Algebraische Srukturen

Monide, Gruppen, Ringe
Basisdefinitionen

M.B. Wischnewsky

15.12.2006

Algebraische Strukturen

	Natürliche Zahlen N	Ganze Zahlen Z	Rationale Zahlen Q	Reelle Zahlen R	Komplexe Zahlen C
Monoid*	*	*	*	*	*
Gruppe		*	*	*	*
Ring		*	*	*	*
Körper			*	*	*

* = Halbgruppe

Monide, Gruppen, Ringe, Körper

Definition 1.1.

(i) Eine Verknüpfung T auf einer Menge A ist eine Abbildung

$$T : A \times A \to A$$
$$(a, b) \to a\,T\,b\,,$$

die jedem geordneten Paar (a, b) von Elementen a, b der Menge A ein weiteres Element $(a\,T\,b) \in A$ zuordnet.

(ii) Eine Verknüpfung T heißt assoziativ, wenn gilt

$$aT\,(bT\,c) = (aT\,b)Tc \quad \text{für alle } a, b, c \in A.$$

(iii) Die Verknüpfung heißt kommutativ oder abelsch genau dann, wenn gilt $aT\,b = bT\,a$ für alle $a, b \in A$.

Ist eine Verknüpfung assoziativ, so liefern Ausdrücke der Form $a_1T\,a_2\,\ldots T\,a_n$ wohlbestimmte Elemente von A, das Resultat ist unabhängig davon, wie man die Klammern setzt.

Monide, Gruppen, Ringe, Körper

Definition 1.1.1. (Verallgemeinerung) Sei $n \in N_0$

(i) Eine **n-stellige (innere) Verknüpfung** T auf einer Menge A ist eine Abbildung

$$T : A^n \rightarrow A$$

$$(a_1, \ldots, a_n) \rightarrow T(a_1, \ldots, a_n)$$

die jedem n-Tupel $(a_1, \ldots, a_n)$ von Elementen $a_1, \ldots, a_n$ der Menge A ein weiteres Element $T(a_1, \ldots, a_n) \in A$ zuordnet.

(ii) Eine Menge A zusammen mit einer Menge von n_i-stelligen Verknüpfungen $T_1, \ldots, T_k$ auf A

$(n_i \in N_0, i=1,\ldots,k)$ ist eine **algebraische Sruktur.**

Monide, Gruppen, Ringe, Körper

Definition 1.2

Es seien **M** eine nichtleere Menge und **T** eine binäre Verknüpfung **T** : M x M → M

Man nennt (M, **T**) eine **Monoid oder Halbgruppe**, wenn gilt:

M1) (M, **T**) ist **assoziativ**, d.h.

$\forall$ **a,b, c**$\in$**M: (aTb) Tc = aT (bTc)**

Gibt es zusätzlich ein Element **e**$\in$**M mit**

M2) $\forall$ **a** $\in$**M: eTa=aTe=a**

so heißt e ist ein **neutrales Element**:

Beispiel: (**N**,+), (**N**,*) sind Halbgruppen.

$M = \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Addition $+ : M \times M \longrightarrow M$

$(x,y) \longmapsto x+y$

Multiplikation $* : M \times M \longrightarrow M$

$(x,y) \longmapsto x*y$

1) $(M,+)$ ist ein Monoid mit Einselement 0

d.h. a) $\forall_{x,y,z \in M}$ $(x+y)+z = x+(y+z)$ u.

b) $\forall_{x \in M}$ $x+0 = x = 0+x$

2) $(M,*)$ ist ein Monoid mit Einselement 1.

d.h. a) $\forall_{x,y,z \in M}$ $(x*y)*z = x*(y*z)$

b) $\forall_{x \in M}$ $x*1 = 1*x = x$

Monide, Gruppen, Ringe, Körper

Definition 1.2

Es seien **M** eine nichtleere Menge und **T** eine binäre Verknüpfung **T** : M x M → M

Man nennt (M, **T**) eine **Monoid oder Halbgruppe**, wenn gilt:

M1) (M, **T**) ist **assoziativ**, d.h.

$\forall$ **a,b, c**$\in$**M: (aTb) Tc = aT (bTc)**

Gibt es zusätzlich ein Element **e**$\in$**M mit**

M2) $\forall$ **a** $\in$**M: eTa=aTe=a**

so heißt e ist ein **neutrales Element**:

Beispiel: (**N**,+), (**N**,*) sind Halbgruppen.

