Diskrete Mathematik für Informatiker

Universität Leipzig

WS 2007 / 08

Claus Diem

Kapitel 1

Algebraische Strukturen

1.1 Boolesche Ringe und boolesche Algebren

Boolesche Ringe

Definition Sei X eine Menge und $\circ$ eine Verknüpfung auf X. Sei nun $x \in X$. Dann heißt x *idempotent* (bez. $\circ$), wenn $x \circ x = x$. Die Verknüpfung $\circ$ heißt *idempotent*, wenn $x \circ x = x$ für alle $x \in X$.

Folgerung 1.1 *Sei $(H, \cdot)$ eine abelsche Halbgruppe mit einer idempotenten Verknüpfung. Wir definieren wie folgt eine Relation $\leq$ auf H:*

$$a \leq b :\Longleftrightarrow ab = a$$

Dann ist $\leq$ eine Ordnungsrelation.

Beweis.
(R) Nach Definition ist $a^2 = a$ für alle $a \in R$.
(A) Seien $a, b \in B$ mit $a \leq b$ und $b \leq a$. Dann ist $a = ab = ba = b$.
(T) Seien $a, b, c \in B$ mit $a \leq b, b \leq c$. Dann ist $a = ab = a(bc) = (ab)c = ac$. □

Definition Sei R ein Ring.[1] Dann heißt R *boolesch*, wenn die Multiplikation auf R idempotent ist.

Beispiel 1.2 Die Standardbeispielklasse zu booleschen Ringen ist wie folgt: Sei S eine Menge. Nun ist die Potenzmenge $\mathcal{P}(S)$ mit der symmetrischen Differenz Δ als Addition und dem Durchschnitt ($\cap$) als Multiplikation ein

[1] Ringe haben bei uns immer eine 1 ($(R, \cdot)$ ist ein Monoid). Dies wird in der Literatur nicht immer vorausgesetzt.

boolescher Ring. Die Null ist die leere Menge und die Eins ist S. Wir nennen diesen Ring den *vollen Mengenring* auf S.

Sei im Folgenden R ein boolescher Ring.

Folgerung 1.3 *R ist kommutativ (d.h. die Multiplikation ist kommutativ). Außerdem gilt: $a + a = 0$ für alle $a \in R$ (d.h. $a = -a$).*

Bemerkung Für $a \in R$ und $n \in \mathbb{N}$ setzen wir $na := \overbrace{a + \cdots + a}^{n \text{ mal}}$ (siehe [LA, S. 27])[2]. Die Aussage ist also, dass in R stets $2a = 0$ gilt.

Beweis der Folgerung. Sei zunächst $a \in R$. Dann gilt $2a = (2a)^2 = 4a^2 = 4a$. Damit ist also $2a = 0$.

Seien $a, b \in R$. Dann gilt $a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$. Somit gilt $0 = ab + ba$. Da $ba = -ba$, folgt $ab = ba$. □

Betrachten wir die Abbildung $\varphi : \mathbb{F}_2 \longrightarrow R, 0 \mapsto 0_R, 1 \mapsto 1_R$. Diese Abbildung ist ein Ringhomomorphismus. Die einzige nicht-triviale Aussage ist, dass $\varphi(1+1) = \varphi(1) + \varphi(1)$. Dies stimmt aber, da $\varphi(1+1) = \varphi(0) = 0_R$ und $\varphi(1) + \varphi(1) = 1_R + 1_R = 0_R$ ist (s.o.).

Insbesondere definiert ein boolescher Ring "in offensichtlicher Weise" einen $\mathbb{F}_2$-Vektorraum. (Wenn immer ein Körper K, ein Ring R und ein Ringhomomorphismus $\varphi : K \longrightarrow R$ gegeben ist, ist R mittels der Skalarmultiplikation $\cdot : K \times R \longrightarrow R\,, r := \varphi(a) \cdot r$ für $a \in K, r \in R$ ein K-Vektorraum.)

Somit haben wir insbesondere:

Folgerung 1.4 *Wenn R endlich ist, dann ist $\#R$ ist eine Zweierpotenz.*

Wie in Folgerung 1.1 definieren wir für $a, b \in R$:

$$a \leq b :\Longleftrightarrow ab = a$$

Nach Folgerung 1.1 ist $\leq$ eine Ordnungsrelation auf R.

Definition Ein bez. $\leq$ minimales Element in $R - \{0\}$ heißt *Atom*.

Mit anderen Worten: Ein Atom ist ein Element $a \in R$ mit $a \neq 0$ und

$$\forall b \in R - \{0\} : b \leq a \longrightarrow b = a\ .$$

Beachten Sie hier: $b \leq a$ bedeutet $ab = b$.

Beispiel 1.5 Im vollen Mengenring $\mathcal{P}(S)$ gilt $X \subseteq Y \longleftrightarrow X \leq Y$, und die Atome in $\mathcal{P}(S)$ sind die ein-elementigen Mengen.

[2] Mit [LA] ist das Skript zur meiner Vorlesung Lineare Algebra gemeint.

Lemma 1.6

- *Sei a ein Atom. Dann gilt für alle $b \in R$: $a \leq b$ oder $ab = 0$.*
- *Für zwei verschiedene Atome a, b gilt: $ab = 0$.*

Beweis. Sei a ein Atom und $b \in R$. Dann gilt $(ab) \cdot a = a^2 b = ab$, und somit $ab \leq a$. Da a ein Atom ist, impliziert dies: $ab = a$ oder $ab = 0$. Die Aussage $ab = a$ bedeutet gerade, dass $a \leq b$.

Sei nun b ein von a verschiedenes Atom. Wenn nun $a \leq b$ gelten würde, würde $a = b$ gelten nach Definition. Also gilt $ab = 0$. □

Lemma 1.7 *Sei R endlich. Dann gilt:*

- *Zu jedem Element $x \in R$ gilt es Atom $a \in R$ mit $a \leq x$.*
- *Es gilt die Gleichung $1 = \sum_{a\ Atom} a$.*

Beweis. Die erste Aussage ist leicht.

Zur zweiten Aussage: Wir nehmen an, dass $1 - \sum_{a\ \mathrm{Atom}} a = 1 + \sum_{a\ \mathrm{Atom}} a \neq 0$. Dann gibt es ein Atom a_0 mit $a_0 \leq 1 + \sum_{a\ \mathrm{Atom}} a$. Somit gilt $a_0 = a_0(1 + \sum_{a\ \mathrm{Atom}} a) = a_0 + \sum_{a\ \mathrm{Atom}} (a_0 a) = a_0 + a_0$ nach dem obigen Lemma. Dies ist ein Widerspruch. □

Dies impliziert:

Folgerung 1.8 *Sei $b \in R$ und sei $X := \{a \in R |\ a \leq b\,, a\ Atom\}$. Dann gilt:*

$$b = \sum_{a \in X} a\ .$$

Ferner gilt für $Y \subseteq R$: Wenn $b = \sum_{a \in Y} a$, dann ist $X = Y$.

Beweis. Es ist $b = 1 \cdot b = (\sum_{a\ \mathrm{Atom}} a) b = \sum_{a\ \mathrm{Atom}} (ab) = \sum_{a \in X} a$.

