Woche 12: *11. Juli 2024*

Thema: *Algebraische Strukturen*

12.1 Einleitung

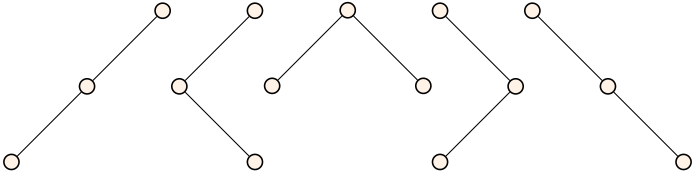
Erinnerung: Wieviele Binärbäume mit n Knoten gibt es?

Frage. Wieviele Binärbäume mit n Knoten gibt es?

(Erinnerung. Wir unterscheiden zwischen linkem und rechtem Nachfolger.)

Beispiel.

Es gibt 5 Binärbäume der Größe 3:



und 14 Binärbäume der Größe 4.

Satz. Für die Anzahl B_n der Binärbäume mit n Knoten gilt:

$$B_0 = 1 \qquad \text{und für } n > 0, \qquad B_n = \sum_{k=1}^{n} B_{k-1} B_{n-k}.$$

Binärbäume mit n Knoten.

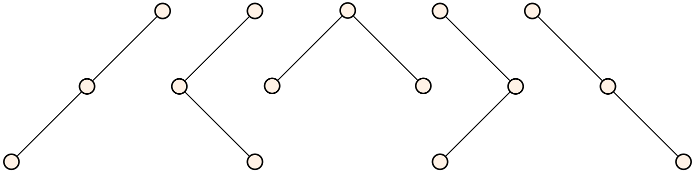
n	Anzahl Bäume
0	1
1	1
2	2
3	5
4	14

Erinnerung: Wieviele Binärbäume mit n Knoten gibt es?

Frage. Wieviele Binärbäume mit n Knoten gibt es, wenn wir NICHT zwischen linkem und rechtem Nachfolger unterscheiden?

Beispiel.

Es gibt ~~5~~ 2 Binärbäume der Größe 3:

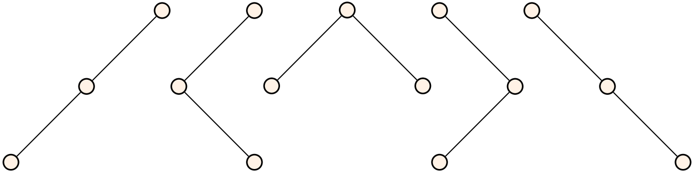


Erinnerung: Wieviele Binärbäume mit n Knoten gibt es?

Frage. Wieviele Binärbäume mit n Knoten gibt es, wenn wir NICHT zwischen linkem und rechtem Nachfolger unterscheiden?

Beispiel.

Es gibt ~~5~~ 2 Binärbäume der Größe 3:



Frage. Wie können wir das berechnen?

Wieviele Binärbäume mit n Knoten gibt es?

Erinnerung. Die Catalan-Zahlen lieferten die Zahl der Binärbäume auf n Knoten, bei denen links und rechts unterschieden wurde.

Ungeordnete Binärbäume.

Hier betrachten wir Binärbäume als Wurzelbäume in denen jeder Knoten Grad ≤ 3, d.h. höchstens 2 Nachfolger, hat.

Frage. Wann sind zwei Binärbäume „gleich“?

1. Sicherlich sollte $|V(T)| = |V(T')|$.
2. T und T' sollten die gleiche „Struktur“ haben.

Wieviele Binärbäume mit n Knoten gibt es?

Erinnerung. Die Catalan-Zahlen lieferten die Zahl der Binärbäume auf n Knoten, bei denen links und rechts unterschieden wurde.

Ungeordnete Binärbäume.
Hier betrachten wir Binärbäume als Wurzelbäume in denen jeder Knoten Grad ≤ 3, d.h. höchstens 2 Nachfolger, hat.

Frage. Wann sind zwei Binärbäume „gleich“?

1. Sicherlich sollte $|V(T)| = |V(T')|$.
2. T und T' sollten die gleiche „Struktur“ haben.

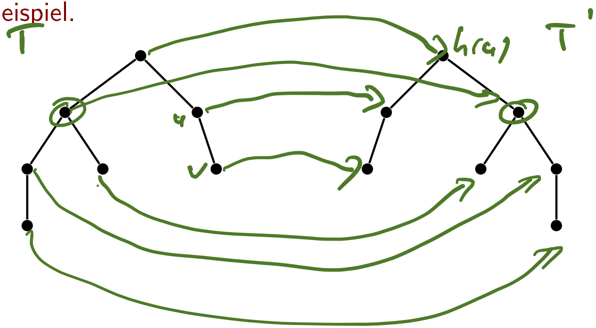
Definition (Isomorphismus). Ein *Isomorphismus* zwischen zwei Binärbäumen T und T' ist eine bijektive Abbildung $h : V(T) \to V(T')$ zwischen den Knotenmengen, so dass

- h die Wurzel von T auf die Wurzel von T' abbildet und
- für alle $u, v \in V(T)$ gilt:

$$(u, v) \in E(T) \text{ gdw. } (h(u), h(v)) \in E(T').$$

Isomorphismen zwischen Bäumen

Beispiel.

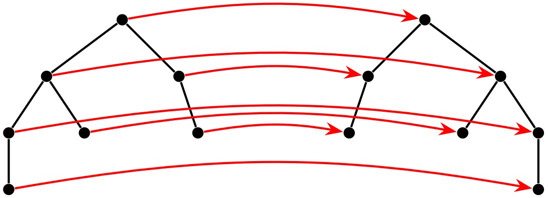


Definition (Isomorphismus). Ein *Isomorphismus* zwischen zwei Binärbäumen T und T' ist eine bijektive Abbildung $h : V(T) \to V(T')$ zwischen den Knotenmengen, so dass

- h die Wurzel von T auf die Wurzel von T' abbildet und
- für alle $u, v \in V(T)$ gilt: $(u, v) \in E(T)$ gdw. $(h(u), h(v)) \in E(T')$.

Isomorphismen zwischen Bäumen

Beispiel.



Beobachtung. Sei $h : V(T) \to V(T')$ ein Isomorphismus.

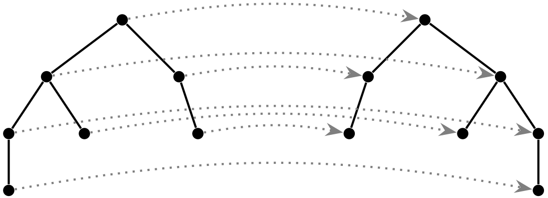
- Es gilt $|V(T)| = |V(T')|$
- Für alle $u \in V(T)$ haben u und $h(u)$ genau gleich viele Nachfolger.

Definition (Isomorphismus). Ein *Isomorphismus* zwischen zwei Binärbäumen T und T' ist eine bijektive Abbildung $h : V(T) \to V(T')$ zwischen den Knotenmengen, so dass

- h die Wurzel von T auf die Wurzel von T' abbildet und
- für alle $u, v \in V(T)$ gilt: $(u, v) \in E(T)$ gdw. $(h(u), h(v)) \in E(T')$.

Strukturerhaltende Transformationen

Beispiel.



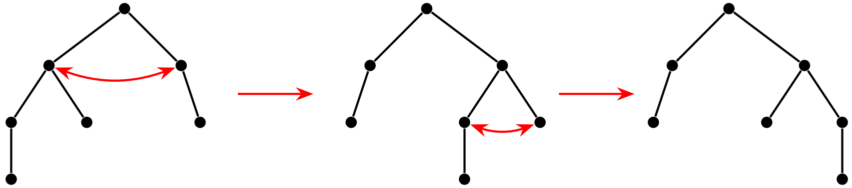
Strukturerhaltende Transformationen.

