelation, denn

- für alle $a \in G$ gilt $aa^{-1} \in U$ also ist „$\sim$“ reflexiv,
- für alle $a, b \in G$ folgt aus $ba^{-1} \in U$ auch $(ba^{-1})^{-1} = ab^{-1} \in U$, d.h. wenn $a \sim b$ gilt, dann ergibt sich auch $b \sim a$, was zeigt, dass „$\sim$“ symmetrisch ist, und
- seien $a, b, c \in G$, $a \sim b$ und $b \sim c$. Also gilt $ba^{-1} \in U$ und $cb^{-1} \in U$. Damit ergibt sich $cb^{-1}ba^{-1} = ca^{-1} \in U$ und $a \sim c$, was die Transitivität von „$\sim$“ zeigt.

Sei $a \in U$, dann gilt $[a]_\sim = Ua$, d.h. die Äquivalenzklassen von „$\sim$“ entsprechen den Rechtsnebenklassen von U.

$\supseteq$: Sei $b \in Ua$, also gibt es ein $x \in U$ mit $b = x \cdot a$. Damit ist $ba^{-1} = x \in U$ und $a \sim b$.

$\subseteq$: Sei $a \sim b$, also $ba^{-1} = x \in U$, dann ist $b = x \cdot a$ und $b \in Ua$.

Sei nun $\pi_a\colon U \to Ua$ mit $\pi_a(x) = x \cdot a$, dann ist π_a total und surjektiv, denn zu jedem $y \in Ua$ gibt es ein $x \in U$ mit $\pi_a(x) = y$. Weiterhin ist π_a injektiv, denn aus $\pi_a(x) = \pi_a(x')$ folgt $xa = x'a$ und $x = x'$. Damit gilt $\#Ua = \#U$ was zeigt, dass alle Äquivalenzklassen gleich mächtig sind. Da die Äquivalenzklassen eine Partition bilden, gibt es also ein $r \in \mathbb{N}$ mit $\#G = r \cdot \#U$ und damit ist $\#G$ ein Vielfaches von $\#U$. #

[7] Der französische Mathematiker wurde 1736 in Turin, Sardinia-Piedmont geboren und starb 1813 in Paris.

Bemerkung 65: *Aus dem Beweis von Satz 64 folgt auch, dass für zwei Nebenklassen Ua und Ub entweder $Ua = Ub$ oder $Ua \cap Ub = \emptyset$ gilt.*

Folgerung 66: *Sei G eine Gruppe und $\#G = p$, wobei $p \in \mathbb{P}$, dann hat G nur die trivialen Untergruppen.*

Folgerung 67: *Sei G eine Gruppe und $\#G = p$, wobei $p \in \mathbb{P}$, dann gibt es ein $g \in G$ mit $\{g^0, g^1, g^2, \ldots, g^{p-1}\} = G$.*

Beweis: Da G keine echten Untergruppen besitzt (siehe Folgerung 66), muss für die Menge $\{g^0, g^1, g^2, g^3, g^5, g^6, \ldots\} = G$ gelten, wenn $g \in G \backslash \{e\}$, denn nach Kürzungsregel (siehe Theorem 46) gilt $g^i \neq g^{i-1}$ für $0 \leq i < p$. Damit ist aber $\{g^0, g^1, g^2, \ldots, g^{p-1}\} = G$, da G nur aus p verschiedenen Elementen besteht. #

Bemerkung 68: *Sei $\langle g \rangle = \{g^i \mid i \in \mathbb{N}\}$ das* Erzeugnis *von g. Gibt es ein $g \in G$ mit $\langle g \rangle = G$, dann heißt die Gruppe G* zyklisch. *Zyklische Gruppen sind die Gruppen mit einer sehr einfachen Untergruppenstruktur, denn sei n die Ordnung von G, dann hat G (bis auf Isomorphie) für alle Teiler d von n genau eine Untergruppe der Ordnung d, die auch wieder zyklisch ist.*

4. Elementare Zahlentheorie

4.1. Restklassen und Restklassenringe

In diesem Abschnitt sollen einige (algebraische) Strukturen in Verbindung mit der Menge der ganzen Zahlen $\mathbb{Z}$ untersucht werden. Dazu wird die folgende grundlegende Definition benötigt:

Definition 69: *Eine Zahl $a \in \mathbb{Z}$* teilt *eine Zahl $n \in \mathbb{Z}$ (Schreibweise: $a \mid n$), wenn es ein $c \in \mathbb{Z}$ gibt mit $n = a \cdot c$. Gibt es kein solches c, so teilt a die Zahl n nicht (Schreibweise: $a \nmid n$).*

Damit ist n ein Vielfaches von a genau dann, wenn $a \mid n$ und aus dieser Definition ergeben sich die folgenden Rechenregeln:

Satz 70 (Teilbarkeitsregeln): *Seien $a, b, c \in \mathbb{Z}$, dann gilt:*

1. *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*
2. *Aus $a \mid b$ folgt $ac \mid bc$ für alle c.*
3. *Aus $c \mid a$ und $c \mid b$ folgt $c \mid (da + eb)$ für alle $d \in \mathbb{Z}$ und $e \in \mathbb{Z}$.*
4. *Aus $a \mid b$ und $b \neq 0$ folgt $|a| \leq |b|$.*
5. *Aus $a \mid b$ und $b \mid a$ folgt $|a| = |b|$.*

Beweis: Übungsaufgabe. #

Definition 71: *Die Menge aller* Teiler *einer Zahl n wird wie folgt definiert:*

$$T_n =_{\text{def}} \{d \in \mathbb{Z} \mid d \text{ teilt } n\}$$

Beispiel 72: *Für $n = 28$ ergibt sich $T_{28} = \{1, 2, 4, 7, 14, 28\}$. Sei nun*

$$\sigma(n) = \sum_{x \in T_n \setminus \{n\}} x.$$

Eine Zahl n heißt vollkommen*, wenn $\sigma(n) = n$. Mit dieser Definition ist 28 eine vollkommene Zahl. Bis heute sind nur 44 vollkommene Zahlen bekannt[8]. Die größte bekannte vollkommene Zahl hat ungefähr $1.96 * 10^7$ Dezimalstellen.*

Lemma 73 (Division mit Rest): *Seien $a, b \in \mathbb{Z}$, dann gibt es* eindeutig *bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < b$, so dass $a = qb + r$.*

Beweis: Übung. #

Vergleichbar mit der Konstruktion des Monoids in Beispiel 42 definieren wir nun eine Äquivalenzrelation auf $\mathbb{Z}$ und studieren die Äquivalenzklassen:

Definition 74: *Sei $m \in \mathbb{N}$ und $m \geq 2$, dann definieren wir $\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$ mit $x \equiv_m y$ gdw. $m \mid (x - y)$. Üblicherweise schreibt man $x \equiv y \bmod n$ statt $x \equiv_m y$ (Sprechweise: x* kongruent *y modulo n). Diese Definition geht auf Carl Friedrich Gauss[9] zurück.*

Lemma 75: *Sei $m \in \mathbb{N}$, $m \geq 2$, dann ist „$\equiv_m$“ eine Äquivalenzrelation mit m verschiedenen Äquivalenzklassen.*

Beweis: Sei $a \in \mathbb{Z}$, dann gilt $m \mid (a - a)$, da $m \mid 0$. Also ist $\equiv_m$ reflexiv. Seien $a, b \in Z$ und $m \mid (a - b)$, dann gilt $a - b = c \cdot m$, $b - a = (-c) \cdot m$ und damit ist $b \equiv_m a$, was die Symmetrie zeigt. Seien $a, b, c \in \mathbb{Z}$, $a \equiv_m b$, $b \equiv_m c$, dann gibt es d und d' mit $a - b = d \cdot m$ bzw. $b - c = d' \cdot m$. Also ist $a - b + b - c = dm + d'm$, $a - c = (d + d')m$ und somit $a \equiv_m c$, womit auch die Transitivität gezeigt ist.

Mit Lemma 73 ergeben sich die m verschiedenen Äquivalenzklassen:

$$\begin{array}{rcll}
[0]_{\equiv_m} & = & \{x \in \mathbb{Z} \mid x = m \cdot q\} & = \{x \in \mathbb{Z} \mid x/m \text{ ergibt Rest } 0\} \\
[1]_{\equiv_m} & = & \{x \in \mathbb{Z} \mid x = m \cdot q + 1\} & = \{x \in \mathbb{Z} \mid x/m \text{ ergibt Rest } 1\} \\
[2]_{\equiv_m} & = & \{x \in \mathbb{Z} \mid x = m \cdot q + 2\} & = \{x \in \mathbb{Z} \mid x/m \text{ ergibt Rest } 2\} \\
 & \vdots & & \vdots \\
[m-1]_{\equiv_m} & = & \{x \in \mathbb{Z} \mid x = m \cdot q + (m-1)\} & = \{x \in \mathbb{Z} \mid x/m \text{ ergibt Rest } m-1\}
\end{array}$$

Da „$\equiv_m$“ eine Äquivalenzrelation ist, bilden die Äquivalenzklassen eine Partition, d.h. jede ganze Zahl gehört zu *genau einer* Klasse. #

Offensichtlich ist jedes $a \in \mathbb{Z}$ kongruent zu einer Zahl $0 \leq r < m$, d.h. die Zahlen $0 \leq r < m$ sind Repräsentanten für alle Restklassen in $\mathbb{Z}_m$. Sie heißen auch die *natürlichen Repräsentanten*. Mit Hilfe dieser Beobachtungen gilt offensichtlich:

Folgerung 76: *Seien $x, y \in \mathbb{Z}$, dann sind die folgenden Aussagen äquivalent:*

i) $x \equiv_m y$

ii) $x \equiv y \bmod m$

iii) es gibt ein $q \in \mathbb{Z}$ mit $x = q \cdot m + y$

iv) x und y lassen bei der Division durch m den gleichen Rest

Bemerkung 77: *Die Klassen $[a]_{\equiv_m}$ heißen* Restklassen $\bmod m$ *und mit $\mathbb{Z}_m$ bezeichnen wir die Menge aller dieser Restklassen, d.h. $\mathbb{Z}_m =_{\text{def}} \{[a]_{\equiv_m} \mid 0 \leq a < m\}$.*

[8] Siehe z.B. http://www.mersenne.org/

[9] Carl Friedrich Gauss wurde 1777 in Braunschweig geboren und starb 1855 in Göttingen. Er wird oft als der bedeutendste Mathematiker aller Zeiten betrachtet.

4.2. Weitere algebraische Strukturen

Definition 78: *Eine Algebra* $\mathcal{R} = (R, +, \cdot)$ *vom Typ* $(2, 2)$ *heißt* Ring*, wenn*

i) $(R, +)$ *eine abelsche Gruppe,*

ii) $(R, \cdot)$ *eine Halbgruppe ist und*

iii) für alle $a, b, c \in R$ *die zwei Distributivgesetze gelten:*

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $(a + b) \cdot c = a \cdot c + b \cdot c$

Ist „·“ zusätzlich noch kommutativ, so heißt $\mathcal{R}$ kommutativer Ring*. Existiert ein neutrales Element für „·“, dann heißt* $\mathcal{R}$ Ring mit Eins(element)*.*

Beispiel 79:

- $(\mathbb{Z}, +, \cdot)$ *ist ein kommutativer Ring mit Eins*
- *Sei* $n \in \mathbb{N}$*, dann ist die Menge der reellwertigen* $n \times n$ *Matrizen mit der normalen Addition und Multiplikation von Matrizen ein Ring mit Eins.*

Definition 80: *Eine Algebra* $\mathcal{F} = (F, +, \cdot)$ *heißt* Körper *(engl.* Field*), wenn*

- $(F, +, \cdot)$ *ein Ring und*
- $(F \setminus \{0\}, \cdot)$ *eine abelsche Gruppe*[10] *ist.*

Beispiel 81: *Die Algebren* $(\mathbb{Q}, +, \cdot)$*,* $(\mathbb{R}, +, \cdot)$ *und* $(\mathbb{C}, +, \cdot)$ *sind Körper.*

4.3. Restklassenringe

Wir wissen schon, dass die Relation $\equiv_m \subseteq \mathbb{Z} \times \mathbb{Z}$ eine Äquivalenzrelation ist, d.h. $\mathbb{Z}$ wird in (endlich viele) Klassen partitioniert. Damit erscheint die folgende Definition natürlich:

Definition 82: *Sei* $m \in \mathbb{N}, m \geq 2$*, dann*

- $[a]_{\equiv_m} \oplus [b]_{\equiv_m} =_{\text{def}} [a + b]_{\equiv_m}$
- $[a]_{\equiv_m} \odot [b]_{\equiv_m} =_{\text{def}} [a \cdot b]_{\equiv_m}$

Satz 83: *Sowohl die Addition von Restklassen „⊕“ als auch die Multiplikation von Restklassen „⊙“ ist wohldefiniert, d.h. für* $m \in \mathbb{N}, m \geq 2$ *und* $a, a', b, b' \in \mathbb{Z}$ *gilt: Wenn* $a \equiv a' \bmod m$ *und* $b \equiv b' \bmod m$*, dann ist auch:*

- $[a]_{\equiv_m} \oplus [b]_{\equiv_m} = [a']_{\equiv_m} \oplus [b']_{\equiv_m}$ *und*
- $[a]_{\equiv_m} \odot [b]_{\equiv_m} = [a']_{\equiv_m} \odot [b']_{\equiv_m}$.

[10] Fordert man für $(F \setminus \{0\}, \cdot)$ nur die Gruppeneigenschaft, dann erhält man die Definition der so genannten *Schiefkörper*. Ein bekannter Schiefkörper sind die Quaternion über $\mathbb{C}$. Endliche Schiefkörper gibt es nicht, da man zeigen kann, dass jeder endliche Schiefkörper kommutativ ist, d.h. schon ein Körper ist (vgl. Satz von Wedderburn).

Beweis: Da $\equiv_m$ ein Äquivalenzrelation ist, reicht es die Beziehungen $a+b \equiv a'+b' \bmod m$ und $a \cdot b \equiv a' \cdot b' \bmod m$ zu zeigen.

Wir wissen, dass $m \mid (a - a')$, also $a - a' = c_1 \cdot m$ und analog $b - b' = c_2 \cdot m$. Also ergibt sich

$$\begin{aligned} & (a - a') + (b - b') &=& \; c_1 \cdot m + c_2 \cdot m \\ \Leftrightarrow \; & (a + b) - (a' + b') &=& \; (c_1 + c_2) \cdot m. \end{aligned}$$

Damit folgt $m \mid (a + b) - (a' + b')$ und $a + b \equiv a' + b' \bmod m$. Außerdem gilt

$$\begin{aligned} ab - a'b' &= (c_1 m + a') \cdot b - a'b' \\ &= bc_1 m + a'b - a'b' \\ &= bc_1 m + (b - b')a' \\ &= bc_1 m + c_2 m a' \\ &= (c_1 b + c_2 a') \cdot m, \end{aligned}$$

d.h. $m \mid (ab - a'b')$ und damit $ab \equiv a'b' \bmod m$. #

Satz 84: *Sei $m \in \mathbb{N}, m \geq 2$, dann ist $(\mathbb{Z}_m, \oplus, \odot)$ ein Ring und heißt der Restklassenring* $\bmod m$.

