Diskrete Strukturen

WiSe 2012/13 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

15. Februar 2013

Diskrete Strukturen Gesamtübersicht

- Organisatorisches und Einführung
- Mengenlehre
- Relationen und Funktionen
- Kombinatorik: Die Kunst des Zählens
- Diskrete Stochastik
- Graphen
- Grundbegriffe (algebraischer) Strukturen

Bemerkungen zu algebraischen Strukturen

Def.: Unter dem *Typ einer Struktur* versteht man ein Tripel $(\mathcal{F}, \mathcal{R}, \sigma)$, wobei gelten soll: $\mathcal{F} \cap \mathcal{R} = \emptyset$.
$\mathcal{F}$ ist die Menge der *Funktionensymbole*,
$\mathcal{R}$ ist die Menge der *Relationensymbole*,
$\sigma : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$ liefert die *Stelligkeit* zu dem betreffenden Symbol.

Der Typ einer Struktur ist ein rein syntaktisches Objekt.
Wenn es auf die Namen der Symbole nicht ankommt, erwähnt man oft auch nur den Stelligkeitstyp.

Informatisch gesprochen beschreibt ein Typ das Interface zwischen Strukturen.

Operationen und Relationen (spezialisiert)

Es sei $A \neq \emptyset$ eine Menge und $n \in \mathbb{N}$.
Eine Abbildung $A^n \to A$ heißt *n-stellige Operation auf A*.
(Hier ist $A^n = A \times \cdots \times A$ das $(n-1)$-fache kartesische Produkt.)
Nullstellige Operationen heißen auch *Konstanten*.
$\mathrm{Op}_n(A)$ sei die Menge der n-stelligen Operationen auf A, d.h., $\mathrm{Op}_n(A) = A^{A^n}$.
$\mathrm{Rel}_n(A)$ sei die Menge der n-stelligen Relationen über A, d.h., $\mathrm{Rel}_n(A) = 2^{A^n}$.
Schließlich setzen wir:
$\mathrm{Op}(A) = \bigcup_{n=0}^{\infty} \mathrm{Op}_n(A)$ und $\mathrm{Rel}(A) = \bigcup_{n=1}^{\infty} \mathrm{Rel}_n(A)$.

Strukturen und Algebren

Def.: Eine *Struktur* vom Typ $(\mathcal{F}, \mathcal{R}, \sigma)$ ist ein Tripel $\mathbb{S} = (\mathrm{A}, \mathrm{F}, \mathrm{R})$, $\mathrm{A} \neq \emptyset$,
mit $\mathrm{F} = \{\mathrm{f}_{\mathbb{S}} \mid \mathrm{f} \in \mathcal{F}\}$,
wobei jedem $\mathrm{f} \in \mathcal{F}$ genau eine Operation $\mathrm{f}_{\mathbb{S}} \in \mathrm{Op}_{\sigma(\mathrm{f})}(\mathrm{A})$ zugeordnet ist;
entsprechend: $\mathrm{R} = \{\mathrm{r}_{\mathbb{S}} \mid \mathrm{r} \in \mathcal{R}\}$,
wobei jedem $\mathrm{r} \in \mathcal{R}$ genau eine Relation $\mathrm{r}_{\mathbb{S}} \in \mathrm{Rel}_{\sigma(\mathrm{r})}(\mathrm{A})$ zugeordnet ist.
Gibt es gar keine Relationen, so spricht man auch von einer *Algebra*.
Gibt es umgekehrt keine Operationen, so spricht man von einer *relationalen Struktur*.
Natürlich kann man dann auf die Angabe “leerer Komponenten” verzichten.

Strukturen bzw. Algebren liefern die semantische Ebene.
Diese Unterschiede werden später noch klar(er) werden.

Bemerkungen

Die meisten von uns (bereits oder zukünftig) untersuchten Strukturen haben eine oder zwei Operationen oder eine Relation.
Wichtig sind dabei besondere Eigenschaften von Strukturen, denen wir im Folgenden Namen geben wollen.
Eine Algebra mit nur einer zweistelligen Operation (also vom Stelligkeitstyp 2) heißt auch ein *Gruppoid*.
Zweistellige Operationen notieren wir auch meist wie gewohnt in Infix-Notation.
Eine zweistellige Operation $\circ \in \mathrm{Rel}_2(A)$ ist *assoziativ* gdw.

$$\forall x, y, z \in A : ((x \circ y) \circ z) = (x \circ (y \circ z)).$$

Ein Gruppoid heißt *Halbgruppe*, wenn seine (einzige) Operation assoziativ ist.

Beispiele

- $(\mathbb{N}, +)$ ist eine Halbgruppe.
  Achtung: Bei dieser üblichen Notation wird der Unterschied zwischen Syntax und Semantik leicht verwischt: $+$ ist ein Funktionensymbol mit Stelligkeit 2, deren beigeordneter Semantik gerade die übliche Addition entspricht. Bei nur wenigen Operationen wird überdies auf die Mengenschreibweise der Operationen verzichtet.
- $(\mathbb{N}, \cdot)$ ist eine Halbgruppe.
- $(\mathbb{N}, \max)$ ist eine Halbgruppe.
- $(\mathbb{N}, \min)$ ist eine Halbgruppe.
- Mit Maximum- bzw. Minimumbildung kann man auch leicht Operationen höherer Stelligkeit definieren.

Mehr Beispiele

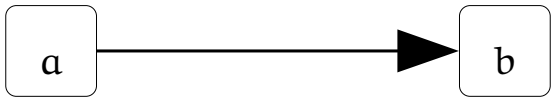
- Jeder gerichtete Graph ist eine relationale Struktur (mit genau einer Relation, der Adjazenz).
- Speziellere relationale Strukturen kann man wieder mit speziellen Eigenschaften definieren, z.B. Äquivalenzrelationen.
- Ist $G = (V, E)$ ein Graph, so kann man ihm ein Gruppoid $\mathbb{G}_G = (V, \circ_E)$ zuordnen vermöge

$$x \circ_E y = \begin{cases} y, & \text{falls } (x, y) \in E \\ x, & \text{falls } (x, y) \notin E \end{cases}$$

Verknüpfungstafeln

Gruppoide lassen sich auch gut mithilfe von *Verknüpfungstafeln* angeben, sofern die betreffende Grundmenge endlich ist.

$G = (V, E)$ ist gegeben durch:
$V = \{a, b\}$, $E = \{(a, b)\}$, oder im Bilde:



Zu $\mathbb{G}_G$ gehörende Verknüpfungstafel:

$\circ_E$	a	b
a	a	b
b	b	b

Erinnerung:

$$x \circ_E y = \begin{cases} y, & \text{falls } (x, y) \in E \\ x, & \text{falls } (x, y) \notin E \end{cases}$$

Unterstrukturen

Es sei $\tau = (\mathcal{F}, \mathcal{R}, \sigma)$ der Typ einer Struktur.
Es seien $\mathbb{S} = (A, F, R)$ und $\mathbb{S}' = (A', F', R')$ Strukturen vom Typ τ.
$\mathbb{S}'$ heißt *Unterstruktur* von $\mathbb{S}$, falls gilt:

- $A' \subseteq A$.
- Ist $f \in \mathcal{F}$, so gilt für alle $a_1, \ldots, a_{\sigma(f)} \in A'$: $f_{\mathbb{S}}(a_1, \ldots, a_{\sigma(f)}) = f_{\mathbb{S}'}(a_1, \ldots, a_{\sigma(f)})$.
- Ist $r \in \mathbb{R}$, so gilt: $r_{\mathbb{S}'} \subseteq r_{\mathbb{S}}\big|_{(A')^{\sigma(r)}}$, wobei letzteres die Restriktion von $r_{\mathbb{S}}$ auf das $(\sigma(r) - 1)$-fache Mengenprodukt von A' meint.

