Algebra 3

Halbgruppen, Monoide, Ringe, Körper

- Am Beispiel der Gruppe haben wir das zentrale Konzept der Algebra kennengelernt: man hat eine Menge zusammen mit einer Operation, welche die Elemente der Menge verknüpft, wobei bestimmte Eigenschaften (Rechenregeln) gelten. Aus diesen einfachen Voraussetzungen kann man weitreichende Folgerungen ziehen, und es entfaltet sich eine außerordentlich reichhaltige Struktur.

  Wir wollen die Grundidee, der „Operation auf einer Menge“, die immer noch etwas vage ist, genauer fassen. Was bedeutet es, wenn zwei Elemente einer Menge „verknüpft“ werden? Man hat ein geordnetes Paar aus dem ersten und dem zweiten Element und ordnet diesem Paar ein Element der Menge zu, was dann als Ergebnis einer Operation angesehen wird. Dazu die folgende Definition.

- Definition

  Es sei M eine nichtleere Menge. Eine Abbildung $M \times M \to M$ heißt eine ***innere Verknüpfung*** auf M. (Oder kurz *Verknüpfung* oder *innere Komposition* oder *binäre Operation* auf M.)

  Es seien A und M zwei nichtleere Mengen. Eine Abbildung $A \times M \to M$ heißt eine ***äußere Verknüpfung*** von M mit A.

- Anmerkung: Die Mengen A und M können endlich oder unendlich sein. Auf M kann es mehrere Verknüpfungen geben.

- Definition

  Eine nichtleere Menge mit mindestens einer Verknüpfung heißt eine ***algebraische Struktur***.

- Beispiele

- Anmerkung: Es sei $f : M \times M \to M$ eine innere Verknüpfung auf M. Wird dem Paar $(a, b) \in M$ das Element $c \in M$ zugeordnet, kann man das durch $f((a, b)) = c$ oder einfacher $f(a, b) = c$ ausdrücken. Als kürzere Schreibweise wird allgemein

$$a * b = c \quad \text{oder} \quad ab = c$$

verwendet; konkret hat man dann $+$, $\cdot$, $\oplus$, $\odot$, u.s.w. als Operatoren.

Für eine Menge M mit einer inneren Verknüpfung $*$ wird $(M, *)$ geschrieben, zum Beispiel $(\mathbb{N}, +)$, $(\mathbb{Z}_n, \oplus)$ und $(\mathbb{Q}, \cdot)$. Beispiele mit zwei inneren Verknüpfungen sind $(\mathbb{Z}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$.

Eine Verknüpfung auf einer Menge M kann bestimmte Eigenschaften haben. Bei der Definition der Gruppe haben wir die Assoziativität (A), die Existenz eines neutralen Elementes (N), die Existenz inverser Elemente (I) und die Kommutativität (K) kennengelernt.

Man bekommt verschiedene algebraische Strukturen, je nachdem welche Verknüpfungen vorliegen und welche Eigenschaften (Rechenregeln) gelten.

- Anmerkung: Aufgrund der Definition ist bei einer Verknüpfung auf M die Eigenschaft der Verknüpfungsabgeschlossenheit (V) automatisch erfüllt.

- Definition

  Eine nichtleere Menge M mit einer assoziativen Verknüpfung heißt ***Halbgruppe***.

  Eine Halbgruppe mit einem neutralen Element heißt ***Monoid***.

- Übersicht

	(V)	(A)	(N)	(I)	(K)
innere Verknüpfung	×				
Halbgruppe	×	×			
Monoid	×	×	×		
Gruppe	×	×	×	×	
abelsche Gruppe	×	×	×	×	×

- Beispiele

- Satz

  (a) Eine Halbgruppe $(H, *)$, in der die Gleichungen $a * x = b$ und $y * a = b$ für alle a, $b \in H$ lösbar sind, ist eine Gruppe.