$M = \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Addition $+ : M \times M \longrightarrow M$

$(x,y) \longmapsto x+y$

Multiplikation $* : M \times M \longrightarrow M$

$(x,y) \longmapsto x*y$

1) $(M,+)$ ist ein Monoid mit Einselement 0

d.h. a) $\forall_{x,y,z \in M}$ $(x+y)+z = x+(y+z)$ u.

b) $\forall_{x \in M}$ $x+0 = x = 0+x$

2) $(M,*)$ ist ein Monoid mit Einselement 1.

d.h. a) $\forall_{x,y,z \in M}$ $(x*y)*z = x*(y*z)$

b) $\forall_{x \in M}$ $x*1 = 1*x = x$

Monide, Gruppen, Ringe, Körper

Definition 1.3

Es seien **G** eine nichtleere Menge,
eine binäre Verknüpfung **T** : G x G → G
und e ∈ G ein Element.
Man nennt (G, **T**,e) eine **Gruppe**, wenn gilt

G1) ist **assoziativ**,

$$\forall\ a,b,c \in G: (aTb)\ Tc = aT\ (bTc)$$

G2) e ist ein **neutrales Element**:

$$\forall\ a \in G: eTa = aTe = a$$

G3 Alle Elemente haben ein **Inverses**,

$$\forall\ a \in G\ \exists\ a^{-1} \in G : aT\ a^{-1} = a^{-1}Ta = e$$

Beispiele $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mit $\tau = +$, $\mu \cdot e = 0$ sind additive abelsche Gruppen, d.h. es gelten

① $\forall_{x,y,z \in G}$ $(x+y)+z = x+(y+z)$

② $\forall_{x \in G}$ $x+0 = 0+x = x$

③ $\forall_{x \in G}$ $x+(-x) = 0$

④ $\forall_{x,y \in G}$ $x+y = y+x$

Monide, Gruppen, Ringe, Körper

Definition 1.4 Seien R eine Menge und +, * binäre Verknüpfungen auf R .
R heißt Ring (mit Einselement), wenn gilt:

R1) (R,+) ist abelsche Gruppe.

R2) (R,*) ist Halbgruppe mit Einselement.

R3) Es gelten $a*(b + c) = ab+ac$ **und**
$(b+c)*a = ba + ca$
für alle $a,b,c \in R$ **. (Distributivgesetze)**

Der Ring heißt kommutativ, falls * kommutativ **ist.**

Monide, Gruppen, Ringe, Körper

Wie allgemein üblich bei additiv notierter Verknüpfung, bezeichnen wir das neutrale Element von (R,+) mit 0 und sprechen vom **Nullelement oder der Null von R**;

Das neutrale Element von (*R*, *) heißt **Eins oder Einselement** und wird in der Regel mit 1 bezeichnet, zur besseren Unterscheidung manchmal auch mit 1_R.

Homomorphismus
(= strukturverträgliche Abbildung)

Definition 1.5

Seien $(A, T_1,.., T_n)$ und $(A', T_1,.., T_n)$ zwei Mengen mit mit binären Verknüpfungen $T_1,.., T_n$.

Ist $\varphi : A \rightarrow A'$ eine Abbildung, dann nennen wir φ einen **Homomorphismus**, falls sie die folgende Bedingung erfüllt

$$\forall\ i= 1,..,n \forall\ \mathbf{x; y} \in \mathbf{A\ gilt}\ \varphi(x\ T_i\ y) = \varphi(x)\ T_i\ \varphi(y)$$

Homomorphismus
(= strukturverträgliche Abbildung)

Definition 1.5.1(Verallgemeinerung

Seien $(A, T_1,.., T_n)$ und $(A', T_1,.., T_n)$ zwei Mengen mit mit n-stelligen Verknüpfungen $T_1,.., T_n$.

Ist $\varphi : A \rightarrow A'$ eine Abbildung, dann nennen wir φ einen **Homomorphismus**, falls sie die folgende Bedingung erfüllt

$\forall$ **i= 1,..,n gilt**

$$\varphi(T_i (a_1, \ldots, a_{ni})) = (T_i (\varphi (a_1), \ldots, \varphi(a_{ni})) \text{ für alle } a_i \in A$$

Homomorphismen

Definition 1.6

Seien $(M, T_1,.., T_n)$ und $(M', T_1,.., T_n)$ zwei Mengen mit Verknüpfungen $T_1,.., T_n$., und $\varphi : M \rightarrow M'$ ein **Homomorphismus**

1. Ein injektiver Homomorphismus heißt auch **Monomorphismus**.

(Cf. griechisch **μονος einzig**, z.B. der Monarch als Alleinherrscher.)

2. Ein surjektiver Homomorphismus heißt auch **Epimorphismus**.

(Cf. griechisch **επι darauf**, z.B. das Epizentrum eines Erdbebens, das auf der Erdoberfläche ¨uber dem Zentrum im Erdinneren liegt.)