Seien nun $Y, Z \subseteq R$ mit $b = \sum_{a \in Y} a = \sum_{a \in Z} a$. Wir nehmen an, dass $Y \neq Z$. Dann gibt OBdA es ein Atom $a_0 \in Z - Y$. Nun haben wir einerseits $ba_0 = \sum_{a \in Z} a a_0 = a_0$ und andererseits $ba_0 = \sum_{a \in Y} a a_0 = 0$, ein Widerspruch. □

Wir haben nun den folgenden Satz:

Satz 1.1 *Sei R ein endlicher boolescher Ring und A die Menge der Atome in R. Dann ist die Abbildung*

$$\varphi : \mathcal{P}(A) \longrightarrow R\ ,\ X \mapsto \sum_{a \in X} a$$

ein Isomorphismus von Ringen, wobei wir $\mathcal{P}(A)$ wie in Beispiel 1.2 als booleschen Ring auffassen. Die Umkehrabbildung ist

$$R \longrightarrow \mathcal{P}(A)\ ,\ b \mapsto \{a \in R \mid a \leq b\,, a\ Atom\ \}\ .$$

Beweis. Wir wissen schon, dass wir eine Bijektion haben. Ferner gilt für $X, Y \subseteq A$: $\varphi(X) + \varphi(Y) = (\sum_{a \in X} a) + (\sum_{a \in Y} a) = \sum_{a \in X \Delta Y} a = \varphi(X \Delta Y)$ und $\varphi(X) \cdot \varphi(Y) = (\sum_{a \in X} a) \cdot (\sum_{a \in Y} a) = \sum_{(a,b) \in X \times Y} ab = \sum_{a \in X \cap Y} a = \varphi(X \cap Y)$, d.h. φ ist ein Ringhomomorphismus. □

Bemerkung Sei $A = \{a_1, \ldots, a_n\}$ mit paarweise verschiedenen a_i. Dann gilt also: Für alle $b \in R$ gibt es eindeutig bestimmte Elemente $c_1, \ldots, c_n \in \mathbb{F}_2$ mit $b = \sum_{i=1}^{n} c_i a_i$. Mit anderen Worten: $a_1, \ldots, a_n$ ist eine $\mathbb{F}_2$-Vektorraumbasis von A. (Man kann auch sagen: A ist eine $\mathbb{F}_2$-Vektorraumbasis von R.)

Boolesche Algebren

Boolesche Ringe stehen in enger Beziehung zu *booleschen Algebren*.

Definition Eine *boolesche Algebra* ist eine Menge B zusammen mit zwei Verknüpfungen $\wedge$ und $\vee$ so dass das gilt:

- $(B, \vee)$ ist ein abelsches Monoid.
- $(B, \wedge)$ ist ein abelsches Monoid.
- Es gelten die *Distributivgesetze*

  $$\forall a, b, c : (a \vee b) \wedge c = (a \vee c) \wedge (b \vee c) \,, \quad (a \wedge b) \vee c = (a \wedge c) \vee (b \wedge c) \,.$$

- Sei 0 das neutrale Element von $(B, \vee)$ und 1 das neutrale Element von $(B, \wedge)$. Dann gilt: Für alle $a \in B$ gibt es ein $b \in B$ mit

  $$a \vee b = 1 \text{ und } a \wedge b = 0 \,.$$

Gegeben ein Element $a \in B$ heißt ein Element b wie im letzten Punkt ein *Komplement* von a.

Bemerkung Eine etwas formalere Definition (mit dem selben Inhalt) ist: Eine boolesche Algebra ist ein Tupel $(B, \wedge, \vee)$, wobei B eine Menge, $\wedge$ and $\vee$ Verknüpfungen auf B sind, so dass die obigen Eigenschaften gelten. Die Rollen von $\wedge$ und $\vee$ bzw. 0 und 1 sind nun symmetrisch. D.h. wenn $(B, \wedge, \vee)$ eine boolesche Algebra ist, dann ist auch $(B, \vee, \wedge)$ eine.

Beispiel 1.9 Die Standardbeispielklasse zu booleschen Algebren ist: Sei S eine Menge. Dann ist $\mathcal{P}(S)$ mit der Vereinigung als Operation $\vee$ und dem Durchschnitt als Operation $\wedge$ eine boolesche Algebra. Dabei ist $0 = \emptyset$ und $1 = S$. Wir nennen $\mathcal{P}(S)$ die *volle Mengenalgebra* auf S.

Wie immer definieren wir gleich auch die entsprechenden Morphismen.

Definition Seien B, B' zwei boolesche Algebren. Dann ist ein *Homomorphismus von booleschen Algebren* von B nach B' eine Abbildung $\varphi : B \longrightarrow B'$, die ein Homomorphismus von Monoiden von $(B, \vee)$ nach $(B', \vee')$ sowie von $(B, \wedge)$ nach $(B, \wedge')$ ist. Mit anderen Worten: Es muss gelten: $\varphi(a \wedge_B b) = \varphi(a) \wedge_{B'} \varphi(b'), \varphi(0_B) = 0_{B'}, \varphi(a \vee_B b) = \varphi(a) \vee_{B'} \varphi(b), \varphi(1_B) = 1_{B'}$ für alle $a, b \in B$.

Sei nun B eine boolesche Algebra. Wir leiten einige "Rechenregeln" ab und beweisen unter anderen, dass Komplemente stets eindeutig sind.

Lemma 1.10 *Für $a, b \in B$ gilt:*

- $a \vee a = a\,, \qquad a \wedge a = a$
- $a \vee 1 = 1\,, \qquad a \wedge 0 = 0$
- $a \vee (a \wedge b) = a\,, \qquad a \wedge (a \vee b) = 0$

Beweis. Aufgrund der Symmetrie von $\vee$ und $\wedge$ müssen wir jeweils nur eine der drei Aussagen beweisen.

Sei $c \in B$ ein Komplement von a. Dann ist

$$a = a \vee 0 = a \vee (a \wedge c) = (a \vee a) \wedge (a \vee c) = (a \vee a) \wedge 1 = a \vee a$$
$$a \vee 1 = a \vee (a \vee c)) = (a \vee a) \vee c = a \vee c = 1$$
$$a \vee (a \wedge b) = (a \wedge 1) \vee (a \wedge b) = a \wedge (1 \vee b) = a \vee 1 = a\,.$$

□

Lemma 1.11 *Sei $a \in B$, und seien $b, c \in B$ Komplemente zu a. Dann gilt $b = c$.*

Beweis. Es ist $b = 1 \wedge b = (a \vee c) \wedge b = (a \wedge b) \vee (c \wedge b) = 0 \vee (c \wedge b) = c \wedge b$. Analog gilt $c = b \wedge c = c \wedge b$. Also gilt $b = c$. □

Definition Sei $a \in B$, und sei $b \in B$ das nach Lemma 1.11 eindeutig bestimmte Element mit $a \vee b = 1, a \wedge b = 0$. Dann setzen wir $a^* := b$.

Lemma 1.12 *Seien $a, b \in B$. Dann sind äquivalent:*

- $a \vee b = b$
- $a \wedge b = a$

Beweis. Aufgrund der Symmetrie müssen wir nur zeigen, dass die erste Aussage die zweite impliziert.

Sei also $a \vee b = b$. Dann ist $a \wedge b = a \wedge (a \vee b) = (a \wedge a) \vee (a \wedge b) = a \vee (a \wedge b) = a$. □

Definition Wir definieren $a \leq b :\Longleftrightarrow a \wedge b = a$.

Nach Folgerung 1.1 ist $\leq$ wiederum eine Ordnungsrelation.

Normalerweise bezeichnen wir eine Menge "mit Zusatzstruktur" genau wie die Menge selbst. (Z.B. machen wir keinen Unterschied zwischen dem booleschen Ring R und der zugehörigen Menge). Dies ist jedoch für das Folgende unpraktisch.

Die folgende Folgerung kann man mit relativ einfachen aber teilweise länglichen Rechnungen beweisen. Die Idee ist, dass man den offensichtlichen Zusammenhang zwischen $(\mathcal{P}(S), \Delta, \cap)$ und $(\mathcal{P}(S), \cup, \cap)$ verallgemeinern kann.

Folgerung 1.13 *Sei M eine Menge.*

- *Seien $+, \cdot$ zwei Verknüpfungen auf M so dass $(M, +, \cdot)$ ein boolescher Ring ist. Wir definieren eine Verknüpfung $\vee$ auf M durch*

$$a \vee b := a + b + ab$$

  für $a, b \in M$. Dann ist $(M, \vee, \cdot)$ eine boolesche Algebra. (Es macht Sinn, die Verknüpfung $\cdot$ dann $\wedge$ zu nennen.) Außerdem gilt dann $a^* = 1 - a = 1 + a$ für alle $a \in M$.