Wenn wir in T die beiden Nachfolger eines Knotens vertauschen, erhalten wir wieder den gleichen Baum.

Isomorphe Bäume (mit der gleichen Knotenmenge) können durch solche Transformationen ineinander umgewandelt werden.

Strukturerhaltende Transformationen

Beispiel.



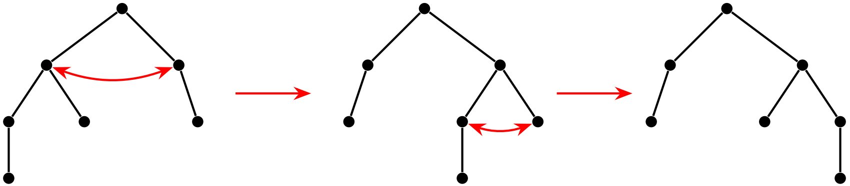
Strukturerhaltende Transformationen.

Wenn wir in T die beiden Nachfolger eines Knotens vertauschen, erhalten wir wieder den gleichen Baum.

Isomorphe Bäume (mit der gleichen Knotenmenge) können durch solche Transformationen ineinander umgewandelt werden.

Strukturerhaltende Transformationen

Beispiel.



Strukturerhaltende Transformationen.

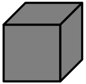
Wenn wir in T die beiden Nachfolger eines Knotens vertauschen, erhalten wir wieder den gleichen Baum.

Isomorphe Bäume (mit der gleichen Knotenmenge) können durch solche Transformationen ineinander umgewandelt werden.

Anzahl Binärbäume mit n Knoten. Zum Zählen von Binärbäumen ohne Nachfolgerordnung reicht es also zu wissen, in wieviele Bäume ein (geordneter) Baum T auf diese Art umgewandelt werden kann.

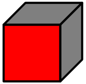
Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau*, *rot*$\}$ gefärbt wird.



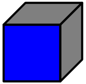
Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{blau, rot\}$ gefärbt wird.



Ein weiteres Beispiel

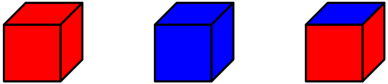
Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau, rot*$\}$ gefärbt wird.



Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau, rot*$\}$ gefärbt wird.

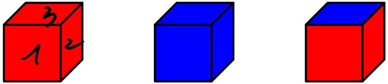
Wieviele verschiedene gefärbte Würfel gibt es?



Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau, rot*$\}$ gefärbt wird.

Wieviele verschiedene gefärbte Würfel gibt es?



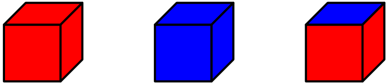
Anzahl gefärbter Würfel?

Wenn die Seitenflächen nummeriert wären, gäbe es genau verschiedene Färbungen.

Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau*, *rot*$\}$ gefärbt wird.

Wieviele verschiedene gefärbte Würfel gibt es?



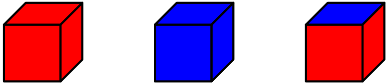
Anzahl gefärbter Würfel?

Wenn die Seitenflächen nummeriert wären, gäbe es genau $2^6 = 64$ verschiedene Färbungen.

Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau, rot*$\}$ gefärbt wird.

Wieviele verschiedene gefärbte Würfel gibt es?



Anzahl gefärbter Würfel?

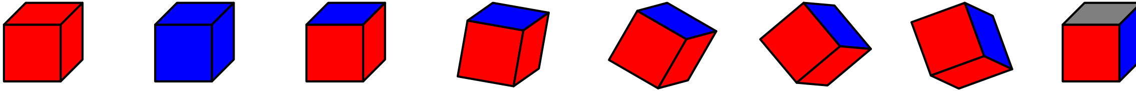
Wenn die Seitenflächen nummeriert wären, gäbe es genau $2^6 = 64$ verschiedene Färbungen.

Aber was, wenn die Seiten nicht unterscheidbar sind, sondern nur *oben, unten, vorne, links, hinten, rechts* unterschieden wird?

Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau, rot*$\}$ gefärbt wird.

Wieviele verschiedene gefärbte Würfel gibt es?



Anzahl gefärbter Würfel?

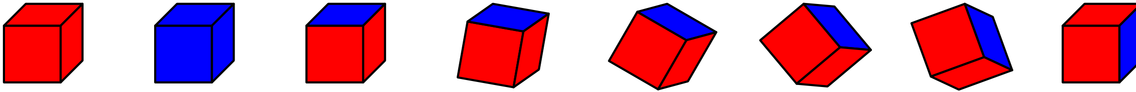
Wenn die Seitenflächen nummeriert wären, gäbe es genau $2^6 = 64$ verschiedene Färbungen.

Aber was, wenn die Seiten nicht unterscheidbar sind, sondern nur *oben, unten, vorne, links, hinten, rechts* unterschieden wird?

Ein weiteres Beispiel

Gefärbte Würfel. Wir betrachten 6-seitige Würfel, bei denen jede der 6 Seiten durch eine der Farben $\{$*blau, rot*$\}$ gefärbt wird.

Wieviele verschiedene gefärbte Würfel gibt es?



Anzahl gefärbter Würfel?

Wenn die Seitenflächen nummeriert wären, gäbe es genau $2^6 = 64$ verschiedene Färbungen.

Aber was, wenn die Seiten nicht unterscheidbar sind, sondern nur *oben, unten, vorne, links, hinten, rechts* unterschieden wird?

Bei zwei möglichen Farben gibt es 10 Färbungen.

Bei drei möglichen Farben gibt es 57 Färbungen.

Aber wie rechnet man das aus?

Gemeinsamkeiten der beiden Beispiele

Was haben die Binärbäume mit den Würfeln gemeinsam?

In beiden Fällen gibt es eine Menge M möglicher Positionen.

$M =$ Menge $\mathcal{B}_n$ aller Binärbäume mit n Knoten und „rechts/links“.

$M =$ Menge der Färbungen von $\{oben, unten, vorne, links, hinten, rechts\}$.

Gemeinsamkeiten der beiden Beispiele

Was haben die Binärbäume mit den Würfeln gemeinsam?

In beiden Fällen gibt es eine Menge M möglicher Positionen.

$M =$ Menge $\mathcal{B}_n$ aller Binärbäume mit n Knoten und „rechts/links“.

$M =$ Menge der Färbungen von $\{oben, unten, vorne, links, hinten, rechts\}$.

Zusätzlich haben wir in beiden Fällen noch eine Menge von *Abbildungen* oder *Operationen*, die Elemente von M auf Elemente von M abbilden.

„Vertauschen der Nachfolger“ von Knoten eines Baums.

„Drehen“ des Würfels entlang einer der möglichen Axen.

Gemeinsamkeiten der beiden Beispiele

Was haben die Binärbäume mit den Würfeln gemeinsam?

In beiden Fällen gibt es eine Menge M möglicher Positionen.

$M =$ Menge $\mathcal{B}_n$ aller Binärbäume mit n Knoten und „rechts/links“.

$M =$ Menge der Färbungen von $\{$*oben, unten, vorne, links, hinten, rechts*$\}$.

Zusätzlich haben wir in beiden Fällen noch eine Menge von *Abbildungen* oder *Operationen*, die Elemente von M auf Elemente von M abbilden.

„Vertauschen der Nachfolger“ von Knoten eines Baums.

„Drehen“ des Würfels entlang einer der möglichen Axen.

In beiden Fällen wollen wir die maximale Zahl der Elemente aus M berechnen, die paarweise nicht ineinander umgeform werden können.

Gemeinsamkeiten der beiden Beispiele

Was haben die Binärbäume mit den Würfeln gemeinsam?

In beiden Fällen gibt es eine Menge M möglicher Positionen.

$M =$ Menge $\mathcal{B}_n$ aller Binärbäume mit n Knoten und „rechts/links“.