Beweis: Übung #

Folgerung 85: *Sei $m \in \mathbb{N}, m \geq 2$, dann ist $(\mathbb{Z}_m, \oplus, \odot)$ ein kommutativer Ring mit Eins.*

Bemerkung 86:

- *In der Literatur wird sehr oft auch die Schreibweise $\mathbb{Z}/m\mathbb{Z}$ für $\mathbb{Z}_m$ verwendet (Stichwort: Quotientenring).*
- *Statt „$\oplus$“ (bzw. „$\odot$“) schreibt man aus Bequemlichkeit auch oft „$+$“ (bzw. „$\cdot$“).*
- *Für eine Restklasse $[a]_{\equiv_m}$ schreibt man häufig nur a (Repräsentant der Restklasse).*

4.4. Der größte gemeinsame Teiler

Definition 87: *Seien $a, b \in \mathbb{Z}$ mit $|a| + |b| \neq 0$, dann heißt die größte Zahl $g \in \mathbb{Z}$ mit $g \mid a$ und $g \mid b$ der* größte gemeinsame Teiler *von a und b (Schreibweise:* $\mathrm{ggT}(a, b)$ *oder $gcd(a, b)$ für greatest common divisor). Weiterhin soll* $\mathrm{ggT}(0, 0) =_{\mathrm{def}} 0$ *gelten. Zwei Zahlen heißen* teilerfremd *(*coprim*,* relativ prim*), wenn* $\mathrm{ggT}(a, b) = 1$ *gilt.*

Satz 88 (Rechenregeln für den ggT): *Für alle $a, b, c \in \mathbb{Z}$ gelten die folgenden Rechenregeln:*

i) $\mathrm{ggT}(a, b) = \mathrm{ggT}(-a, b) = \mathrm{ggT}(a, -b)$

ii) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$

iii) $\mathrm{ggT}(a, b) = \mathrm{ggT}(a + bc, b)$

Beweis:

i) Offensichtlich gilt für die Menge der Teiler von a bzw. $-a$ die Gleichheit, d.h. $T_a = T_{-a}$. Daraus ergibt sich $\mathrm{ggT}(a, b) = \max(T_a \cap T_b) = \max(T_a \cap T_{-b}) = \max(T_{-a} \cap T_b) = \mathrm{ggT}(-a, b) = \mathrm{ggT}(a, -b)$.

ii) ergibt sich direkt aus der Definition

iii) **Fall** $b = 0$**:** $\mathrm{ggT}(a + bc, b) = \mathrm{ggT}(a, 0) = \mathrm{ggT}(a, b) = a$, da alle ganzen Zahlen die 0 teilen, weshalb $\mathrm{ggT}(a, 0) = a$ gelten muss.

Fall $b \neq 0$**:** Es gilt $\#T_b < \infty$, d.h. auch $\#(T_a \cap T_b) < \infty$ und $\#(T_b \cap T_{a+bc}) < \infty$. Wir zeigen $T_a \cap T_b = T_b \cap T_{a+bc}$.

„$\subseteq$“ Sei $t \in T_a \cap T_b$, also gilt sowohl $t \mid a$ als auch $t \mid b$. Mit der Teilbarkeitsregel *iii*) des Satzes 70 ergibt sich $t \mid (a + bc)$ und damit $t \in T_b \cap T_{a+bc}$.

„$\supseteq$“ Sei $t \in T_b \cap T_{a+bc}$, dann gibt es $d_1, d_2 \in \mathbb{Z}$ mit $td_1 = b$ und $td_2 = a + bc$, denn $t \mid b$ und $t \mid (a + bc)$. Also gilt $tcd_1 = bc$ und damit $td_2 - tcd_1 = a + bc - bc = a$. Deshalb gilt $(d_2 - cd_1)t = a$ und $t \mid a$, d.h. $t \in T_a \cap T_b$.

Damit haben die endlichen Teilermengen $T_a \cap T_b$ und $T_{a+bc} \cap T_b$ das gleiche Maximum, was $\mathrm{ggT}(a, b) = \mathrm{ggT}(a + bc, b)$ für den Fall $b \neq 0$ zeigt.

Damit sind diese Rechenregeln für den ggT gezeigt. #

Folgerung 89 (Schleifeninvariante des euklidischen Algorithmus): *Es gilt für* $a, b \in \mathbb{Z}$

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b).$$

Satz 90 (Lineardarstellung des ggT): *Seien* $a, b \in \mathbb{Z}$*, dann existieren* $x, y \in \mathbb{Z}$ *mit*

$$d = \mathrm{ggT}(a, b) = ax + by$$

Beweis: Dies kann z.B. durch die Analyse des „erweiterten Euklidischen Algorithmus“ gezeigt werden. #

Folgerung 91: *Sei* $m \in \mathbb{N}, m \geq 2$*. Gilt* $\mathrm{ggT}(a, m) = 1$ *mit* $0 \leq a < m$*, dann hat* a *ein multiplikativ Inverses im Restklassenring* $\mathbb{Z}_m$*.*

Beweis: Gilt $\mathrm{ggT}(a, m) = 1$, dann gibt es nach Satz 90 Zahlen $x, y \in \mathbb{Z}$ mit $ax + my = 1$, also $ax \equiv 1 \bmod m$, d.h. x ist das multiplikativ inverse Element von a in $\mathbb{Z}_m$. #

Folgerung 92: *Sei* $p \in \mathbb{P}$*, dann ist* $\mathbb{Z}_p$ *ein Körper.*

Definition 93: *Sei* $\Phi \colon \mathbb{N} \to \mathbb{N}$ *eine Funktion, die wie folgt definiert wird:*

$$\Phi(m) =_{\mathrm{def}} \#\{a \mid 0 \leq a < m \text{ und } \mathrm{ggT}(a, m) = 1\}.$$

Diese Funktion wird als Eulersche Φ-Funktion *bezeichnet (engl. Euler's totient function).*

Die Eulersche[11] Φ-Funktion gibt die Anzahl der Zahlen $1 \leq a < m$ an, die teilerfremd zu m sind. D.h. aufgrund von Folgerung 91 gibt $\Phi(m)$ auch die Mächtigkeit der multiplikativen Einheitengruppe des Restklassenrings $\mathbb{Z}_m$ an.

[11] Der Schweizer Mathematiker Leonhard Euler wurde 1707 in Basel geboren und starb 1783 in St. Petersburg.

Satz 94 (Satz von Euler): *Sei $a \in \mathbb{N} \setminus \{0\}$ und $m \in \mathbb{N}, m \geq 2$. Gilt* $\mathrm{ggT}(a, m) = 1$*, dann ist*

$$a^{\Phi(m)} \equiv 1 \bmod m.$$

Beweis: Sei $\mathbb{Z}_m^* = \{a_1, \ldots, a_{\Phi(m)}\}$ die Einheitengruppe des multiplikativen Monoids des Restklassenrings $\mathbb{Z}_m$, dann gilt

$$\begin{aligned} a^{\Phi(m)} \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{\Phi(m)} &\equiv aa_1 \cdot aa_2 \cdot \ldots \cdot aa_{\Phi(m)} \\ &\equiv a_1 \cdot a_2 \cdot \ldots \cdot a_{\Phi(m)} \bmod m \end{aligned}$$

Da $\mathbb{Z}_m^*$ eine Gruppe ist, ergibt sich mit den Kürzungsregeln in Gruppen (siehe Satz 46 auf Seite 19) $a^{\Phi(m)} \equiv 1 \bmod m$. #

Damit ergibt sich die folgende Aussage, die Fermat[12] zugeschrieben wird:

Folgerung 95 (Kleiner Satz von Fermat): *Sei $p \in \mathbb{P}$ und $a \not\equiv 0 \bmod p$, dann gilt*

$$a^{p-1} \equiv 1 \bmod p.$$

Beweis: Wenn $p \in \mathbb{P}$, dann gilt $\Phi(p) = p - 1$. Dann folgt die Aussage direkt aus dem Satz von Euler (siehe Satz 94). #

Sowohl Satz 94 als auch Folgerung 95 können als Spezialfall des Satzes von Lagrange (vgl. Satz 64) ausgefasst werden, denn die Menge der Einheiten $\mathbb{Z}_m^*$ von $\mathbb{Z}_m$ bilden eine *kommutative* Gruppe. Eine direkte Anwendung des Satzes von Euler ist das asymmetrische RSA[13] Public-Key Cryptosystem:

Anwendung 96: *Zur Durchführung des RSA-Verfahrens werden zwei Phasen benötigt:*

Schlüsselerzeugung:

i) Wähle zwei Primzahlen p und q

ii) Berechne $n = p \cdot q$ und $\Phi(n) = (p-1)(q-1)$

iii) Wähle ein e mit $\mathrm{ggT}(e, \Phi(n)) = 1$

iv) Berechne ein d mit $e \cdot d \equiv 1 \bmod \Phi(n)$

Ver- und Entschlüsselung:

- *Verschlüsselung:* $E(x) = x^e \bmod n$.
- *Entschlüsselung:* $D(x) = x^d \bmod n$

Satz 97: *Sei E die RSA-Verschlüsselungsfunktion und D die dazu passende Entschlüsselungsfunktion, dann gilt:*

$$E \circ D \;=\; D \circ E \;=\; id.$$

Beweis: Wir müssen zeigen: $x^{ed} \equiv x \bmod n$ für alle Nachrichten $x \in \mathbb{Z}_n$.

Fall $x \in \mathbb{Z}_n^*$**:** Wir wissen $ed - k\phi(n) = 1$, da $\phi(n) \mid (ed - 1)$, also $ed = 1 + k\phi(n)$ und damit:

$$x^{ed} \;\equiv\; x^{1+k\phi(n)} \equiv x \cdot (\underbrace{x^{\phi(n)}}_{\equiv 1 \text{ „Euler“}})^k \;\equiv\; x \bmod n.$$

[12] Der französische Mathematiker Pierre de Fermat wurde am 1601 in Beaumont-de-Lomagne geboren und starb am 1665 in Castres.

[13] Das RSA-Verfahren ist nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannt.

Fall $x \notin Z_n^*$**:** Wenn $p \mid x$ und $q \mid x$, dann $x \equiv 0 \bmod n$ und damit $x^{ed} \equiv x \bmod n$. O.B.d.A. sei nun $p \mid x$ und $q \nmid x$, also $x^{ed} \equiv x \bmod p$, weil $x \equiv 0 \bmod p$, und analog zum obigen $x^{ed} \equiv x \bmod q$, weil $1 = ed - k\phi(n) = ed - k(p-1)(q-1) = ed - k(p-1)\phi(q)$. Also insgesamt $x^{ed} \equiv (x^e)^d \equiv x \bmod n$.

Offensichtlich können wir die Rollen des öffentlichen Exponenten e und des privaten Exponenten d vertauschen, was auch $D \circ E = id$ zeigt. #

Beispiel 98: *Sei* $p = 11$, $q = 17$ *und* $e = 3$. *Dann ergibt sich* $n = 11 \cdot 17 = 187$, $\Phi(n) = 10 \cdot 16 = 160 = 2^5 \cdot 5$. *Also ist* $\mathrm{ggT}(3, 160) = 1$ *und damit existiert ein multiplikativ Inverses von* 3 *in* $\mathbb{Z}_{160}$ *und der öffentliche Schlüssel wurde korrekt gewählt.*

Wir wissen, durch Abarbeiten des Euklidischen Algorithmus, dass $160 = 50 \cdot 3 + 10$ *und* $10 = 3 \cdot 3 + 1$. *Damit gilt* $10 - 3 \cdot 3 = 1$ *bzw.* $160 - 50 \cdot 3 = 10$. *Zusammen ergibt sich* $160 - 50 \cdot 3 - 3 \cdot 3 = 1$ *und* $1 \cdot 160 - 53 \cdot 3 = 1$. *D.h.* $-53 \cdot 3 \equiv 1 \bmod 160$, *also ist das gesuchte Inverse von* 3 *in* $\mathbb{Z}_{160}$ *ist gegeben durch* $-53 \equiv 160 - 53 \equiv \mathbf{107} \bmod 160$. *Probe:* $107 \cdot 3 \equiv 321 \equiv 2 \cdot 160 + 1 \equiv 1 \bmod 160$. *Damit sind die RSA-Schlüssel:*

- *Öffentlicher Schlüssel:* $(3, 187)$
- *Geheimer Schlüssel:* $(107, 187)$

Wir verschlüsseln $x = 5$ *und erhalten* $5^3 \equiv 25 \cdot 5 \equiv 125 \bmod 187$. *Für die Entschlüsselung berechnen wir* $127^{107} \equiv 5 \bmod 187$ *schrittweise wie folgt:*

$$\begin{array}{lcllcll}
125^{107} & \equiv & (125)^{106} \cdot 125 & \equiv & 15 \cdot 125 & \equiv & \mathbf{5} \bmod 187 \\
125^{106} & \equiv & ((125)^{53})^2 & \equiv & 75^2 & \equiv & 15 \bmod 187 \\
125^{53} & \equiv & (125)^{52} \cdot 125 & \equiv & 38 \cdot 125 & \equiv & 75 \bmod 187 \\
125^{52} & \equiv & ((125)^{26})^2 & \equiv & 15^2 & \equiv & 38 \bmod 187 \\
125^{26} & \equiv & ((125)^{13})^2 & \equiv & 163^2 & \equiv & 15 \bmod 187 \\
125^{13} & \equiv & (125)^{12} \cdot 125 & \equiv & 115 \cdot 125 & \equiv & 163 \bmod 187 \\
125^{12} & \equiv & ((125)^6)^2 & \equiv & 59^2 & \equiv & 115 \bmod 187 \\
125^6 & \equiv & ((125)^3)^2 & \equiv & 97^2 & \equiv & 59 \bmod 187
\end{array}$$

D.h. Zwischenwerte wie z.B. $125^2 \equiv 15 \bmod 187$ *werden rekursiv berechnet.*

5. Funktionen und Rekurrenzen

5.1. Asymptotische Notationen

Bei der Analyse von Algorithmen wird oft die O-Notation verwendet

$$O(f) = \{g(n) \mid \exists c \exists n_0 \forall n \text{ mit } n \geq n_0 \text{ gilt } g(n) \leq c \cdot f(n)\}.$$

Da hier f nur eine *asymptotische obere Schranke* für die Funktionen aus $O(f)$ darstellt, kann diese Schranke sehr grob ausfallen:

$$n^2 \in O(2^n)$$

Die folgende Modifikation soll helfen die Abschätzungen genauer vornehmen zu können:

Definition 99 (Θ-Notation): *Sei* $f : \mathbb{N} \to \mathbb{N}$ *eine Funktion, dann ist*

$$\Theta(f) =_{\text{def}} \{g(n) \mid \exists c_1 \exists c_2 \exists n_0 \text{ mit } c_1, c_2, n_0 \in \mathbb{N} \text{ und } \forall n\ n \geq n_0 \text{ ist } 0 \leq c_1 \cdot f(n) \leq g(n) \leq c_2 \cdot f(n)\}$$

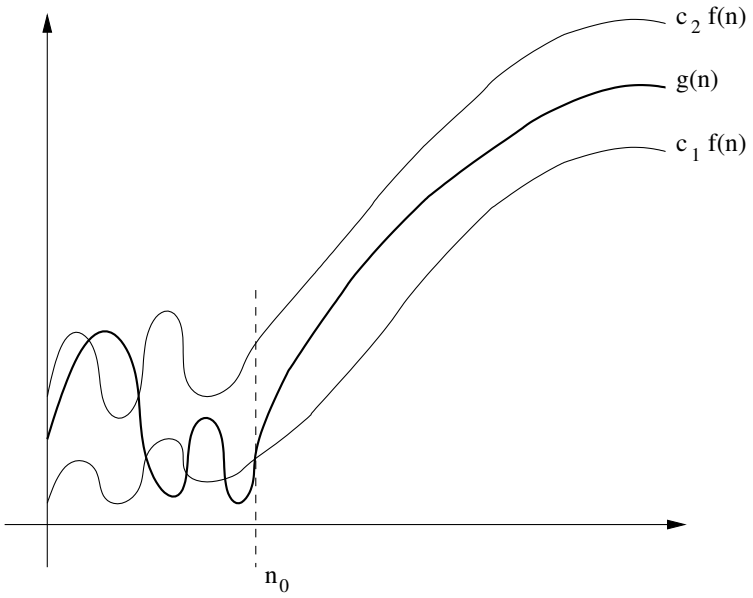


Abbildung 3: Graphische Darstellung der Θ-Notation

Diese Definition bewirkt, dass die Funktion g ab n_0 zwischen $c_1 \cdot f(n)$ und $c_2 \cdot f(n)$ „eingeklemmt“ (siehe Abbildung 3) ist. Für $g(n) \in \Theta(f(n))$ bezeichnet man f als eine *asymptotische dichte Schranke*.