- *Seien umgekehrt Verknüpfungen $\wedge$, $\vee$ auf M gegeben so dass $(M, \vee, \wedge)$ eine boolesche Algebra ist. Wir definieren eine Verknüpfung $+$ auf M durch*

$$a + b := (a \wedge b^*) \vee (a^* \wedge b) \ .$$

  Dann ist $(M, +, \wedge)$ ein boolescher Ring. (Es macht Sinn, die Verknüpfung $\wedge$ dann $\cdot$ zu nennen.)

- *Sei $\mathfrak{R}$ die Menge der booleschen Ringe auf M (d.h. $\mathfrak{R}$ ist die Menge der booleschen Ringe, deren unterliegende Menge M ist), und sei $\mathfrak{B}$ die Menge der booleschen Algebren auf M. Dann definieren die obigen Zuordnungen $(M, +, \cdot) \mapsto (M, \wedge, \cdot)$ und $(M, \vee, \wedge) \mapsto (M, +, \wedge)$ zueinander inverse Bijektionen zwischen $\mathfrak{R}$ und $\mathfrak{B}$.*

(Beweis Übungsaufgabe.)

Gegeben ein boolescher Ring, macht es also Sinn, von der *zugehörigen booleschen Algebra* zu sprechen, und gegeben eine boolesche Algebra, macht es Sinn vom *zugehörigen booleschen Ring* zu sprechen. Beachten Sie außerdem, dass die Relation $\leq$ für einen booleschen Ring mit der Relation $\leq$ für die zugehörige boolesche Algebra identisch ist.

Folgerung 1.14 *Seien nun M, M' zwei Mengen. Sei R ein boolescher Ring auf M, R' ein boolscher Ring auf M, und seien B bzw. B' die entsprechenden booleschen Algebren. Sei $\varphi : M \longrightarrow M'$ eine Abbildung. Dann ist φ genau dann ein Homomorphismus von booleschen Ringen von R nach R', wenn φ ein Homomorphismus von B nach B' ist.*

(Beweis Übungsaufgabe).

Sei nun B eine boolesche Algebra. Die Relation $\leq$ ist genau so definiert wie für boolesche Ringe. (Mit $\wedge$ anstelle von $\cdot$.) (Mit anderen Worten: Die Relation $\leq$ auf B ist die Relation $\leq$ des zugehörigen booleschen Rings.) Atome sind dann genau so definiert wie für boolesche Ringe. (D.h. die Menge der Atome in der booleschen Algebra und im zugehörigen booleschen Ring sind identisch.)

Sei $+$ die Addition des zugehörigen booleschen Rings. Dann gilt für Atome $a, b : a \vee b = a + b + ab = a + b$. Allgemeiner gilt für eine endliche Menge X von Atomen: $\sum_{a \in X} a = \bigvee_{a \in X} a$.

Wir erhalten das folgende Korollar zu Satz 1.1:

Korollar 1.15 *Sei B eine endliche boolesche Algebra, und sei A die Menge der Atome von B. Dann ist*

$$\varphi : \mathcal{P}(A) \longrightarrow B \, , X \mapsto \bigvee_{a \in X} a$$

ein Isomorphismus von booleschen Algebren, wobei wir die Potenzmenge $\mathcal{P}(A)$ wie in Beispiel 1.9 als boolesche Algebra auffassen.

Beweis. Die Abbildung φ ist genau die in Satz 1.1 definierte Abbildung. Nach Satz 1.1 wissen also schon, dass die Abbildung ein Isomorphismus der zugehörigen booleschen Algebren ist. Somit ist die Abbildung insbesondere bijektiv. Es ist ein Homomorphismus nach Folgerung 1.14. Alternativ kann man auch leicht direkt nachrechnen, dass es sich um einen Homomorphismus handelt. □

1.2 Allgemeine Algebra

Motivation

Wir setzen uns das Ziel, möglichst formal zu definieren, was wir unter einer Halbgruppe, einem Monoid und einer Gruppe meinen. Die Idee ist, dass die Strukturen jeweils aus einer Menge und einer Verknüpfung bestehen so dass gewissen Eigenschaften gelten. Wir wollen diese Eigenschaften mit Aussagen der Prädikatenlogik beschreiben.

Definition (alt)

- Eine Halbgruppe ist ein Tupel $(H, \cdot)$, wobei H eine Menge und $\cdot$ eine Verknüpfung auf H ist so dass gilt:

$$\forall a, b, c \in H : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- Ein Monoid ist ein Tupel $(M, \cdot)$, wobei M eine Menge und $\cdot$ eine Verknüpfung auf M ist so dass gilt:

$$\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$\exists e \in M : \forall a \in M : e \cdot a = e \wedge a \cdot e = a$$

- Eine Gruppe ist ein Tupel $(G, \cdot)$, wobei G eine Menge und $\cdot$ eine Verknüpfung auf G ist so dass gilt:

$$\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$\exists e \in G : ((\forall a \in G : e \cdot a = e \wedge a \cdot e = a) \wedge (\forall a \in G \, \exists b \in G : a \cdot b = e \wedge b \cdot a = e))$$

Ist es auch möglich die Objekte durch, "durch Identitäten" zu definieren, wobei man auf den Existenz-Quantor verzichtet?

Für Halbgruppen ist dies kein Problem. Bez. Monoide erinnern wir uns, dass das neutrale Element stets eindeutig bestimmt ist. Anstatt des Tupels $(M, \cdot)$ kann man auch das Tupel $(M, \cdot, e)$ betrachten, wobei e das neutrale Element ist. (Formal ist dieses 3-er-Tupel ein anderes Objekt als das ursprüngliche Zweiertupel, aber dieser Unterschied ist "vernachlässigbar".) Wir erhalten also neue Definition eines Monoids:

Definition (neu) Ein Monoid ist ein Tupel $(M, \cdot, e)$, wobei M eine Menge, $\cdot$ eine Verknüpfung auf M und $e \in M$ ist so dass gilt:

$$\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$\forall a \in M : e \cdot a = e \wedge a \cdot e = a$$

Für Gruppen geht es ähnlich, nur müssen wir nun auch die Inversion betrachten. Wir erhalten:

Definition (neu) Eine Gruppe ist ein Tupel $(G, \cdot, \iota, e)$, wobei G eine Menge, $\cdot$ eine Verknüpfung auf G, $\iota : G \longrightarrow G$ eine Abbildung und $e \in G$ ist so dass gilt:

$$\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$\forall a \in G : a \cdot \iota(a) = e \wedge \iota(a) \cdot a = e$$
$$\forall a \in G : e \cdot a = e \wedge a \cdot e = a \, .$$

Natürlich schreibt man wieder $a^{-1} = \iota(a)$ für alle $a \in G$.

Die *Allgemeine Algebra*[3] ist eine Theorie, die eine solche Art von Beschreibungen algebraischer Objekte in einen allgemeinen Rahmen gibt. Aussagen der Allgemeinen Algebra ergeben dann als Spezialfälle Aussagen über die verschiedensten algebraischen Objekte wie z.B. Halbgruppen, Monoide, Gruppen, Ringe, Vektorräume.

Erste Definitionen

Bisher haben wir die folgende Definition für eine "Verknüpfung" benutzt:

Definition Sei X eine Menge. Dann ist eine Verknüpfung auf X eine Abbildung $X \times X \longrightarrow X$.

In der Theorie der "Allgemeinen Algebra" verallgemeinert man diese Definition.

Sei im Folgenden X eine beliebige Menge. Erinnern Sie sich, dass wir für $n \in \mathbb{N}$ $X^n := X^{\{1,\dots,n\}}$ definiert haben (die Menge der Abbildungen von $\{1, \dots, n\}$ nach X).[4]

Es macht deshalb Sinn, $X^0 := X^{\emptyset}$ zu definieren. Diese Menge hat genau ein Element, welches wir mit $*$ bezeichnen.

