Tutorium: Diskrete Mathematik

Algebraische Strukturen

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Algebraische Strukturen I

Eine *algebraische Struktur* ist ein Paar

$$\big(A, (f_i)\big),$$

bestehend aus einer nichtleeren Menge A, der *Trägermenge* der Algebra, und einer Familie (Menge) von (endlichstelligen) Verknüpfungen auf A, die auch *fundamentale Operationen* genannt werden.

Meistens hat eine Algebra nur endlich viele Verknüpfungen $f_1, \ldots, f_n$; man schreibt dann für die Algebra einfach nur

$$\big(A, f_1, \ldots, f_n\big).$$

Algebraische Strukturen II

Die Trägermenge A der Algebra ist *abgeschlossen* bezüglich der definierten Operationen, d.h., Verknüpfung von zwei Elementen $a, b \in A$ (im Fall einer binären Verknüpfung) liefert stets ein Element $c \in A$. a, b und c müssen dabei nicht notwendigerweise verschieden sein.

Halbgruppen I

Eine *Halbgruppe* ist eine algebraische Struktur

$$\mathcal{H} = \big(H, \star\big)$$

mit der Trägermenge H und einer zweistelligen Verknüpfung $\star$.

Für alle Elemente in H gilt das Assoziativgesetz, d.h., für alle $a, b, c \in H$ gilt stets

$$a \star (b \star c) = (a \star b) \star c.$$

Halbgruppen II

Häufig wird für die Verknüpfung $\star$ das Symbol $\cdot$ benutzt, man spricht dann von einer *multiplikativ geschriebenen Halbgruppe*. Wie auch bei der gewöhnlichen Multiplikation, kann in vielen Situationen der Malpunkt weggelassen werden.

Eine Halbgruppe lässt sich auch *additiv* notieren, indem für die Verknüpfung $\star$ das Symbol $+$ benutzt wird.

Halbgruppen III

Da das Assoziativgesetz gilt, kann eine vereinfachte, klammerfreie Notation verwendet werden:

$$a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

Monoide I

Eine *Monoid* ist eine algebraische Struktur

$$\mathcal{M} = \big(M, \star\big)$$

mit der Trägermenge M und einer zweistelligen Verknüpfung $\star$.

Ein Monoid ist eine Halbgruppe mit einem *neutralen Element* e.

Monoide II

Für Monoide gelten also die folgenden Eigenschaften:

- Für die Verknüpfung $\star$ gilt das Assoziativgesetz:

$$\forall a, b, c \in M : a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

- Es existiert ein neutrales Element e, für das gilt:

$$\forall a \in M : e \star a = a \star e = a.$$

Das Element e ist also sowohl links- als auch rechtsneutral bzgl. der definierten Operation $\star$.

Monoide III

Aufgabe 1

Welche der folgenden algebraischen Strukturen sind Monoide? Begründe deine Antworten.

a) $\left(\mathbb{N}_0, +\right)$

b) $\left(\mathbb{N}_0, :\right)$

c) $\left(\mathbb{Z}, -\right)$

d) $\left(\mathbb{R}^{3\times 3}, \cdot\right)$

Gruppen I

Eine *Gruppe* ist eine algebraische Struktur

$$\mathcal{G} = \left(G, \star\right)$$

mit der Trägermenge G und einer zweistelligen Verknüpfung $\star$.

Eine Gruppe ist eine Monoid, in dem für jedes Element $a \in G$ das zugehörige *inverse Element* a^{-1} in G enthalten ist.

Gruppen II

Für Gruppen gelten also die folgenden Eigenschaften:

- Für die Verknüpfung $\star$ gilt das Assoziativgesetz:

$$\forall a, b, c \in G : a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

- Es existiert ein neutrales Element e, für das gilt:

$$\forall a \in G : e \star a = a \star e = a.$$

- Existenz inverser Elemente:

$$\forall a \in G : \exists a^{-1} \in G \text{ mit } a \star a^{-1} = a^{-1} \star a = e.$$