Beispiel 100: *Es gilt* $\frac{1}{2}n^2 - 3n \in \Theta(n^2)$*, da*

$$\frac{1}{2}n^2 - 3n \leq \frac{1}{2}n^2 + \frac{1}{2}n \underbrace{\leq}_{ab\ n \geq 2} \frac{1}{2}n^2 + \frac{1}{2}n^2 = \underbrace{1}_{c_2} \cdot n^2$$

und

$$\frac{1}{2}n^2 - 3n \underbrace{\geq}_{ab\ n \geq 12} \frac{1}{2}n^2 - \frac{1}{4}n^2 = \underbrace{\frac{1}{4}}_{c_1} \cdot n^2.$$

Damit gilt für $n \geq 12$

$$0 \leq \underbrace{\frac{1}{4}}_{c_1} \cdot n^2 \leq \frac{1}{2}n^2 - 3n \leq \underbrace{1}_{c_2} \cdot n^2,$$

womit $\frac{1}{2}n^2 - 3n \in \Theta(n^2)$ *gezeigt ist.*

Beispiel 101: $n^2 \notin \Theta(2^n)$*, denn für alle* $c > 0$ *gilt*

$$c \cdot 2^n \underbrace{>}_{ab\ n_0} n^2.$$

Betrachtet man nun nur die obere Schranke, dann ergibt sich

Definition 102 (*O*-Notation): *Sei* $f \colon \mathbb{N} \to \mathbb{N}$ *eine Funktion, dann ist*

$$O(f) =_{\text{def}} \{g(n) \mid \exists c_2 \exists n_0 \text{ mit } c_2, n_0 \in \mathbb{N} \text{ und } \forall n\ n \geq n_0 \text{ ist } 0 \leq g(n) \leq c_2 \cdot f(n)\}$$

und für die asymptotische untere Schranke

Definition 103 (Ω-Notation): *Sei* $f\colon \mathbb{N} \to \mathbb{N}$ *eine Funktion, dann ist*

$$\Omega(f) =_{\text{def}} \{g(n) \mid \exists c_1 \exists n_0 \text{ mit } c_1, n_0 \in \mathbb{N} \text{ und } \forall n\ n \geq n_0 \text{ ist } 0 \leq c_1 \cdot f(n) \leq g(n)\}.$$

Lemma 104: *Für eine Funktion* g *gilt:*

$$g \in \Theta(f) \text{ gdw. } g \in O(f) \text{ und } g \in \Omega(f)$$

Beweis: Dies ist eine direkte Konsequenz aus den Definitionen 99, 102 und 103.# Eine asymptotische obere Schranke kann dicht für eine Funktion sein (z.B. $2n^2 \in O(n^2)$) oder auch nicht (z.B. $(3n \in O(n^2))$. Um notieren zu können, dass eine obere Schranke nicht dicht ist, führen wir die o-Notation (gesprochen: „little o“) ein:

Definition 105 (o-Notation): *Sei* $f\colon \mathbb{N} \to \mathbb{N}$ *eine Funktion, dann ist*

$$o(f(n)) =_{\text{def}} \{g(n) \mid \forall c \exists n_0 \text{ mit } c, n_0 \in \mathbb{N} \text{ und } \forall n\ n \geq n_0 \text{ ist } 0 \leq g(n) < c \cdot f(n)\}$$

Bemerkung 106: *Die Definitionen der O-Notation und der o-Notation sind sich recht ähnlich. Der Unterschied ist, dass bei der O-Notation für alle* $n \geq n_0$ $g(n) \leq c \cdot f(n)$ *für* eine *Konstante* c *gilt, wogegen bei der o-Notation* für alle c' *die Ungleichung* $g(n) < c' \cdot f(n)$ *gilt, wenn* $n \geq n_0$.

Lemma 107: *Sei* $\mathcal{F} \in \{\Theta, O, \Omega\}$*, dann gilt für Funktionen* f*,* g *und* h *die folgende Transitivitätseigenschaft*

$$\text{Wenn } f \in \mathcal{F}(g) \text{ und } g \in \mathcal{F}(h), \text{ dann } f \in \mathcal{F}(h).$$

Weiterhin gilt auch die Reflexivität

$$f \in \mathcal{F}(f).$$

Beweis: Wenn $f \in \Theta(g)$, dann existieren Konstanten $c_1', c_2' \geq 0$ und ein n_0' mit $0 \leq c_1' \cdot g(n) \leq f(n) \leq c_2' \cdot g(n)$, wenn $n \geq n_0'$. Wegen $g \in \Theta(h)$ existieren Konstanten $c_1'', c_2'' \geq 0$ und n_0'' mit $0 \leq c_1'' \cdot h(n) \leq g(n) \leq c_2'' \cdot h(n)$, wenn $n \geq n_0''$. Setzt man diese Ungleichungen zusammen, dann ergibt sich

$$0 \leq \underbrace{c_1' c_1''}_{=c_1} \cdot h(n) \leq c_1' \cdot g(n) \leq f(n) \leq c_2' \cdot g(n) \leq \underbrace{c_2' \cdot c_2''}_{=c_2} \cdot h(n).$$

Damit gilt $0 \leq c_1 \cdot h(n) \leq f(n) \leq c_2 \cdot h(n)$, was $f \in \Theta(h)$ zeigt. Analog argumentiert man für die Fälle $\mathcal{F} \in \{O, \Omega\}$.

Die Reflexivität folgt direkt aus den Definitionen 99, 102 und 103. #

5.2. Rekurrenzen

Eine Rekurrenz ist eine Gleichung (oder auch Ungleichung), bei der das Funktionssymbol auf der linken *und* rechten Seite vorkommt. D.h. eine Funktion wird durch Funktionswerte für kleinere Argumente beschrieben.

Beispiel 108: *Für MergeSort ergibt sich die folgende Laufzeit*

$$T(n) = \begin{cases} \Theta(1), & \text{falls } n = 1 \\ 2T(n/2) + \Theta(n), & \text{falls } n > 1 \end{cases}$$

Später wird gezeigt, dass $T(n) \in \Theta(n \log n)$ gilt. Zur Lösung von Rekurrenzen sind verschiedene Methoden bekannt, von denen hier nur die „Substitutionsmethode“ und das „Master-Theorem“ erwähnt werden sollen.

5.2.1. Substitutionsmethode

Die Substitutionsmethode besteht aus zwei Schritten:

i) Raten einer der Lösung

ii) Benutzen eine Induktion um evtl. Konstanten zu finden und um die Richtigkeit der geratenen Lösung zu zeigen.

Es soll nun eine obere Schranke für die Rekurrenz

$$T(n) = 2T(\lfloor n/2 \rfloor) + n$$

gefunden werden. Dabei soll angenommen[14] werden, dass $T(n) \in O(n \log n)$ gilt, damit ist $T(n) \leq c \cdot n \cdot \log n$ für eine geeignete Konstante c. Somit gilt auch $T(\lfloor n/2 \rfloor) \leq 2 \cdot \lfloor n/2 \rfloor \cdot \log \lfloor n/2 \rfloor$. Einsetzen ergibt

$$\begin{aligned} T(n) &\leq 2 \cdot (c \cdot \lfloor n/2 \rfloor \cdot \log \lfloor n/2 \rfloor) + n \\ &\leq c \cdot n \cdot \log n/2 + n \\ &= c \cdot n \log n - c \cdot n \cdot \log 2 + n \\ &= c \cdot n \cdot \log n - c \cdot n + n \\ &\leq c \cdot n \cdot \log n \end{aligned}$$

Dieses Vorgehen entspricht dem Induktionsschritt unter Anwendung der Induktionsvoraussetzung ($\triangleq$ Vermutung), d.h. der Induktionsanfang ist noch zu prüfen.

Annahme: $T(n) = 1$, dann gilt $T(1) \leq c \cdot 1 \log 1 = 0$. Damit würde der Induktionsanfang nicht gelten. Allerdings macht die O-Notation nur Aussagen über Zahlen n, die größer oder gleich einem n_0 sind, d.h. der Induktionsanfang ist für ein geeignetes n_0 zu prüfen. Also ist $T(1) = 1$ und mit der gegebenen Rekurrenz gelten $T(2) = 2T(1)+2 = 4$ und $T(3) = 2T(1)+3 = 5$. Wir wählen $n_0 = 2$ und müssen zeigen, dass $T(n) \leq c \cdot n \cdot \log n$ für $n \geq 2$ gilt. $4 = T(2) \leq 2 \cdot 2 \cdot \log 2$ und $5 = T(3) \leq 2 \cdot 3 \cdot \log 3$, d.h. ab $n_0 = 2$ gilt die Induktionsvoraussetzung.

Bei dieser Methode ergibt sich ein Problem, denn es ist unklar wie man im allgemeinen Fall die Lösung „rät“. Leider ist keine Standardmethode bekannt, d.h. Erfahrung und Kreativität sind gefragt. Eine weitere Möglichkeit zur Lösung von Rekurrenzen ist das Aufstellen von so genannten „Rekursionsbäumen“, da an dieser Stelle nicht näher auf diese Methode eingegangen werden soll wird auf [CLRS01] verwiesen. Statt dessen kann in vielen Fällen das „Master-Theorem“ zum Einsatz kommen.

5.2.2. Das Master-Theorem

Mit Hilfe von „Rekursionsbäumen“ (siehe [CLRS01]) lässt sich der folgende universell einsetzbare Satz zeigen.

Satz 109 (Master-Theorem): *Seien $a \geq 1$ und $b > 1$ Konstanten und $f(n)$ eine Funktion. Für $T\colon \mathbb{N} \to \mathbb{N}$ und*

$$T(n) = aT(n/b) + f(n),$$

wobei n/b als $\lceil n/b \rceil$ oder $\lfloor n/b \rfloor$ interpretiert werden kann, ergibt sich:

i) Falls $f(n) \in O(n^{\log_b a - \epsilon}), \epsilon > 0$, dann gilt $T(n) \in \Theta(n^{\log_b a})$.

ii) Falls $f(n) \in \Theta(n^{\log_b a})$, dann gilt $T(n) \in \Theta(n^{\log_2 a} \cdot \log_2 n)$.

[14] Die Vermutung ergibt sich an dieser Stelle leicht, da wir die Laufzeit von MergeSort schon kennen.

iii) Falls $f(n) \in \Omega(n^{\log_b a+\epsilon}), \epsilon > 0$ *und* $a \cdot f(n/b) \leq c \cdot f(n)$ *für eine Konstante* c*, dann ist* $T(n) \in \Theta(f(n))$*.*

Beispiel 110: *Sei* $T(n) = 9T(n/3) + n$*, dann ist* $a = 9$*,* $b = 3$ *und* $f(n) = n$*. Also ist* $f(n) \in O(n^{\log_3 9-\epsilon}), \epsilon = 1$*. Mit dem ersten Fall des „Master-Theorems“ (siehe Satz 109) ergibt sich* $T(n) \in \Theta(n^2)$*.*

Beispiel 111: *Sei* $T(n) = T(2n/3) + 1$*, also* $a = 1$*,* $b = 3/2$ *und* $f(n) = 1$*. Damit gilt* $n^{\log_b a} = n^{\log_{3/2} 1} = n^0 = 1$ *und deshalb gilt* $f(n) \in \Theta(n^{\log_b a})$*. Also ist* $T(n) \in \Theta(n^{\log_2 1} \cdot \log_2 n) = \Theta(\log_2 n)$*.*

⋆⋆⋆ Ende ⋆⋆⋆

A. Grundlagen und Schreibweisen

A.1. Mengen

Es ist sehr schwer den fundamentalen Begriff der Menge mathematisch exakt zu definieren. Aus diesem Grund soll uns hier die von Cantor 1895 gegebene Erklärung genügen, da sie für unsere Zwecke völlig ausreichend ist:

Erklärung 112 (Georg Cantor ([Can95])): *Unter einer ‚Menge' verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unsrer Anschauung oder unseres Denkens (welche die ‚Elemente' von M genannt werden) zu einem Ganzen*[15]*.*

Für die Formulierung „genau dann wenn" verwenden wir im Folgenden die Abkürzung gdw. um Schreibarbeit zu sparen.

A.1.1. Die Elementbeziehung und die Enthaltenseinsrelation

Definition 113: *Sei M eine beliebige Menge, dann ist*

- *$a \in M$ gdw. a ist ein Element der Menge M,*
- *$a \notin M$ gdw. a ist kein Element der Menge M,*
- *$M \subseteq N$ gdw. aus $a \in M$ folgt $a \in N$ (M ist Teilmenge von N),*
- *$M \not\subseteq N$ gdw. es gilt nicht $M \subseteq N$. Gleichwertig: es gibt ein $a \in M$ mit $a \notin N$ (M ist keine Teilmenge von N) und*
- *$M \subset N$ gdw. es gilt $M \subseteq N$ und $M \neq N$ (M ist echte Teilmenge von N).*

Statt $a \in M$ schreibt man auch $M \ni a$, was in einigen Fällen zu einer deutlichen Vereinfachung der Notation führt.

A.1.2. Definition spezieller Mengen

Spezielle Mengen können auf verschiedene Art und Weise definiert werden, wie z.B.

- durch Angabe von Elementen: So ist $\{a_1, \ldots, a_n\}$ die Menge, die aus den Elementen $a_1, \ldots, a_n$ besteht, oder
- durch eine Eigenschaft E: Dabei ist $\{a \mid E(a)\}$ die Menge aller Elemente a, die die Eigenschaft[16] E besitzen.

Beispiel 114:

- *Mengen, die durch die Angabe von Elementen definiert sind:*
  - $\mathbb{B} =_{\text{def}} \{0, 1\}$
  - $\mathbb{N} =_{\text{def}} \{0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots\}$ *(Menge der natürlichen Zahlen)*
  - $\mathbb{Z} =_{\text{def}} \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ *(Menge der ganzen Zahlen)*
  - $2\mathbb{Z} =_{\text{def}} \{0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\}$ *(Menge der geraden ganzen Zahlen)*

[15] Diese Zitat entspricht der originalen Schreibweise von Cantor.
[16] Die Eigenschaft E kann man dann auch als *Prädikat* bezeichnen.

  - $\mathbb{P} =_{\text{def}} \{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$ *(Menge der Primzahlen)*

- *Mengen, die durch eine Eigenschaft E definiert sind:*
  - $\{n \mid n \in \mathbb{N}$ *und* n *ist durch* 3 *teilbar}$
  - $\{n \mid n \in \mathbb{N}$ *und* n *ist Primzahl und* $n \leq 40\}$
  - $\emptyset =_{\text{def}} \{a \mid a \neq a\}$ *(die leere Menge)*

Aus Definition 113 ergibt sich, dass die leere Menge $\emptyset$ Teilmenge jeder Menge ist.

A.1.3. Operationen auf Mengen

Definition 115: *Seien A und B beliebige Mengen, dann ist*

- $A \cap B =_{\text{def}} \{a \mid a \in A$ *und* $a \in B\}$ *(Schnitt von A und B),*
- $A \cup B =_{\text{def}} \{a \mid a \in A$ *oder* $a \in B\}$ *(Vereinigung von A und B),*
- $A \setminus B =_{\text{def}} \{a \mid a \in A$ *und* $a \notin B\}$ *(Differenz von A und B),*
- $\overline{A} =_{\text{def}} M \setminus A$ *(Komplement von A bezüglich einer festen Grundmenge M) und*
- $\mathcal{P}(A) =_{\text{def}} \{B \mid B \subseteq A\}$ *(Potenzmenge von A).*

Zwei Mengen A und B mit $A \cap B = \emptyset$ nennt man disjunkt.