Beispielsweise besitzt $\mathbb{G}_G$ (vorige Folie) zwei echte Unterstrukturen.

Unterstrukturen

heißen, wenn keine Relationen vorkommen, auch *Unteralgebren*.

Haben diese Algebren spezielle Eigenschaften, so werden auch die Unterstrukturen entsprechend angesprochen.

$(\{\mathfrak{a}\}, (\mathfrak{a}, \mathfrak{a}) \mapsto \mathfrak{a})$ kann man also als Unterhalbgruppe von $\mathbb{G}_{\mathrm{G}}$ ansprechen.

Zur Angabe von Unteralgebren genügt im Grunde die Angabe der "neuen Grundmenge" $\mathcal{A}' \neq \emptyset$.

Zum Nachweis der Unteralgebraeigenschaft muss man noch nachrechnen, dass $\mathcal{A}'$ bzgl. aller Operationen abgeschlossen ist, also wirklich eine Algebra gebildet werden kann.

Wir sagen auch: $\mathcal{A}'$ *beschreibt* eine Unteralgebra.

Aber auch der früher betrachtete Begriff eines Untergraphen ist eine Spezialisierung des soeben eingeführten Unterstrukturbegriffes.

Ein ausführlicheres Beispiel

Auf der Grundmenge $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ betrachte folgende Addition:

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

Die Einträge ergeben sich auch dadurch, dass man zwei Zahlen “wie üblich” addiert, das Ergebnis durch 6 teilt und dann den dabei gelassenen Rest einträgt.

Mühsames Nachrechnen liefert:
$(\mathbb{Z}_6, +)$ ist eine Halbgruppe.
Unterhalbgruppen sind beschrieben durch $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$.
Für die letzte Menge ergibt sich folgende Verknüpfungstafel:

$+$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Erzeugendensysteme

Satz: Es sei (A, F) eine Algebra vom Typ $(\mathcal{F}, \sigma)$.
Ist I eine beliebige Indexmenge und sind (A_i, F_i) für $i \in I$ Unteralgebren von (A, F), so beschreibt $\bigcap_{i\in I} A_i$ eine Unteralgebra von (A, F).
Beweis: Betrachte $f \in \mathcal{F}$ mit Stelligkeit $n = \sigma(f)$. Es seien $a_1, \ldots, a_n \in \bigcap_{i\in I} A_i$.
Für jedes A_i ist nun $a_j \in A_i$, mithin $f(a_1, \ldots, a_n) \in A_i$. Also gilt: $f(a_1, \ldots, a_n) \in \bigcap_{i\in I} A_i$. □

Im Folgenden sei $\mathrm{Sub}(A)$ die Menge aller Unteralgebren von (A, F).
Zwar liefert nicht jede Teilmenge A' von A eine Algebra, aber man kann A' als *Erzeugendensystem* betrachten von der Algebra, die beschrieben ist durch $\bigcap_{B\in\mathrm{Sub}(A),B\supseteq A'} B$. Diese Algebra notieren wir auch $\langle A'\rangle$.

Im Beispiel $(\mathbb{Z}_6, +)$ gilt: $\langle\{0\}\rangle = (\{0\}, +)$, $\langle\{2\}\rangle = (\{0, 2, 4\}, +)$, $\langle\{3\}\rangle = (\{0, 3\}, +)$, $\langle\{1\}\rangle = \langle\{2, 3\}\rangle = (\mathbb{Z}_6, +)$.
Im Beispiel $(\mathbb{N}, +)$ gilt: $\langle\{1\}\rangle = (\{n > 0 \mid n \in \mathbb{N}\}, +)$, $\langle\{2, 5\}\rangle = (\mathbb{N} \setminus \{0, 1, 3\}, +)$.

Eigenschaften zweistelliger Operationen

Oben hatten wir bereits die Assoziativität kennengelernt.
Es sei $\circ$ eine zweistellige Operation auf A, also $\circ : A \times A \to A$.

Def.: $\circ$ heißt *kommutativ* gdw. $\forall x, y \in A : (x \circ y) = (y \circ x)$.
Def.: $\circ$ heißt *idempotent* gdw. $\forall x \in A : x \circ x = x$.

Def.: Eine Konstante $e \in A$ (bei uns eine nullstellige Operation) heißt *neutrales Element* von $\circ$ gdw. $\forall x \in A : x \circ e = e \circ x = x$.
Def.: Eine Konstante $\mathfrak{o} \in A$ (bei uns eine nullstellige Operation) heißt *absorbierendes Element* von $\circ$ gdw. $\forall x \in A : x \circ \mathfrak{o} = \mathfrak{o} \circ x = \mathfrak{o}$.

Beispiele

Wir bezeichnen das *kleinste gemeinsame Vielfache* zweier positiver ganzer Zahlen a, b mit $kgV(a, b)$.
Also: $kgV(a, b) = \min\{n \in \mathbb{N} \setminus \{0\} \mid \exists k, \ell \in \mathbb{N} \setminus \{0\} : a \cdot k = b \cdot \ell = n\}$.
Ihren *größten gemeinsamen Teiler* schreiben wir $ggT(a, b)$.

- $(\mathbb{N} \setminus \{0\}, kgV)$ ist eine Halbgruppe, deren Operation kommutativ und idempotent ist. Was müssen wir im Einzelnen nachprüfen?
- 1 ist neutrales Element in obigem Beispiel.
- $(\mathbb{N} \setminus \{0\}, ggT)$ ist eine Halbgruppe, deren Operation kommutativ und idempotent ist.
- 1 ist absorbierendes Element in diesem Beispiel.

Wichtige Algebren

Wie üblich (doch etwas ungenau) werden wir die Operationennamen im Folgenden in den Definitionen der Algebren auflisten und müssen dann nur noch die Stelligkeiten angeben.

Def.: Eine Algebra $(A, \circ, e)$ vom Stelligkeitstyp $(2, 0)$ heißt *Monoid*, falls $(A, \circ)$ eine Halbgruppe ist und e neutrales Element von $\circ$.

Def.: Eine Algebra $(A, \circ)$ vom Stelligkeitstyp (2) heißt *Halbverband*, falls $(A, \circ)$ eine Halbgruppe ist und $\circ$ kommutativ und idempotent ist.

Def.: Eine Algebra $(A, \circ, \mathfrak{o})$ vom Stelligkeitstyp $(2, 0)$ heißt *beschränkter Halbverband*, falls $(A, \circ)$ Halbverband ist und $\mathfrak{o}$ absorbierendes Element von $\circ$ ist.

Lemma: Eine Halbgruppe besitzt höchstens ein neutrales Element.

Beweis: Angenommen, es gibt in $(A, \circ)$ neutrale Elemente e, e'. Dann gilt: $e = e \circ e' = e'$; die erste Gleichheit gilt, weil e' neutrales Element ist, und die zweite, da e neutrales Element ist. $\square$

Ähnlich zeigt man:

Lemma: Eine Halbgruppe besitzt höchstens ein absorbierendes Element.