$M =$ Menge der Färbungen von $\{oben, unten, vorne, links, hinten, rechts\}$.

Zusätzlich haben wir in beiden Fällen noch eine Menge von *Abbildungen* oder *Operationen*, die Elemente von M auf Elemente von M abbilden.

„Vertauschen der Nachfolger“ von Knoten eines Baums.

„Drehen“ des Würfels entlang einer der möglichen Axen.

In beiden Fällen wollen wir die maximale Zahl der Elemente aus M berechnen, die paarweise nicht ineinander umgeform werden können.

Abstraktion durch algebraische Strukturen.

Diesen gemeinsamen Kern beider Probleme kann man elegant durch *algebraische Strukturen* modellieren.

Hier: Orbits einer Gruppe G, die auf der Menge M operiert.

12.2 Universelle Algebra

Universelle Algebra

Definition (Universelle Algebra).

Sei S eine Menge.

1. Ein Operator ist eine Abbildung $f : S^m \to S$.

   Man nennt m die Stelligkeit von f.
2. Eine (universelle) Algebra $(S, f_1, \ldots, f_t)$ besteht aus
   - einer nicht-leeren Menge S, der Trägermenge oder Universum, sowie
   - Operatoren $f_1, \ldots, f_t$ auf S.

Universelle Algebra

Definition (Universelle Algebra).

Sei S eine Menge.

1. Ein Operator ist eine Abbildung $f : S^m \to S$.

   Man nennt m die Stelligkeit von f.
2. Eine (universelle) Algebra $(S, f_1, \dots, f_t)$ besteht aus
   - einer nicht-leeren Menge S, der Trägermenge oder Universum, sowie
   - Operatoren $f_1, \dots, f_t$ auf S.

Beispiele. Einige Beispiele für Algebren sind:

- $(\mathbb{N}, +)$,
- $(\mathbb{R}, \cdot, +, -)$,
- die Boolesche Algebra $(\{0, 1\}, \vee, \wedge, \neg)$
- Sei Σ ein endliches Alphabet. Dann ist $(\Sigma^*, \circ)$ eine Algebra, wobei $\circ$ die *Wortkonkatenation* bezeichnet.

  串联

  $$a_1 \dots a_n \circ b_1 \dots b_m = a_1 \dots a_n b_1 \dots b_m$$

Beispiele

Beispiel. Permutationen.

Sei S_n die Menge der Permutationen einer n-elementigen Menge.

Da Permutationen bijektive Abbildungen sind, können wir als Operator $\circ$ die „Hintereinanderausführung" benutzen.

Für $f, g \in S_n$ definieren wir also $f \circ g \in S_n$ durch die Abbildung $f(g(x))$.

Dann bildet $(S_n, \circ)$ eine Algebra (die *symmetrische Gruppe* $\mathfrak{S}_n$)

Beispiele

Beispiel. Permutationen.

Sei S_n die Menge der Permutationen einer n-elementigen Menge.

Da Permutationen bijektive Abbildungen sind, können wir als Operator $\circ$ die „Hintereinanderausführung“ benutzen.

Für $f, g \in S_n$ definieren wir also $f \circ g \in S_n$ durch die Abbildung $f(g(x))$.

Dann bildet $(S_n, \circ)$ eine Algebra (die *symmetrische Gruppe* $\mathfrak{S}_n$)

Beispiel. Binärbäume zum zweiten.

Sei nun $\mathcal{I}_n$ die Menge der Isomorphismen zwischen Binärbäumen mit n Elementen und ohne „rechts/links“ Unterschied.

Es gilt $\mathcal{I}_n \subseteq S_n$, denn Isomorphismen waren ja spezielle Permutationen.

Also können wir auch $\mathcal{I}_n$ zusammen mit $\circ$ betrachten.

Beispiele

Beispiel. Permutationen.

Sei S_n die Menge der Permutationen einer n-elementigen Menge.

Da Permutationen bijektive Abbildungen sind, können wir als Operator $\circ$ die „Hintereinanderausführung“ benutzen.

Für $f, g \in S_n$ definieren wir also $f \circ g \in S_n$ durch die Abbildung $f(g(x))$.

Dann bildet $(S_n, \circ)$ eine Algebra (die *symmetrische Gruppe* $\mathfrak{S}_n$)

Beispiel. Binärbäume zum zweiten.

Sei nun $\mathcal{I}_n$ die Menge der Isomorphismen zwischen Binärbäumen mit n Elementen und ohne „rechts/links“ Unterschied.

Es gilt $\mathcal{I}_n \subseteq S_n$, denn Isomorphismen waren ja spezielle Permutationen.

Also können wir auch $\mathcal{I}_n$ zusammen mit $\circ$ betrachten.

Frage. Ist das eine Algebra?

Beispiele

Beispiel. Permutationen.

Sei S_n die Menge der Permutationen einer n-elementigen Menge.

Da Permutationen bijektive Abbildungen sind, können wir als Operator $\circ$ die „Hintereinanderausführung“ benutzen.

Für $f, g \in S_n$ definieren wir also $f \circ g \in S_n$ durch die Abbildung $f(g(x))$.

Dann bildet $(S_n, \circ)$ eine Algebra (die *symmetrische Gruppe* $\mathfrak{S}_n$)

Beispiel. Binärbäume zum zweiten.

Sei nun $\mathcal{I}_n$ die Menge der Isomorphismen zwischen Binärbäumen mit n Elementen und ohne „rechts/links“ Unterschied.

Es gilt $\mathcal{I}_n \subseteq S_n$, denn Isomorphismen waren ja spezielle Permutationen.

Also können wir auch $\mathcal{I}_n$ zusammen mit $\circ$ betrachten.

Frage. Ist das eine Algebra? Antwort. Ja, denn zwei Isomorphismen hintereinander ergeben wieder einen Isomorphismus.

$(\mathcal{I}_n, \circ)$ ist eine *Unteralgebra* von $(S_n, \circ)$.

Unteralgebren

Definition. Sei $\mathcal{A} := (S, f_1, \dots, f_k)$ eine Algebra, wobei f_i ein r_i-stelliger Operator sei, für alle $1 \leq i \leq k$.

Eine nichtleere Teilmenge $S' \subseteq S$ erzeugt eine Unteralgebra von $\mathcal{A}$, falls S' unter den Operatoren f_i abgeschlossen ist, d.h. falls für alle $1 \leq i \leq k$ und alle $a_1, \dots, a_{r_i} \in S'$ gilt:

$$f_i(a_1, \dots, a_{r_i}) \in S'.$$

Beispiel.

Sei $\mathcal{Z} := (\mathbb{Z}, +)$, wobei $+$ die übliche Addition auf $\mathbb{Z}$ ist.

- Dann erzeugt $\mathbb{N}$ eine Unteralgebra $(\mathbb{N}, +)$, da die Summe zweier natürlicher Zahlen wieder eine natürliche Zahl ist.
- Allerdings erzeugt $\mathbb{N} \cup \{-1\}$ keine Unteralgebra, da $-1 + (-1) \notin \mathbb{N} \cup \{-1\}$.

Inverse und neutrale Elemente

Neutrale Elemente

Beispiel.

Betrachten wir die Algebra $(\mathbb{R}, +)$ der reellen Zahlen mit Addition.

Die 0 spielt eine besondere Rolle, da $x + 0 = 0 + x = x$ für alle $x \in \mathbb{R}$.

0 ist also bezüglich der Addition *neutral*.

Neutrale Elemente

Beispiel.

Betrachten wir die Algebra $(\mathbb{R}, +)$ der reellen Zahlen mit Addition.

Die 0 spielt eine besondere Rolle, da $x + 0 = 0 + x = x$ für alle $x \in \mathbb{R}$.

0 ist also bezüglich der Addition *neutral*.