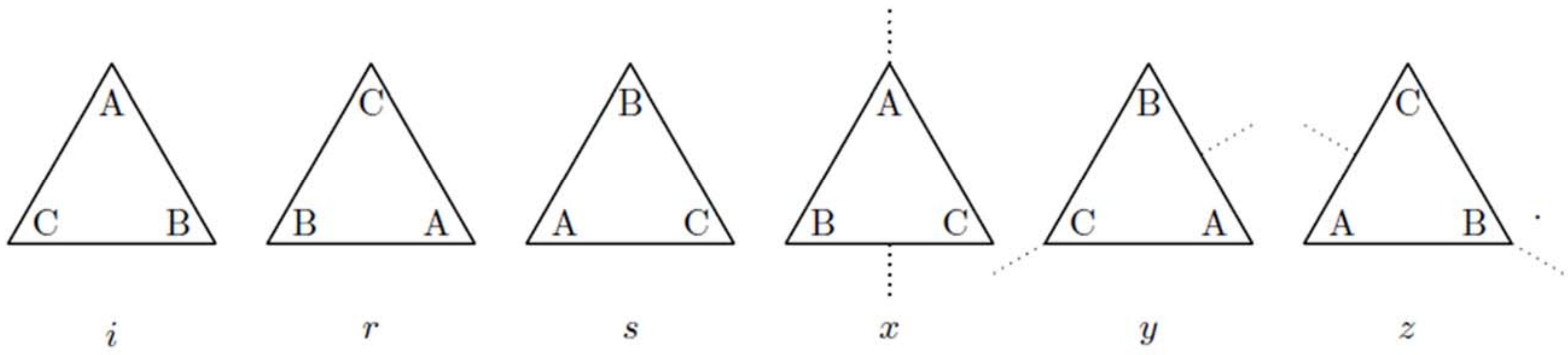
Gruppen III

Beispiele für Gruppen

- $\big(\mathbb{Z}, +\big)$
- $\big(\mathbb{Q} \setminus \{0\}, \cdot\big)$
- $\big(\mathbb{R}, +\big)$
- Kleinsche Vierergruppe
- Dreiecksgruppe

Die Dreiecksgruppe I

Die Dreiecksgruppe G_Δ ist eine Gruppe, die die folgenden Elemente enthält:



i, r und s sind dabei Drehungen um 0°, 60° bzw. 120°. x, y und z sind Spiegelungen an den Winkelhalbierenden des Dreiecks.

Die Dreiecksgruppe II

Diese Gruppe besitzt die folgende *Gruppentafel*, in der die Ergebnisse der Veknüpfung der Elemente tabellarisch notiert sind:

	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	y	z	x
s	s	i	r	z	x	y
x	x	z	y	i	s	r
y	y	x	z	r	i	s
z	z	y	x	s	r	i

Die Rechteckgruppe

Aufgabe 2

Bestimme die Elemente der Rechteckgruppe und stelle die Gruppentafel dieser Gruppe auf.

Die Ordnung einer Gruppe

Die Mächtigkeit (Kardinalität) $|G|$ der Trägermenge der Gruppe nennt man die *Ordnung der Gruppe* oder auch die *Gruppenordnung.*

Für endliche Mengen G ist dies einfach die Anzahl der Elemente in G.

Die Ordnung eines Gruppenelements

Unter der *Ordnung eines Elements* $a \in G$ einer Gruppe $\mathcal{G} = (G, \star)$ versteht man die kleinste natürliche Zahl $m > 0$, für die $a^m = e$ gilt; e ist dabei das neutrale Element der Gruppe.

Man definiert die Potenzen eines Gruppenelements wie folgt:

$$\begin{aligned} a^0 &:= e \\ a^{n+1} &:= a^n \star a. \end{aligned}$$

Gibt es keine derartige Zahl, so hat a *unendliche Ordnung*.

Untergruppen I

Ist U eine Teilmenge der Trägermenge G einer Gruppe $\mathcal{G} = (G, \star)$ (also $U \subseteq G$) und ist $\mathcal{U} = (U, \star)$ selbst eine Gruppe, so nennt man $\mathcal{U}$ eine Untergruppe von $\mathcal{G}$.

Um zu zeigen, dass $\mathcal{U}$ eine Untergruppe von $\mathcal{G}$ ist, genügt es zu zeigen, dass Folgendes gilt:

- $a, b \in U \Rightarrow a \star b \in U$;
- $a \in U \Rightarrow a^{-1} \in U$.

Untergruppen II

Aufgabe 3

Gegeben seien die beiden Gruppen $\mathcal{G} = (G, \star)$ und $\mathcal{H} = (H, \star)$. Zeige, dass $(G \cap H, \star)$ eine Untergruppe sowohl von $\mathcal{G}$ als auch von $\mathcal{H}$ ist.

Untergruppen III

Jedes Element $a \in G$ einer Gruppe $\mathcal{G}$ erzeugt eine Untergruppe $\mathcal{H}$.

Die durch $a \in G$ erzeugte Untergruppe wird mit $< a >$ bezeichnet.

Der Satz von Lagrange

Der *Satz von Lagrange* wurde nach dem italienischen Mathematiker Joseph-Louis Lagrange benannt.

Der Satz besagt, dass die Mächtigkeit (oder Ordnung) einer Untergruppe stets die Mächtigkeit der Gruppe teilt.

Es sei $\mathcal{G}$ eine endliche Gruppe:

- Ist $\mathcal{H}$ eine Untergruppe von $\mathcal{G}$, so ist die Mächtigkeit $|H|$ ein Teiler von $|G|$.
- Insbesondere teilt die Ordnung eines Elements $a \in G$ die Mächtigkeit $|G|$ von G.