Beispiel 116: *Sei $A = \{2, 3, 5, 7\}$ und $B = \{1, 2, 4, 6\}$, dann ist $A \cap B = \{2\}$, $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$ und $A \setminus B = \{3, 5, 7\}$. Wählen wir als Grundmenge die natürlichen Zahlen, also $M = \mathbb{N}$, dann ist $\overline{A} = \{n \in \mathbb{N} \mid n \neq 2$ und $n \neq 3$ und $n \neq 5$ und $n \neq 7\} = \{1, 4, 6, 8, 9, 10, 11, \dots\}$.*

Als Potenzmenge der Menge A ergibt sich die folgende Menge von Mengen von natürlichen Zahlen $\mathcal{P}(A) = \{\emptyset, \{2\}, \{3\}, \{5\}, \{7\}, \{2, 3\}, \{2, 5\}, \{2, 7\}, \{3, 5\}, \{3, 7\}, \{5, 7\}, \{2, 3, 5\}, \{2, 3, 7\}, \{2, 5, 7\}, \{3, 5, 7\}, \{2, 3, 5, 7\}\}$.

Offensichtlich sind die Menge $\{0, 2, 4, 6, 8, \dots\}$ der geraden natürlichen Zahlen und die Menge $\{1, 3, 5, 7, 9, \dots\}$ der ungeraden natürlichen Zahlen disjunkt.

A.1.4. Gesetze für Mengenoperationen

Für die klassischen Mengenoperationen gelten die folgenden Beziehungen:

$A \cap B$	$=$	$B \cap A$	Kommutativgesetz für den Schnitt
$A \cup B$	$=$	$B \cup A$	Kommutativgesetz für die Vereinigung
$A \cap (B \cap C)$	$=$	$(A \cap B) \cap C$	Assoziativgesetz für den Schnitt
$A \cup (B \cup C)$	$=$	$(A \cup B) \cup C$	Assoziativgesetz für die Vereinigung
$A \cap (B \cup C)$	$=$	$(A \cap B) \cup (A \cap C)$	Distributivgesetz
$A \cup (B \cap C)$	$=$	$(A \cup B) \cap (A \cup C)$	Distributivgesetz
$A \cap A$	$=$	A	Duplizitätsgesetz für den Schnitt
$A \cup A$	$=$	A	Duplizitätsgesetz für die Vereinigung
$A \cap (A \cup B)$	$=$	A	Absorptionsgesetz
$A \cup (A \cap B)$	$=$	A	Absorptionsgesetz
$\overline{A \cap B}$	$=$	$(\overline{A} \cup \overline{B})$	de-Morgansche Regel
$\overline{A \cup B}$	$=$	$(\overline{A} \cap \overline{B})$	de-Morgansche Regel
$\overline{\overline{A}}$	$=$	A	Gesetz des doppelten Komplements

Die „de-Morganschen Regeln“ wurden nach dem englischen Mathematiker Augustus De Morgan[17] benannt.

Als Abkürzung schreibt man statt $X_1 \cup X_2 \cup \cdots \cup X_n$ (bzw. $X_1 \cap X_2 \cap \cdots \cap X_n$) einfach $\bigcup_{i=1}^{n} X_i$ (bzw. $\bigcap_{i=1}^{n} X_i$). Möchte man alle Mengen X_i mit $i \in \mathbb{N}$ schneiden (bzw. vereinigen), so schreibt man kurz $\bigcap_{i\in\mathbb{N}} X_i$ (bzw. $\bigcup_{i\in\mathbb{N}} X_i$).

Oft benötigt man eine Verknüpfung von zwei Mengen, eine solche Verknüpfung wird allgemein wie folgt definiert:

Definition 117 („Verknüpfung von Mengen“): *Seien A und B zwei beliebige Mengen und „$\odot$“ eine beliebige Verknüpfung zwischen den Elementen dieser Mengen, dann definieren wir*

$$A \odot B =_{\text{def}} \{a \odot b \mid a \in A \text{ und } b \in B\}.$$

Beispiel 118: *Die Menge $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \dots\}$ enthält alle Vielfachen[18] von 3, damit ist $3\mathbb{Z} + \{1\} = \{1, 4, -2, 7, -5, 10, -8, \dots\}$. Die Menge $3\mathbb{Z} + \{1\}$ schreibt man kurz oft auch als $3\mathbb{Z} + 1$, wenn klar ist, was mit dieser Abkürzung gemeint ist.*

A.1.5. Tupel (Vektoren) und das Kreuzprodukt

Seien $A, A_1, \dots, A_n$ im folgenden Mengen, dann bezeichnet

- $(a_1, \dots, a_n) =_{\text{def}}$ die Elemente $a_1, \dots, a_n$ in genau dieser festgelegten *Reihenfolge* und z.B. $(3, 2) \neq (2, 3)$. Wir sprechen von einem n-Tupel.
- $A_1 \times A_2 \times \cdots \times A_n =_{\text{def}} \{(a_1, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$ (Kreuzprodukt der Mengen $A_1, A_2, \dots, A_n$),
- $A^n =_{\text{def}} \underbrace{A \times A \times \cdots \times A}_{n\text{-mal}}$ (n-faches Kreuzprodukt der Menge A) und
- speziell gilt $A^1 = \{(a) \mid a \in A\}$.

Wir nennen 2-Tupel auch *Paare*, 3-Tupel auch *Tripel*, 4-Tupel auch *Quadrupel* und 5-Tupel *Quintupel*. Bei n-Tupeln ist, im Gegensatz zu Mengen, eine Reihenfolge vorgegeben, d.h. es gilt z.B. immer $\{a, b\} = \{b, a\}$, aber im Allgemeinen $(a, b) \neq (b, a)$.

Beispiel 119: *Sei $A = \{1, 2, 3\}$ und $B = \{a, b, c\}$, dann bezeichnet das Kreuzprodukt von A und B die Menge von Paaren $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$.*

A.1.6. Die Anzahl von Elementen in Mengen

Sei A eine Menge, die endlich viele Elemente[19] enthält, dann ist

$$\#A =_{\text{def}} \text{Anzahl der Elemente in der Menge } A.$$

Beispielsweise ist $\#\{4, 7, 9\} = 3$. Mit dieser Definition gilt

[17] ⋆1806 in Madurai, Tamil Nadu, Indien - †1871 in London, England
[18] Eigentlich müsste man statt $3\mathbb{Z}$ die Notation $\{3\}\mathbb{Z}$ verwenden. Dies ist allerdings unüblich.
[19] Solche Mengen werden als *endliche Mengen* bezeichnet.

- $\#(A^n) = (\#A)^n$,
- $\#\mathcal{P}(A) = 2^{\#A}$,
- $\#A + \#B = \#(A \cup B) + \#(A \cap B)$ und
- $\#A = \#(A \setminus B) + \#(A \cap B)$.

A.2. Relationen und Funktionen

A.2.1. Eigenschaften von Relationen

Seien $A_1, \ldots, A_n$ beliebige Mengen, dann ist R eine *n-stellige Relation* gdw. $R \subseteq A_1 \times A_2 \times \cdots \times A_n$. Eine zweistellige Relation nennt man auch *binäre Relation*. Oft werden auch Relationen $R \subseteq A^n$ betrachtet, diese bezeichnet man dann als n-stellige Relation über der Menge A.

Definition 120: *Sei R eine zweistellige Relation über A, dann ist R*

- reflexiv *gdw. $(a, a) \in R$ für alle $a \in A$,*
- symmetrisch *gdw. aus $(a, b) \in R$ folgt $(b, a) \in R$,*
- antisymmetrisch *gdw. aus $(a, b) \in R$ und $(b, a) \in R$ folgt $a = b$,*
- transitiv *gdw. aus $(a, b) \in R$ und $(b, c) \in R$ folgt $(a, c) \in R$ und*
- linear *gdw. es gilt immer $(a, b) \in R$ oder $(b, a) \in R$.*
- *Wir nennen R eine* Halbordnung *gdw. R ist reflexiv, antisymmetrisch und transitiv,*
- *eine* Ordnung *gdw. R ist eine lineare Halbordnung und*
- *eine* Äquivalenzrelation *gdw. R reflexiv, transitiv und symmetrisch ist.*

Beispiel 121: *Die Teilmengenrelation „$\subseteq$“ auf allen Teilmengen von $\mathbb{Z}$ ist eine Halbordnung, aber keine Ordnung. Wir schreiben $a \equiv b \bmod n$, falls es eine ganze Zahl q gibt, für die $a - b = qn$ gilt. Für $n \geq 2$ ist die Relation $R_n(a, b) =_{\text{def}} \{(a, b) \mid a \equiv b \bmod n\} \subseteq \mathbb{Z}^2$ eine Äquivalenzrelation.*

A.2.2. Eigenschaften von Funktionen

Seien A und B beliebige Mengen. f ist eine *Funktion* von A nach B (Schreibweise: $f\colon A \to B$) gdw. $f \subseteq A \times B$ und für jedes $a \in A$ gibt es *höchstens* ein $b \in B$ mit $(a, b) \in f$. Ist also $(a, b) \in f$, so schreibt man $f(a) = b$.

Bemerkung 122: *Unsere Definition von Funktion umfasst auch mehrstellige Funktionen. Seien C und B Mengen und $A = C^n$ das n-fache Kreuzprodukt von C. Die Funktion $f\colon A \to B$ ist dann eine n-stellige Funktion, denn sie bildet n-Tupel aus C^n auf Elemente aus B ab.*

Definition 123: *Sei f eine n-stellige Funktion. Möchte man die Funktion f benutzen, aber keine Namen für die Argumente vergeben, so schreibt man auch*

$$f(\underbrace{\cdot, \cdot, \ldots, \cdot}_{n\text{-}mal})$$

Ist also der Namen des Arguments einer einstelligen Funktion $g(x)$ für eine Betrachtung unwichtig, so kann man $g(\cdot)$ schreiben, um anzudeuten, dass g einstellig ist, ohne dies weiter zu erwähnen.

Sei nun $R \subseteq A_1 \times A_2 \times \cdots \times A_n$ eine n-stellige Relation, dann definieren wir $P_R^n \colon A_1 \times A_2 \times \cdots \times A_n \to \{0, 1\}$ wie folgt:

$$P_R^n(x_1, \ldots, x_n) =_{\text{def}} \begin{cases} 1, & \text{falls } (x_1, \ldots, x_n) \in R \\ 0, & \text{sonst} \end{cases}$$

Eine solche (n-stellige) Funktion, die „anzeigt“, ob ein Element aus $A_1 \times A_2 \times \cdots \times A_n$ entweder zu R gehört oder nicht, nennt man (n-stelliges) *Prädikat*.

Beispiel 124: *Sei $\mathbb{P} =_{\text{def}} \{n \in \mathbb{N} \mid n \text{ ist Primzahl}\}$, dann ist $\mathbb{P}$ eine 1-stellige Relation über den natürlichen Zahlen. Das Prädikat $P_{\mathbb{P}}^1(n)$ liefert für eine natürliche Zahl n genau dann 1, wenn n eine Primzahl ist.*

Ist für ein Prädikat P_R^n sowohl die Relation R als auch die Stelligkeit n aus dem Kontext klar, dann schreibt man auch kurz P oder verwendet das Relationensymbol R als Notation für das Prädikat P_R^n. Nun legen wir zwei spezielle Funktionen fest, die oft sehr hilfreich sind:

Definition 125: *Sei $\alpha \in \mathbb{R}$ eine beliebige reelle Zahl, dann gilt*

- $\lceil x \rceil =_{\text{def}}$ *die kleinste ganze Zahl, die größer oder gleich α ist ($\triangleq$ „Aufrunden“)*
- $\lfloor x \rfloor =_{\text{def}}$ *die größte ganze Zahl, die kleiner oder gleich α ist ($\triangleq$ „Abrunden“)*

Definition 126: *Für eine beliebige Funktion f legen wir fest:*

- *Der* Definitionsbereich *von f ist $D_f =_{\text{def}} \{a \mid$ es gibt ein b mit $f(a) = b\}$.*
- *Der* Wertebereich *von f ist $W_f =_{\text{def}} \{b \mid$ es gibt ein a mit $f(a) = b\}$.*
- *Die Funktion $f \colon A \to B$ ist* total *gdw. $D_f = A$.*
- *Die Funktion $f \colon A \to B$ heißt* surjektiv *gdw. $W_f = B$.*
- *Die Funktion f heißt* injektiv *(oder eineindeutig[20]) gdw. immer wenn $f(a_1) = f(a_2)$ gilt auch $a_1 = a_2$.*
- *Die Funktion f heißt* bijektiv *gdw. f ist injektiv und surjektiv.*

Beispiel 127: *Sei die Funktion $f \colon \mathbb{N} \to \mathbb{Z}$ durch $f(n) = (-1)^n \lceil \frac{n}{2} \rceil$ gegeben. Die Funktion f ist surjektiv, denn $f(0) = 0, f(1) = -1, f(2) = 1, f(3) = -2, f(4) = 2, \ldots$, d.h. die ungeraden natürlichen Zahlen werden auf die negativen ganzen Zahlen abgebildet, die geraden Zahlen aus $\mathbb{N}$ werden auf die positiven ganzen Zahlen abgebildet und deshalb ist $W_f = \mathbb{Z}$.*

[20] Achtung: Dieser Begriff wird manchmal unterschiedlich, je nach Autor, in den Bedeutungen „bijektiv“ oder „injektiv“ verwendet.

Weiterhin ist f auch injektiv, denn aus[21] $(-1)^{a_1}\lceil\frac{a_1}{2}\rceil = (-1)^{a_2}\lceil\frac{a_2}{2}\rceil$ *folgt, dass entweder a_1 und a_2 gerade oder a_1 und a_2 ungerade, denn sonst würden auf der linken und rechten Seite der Gleichung unterschiedliche Vorzeichen auftreten. Ist a_1 gerade und a_2 gerade, dann gilt $\lceil\frac{a_1}{2}\rceil = \lceil\frac{a_2}{2}\rceil$ und auch $a_1 = a_2$. Sind a_1 und a_2 ungerade, dann gilt $-\lceil\frac{a_1}{2}\rceil = -\lceil\frac{a_2}{2}\rceil$, woraus auch folgt, dass $a_1 = a_2$. Damit ist die Funktion f bijektiv. Weiterhin ist f auch total, d.h. $D_f = \mathbb{N}$.*

A.3. Summen und Produkte

A.3.1. Summen

Zur abkürzenden Schreibweise verwendet man für Summen das Summenzeichen $\sum$. Dabei ist

$$\sum_{i=1}^{n} a_i =_{\text{def}} a_1 + a_2 + \cdots + a_n.$$

Mit Hilfe dieser Definition ergeben sich auf elementare Weise die folgenden Rechenregeln:

- Sei $a_i = a$ für $1 \leq i \leq n$, dann gilt $\sum\limits_{i=1}^{n} a_i = n \cdot a$ (Summe gleicher Summanden).
- $\sum\limits_{i=1}^{n} a_i = \sum\limits_{i=1}^{m} a_i + \sum\limits_{i=m+1}^{n} a_i$, wenn $1 < m < n$ (Aufspalten einer Summe).
- $\sum\limits_{i=1}^{n}(a_i + b_i + c_i + \dots) = \sum\limits_{i=1}^{n} a_i + \sum\limits_{i=1}^{n} b_i + \sum\limits_{i=1}^{n} c_i + \dots$ (Addition von Summen).
- $\sum\limits_{i=1}^{n} a_i = \sum\limits_{i=l}^{n+l-1} a_{i-l+1}$ und $\sum\limits_{i=l}^{n} a_i = \sum\limits_{i=1}^{n-l+1} a_{i+l-1}$ (Umnumerierung von Summen).
- $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} a_{i,j} = \sum\limits_{j=1}^{m}\sum\limits_{i=1}^{n} a_{i,j}$ (Vertauschen der Summationsfolge).