3. Ein bijektiver Homomorphismus heißt auch **Isomorphismus**.

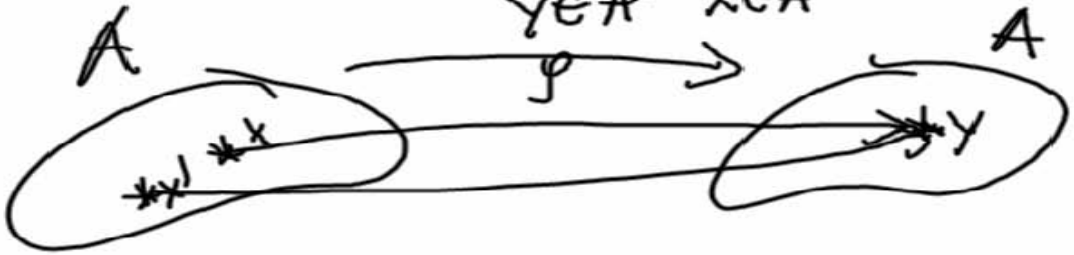
(Cf. griechisch **ισος derselbe**, z.B. Isotop als Element am selben Platz des Periodensystems.)

(W)

1) Abb. $\varphi: A \longrightarrow A'$

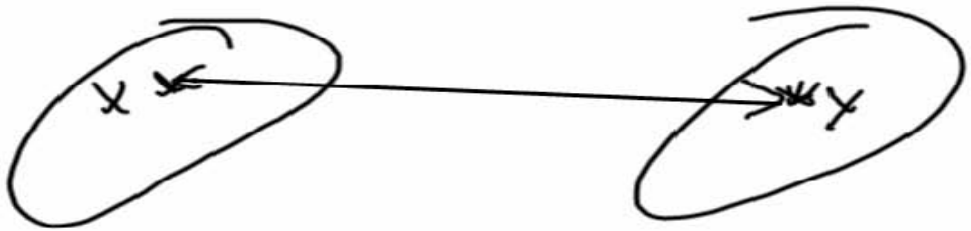
φ <u>injektiv</u> $\Leftrightarrow \underset{x,y \in A}{\forall} \; \varphi(x) = \varphi(y) \Rightarrow x = y$

2) φ <u>surjektiv</u> $\Leftrightarrow \underset{y \in A'}{\forall} \; \underset{x \in A}{\exists} \; \varphi(x) = y$



3) φ bijektiv $\Leftrightarrow \varphi$ injektiv + surjektiv

$\Leftrightarrow \underset{y \in A'}{\forall} \; \underset{x \in A}{\exists!} \; \varphi(x) = y$



Homomorphismus
Beispiel: Gruppenhomomorphismus

Definition 1.7

Seien G und G´ zwei Gruppen, wobei die jeweiligen neutralen Elemente mit $e \in G$ bzw. mit $e' \in G'$ bezeichnet seien.

Ist $\varphi : G \rightarrow G'$ eine Abbildung, dann nennen wir φ einen **Gruppenhomomorphismus**, falls sie die folgende Bedingung erfüllt

$$\forall\ x; y \in G \text{ gilt } \varphi(x*y) = \varphi(x) *\varphi(y)$$

und in diesem Fall erfüllllt φ sogar die beiden weiteren Eigenschaften

$$\varphi(e) = e' \text{ und } \varphi(x^{-1}) = \varphi(x)^{-1}$$

$\forall \exists \{ \} | \in$

Homomorphismus
Beispiel: Ringhomorphismus

Definition 1.8 Es seien R; S zwei Ringe. Unter einem **Ringhomorphismus**

von R nach S versteht man eine Abbildung

$$\varphi : R \rightarrow S \text{ mit}$$

$$\forall x; y \in R$$

$$\varphi(x + y) = \varphi(x) + \varphi(y);$$

$$\varphi(x * y) = \varphi(x) * \varphi(y) :$$

Satz geg. Hom. $\varphi: G \longrightarrow G'$
G, G' Gruppen*. Dann gelten

1) $\varphi(e) = e'$
2) $\varphi(x^{-1}) = \varphi(x)^{-1}$

Beweis

1) $ex = x$ für alle $x \in G$ $\Rightarrow$
$ee = e$
$\varphi(ee) = \varphi(e)$
$\varphi(e) \overset{!!}{\cdot} \varphi(e)$

* $(G, *, e), (G', *, e')$

sei $\varphi(e)^{-1} \in G'$ das Inverse zu $\varphi(e)$
d.h. $\varphi(e) \cdot \varphi(e)^{-1} = e'$