Beispiele

- $(\mathbb{N} \setminus \{0\}, \mathrm{ggT}, 1)$ ist ein beschränkter Halbverband.
- $(\mathbb{N} \setminus \{0\}, \mathrm{kgV}, 1)$ ist ein kommutatives Monoid.
- $(\mathbb{N}, \cdot, 1)$ ist ein Monoid mit 0 als absorbierendem Element.
- Gleitkomma-Arithmetik gemäß dem IEEE-754 Standard enthält eine "Zahl" NaN (not-a-number), intendiert als Fehlerindikator, die absorbierend bzgl. alle üblichen Zahloperationen ist.
- Es sei M eine Menge.
  Dann ist $(2^M, \cap, \emptyset)$ beschränkter Halbverband, ebenso wie $(2^M, \cup, M)$.

Noch mehr Beispiele

Es sei M eine Menge.
$2^{M \times M}$ bezeichnet dann die Menge der Binärrelationen auf M.
Wir wissen: (1) Das Relationenprodukt ist eine assoziative Operation auf $2^{M \times M}$.
(2) Die Diagonale Δ_M ist neutrales Element.
$\rightsquigarrow (2^{M \times M}, \circ, \Delta_M)$ ist ein Monoid.

Ist dieses Monoid kommutativ? Nein! Beispiel!
Ist es idempotent? Nein! Beispiel!

M^M, die Menge der Abbildungen von M nach M, kann man als Teilmenge von $2^{M \times M}$ begreifen (Funktionen als spezielle Relationen).
Damit wird $(M^M, \circ, \Delta_M)$ Untermonoid von $(2^{M \times M}, \circ, \Delta_M)$.

Bijektionen sind wiederum spezielle Funktionen, und die Komposition von Bijektionen liefert wieder eine Bijektion. So erhalten wir ein Untermonoid von $(M^M, \circ, \Delta_M)$.

Ein abstraktes Beispiel: Das Komplexprodukt

Es sei $\mathbb{M} = (M, \circ, e)$ ein Monoid.
Dann definiere auf 2^M die folgende zweistellige Operation, *Komplexprodukt zu* $\mathbb{M}$ genannt:

$$M_1 \circ M_2 := \{x_1 \circ x_2 \mid x_1 \in M_1, x_2 \in M_2\}$$

Lemma: $2^{\mathbb{M}} := (2^M, \circ, \{e\})$ ist ein Monoid mit absorbierendem Element $\emptyset$.
Beweis zur Übung.
Da nun $2^{\mathbb{M}}$ Monoid, kann man natürlich auch das Monoid $2^{2^{\mathbb{M}}}$ betrachten usf.

Ein abstraktes Beispiel: Funktionenmonoide

Es sei $\mathbb{M} = (M, \Box, e)$ ein Monoid.
Es sei ferner N eine beliebige Menge.
Erweitere nun $\Box$ “punktweise” zu einer Operation auf M^N:
$h := f \Box g$ mit

$$h(n) := f(n) \Box g(n)$$

für alle $n \in N$.

Lemma: $\mathbb{M}^N := (M^N, \Box, \{n \mapsto e\})$ ist ein Monoid.
Dieses werden wir auch als *Funktionenmonoid* ansprechen.
Beweis zur Übung.
Anwendung:
Betrachte das Monoid $\mathrm{REALPLUS} = (\mathbb{R}, +, 0)$.
Vektoren $\vec{x} \in \mathbb{R}^m$ “entsprechen” Abbildungen $\{1, \ldots, m\} \to \mathbb{R}$.
Die im Funktionenmonoid $\mathrm{REALPLUS}^{\{1,\ldots,m\}}$ definierte Addition ist die bekannte Vektoraddition.
Entsprechend kannn man die Addition von Matrizen begreifen.

Vorteile der Abstraktion

- Beweise für abstrakte Objekte gestatten die Konzentration auf das Wesentliche.
- Hat man solch eine “abstrakte Eigenschaft” nachgewiesen, so gilt sie für alle “konkreten Fälle”.
- Beispiel: Da wir wissen, dass es in einer Halbgruppe nur höchstens ein neutrales Element gibt, brauchen wir in $(\mathbb{Z}, +)$ nicht mühsam nach weiteren neutralen Elementen fahnden, wenn wir einmal 0 gefunden haben.
- Beispiel: Dass die Gültigkeit des Assoziativitätsgesetzes “bedeutet”, dass man “Klammern weglassen” kann, lässt sich formal allgemein für Halbgruppen formulieren und mit Induktion beweisen. Es ist also unnötig, dies für jede assoziative Operation einzeln zu tun (so wie wir dies teils früher gemacht haben).
- Beispiel: Komplexprodukte und Funktionenmonoide werden Ihnen immer wieder begegnen.

Halbverbände und Halbordnungen

Def.: Es sei $(A, \sqcup)$ ein Halbverband. Dann ist die Binärrelation $\sqsubseteq \subseteq A \times A$ mit

$$a \sqsubseteq b : \Longleftrightarrow \; a \sqcup b = b$$

die von $\sqcup$ *induzierte Halbordnung*.

Satz: $(A, \sqsubseteq)$ ist eine Halbordnung.

Beweis: Es seien $a, b, c \in A$ beliebig.

$a \sqsubseteq a$, denn $a \sqcup a = a$, da $\sqcup$ idempotent.

Gilt $a \sqsubseteq b$ und $b \sqsubseteq a$, so ist: $b = a \sqcup b = b \sqcup a = a$ aufgrund der Kommutativität von $\sqcup$.

Gilt $a \sqsubseteq b$ und $b \sqsubseteq c$, so ist: $c = b \sqcup c = (a \sqcup b) \sqcup c = a \sqcup (b \sqcup c) = a \sqcup c$, da $\sqcup$ assoziativ. □

Es folgt auch unmittelbar die folgende Monotonie / Verträglichkeit:

Lemma: Sei $(A, \sqcup)$ ein Halbverband mit induzierter Halbordnung $\sqsubseteq$ und $a, b, c \in A$ beliebig. Gilt $a \sqsubseteq b$, so auch $a \sqcup c \sqsubseteq b \sqcup c$.

Beweis: $b \sqcup c = (a \sqcup b) \sqcup c = (a \sqcup b) \sqcup (c \sqcup c) = (a \sqcup c) \sqcup (b \sqcup c)$ aufgrund der Idempotenz, Assoziativität und Kommutativität von $\sqcup$. □

Beispiele

- Die vom Halbverband $(\mathbb{N} \setminus \{0\}, \mathrm{kgV})$ induzierte Halbordnung ist die Teilerrelation $|$.
- Die vom Halbverband $(2^M, \cup)$ induzierte Halbordnung ist die Teilmengenrelation $\subseteq$.
- Die vom Halbverband $(\mathbb{R}, \max)$ induzierte Halbordnung ist $\leq$.

Unmittelbar aus der Def. folgt:
Lemma: Es sei $(A, \sqcup)$ ein Halbverband.
Ist o absorbierendes Element in $(A, \sqcup)$, so ist o in $(A, \sqsubseteq)$ obere Grenze von A.
Ist e neutrales Element in $(A, \sqcup)$, so ist e in $(A, \sqsubseteq)$ untere Grenze von A.

Halbordnungen und Halbverbände

Ist $(M, \sqsubseteq)$ eine Halbordnung, bei der $(*)$ zu zwei Elementen $a, b \in M$ stets eine obere Grenze (Supremum) von $\{a, b\}$ existiert, so definiere

$$a \sqcup b := \sup\{a, b\}$$

Def.: $\sqcup$ ist die von $\sqsubseteq$ *induzierte Supremumsoperation*.

