

Übersicht über die Algebraischen Strukturen aus der Vorlesung "Mathematische Methoden für Informatiker II"

Klaus-Rudolf Kladny

Gruppentheorie:

1. Halbgruppe $(S, *)$

Eigenschaften:

1. Existenz einer Menge S (darf auch leer sein)
2. Existenz einer zweistelligen Operation:

$$* : S \times S \rightarrow S, (a, b) \mapsto a * b$$

3. Assoziativität bezüglich $*$:

$$\forall a, b, c \in S : a * (b * c) = (a * b) * c$$

4. Abgeschlossenheit bezüglich $*$:

$$\forall a, b \in S : (a * b) \in S$$

Unterhalbgruppe

Eine Unterhalbgruppe $(U, *)$ einer Halbgruppe $(S, *)$ ist eine Halbgruppe mit folgenden Eigenschaften:

1. $U \subseteq S$ und $U \neq \emptyset$
2. $a, b \in U \Rightarrow (a * b) \in U$

2. Monoid $(S, *, e)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Halbgruppen
2. Existenz eines neutralen Elements e :

$$\forall a \in S : e * a = a * e = a$$

3. Gruppe $(S, *, e)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Monoide
2. Es existieren inverse Elemente:

$$\forall a \in S : \exists ! a^{-1} : a * a^{-1} = a^{-1} * a = e$$

Beispiele für Gruppen:

Permutationsgruppen, Automorphismengruppen, Faktorgruppen, Menge der ganzen Zahlen mit der Addition $(\mathbb{Z}, +)$

3.1 Abelsche Gruppe $(S, *, e)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Gruppen
2. Kommutativität bezüglich $*$:

$$\forall a, b \in S : a * b = b * a$$

3.2 Zyklische Gruppe $(S, *, e)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Gruppen
2. Es existiert ein Element, welches mit \cdot die gesamte Gruppe erzeugt. (erzeugendes Element)

Bemerkung zu zyklischen Gruppen:

Sei im Allgemeinen n die Kardinalität der Gruppe

1. Es gibt zu jedem $n \in \mathbb{N}$ bis auf Isomorphie genau eine zyklische Gruppe mit dieser Kardinalität.
2. Die Gruppe hat $\phi(n)$ erzeugende Elemente.
3. Jede zyklische Gruppe ist abelsch (kommutativ bzgl. \cdot).
4. Das direkte Produkt zweier zyklischer Gruppen ist zyklisch, gdw. die Kardinalitäten der Gruppen teilerfremd sind.
5. Es gibt immer mindestens ein Element, welches mit \cdot die gesamte Gruppe alleine erzeugt.
6. Zu jedem Teiler t von n existiert genau eine Untergruppe. Sei a ein erzeugendes Element der gesamten Gruppe. Dann wird die Untergruppe der Ordnung t vom Element $a^{n/t}$ erzeugt.

Untergruppe

Eine Untergruppe $(U, *)$ einer Gruppe $(S, *)$ mit dem neutralen Element e ist eine Gruppe mit folgenden Eigenschaften:

1. $U \subseteq S$ und $U \neq \emptyset$
2. $e \in U$
3. $a, b \in U \Rightarrow (a * b) \in U$
4. $a \in S \Rightarrow a^{-1} \in U$ (Muss nur in nicht endlichen Gruppen gezeigt werden)

Satz von Lagrange:

$$|S| = [S : U] \cdot |U|$$

Folgerung: Die Mächtigkeit jeder Untergruppe teilt die Mächtigkeit der Gruppe.