Definition. Sei $(S, \circ)$ eine Algebra mit zweistelligem Operator $\circ$.
Ein Element $e \in S$ heißt linksneutrales Element für $\circ$, wenn

$$e \circ a = a \qquad \text{für alle } a \in S.$$

e heißt rechtsneutrales Element, wenn

$$a \circ e = a \qquad \text{für alle } a \in S.$$

e ist ein neutrales Element, wenn es links- und rechtsneutral ist.

Neutrale Elemente

Lemma. *Sei $(S, \circ)$ eine Algebra mit zweistelliger Verknüpfung $\circ$. Ist c ein linksneutrales und d ein rechtsneutrales Element, so ist $c = d$.*

Insbesondere enthält also $(S, \circ)$ höchstens ein neutrales Element.

Beweis. Da c linksneutral ist, gilt $c \circ d = d$.

Und da d rechtsneutral ist, gilt $c \circ d = c$.

Definition. $(S, \circ)$ Algebra.

$e \in S$ *linksneutral*, wenn

$$e \circ a = a \quad \text{für alle } a \in S.$$

e *rechtsneutral*, wenn

$$a \circ e = a \quad \text{für alle } a \in S.$$

e *neutrales Element*, wenn es links- und rechtsneutral ist.

Neutrale Elemente

Lemma. *Sei $(S, \circ)$ eine Algebra mit zweistelliger Verknüpfung $\circ$. Ist c ein linksneutrales und d ein rechtsneutrales Element, so ist $c = d$.*

Insbesondere enthält also $(S, \circ)$ höchstens ein neutrales Element.

Beweis. Da c linksneutral ist, gilt $c \circ d = d$.

Und da d rechtsneutral ist, gilt $c \circ d = c$.

Also gilt $c = d$.

Definition. $(S, \circ)$ Algebra.

$e \in S$ *linksneutral*, wenn

$$e \circ a = a \quad \text{für alle } a \in S.$$

e *rechtsneutral*, wenn

$$a \circ e = a \quad \text{für alle } a \in S.$$

e *neutrales Element*, wenn es links- und rechtsneutral ist.

Neutrale Elemente

Definition. $(S, \circ)$ Algebra.

$e \in S$ *linksneutral*, wenn

$e \circ a = a \quad$ für alle $a \in S$.

e *rechtsneutral*, wenn

$a \circ e = a \quad$ für alle $a \in S$.

e *neutrales Element*, wenn es links- und rechtsneutral ist.

Lemma. *Sei $(S, \circ)$ eine Algebra mit zweistelliger Verknüpfung $\circ$. Ist c ein linksneutrales und d ein rechtsneutrales Element, so ist $c = d$.*
Insbesondere enthält also $(S, \circ)$ höchstens ein neutrales Element.

Beweis. Da c linksneutral ist, gilt $c \circ d = d$.

Und da d rechtsneutral ist, gilt $c \circ d = c$.

Also gilt $c = d$.

Da neutrale Elemente sowohl links- als auch rechtsneutral sind, kann es daher auch keine zwei verschiedenen neutralen Elemente geben. □

Beispiele

Beispiel. Betrachten wir die Algebra $(\mathbb{R}, +)$ der reellen Zahlen mit Addition.

Die 0 spielt eine besondere Rolle, da $x + 0 = 0 + x = x$ für alle $x \in \mathbb{R}$.

0 ist also bezüglich der Addition *neutral*.

Weiterhin gibt es für jedes $x \in \mathbb{R}$ eine Zahl $y \in \mathbb{R}$ für die gilt:

$$x + y = y + x = 0.$$

$y = -x$ ist das *inverse* Element zu x.

Definition. $(S, \circ)$ Algebra.

$e \in S$ *linksneutral*, wenn

$$e \circ a = a \quad \text{für alle } a \in S.$$

e *rechtsneutral*, wenn

$$a \circ e = a \quad \text{für alle } a \in S.$$

e *neutrales Element*, wenn es links- und rechtsneutral ist.

Inverse Elemente

Definition. Sei $(S, \circ)$ eine Algebra mit einem zweistelligen Operator $\circ$ und einem neutralen Element e.

Sei $a \in S$.

Ein Element $x \in S$ heißt linksinverses Element von a, falls $x \circ a = e$.

x heißt rechtsinverses Element von a, falls $a \circ x = e$.

Wie zuvor heißt x inverses Element von a, falls x sowohl rechts- also auch linksinverses Element von a ist.

Inverse Elemente

Definition. Sei $(S, \circ)$ eine Algebra mit einem zweistelligen Operator $\circ$ und einem neutralen Element e.

Sei $a \in S$.

Ein Element $x \in S$ heißt linksinverses Element von a, falls $x \circ a = e$.

x heißt rechtsinverses Element von a, falls $a \circ x = a$.

Wie zuvor heißt x inverses Element von a, falls x sowohl rechts- also auch linksinverses Element von a ist.

Anmerkung.
Im Allgemeinen hat nicht jedes Element einer Algebra mit neutralem Element auch immer ein inverses.

Auch gibt es Algebren, in denen Elemente mehrere verschiedene inverse Elemente haben.

Inverse Elemente

Definition. Ein Operator $\circ : S \times S \to S$ heißt assoziativ, wenn für alle $x, y, z \in S$ gilt:

$$(x \circ y) \circ z \quad = \quad x \circ (y \circ z).$$

Lemma. *Sei $(S, \circ)$ eine Algebra mit einem assoziativen zweistelligen Operator $\circ$ und neutralem Element $e \in S$.*

Dann gilt für alle $a \in S$: Ist x ein links- und y ein rechtsinverses Element von a, so ist $x = y$.

Insbesondere besitzt jedes Element $a \in S$ höchstens ein inverses Element.

Definition. $(S, \circ)$ Algebra.

$e \in S$ *linksneutral*, wenn

$$e \circ a = a \quad \text{für alle } a \in S.$$

e *rechtsneutral*, wenn

$$a \circ e = a \quad \text{für alle } a \in S.$$

e *neutrales Element*, wenn es links- und rechtsneutral ist.

Definition.
$(S, \circ)$ Algebra und $a \in S$.

$x \in S$ *linksinvers* zu a, wenn

$$x \circ a = e$$

x *rechtsinvers* zu a, wenn

$$a \circ x = e.$$

x *inverses Element* von a, wenn es links- und rechtsinvers ist.

Beweis des Lemmas

Lemma. *Sei $(S, \circ)$ eine Algebra mit einem assoziativen zweistelligen Operator $\circ$ und neutralem Element $e \in S$.*

Dann gilt für alle $a \in S$: Ist x ein links- und y ein rechtsinverses Element von a, so ist $x = y$.

Insbesondere besitzt jedes Element $a \in S$ höchstens ein inverses Element.

Beweis. Da e ein neutrales Element ist, gilt $y = e \circ y$ sowie $x \circ e = x$.

Es gilt also

$$y = e \circ y = (x \circ a) \circ y = x \circ (a \circ y) = x \circ e = x.$$

Dabei gilt die zweite Gleichheit, da $e = (x \circ a)$, denn x ist linksinvers.

Ebenso gilt die vierte Gleichheit, da y rechtsinvers ist. □

Definition. $(S, \circ)$ Algebra.

$e \in S$ *linksneutral*, wenn

$$e \circ a = a \quad \text{für alle } a \in S.$$

e *rechtsneutral*, wenn

$$a \circ e = a \quad \text{für alle } a \in S.$$

e *neutrales Element*, wenn es links- und rechtsneutral ist.

Definition.
$(S, \circ)$ Algebra und $a \in S$.

$x \in S$ *linksinvers* zu a, wenn

$$x \circ a = e$$

x *rechtsinvers* zu a, wenn

$$a \circ x = e.$$

x *inverses Element* von a, wenn es links- und rechtsinvers ist.

Spezielle Algebren: Halbgruppen, Monoide und Gruppen

Monoide und Gruppen

Definition (Halbgruppen, Monoide und Gruppen).