$\varphi(e) \cdot \varphi(e) = \varphi(e)$ $\Rightarrow$

$\varphi(e) \cdot \underbrace{\varphi(e) \cdot \varphi(e)^{-1}}_{e'} = \varphi(e)\varphi(e)^{-1} = e'$

$\varphi(e) = e'$
$\varphi(e)$

2) $\varphi(x^{-1}) = \varphi(x)^{-1}$

$x x^{-1} = e$ *

$\varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1}) = \varphi(e) = e$)

$\varphi(x)^{-1} \quad (\varphi(x)^{-1} \cdot \varphi(x)) \varphi(x^{-1}) = \varphi(x)^{-1}$

e "

$\varphi(x^{-1}) = \varphi(x)^{-1}$ □

* $(\mathbb{Z}, +)$: $x + (-x) = 0$

$(\mathbb{Q} \setminus \{0\}, *)$ $x \cdot \frac{1}{x} = 1$

II Gruppen

Monide, Gruppen, Ringe, Körper

Definition 2.1

Es seien **G** eine nichtleere Menge,
eine Abbildung **T** T : G x G → G
und e ∈ G ein Element.
Man nennt (G, **T**,e) eine **Gruppe**, wenn gilt

G1) ist **assoziativ**,

$$\forall\ a,b,c \in G: (aTb)\ Tc = aT\ (bTc)$$

G2) e ist ein **neutrales Element**:

$$\forall\ a \in G: eTa = aTe = a$$

G3 Alle Elemente haben ein **Inverses**,

$$\forall\ a \in G\ \exists\ a^{-1} \in G : aT\ a^{-1} = a^{-1}Ta = e$$

Grundlegende Definitionen und Beispiele

2.3 Beispiele für Gruppen

- Die ganzen Zahlen **Z** mit der Addition, $(\mathbb{Z}, +, 0)$
- Die rationalen Zahlen **Q** ohne Null mit der Multiplikation (**Q**\{0},*,1)
- Für jede nichtleere Menge M ist die Menge

$$S(M) := \{f : M \to M \mid f \text{ bijektiv}\}$$

aller bijektiven Selbstabbildungen mit der Abbildungskomposition eine Gruppe. S(M) heißt die **symmetrische Gruppe** auf M,

ihre Elemente heißen ***Permutationen* von M**.

2.4 Satz:
Die Menge S(M) der bijektiven Abbildungen über einer nicht leeren Menge ist eine Gruppe bzgl. der Hintereinanderausführung von Abbildungen als Verknüpfung.

Beweis

$M \neq \emptyset$

$S(M) := \{ \text{Abb. } f : M \to M ; f \text{ bijektiv} \}$

Symmetrische Gruppe über M.

$f, g \in S(M)$

$g \circ f$

$x \in M \quad g \circ f(x) := g[f(x)]$

1) $g \circ (f \circ h) = (g \circ f) \circ h$

2) Einselement $id : M \to M : x \mapsto id(x) = x$

$id \circ f(x) = id[f(x)] = f(x)$

3) Inverse

$y \in M \quad f^{-1}(y) = x \text{ falls } f(x) = y$

$f \text{ bijektiv} \Leftrightarrow \underset{y \in M}{\forall} \; \underset{x \in M}{\exists!} \; f(x) = y$

$f \circ f^{-1}(y) = f[f^{-1}(y)] =$

$f(x) = y \rightarrow f \circ f^{-1} = id$ ∎

$M = \mathbb{N}_n = \{1, 2, \dots, n\}$

$$\varphi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & \cdots & \varphi(n) \end{pmatrix}$$

$\varphi : \mathbb{N}_n \longrightarrow \mathbb{N}_n$ Bijektion

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$S_{n!} = S(\mathbb{N}_n)$ n-te Permutations-gruppe.

Als Produkt zweier Permutationen φ und π aus S_n erhält man für das Produkt $\varphi * \pi$

Man fängt also die Auswertung beim rechten Faktor an, so wie es sich für ein Produkt von Abbildungen gehört.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & \cdots & \varphi(n) \end{pmatrix} * \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(\pi(1)) & \varphi(\pi(2)) & \cdots & \varphi(\pi(n)) \end{pmatrix}$$

Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Beispiel

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Vertauschen der Zeilen $\Longrightarrow$

$$\begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

natürliche Anordnung $\Longrightarrow$

$$\varphi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

Bemerkung:

$\varphi : M \longrightarrow M$ bijektiv *

φ^{-1}

$$\varphi^{-1}(y) = x \iff \varphi(x) = y$$