Abgeschlossenheit

Definition 54

Sei $\langle S, \Phi \rangle$ eine Algebra, T eine Teilmenge von S.

- T ist unter den Operatoren in Φ abgeschlossen (stabil), falls ihre Anwendung auf Elemente aus T wieder Elemente aus T ergibt.
- $\langle T, \Phi \rangle$ heißt Unteralgebra von $\langle S, \Phi \rangle$, falls $T \neq \emptyset$ und T unter den Operatoren $\in \Phi$ abgeschlossen ist.

Beispiel 55

- $\langle \mathbb{N}_0, + \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \ \cdot \ \rangle$ ist Unteralgebra von $\langle \mathbb{N}_0, \ \cdot \ \rangle$
- $\langle \{0, 1\}, + \rangle$ ist keine Unteralgebra von $\langle \mathbb{Z}, + \rangle$, da sie nicht abgeschlossen ist $(1 + 1 = 2)$.

2. Morphismen

Seien $A = \langle S, \Phi \rangle$ und $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$ zwei Algebren mit derselben Signatur.

2.1 Isomorphismus

Definition 56

Eine Abbildung

$$h : S \to \tilde{S}$$

heißt ein Isomorphismus von A nach $\tilde{A}$, falls

- h bijektiv ist und
- h mit den in Φ und $\tilde{\Phi}$ einander entsprechenden Operatoren vertauschbar ist (kommutatives Diagramm):

$$\begin{array}{ccc} S^m & \xrightarrow{\circ} & S \\ {\scriptstyle (h,\ldots,h)}\big\downarrow & & \big\downarrow{\scriptstyle h} \\ \tilde{S}^m & \xrightarrow{\tilde{\circ}} & \tilde{S} \end{array}$$

h ist also ein Isomorphismus gdw

- $h(c) = \tilde{c}$ für alle nullstelligen Operatoren (Konstanten) c
- $h\big(u(x)\big) = \tilde{u}\big(h(x)\big)$ für alle unären Operatoren $u \in \Phi$, $\forall x \in S$
- $h\big(b(x,y)\big) = \tilde{b}\big(h(x), h(y)\big)$ für alle binären Operatoren $b \in \Phi$, $\forall x, y \in S$
- usw.

Notation: $A \cong \tilde{A}$: „A isomorph zu $\tilde{A}$“, d. h. es existiert ein Isomorphismus von A nach $\tilde{A}$ (und von $\tilde{A}$ nach A).

Ein Isomorphismus von A nach A heißt Automorphismus.

Zur Vereinfachung der Notation schreiben wir statt $\langle S, \{o_1, \ldots, o_k\}\rangle$ auch

$$\langle S, o_1, \ldots, o_k \rangle \ ,$$

solange keine Verwechslung zu befürchten ist.

Beispiel 57

$\langle \mathbb{N}_0, + \rangle$ und $\langle 2 \cdot \mathbb{N}_0, + \rangle$ ($2 \cdot \mathbb{N}_0$: gerade Zahlen) mit

$$h : \mathbb{N}_0 \ni n \mapsto 2 \cdot n \in 2\mathbb{N}_0$$

ist ein Isomorphismus zwischen den beiden Algebren.

Beispiel 58

$\langle \mathbb{R}^+, \cdot \rangle$ und $\langle \mathbb{R}, + \rangle$ $\left(\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}\right)$

$$h : \mathbb{R}^+ \ni x \mapsto \log x \in \mathbb{R}$$

ist ein Isomorphismus (der sog. Rechenschieberisomorphismus)

Satz 59

Ein Algebra-Isomorphismus bildet Einselemente auf Einselemente, Nullelemente auf Nullelemente und Inverse auf Inverse ab.