Sei $\mathcal{A} := (S, \circ)$ eine Algebra mit einem zweistelligen Operator $\circ$.

1. $\mathcal{A}$ heißt Halbgruppe (engl. semigroup), wenn $\circ$ assoziativ ist.
2. Ist $\mathcal{A}$ eine Halbgruppe und gibt es zusätzlich noch ein neutrales Element $e \in S$, dann heißt $\mathcal{A}$ ein Monoid.
3. Ist $\mathcal{A}$ ein Monoid in dem jedes Element $a \in S$ ein inverses Element besitzt, dann heißt $\mathcal{A}$ eine Gruppe.
4. Ist in den obigen Definitionen der Operator $\circ$ kommutativ, dann heißt $\mathcal{A}$ eine *abelsche* Halbgruppe (Monoid, Gruppe).

Beispiele

Beispiele.

1. Die natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition $\circ := +$ bilden ein Monoid mit neutralem Element $e = 0$.

   Ebenso bildet $\mathbb{N}$ zusammen mit der Multiplikation $\circ := \cdot$ ein Monoid mit neutralem Element $e = 1$.

   Allerdings bildet $(\mathbb{N}, +)$ keine Gruppe.

$\mathcal{A} := (S, \circ)$ Algebra.

Halbgruppe:
- $\circ$ assoziativ.

Monoid:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.

Gruppe:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.
- jedes $a \in S$ hat Inverses.

Beispiele

Beispiele.

1. Die natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition $\circ := +$ bilden ein Monoid mit neutralem Element $e = 0$.

   Ebenso bildet $\mathbb{N}$ zusammen mit der Multiplikation $\circ := \cdot$ ein Monoid mit neutralem Element $e = 1$.

   Allerdings bildet $(\mathbb{N}, +)$ keine Gruppe.

2. Sei S_n die Menge der Permutationen (also Bijektionen) einer n-elementigen Menge.

   Dann bildet S_n zusammen mit $\circ$ eine Gruppe.
   - $\circ$ ist assoziativ.
   - Die Identitätsabbildung $f(x) = x$ ist ein neutrales Element.
   - Zu jeder Bijektion f können wir die Umkehrabbildung f^{-1} bilden, die das *inverse* Element zu f ist.

Definition. Die Gruppe $(S_n, \circ)$ heißt die *symmetrische Gruppe* $\mathfrak{S}_n$ der Ordnung n.

$\mathcal{A} := (S, \circ)$ Algebra.

Halbgruppe:
- $\circ$ assoziativ.

Monoid:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.

Gruppe:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.
- jedes $a \in S$ hat Inverses.

12.3 Monoide

Beispiele für Monoide

Beispiel. Die natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition $\circ := +$ bilden ein Monoid $(\mathbb{N}, +)$ mit neutralem Element $e = 0$.

Ebenso bildet $\mathbb{N}$ zusammen mit der Multiplikation $\circ := \cdot$ ein Monoid $(\mathbb{N}, \cdot)$ mit neutralem Element $e = 1$.

Beispiel.

Sei $M := \{0, 1\}$ und sei die Operation $\oplus : M \times M \to M$ definiert durch $a \oplus b := a + b \mod 2$.

Dann ist $\mathcal{M} := (M, \oplus)$ ein Monoid mit neutralem Element 0.

$\mathcal{A} := (S, \circ)$ Algebra.

Halbgruppe:

- $\circ$ assoziativ.

Monoid:

- $\circ$ assoziativ.
- neutrales Element $e \in S$.

Gruppe:

- $\circ$ assoziativ.
- neutrales Element $e \in S$.
- jedes $a \in S$ hat Inverses.

Beispiele für Monoide

Beispiel. Die natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition $\circ := +$ bilden ein Monoid $(\mathbb{N}, +)$ mit neutralem Element $e = 0$.

Ebenso bildet $\mathbb{N}$ zusammen mit der Multiplikation $\circ := \cdot$ ein Monoid $(\mathbb{N}, \cdot)$ mit neutralem Element $e = 1$.

Beispiel.

Sei $M := \{0, 1\}$ und sei die Operation $\oplus : M \times M \to M$ definiert durch $a \oplus b := a + b \mod 2$.

Dann ist $\mathcal{M} := (M, \oplus)$ ein Monoid mit neutralem Element 0.

Definition. Seien $\mathcal{N} := (N, \circ)$ und $\mathcal{M} := (M, \cdot)$ Monoide.

Eine Abbildung $h : N \to M$ heißt *Homomorphismus* von $\mathcal{N}$ nach $\mathcal{M}$, wenn für alle $a, b \in N$ gilt:

$$h(a \circ b) \;=\; h(a) \cdot h(b).$$

$\mathcal{A} := (S, \circ)$ Algebra.

Halbgruppe:
- $\circ$ assoziativ.

Monoid:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.

Gruppe:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.
- jedes $a \in S$ hat Inverses.

Beispiele für Monoide

Definition. Seien $\mathcal{N} := (N, \circ)$ und $\mathcal{M} := (M, \cdot)$ Monoide.

Eine Abbildung $h : N \to M$ heißt *Homomorphismus* von $\mathcal{N}$ nach $\mathcal{M}$, wenn für alle $a, b \in N$ gilt: $h(a \circ b) = h(a) \cdot h(b)$.

Beispiel. Betrachten wir die vorherigen Beispiele.

Sei $\mathcal{N} := (\mathbb{N}, +)$ und $\mathcal{M} := (M, \oplus)$, wobei $M := \{0, 1\}$ und $a \oplus b := a + b \mod 2$.

Dann ist $h : \mathbb{N} \to M$ definiert durch

$$h(n) := \begin{cases} 0 & n \text{ gerade} \\ 1 & n \text{ ungerade} \end{cases}$$

ein Homomorphismus von $\mathcal{N}$ nach $\mathcal{M}$.

Denn für alle $a, b \in \mathbb{N}$ gilt:

$a + b$ gerade gdw. a, b beide gerade oder beide ungerade sind.

Also $h(a + b) = 0$ gdw. $h(a) = h(b) = 0$ oder $h(a) = h(b) = 1$

gdw. $h(a) \oplus h(b) = 0$.

$\mathcal{A} := (S, \circ)$ Algebra.

Halbgruppe:
- $\circ$ assoziativ.

Monoid:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.

Gruppe:
- $\circ$ assoziativ.
- neutrales Element $e \in S$.
- jedes $a \in S$ hat Inverses.

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet.

Wir definieren $\cdot$ als die *Konkatenation* zweier Wörter.

Dann ist $\mathcal{S} := (\Sigma^*, \cdot)$ ein Monoid mit neutralem Element ϵ.

Wir nennen $(\Sigma^*, \cdot)$ das *freie Monoid* über Σ.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide

$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet.

Wir definieren $\cdot$ als die *Konkatenation* zweier Wörter.

Dann ist $\mathcal{S} := (\Sigma^*, \cdot)$ ein Monoid mit neutralem Element ϵ.

Wir nennen $(\Sigma^*, \cdot)$ das *freie Monoid* über Σ.

Beispiel.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Frage. Wie sehen Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$ aus?

$h(\underline{\varepsilon}) = \underline{0}$

Homomorphismen.

$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide

$h : N \to M$ *Homomorphismus*:

für alle $a, b \in N$ gilt:

$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet.

Wir definieren $\cdot$ als die *Konkatenation* zweier Wörter.

Dann ist $\mathcal{S} := (\Sigma^*, \cdot)$ ein Monoid mit neutralem Element ϵ.

Wir nennen $(\Sigma^*, \cdot)$ das *freie Monoid* über Σ.

Beispiel.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Frage. Wie sehen Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$ aus?

- Es gilt $h(\epsilon) = 0$.