Definition Sei $n \in \mathbb{N}_0$. Dann ist eine *n-stellige Verknüpfung* (oder *Operation*) auf X eine Abbildung $X^n \longrightarrow X$. Eine *(endlichstellige) Verknüpfung* ist eine n-stellige Verknüpfung für ein n. Wenn σ eine n-stellige Verknüpfung ist, setzen wir $\mathrm{ar}(\sigma) := n$.[5]

Eine Verknüpfung im Sinne der bisherigen Definition ist nach dieser Definition also eine 2-stellige Verknüpfung, die man auch *binäre Verknüpfung* nennt. Was den Sprachgebrauch betrifft, muss man etwas aufpassen: Normalerweise meint man mit einer Verknüpfung immer eine 2-stellige Verknüpfung. In der Theorie der Allgemeinen Algebra versteht man unter einer Verknüpfung allerdings eine beliebige endlichstellige Verknüpfung, und so verfahren wir auch in diesem Abschnitt.

Auch in der Allgemeinen Algebra bezeichnet man eine binäre Verknüpfung oft mittels eines "Verknüpfungssymbols" (z.B. "$\circ$", "$\cdot$", "$+$"), dass man zwischen die zu verknüpfenden Elemente schreibt. Man schreibt also nicht

[3] "Allgemeine Algebra" wird traditioneller Weise "Universelle Algebra" genannt. Im Englischen wird traditionell von "Universal Algebra" gesprochen, aber es kommt immer mehr auch die Bezeichnung "General Algebra" auf.

[4] Wie in der Vorlesung Lineare Algebra, bezeichne ich 0 nicht als natürliche Zahl.

[5] "ar" bezieht sich auf "arity" (Englisch für "Stelligkeit").

$+(x, y)$ sondern (wie gewohnt) $x + y$ für die Addition zweier Zahlen (z.B. in $\mathbb{Z}$).

Eine 0-stellige Verknüpfung auf X ist per Definition eine Abbildung $\{*\} \longrightarrow X$. Diese Abbildung ist durch die Angabe des Bildes von X eindeutig bestimmt, und umgehehrt kann man jedem $x \in X$ die Abbildung $\{*\} \longrightarrow X$, $* \mapsto x$ zuordnen. Mit anderen Worten, wir haben einen eine Bijektion

$$X \xrightarrow{\sim} \mathrm{Abb}(\{*\}, X),\ x \mapsto (* \mapsto x)$$

(siehe auch [LA, Beispiel 1.4].)

Es macht Sinn, eine nullstellige Verknüpfung mit dem Bild von $*$ in X "zu identifizieren", und so verfahren wir auch im Folgenden. Eine nullstellige Verknüpfung (bzw. die Elemente von X) heißen auch *Konstanten*.

Beachten Sie ferner, dass eine 1-stellige Verknüpfung nichts anderes als eine Abbildung $X \longrightarrow X$ ist. Man spricht auch von einer *unären Verknüpfung*.

Definition Ein *Typ von Algebren* ist eine Menge I zusammen mit Familie $(n_i)_{i\in I} \in \mathbb{N}_0^I$. (Zur Erinnerung: Eine "Familie" ist nichts anderes als eine Abbildung.)

Wir nennen die Menge I *(Verknüpfungs-)indexmenge* und die Familie $(n_i)_{i\in I} \in \mathbb{N}_0^I$ *Familie von Stelligkeiten*. Oftmals ist die Menge I gleich $\{1, \ldots, \ell\}$ für ein $\ell \in \mathbb{N}$. In diesem Fall kann man I in der Beschreibung weglassen und einfach das Tupel $(n_1, \ldots, n_\ell)$ angeben. Normalerweise wählt man die Stelligkeiten so, dass dann $n_1 \geq n_2 \geq \cdots \geq n_\ell$.

Es sind jedoch auch unendliche Indexmengen möglich.

Sei nun $\Omega = (I, (n_i)_{i\in I})$ ein Typ.

Definition Eine Ω-*Algebra* ist eine Menge A zusammen mit einer Familie $(\sigma_i)_{i\in I}$ von Verknüpfungen auf A so dass $\mathrm{ar}(\sigma_i) = n_i$ für alle $i \in I$.

Eine Ω-Algebra wird auch *Algebra* vom *Typ* Ω genannt. Wiederum muss man aufpassen, was den Sprachgebrauch betrifft: Außerhalb der Allgemeinen Algebra hat das Wort "Algebra" eine andere Bedeutung.

Wir bezeichnen eine Ω-Algebra $(A, (\sigma_i)_{i\in I})$ wieder mit A.Wie immer definieren wir gleich, was die entsprechenden Homomorphismen sind:

Definition Seien A, A' zwei Ω-Algebren. Dann ist ein *Homomorphismus von Ω-Algebren* von A nach A' eine Abbildung $\varphi : A \longrightarrow A'$ so dass für alle $i \in I$ gilt:

$$\forall a_1, \ldots, a_{n_i} \in A : \varphi(\sigma_i(a_1, \ldots, a_{n_i})) = \sigma_i(\varphi(a_1), \ldots, \varphi(a_{n_i}))$$

Bemerkung Die Bedingung an φ kann man auch so formulieren: Für alle $i \in I$ gilt $\varphi \circ \sigma_i = \sigma_i \circ (\overbrace{\varphi \times \cdots \times \varphi}^{n_i \text{ mal}}) : A^{\mathrm{ar}(i)} \longrightarrow A$.

Definition Seien A, A' wiederum Ω-Algebren, $\varphi : A \longrightarrow A'$ ein Homomorphismus. Dann ist φ ein *Isomorphismus*, wenn es einen Homomorphismus $\psi : A' \longrightarrow A$ mit $\psi \circ \varphi = \mathrm{id}_A$ und $\varphi \circ \psi = \mathrm{id}_{A'}$ gibt.

Bemerkung Ein Homomorphismus von Ω-Algebren ist genau dann ein Isomorphismus, wenn er bijektiv ist (Übungsaufgabe).

Beispiel 1.16 Nach den ursprünglichen Definitionen sind Halbgruppen, Monoide und Gruppe Algebren vom Typ (2). Nach der erneuerten Definition "im Sinne der allgemeinen Algebra" sind es jeweils Algebren vom Typ $(2), (2,0)$ bzw. $(2,1,0)$.

Bemerkung / Definition Sei A eine Ω-Algegra, und sei $B \subseteq A$ *abgeschlossen* unter allen Verknüpfungen. D.h.: Für alle $i \in I$ und alle $a_1, \ldots, a_{n_i} \in B$ gilt $\sigma_i(a_1, \ldots, a_{n_i}) \in B$. Dann ist B mit den *induzierten Verknüpfungen* $\sigma_i|_{B^{n_i}}$ eine Ω-Algebra, genannt eine Ω-*Unteralgebra* von A.

Bemerkung Sei σ_i eine 0-stellige Verknüpfung. Dann ist eine Teilmenge $B \subseteq A$ genau dann abgeschlossen unter σ_i, wenn $\sigma_i(*) \in B$.

Beispiel 1.17 Sei M ein Monoid. Wenn wir nun wie oben M als eine Algebra vom Typ $(2,1)$ betrachten, ergibt sich die Definition eines Untermonoids als ein Spezialfall der obigen Definition (siehe auch [LA]).

Dies gilt auch für Halbgruppen und Gruppen, aber bei Gruppen ist es egal, von welcher Definition man startet.

Bemerkung Sei A eine Ω-Algebra, und sei $\mathcal{B}$ eine Menge von Ω-Unteralgebren von A. Dann ist $\bigcap_{B \in \mathcal{B}} B$ eine Ω-Unteralgebra von A.

Bemerkung / Definition Sei A eine Ω-Algebra, und sei $X \subseteq A$ eine Teilmenge. Sei

$$\mathcal{B} := \{B \subseteq A \mid B \text{ ist } \Omega\text{-Unteralgebra von A mit } X \subseteq B\} .$$

Dann ist $\bigcap_{B \in \mathcal{B}} B$ die kleinste Ω-Unteralgebra von A, die X enthält; sie wird mit $\langle X \rangle$ bezeichnet und heißt die *von X erzeugte* Unteralgebra von A. Falls $\langle X \rangle = A$, sagen wir, dass A von X *erzeugt* wird.

