

WS 2005/06

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2005WS/ds/index.html.de>

11. November 2005

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 53

Eine Abbildung

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

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**):

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

h ist also ein Isomorphismus gdw

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

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 $\langle S, \{o_1, \dots, o_k\} \rangle$ auch

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

solange keine Verwechslung zu befürchten ist.

Beispiel 54

$\langle \mathbb{N}_0, + \rangle$ 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 55

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

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

ist ein Isomorphismus (der sog. **Rechenschieberisomorphismus**)

Satz 56

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

Beweis:

Sei die Abbildung $h : S \rightarrow \tilde{S}$ 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 $\tilde{b} \in \tilde{S}$:

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

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

2.2 Homomorphismus

Definition 57

Eine Abbildung

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

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

Beispiel 58

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

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

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

Beispiel 59

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

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

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

Satz 60

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. □

3. Halbgruppen

Definition 61

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 62

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

Beispiel 63

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

Beispiel 64

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

\circ	b	c
b	b	b
c	c	c

Auch diese Operation ist assoziativ.

Beweis:

$$c = c \circ (c \circ c) = (c \circ c) \circ c = c$$

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

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

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

$$b = b \circ (b \circ b) = (b \circ b) \circ b = b$$

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

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

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



3.1 Unterhalbgruppen

Definition 65

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 66

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

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

4. Monoide

Definition 67

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 68

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

Beispiel 69

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

5. Gruppen

5.1 Grundlagen

Definition 70

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).

Beispiel 71

$\langle \mathbb{Z}_n, +_{(n)}, 0 \rangle$ 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 72

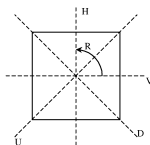
$\langle \mathbb{R}, \cdot, 1 \rangle$ oder $\langle \mathbb{Q}, \cdot, 1 \rangle$ sind keine Gruppen! Zu dem Element $0 \in \mathbb{Q}$ gibt es kein inverses Element.

$\langle \mathbb{R} \setminus \{0\}, \cdot, 1 \rangle$ bzw. $\langle \mathbb{Q} \setminus \{0\}, \cdot, 1 \rangle$ sind Gruppen.

Beispiel 73

Automorphismengruppe des Quadrats

○ ist die **Komposition** von Abbildungen

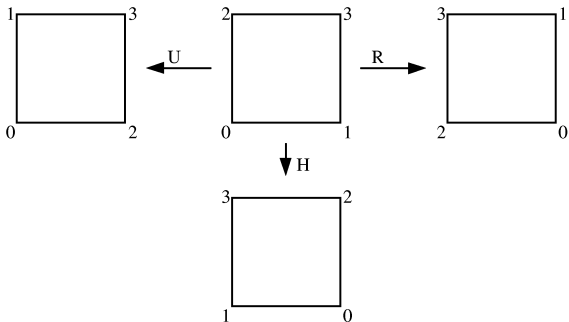


I identische Abbildung,

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 74

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

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

$$a \circ b = a' \circ b \Rightarrow a = a'$$

$$b \circ a = b \circ a' \Rightarrow a = a'$$

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

$$a \circ x = b \iff x = a^{-1} \circ b$$

$$x \circ a = b \iff x = b \circ a^{-1}$$

- 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 $a \circ c = b \circ c$.

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

□

5.2 Potenzen

Definition 75

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 $a^{-n} := (a^{-1})^n$

Satz 76

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 $(a^n)^m = a^{m \cdot n}$
- 3 $a^m = a^n \iff a^{m-n} = 1$

Beweis:

Übung!



5.3 Ordnung eines Gruppenelements

Definition 77

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** $\text{ord}(a)$ von a das minimale $r \in \mathbb{N}$, so dass

$$a^r = 1.$$

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

Beispiel 78

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

Satz 79

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

Beweis:

Betrachte die Abbildung

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

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 $\text{ord}(a) = k$. □

Beispiel 80

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

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

5.4 Untergruppen

Definition 81

Eine Unteralgebra $\langle T, \circ, 1 \rangle$ einer Gruppe $G = \langle S, \circ, 1 \rangle$ heißt **Untergruppe** von G , falls $\langle T, \circ, 1 \rangle$ eine Gruppe ist.

Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel 82

$\langle \mathbb{N}_0, +, 0 \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0 \rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz 83

Eine Unteralgebra (bzgl. \circ) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis:

Folgt sofort aus der Definition. □

Satz 84

Jede Unteralgebra (bzgl. \circ) einer *endlichen* Gruppe ist eine Untergruppe.

Beweis:

Sei $\langle T, \circ, 1 \rangle$ eine Unteralgebra einer endlichen Gruppe $\langle S, \circ, 1 \rangle$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\text{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \text{ord}(b)$. Dann gilt:

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

d. h. $b^{m-1} \in T$ ist das Inverse zu b . □