Lemma: Unter der Bedingung $(*)$ ist $(M, \sqsubseteq)$ ein Halbverband.

Die beiden Induktionsbegriffe "passen zusammen":
So ist die von einer Halbverbandsoperation $\sqsubseteq$ induzierte Halbordnung derart, dass sie $(*)$ erfüllt und wiederum eine Supremumsoperation induziert, die mit $\sqsubseteq$ identisch ist.

Terme über Algebren

Def.: Es sei $\mathbb{A} = (A, F)$ eine Algebra vom Typ $(\mathcal{F}, \sigma)$.
Dann sind *Terme über* $\mathbb{A}$ induktiv wie folgt definiert:

1. Jedes $a \in A$ ist ein Term.
2. Sind $t_1, \ldots, t_n$ Terme über $\mathbb{A}$ und ist $f \in \mathcal{F}$ mit $\sigma(f) = n$, so ist $f(t_1, \ldots, t_n)$ ein Term über $\mathbb{A}$.
3. Nichts anderes sind Terme über $\mathbb{A}$.

Wir sammeln alle Terme über $\mathbb{A}$ in der Menge $\mathrm{Term}(\mathbb{A})$.

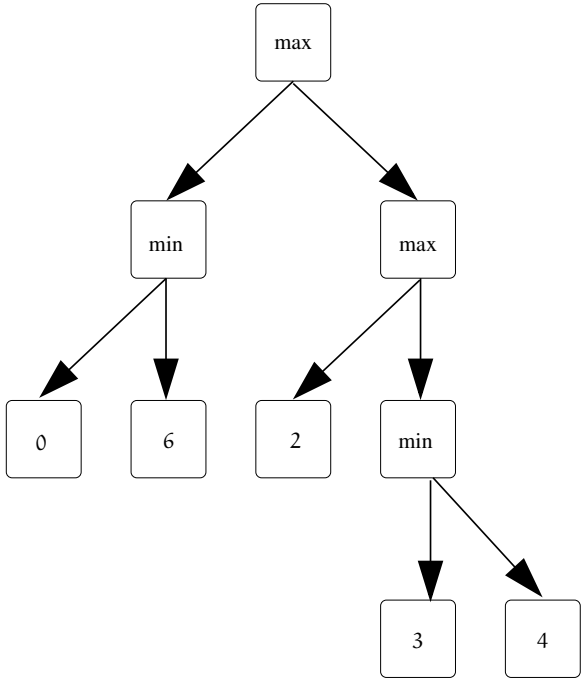
Beachte: Terme sind rein syntaktische Objekte.
Betrachte z.B. die Algebra $\mathbb{A} = (\mathbb{N}, \{\max_{\mathbb{N}}, \min_{\mathbb{N}}\})$ mit zwei zweistelligen Operationen.
Dann ist $\max(\min(0, 6), \max(2, \min(3, 4)))$ ein Term über $\mathbb{A}$.

Terme und Bäume

Einem Term über einer Algebra kann man durch einen knotenbeschrifteten gerichteten geordneten Baum darstellen.
Umgekehrt entsprechen einem knotenbeschrifteten gerichteten geordneten Baum Terme über einer geeignet definierten Algebra.
Wie wir sehen, kann man Berechnungen in Algebren über Terme definieren.
Dies erklärt die Bedeutung dieser Art von Bäumen z.B. im Compilerbau.

Im Beispiel:

$\max(\min(0, 6), \max(2, \min(3, 4)))$:



Zur Auswertung von Termen

Def.: Es sei $\mathbb{A} = (A, F)$ eine Algebra vom Typ $(\mathcal{F}, \sigma)$.
Wir definieren die *Auswertefunktion* $eval : \mathrm{Term}(\mathbb{A}) \to A$ induktiv wie folgt:

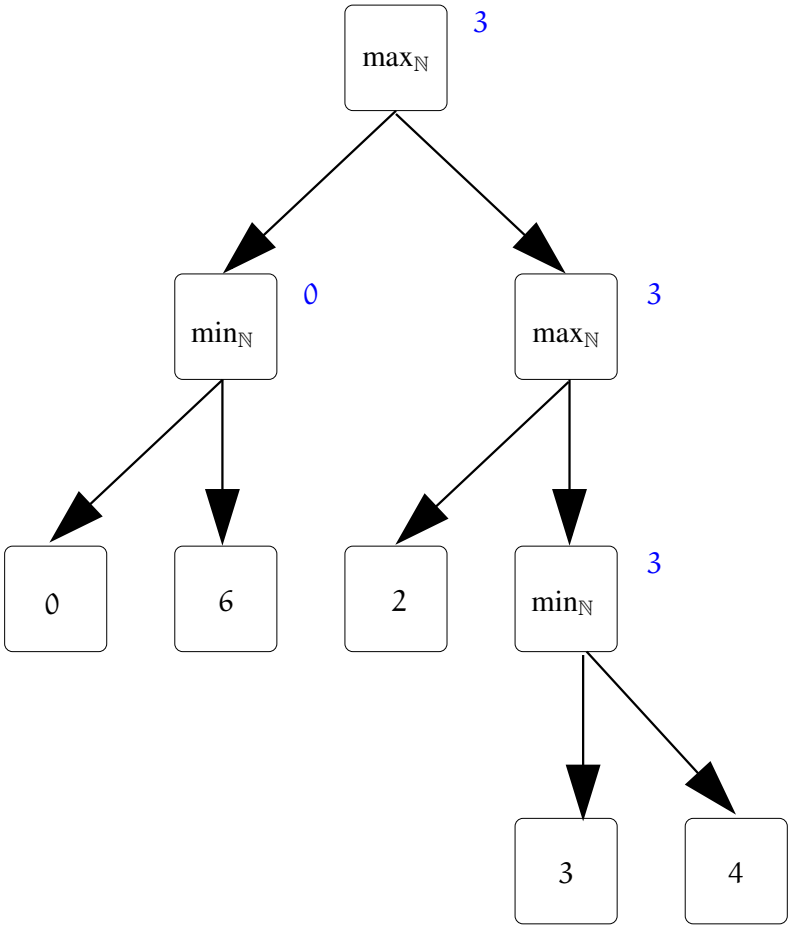
1. Für $a \in A$ sei $eval(a) := a$.
2. Sind $t_1, \ldots, t_n$ Terme über $\mathbb{A}$ und ist $f \in \mathcal{F}$ mit $\sigma(f) = n$, so ist

$$eval(f(t_1, \ldots, t_n)) := f_{\mathbb{A}}(eval(t_1), \ldots, eval(t_n)).$$

Zur Auswertung von Termen: Unser Beispiel

$$
\begin{aligned}
eval(\max(\min(0,6),\max(2,\min(3,4)) &= \max_{\mathbb{N}}(eval(\min(0,6)), eval(\max(2,\min(3,4)))) \\
&= \max_{\mathbb{N}}(\min_{\mathbb{N}}(eval(0), eval(6)), \max_{\mathbb{N}}(eval(2), eval(\min(3,4)))) \\
&= \max_{\mathbb{N}}(\min_{\mathbb{N}}(0,6), \max_{\mathbb{N}}(2, \min_{\mathbb{N}}(eval(3), eval(4)))) \\
&= \max_{\mathbb{N}}(0, \max_{\mathbb{N}}(2, \min_{\mathbb{N}}(3,4))) \\
&= \max_{\mathbb{N}}(0, \max_{\mathbb{N}}(2,3)) \\
&= \max_{\mathbb{N}}(0,3) \\
&= 3
\end{aligned}
$$

Zur Auswertung von Bäumen: Auswertung von unten nach oben



Querbezüge

Knotenbeschriftete geordnete gerichtete Bäume werden Ihnen im Laufe Ihres Studiums verschiedentlich begegnen.