(*Begründung*: Nach der obigen Bemerkung ist es eine Ω-Unteralgebra, und offensichtlich enthält sie auch alle andenen.)

Wir geben nun eine exlizite Beschreibung der von einer Menge erzeugten Unteralgebra.

Folgerung 1.18 *Sei A eine Ω-Algebra und sei $X \subseteq A$. Sei für $j \in \mathbb{N}_0$:*

$$S^{(0)} := X$$

$$S^{(j+1)} := S^{(j)} \cup \{\sigma_i(a_1, \ldots, a_{n_i}) \mid i \in I, a_1, \ldots, a_{n_i} \in S^{(j)}\} .$$

Dann ist $\langle X \rangle = \bigcup_{j=0}^{\infty} S^{(j)}$.

Beweis. Wir zeigen, dass $\bigcup_{j=0}^{\infty} S^{(j)}$ die kleinste Ω-Unteralgebra von A ist, die X enthält. Sicher enthält sie X. Außerdem ist sie abgeschlossen unter allen Verknüpfungen, also ist eine Ω-Unteralgebra.

Sei nun B eine beliebige Ω-Unteralgebra von A, die X enthält. Mit Induktion nach j sieht man sofort, dass $S^{(j)} \subseteq B$ für alle $j \in \mathbb{N}_0$. □

Folgerung 1.19 *Sei A eine Ω-Algebra, die von $X \subseteq A$ erzeugt wird, und sei B eine zweite Ω-Algebra. Sei $f : X \longrightarrow B$ eine Abbildung. Dann gibt es höchstens einen Homomorphismus $\varphi : A \longrightarrow B$ mit $\varphi(x) = f(x)$ für alle $x \in X$.*

Beweis. Seien φ, φ' zwei Homomorphismen wie in der Behauptung. Dann gilt per Induktion nach j: $\varphi(a) = \varphi'(a)$ für alle $x \in S^{(j)}$.

Dies ist richtig für $j = 0$ nach Voraussetzung. Der Induktionsschluss $j - 1 \curvearrowright j$ ist wie folgt:

Für $a \in S^{(j-1)}$ ist die Behaupung klar nach Induktionsvoraussetzung. Sei also $a \in S^{(j)} - S^{(j-1)}$. Dann gilt $a = \sigma_i(a_1, \ldots, a_{n_i})$ für ein $i \in I$ und $a_1, \ldots, a_{n_i} \in S^{(j-1)}$. Damit ist $\varphi(a) = \varphi(\sigma_i(a_1, \ldots, a_{n_i})) = \sigma_i(\varphi(a_1), \ldots, \varphi(a_{n_i})) = \sigma_i(\varphi'(a_1), \ldots, \varphi'(a_{n_i})) = \varphi'(\sigma_i(a_1, \ldots, a_{n_i}))$. □

Termalgebren

Definition Sei X eine Menge. Eine Ω-*Termalgebra* auf X ist eine Ω-Algebra $(T, (\sigma_i)_{i \in I})$ zusammen mit einer Inklusion $\iota : X \hookrightarrow T$ so dass gilt:

- T ist von $\iota(X)$ erzeugt.
- Für alle $t \in T$ gilt: *Entweder* es ist $t = \iota(x)$ für ein $x \in X$ *oder* es gibt ein $i \in I$ und $t_1, \ldots, t_{n_i} \in t$ mit $t = \sigma_i(t_1, \ldots, t_{n_i})$. Im zweiten Fall sind i und $t_1, \ldots, t_{n_i}$ *eindeutig* (durch t) *bestimmt*.

Wir zeigen nun, dass Termalgebren immer existieren und in einer gewissen Hinsicht "im Wesentlichen" eindeutig bestimmt sind.

Definition Sei weiterhin X eine Menge. Eine *freie* Ω-Algebra auf X ist eine Ω-Algebra $(F, (\sigma_i)_{i\in I})$ zusammen mit einer Abbildung $u : X \longrightarrow F$ so dass gilt:

Für alle Ω-Algebren A und alle Abbildungen $f : X \longrightarrow A$ gibt es genau einen Homomorphismus von Ω-Algebren $\varphi : F \longrightarrow A$ mit $\varphi \circ u = f$.

Bemerkung Eine Ω-Algebra F zusammen mit einer Abbildung $u : X \longrightarrow F$ ist also genau dann eine freie Ω-Algebra, wenn gilt: Für alle Ω-Algebren A ist der Homomorphismus

$$\mathrm{Hom}(F, A) \longrightarrow A^X = \mathrm{Abb}(X, A)\ ,\ \varphi \mapsto \varphi \circ u$$

bijektiv.

Bemerkung Die Eigenschaft in der Definition heißt auch *universelle Eigenschaft*. Es würde Sinn machen, freie Ω-Algebren "universelle Ω-Algebren" zu nennen. Leider wird aber in vielen Büchern über Allgemeine Algebra ("Universelle Algebra") *jede* Ω-Algebra auch "universelle Algebra" genannt.

Lemma 1.20 *Seien (F, u), (F, u') zwei freie Ω-Algebren auf X. Dann ist der eindeutig bestimmte Homomorphismus $\varphi : F \longrightarrow F'$ mit $\varphi \circ u = u'$ ein Isomorphismus.*

Beweis. Sei φ wie im Lemma, und sei $\psi : F' \longrightarrow F$ der eindeutig bestimmte Homomorphismus mit $\psi \circ u' = u$. Dann gilt $\psi \circ \varphi \circ u = u$ und natürlich auch $\mathrm{id}_F \circ u = u$. Somit ist (nach der definierenden Eigenschaft von F und u) $\psi \circ \varphi = \mathrm{id}_F$. Analog gilt $\varphi \circ \psi \circ u' = u'$ und somit $\varphi \circ \psi = \mathrm{id}_{F'}$. □

Satz 1.2 *Sei X eine Menge. Dann gilt:*

a) Es gibt eine Ω-Termalgebra auf X.

b) Jede Ω-Termalgebra auf X ist eine freie Algebra auf X.

c) Seien $(T, \iota), (T', \iota')$ zwei Ω-Termalgebren auf X. Dann gibt es einen eindeutig bestimmten Isomorphismus von Ω-Algebren $\varphi : T \longrightarrow T$ mit $\varphi \circ \iota = \iota'$.

Beweis. a) Wir setzen für $j \in \mathbb{N}_0$:

$$T^{(0)} := \{(*, x) \mid x \in X\}$$
$$T^{(j+1)} := T^{(j)} \cup \{(i, (t_1, \ldots, t_{n_i})) \mid i \in I, t_1, \ldots, t_{n_i} \in S^{(j)}\}$$

Wir setzen nun $T := \bigcup_{j=0}^{\infty} T^{(j)}$ und $\iota : X \longrightarrow T$ $x \mapsto (*, x)$, $\sigma_i : T^{n_i} \longrightarrow T$, $(t_1, \ldots, t_{n_i}) \mapsto (i, (t_1, \ldots, t_{n_i}))$.

Nun ist $(T, (\sigma_i)_{i \in I}$ eine Ω-Algebra. Es ist offensichtlich, dass die von $\iota(X)$ erzeugt wird. (Wir haben $S^{(j)} = T^{(j)}$ mit den Bezeichnungen von Folgerung 1.18.) Die zweite Bedingung ist offensichtlich auch erfüllt.

Sei nun T eine Termalgebra. (Beachten Sie: T muss nicht wie im Beweis von a) "konstruiert" sein.)