A.3.2. Produkte

Zur abkürzenden Schreibweise verwendet man für Produkte das Produktzeichen $\prod$. Dabei ist

$$\prod_{i=1}^{n} a_i =_{\text{def}} a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

Mit Hilfe dieser Definition ergeben sich auf elementare Weise die folgenden Rechenregeln:

- Sei $a_i = a$ für $1 \leq i \leq n$, dann gilt $\prod\limits_{i=1}^{n} a_i = a^n$ (Produkt gleicher Faktoren).
- $\prod\limits_{i=1}^{n}(ca_i) = c^n \prod\limits_{i=1}^{n} a_i$ (Vorziehen von konstanten Faktoren)
- $\prod\limits_{i=1}^{n} a_i = \prod\limits_{i=1}^{m} a_i \cdot \prod\limits_{i=m+1}^{n} a_i$, wenn $1 < m < n$ (Aufspalten in Teilprodukte).

[21] Für die Definition der Funktion $\lceil\cdot\rceil$ siehe Definition 125.

- $\prod_{i=1}^{n}(a_i \cdot b_i \cdot c_i \cdot \ldots) = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i \cdot \prod_{i=1}^{n} c_i \cdot \ldots$ (Das Produkt von Produkten).
- $\prod_{i=1}^{n} a_i = \prod_{i=l}^{n+l-1} a_{i-l+1}$ und $\prod_{i=l}^{n} a_i = \prod_{i=1}^{n-l+1} a_{i+l-1}$ (Umnumerierung von Produkten).
- $\prod_{i=1}^{n}\prod_{j=1}^{m} a_{i,j} = \prod_{j=1}^{m}\prod_{i=1}^{n} a_{i,j}$ (Vertauschen der Reihenfolge bei Doppelprodukten).

A.4. Logarithmieren, Potenzieren und Radizieren

Die Schreibweise a^b ist eine Abkürzung für

$$a^b =_{\text{def}} \underbrace{a \cdot a \cdot \ldots \cdot a}_{b-\text{mal}}$$

und wird als *Potenzierung* bezeichnet. Dabei wird a als *Basis*, b als *Exponent* und a^b als b-te *Potenz* von a bezeichnet. Seien nun $r, s, t \in \mathbb{R}$ und $r, t \geq 0$ durch die folgende Gleichung verbunden:

$$r^s = t.$$

Dann läßt sich diese Gleichung wie folgt umstellen und es gelten die folgenden Rechenregeln:

Logarithmieren	Potenzieren	Radizieren
$\mathbf{s = \log_r t}$	$\mathbf{t = r^s}$	$\mathbf{r = \sqrt[s]{t}}$
i) $\log_r(\frac{u}{v}) = \log_r u - \log_r v$	i) $r^u \cdot r^v = r^{u+v}$	i) $\sqrt[s]{u} \cdot \sqrt[s]{v} = \sqrt[s]{u \cdot v}$
ii) $\log_r(u \cdot v) = \log_r u + \log_r v$	ii) $\frac{r^u}{r^v} = r^{u-v}$	ii) $\frac{\sqrt[s]{u}}{\sqrt[s]{v}} = \sqrt[s]{\left(\frac{u}{v}\right)}$
iii) $\log_r(t^u) = u \cdot \log_r t$	iii) $u^s \cdot v^s = (u \cdot v)^s$	iii) $\sqrt[u]{\sqrt[v]{t}} = \sqrt[u \cdot v]{t}$
iv) $\log_r(\sqrt[u]{t}) = \frac{1}{u} \cdot \log_r t$	iv) $\frac{u^s}{v^s} = \left(\frac{u}{v}\right)^s$	
v) $\frac{\log_r t}{\log_r u} = \log_u t$ (Basiswechsel)	v) $(r^u)^v = r^{u \cdot v}$	

Zusätzlich gilt: Wenn $r > 1$, dann ist $s_1 < s_2$ gdw. $r^{s_1} < r^{s_2}$ (Monotonie).

Da $\sqrt[s]{t} = t^{(\frac{1}{s})}$ gilt, können die Gesetze für das Radizieren leicht aus den Potenzierungsgesetzen abgeleitet werden. Weiterhin legen wir spezielle Schreibweisen für die Logarithmen zur Basis 10, e (Eulersche Zahl) und 2 fest: $\lg t =_{\text{def}} \log_{10} t$, $\ln t =_{\text{def}} \log_e t$ und $\text{lb}\, t =_{\text{def}} \log_2 t$.

A.5. Gebräuchliche griechische Buchstaben

In der Informatik, Mathematik und Physik ist es üblich, griechische Buchstaben zu verwenden. Ein Grund hierfür ist, dass es so möglich wird mit einer größeren Anzahl von Unbekannten arbeiten zu können, ohne unübersichtliche und oft unhandliche Indizes benutzen zu müssen.

Kleinbuchstaben:

Symbol	Bezeichnung	Symbol	Bezeichnung	Symbol	Bezeichnung
α	Alpha	β	Beta	γ	Gamma
δ	Delta	ϕ	Phi	φ	Phi
ξ	Xi	ζ	Zeta	ϵ	Epsilon
θ	Theta	λ	Lambda	π	Pi
σ	Sigma	η	Eta	μ	Mu

Grossbuchstaben:

Symbol	Bezeichnung	Symbol	Bezeichnung	Symbol	Bezeichnung
Γ	Gamma	Δ	Delta	Φ	Phi
Ξ	Xi	Θ	Theta	Λ	Lambda
Π	Pi	Σ	Sigma	Ψ	Psi
Ω	Omega				

B. Einige (wenige) Grundlagen der elementaren Logik

Aussagen sind entweder *wahr* ($\triangleq 1$) oder *falsch* ($\triangleq 0$). So sind die Aussagen

„Wiesbaden liegt am Mittelmeer“ und „$1 = 7$“

sicherlich falsch, wogegen die Aussagen

„Wiesbaden liegt in Hessen“ und „$11 = 11$“

sicherlich wahr sind. Aussagen werden meist durch *Aussagenvariablen* formalisiert, die nur die Werte 0 oder 1 annehmen können. Oft verwendet man auch eine oder mehrere Unbekannte, um eine Aussage zu parametrisieren. So könnte „$P(x)$“ etwa für „Wiesbaden liegt im Bundesland x“ stehen, d.h. „P(Hessen)“ wäre wahr, wogegen „P(Bayern)“ eine falsche Aussage ist. Solche Aussagen mit Parameter nennt man auch *Prädikat*.

Um die Verknüpfung von Aussagen auch formal aufschreiben zu können, werden die folgenden logischen Operatoren verwendet

Symbol	umgangssprachlicher Name	Name in der Logik
$\wedge$	und	Konjunktion
$\vee$	oder	Disjunktion / Alternative
$\neg$	nicht	Negation
$\rightarrow$	folgt	Implikation
$\leftrightarrow$	genau dann wenn (*gdw.*)	Äquivalenz

Zusätzlich werden noch die Quantoren $\exists$ („es existiert“) und $\forall$ („für alle“) verwendet, die z.B. wie folgt gebraucht werden können

$\forall x\colon P(x)$ bedeutet „Für alle x gilt die Aussage $P(x)$.

$\exists x\colon P(x)$ bedeutet „Es existiert ein x, für das die Aussage $P(x)$ gilt.

Oft läßt man sogar den Doppelpunkt weg und schreibt statt $\forall x\colon P(x)$ vereinfachend $\forall x P(x)$.

Beispiel 128: *Die Aussage „Jede gerade natürliche Zahl kann als Produkt von* 2 *und einer anderen natürlichen Zahl geschrieben werden“ lässt sich dann wie folgt schreiben*

$$\forall n \in \mathbb{N}\colon ((n \text{ ist gerade}) \to (\exists m \in \mathbb{N}\colon n = 2 \cdot m))$$

Die folgende logische Formel wird wahr gdw. n *eine ungerade natürliche Zahl ist.*

$$\exists m \in \mathbb{N}\colon (n = 2 \cdot m + 1)$$

Für die logischen Konnektoren sind die folgenden Wahrheitswertetafeln festgelegt:

p	$\neg p$
0	1
1	0

und

p	q	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Jetzt kann man Aussagen auch etwas komplexer verknüpfen:

Beispiel 129: *Nun wird der* $\wedge$*-Operator verwendet werden. Dazu soll die Aussage „Für alle natürlichen Zahlen* n *und* m *gilt, wenn* n *kleiner gleich* m *und* m *kleiner gleich* n *gilt, dann ist* m *gleich* n*“*

$$\forall n, m \in \mathbb{N}\colon (((n \leq m) \wedge (m \leq n)) \to (n = m))$$

Oft benutzt man noch den negierten Quantor $\nexists$ („es existiert kein“).

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Beispiel 130 („Großer Satz von Fermat“): *Die Richtigkeit dieser Aussage konnte erst* 1994 *nach mehr als* 350 *Jahren von Andrew Wiles und Richard Taylor gezeigt werden:*

$$\forall n \in \mathbb{N} \nexists a, b, c \in \mathbb{N}\colon (((n > 2) \wedge (a \cdot b \cdot c \neq 0)) \to a^n + b^n = c^n)$$

Für den Fall $n = 2$ *hat die Gleichung* $a^n + b^n = c^n$ *unendlich viele ganzzahlige Lösungen (so genannte Pythagoräische Zahlentripel) wie z.B.* $3^2 + 4^2 = 5^2$*. Diese sind seit mehr als* 3500 *Jahren bekannt und haben z.B. geholfen die Cheops-Pyramide zu bauen.*

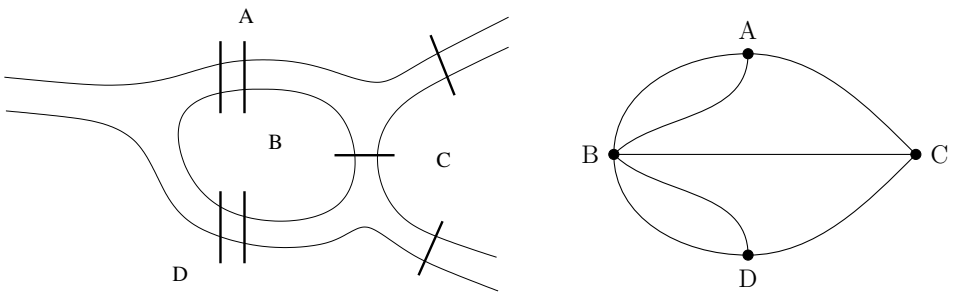
C. Graphen und Graphenalgorithmen

C.1. Einführung

Sehr viele Probleme lassen sich durch Objekte und Verbindungen oder Beziehungen zwischen diesen Objekten beschreiben. Ein schönes Beispiel hierfür ist das *Königsberger Brückenproblem*, das 1736 von Leonhard Euler[22] formuliert und gelöst wurde. Zu dieser Zeit hatte Königsberg[23] genau sieben Brücken wie die folgende sehr grobe Karte zeigt:
Die verschiedenen Stadtteile sind dabei mit A-D bezeichnet. Euler stellte sich nun die Frage, ob es möglich ist, einen Spaziergang in einem beliebigen Stadtteil zu beginnen, jede Brücke *genau einmal* zu überqueren und den Spaziergang am Startpunkt zu beenden. Ein solcher Weg soll *Euler-Spaziergang* heißen. Die Frage lässt sich leicht beantworten, wenn der Stadtplan wie nebenstehend formalisiert wird.

[22] Der Schweizer Mathematiker Leonhard Euler wurde 1707 in Basel geboren und starb 1783 in St. Petersburg.

[23] Königsberg heißt heute Kaliningrad.



(a) Ein grober Stadtplan (b) Der formalisierte Stadtplan

Abbildung 4: Das Königsberger-Brückenproblem

Die Stadtteile sind bei der Formalisierung zu Knoten geworden und die Brücken werden durch Kanten zwischen den Knoten symbolisiert[24]. Angenommen es gäbe in Königsberg einen Euler-Spaziergang, dann müsste für jeden Knoten in Abbildung 4 die folgende Eigenschaft erfüllt sein: die Anzahl der Kanten die mit einem Knoten verbunden sind ist gerade, weil für jede Ankunft (über eine Brücke) in einem Stadtteil ein Verlassen eines Stadtteil (über eine Brücke) notwendig ist.

C.2. Grundlagen

Die Theorie der Graphen ist heute zu einem unverzichtbaren Bestandteil der Informatik geworden. Viele Probleme, wie z.B. das Verlegen von Leiterbahnen auf einer Platine, die Modellierung von Netzwerken oder die Lösung von Routingproblemen in Verkehrsnetzen benutzen Graphen oder Algorithmen, die Graphen als Datenstruktur verwenden. Auch schon bekannte Datenstrukturen wie Listen und Bäume können als Graphen aufgefasst werden. All dies gibt einen Anhaltspunkt, dass die Graphentheorie eine sehr zentrale Rolle für die Informatik spielt und vielfältige Anwendungen hat. In diesem Kontext ist es wichtig zu bemerken, dass der Begriff des Graphen in der Informatik *nicht* im Sinne von Graph einer Funktion gebraucht wird, sondern wie folgt definiert ist:

Definition 131: *Ein* gerichteter Graph $G = (V, E)$ *ist ein Paar, das aus einer Menge von* Knoten V *und einer Menge von* Kanten $E \subseteq V \times V$ *(*Kantenrelation*) besteht. Eine Kante $k = (u, v)$ aus E kann als Verbindung zwischen den Knoten $u, v \in V$ aufgefasst werden. Aus diesem Grund nennt man u auch* Startknoten *und v* Endknoten*. Zwei Knoten, die durch eine Kante verbunden sind, heißen auch* benachbart *oder* adjazent*.*
Ein Graph $H = (V', E')$ mit $V' \subseteq V$ und $E' \subset E$ heißt Untergraph *von G.*

Ein Graph (V, E) heißt *endlich* gdw. die Menge der Knoten V endlich ist. Obwohl man natürlich auch unendliche Graphen betrachten kann, werden wir uns in diesem Abschnitt nur mit endlichen Graphen beschäftigen, da diese für den Informatiker von großem Nutzen sind.

Da wir eine Kante (u, v) als Verbindung zwischen den Knoten u und v interpretieren können, bietet es sich an, Graphen durch Diagramme darzustellen. Dabei wird die Kante (u, v) durch einen Pfeil von u nach v dargestellt. Drei Beispiele für eine bildliche Darstellung von gerichteten Graphen finden sich in Abbildung 5.

[24] Abbildung 4 nennt man *Multigraph*, denn hier starten mehrere Kanten von *einem* Knoten und enden in *einem* anderen Knoten.

C.3. Einige Eigenschaften von Graphen

Der Graph in Abbildung 5(c) hat eine besondere Eigenschaft, denn offensichtlich kann man die Knotenmenge $V_{1c} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ in zwei disjunkte Teilmengen $V_{1c}^l = \{0, 1, 2, 3\}$ und $V_{1c}^r = \{4, 5, 6, 7, 8\}$ so aufteilen, dass keine Kante zwischen zwei Knoten aus V_{1c}^l oder V_{1c}^r verläuft.

Definition 132: *Ein Graph $G = (V, E)$ heißt* bipartit*, wenn gilt:*

1. *Es gibt zwei Teilmengen V^l und V^r von V mit $V = V^l \cup V^r$, $V^l \cap V^r = \emptyset$ und*
2. *für jede Kante $(u, v) \in E$ gilt $u \in V^l$ und $v \in V^r$.*

Bipartite Graphen haben viele Anwendungen, weil man jede binäre Relation $R \subseteq A \times B$ mit $A \cap B = \emptyset$ ganz natürlich als bipartiten Graph auffassen kann, dessen Kanten von Knoten aus A zu Knoten aus B laufen.