  (b) In einem Monoid gibt es genau ein neutrales Element.

- Beweis

- Definition

  Es sei R eine Menge mit zwei Verknüpfungen, einer Addition $+$, und einer Multiplikation $\cdot$. Dann heißt $(R, +, \cdot)$ ein ***Ring***, wenn die folgenden Eigenschaften gelten.

  (a) $(R, +)$ ist eine kommutative Gruppe.

  (b) $(R, \cdot)$ ist eine Halbgruppe.

  (c) Für alle a, b, $c \in R$ gelten die Distributivgesetze

  $$\begin{aligned} a(b+c) &= ab + ac, \\ (a+b)c &= ac + bc. \end{aligned}$$

- Anmerkung:

  (a) Das neutrale Element von $(R, +)$ ist 0.

  (b) Enthält $(R, \cdot)$ ein neutrales Element 1, gilt also $1 \cdot a = a$ und $a \cdot 1 = a$ für alle $a \in R$, so heißt R ein ***Ring mit Einselement***. Manchmal wird das von vorneherein in die Definition eines Ringes aufgenommen.

  (c) Ist $(R, \cdot)$ kommutativ, heißt R ein ***kommutativer Ring***.

- Beispiele

- Satz

  Es sei $(R, +, \cdot)$ ein Ring. Für beliebige a, $b \in R$ gilt

  (a) $a \cdot 0 = 0 \cdot a = 0$,

  (b) $a(-b) = (-a)b = -ab$,

  (c) $(-a)(-b) = ab$.

- Beweis

- Anmerkung: Ist $1 = 0$ folgt $R = \{0\}$, da für alle $a \in R$ die Umformung $a = 1 \cdot a = 0 \cdot a = 0$ gilt. Also folgt: Ist $R \neq \{0\}$, dann ist $1 \neq 0$.

- Definition

  Gibt es zu dem Element $a \neq 0$ aus dem Ring R ein Element $b \neq 0$ aus R so, daß $a \cdot b = 0$ gilt, dann heißt a ein ***linker Nullteiler***. Entsprechend wird der Begriff des rechten Nullteilers definiert.

  Ist ein Ringelement linker und rechter Nullteiler, heißt es einfach ein ***Nullteiler***. (Also ist in einem kommutativen Ring die Unterscheidung zwischen linkem und rechtem Nullteiler nicht nötig.)

- Beispiele

- Definition

  Es sei $(K, +, \cdot)$ ein Ring.

  (a) Ist $(K \setminus \{0\}, \cdot)$ eine Gruppe, so heißt $(K, +, \cdot)$ ein ***Schiefkörper***.

  (b) Ist $(K \setminus \{0\}, \cdot)$ eine kommutative Gruppe, heißt $(K, +, \cdot)$ ***Körper***.

- Beispiele

- Anmerkung: In einem Körper kann es wegen der Verknüpfungsabgeschlossenheit von $(K \setminus \{0\}, \cdot)$ keine Nullteiler geben.

- Satz

  $(\mathbb{Z}_n, \oplus, \odot)$ ist genau dann ein Körper, wenn n eine Primzahl ist.

- Beweis

- Satz

  (a) Es sei K ein endlicher Körper. Dann ist $|K| = p^n$ mit einer Primzahl p und einem $n \in \mathbb{N}$.

  (b) Zu jeder Primzahl p und jedem $n \in \mathbb{N}$ gibt es genau einen Körper mit p^n Elementen.

  (Ohne Beweis)

- Anmerkung: Der eindeutig existierende Körper mit p^n Elementen wird oft Galoisfeld der Ordnung p^n genannt und durch $GF(p^n)$ bezeichnet.

- Anmerkung: Es empfiehlt sich, an das modulare Rechnen mit den Zahlen 0, 1, ..., $(p-1)$ als „Standardmodell“ zu denken, wenn es um die Veranschaulichung endlicher Körper der Primzahlordnung p geht.