Algebra für Informationssystemtechniker

Prof. Dr. Ulrike Baumann

Fachrichtung Mathematik

Institut für Algebra

www.math.tu-dresden.de/∼baumann

Ulrike.Baumann@tu-dresden.de

23.04.2018

9. Vorlesung

Halbgruppe $\rightarrow$ Monoid $\rightarrow$ Gruppe

- (2-stellige) Operationen
- assoziativ, kommutativ
- neutrale Elemente
- inverse Elemente
- Kürzungsregeln
- Lösbarkeit von Gleichungen

Methode: Folgerungen aus einem Axiomensystem herleiten

Auf Beispiele, die das Axiomensystem erfüllen, treffen auch alle Folgerungen zu.

Halbgruppen

- Es sei H eine nichtleere Menge und $\circ$ eine assoziative Operation auf H, d.h. es gilt:

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

  Dann nennt man $(H, \circ)$ eine **Halbgruppe**.

- $|H|$ heißt **Ordnung** der Halbgruppe $(H, \circ)$.

- Eine Halbgruppe $(H, \circ)$ wird **kommutative Halbgruppe** genannt, wenn gilt:

$$\forall a, b \in H : \ a \circ b = b \circ a$$

Monoide

- $e \in H$ heißt **neutrales Element** in einer Halbgruppe $(H, \circ)$, wenn gilt:

$$\forall a \in H : \; e \circ a = a \circ e = a$$

- Es sei $(H, \circ)$ eine Halbgruppe mit einem neutralen Element. Dann nennt man $(H, \circ)$ ein **Monoid**.

- Eine Halbgruppe enthält höchstens ein neutrales Element. Ein Monoid enthält genau ein neutrales Element.

Beispiele

- $(\mathbb{Z}, -)$ ist keine Halbgruppe.
- $(2\mathbb{Z}, \cdot)$ ist eine kommutative Halbgruppe.
- $(\mathbb{Z}, \cdot)$ ist ein kommutatives Monoid mit $e = 1$.
- $(\mathbb{N}, +)$ ist eine kommutatives Monoid mit $e = 0$.
- $(\mathbb{R}^{n \times n}, \cdot)$ ist ein Monoid mit $e = E_n$.
- $(\mathbb{Z}_n, +)$ ist ein kommutatives Monoid mit $e = 0$.
- $(\mathbb{Z}_n, \cdot)$ ist ein kommutatives Monoid mit $e = 1$.
- Freies Monoid über dem Alphabet Σ,
  ε bezeichnet das leere Wort:
  $(\Sigma^*, \circ)$ ist ein Monoid mit $e = \varepsilon$.

Unterhalbgruppen

- Es sei $(H, \circ)$ eine Halbgruppe und $\emptyset \neq U \subseteq H$.
  U heißt **Unterhalbgruppe** von H, wenn U mit der Verknüpfung $\circ$ von H eine Halbgruppe bildet, d.h. wenn gilt:
  $$a, b \in U \;\Rightarrow\; a \circ b \in U$$

- H ist eine (triviale) Unterhalbgruppe von $(H, \circ)$.

- Der Durchschnitt von Unterhalbgruppen von $(H, \circ)$ ist eine Unterhalbgruppe von $(H, \circ)$ oder $\emptyset$.

Invertierbare Elemente in Halbgruppen

- Es sei $(H, \circ)$ ein Monoid mit dem neutralen Element e.
  Ein Element $a \in H$ heißt **invertierbar**, wenn ein $b \in H$ mit

  $$a \circ b = b \circ a = e$$

  existiert.

- Für jedes $a \in H$ existiert höchstens ein Element $b \in H$ mit $a \circ b = b \circ a = e$.

- Ist $a \in H$ invertierbar, dann existiert genau ein Element $b \in H$ mit $a \circ b = b \circ a = e$.

  Dieses Element b wird auch mit a^{-1} bezeichnet und **das Inverse** von a genannt.

Gruppen

- Es sei $(H, \circ)$ ein Monoid mit dem neutralen Element e.
  H^* bezeichnet die Menge der invertierbaren Elemente von H.
  Es gilt:

  (1) $e \in H^*$ und $e^{-1} = e$
  (2) $a \in H^* \Rightarrow a^{-1} \in H^*$ und $(a^{-1})^{-1} = a$
  (3) $a, b \in H^* \Rightarrow a \circ b \in H^*$ und $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

- Für jedes Monoid $(H, \circ)$ ist die Menge H^* eine Unterhalbgruppe von $(H, \circ)$.

  (Diese Unterhalbgruppe ist sogar eine Gruppe.)

- Ein Monoid $(H, \circ)$ heißt **Gruppe**,
  wenn $H^* = H$ gilt.

- Beispiele für abelsche Gruppen:

  $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,
  $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ (p prim)

Gruppen

- Eine Gruppe ist eine Algebra $(G; \circ, ^{-1}, e)$ vom Typ $(2, 1, 0)$ mit:

  (1) $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in G$

  (2) $g \circ e = g = e \circ g$ für alle $g \in G$

  (3) $g \circ g^{-1} = g^{-1} \circ g = e$ für alle $g \in G$

- G ist die **Trägermenge** der Gruppe.

  $\circ$, $^{-1}$, e sind die Symbole für die **fundamentalen Operationen**.

  Der **Typ** $(2, 1, 0)$ gibt an, dass $\circ$ eine 2-stellige Operation, $^{-1}$ eine 1-stellige und e eine 0-stellige Operation bezeichnet.

  Man nennt e das **neutrale Element** der Gruppe und g^{-1} das zu g **inverse Element**.

Untergruppen

- Eine Teilmenge U einer Gruppe $(G; \circ, ^{-1}, e)$,
  die das neutrale Element enthält (d.h. $e \in U$)
  und die gegen die Operationen $\circ$ und $^{-1}$ abgeschlossen ist
  (d.h. $a, b \in G \;\Rightarrow\; a \circ b \in G$ für alle $a, b \in G$
  und $a \in G \;\Rightarrow\; a^{-1} \in G$ für alle $a \in G$)
  nennt man eine **Untergruppe** der Gruppe $(G; \circ, ^{-1}, e)$.

  Schreibweise: $U \leq G$

- Jede Untergruppe ist mit den eingeschränkten Operationen selbst eine Gruppe.

- Jede Gruppe $(G; \circ, ^{-1}, e)$ mit $|G| > 1$ hat mindestens zwei Untergruppen:

$$U = \{e\} \quad \text{und} \quad U = G$$

  Diese Untergruppen nennt man auch **triviale Untergruppen**.

Eigenschaften von Gruppen

- In jeder Gruppe $(G, \circ)$ gelten die **Kürzungsregeln**:

$$\forall a, x_1, x_2 \in G: \; a \circ x_1 = a \circ x_2 \;\Rightarrow\; x_1 = x_2$$

$$\forall a, y_1, y_2 \in G: \; y_1 \circ a = y_2 \circ a \;\Rightarrow\; y_1 = y_2$$

- In jeder Gruppe $(G, \circ)$ sind alle Gleichungen $a \circ x = b$ und $y \circ a = b$ mit $a, b \in G$ eindeutig lösbar.

- Jede endliche Halbgruppe, in der die Kürzungsregeln gelten, ist eine Gruppe.