  Denn wäre $h(\epsilon) = 1$, dann:

  $$h(\epsilon) = h(\epsilon \cdot \epsilon) \neq h(\epsilon) \oplus h(\epsilon) = 1 \oplus 1 = 0.$$

> **Homomorphismen.**
> $\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
>
> $h : N \to M$ *Homomorphismus*:
>
> für alle $a, b \in N$ gilt:
>
> $$h(a \circ b) \;=\; h(a) \cdot h(b).$$

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

1. $h_1(w) := 0$ für alle $w \in \Sigma^*$.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

1. $h_1(w) := 0$ für alle $w \in \Sigma^*$.
2. $h_2(w) := 1$ für alle $w \in \Sigma^*$ ist hingegen *kein* Homomorphismus.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

1. $h_1(w) := 0$ für alle $w \in \Sigma^*$.
2. $h_2(w) := 1$ für alle $w \in \Sigma^*$ ist hingegen *kein* Homomorphismus.
3. $h_3(w) := \begin{cases} 0 & \text{wenn } |w| \text{ gerade ist} \\ 1 & \text{wenn } |w| \text{ ungerade ist} \end{cases}$

   ist ein Homomorphismus.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Monoide

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

1. $h_1(w) := 0$ für alle $w \in \Sigma^*$.
2. $h_2(w) := 1$ für alle $w \in \Sigma^*$ ist hingegen *kein* Homomorphismus.
3. $h_3(w) := \begin{cases} 0 & \text{wenn } |w| \text{ gerade ist} \\ 1 & \text{wenn } |w| \text{ ungerade ist} \end{cases}$

   ist ein Homomorphismus.

   Da
   $$h(a_1 a_2 \dots a_n) = h(a_1) \oplus h(a_2) \oplus \dots \oplus h(a_n),$$
   reicht es aus, die Werte $h(\epsilon), h(a)$ und $h(b)$ anzugeben.

   Also $h_3(\epsilon) := 0 \quad h_3(a) := 1 \quad h_3(b) := 1$.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide

$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Homomorphismen

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

$$h_3(w) := \begin{cases} 0 & \text{wenn } |w| \text{ gerade ist} \\ 1 & \text{wenn } |w| \text{ ungerade ist} \end{cases}$$

ist ein Homomorphismus.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Beispiel für Homomorphismen

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

$$h_3(w) := \begin{cases} 0 & \text{wenn } |w| \text{ gerade ist} \\ 1 & \text{wenn } |w| \text{ ungerade ist} \end{cases}$$

ist ein Homomorphismus.

Betrachten wir einmal die Menge

$$h_3^{-1}(1) := \{w \in \Sigma^* : h_3(w) = 1\}.$$

Dann ist also $h_3^{-1}(1) \hat{=} \Sigma \cdot (\Sigma \cdot \Sigma)^*$ die Menge aller Wörter ungerader Länge.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$$h(a \circ b) = h(a) \cdot h(b).$$

Noch ein Beispiel für Homomorphismen

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$h(a \circ b) \;=\; h(a) \cdot h(b)$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

Betrachte $h_4 : \Sigma^* \to \{0, 1\}$ spezifiziert durch

$$h_4(\epsilon) := 0 \quad h_4(a) := 0 \quad h_4(b) := 1$$

Frage. Wie sieht die Menge $h_4^{-1}(1)$ aus?

$h_4^{-1}(1) = \{w \in \Sigma^* : h_4(w) = 1\}$

$w = a_1 \dots a_n$ $\quad$ $abbaba$

$h_4(w) = h_4(a_1 \dots a_n) = h_4(a_1) \oplus h_4(a_2) \oplus \dots \oplus h_4(a_n)$

$\cancel{h_4(a)} \oplus h_4(b) \oplus h_4(b) \oplus \cancel{h_4(a)} \oplus h_4(b) \oplus \cancel{h_4(a)}$

$a_i = a \to h_4(a_i) = 0$

Noch ein Beispiel für Homomorphismen

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

Betrachte $h_4 : \Sigma^* \to \{0, 1\}$ spezifiziert durch

$$h_4(\epsilon) := 0 \quad h_4(a) := 0 \quad h_4(b) := 1$$

Frage. Wie sieht die Menge $h_4^{-1}(1)$ aus?

Antwort. $h_4(w) = 1$ gdw. w eine ungerade Anzahl an bs enthält.

$$h_4^{-1}(1) \quad \hat{=} \quad a^* b(a^* ba^* b)^* a^*$$

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$h(a \circ b) = h(a) \cdot h(b)$.

1

Noch ein Beispiel für Homomorphismen

Beispiel. Sei $\Sigma := \{a, b\}$ ein Alphabet und $\mathcal{S} := (\Sigma^*, \cdot)$ Monoid mit $\cdot$ als *Konkatenation* und neutralem Element ϵ.

Sei $M := \{0, 1\}$ und $\mathcal{M} := (M, \oplus)$, wobei $a \oplus x := a + x \mod 2$.

Homomorphismen.
$\mathcal{N} = (N, \circ)$, $\mathcal{M} = (M, \cdot)$ Monoide
$h : N \to M$ *Homomorphismus*:
für alle $a, b \in N$ gilt:
$h(a \circ b) \;=\; h(a) \cdot h(b)$.

Homomorphismen h von $\mathcal{S}$ nach $\mathcal{M}$.

Betrachte $h_4 : \Sigma^* \to \{0, 1\}$ spezifiziert durch

$$h_4(\epsilon) := 0 \quad h_4(a) := 0 \quad h_4(b) := 1$$

Frage. Wie sieht die Menge $h_4^{-1}(1)$ aus?

Antwort. $h_4(w) = 1$ gdw. w eine ungerade Anzahl an bs enthält.

$$h_4^{-1}(w) \qquad \hat{=} \qquad a^* b (a^* b a^* b)^* a^*$$

Beobachtung. Ein Homomorphismus h von $(\Sigma^*, \cdot)$ nach $\mathcal{M}$ definiert zusammen mit einer Teilmenge $F \subseteq M$ eine Sprache $h^{-1}(F) := \bigcup_{a \in F} h^{-1}(a)$. $\subseteq \Sigma^*$

Monoid erkennbare Sprachen

Definition. Sei Σ ein Alphabet.

Sei nun $\mathcal{M} := (M, \circ)$ ein Monoid mit zweistelligem Operator $\circ$.

Eine Sprache $L \subseteq \Sigma^*$ wird *durch $\mathcal{M}$ erkannt*, wenn es

- einen Homomorphismus h von $(\Sigma^*, \cdot)$ nach $\mathcal{M}$ und eine
- Menge $F \subseteq M$ gibt,

so dass für alle $w \in \Sigma^*$ gilt:

$$w \in L \qquad \text{gdw.} \qquad h(w) \in F.$$

$L = h^{-1}(F)$

Monoid erkennbare Sprachen

Definition. Sei Σ ein Alphabet.

Sei nun $\mathcal{M} := (M, \circ)$ ein Monoid mit zweistelligem Operator $\circ$.

Eine Sprache $L \subseteq \Sigma^*$ wird *durch $\mathcal{M}$ erkannt*, wenn es

- einen Homomorphismus h von $(\Sigma^*, \cdot)$ nach $\mathcal{M}$ und eine
- Menge $F \subseteq M$ gibt,

so dass für alle $w \in \Sigma^*$ gilt:

$$w \in L \qquad \text{gdw.} \qquad h(w) \in F.$$

Satz. *Sei Σ ein (endl.) Alphabet. Eine Sprache $L \subseteq \Sigma^*$ ist ein genau dann regulär, wenn L von einem endlichen Monoid erkannt wird.*

12.4 Kongruenzrelationen, Monoide und minimale Automaten

Kongruenzrelationen

Definition. Sei $(M, \circ)$ ein Monoid und $\sim$ eine Äquivalenzrelation auf M.