Sei A eine Ω-Algebra, und sei $f : X \longrightarrow A$ eine Abbildung. Nach Folgerung 1.19 wissen wir schon, dass es höchstens einen Homomorphismus $\varphi : T \longrightarrow A$ mit $\varphi \circ \iota = f$ gibt. Wir wollen einen Homomorphismus $\varphi : T \longrightarrow A$ mit $\varphi \circ \iota = f$ finden. Seien $S^{(j)} \subseteq T$ wie in Folgerung 1.18 für die Ω-Algebra T und die Menge X. Beachten Sie: Für $j > 0$ gilt nach Definition von $S^{(j)}$ und Voraussetzung an T: Für alle $t \in S^{(j)} - S^{(j-1)}$ gibt ein eindeutig bestimmtes $i \in I$ sowie eindeutig bestimmte $t_1, \ldots, t_{n_i} \in S^{(j-1)}$ mit $t = \sigma_i(t_1, \ldots, t_{n_i})$.

Wir definieren nun $\varphi_j : S^{(j)} \longrightarrow A$ $(j \in \mathbb{N}_0)$ induktiv wie folgt: $\varphi_0(\iota(x)) := f(x)$ für $x \in X$, sowie für $j > 0$: $\varphi_j(t) := \varphi_{j-1}(t)$ falls $t \in S^{(j-1)}$ sowie $\varphi_j(t) := \sigma_j(\varphi_{j-1}(t_1), \ldots, \varphi_{j-1}(t_{n_i}))$, falls $t \notin S^{(j-1)}$ und $t = \sigma_j(t_1, \ldots, t_{n_i})$.

Für $j < k$ gilt nun $\varphi_j|_{S^{(j)}} = \varphi_k$. Wir definieren nun $\varphi : T \longrightarrow A$ durch $\varphi(t) := \varphi_j(t)$ falls $t \in S^{(j)}$. (Dies hängt wie gesagt nicht von j ab.)

Der Definition ist φ nun ein Homomorphismus mit $\varphi \circ \iota = f$. □

Nach dem Satz sind Ω-Termalgebren "so eindeutig wie möglich". Es macht deshalb Sinn, zu definieren:

Definition Sei X eine Menge. Dann bezeichnen wir eine Ω-Termalgebra auf X mit $T_\Omega(X)$.

Bemerkung Sei X endlich, sagen wir $X = \{x_1, \ldots, x_n\}$ mit x_i paarweise verschieden. Dann macht es Sinn, Elemente in $T_\Omega(X)$ mit $t = t(x_1, \ldots, x_n)$ zu bezeichnen. Allgemeiner: Sei I eine "Indexmenge" und $I \longrightarrow X$, $i \mapsto x_i$ eine Bijektion. Dann macht es Sinn, $t = t((x_i)_{i \in I})$ zu schreiben. (Vergleiche die Ähnlichkeit zur Schreibweise von Polynomen.)

Durch Gleichungen definierte Objekte

Sei nach wie vor Ω ein Typ, und sei X eine Menge.

Definition Sei A eine Ω-Algebra. Sei $t \in T_\Omega(X)$, und sei $(a_x)_{x \in X} \in A^X$. Sei $\varphi : T_\Omega(X) \longrightarrow A$ die eindeutig bestimmte Abbildung mit $\varphi(x) = a_x$ für alle $x \in X$. Dann setzen wir $t((a_x)_{x \in X}) := \varphi(t)$.

Wenn $X = \{x_1, \ldots, x_n\}$ mit paarweise verschiedenen x_i, kann man auch definieren: Seien $a_1, \ldots, a_n \in A$, und sei $\varphi : T_\Omega(X) \longrightarrow A$ die eindeutig bestimmte Abbildung mit $\varphi(x_i) = a_i$ für alle $i = 1, \ldots, n$. Dann setzen wir $t(a_1, \ldots, a_n) := \varphi(t)$.

Definition Unter einer *Gleichung* bez. Ω über X verstehen wir ein Tupel $(s, t) \in T_\Omega(X)^2$. Dies schreiben wir auch in der Form $s \stackrel{\circ}{=} t$. (Wir führen das neue Symbol "$\stackrel{\circ}{=}$" ein, um zu verhindern, dass man die "Gleichung" "$s \stackrel{\circ}{=} t$" (d.h. das Tupel (s, t)) mit der Aussage verwechselt, dass der Term s gleich dem Term t ist). (Eine andere sinnvolle Schreibeise wäre $s \stackrel{!}{=} t$; man findet auch $s \approx t$ oder auch einfach $s = t$ in der Literatur.)

Definition Seien $s, t \in T_\Omega(X)$, und sei $(a_x)_{x \in X} \in A^X$. Dann sagen wir "$(a_x)_{x \in X} \in A^X$ erfüllt die Gleichung $s \stackrel{\circ}{=} t$", wenn $s((a_x)_{x \in X}) = t((a_x)_{x \in X})$. Die obigen Bemerkungen falls $X = \{x_1, \ldots, x_n\}$ gelten auch hier.

Beispiel 1.21 Sei $X = \{x_1, x_2, x_3\}$ eine Menge mit drei Elementen, und sei Ω gegeben durch das Tupel (2). (Jede Ω-Algebra hat genau eine Verknüpfung, und diese ist binär.) Wir schreiben die Verknüpfung σ_1 auf $T_\Omega(X)$ wie gewohnt mittels des Symbols "$\circ$". Sei nun A eine Ω-Algebra. Dann ist A genau dann eine Halbgruppe, wenn für alle $a_1, a_2, a_3 \in A$ gilt: (a_1, a_2, a_3) erfüllt die Gleichung $(x_1 \circ x_2) \circ x_3 \stackrel{\circ}{=} x_1 \circ (x_2 \circ x_3)$.

Bemerkung Man sollte allgemein die "Verknüpfungssymbole" für A und in $T_\Omega(X)$ "kompatibel" wählen. Ansonsten können die Aussagen sehr verwirrend sein.

Definition Sei nun A eine Ω-Algebra. Dann sagen wir, dass A "die Gleichung $t \stackrel{\circ}{=} s$ erfüllt", wenn gilt: Alle $(a_x)_{x \in X} \in A^X$ erfüllen die Gleichung $s \stackrel{\circ}{=} t$. Wir schreiben dann

$$A \vDash s \stackrel{\circ}{=} t \ .$$

Wenn Σ eine Menge von Gleichungen ist (beachten Sie die formale Definition von "Gleichung"), dann sagen wir, "A erfüllt Σ", wenn A alle Gleichungen in Σ erfüllt. Wir schreiben dann

$$A \vDash \Sigma \ .$$

Da Ω-Algebren frei sind, ist jeder Homomorphismus $\varphi : T_\Omega(X) \longrightarrow A$ von der Form $t \mapsto t((a_x)_{x \in X})$ für ein eindeutig bestimmtes $(a_x)_{x \in X}$. Damit gilt:

Lemma 1.22 *Es gilt genau dann $A \vDash s \mathrel{\hat{=}} t$, wenn für alle Morphismen $\varphi : T_\Omega(X) \longrightarrow A$ gilt: $\varphi(s) = \varphi(t)$.*

Beispiel 1.23 Sei Ω gegeben durch das Tupel $(2, 1, 0)$. Wir schreiben $\circ$ für die zweistellige Verknüpfung, ι für die einstellige Verknüpfung und e für die "Konstante" zur 0-stelligen Verknüpfung in $T_\Omega(X)$.

Sei nun A eine Ω-Algebra. Dann ist A genau dann eine Gruppe, wenn A die Gleichungen

$$(x \circ y) \circ z \mathrel{\hat{=}} x \circ (y \circ z)$$
$$e \circ x \mathrel{\hat{=}} x$$
$$\iota(x) \circ x \mathrel{\hat{=}} e$$

erfüllt. (Hier steckt eine nicht-triviale Aussage drin, nämlich, dass es auch-reicht, dass ein links-neutrales Element und links-Inverse zu fordern. Können Sie das beweisen?)

Mit anderen Worten: Sei

$$\Sigma := \{(x \circ y) \circ z \mathrel{\hat{=}} x \circ (y \circ z),\ e \circ x \mathrel{\hat{=}} x,\ \iota(x) \circ x \mathrel{\hat{=}} e\} \ .$$

Dann ist A genau dann eine Gruppe, wenn $A \vDash \Sigma$.