Beispiel 133: *Gegeben sei ein bipartiter Graph $G = (V, E)$ mit $V = V^F \cup V^M$ und $V^F \cap V^M = \emptyset$. Die Knoten aus V^F symbolisieren Frauen und V^M symbolisiert eine Menge von Männern. Kann sich eine Frau vorstellen einen Mann zu heiraten, so wird der entsprechende Knoten aus V^F mit dem passenden Knoten aus V^M durch eine Kante verbunden. Eine* Heirat *ist nun eine Kantenmenge $H \subseteq E$, so dass keine zwei Kanten aus H einen gemeinsamen Knoten besitzen. Das* Heiratsproblem *ist nun die Aufgabe für G eine Heirat H zu finden, so dass alle Frauen heiraten können, d.h. es ist das folgende Problem zu lösen:*

Problem:	MARRIAGE
Eingabe:	Bipartiter Graph $G = (V, E)$ mit $V = V^F \cup V^M$ und $V^F \cap V^M = \emptyset$
Ausgabe:	Eine Heirat H mit $\#H = \#V^F$

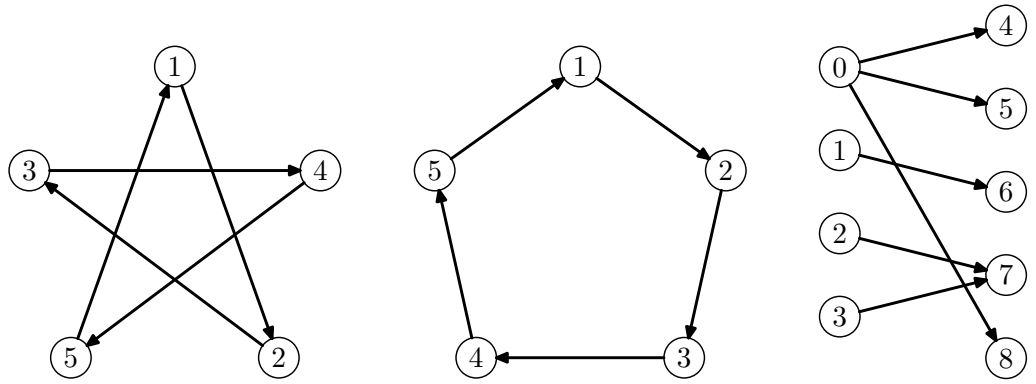
Im Beispielgraphen 5(c) gibt es keine Lösung für das Heiratsproblem, denn für die Knoten ($\triangleq$ Kandidatinnen) 2 und 3 existieren nicht ausreichend viele Partner, d.h. keine Heirat in diesem Graphen enthält zwei Kanten die sowohl 2 als auch 3 als Startknoten haben.

Obwohl dieses Beispiel auf den ersten Blick nur von untergeordneter Bedeutung erscheint, kann man es auf eine Vielfalt von Anwendungen übertragen. Immer wenn die Elemente zweier disjunkter Mengen durch eine Beziehung verbunden sind, kann man dies als bipartiten Graphen auffassen. Sollen nun die Bedürfnisse der einen Menge völlig befriedigt werden, so ist dies wieder ein Heiratsproblem. Beispiele mit mehr praktischem Bezug finden sich u.a. bei Beziehungen zwischen Käufern und Anbietern.

Oft beschränken wir uns auch auf eine Unterklasse von Graphen, bei denen die Kanten keine „Richtung“ haben (siehe Abbildung 6) und einfach durch eine Verbindungslinie symbolisiert werden können:

Definition 134: *Sei $G = (V, E)$ ein Graph. Ist die Kantenrelation E* symmetrisch*, d.h. gibt es zu jeder Kante $(u, v) \in E$ auch eine Kante $(v, u) \in E$ (siehe auch Abschnitt A.2.1), dann bezeichnen wir G als* ungerichteten Graphen *oder kurz als* Graph*.*

Es ist praktisch, die Kanten (u, v) und (v, u) eines ungerichteten Graphen als Menge $\{u, v\}$ mit zwei Elementen aufzufassen. Diese Vorgehensweise führt zu einem kleinen technischen Problem. Eine Kante (u, u) mit gleichem Start- und Endknoten nennen wir, entsprechend der intuitiven Darstellung eines Graphens als Diagramm, *Schleife*. Wandelt man nun solch eine Kante in eine Menge um, so würde nur eine einelementige Menge entstehen. Aus diesem Grund legen wir fest, dass ungerichtete Graphen *schleifenfrei* sind.



(a) Ein gerichteter Graph mit 5 Knoten

(b) Ein planarer gerichteter Graph mit 5 Knoten

(c) Ein gerichteter bipartiter Graph

Abbildung 5: Beispiele für gerichtete Graphen

Definition 135: *Der (ungerichtete) Graph $K = (V, E)$ heißt* vollständig*, wenn für alle $u, v \in V$ mit $u \neq v$ auch $(u, v) \in E$ gilt, d.h. jeder Knoten des Graphen ist mit allen anderen Knoten verbunden. Ein Graph $O = (V, \emptyset)$ ohne Kanten wird als* Nullgraph *bezeichnet.*

Mit dieser Definition ergibt sich, dass die Graphen in Abbildung 6(a) und Abbildung 6(b) vollständig sind. Der Nullgraph $(V, \emptyset)$ ist Untergraph jedes beliebigen Graphen (V, E). Diese Definitionen lassen sich natürlich auch analog auf gerichtete Graphen übertragen.

Definition 136: *Sei $G = (V, E)$ ein gerichteter Graph und $v \in V$ ein beliebiger Knoten. Der* Ausgrad *von v (kurz:* $\text{outdeg}(v)$*) ist dann die Anzahl der Kanten in G, die v als Startknoten haben. Analog ist der* Ingrad *von v (kurz:* $\text{indeg}(v)$*) die Anzahl der Kanten in G, die v als Endknoten haben.*

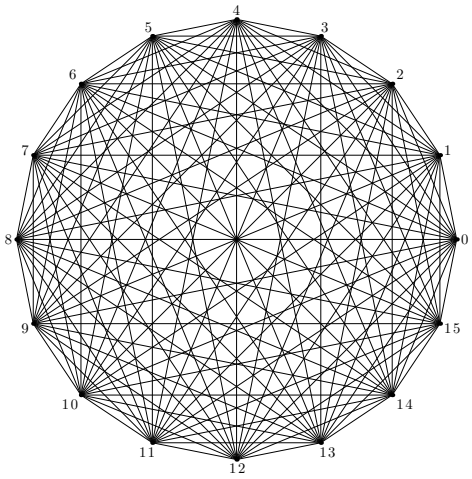
Bei ungerichteten Graphen gilt für jeden Knoten $\text{outdeg}(v) = \text{indeg}(v)$*. Aus diesem Grund schreiben wir kurz* $\deg(v)$ *und bezeichnen dies als* Grad von v*. Ein Graph G heißt* regulär *gdw. alle Knoten von G den gleichen Grad haben.*

Die Diagramme der Graphen in den Abbildungen 5 und 6 haben die Eigenschaft, dass sich einige Kanten schneiden. Es stellt sich die Frage, ob man diese Diagramme auch so zeichnen kann, dass keine Überschneidungen auftreten. Diese Eigenschaft von Graphen wollen wir durch die folgende Definition festhalten:

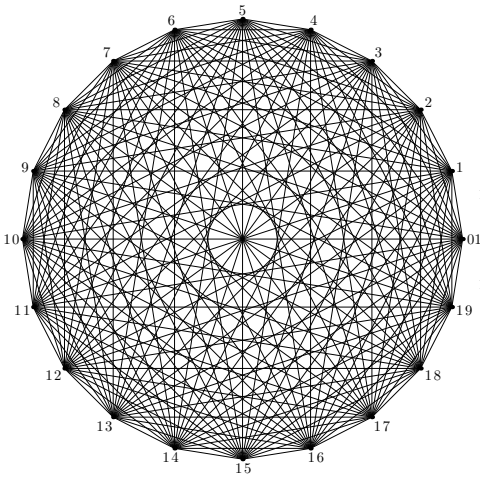
Definition 137: *Ein Graph G heißt* planar*, wenn sich sein Diagramm ohne Überschneidungen zeichnen läßt.*

Beispiel 138: *Der Graph in Abbildung 5(a) ist, wie man leicht nachprüfen kann, planar, da die Diagramme aus Abbildung 5(a) und 5(b) den gleichen Graphen repräsentieren.*

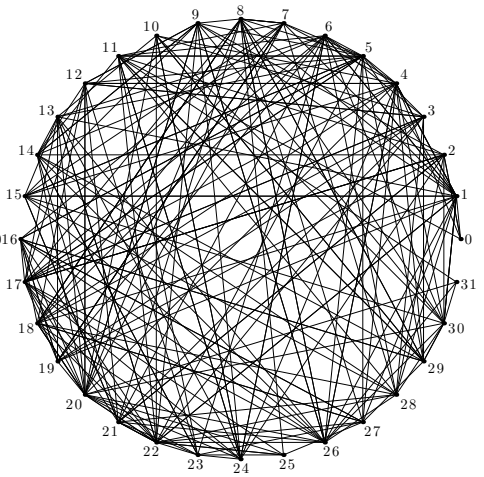
Auch planare Graphen haben eine anschauliche Bedeutung. Der Schaltplan einer elektronischen Schaltung kann als Graph aufgefasst werden. Die Knoten entsprechen den Stellen an denen die Bauteile aufgelötet werden müssen, und die Kanten entsprechen den Leiterbahnen auf der Platine. In diesem Zusammenhang bedeutet planar, ob man die Leiterbahnen kreuzungsfrei verlegen kann, d.h. ob es möglich ist, eine Platine zu



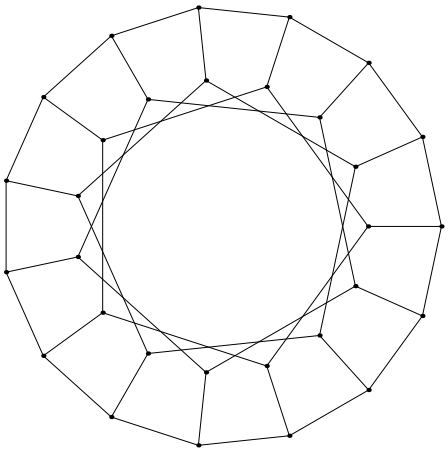
(a) Vollständiger ungerichteter Graph K_{16}



(b) Vollständiger ungerichteter Graph K_{20}



(c) Zufälliger Graph mit 32 Knoten



(d) Regulärer Graph mit Grad 3

Abbildung 6: Beispiele für ungerichtete Graphen

fertigen, die mit einer Kupferschicht auskommt. In der Praxis kommen oft Platinen mit mehreren Schichten zum Einsatz („Multilayer-Platine“). Ein Grund dafür kann sein, dass der „Schaltungsgraph“ nicht planar war und deshalb mehrere Schichten benötigt werden. Da Platinen mit mehreren Schichten in der Fertigung deutlich teurer sind als solche mit einer Schicht, hat die Planaritätseigenschaft von Graphen somit auch unmittelbare finanzielle Auswirkungen.

C.4. Wege, Kreise, Wälder und Bäume

Definition 139: *Sei $G = (V, E)$ ein Graph und $u, v \in V$. Eine Folge von Knoten $u_0, \ldots, u_l \in V$ mit $u = u_0$, $v = u_l$ und $(u_i, u_{i+1}) \in E$ für $0 \leq i \leq l-1$ heißt* Weg von u nach v der Länge l. *Der Knoten u wird* Startknoten *und v wird* Endknoten *des Wegs genannt.*

Ein Weg, bei dem Start- und Endknoten gleich sind, heißt geschlossener Weg. *Ein geschlossener Weg, bei dem kein Knoten außer dem Startknoten mehrfach enthalten ist, wird* Kreis *genannt.*

Mit Definition 139 wird klar, dass der Graph in Abbildung 5(a) den Kreis $1, 2, 3, \ldots, 5, 1$ mit Startknoten 1 hat.

Definition 140: *Sei $G = (V, E)$ ein Graph. Zwei Knoten $u, v \in V$ heißen* zusammenhängend, *wenn es einen Weg von u nach v gibt. Der Graph G heißt* zusammenhängend, *wenn jeder Knoten von G mit jedem anderen Knoten von G zusammenhängt.*

Sei G' ein zusammenhängender Untergraph von G mit einer besonderen Eigenschaft: Nimmt man einen weiteren Knoten von G zu G' hinzu, dann ist der neu entstandene Graph nicht mehr zusammenhängend, d.h. es gibt keinen Weg zu diesem neu hinzugekommenen Knoten. Solch einen Untergraph nennt man Zusammenhangskomponente.

Offensichtlich sind die Graphen in den Abbildungen 5(a), 6(a), 6(b) und 6(d) zusammenhängend und haben genau eine Zusammenhangskomponente. Man kann sich sogar leicht überlegen, dass die Eigenschaft „u hängt mit v“ zusammen eine *Äquivalenzrelation* (siehe Abschnitt A.2.1) darstellt.

Mit Hilfe der Definition des geschlossenen Wegs lässt sich nun der Begriff der Bäume definieren, die eine sehr wichtige Unterklasse der Graphen darstellen.

Definition 141: *Ein Graph G heißt*

- Wald, *wenn es keinen geschlossenen Weg mit Länge ≥ 1 in G gibt und*
- Baum, *wenn G ein zusammenhängender Wald ist, d.h. wenn er nur genau eine Zusammenhangskomponente hat.*

C.5. Die Repräsentation von Graphen und einige Algorithmen

Nachdem Graphen eine große Bedeutung sowohl in der praktischen als auch in der theoretischen Informatik erlangt haben, stellt sich noch die Frage, wie man Graphen effizient als Datenstruktur in einem Computer ablegt. Dabei soll es möglich sein, Graphen effizient zu speichern und zu manipulieren.

Die erste Idee, Graphen als dynamische Datenstrukturen zu repräsentieren, scheitert an dem relativ ineffizienten Zugriff auf die Knoten und Kanten bei dieser Art der Darstellung. Sie ist nur von Vorteil, wenn ein Graph nur sehr wenige Kanten enthält. Die folgende Methode der Speicherung von Graphen hat sich als effizient erwiesen und ermöglicht auch die leichte Manipulation des Graphens:

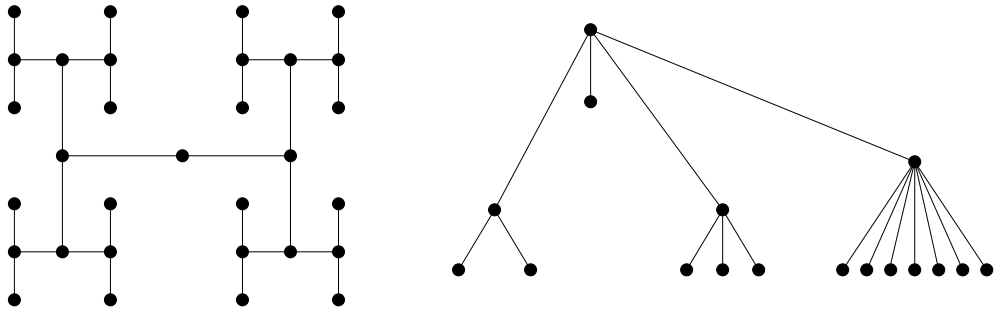


Abbildung 7: Ein Wald mit zwei Bäumen

Definition 142: *Sei $G = (V, E)$ ein gerichteter Graph mit $V = \{v_1, \ldots, v_n\}$. Wir definieren eine $n \times n$ Matrix $A_G = (a_{i,j})_{1 \leq i,j, \leq n}$ durch*

$$a_{i,j} = \begin{cases} 1, & \textit{falls } (v_i, v_j) \in E \\ 0, & \textit{sonst} \end{cases}$$

Die so definierte Matrix A_G mit Einträgen aus der Menge $\{0, 1\}$ heißt Adjazenzmatrix *von G.*

Beispiel 143: *Für den gerichteten Graphen aus Abbildung 5(a) ergibt sich die folgende Adjazenzmatrix:*

$$A_{G_5} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Die Adjazenzmatrix eines ungerichteten Graphen erkennt man daran, dass sie spiegelsymmetrisch zu Diagonale von links oben nach rechts unten ist (die Kantenrelation ist symmetrisch) und dass die Diagonale aus 0-Einträgen besteht (der Graphen hat keine Schleifen). Für den vollständigen Graphen K_{16} aus Abbildung 6(a) ergibt sich offensichtlich die folgende Adjazenzmatrix:

$$A_{K_{16}} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Mit Hilfe der Adjazenzmatrix und Algorithmus 1 kann man leicht berechnen, ob ein Weg von einem Knoten u zu einem Knoten v existiert. Mit einer ganz ähnlichen Idee kann man auch leicht die Anzahl der Zusammenhangskomponenten berechnen (siehe Algorithmus 2). Dieser Algorithmus markiert die Knoten der einzelnen Zusammenhangskomponenten auch mit unterschiedlichen „Farben“, die hier durch Zahlen repräsentiert werden.