- Ableitungsbäume sind ein bekanntes Konzept aus den Formalen Sprachen.
- Diese werden auch im Compilerbau benutzt; dort sind auch Auswertefunktionen nützlich.
- Semistrukturierte Daten (z.B. XML) lassen sich (abstrakt) so begreifen.

Homomorphismen

Def.: Es seien $\mathbb{S} = (A, F, R)$ und $\mathbb{S}' = (A', F', R')$ zwei Strukturen desselben Typs $\tau = (\mathcal{F}, \mathcal{R}, \sigma)$. Eine Abbildung $h : A \to A'$ heißt *Homomorphismus* von $\mathbb{S}$ nach $\mathbb{S}'$, wenn die folgenden *Homomorphiebedingungen* erfüllt sind:

- Für alle $f \in \mathcal{F}$ und alle $a_1, \ldots, a_n$ (mit $n = \sigma(f)$) gilt:

$$h(f_{\mathbb{S}}(a_1, \ldots, a_n)) = f_{\mathbb{S}'}(h(a_1), \ldots, h(a_n)).$$

- Für alle $r \in \mathcal{R}$ und alle $a_1, \ldots, a_n$ (mit $n = \sigma(r)$) gilt:

$$(a_1, \ldots, a_n) \in r_{\mathbb{S}} \implies (h(a_1), \ldots, h(a_n)) \in r_{\mathbb{S}'}.$$

Homomorphismen erhalten Struktur

Dieses Wesen von Homomorphismen sieht man am besten an Beispielen.

- $(\mathbb{Z}, +, 0)$ und $(\mathbb{Z}_6, +, 0)$ sind Monoide.
  $h : \mathbb{Z} \to \mathbb{Z}_6, x \mapsto x \pmod 6$ ist ein Homomorphismus.
  Also gilt: $h(a + b) = h(a) + h(b)$.
  Achtung: $+$ "meint" unterschiedliche Additionen...

- Sind $\mathbb{O}_1 = (M_1, \leq_1)$ und $\mathbb{O}_2 = (M_2, \leq_2)$ Halbordnungen und
  ist $h : M_1 \to M_2$ ein Homomorphismus, so ist h "ordnungserhaltend":
  aus $a \leq_1 b$ folgt $h(a) \leq_2 h(b)$.
  Konkret: $\mathbb{O}_1 = (\mathbb{N} \setminus \{0\}, |)$, wobei $|$ die Teilerrelation meint, $\mathbb{O}_2 = (2^{\mathbb{N}}, \subseteq)$ und
  $h : m \mapsto T(m) = \{n \in \mathbb{N} : n|m\}$.

Noch ein Beispiel

- Betrachte das Monoid $\mathrm{REALPLUS} = (\mathbb{R}, +, 0)$.
  Sei ferner (S, P) ein diskreter Wahrscheinlichkeitsraum.
  Dann ist $\mathbb{R}^S$ die Menge der Zufallsgrößen (auf (S, P)).
  Der Erwartungswert lässt sich als Abbildung $E : \mathbb{R}^S \to \mathbb{R}$ auffassen.
  Begreift man nun $\mathbb{R}^S$ als Grundmenge des Funktionenmonoids $\mathrm{REALPLUS}^S$, so ist E ein Monoidhomomorphismus.
  Insbesondere ist der Erwartungswert der Zufallsgröße, die jedem elementaren Ereignis den Wert 0 zuweist, gleich Null.
  Zudem gilt: $E(X + Y) = E(X) + E(Y)$.

. . . und noch eines

Es sei M eine endliche Menge.
Wir wissen: $(2^{M\times M}, \circ, \Delta_M)$ ist ein Monoid.

Betrachte nun die Abbildung f, die $R \subseteq M \times M$ ihre Relationenmatrix $M_R \in \{0,1\}^{M\times M}$ zuordnet. Mit irgendeiner Bijektion $M \to \{1,\ldots,m\}$, $m = |M|$, kann man auch $M_R \in \{0,1\}^{m,m}$ auffassen.
Wir bezeichnen im Folgenden mit $\cdot$ das übliche Matrixprodukt und das Produkt zweier reeller Zahlen.
Für Matrizen $A, B, C \in \mathbb{R}^{m,m}$ gilt daher $A = B \cdot C$, falls für den Eintrag $A[i,j]$ in der i-ten Zeile und j-ten Spalte von A gilt: $A[i,j] = \sum_{k=1}^{m} B[i,k] \cdot C[k,j]$.
Wenn E_m die m-dimensionale Einheitsmatrix bezeichnet (sie hat nur auf der Hauptdiagonalen nichtverschwindene Einträge, und diese sind Eins), so gilt: $(\mathbb{R}^{m,m}, \cdot, E_m)$ ist ein Monoid, und $f : 2^{M\times M} \to \mathbb{R}^{m,m}$ ist ein Monoidhomomorphismus.

Homomorphismen zwischen Algebren

Satz: Es seien $\mathbb{A}_1 = (A_1, F_1)$ und $\mathbb{A}_2 = (A_2, F_2)$ zwei Algebren vom Typ $(\mathcal{F}, \sigma)$. Sei $h : A_1 \to A_2$ ein Homomorphismus.
1. Ist $\mathbb{A}_1' = (A_1', F_1')$ eine Unteralgebra von $\mathbb{A}_1$, so beschreibt $h(A_1')$ eine Unteralgebra von $\mathbb{A}_2$.
2. Ist $\mathbb{A}_2' = (A_2', F_2')$ eine Unteralgebra von $\mathbb{A}_2$, so beschreibt $h^{-1}(A_2')$ eine Unteralgebra von $\mathbb{A}_1$.

Beweis: Betrachte $f \in \mathcal{F}$ mit $\sigma(f) = n$. Es seien $h(a_1), \ldots, h(a_n) \in h(A_1')$. Dann gilt:

$$f_{\mathbb{A}_2}(h(a_1), \ldots, h(a_n)) = h(f_{\mathbb{A}_1}(a_1), \ldots, f_{\mathbb{A}_1}(a_n)) = h(f_{\mathbb{A}_1'}(a_1), \ldots, f_{\mathbb{A}_1'}(a_n)) \in h(A_1').$$

Betrachte nun $a_1, \ldots, a_n \in h^{-1}(A_2')$. Dann ist:

$$h(f_{\mathbb{A}_1}(a_1), \ldots, f_{\mathbb{A}_1}(a_n)) = f_{\mathbb{A}_2}(h(a_1), \ldots, h(a_n)) = f_{\mathbb{A}_2'}(h(a_1), \ldots, h(a_n)) \in A_2'. \qquad \square$$

Unterstrukturen und Homomorphismen

Lemma: Es sei $\tau = (\mathcal{F}, \mathcal{R}, \sigma)$ der Typ einer Struktur.
Es seien $\mathbb{S} = (A, F, R)$ und $\mathbb{S}' = (A', F', R')$ Strukturen vom Typ τ.
Ist $\mathbb{S}'$ Unterstruktur von $\mathbb{S}$, so gilt:
Die Inklusionsabbildung $\iota : A' \to A, x \mapsto x$ ist ein injektiver Homomorphismus.

Beweis: Die Injektivität der Inklusionsabbildung ist bekannt.