Definition Sei nun $\mathcal{K}$ eine Klasse[6] von Ω-Algebren, und sei Σ eine Menge von Gleichungen in $T_\Omega(X)$. Dann sagen wir, "$\mathcal{K}$ erfüllt Σ", wenn für alle A aus $\mathcal{K}$ gilt: $A \vDash \Sigma$. Wir schreiben dann

$$\mathcal{K} \vDash \Sigma \ .$$

Wenn Σ nur aus einer Gleichung $s \mathrel{\hat{=}} t$ besteht, schreiben wir dann auch

$$\mathcal{K} \vDash s \mathrel{\hat{=}} t \ .$$

Definition Sei $\mathcal{K}$ eine Klasse. Die *Menge der Identitäten* von $\mathcal{K}$ über X ist dann die Menge der Gleichungen, welche von $\mathcal{K}$ erfüllt werden:

$$\Sigma_{\mathcal{K}}(X) := \{s \mathrel{\hat{=}} t \in T_\Omega(X) \mid \mathcal{K} \vDash s \mathrel{\hat{=}} t\}$$

Bemerkung Per Definition ist $\Sigma_{\mathcal{K}}(X) \subseteq T_\Omega(X)^2$. Offensichtlich definiert $\Sigma_{\mathcal{K}}(X)$ eine Äquivalenzrelation. Es macht Sinn, hierfür $\mathrel{\hat{=}}_{\mathcal{K}}$ zu schreiben. Also: $s \mathrel{\hat{=}}_{\mathcal{K}} t \longleftrightarrow \forall A \in \mathcal{K} : A \vDash s \mathrel{\hat{=}} t$.

[6]Der Begriff der "Klasse" ist allgemeiner als der der Menge. Z.B. sollte man nicht von der "Menge aller Mengen" reden (siehe [LA]), aber es macht Sinn von der "Klasse aller Mengen" zu reden.

Definition Sei Σ eine Menge von Gleichungen. Dann ist die *durch* Σ *definierte Klasse* die Klasse der Ω-Algebren A mit $A \models \Sigma$. Die Klasse $\mathcal{K}$ heißt dann auch *durch* Σ *definiert* oder *axiomatisiert*. Man nennt $\mathcal{K}$ auch die *Varietät* zu Σ, Bezeichnung: $V(\Sigma)$. Wenn $\mathcal{K}$ durch irgendein Σ definiert ist, nennt man $\mathcal{K}$ auch einfach eine Varietät oder "durch Gleichungen definiert".

Satz 1.3 *(Birkhoff) Sei $\mathcal{K}$ eine Klasse von Ω-Algebren. Dann ist $\mathcal{K}$ genau dann eine Varietät, wenn gilt:*

- *Seien A und B Ω-Algebren mit $B \in \mathcal{K}$ und sei $\iota : A \longrightarrow B$ ein injektiver Homomorphismus. Dann ist auch $A \in \mathcal{K}$.*
- *Seien A und B Ω-Algebren mit $A \in \mathcal{K}$ und sei $p : A \longrightarrow B$ ein surjektiver Homomorphismus. Dann ist auch $B \in \mathcal{K}$.*
- *Sei I eine Menge und sei $(A_i)_{i \in I}$ eine Familie von Ω-Algebren in $\mathcal{K}$. Dann ist auch $\prod_{i \in I} A_i$ in $\mathcal{K}$.*

Zum Beweis. Es ist leicht zu zeigen, dass jede Varietät diese Eigenschaften hat. Die Umkehrung zeigen wir nicht.

Definition Sei weiterhin $\mathcal{K}$ eine Klasse von Ω-Algebren. Eine *freie Algebra* in $\mathcal{K}$ über X ist eine Ω-Algebra F in $\mathcal{K}$ zusammen mit einer Abbildung $u : X \longrightarrow F$ so dass gilt:

Für alle Ω-Algebren A und alle Abbildungen $f : X \longrightarrow A$ gibt es genau einen Homomorphismus von Ω-Algebren $\varphi : F \longrightarrow A$ mit $\varphi \circ u = f$.

Satz 1.4 *In jeder Varietät gibt es freie Algebren über X. Zwei solche Algebren sind "im wesentlichen eindeutig" wie in Lemma 1.20 beschrieben. Wenn (F, u) eine solche Algebra ist, dann ist der eindeutig bestimmte Homomorphismus $\varphi : T_\Omega(X) \longrightarrow F$ mit $\varphi \circ \iota = u$ surjektiv.*

Diese Aussage zeigen wir nicht.

Definition Wir bezeichnen eine freie Algebra von $\mathcal{K}$ über X mit $F_\mathcal{K}(X)$ und den eindeutig bestimmten Homomorphismus $\varphi : T_\Omega(X) \longrightarrow F_\mathcal{K}(X)$ mit $\varphi \circ \iota = u$ mit π. Wenn t ein Term über X ist, setzen wir $\overline{t} := \pi(t)$.

Definition Sei Σ eine Menge von Gleichungen (wie immer über X), und seien s, t Terme. Dann sagen wir, dass $s \stackrel{\circ}{=} t$ aus Σ *folgt*, wenn $V(\Sigma) \models s \stackrel{\circ}{=} t$, d.h. wenn für alle $A \in V(\Sigma)$ gilt: $A \models s \stackrel{\circ}{=} t$. Wir schreiben dann:

$$\Sigma \models s \stackrel{\circ}{=} t$$

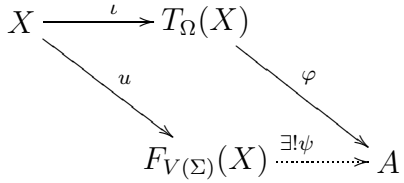
Folgerung 1.24 *Sei Σ eine Menge von Gleichungen, und sei $s \stackrel{\circ}{=} t$ eine Gleichung. Dann sind äquivalent:*

- $\Sigma \vDash s \stackrel{\circ}{=} t$
- $\overline{s} = \overline{t} \in F_{V(\Sigma)}(X)$

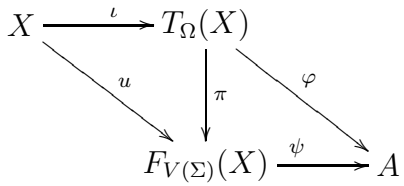
Beweis. Es gelte $\Sigma \vDash s \stackrel{\circ}{=} t$. Dann gilt insbesondere $F_{V(\Sigma)}(X) \vDash s \stackrel{\circ}{=} t$. Mit anderen Worten: Für alle Morphismen $\varphi : T_\Omega(X) \longrightarrow F_{V(\Sigma)}(X)$ gilt: $\varphi(s) = \varphi(t)$. Damit gilt insbesondere $\overline{s} = \overline{t}$.

Es gelte nun $\overline{s} = \overline{t} \in F_{V(\Sigma)}(X)$. Sei A eine beliebige Ω-Algebra in $\mathcal{K}$. Wir müssen zeigen: Für alle Morphismen $\varphi : T_\Omega(X) \longrightarrow A$ gilt: $\varphi(s) = \varphi(t)$.

Sei also $\varphi : T_\Omega(X) \longrightarrow A$ so ein Homomorphismus. Dann gibt es per Definition von $F_{V(\Sigma)}(X)$ genau einen Homomorphismus $\psi : F_{V(\Sigma)}(X) \longrightarrow A$ mit $\psi \circ u = \varphi \circ \iota$.



Ich behaupte, dass nun auch $\varphi = \psi \circ \pi$ gilt. Hierzu: Es gilt $\varphi \circ \iota = \psi \circ u = \psi \circ (\pi \circ \iota) = (\psi \circ p) \circ \iota$. Damit ist, da $T_\Omega(X)$ frei auf X ist, $\varphi = \psi \circ \pi$.