1. Die Relation $\sim$ heißt *verträglich* mit der Monoidoperation $\circ$, wenn für alle $a, a', b, b' \in M$ gilt:

   Wenn $a \sim b$ und $a' \sim b'$, dann auch $a \circ a' \sim b \circ b'$.

$b \sim b'$

$a \circ b \sim a \circ b'$

$b \circ a \sim b' \circ a$

2. Eine *Kongruenzrelation* $\sim$ auf M ist eine Äquivalenzrelation auf M, die mit $\circ$ verträglich ist.

Kongruenzrelationen

Definition. Sei $(M, \circ)$ ein Monoid und $\sim$ eine Äquivalenzrelation auf M.

1. Die Relation $\sim$ heißt *verträglich* mit der Monoidoperation $\circ$, wenn für alle $a, a', b, b' \in M$ gilt:

   Wenn $a \sim b$ und $a' \sim b'$, dann auch $a \circ a' \sim b \circ b'$.

2. Eine *Kongruenzrelation* $\sim$ auf M ist eine Äquivalenzrelation auf M, die mit $\circ$ verträglich ist.

Beispiel. Sei Σ ein Alphabet und $\sim$ die Relation auf Σ^* definiert durch:

$$w \sim w' \quad \text{gdw.} \quad |w| \mod 2 = |w'| \mod 2.$$

$\sim$ ist Kongruenzrelation auf $(\Sigma^*, \cdot)$.

Quotientenstrukturen

Definition.

Sei $\mathcal{M} := (M, \circ)$ ein Monoid und $\sim$ eine Kongruenzrelation auf M.

1. Für $a \in M$ bezeichnen wir die Äquivalenzklasse

$$\{b \in M : a \sim b\} \text{ mit } [a]_\sim.$$

2. Die *Quotientenmenge* von M und $\sim$ ist die Menge

$$M_{/\sim} := \{[a]_\sim : a \in M\}.$$

3. Der *Quotientenmonoid* ist der Monoid $\mathcal{M}_{/\sim} := (M_{/\sim}, \circ_\sim)$, wobei $[a]_{/\sim} \circ_\sim [b]_{/\sim} := [a \circ b]_{/\sim}$.

Oft werden auch die Begriffe *Faktormenge* und *Faktormonoid* verwendet.

Quotientenstrukturen

Definition.

Sei $\mathcal{M} := (M, \circ)$ ein Monoid und $\sim$ eine Kongruenzrelation auf M.

1. Die *Quotientenmenge* von M und $\sim$ ist die Menge $M_{/\sim} := \{[a]_\sim : a \in M\}$.
2. Der *Quotientenmonoid* ist der Monoid $\mathcal{M}_{/\sim} := (M_{/\sim}, \circ_\sim)$, wobei $[a]_{/\sim} \circ [b]_{/\sim} := [a \circ b]_{/\sim}$.

Beispiel (Fort.). Kongruenzrelation $\sim$ auf $(\Sigma^*, \cdot)$definiert durch:

$$w \sim w' \quad \text{gdw.} \quad |w| \mod 2 = |w'| \mod 2.$$

Äquivalenzklassen: $[a]_\sim$ und $[aa]_\sim$.

Dann ist $(\Sigma^*, \cdot)_{/\sim} := \big(\{[a]_\sim, [aa]_\sim\}, \cdot_\sim\big)$, mit

$\cdot_\sim$	$[a]_\sim$	$[aa]_\sim$
$[a]_\sim$	$[aa]_\sim$	$[a]_\sim$
$[aa]_\sim$	$[a] \sim$	$[aa]_\sim$

Quotientenstrukturen

Definition.

Sei $\mathcal{M} := (M, \circ)$ ein Monoid und $\sim$ eine Kongruenzrelation auf M.

1. Die *Quotientenmenge* von M und $\sim$ ist die Menge $M_{/\sim} := \{[a]_\sim : a \in M\}$.
2. Der *Quotientenmonoid* ist der Monoid $\mathcal{M}_{/\sim} := (M_{/\sim}, \circ_\sim)$,
   wobei $[a]_{/\sim} \circ [b]_{/\sim} := [a \circ b]_{/\sim}$.

Beispiel (Fort.). Kongruenzrelation $\sim$ auf $(\Sigma^*, \cdot)$ definiert durch:

$$w \sim w' \quad \text{gdw.} \quad |w| \mod 2 = |w'| \mod 2.$$

Äquivalenzklassen: $[a]_\sim$ und $[aa]_\sim$.

Dann ist $(\Sigma^*, \cdot)_{/\sim} := \Big(\{[a]_\sim, [aa]_\sim\}, \cdot_\sim\Big)$, mit

$\cdot_\sim$	$[a]_\sim$	$[aa]_\sim$
$[a]_\sim$	$[aa]_\sim$	$[a]_\sim$
$[aa]_\sim$	$[a] \sim$	$[aa]_\sim$

Vergleiche.
$\mathcal{M}' := (\{0, 1\}, \oplus)$ mit
$a \oplus x := a + x \mod 2$

Quotientenstrukturen

Definition.

Sei $\mathcal{M} := (M, \circ)$ ein Monoid und $\sim$ eine Kongruenzrelation auf M.

1. Für $a \in M$ bezeichnen wir die Äquivalenzklasse

   $$\{b \in M : a \sim b\} \text{ mit } [a]_\sim.$$

2. Die *Quotientenmenge* von M und $\sim$ ist die Menge

   $$M_{/\sim} := \{[a]_\sim : a \in M\}.$$

3. Der *Quotientenmonoid* ist der Monoid $\mathcal{M}_{/\sim} := (M_{/\sim}, \circ_\sim)$, wobei $[a]_{/\sim} \circ [b]_{/\sim} := [a \circ b]_{/\sim}$.

Oft werden auch *Faktormenge* und *Faktormonoid* verwendet.

Lemma. *Für alle Monoide $\mathcal{M} := (M, \circ)$ und Kongruenzrelationen $\sim$ auf M ist $\mathcal{M}_{/\sim}$ ein Monoid.*

Das syntaktische Monoid

Definition (Syntaktische Kongruenz $\cong_L$.).

Sei Σ ein Alphabet und $L \subseteq \Sigma^*$.

Wir definieren eine Relation $\cong_L \subseteq \Sigma^* \times \Sigma^*$ wie folgt:

Für $w, w' \in \Sigma^*$ gilt

$w \cong_L w'$ gdw. für alle $x, y \in \Sigma^*$ gilt:

$$xwy \in L \quad \text{gdw.} \quad xw'y \in L.$$

Behauptung. $\cong_L$ ist Kongruenzrelation auf $(\Sigma^*, \cdot)$, d.h. es gilt:

Wenn $u \cong_L v$ und $u' \cong_L v'$, dann $u \cdot u' \cong_L v \cdot v'$.

Das syntaktische Monoid

Definition (Syntaktische Kongruenz $\cong_L$.).
Sei Σ ein Alphabet und $L \subseteq \Sigma^*$.
Wir definieren eine Relation $\cong_L \subseteq \Sigma^* \times \Sigma^*$ wie folgt:
Für $w, w' \in \Sigma^*$ gilt
$w \cong_L w'$ gdw. für alle $x, y \in \Sigma^*$ gilt:

$$xwy \in L \quad \text{gdw.} \quad xw'y \in L.$$

Behauptung. $\cong_L$ ist Kongruenzrelation auf $(\Sigma^*, \cdot)$, d.h. es gilt:

Wenn $u \cong_L v$ und $u' \cong_L v'$, dann $u \cdot u' \cong_L v \cdot v'$.

Folgerung. $(\Sigma^* / \cong_L, \cdot)$ ist ein Monoid, das *syntaktische Monoid*.

$\Sigma^* / \cong_L$

Beispiel

Beispiel. Sei $\Sigma := \{a, b\}$ und $L := \{w \in \Sigma^* : |w| \text{ ist gerade }\}$.