Betrachte bel. $f \in \mathcal{F}$ mit $\sigma(f) = n$ und $a_1, \ldots, a_n \in A'$.

$\iota(f_{\mathbb{S}'}(a_1, \ldots, a_n)) = f_{\mathbb{S}'}(a_1, \ldots, a_n) = f_{\mathbb{S}}(a_1, \ldots, a_n) = f_{\mathbb{S}}(\iota(a_1), \ldots, \iota(a_n))$.

Für die erste und letzte Gleichheit benutze Def. von ι, für die mittlere Def. von Unterstruktur.

Die Bedingung für die Relationen sieht man ähnlich ein. □

Zur Komposition von Homomorphismen

Lemma: Es sei $\tau = (\mathcal{F}, \mathcal{R}, \sigma)$ der Typ einer Struktur.
Es seien $\mathbb{S}_1 = (A_1, F_1, R_1)$, $\mathbb{S}_2 = (A_2, F_2, R_2)$ und $\mathbb{S}_3 = (A_3, F_3, R_3)$ Strukturen vom Typ τ.
Ist $f : A_1 \to A_2$ ein Homomorphismus von $\mathbb{S}_1$ nach $\mathbb{S}_2$ und
ist $g : A_2 \to A_3$ ein Homomorphismus von $\mathbb{S}_2$ nach $\mathbb{S}_3$,
so ist $f \circ g : A_1 \to A_3$ ein Homomorphismus von $\mathbb{S}_1$ nach $\mathbb{S}_3$.

Beweis zur Übung.

Wir können also leicht Homomorphismen zwischen Strukturen desselben Typs als Halbgruppe bzgl. der Komposition begreifen.

Mehr Morphismen

Es seien $\mathbb{S} = (A, F, R)$ und $\mathbb{S}' = (A', F', R')$ zwei Strukturen desselben Typs $\tau = (\mathcal{F}, \mathcal{R}, \sigma)$. Ein Homomorphismus $h : A \to A'$ von $\mathbb{S}$ nach $\mathbb{S}'$ heißt:

- *Isomorphismus*, falls h bijektiv ist und h^{-1} Homomorphismus;
- *Automorphismus*, falls h Isomorphismus und $A = A'$.

Beispiel: Wir hatten oben gesehen, dass man die Zuordnung $R \mapsto M_R$ von Relationenmatrizen zu Relationen als Homomorphismus auffassen kann.
Durch Modifikation des Matrixproduktes (siehe oben) und Einschränkung auf Matrizen mit Einträgen aus $\{0, 1\}$ liefert dies sogar einen Isomorphismus.

Hinweis: Der Begriff des Graphisomorphismus stimmt mit diesem Isomorphiebegriff überein.

Erinnerung: Graphisomorphie

Wir wollen im Folgenden Graphen und ihre Eigenschaften untersuchen.
Es ist dabei gleichgültig, wie wir Knoten und Kanten konkret benennen.
Dies führt auf folgenden Begriff:

Def.: Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ heißen *isomorph*, i.Z. $G \simeq G'$ gdw. es eine Bijektion $\phi : V \to V'$ gibt, sodass

$$xy \in E \iff \phi(x)\phi(y) \in E'.$$

$\phi : V \to V'$ heißt dann auch *Isomorphismus* von G auf G'.

Isomorphismen zwischen Algebren

Satz: Es seien $\mathbb{A} = (A, F)$ und $\mathbb{A}' = (A', F')$ zwei Algebren desselben Typs $\tau = (\mathcal{F}, \sigma)$. Ist $h : A \to A'$ ein bijektiver Homomorphismus von $\mathbb{A}$ nach $\mathbb{A}'$, so ist h^{-1} ein Isomorphismus von $\mathbb{A}'$ nach $\mathbb{A}$.

Beweis: Betrachte $f \in \mathcal{F}$ mit $\sigma(f) = n$.
Es seien $b_1, \ldots, b_n \in A'$. Setze $a_1 = h^{-1}(b_1), \ldots, a_n = h^{-1}(b_n)$.
Dann gilt:

$$\begin{aligned} h^{-1}(f_{\mathbb{A}'}(b_1, \ldots, b_n)) &= h^{-1}(f_{\mathbb{A}'}(h(a_1), \ldots, h(a_n)) \\ &= h^{-1}(h(f_{\mathbb{A}}(a_1, \ldots, a_n))) \\ &= f_{\mathbb{A}}(a_1, \ldots, a_n) \\ &= f_{\mathbb{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_n)) \end{aligned}$$

□

Anwendung: Logarithmentafeln

Lemma: $(\mathbb{R}_{>0}, \cdot, 1)$ ist ein Monoid.
Lemma: $(\mathbb{R}, +, 0)$ ist ein Monoid.

Satz: $h : \mathbb{R}_{>0} \to \mathbb{R}, x \mapsto \log_{10}(x)$ ist ein Monoidisomorphismus.

Beweis: Für jede positive reelle Zahl kann der Logarithmus berechnet werden.
Auch die Umkehrfunktion des Logarithmus ist wohlbekannt: Die Exponentialfunktion.
$\log(x \cdot y) = \log(x) + \log(y)$ ist ein bekanntes Logarithmenrechengesetz.
Dieses entspricht der Homomorphiebedingung für $\cdot$ bzw. $+$; $\log_{10}(1) = 0$ überträgt Konstanten.□

Logarithmentafeln wurden früher zur beschleunigten Berechnung von Multiplikationen verwendet:
Statt $x \cdot y$ wurde
(1) durch Nachschlagen $x' = \log_{10}(x)$, $y' = \log_{10}(y)$ bestimmt,
(2) sodann $z' = x' + y'$ berechnet und
(3) erneut durch Nachschlagen das Endergebnis $z = 10^{z'}$.

Beispiel Bitvektoren

Es sei $\mathcal{U}$ ein Universum (Grundmenge).
Dann ist $\mathbb{U} = (2^{\mathcal{U}}, \cup, \emptyset)$ ein Monoid.
Ebenso ist $\mathbb{2} = (\{0,1\}, \max, 0)$ ein Monoid.
Damit ist das Funktionenmonoid $\mathbb{2}^{\mathcal{U}} = (\{0,1\}^{\mathcal{U}}, \max, 0 := \{u \mapsto 0\})$ definiert.

Lemma: $\mathbb{U}$ ist monoidisomorph zu $\mathbb{2}^{\mathcal{U}}$.
Als Homomorphismus betrachte die "Bitvektorenabbildung" $\chi : A \mapsto \chi_A$,
die $A \subseteq \mathcal{U}$ ihre charakteristische Funktion χ_A zuordnet.
Die Homomorphiebedingung bedeutet jetzt: $\chi_{A \cup B} = \max(\chi_A, \chi_B)$ bzw. $\chi_\emptyset = 0$.

Hinweis: Diese Homomorphie (und ähnliche...) wird bei effizienten Implementierungen von Mengenoperationen ausgenutzt.

Mengensysteme bringen Ordnung in Halbordnungen

Satz: Zu jeder Halbordnung $(X, \leq)$ gibt gibt es ein Mengensystem $\mathcal{M}_X$, sodass die Halbordnungen $(X, \leq)$ und $(\mathcal{M}_X, \subseteq)$ isomorph sind.
Folgerung: Es gibt also im Wesentlichen nur Unterhalbordnungen von $(2^M, \subseteq)$ für irgendeine Menge M als mögliche Halbordnungen.

Beweis: Wir definieren $\mathcal{M}_X \subseteq 2^X$ als Bildbereich der Abbildung $f : x \mapsto \{y \in X \mid y \leq x\}$.