Beweis:

Sei die Abbildung $h : S \to \tilde{S}$ ein Isomorphismus von $A = \langle S, \Phi \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$. Sei 1 ein rechtes Einselement für den Operator $\circ \in \Phi$ in A. Dann gilt für alle $\tilde{b} \in \tilde{S}$:

$$\tilde{b} \tilde{\circ} h(1) = h(b) \tilde{\circ} h(1) = h(b \circ 1) = h(b) = \tilde{b}$$

Also ist $h(1)$ ein rechtes Einselement in $\tilde{A}$. Die Argumentation für linke Einselemente, Nullelemente und Inverse ist analog. □

2.2 Homomorphismus

Definition 60

Eine Abbildung

$$h\colon S \to \tilde{S}$$

heißt ein Homomorphismus von A nach $\tilde{A}$, falls h mit den in Φ und $\tilde{\Phi}$ einander entsprechenden Operatoren vertauschbar ist.

Beispiel 61

$\langle \mathbb{N}_0, + \rangle$ und $\tilde{A} = \langle \mathbb{Z}_m, +_{(m)} \rangle$ mit $+_{(m)}$ als Addition modulo m.

$$h\colon \mathbb{N}_0 \ni n \mapsto n \bmod m \in \mathbb{Z}_m$$

ist ein (surjektiver) Homomorphismus ($\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$).

Beispiel 62

$\langle \Sigma^*, \circ \rangle$ und $\langle \mathbb{N}_0, + \rangle$ mit Σ^* Menge der endlichen Zeichenreihen über dem Alphabet Σ.

$$h\colon \Sigma^* \ni \sigma \mapsto |\sigma| \in \mathbb{N}_0$$

mit $|\sigma|$ der Länge der Zeichenreihe ist ein Homomorphismus.

Satz 63

Sei h ein Homomorphismus von $A = \langle S, \Phi \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$. Dann ist $\langle h(S), \tilde{\Phi} \rangle$ eine Unteralgebra von $\tilde{A}$.

Beweis:

Offensichtlich. $\square$

3. Halbgruppen

Definition 64

Eine Halbgruppe ist eine Algebra $\langle S, \circ \rangle$ mit einem assoziativen binären Operator $\circ$, d. h. für alle $a, b, c \; \in S$ gilt:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

Beispiel 65

$\langle \Sigma^*, \circ \rangle$: Menge der endlichen Zeichenreihen über dem Alphabet Σ, mit Konkatenation als $\circ$.

Beispiel 66

$S \subseteq \mathbb{R}$, $\langle S, \max \rangle$: Da die Maximumbildung assoziativ ist, ist $\langle S, \max \rangle$ eine Halbgruppe.

Beispiel 67

$\langle\{b,c\},\circ\rangle$ mit

$\circ$	b	c
b	b	b
c	c	c

Auch diese Operation ist assoziativ.

Beweis:

$$\begin{aligned}
c = c\circ(c\circ c) &= (c\circ c)\circ c = c\\
b = b\circ(c\circ c) &= (b\circ c)\circ c = b\\
c = c\circ(b\circ c) &= (c\circ b)\circ c = c\\
c = c\circ(c\circ b) &= (c\circ c)\circ b = c\\
b = b\circ(b\circ b) &= (b\circ b)\circ b = b\\
c = c\circ(b\circ b) &= (c\circ b)\circ b = c\\
b = b\circ(c\circ b) &= (b\circ c)\circ b = b\\
b = b\circ(b\circ c) &= (b\circ b)\circ c = b
\end{aligned}$$

$\square$

3.1 Unterhalbgruppen

Definition 68

Sei $\langle S, \circ \rangle$ eine Halbgruppe, $\emptyset \neq T \subseteq S$. $\langle T, \circ \rangle$ heißt Unterhalbgruppe, falls es eine Unteralgebra ist.

3.2 Abelsche Halbgruppen

Definition 69

Eine Halbgruppe $\langle S, \circ \rangle$ heißt abelsch, falls $\circ$ symmetrisch (kommutativ) ist. Also

$$a \circ b = b \circ a \quad \forall a, b \in S\,.$$

Abelsche (Halb-)Gruppen sind nach Nils H. Abel (1802–1829) benannt.