Dann gilt für $w, w' \in \Sigma^*$

$$w \cong_L w' \quad \text{gdw.} \quad \text{für alle } x, y \in \Sigma^* \text{ gilt:}$$

$$xwy \in L \qquad \text{gdw.} \qquad xw'y \in L.$$

Also gilt $w \cong_L w'$ gdw. $|w| \mod 2 = |w'| \mod 2$.

Beispiel

Beispiel. Sei $\Sigma := \{a, b\}$ und $L := \{w \in \Sigma^* : |w| \text{ ist gerade } \}$.

Dann gilt für $w, w' \in \Sigma^*$

$w \cong_L w'$ gdw. für alle $x, y \in \Sigma^*$ gilt:

$$xwy \in L \quad \text{gdw.} \quad xw'y \in L.$$

Also gilt $w \cong_L w'$ gdw. $|w| \mod 2 = |w'| \mod 2$.

Dann ist $(\Sigma^*, \cdot)_{/\cong_L} := \left(\{[a]_{\cong_L}, [aa]_{\cong_L}\}, \cdot_{\cong_L}\right)$, mit

$\cdot_{\cong_L}$	$[a]_{\cong_L}$	$[aa]_{\cong_L}$
$[a]_{\cong_L}$	$[aa]_{\cong_L}$	$[a]_{\cong_L}$
$[aa]_{\cong_L}$	$[a]_{\cong_L}$	$[aa]_{\cong_L}$

Das syntaktische Monoid

Definition (Syntaktische Kongruenz $\cong_L$).

Sei Σ ein Alphabet und $L \subseteq \Sigma^*$.

Wir definieren eine Relation $\cong_L \subseteq \Sigma^* \times \Sigma^*$ wie folgt:

Für $w, w' \in \Sigma^*$ gilt

$w \cong_L w'$ gdw. für alle $x, y \in \Sigma^*$ gilt:

$$xwy \in L \quad \text{gdw.} \quad xw'y \in L.$$

Folgerung. $(\Sigma^* / \cong_L, \cdot)$ ist ein Monoid, das *syntaktische Monoid*.

Definition (Syntaktischer Homomorphismus von L).

Der *syntaktische Homomorphismus von* L ist die Abbildung h_L mit

$$h_L(x) := [x]_{\cong_L}$$

Beobachtung. Sei nun $F_L := \{[w]_{\cong_L} : w \in L\}$.

Dann wird L von $(\Sigma^* / \cong_L, \cdot)$ durch h_L und F_L erkannt.

Monoide und Automaten

Von Automaten zu Monoiden. Sei $\mathcal{A} := (Q, \Sigma, \delta, q_0, F)$ ein deterministischer endlicher Automat und sei $L = L(\mathcal{A})$.

Wir definieren $\delta^* : Q \times \Sigma^* \to Q$ induktiv durch

- $\delta^*(q, \epsilon) := q$ und
- $\delta^*(q, wa) := \delta(\delta^*(q, w), a)$.

$\delta^*(q, w)$: Zustand des Aut $\mathcal{A}$ wenn er von q ausgehend w liest.

Monoide und Automaten

Von Automaten zu Monoiden. Sei $\mathcal{A} := (Q, \Sigma, \delta, q_0, F)$ ein deterministischer endlicher Automat und sei $L = L(\mathcal{A})$.

Wir definieren $\delta^* : Q \times \Sigma^* \to Q$ induktiv durch

- $\delta^*(q, \epsilon) := q$ und
- $\delta^*(q, wa) := \delta(\delta^*(q, w), a)$.

Jedes Wort $w \in \Sigma^*$ induziert eine Abbildung $w_{\mathcal{A}} : Q \to Q$:

$$w_{\mathcal{A}}(q) := \delta^*(q, w) \quad \text{für alle } q \in Q.$$

Sei nun $A := \{w_{\mathcal{A}} : w \in \Sigma^*\}$ und $\circ$ die Operation auf A mit

$$(f \circ g)(q) = g(f(q)) \qquad \text{für alle } q \in Q \text{ und } f, g \in A.$$

Monoide und Automaten

Von Automaten zu Monoiden. Sei $\mathcal{A} := (Q, \Sigma, \delta, q_0, F)$ ein deterministischer endlicher Automat und sei $L = L(\mathcal{A})$.

Wir definieren $\delta^* : Q \times \Sigma^* \to Q$ induktiv durch

- $\delta^*(q, \epsilon) := q$ und
- $\delta^*(q, wa) := \delta\big(\delta^*(q, w), a\big)$.

Jedes Wort $w \in \Sigma^*$ induziert eine Abbildung $w_{\mathcal{A}} : Q \to Q$:

$$w_{\mathcal{A}}(q) := \delta^*(q, w) \quad \text{für alle } q \in Q.$$

Sei nun $A := \{w_{\mathcal{A}} : w \in \Sigma^*\}$ und $\circ$ die Operation auf A mit

$$(f \circ g)(q) = g(f(q)) \qquad \text{für alle } q \in Q \text{ und } f, g \in A.$$

Transitionsmonoid. $\circ$ ist assoziativ und die Abbildung $\epsilon_{\mathcal{A}}$ ist ein neutrales Element von $(A, \circ)$.

Also ist $(A, \circ)$ ein Monoid, das sogenannte *Transitionsmonoid*.

Das syntaktische Monoid

Satz. *Sei $L \subseteq \Sigma^*$ eine reguläre Sprache und sei $\mathcal{A}_L$ der minimale deterministische Automat mit $L(\mathcal{A}) = L$.*

Dann ist $(\Sigma^* / \cong_L, \cdot)$ isomorph zum Transitionsmonoid von $\mathcal{A}_L$.

Das syntaktische Monoid

Satz. *Sei $L \subseteq \Sigma^*$ eine reguläre Sprache und sei $\mathcal{A}_L$ der minimale deterministische Automat mit $L(\mathcal{A}) = L$.*

Dann ist $(\Sigma^* / \cong_L, \cdot)$ isomorph zum Transitionsmonoid von $\mathcal{A}_L$.

Theorem. Sei Σ ein (endl.) Alphabet. Eine Sprache $L \subseteq \Sigma^*$ ist ein genau dann regulär, wenn L von einem endlichen Monoid erkannt wird.

Das syntaktische Monoid

Satz. *Sei $L \subseteq \Sigma^*$ eine reguläre Sprache und sei $\mathcal{A}_L$ der minimale deterministische Automat mit $L(\mathcal{A}) = L$.*

Dann ist $(\Sigma^* / \cong_L, \cdot)$ isomorph zum Transitionsmonoid von $\mathcal{A}_L$.

Theorem. Sei Σ ein (endl.) Alphabet. Eine Sprache $L \subseteq \Sigma^*$ ist ein genau dann regulär, wenn L von einem endlichen Monoid erkannt wird.

Vergleiche mit ForSA.

Definition. Sei Σ ein Alphabet und sei $L \subseteq \Sigma^*$ eine Sprache. Für $w, w' \in \Sigma^*$ definieren wir $w \sim_L w'$, wenn für alle $x \in \Sigma^*$ gilt:

$$w \cdot x \in L \qquad \text{gdw.} \qquad w' \cdot x \in L.$$

Theorem (Myhill, Nerode). Sei $L \subseteq \Sigma^*$ eine Sprache.

L ist genau dann regulär, wenn der Index, d.h. die Anzahl der Äquivalenzklassen, von $\sim_L$ endlich ist.

Automaten, Sprachen, Monoide

Sichtweisen auf reguläre Sprachen. $L \subseteq \Sigma^*$ ist regulär, wenn

L wird durch einen Computer ohne eigenen Hauptspeicher akzeptiert.

L kann durch einen regulären Ausdruck definiert werden

L wird durch einen endlichen Monoid erkannt