Die symmetrische Gruppe

Als *symmetrische Gruppe* bezeichnet man die Gruppe S_n aller möglichen Permutationen über n Elementen.

Die Operation der Gruppe ist die Nacheinanderausführung von Permutationen.

Da es $n!$ verschiedene Permutationen über n Elementen gibt, gilt

$$|S_n| = n!$$

Permutationsgruppen

Als *Permutationsgruppe* bezeichnet man eine Untergruppe einer symmetrischen Gruppe S_n.

Isomorphie von Gruppen I

Zwei Gruppen heißen *isomorph* oder *strukturgleich*, wenn ihre Gruppentafeln bis auf die Bezeichnungen der Elemente übereinstimmen.

Eine wichtige Voraussetzung für Isomorphie ist, dass die Gruppen gleichviele Elemente einer jeweiligen Ordnung besitzen.

Isomorphie von Gruppen II

Aufgabe 4

Zeige, dass (bis auf Isomorphie) genau 2 verschiedene Gruppen der Ordnung 4 existieren.

Zyklische Gruppen

Eine Gruppe $\mathcal{G} = (G, \star)$ heißt *zyklisch*, wenn sie mindestens ein Element enthält, aus dem sämtliche Elemente der Gruppe erzeugt werden können.

Mit anderen Worten: In G muss mindestens ein Element der Ordnung $|G|$ existieren.

Abelsche Gruppen

Eine Gruppe $\mathcal{G} = (G, \star)$ heißt *abelsch* oder *kommutativ*, wenn zusätzlich zu den bisher genannten Gruppeneigenschaften das Kommutativgesetz gilt, d.h.:

$$\forall a, b \in G : a \star b = b \star a.$$

Nebenklassen I

Es sei $\mathcal{H}$ eine Untergruppe einer Gruppe $\mathcal{G}$ und a sei ein Element von G. Mit Hilfe von a und $\mathcal{H}$ definieren wir eine Teilmenge von $\mathcal{G}$ wie folgt:

$$a\mathcal{H} := \Big\{ g \in G : \text{ Es gibt ein } h \in H \text{ mit } g = ah \Big\}.$$

Man nennt eine solche Teilmenge $a\mathcal{H}$ eine *Linksnebenklasse* von $\mathcal{H}$ in $\mathcal{G}$.

Analog wird der Begriff *Rechtsnebenklasse* definiert.

Nebenklassen II

Aufgabe 5

Es sei $\mathcal{G}$ die symmetrische Gruppe S_3 und H die durch das Element $(1, 2)$ erzeugte Untergruppe von $\mathcal{G}$. Bestimme die Linksnebenklassen von $\mathcal{H}$.

Ringe I

Ein *Ring* ist eine algebraische Struktur

$$\mathcal{R} = \big(R, +, \cdot\big)$$

mit der Trägermenge R und zwei zweistelligen Verknüpfungen $+$ und $\cdot$.

Ringe II

In einem Ring gelten die folgenden Eigenschaften:

- Bezüglich der Operation $+$ bildet $(R, +)$ eine kommutative Gruppe.
- Bezüglich der Operation $\cdot$ bildet $(R, \cdot)$ einen Monoid.
- Es gelten die Distributivgesetze

$$a \cdot (b + c) = ab + ac;$$
$$(a + b) \cdot c = ac + bc.$$

Körper I

Ein *Körper* ist eine algebraische Struktur

$$\mathcal{K} = \big(K, +, \cdot\big)$$

mit der Trägermenge K und zwei zweistelligen Verknüpfungen $+$ und $\cdot$.

Körper II

In einem Körper gelten die folgenden Eigenschaften:

- Bezüglich der Operation $+$ bildet $(K, +)$ eine kommutative Gruppe.
- Bezüglich der Operation $\cdot$ bildet $(K \setminus \{e_+\}, \cdot)$ eine kommutative Gruppe.
- Es gelten die Distributivgesetze

$$a \cdot (b + c) = ab + ac;$$
$$(a + b) \cdot c = ac + bc.$$

Körper III

<u>Beispiele für Körper</u>

- $(\mathbb{Q}, +, \cdot)$
- $(\mathbb{R}, +, \cdot)$
- $(\mathbb{C}, +, \cdot)$
- der *Galoiskörper* GF_2 (oder auch $\mathbb{F}_2$)

Körper IV

Aufgabe 6

Zeige, dass die Menge der invertierbaren 2×2 - Matrizen zusammen mit der üblichen Matrizenaddition und -multiplikation einen Ring, aber keinen Körper bildet.

Vielen Dank für die Aufmerksamkeit ☺