4. Monoide

Definition 70

Ein Monoid $\langle S, \circ, 1\rangle$ ist eine Halbgruppe $\langle S, \circ\rangle$ mit (linkem und rechtem) Einselement 1. Eine Algebra $\langle T, \circ\rangle$, $T \subseteq S$ heißt Untermonoid von $\langle S, \circ, 1\rangle$, wenn $\langle T, \circ\rangle$ eine Halbgruppe mit Einselement ist.

Beispiel 71

$\langle \mathbb{N}_0, \max\rangle$ ist ein Monoid mit 0 als Einselement, ein Untermonoid davon ist $\langle \{0, 1\}, \max\rangle$.

Beispiel 72

$\langle \Sigma^*, \circ\rangle$, mit $\circ$ Konkatenation von Zeichenreihen und der leeren Zeichenreihe ε als Einselement ist ein Monoid.

5. Gruppen

5.1 Grundlagen

Definition 73

Eine Gruppe ist eine Algebra $\langle S, \circ, 1 \rangle$ mit folgenden Eigenschaften:

- Der Operator $\circ$ ist assoziativ.
- 1 ist Einselement $\in S$.
- Für jedes $b \in S$ existiert $b^{-1} \in S$ mit

$$b \circ b^{-1} = 1 = b^{-1} \circ b$$

(Existenz des Inversen).
Beachte: Das Zeichen „1“wird hier in zwei (i.a.) verschiedenen Bedeutungen gebraucht, nämlich als Zeichen für das Einselement $\in S$ und (im Exponenten „-1“) als Zeichen für die natürliche Zahl $1 \in \mathbb{N}$.

Beispiel 74

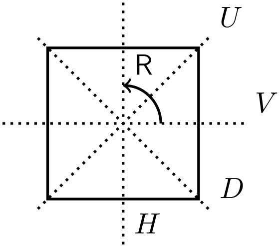
$\langle \mathbb{Z}_n, +_{(n)}, 0 \rangle$ ist nicht Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, da $+_{(n)}$ nicht die Restriktion (Einschränkung) von $+$ auf $\mathbb{Z}_n$ ist. Beide sind aber Gruppen.

Beispiel 75

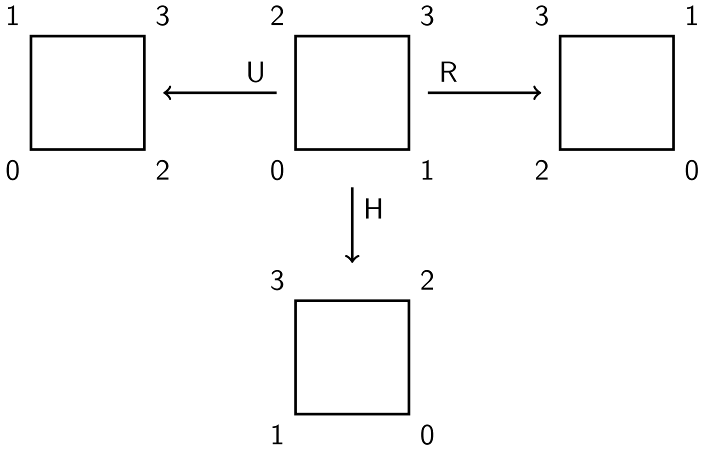
$\langle \mathbb{R}, \ \cdot \ , 1 \rangle$ oder $\langle \mathbb{Q}, \ \cdot \ , 1 \rangle$ sind keine Gruppen! Zu dem Element $0 \in \mathbb{Q}$ gibt es kein inverses Element.
$\langle \mathbb{R} \setminus \{0\}, \ \cdot \ , 1 \rangle$ bzw. $\langle \mathbb{Q} \setminus \{0\}, \ \cdot \ , 1 \rangle$ sind Gruppen.

Beispiel 76

Automorphismengruppe des Quadrats
$\circ$ ist die Komposition von Abbildungen



I identische Abbildung,
R Rotation um 90° gegen den Uhrzeigersinn
H horizontale Spiegelung, V vertikale Spiegelung,
D Spiegelung an der fallenden Diagonale, U Spiegelung an der steigenden.



Die Abbildungen $I, R, R^2, R^3, H, V, D, U$ bilden die Automorphismengruppe des Quadrats.