Algorithmus 1 : Erreichbarkeit in Graphen

Eingabe : Ein Graph $G = (V, E)$ und zwei Knoten $u, v \in V$
Ergebnis : `true` wenn es einen Weg von u nach v gibt, `false` sonst

```
markiert = true;
markiere Startknoten u ∈ V;
while (markiert) do
    markiert = false;
    for (alle markierten Knoten w ∈ V) do
        if (w ∈ V ist adjazent zu einem unmarkierten Knoten w' ∈ V) then
            markiere Knoten w';
            markiert = true;
        end
    end
end
if (v ist markiert) then
    return true;
else
    return false;
end
```

Definition 144: *Sei $G = (V, E)$ ein ungerichteter Graph. Eine Funktion der Form $f\colon V \to \{1, \ldots, k\}$ heißt* Farbung=k-Färbung *des Graphen G. Anschaulich ordnet die Funktion f jedem Knoten eine von k verschiedenen Farben zu, die hier durch die Zahlen $1, \ldots, k$ symbolisiert werden. Eine Färbung heißt* verträglich*, wenn für alle Kanten $(u, v) \in E$ gilt, dass $f(u) \neq f(v)$, d.h. zwei adjazente Knoten werden nie mit der gleichen Farbe markiert.*

Auch das Färbbarkeitsproblem spielt in der Praxis der Informatik eine wichtige Rolle. Ein Beispiel dafür ist die Planung eines Mobilfunknetzes. Dabei werden die Basisstationen eines Mobilfunknetzes als Knoten eines Graphen repräsentiert. Zwei Knoten werden mit einer Kante verbunden, wenn Sie geographisch so verteilt sind, dass sie sich beim Senden auf der gleichen Frequenz gegenseitig stören können. Existiert eine verträgliche k-Färbung für diesen Graphen, so ist es möglich, ein störungsfreies Mobilfunktnetz mit k verschiedenen Funkfrequenzen aufzubauen. Dabei entsprechen die Farben den verfügbaren Frequenzen. Bei der Planung eines solchen Mobilfunknetzes ist also das folgende Problem zu lösen:

Problem:	kCOL
Eingabe:	Ein ungerichteter Graph G und eine Zahl $k \in \mathbb{N}$.
Frage:	Gibt es eine verträgliche Färbung von G mit k Farben?

Dieses Problem gehört zu einer (sehr großen) Klasse von (praktisch relevanten) Problemen, für die bis heute keine effizienten Algorithmen bekannt sind (Stichwort: **NP**-Vollständigkeit). Vielfältige Ergebnisse der Theoretischen Informatik zeigen sogar, dass

Algorithmus 2 : Zusammenhangskomponenten

Eingabe : Ein Graph $G = (V, E)$
Ergebnis : Anzahl der Zusammenhangskomponenten von G

```
kFarb = 0;
while (es gibt einen unmarkierten Knoten u ∈ V) do
    kFarb++;
    markiere u ∈ V mit kFarb;
    markiert=true;
    while (markiert) do
        markiert=false;
        for (alle mit kFarb markierten Knoten v ∈ V) do
            if (v ∈ V ist adjazent zu einem unmarkierten Knoten v' ∈ V) then
                markiere Knoten v' ∈ V mit kFarb;
                markiert=true;
            end
        end
    end
end
return kFarb.
```

man nicht hoffen darf, dass ein schneller Algorithmus zur Lösung des Färbbarkeitsproblems existiert.

D. Einige formale Grundlagen von Beweistechniken

Praktisch arbeitende Informatiker glauben oft völlig ohne (formale) Beweistechniken auskommen zu können. Dabei meinen sie sogar, dass formale Beweise keinerlei Berechtigung in der Praxis der Informatik haben und bezeichnen solches Wissen als „in der Praxis irrelevantes Zeug, das nur von und für seltsame Wissenschaftler erfunden wurde“. Studenten in den ersten Semestern unterstellen sogar oft, dass mathematische Grundlagen und Beweistechniken nur als „Filter“ dienen, um die Anzahl der Studenten zu reduzieren. Oft stellen sich beide Gruppen sich auf den Standpunkt, dass die Korrektheit von Programmen und Algorithmen durch „Lassen wir es doch mal laufen und probieren es aus!“ ($\triangleq$ Testen) belegt werden könne. Diese Einstellung zeigt sich oft auch darin, dass Programme mit Hilfe einer IDE schnell „testweise“ übersetzt werden, in der Hoffnung oder (schlimmer) in der Überzeugung, dass ein übersetzbares Programm immer auch semantisch korrekt sei.

Theoretiker, die sich mit den Grundlagen der Informatik beschäftigen, vertreten oft den Standpunkt, dass die Korrektheit *jedes* Programms rigoros *bewiesen* werden muss. Wahrscheinlich ist die Position zwischen diesen beiden Extremen richtig, denn zum einen ist der formale Beweis von (großen) Programmen oft nicht praktikabel (oder möglich) und zum anderen kann das Testen mit einer (relativ kleinen) Menge von Eingaben sicherlich nicht belegen, dass ein Programm vollständig den Spezifikationen entspricht. Im praktischen Einsatz ist es dann oft mit Eingaben konfrontiert, die zu einer fehlerhaften Reaktion führen oder es sogar abstürzen[25] lassen. Bei einfacher Anwendersoftware sind solche Fehler ärgerlich, aber oft zu verschmerzen. Bei sicherheitskritischer

[25] Dies wird eindrucksvoll durch viele Softwarepakete und verbreitete Betriebssysteme im PC-Umfeld belegt.

Software (z.B. bei der Regelung von Atomkraftwerken, Airbags und Bremssystemen in Autos, in der Medizintechnik, bei Finanztransaktionssystemen oder bei der Steuerung von Raumsonden) gefährden solche Fehler menschliches Leben oder führen zu extrem hohen finanziellen Verlusten und müssen deswegen unbedingt vermieden werden.

Für den Praktiker bringen Kenntnisse über formale Beweise aber noch andere Vorteile. Viele Beweise beschreiben direkt den zur Lösung benötigten Algorithmus, d.h. eigentlich wird die Richtigkeit einer Aussage durch die (implizite) Angabe eines Algorithmus gezeigt. Aber es gibt noch einen anderen Vorteil. Ist der umzusetzende Algorithmus komplex (z.B. aufgrund einer komplizierten Schleifenstruktur oder einer verschachtelten Rekursion), so ist es unwahrscheinlich, eine korrekte Implementation an den Kunden liefern zu können, ohne die Hintergründe ($\triangleq$ Beweis) verstanden zu haben. All dies zeigt, dass auch ein praktischer Informatiker Einblicke in Beweistechniken haben sollte. Interessanterweise zeigt die persönliche Erfahrung im praktischen Umfeld auch, dass solches (theoretisches) Wissen über die Hintergründe oft zu klarer strukturierten und effizienteren Programmen führt.

Aus diesen Gründen sollen in den folgenden Abschnitten einige grundlegende Beweistechniken mit Hilfe von Beispielen (unvollständig) kurz vorgestellt werden.

D.1. Direkte Beweise

Um einen *direkten Beweis* zu führen, müssen wir, beginnend von einer initialen Aussage ($\triangleq$ Hypothese), durch Angabe einer Folge von (richtigen) Zwischenschritten zu der zu beweisenden Aussage ($\triangleq$ Folgerung) gelangen. Jeder Zwischenschritt ist dabei entweder unmittelbar klar oder muss wieder durch einen weiteren (kleinen) Beweis belegt werden. Dabei müssen nicht alle Schritte völlig formal beschrieben werden, sondern es kommt darauf an, dass sich dem Leser die eigentliche Strategie erschließt.

Satz 145: *Sei* $n \in \mathbb{N}$. *Falls* $n \geq 4$, *dann ist* $2^n \geq n^2$.

Wir müssen also, in Abhängigkeit des Parameters n, die Richtigkeit dieser Aussage belegen. Einfaches Ausprobieren ergibt, dass $2^4 = 16 \geq 16 = 4^2$ und $2^5 = 32 \geq 25 = 5^2$, d.h. intuitiv scheint die Aussage richtig zu sein. Wir wollen die Richtigkeit der Aussage nun durch eine Reihe von (kleinen) Schritten belegen:

Beweis:

Wir haben schon gesehen, dass die Aussage für $n = 4$ und $n = 5$ richtig ist. Erhöhen wir n auf $n + 1$, so verdoppelt sich der Wert der linken Seite der Ungleichung von 2^n auf $2 \cdot 2^n = 2^{n+1}$. Für die rechte Seite ergibt sich ein Verhältnis von $(\frac{n+1}{n})^2$. Je größer n wird, desto kleiner wird der Wert $\frac{n+1}{n}$, d.h. der maximale Wert ist bei $n = 4$ mit 1.25 erreicht. Wir wissen $1.25^2 = 1.5625$. D.h. immer wenn wir n um eins erhöhen, verdoppelt sich der Wert der linken Seite, wogegen sich der Wert der rechten Seite um maximal das 1.5625 fache erhöht. Damit muss die linke Seite der Ungleichung immer größer als die rechte Seite sein. #

Dieser Beweis war nur wenig formal, aber sehr ausführlich und wurde am Ende durch das Symbol „#“ markiert. Im Laufe der Zeit hat es sich eingebürgert, das Ende eines Beweises mit einem besonderen Marker abzuschließen. Besonders bekannt ist hier „qed“, eine Abkürzung für die lateinische Floskel „quod erat demonstrandum“, die mit „was zu beweisen war“ übersetzt werden kann. In neuerer Zeit werden statt „qed“ mit der gleichen Bedeutung meist die Symbole „□“ oder „#“ verwendet.

Nun stellt sich die Frage: „Wie formal und ausführlich muss ein Beweis sein?“ Diese Frage kann so einfach nicht beantwortet werden, denn das hängt u.a. davon ab, welche Lesergruppe durch den Beweis von der Richtigkeit einer Aussage überzeugt werden soll

und wer den Beweis schreibt. Ein Beweis für ein Übungsblatt sollte auch auf Kleinigkeiten Rücksicht nehmen, wogegen ein solcher Stil für eine wissenschaftliche Zeitschrift vielleicht nicht angebracht wäre, da die potentielle Leserschaft über ganz andere Erfahrungen und viel mehr Hintergrundwissen verfügt. Nun noch eine Bemerkung zum Thema „Formalismus“: Die menschliche Sprache ist unpräzise, mehrdeutig und Aussagen können oft auf verschiedene Weise interpretiert werden, wie das tägliche Zusammenleben der Geschlechter eindrucksvoll demonstriert. Diese Defizite sollen Formalismen[26] ausgleichen, d.h. die Antwort muss lauten: „So viele Formalismen wie notwendig und so wenige wie möglich!“. Durch Übung und Praxis lernt man die Balance zwischen diesen Anforderungen zu halten und es zeigt sich bald, dass „Geübte“ die formale Beschreibung sogar wesentlich leichter verstehen.

Oft kann man andere, schon bekannte, Aussagen dazu verwenden, die Richtigkeit einer neuen (evtl. kompliziert wirkenden) Aussage zu belegen.

Satz 146: *Sei $n \in \mathbb{N}$ die Summe von 4 Quadratzahlen, die größer als 0 sind, dann ist $2^n \geq n^2$.*

Beweis: Die Menge der Quadratzahlen ist $\mathbb{S} = \{0, 1, 4, 9, 16, 25, 36, \dots\}$, d.h. 1 ist die kleinste Quadratzahl, die größer als 0 ist. Damit muss unsere Summe von 4 Quadratzahlen größer als 4 sein. Die Aussage folgt direkt aus Satz 145. #

D.1.1. Die Kontraposition

Mit Hilfe von direkten Beweisen haben wir Zusammenhänge der Form „Wenn Aussage H richtig ist, dann folgt daraus die Aussage C“ untersucht. Manchmal ist es schwierig einen Beweis für eine solchen Zusammenhang zu finden. Völlig gleichwertig ist die Behauptung „Wenn die Aussage C falsch ist, dann ist die Aussage H falsch“ und oft ist eine solche Aussage leichter zu zeigen.

Die *Kontraposition* von Satz 145 ist also die folgende Aussage: „Wenn nicht $2^n \geq n^2$, dann gilt nicht $n \geq 4$.“. Das entspricht der Aussage: „Wenn $2^n < n^2$, dann gilt $n < 4$.“, was offensichtlich zu der ursprünglichen Aussage von Satz 145 gleichwertig ist.

Diese Technik ist oft besonders hilfreich, wenn man die Richtigkeit einer Aussage zeigen soll, die aus zwei Teilaussagen zusammengesetzt und die durch ein „genau dann wenn“[27] verknüpft sind. In diesem Fall sind zwei Teilbeweise zu führen, denn zum einen muss gezeigt werden, dass aus der ersten Aussage die zweite folgt und umgekehrt muss gezeigt werden, dass aus der zweiten Aussage die erste folgt.

Satz 147: *Eine natürliche Zahl n ist durch drei teilbar genau dann, wenn die Quersumme ihrer Dezimaldarstellung durch drei teilbar ist.*

Beweis: Für die Dezimaldarstellung von n gilt

$$n = \sum_{i=0}^{k} a_i \cdot 10^i, \text{wobei } a_i \in \{0, 1, \dots, 9\} \text{ („Ziffern“) und } 0 \leq i \leq k.$$

Mit $\mathrm{QS}(n)$ wird die Quersumme von n bezeichnet, d.h. $\mathrm{QS}(n) = \sum_{i=0}^{k} a_i$. Mit Hilfe einer einfachen vollständigen Induktion kann man zeigen, dass für jedes $i \geq 0$ ein $b \in \mathbb{N}$

[26] In diesem Zusammenhang sind Programmiersprachen auch Formalismen, die eine präzise Beschreibung von Algorithmen erzwingen und die durch einen Compiler verarbeitet werden können.

[27] Oft wird „genau dann wenn“ durch *gdw.* abgekürzt.

existiert, sodass $10^i = 9b + 1$. Damit gilt $n = \sum_{i=0}^{k} a_i \cdot 10^i = \sum_{i=0}^{k} a_i(9b_i + 1) = \mathrm{QS}(n) + 9\sum_{i=0}^{k} a_i b_i$, d.h. es existiert ein $c \in \mathbb{N}$, so dass $n = \mathrm{QS}(n) + 9c$.

„⇒“: Wenn n durch 3 teilbar ist, dann muss auch $\mathrm{QS}(n) + 9c$ durch 3 teilbar sein. Da $9c$ sicherlich durch 3 teilbar ist, muss auch $\mathrm{QS}(n) = n - 9c$ durch 3 teilbar sein.

„⇐“: Dieser Fall soll durch Kontraposition gezeigt werden. Sei nun n nicht durch 3 teilbar, dann darf $\mathrm{QS}(n)$ nicht durch 3 teilbar sein, denn sonst wäre $n = 9c + \mathrm{QS}(n)$ durch 3 teilbar. #

D.2. Der Ringschluss

Oft findet man mehrere Aussagen, die zueinander äquivalent sind. Ein Beispiel dafür ist Satz 148. Um die Äquivalenz dieser Aussagen zu beweisen, müssten jeweils zwei „genau dann wenn“ Beziehungen untersucht werden, d.h. es werden vier Teilbeweise notwendig. Dies kann mit Hilfe eines so genannten *Ringschlusses* abgekürzt werden, denn es reicht zu zeigen, dass aus der ersten Aussage die zweite folgt, aus der zweiten Aussage die dritte und dass schließlich aus der dritten Aussage wieder die erste folgt. Im Beweis zu Satz 148 haben wir deshalb nur drei anstatt vier Teilbeweise zu führen, was zu einer Arbeitsersparnis führt. Diese Arbeitsersparnis wird um so größer, je mehr äquivalente Aussagen zu untersuchen sind. Dabei ist die Reihenfolge der Teilbeweise nicht wichtig, solange die einzelnen Teile zusammen einen Ring bilden.