Ringtheorie:

1. Halbring (auch: Semiring) $(H, +, \cdot)$

Eigenschaften:

1. Existenz einer nichtleeren (!) Menge H
2. Existenz zweier zweistelliger Operationen:

$$+ : H \times H \rightarrow H, (a, b) \mapsto a + b$$

$$\cdot : H \times H \rightarrow H, (a, b) \mapsto a \cdot b$$

3. $(H, +)$ ist eine kommutative Halbgruppe.
4. (H, \cdot) ist eine Halbgruppe.
5. Es gelten die Distributivgesetze:

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

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

2. Ring $(H, +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Halbringe.
2. $(H, +)$ ist eine abelsche Gruppe.
 - (a) Das neutrale Element wird als Nullelement 0 bezeichnet

3.1 kommutativer Ring $(H, +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Ringe
2. (H, \cdot) ist eine kommutative Halbgruppe

3.2 euklidischer Ring $(H, +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Ringe
2. $\forall a, b \in H \setminus \{0\}$: Es kann ein größter gemeinsamer Teiler $ggT(a, b)$ mit dem euklidischen Algorithmus bestimmt werden.

3.3 Integritätsring $(H, +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften für kommutative (!) Ringe.
2. Es gibt ein neutrales Element bezüglich der Multiplikation, welches als Einselement 1 bezeichnet wird.
3. Es existieren keine Nullteiler:

(Erinnerung)

$$a \in H \text{ ist Nullteiler} \Leftrightarrow \exists b \in H : a \cdot b = 0$$

3.3.1 Polynomring $(R[x], +, \cdot)$

Eigenschaften:

1. $(R, +, \cdot)$ ist ein Ring.
2. Er ist ein nicht endlicher Integritätsring, also kein Körper.

3.4 Körper $(H, +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften für kommutative (!) Ringe
2. Es gibt ein neutrales Element bezüglich der Multiplikation, welches als Einselement 1 bezeichnet wird.
3. (H, \cdot) ist eine Gruppe

Unterring:

Ein Unterring $(U, +, \cdot)$ eines Rings $(H, +, \cdot)$ ist ein Ring mit folgenden Eigenschaften:

1. $U \subseteq S$ und $U \neq \emptyset$
2. (a) $a, b \in U \Rightarrow (a + b) \in U$
(b) $a, b \in U \Rightarrow (a \cdot b) \in U$
3. $a \in U \Rightarrow a^{-1} \in U$ (Dies muss nur in nicht endlichen Ringen gezeigt werden)

Zusammenhang zwischen Integritätsring und Körper:

Jeder Körper ist ein Integritätsring und jeder endliche Integritätsring ist ein Körper.

3.4.1 Endlicher Körper (auch: Galois Körper) $(H, +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften für Körper
2. Die Anzahl der Elemente ist endlich und sogar eine Primzahlpotenz

Multiplikative Gruppe:

Ist die Gruppe, welche aus allen Elementen des Körpers mit Ausnahme des Nullelements mit \cdot entsteht.

Bemerkung zu endlichen Körpern:

1. Es gibt zu jeder Primpotenz bis auf Isomorphie genau einen endlichen Körper.
2. Es gibt immer ein primitives Element, welches mit \cdot den gesamten Körper bis auf das Nullelement alleine erzeugt.

3.4.1.1 Endlicher Polynomkörper $(K[x]/f(x), +, \cdot)$

Eigenschaften:

1. Es gelten alle Eigenschaften von endlichen Körpern.
2. $f(x)$ ist ein irreduzibles Polynom. Also $\nexists g(x), h(x) \in K[x]/f(x) : g(x) \cdot h(x) = f(x)$

Zusätzliche Eigenschaft:

Ist x ein Erzeuger (*Primitives Element* genannt) der multiplikativen Gruppe $K[x]/f(x) \setminus \{0\}$, so wird $f(x)$ als *Primitives Polynom* bezeichnet.

Bemerkung zu endlichen Polynomkörpern:

Sei im Allgemeinen p die Primzahl und k der Grad des irreduziblen Polynoms $f(x)$

1. Der Körper besteht aus p^k Elementen.
2. Die multiplikative Gruppe des Körpers besteht aus $p^k - 1$ Elementen, da die 0 nicht darin vorkommt.