Verknüpfungstafel:

$\circ$	I	R	R^2	R^3	H	V	D	U
I	I	R	R^2	R^3	H	V	D	U
R	R	R^2	R^3	I	D	U	V	H
R^2	R^2	R^3	I	R	V	H	U	D
R^3	R^3	I	R	R^2	U	D	H	V
H	H	U	V	D	I	R^2	R^3	R
V	V	D	H	U	R^2	I	R	R^3
D	D	H	U	V	R	R^3	I	R^2
U	U	V	D	H	R^3	R	R^2	I

Satz 77

Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt:

- *für alle $a \in S$: $a = \left(a^{-1}\right)^{-1}$ (Involutionsgesetz)*
- *für alle $a, a', b \in S$ (Kürzungsregel):*

$$\begin{aligned} a \circ b = a' \circ b \quad &\Rightarrow \quad a = a' \\ b \circ a = b \circ a' \quad &\Rightarrow \quad a = a' \end{aligned}$$

- *für alle $a, x, b \in S$ (eindeutige Lösbarkeit linearer Gleichungen):*

$$\begin{aligned} a \circ x = b \quad &\Longleftrightarrow \quad x = a^{-1} \circ b \\ x \circ a = b \quad &\Longleftrightarrow \quad x = b \circ a^{-1} \end{aligned}$$

- *für alle $a, b, c \in S$ (Injektivität der Operation $\circ$):*

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- *für alle $a, b \in S$ (Surjektivität der Operation $\circ$):*

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

Beweis:

Wir beweisen lediglich: $a \circ c = b \circ c \iff a = b$. Rest: Übung

$\Leftarrow$: Dass

$$a = b \Rightarrow a \circ c = b \circ c$$

gilt, ist offensichtlich.

$\Rightarrow$: Sei $a \circ c = b \circ c$.

$$\begin{aligned} b &= b \circ \left(c \circ c^{-1}\right) = (b \circ c) \circ c^{-1} \overset{\text{n. V.}}{=} (a \circ c) \circ c^{-1} \\ &= a \circ \left(c \circ c^{-1}\right) = a \end{aligned}$$

$\square$

5.2 Potenzen

Definition 78

Sei $\langle S, \circ, 1\rangle$ eine Gruppe, $a \in S$. Man definiert:

1. $a^0 := 1$
2. $a^n := a \circ a^{n-1} = a^{n-1} \circ a \quad \forall n \geq 1$
3. $a^{-n} := \left(a^{-1}\right)^n$

Satz 79

Sei $\langle S, \circ, 1\rangle$ *eine Gruppe. Dann gilt für alle* $m, n \in \mathbb{Z}$, $a \in S$:

1. $a^m \circ a^n = a^{m+n}$
2. $\left(a^n\right)^m = a^{m \cdot n}$
3. $a^m = a^n \iff a^{m-n} = 1$

Beweis:

Übung! $\square$

5.3 Ordnung eines Gruppenelements

Definition 80

Sei $G = \langle S, \circ, 1\rangle$ eine Gruppe mit dem Einselement 1. Sei $a \in G$ (genauer: $a \in S$) ein Gruppenelement, $a \neq 1$. Dann ist die Ordnung $\operatorname{ord}(a)$ von a das minimale $r \in \mathbb{N}$, so dass

$$a^r = 1\,.$$

Falls kein solches r existiert, dann ist $\operatorname{ord}(a) := \infty$. Falls gewünscht, kann man auch $\operatorname{ord}(1) := 1$ definieren.

Beispiel 81

$\langle \mathbb{Z}, +, 0\rangle$: ord$(1) = \infty$.

Satz 82

Sei G eine endliche Gruppe; dann hat auch jedes Element in G endliche Ordnung.

Beweis:

Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \qquad a \in G \text{ beliebig } \neq 1$$

Also gibt es (pigeon hole principle) minimale k und j, $0 \leq j \leq k-1$, so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da k minimal gewählt wurde, folgt $j = 0$ und $\mathrm{ord}(a) = k$. □

Beispiel 83

Betrachte $\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12