Satz 148: *Seien A und B zwei beliebige Mengen, dann sind die folgenden drei Aussagen äquivalent:*

i) $A \subseteq B$

ii) $A \cup B = B$

iii) $A \cap B = A$

Beweis: Im folgenden soll ein Ringschluss verwendet werden, um die Äquivalenz der drei Aussagen zu zeigen:
„i) ⇒ ii)“: Da nach Voraussetzung $A \subseteq B$ ist, gilt für jedes Element $a \in A$ auch $a \in B$, d.h. in der Vereinigung $A \cup B$ sind alle Elemente nur aus B, was $A \cup B = B$ zeigt.

„ii) ⇒ iii)“: Wenn $A \cup B = B$ gilt, dann ergibt sich durch Einsetzen und mit den Regeln aus Abschnitt A.1.4 (Absorptionsgesetz) direkt $A \cap B = A \cap (A \cup B) = A$.

„iii) ⇒ i)“: Sei nun $A \cap B = A$, dann gibt es kein Element $a \in A$ für das $a \notin B$ gilt. Dies ist aber gleichwertig zu der Aussage $A \subseteq B$.
Damit hat sich ein Ring von Aussagen „i) ⇒ ii)“, „ii) ⇒ iii)“ und „iii) ⇒ i)“ gebildet, was die Äquivalenz aller Aussagen zeigt. #

D.3. Widerspruchsbeweise

Obwohl die Technik der Widerspruchsbeweise auf den ersten Blick sehr kompliziert erscheint, ist sie meist einfach anzuwenden, extrem mächtig und liefert oft sehr kurze Beweise. Angenommen wir sollen die Richtigkeit einer Aussage „aus der Hypothese H folgt C“ zeigen. Dazu beweisen wir, dass sich ein Widerspruch ergibt, wenn wir, von H und der Annahme, dass C falsch ist, ausgehen. Also war die Annahme falsch, und die Aussage C muss richtig sein.
Anschaulicher wird diese Beweistechnik durch folgendes Beispiel: Nehmen wir einmal an, dass Alice eine bürgerliche Frau ist und deshalb auch keine Krone trägt. Es ist klar,

dass jede Königin eine Krone trägt. Wir sollen nun beweisen, dass Alice keine Königin ist. Dazu nehmen wir an, dass Alice eine Königin ist, d.h. Alice trägt eine Krone. Dies ist ein Widerspruch! Also war unsere Annahme falsch, und wir haben gezeigt, dass Alice keine Königin sein kann.
Der Beweis zu folgendem Satz verwendet diese Technik:

Satz 149: *Sei S eine endliche Untermenge einer unendlichen Menge U. Sei T das Komplement von S bzgl. U, dann ist T eine unendliche Menge.*

Beweis: Hier ist unsere Hypothese „S endlich, U unendlich und T Komplement von S bzgl. U“ und unsere Folgerung ist „T ist unendlich“. Wir nehmen also an, dass T eine endliche Menge ist. Da T das Komplement von S ist, gilt $S \cap T = \emptyset$, also ist $\#(S) + \#(T) = \#(S \cap T) + \#(S \cup T) = \#(S \cup T) = n$, wobei n eine Zahl aus $\mathbb{N}$ ist (siehe Abschnitt A.1.6). Damit ist $S \cup T = U$ eine endliche Menge. Dies ist ein Widerspruch zu unserer Hypothese! Also war die Annahme „T ist endlich“ falsch. #

D.4. Der Schubfachschluss

Der *Schubfachschluss* ist auch als *Dirichlets Taubenschlagprinzip* bekannt. Werden $n > k$ Tauben auf k Boxen verteilt, so gibt es mindestens eine Box in der sich wenigstens zwei Tauben aufhalten. Allgemeiner formuliert sagt das Taubenschlagprinzip, dass wenn n Objekte auf k Behälter aufgeteilt werden, dann gibt es mindestens eine Box die mindestens $\lceil \frac{n}{k} \rceil$ Objekte enthält.

Beispiel 150: *Auf einer Party unterhalten sich 8 Personen ($\triangleq$ Objekte), dann gibt es mindestens einen Wochentag ($\triangleq$ Box) an dem $\lceil \frac{8}{7} \rceil = 2$ Personen aus dieser Gruppe Geburtstag haben.*

D.5. Gegenbeispiele

Im wirklichen Leben wissen wir nicht, ob eine Aussage richtig oder falsch ist. Oft sind wir dann mit einer Aussage konfrontiert, die auf den ersten Blick richtig ist und sollen dazu ein Programm entwickeln. Wir müssen also entscheiden, ob diese Aussage wirklich richtig ist, denn sonst ist evtl. alle Arbeit umsonst und hat hohen Aufwand verursacht. In solchen Fällen kann man versuchen, ein einziges Beispiel dafür zu finden, dass die Aussage falsch ist, um so unnötige Arbeit zu sparen.

Wir zeigen, dass die folgenden Vermutungen falsch sind:

Vermutung 151: *Wenn $p \in \mathbb{N}$ eine Primzahl ist, dann ist p ungerade.*

Gegenbeispiel: Die natürliche Zahl 2 ist eine Primzahl und 2 ist gerade. #

Vermutung 152: *Es gibt keine Zahlen $a, b \in \mathbb{N}$, sodass $a \bmod b = b \bmod a$.*

Gegenbeispiel: Für $a = b = 2$ gilt $a \bmod b = b \bmod a = 0$. #

D.6. Induktionsbeweise und das Induktionsprinzip

Eine der wichtigsten und nützlichsten Beweismethoden in der Informatik bzw. Mathematik ist das *Induktionsprinzip*. Wir wollen jetzt nachweisen, dass für jedes $n \in \mathbb{N}$ eine bestimmte Eigenschaft E gilt. Wir schreiben kurz $E(n)$ für die Aussage „n besitzt

die Eigenschaft E". Mit der Schreibweise $E(0)$ drücken[28] wir also aus, dass die erste natürliche Zahl 0 die Eigenschaft E besitzt.

Induktionsprinzip: Es gelten

(IA) $E(0)$

(IS) Für $n \geq 0$ gilt, wenn $E(k)$ für $k \leq n$ korrekt ist, dann ist auch $E(n+1)$ richtig.

Dabei ist **IA** die Abkürzung für *Induktionsanfang* und **IS** ist die Kurzform von *Induktionsschritt*. Die Voraussetzung ($\triangleq$ Hypothese) $E(k)$ ist korrekt für $k \leq n$ und wird im Induktionsschritt als *Induktionsvoraussetzung* benutzt (kurz **IV**). Hat man also den Induktionsanfang und den Induktionsschritt gezeigt, dann ist es anschaulich, dass jede natürliche Zahl die Eigenschaft E haben muss.

Es gibt verschiedene Versionen von Induktionsbeweisen. Die bekannteste Version ist die vollständige Induktion, bei der Aussagen über natürliche Zahlen gezeigt werden.

D.6.1. Die vollständige Induktion

Wie in Piratenfilmen üblich, seien Kanonenkugeln in einer Pyramide mit quadratischer Grundfläche gestapelt. Wir stellen uns die Frage, wieviele Kugeln (in Abhängigkeit von der Höhe) in einer solchen Pyramide gestapelt sind.

Satz 153: *Mit einer quadratische Pyramide aus Kanonenkugeln der Höhe $n \geq 1$ als Munition, können wir $\frac{n(n+1)(2n+1)}{6}$ Schüsse abgeben.*

Beweis: Einfacher formuliert: wir sollen zeigen, dass $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

(IA) Eine Pyramide der Höhe $n = 1$ enthält $\frac{1 \cdot 2 \cdot 3}{6} = 1$ Kugel. D.h. wir haben die Eigenschaft für $n = 1$ verifiziert.

(IV) Für $k \leq n$ gilt $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$.

(IS) Wir müssen nun zeigen, dass $\sum_{i=1}^{n+1} i^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$ gilt und dabei muss die Induktionsvoraussetzung $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ benutzt werden.

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&\overset{\text{IV}}{=} \frac{n(n+1)(2n+1)}{6} + (n^2+2n+1) \\
&= \frac{2n^3+3n^2+n}{6} + (n^2+2n+1) \\
&= \frac{2n^3+9n^2+13n+6}{6} \\
&= \frac{(n+1)(2n^2+7n+6)}{6} \quad (\star) \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \quad (\star\star) \\
&= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}
\end{aligned}$$

Die Zeile $\star$ (bzw. $\star\star$) ergibt sich, indem man $2n^3 + 9n^2 + 13n + 6$ durch $n+1$ teilt (bzw. $2n^2 + 7n + 6$ durch $n+2$). #

Das Induktionsprinzip kann man auch variieren. Dazu soll nun gezeigt werden, dass die Eigenschaft E für alle Zahlen $k \leq n$ erfüllt ist.

Verallgemeinertes Induktionsprinzip: Es gelten

(IA) $E(0)$

[28] Mit E wird also ein Prädikat bezeichnet (siehe Abschnitt A.1.2)

(IS) Wenn für alle $0 \leq k \leq n$ die Eigenschaft $E(k)$ gilt, dann ist auch $E(n+1)$ richtig.

Damit ist das verallgemeinerte Induktionsprinzip eine Verallgemeinerung des oben vorgestellten Induktionsprinzips, wie das folgende Beispiel veranschaulicht:

Satz 154: *Jede natürliche Zahl $n \geq 2$ läßt sich als Produkt von Primzahlen schreiben.*

Beweis: Das verallgemeinerte Induktionsprinzip wird wie folgt verwendet:
(IA) Offensichtlich ist 2 das Produkt von einer Primzahl.
(IV) Jede natürliche Zahl m mit $2 \leq m \leq n$ kann als Produkt von Primzahlen geschrieben werden.
(IS) Nun wird eine Fallunterscheidung durchgeführt:

i) Sei $n+1$ wieder eine Primzahl, dann ist nichts zu zeigen, da $n+1$ direkt ein Produkt von Primzahlen ist.

ii) Sei $n+1$ keine Primzahl, dann existieren mindestens zwei Zahlen p und q mit $2 \leq p, q < n+1$ und $p \cdot q = n+1$. Nach Induktionsvoraussetzung sind dann p und q wieder als Produkt von Primzahlen darstellbar. Etwa $p = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ und $q = q_1 \cdot q_2 \cdot \ldots \cdot q_t$. Damit ist aber $n+1 = p \cdot q = p_1 \cdot p_2 \cdot \ldots \cdot p_s \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_t$ ein Produkt von Primzahlen. #

Solche Induktionsbeweise treten z.B. bei der Analyse von Programmen immer wieder auf.

D.6.2. Induktive Definitionen

Das Induktionsprinzip kann aber auch dazu verwendet werden, (Daten-)Strukturen formal zu spezifizieren. Dazu werden in einem ersten Schritt ($\triangleq$ Induktionsanfang) die „atomaren“ Objekte definiert und dann in einem zweiten Schritt die zusammengesetzten Objekte ($\triangleq$ Induktionsschritt). Diese Technik ist als *induktive Definition* bekannt.

Beispiel 155: *Ein Baum ist wie folgt definiert:*

(IA) *Ein einzelner Knoten w ist ein* Baum *und w ist die* Wurzel *dieses Baums.*
(IS) *Seien $T_1, T_2, \ldots, T_n$ Bäume mit den Wurzeln $k_1, \ldots, k_n$ und w ein einzelner neuer Knoten. Verbinden wir den Knoten w mit allen Wurzeln $k_1, \ldots, k_n$, dann entsteht ein neuer Baum mit der Wurzel w.*

Beispiel 156: *Ein arithmetischer Ausdruck ist wie folgt definiert:*

(IA) *Jeder Buchstabe und jede Zahl ist ein arithmetischer Ausdruck.*
(IS) *Seien E und F Ausdrücke, so sind auch $E+F$, $E*F$ und $[E]$ Ausdrücke.*

D.h. x, $x+y$, $[2*x+z]$ sind arithmetische Ausdrücke, aber beispielsweise sind $x+$, yy, $][x+y$ sowie $x+*z$ keine Ausdrücke im Sinn dieser Definition.

Bei diesem Beispiel ahnt man schon, dass solche Techniken zur präzisen Definition von Programmiersprachen und Dateiformaten gute Dienste leisten. Induktive Definitionen haben noch einen weiteren Vorteil, denn man kann leicht Induktionsbeweise konstruieren, die Aussagen über induktiv definierte Objekte belegen.

D.6.3. Die strukturelle Induktion

Satz 157: *Die Anzahl der öffnenden Klammern eines arithmetischen Ausdrucks stimmt mit der Anzahl der schließenden Klammern überein.*

Es ist offensichtlich, dass diese Aussage richtig ist, denn in Ausdrücken wie $(x + y)/2$ oder $x + ((y/2) * z)$ muss ja zu jeder öffnenden Klammer eine schließende Klammer existieren. Der nächste Beweis verwendet diese Idee zum die Aussage von Satz 157 mit Hilfe einer *strukturellen Induktion* zu zeigen.
Beweis: Wir bezeichnen die Anzahl der öffnenden Klammern eines Ausdrucks E mit $\#_{[}(E)$ und verwenden die analoge Notation $\#_{]}(E)$ für die Anzahl der schließenden Klammern.
(IA) Die einfachsten Ausdrücke sind Buchstaben und Zahlen. Die Anzahl der öffnenden und schließenden Klammern ist in beiden Fällen gleich 0.
(IV) Sei E ein Ausdruck, dann gilt $\#_{[}(E) = \#_{]}(E)$.
(IS) Für einen Ausdruck $E + F$ gilt $\#_{[}(E + F) = \#_{[}(E) + \#_{[}(F) \overset{\text{IV}}{=} \#_{]}(E) + \#_{]}(F) = \#_{]}(E + F)$. Völlig analog zeigt man dies für $E * F$. Für den Ausdruck $[E]$ ergibt sich $\#_{[}([E]) = \#_{[}(E) + 1 \overset{\text{IV}}{=} \#_{]}(E) + 1 = \#_{]}([E])$. In jedem Fall ist die Anzahl der öffnenden Klammern gleich der Anzahl der schließenden Klammern. #

Mit Hilfe von Satz 157 können wir nun leicht ein Programm entwickeln, das einen Plausibilitätscheck (z.B. direkt in einem Editor) durchführt und die Klammern zählt, bevor die Syntax von arithmetischen Ausdrücken überprüft wird. Definiert man eine vollständige Programmiersprache induktiv, dann werden ganz ähnliche Induktionsbeweise möglich, d.h. man kann die Techniken aus diesem Beispiel relativ leicht auf die Praxis der Informatik übertragen.

Stichwortverzeichnis

Symbole

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Literatur

[Can95] Cantor, G.: *Beiträge zur Begründung der transfiniten Mengenlehre.* Mathematische Annalen, 46(4):481–512, 1895.

[CLRS01] Cormen, T. H., C. E. Leiserson, R. L. Rivest, and C. Stein: *Introduction to Algorithms.* MIT Press, 2001.

[GKP94] Graham, R. L., D. E. Knuth, and O. Patashnik: *Concrete Mathematics - A Foundation for Computer Science.* Addison-Wesley, 1994.

[Hag04] Haggarty, R.: *Diskrete Mathematik für Informatiker.* Pearson Studium, 2004.

[MM06] Meinel, C. und M. Mundhenk: *Mathematische Grundlagen der Informatik.* Teubner, 2006.

[SW07] Struckmann, W. und D. Wätjen: *Mathematik für Informatiker - Grundlagen und Anwendungen.* Spektrum Akademischer Verlag, 2007.

[vdW03] Waerden, B. van der: *Algebra*, volume I. Springer, 7^{th} edition, 2003.