Daher ist f surjektiv nach Konstruktion.

Auf $\{y \in X \mid y \leq x\} = f(x) = f(x') = \{y \in X \mid y \leq x'\}$ folgt $x \leq x'$ und $x' \leq x$, also $x = x'$, da $\leq$ antisymmetrisch. Also ist f injektiv.

Aus $x \leq x'$ folgt $\{y \in X \mid y \leq x\} \subseteq \{y \in X \mid y \leq x'\}$, also $f(x) \subseteq f(x')$, d.h., f ist ordnungserhaltend.

Umgekehrt liefert $f(x) = \{y \in X \mid y \leq x\} \subseteq f(x') = \{y \in X \mid y \leq x'\}$, dass $x \leq x'$, d.h., f^{-1} ist ebenfalls ordnungserhaltend. □

Kongruenzrelationen

Def.: Es seien A eine Menge und $\equiv$ eine Äquivalenzrelation auf A.
Ist $f : A^n \to A$ eine Operation auf A, so heißt f *verträglich* mit $\equiv$, gdw.
für alle $a_1, \ldots, a_n, a'_1, \ldots, a'_n \in A$ gilt:

$$((a_1 \equiv a'_1) \wedge \cdots \wedge (a_n \equiv a'_n)) \implies f(a_1, \ldots, a_n) \equiv f(a'_1, \ldots, a'_n).$$

Ist $\mathbb{A} = (A, F)$ eine Algebra, so heißt eine Äquivalenzrelation $\equiv$ auf A
Kongruenzrelation auf $\mathbb{A}$, falls $\equiv$ mit allen Operationen von $\mathbb{A}$ verträglich ist.
Die Äquivalenzklassen einer Kongruenzrelation heißen auch *Kongruenzklassen*.

Beispiel: Diagonale Δ_A und Allrelation $A \times A$ sind stets Kongruenzrelationen.
Für jede Menge A gilt, dass in der Algebra $(A, \mathrm{Op}(A))$ die Äquivalenzrelationen
Δ_A und $A \times A$ die einzigen Kongruenzrelationen sind.

Beispiele für verträgliche Abbildungen

Es sei $\equiv$ eine Äquivalenzrelation auf der Menge A.
Dann gibt es etliche Operationen, die "automatisch" mit $\equiv$ verträglich sind:

- die identische Abbildung (Diagonale) auf A;
- für jedes $c \in A$ und $n \in \mathbb{N}$ die konstante Abbildung

$$f_c : A^n \to A, f_c(x_1, \ldots, x_n) := c;$$

- für $1 \leq i \leq n$ die Projektion

$$pr_i : A^n \to A, (x_1, x_2, \ldots, x_i, \ldots, x_n) \mapsto x_i.$$

Ein Beispiel für eine Äquivalenzrelation

Es sei $p > 1$ eine natürliche Zahl.
Definiere auf $\mathbb{Z}$ die Binärrelation $\equiv_p$ wie folgt:
$a \equiv_p b$ gdw. a und b lassen beim Teilen durch p denselben Rest.

Lemma: $\equiv_p$ ist eine Kongruenzrelation auf dem Monoid $(\mathbb{Z}, +, 0)$.

Beweis: Die bekannten Rechengesetze zeigen: $(\mathbb{Z}, +, 0)$ ist ein Monoid.

Was bedeutet ganzzahlige Division?

a durch p ergibt d_a Rest r_a heißt: $a = p \cdot d_a + r_a$ und $r_a < p$.

Damit: $r_a = r_b$ gdw. $a - pd_a = b - pd_b$.

Aus dieser Darstellung folgen Reflexivität und Symmetrie von $\equiv_p$ sofort.

Auch die Transitivität sieht man so leicht.

Gilt $a \equiv_p a'$ und $b \equiv_p b'$, so $a - pd_a = a' - pd_{a'}$ und $b - pd_b = b' - pd_{b'}$,

woraus $(a + b) - p(d_a + d_b) = (a' + b') - p(d_{a'} + d_{b'})$ folgt.

Daraus folgt fast die Behauptung... (Problem: $d_a + d_b$ muss nicht gleich d_{a+b} sein.) □

Homomorphismen liefern Kongruenzrelationen

Es seien $\mathbb{A}_1 = (A_1, F_1)$ und $\mathbb{A}_2 = (A_2, F_2)$ zwei Algebren vom Typ $(\mathcal{F}, \sigma)$.
Es sei $h : A_1 \to A_2$ ein Homomorphismus von der Algebra $\mathbb{A}_1$ in die Algebra $\mathbb{A}_2$.
Erinnerung: Kern$(h) := \{(a, b) \in A_1^2 | h(a) = h(b)\}$ ist eine Äquivalenzrelation.
Lemma: In der beschriebenen Lage ist Kern(h) eine Kongruenzrelation auf $\mathbb{A}_1$.

Beweis: Zu zeigen ist lediglich noch die Verträglichkeit.

Betrachte also $f \in \mathcal{F}$ mit $\sigma(f) = n$.

Es seien $a_1, \ldots, a_n, a'_1, \ldots, a'_n \in A_1$, sodass

$(a_1, a'_1) \in$ Kern$(h), \ldots, (a_n, a'_n) \in$ Kern(h).

Also gilt: $h(a_1) = h(a'_1), \ldots, h(a_n) = h(a'_n)$.

Da h Homomorphismus, gilt: $h(f_{\mathbb{A}_1}(a_1, \ldots, a_n)) = f_{\mathbb{A}_2}(h(a_1), \ldots, h(a_n)) = f_{\mathbb{A}_2}(h(a'_1), \ldots, h(a'_n)) = h(f_{\mathbb{A}_1}(a_1, \ldots, a_n))$, also folgt: $(f_{\mathbb{A}_1}(a_1, \ldots, a_n), f_{\mathbb{A}_1}(a'_1, \ldots, a'_n)) \in$ Kern(h). □

Eine Veranschaulichung

Betrachten wir die Monoide $(\mathbb{Z}, +, 0)$ und $(\mathbb{Z}_2, +, 0)$.
Dazu passt der Homomorphismus $h : \mathbb{Z} \to \mathbb{Z}_2$, der x die Zahl 0 zuordnet, wenn x gerade ist, und die Zahl 1, wenn x ungerade ist.
Die zu Kern(h) gehörige Zerlegung ist $\mathbb{Z} = G \cup U$ in die **g**eraden und **u**ngeraden Zahlen.
Es gilt: Kern$(h) = \{(a, b) \in \mathbb{Z}^2 \mid a + b \in G\}$.
Was bedeutet “Verträglichkeit” hier?
Gilt $(a, b) \in$ Kern(h), so $a + b \in G$, also $h(a + b) = 0$,
Hierbei gibt es zwei Fälle:
(1) $a, b \in G$: Dann gilt $h(a) = h(b) = 0$, also $h(a) + h(b) = 0$.
(2) $a, b \in U$: Dann gilt $h(a) = h(b) = 1$, also $h(a) + h(b) = 0$ (in $\mathbb{Z}_2$).
Kern(h) ist also eine Kongruenzrelation.