Wir haben also $\varphi(s) = \psi(\overline{s}) = \psi(\overline{t}) = \varphi(t)$. □

Beispiele 1.25

- Die freie Algebra über X zu allen Ω-Algebren ist die Term-Algebra $T_\Omega(X)$ (s.o.).
- Das freie Monoid über X ist die Menge der "Strings" X^* (mit der offensichtlichen Inklusion) (das neutrale Element ist das "leere Wort" $\Box$).
- Die freie Halbgruppe über X ist $X^* - \{\Box\}$.

- Die freie Gruppe über X kann man explizit wie folgt beschreiben: Wir fixieren eine von X disjunkte Menge, die wir mit X^{-1} bezeichnen und eine Bijektion $X \longrightarrow X^{-1}\,, x \mapsto x^{-1}$. Dann betrachten wir die Teilmenge von $(X \cup X^{-1})^*$, die aus Strings besteht so dass gilt: Es kommt niemals ein Element x direkt neben einen Element x^{-1} for. Zwei Elemente werden verknüpft, indem man sie hintereinanderschreibt und ann in offensichtlicher Weise "kürzt". Diese Teilmenge ist dann die freie Gruppe auf X. (Das neutrale Element ist wieder das leere Wort.) (Wie lauten die inversen Elemente?)

Sei ab jetzt $X = \{x_1, x_2, x_3, \ldots\}$ mit paarweise verschiedenen x_i.

Wenn nun Σ endlich ist, könnte man versuchen, die Menge der Identitäten auf $V(\Sigma)$ algorithmisch zu bestimmen. (Diese Idee ist noch sehr allgemein umd muss präzisiert werden.) Hierzu ist es naheliegend, formale Beweisschemata zu betrachten.

Definition Sei Σ eine Menge von Gleichungen, und sei $s \stackrel{\circ}{=} t$ eine Gleichung über X vom Typ Ω. Dann sagen wir, dass $s \stackrel{\circ}{=} t$ *in einem Schritt aus* Σ *(formal) abgeleitet* oder *in einem Schritt aus* Σ *(formal) abgeleitet hergeleitet* oder *in einem Schritt aus* Σ *deduziert* werden kann, wenn (mindestens) eine der folgenden Bedingungen erfüllt ist:

- $s = t \in T_\Omega(X)$ (gemeint ist hier wirklich die Gleichheit von Termen)
- $t \stackrel{\circ}{=} s \in \Sigma$
- Es gibt ein $r \in T_\Omega(X)$ mit $s \stackrel{\circ}{=} r \in \Sigma$ und $r \stackrel{\circ}{=} t \in \Sigma$.
- Es gibt $p \stackrel{\circ}{=} q \in \Sigma$, einen Term r und ein $i \in \mathbb{N}$ so dass gilt: Wenn man in r die Variable x_i durch p ersetzt, erhält man s, wenn man in r die Variable x_i durch q ersetzt, erhält man t.
- Es gibt $p \stackrel{\circ}{=} q \in \Sigma$, einen Term r und ein $i \in \mathbb{N}$ so dass gilt: Wenn man in p die Variable x_i durch r ersetzt, erhält man s, wenn man in q die Variable x_i durch r ersetzt, erhält man t.

Definition Sei Σ eine Menge von Gleichungen über X, und sei $s \stackrel{\circ}{=} t$ eine Gleichung. Dann sagen wir, dass $s \stackrel{\circ}{=} t$ aus Σ *(formal) abgeleitet* oder *hergeleitet* oder *deduziert* werden kann, wenn es eine endliche Folge

$$s_1 \stackrel{\circ}{=} t_1,\ s_2 \stackrel{\circ}{=} t_2, \ldots, s_n \stackrel{\circ}{=} t_n \tag{1.1}$$

von Gleichungen mit $s_n = s$ und $t_n = t$ gibt, so dass jede der Gleichungen $s_i \stackrel{\circ}{=} t_i$ aus der Menge $\Sigma \cup \{s_1 \stackrel{\circ}{=} t_1, \ldots, s_{i-1} \stackrel{\circ}{=} t_{i-1}\}$ in einem Schritt formal hergeleitet werden kann. Die endliche Folge (1.1) nennen wir dann auch eine *formale Herleitung* oder eine *formale Ableitung* oder einen *formalen Beweis* von $s \stackrel{\circ}{=} t$ aus Σ.

In diesem Fall schreiben wir

$$\Sigma \vdash s \stackrel{\circ}{=} t \; .$$

Nun gilt der folgende Satz:

Satz 1.5 *(Vollständigkeitssatz) Sei Σ eine Menge von Gleichungen auf $X = \{x_1, x_2, x_3, \ldots\}$, und sei $s \stackrel{\circ}{=} t$ eine Gleichung auf X. Dann sind äquivalent:*

- $\Sigma \models s \stackrel{\circ}{=} t$
- $\Sigma \vdash s \stackrel{\circ}{=} t$
- $\overline{s} = \overline{t} \in F_{V(\Sigma)}(X)$

Zum Beweis. Man sieht schnell, dass alle Gleichungen, die aus Σ formal abgeleitet werden können, auch aus Σ folgen. (Mit anderen Worten: Wenn $s \stackrel{\circ}{=} t$ aus Σ formal abgeleitet werden kann und A die Gleichungsmenge Σ erfüllt, dann erfüllt A auch $s \stackrel{\circ}{=} t$.) Der schwierige Teil des Beweises ist, die Umkehrung dieser Aussage zu zeigen. Aber diesen Beweis führen wir nicht. Die Äquivalenz des ersten und des dritten Punktes ist Folgerung 1.24. □

Hieraus folgt relativ schnell:

Korollar 1.26 *Es gibt eine "Prozedur" (eine Turing Maschine), die unter Eingabe eines "endlichen" Typs, einer endlichen Menge von Gleichungen Σ auf X bezüglich Ω alle Gleichungen $s \stackrel{\circ}{=} t$, mit $\Sigma \models s \stackrel{\circ}{=} t$ und nur solche ausgibt. (Die Maschine terminiert nicht.)*

Mit anderen Worten: Es gibt eine "Prozedur" (eine Turing Maschine), die unter Eingabe eines "endlichen" Typs Ω, einer endlichen Menge von Gleichungen Σ auf X bezüglich Ω und einer Gleichung $s \stackrel{\circ}{=} t$ genau dann terminiert, wenn $\Sigma \models s \stackrel{\circ}{=} t$.

Es gibt aber keinen Algorithmus, der dieses Problem entscheidet, d.h. der immer terminiert und die korrekte Antwort "Ja", "Nein" ausgibt. Es gilt sogar der folgende berühmte Satz:

Satz 1.6 *Es gibt einen endlichen Typ Ω und eine endliche Menge von Gleichungen Σ so dass es keinen Algorithmus (keine Turing Maschine) gibt, welche unter Eingabe einer Gleichung $s \stackrel{\circ}{=} t$ mit Termen in $T_\Omega(\emptyset)$ ausgibt, ob $\Sigma \vDash s \stackrel{\circ}{=} t$.*

Stichwort: "Wortproblem" für endlich dargestellte Gruppen oder für endlich dargestellte Halbgruppen.

Literatur Wenn Sie sich wirklich für das Themengebiet interessieren, finden Sie vielleicht die folgenden Texte interessant:

Bergman: An Invitation to General Algebra and Universal Constructions (http://math.berkeley.edu/∼gbergman/245)

Burris, Sankappanavar: A Course in Universal Algebra (Signatur Alg 1 82 in der Bibliothek)

Grätzer: Universal Algebra (Signatur Alg 1 39 in der Bibliothek)

Wechler: Universal Algebra for Computer Scientists (Signatur ST 120 W386 in der Bibliothek)

Ich persönlich finde das Buch von Herrn Bergman am besten. Ich möchte noch anmerken, das die Definition von "Typ" in der Vorlesung formal ein Spezialfall der Definition von Herrn Bergman ist. Aber die Darstellung ist in der Vorlesung eine leicht andere ...