Faktoralgebren

Es seien A eine Menge, $\mathbb{A} = (A, F)$ eine Algebra vom Typ $\tau = (\mathcal{F}, \sigma)$ und $\equiv$ eine Kongruenzrelation auf $\mathbb{A}$.
Erinnerung: $A/\equiv := \{[a]_\equiv \mid a \in A\}$ ist die Quotientenmenge von $\equiv$.
Hier ist $A/\equiv$ die Menge aller Kongruenzklassen von $\equiv$.
Wir definieren die *Faktoralgebra* $\mathbb{A}/\equiv = (A/\equiv, F_\equiv)$ vom Typ τ durch Beschreibung der Operationen in $F_\equiv$ wie folgt:
Für $f \in \mathcal{F}$ mit $\sigma(f) = n$ sei

$$f_{\mathbb{A}/\equiv} : (A/\equiv)^n \to A/\equiv,\ ([a_1]_\equiv, \ldots, [a_n]_\equiv) \mapsto [f_{\mathbb{A}}(a_1, \ldots, a_n)]_\equiv.$$

Lemma: Die Operationen $f_{\mathbb{A}/\equiv}$ sind wohldefiniert.

Beweis: Problematisch ist einzig die Vertreterunabhängigkeit.

Betrachte $[a_1]_\equiv = [b_1]_\equiv, \ldots, [a_n]_\equiv = [b_n]_\equiv$, also $a_1 \equiv b_1, \ldots, a_n \equiv b_n$.

Da $\equiv$ Kongruenzrelation, folgt

$f_{\mathbb{A}}(a_1, \ldots, a_n) \equiv f_{\mathbb{A}}(b_1, \ldots, b_n)$, d.h. $[f_{\mathbb{A}}(a_1, \ldots, a_n)]_\equiv = [f_{\mathbb{A}}(b_1, \ldots, b_n)]_\equiv$. □

Eine Veranschaulichung (Forts.)

Betrachte das Monoid $(\mathbb{Z}, +, 0)$ und die Zerlegung $\mathbb{Z} = G \cup U$.
Sei $\equiv_2$ die entsprechene Äquivalenzrelation.
Wir haben gesehen, dass $\equiv_2$ sogar eine Kongruenzrelation ist.
Betrachte das Faktormonoid mit der Grundmenge $\mathbb{Z}/\equiv_2 = \{G, U\}$.
Die Addition ist hier gegeben durch: $G+G = U+U = G$ und $G+U = U+G = U$.
Beachte: Dies entspricht der Monoidoperation auf dem Komplex"produkt" zu auf der Grundmenge $2^{\mathbb{Z}}$.
M.a.W.: $(\mathbb{Z}_2, +)$ ist eine Unterhalbgruppe von $(2^{\mathbb{Z}}, +)$, allerdings mit unterschiedlichen neutralen Elementen, nämlich G bzw. $\{0\}$.

Restklassen

Es sei $p > 1$ eine natürliche Zahl.
Definiere auf $\mathbb{Z}$ die Binärrelation $\equiv_p$ wie folgt:
$a \equiv_p b$ gdw. a und b lassen beim Teilen durch p denselben Rest.

Lemma: $\equiv_p$ ist eine Kongruenzrelation auf dem Monoid $(\mathbb{Z}, +, 0)$.
Die Äquivalenzklassen $[\cdot]_p$ von $\equiv_p$ heißen auch *Restklassen*.
Man schreibt auch $\mathbb{Z}_p := \mathbb{Z}/\equiv_p$.
Als Vertreter der Restklassen wählt man üblicherweise die kleinsten nichtnegativen Zahlen, die in ihnen liegen.
Bsp.: $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$.
Notiert man schließlich nur die Vertreter, gelangen wir zu der früher betrachteten Verknüpfungstafel für $(\{0, 1, 2, 3, 4, 5\}, +, 0)$.

Hinweis: Das Rechnen in Restklassen hat wichtige Anwendungen in der Kryptographie.

Äquivalenzrelationen liefern Homomorphismen

Es sei $\sim$ eine Äquivalenzrelation auf A.

$[a]$ bezeichne die Äquivalenzklasse von a bzgl. $\sim$.

$f_\sim : A \to A/\sim,\ a \mapsto [a]$ ist die kanonische Abbildung von $\sim$.

Lemma: Ist $\sim$ Kongruenzrelation der Algebra $\mathbb{A} = (A, F)$ vom Typ τ, so ist $f_\sim$ ein surjektiver Homomorphismus von $\mathbb{A}$ auf die Algebra $\mathbb{A}/\sim$ vom Typ τ.

Ferner gilt: $\mathrm{Kern}(f_\sim) = \sim$.

Beweis zur Übung.

Beispiel: Betrachte die Algebra $(\mathbb{Z}_6, +0)$ mit der Zerlegung $\{\{0,3\},\{1,4\},\{2,5\}\}$.

Wie sieht die zugehörige Äquivalenzrelation aus?

Geben Sie die Verknüpfungstafel der Faktoralgebra an.

Der Homomorphiesatz

Satz: $\mathbb{A}_1 = (A_1, F_1)$ und $\mathbb{A}_2 = (A_2, F_2)$ zwei Algebren vom Typ $(\mathcal{F}, \sigma)$. Es sei $f : A_1 \to A_2$ ein Homomorphismus von $\mathbb{A}_1$ nach $\mathbb{A}_2$.
Es sei $\equiv = \mathrm{Kern}(f)$.
Dann gibt es einer Darstellung $f = f_{\equiv} \circ f' \circ \iota$, wobei
$f_{\equiv} : A_1 \to A_1/\equiv$ der kanonische Homomorphismus,
$\iota : f(A_1) \to A_2$ die Inklusionsabbildung und
$f' : A_1/\equiv \to f(A_1)$ ein Isomorphismus ist.

Beweis: Definiere für $a \in A_1$: $f'([a]_{\equiv}) := f(a)$.

Zu zeigen bliebe:

(1) f' ist wohldefiniert (also vertreterunabhängig).

(2) f' ist bijektiv.

(3) f' ist ein Homomorphismus.

Daraus folgt die behauptete Darstellung. □

Ausblick Abstrakte Datentypen / Objektorientierung

Erweiterung auf *mehrsortige Algebren* nötig:
Es gibt dabei dann “mehrere Grundmengen” (Sorten).
Eigenschaften werden dann über Gleichungen beschrieben.
Mehr hierzu in Büchern über “Algebraische Spezifikation.”
Das Konzept der Vererbung zeigt die Vorteile der Abstraktion praktisch:
Wieder braucht man nur einmal Schnittstellen und Eigenschaften zu beschreiben, kann dann aber dies auf verschiedene Situationen und Implementierungen anwenden.

Diese mehrsortige Sicht wäre auch schon bei uns hilfreich, um

- Relationen nicht “extra” behandeln zu müssen oder um
- Begriffe wie Vektorräume einfach(er) angeben zu können.

Literatur

1. Th. Ihringer: Allgemeine Algebra, Berliner Studienreihe zur Mathematik, Band 10 (2003), Heldermann Verlag (frühere Auflagen bei Teubner) Th. Ihringer hat auch ein Buch über Diskrete Mathematik verfasst.

2. W. Wechsler: Universal Algebra for Computer Scientists (Monographs in Theoretical Computer Science. An EATCS Series).

3. S. N. Burris and H. P. Sankappanavar online Buch

4. Software

Abschließende Zusammenhänge

- In der Logik wird (strikter als bei uns) zwischen Syntax und Semantik unterschieden.

- Dies führt dort zu zwei Formen des Begründens:
  syntaktisch durch Ableitung und semantisch im Modell.

- Ähnlich kann man auch für allgemeine Algebren formale Beweissysteme erstellen (wollen), die Beweise und auch Berechnungen für unterschiedliche konkrete Algebren gestatten.