Formale Grundlagen

2008W

Institut für Algebra
Johannes Kepler Universität Linz

Vorlesung im 2008S

http://www.algebra.uni-linz.ac.at/Students/Win/fg

Inhalt

Halbgruppen

Definition

Sei A eine Menge und $\circ \in A \to A \to A$ eine zweistellige Operation darin. Dann heißt A zusammen mit $\circ$ eine Halbgruppe genau dann wenn $\circ$ assoziativ ist, d.h. wenn für alle $x, y, z \in A$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

Halbgruppen; Beispiele

1. alle Zahlenmengen, sowohl mit der Addition als auch mit der Multiplikation: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{A}, +)$, $(\mathbb{R}, +)$; $(\mathbb{N}, \cdot)$, $\ldots$, $(\mathbb{R}, \cdot)$;
2. die logischen Aussagen zusammen mit $\wedge$ oder $\vee$, also $(\mathbb{P}, \wedge)$ und $(\mathbb{P}, \vee)$;
3. die Potenzmenge einer Menge X zusammen mit Durchschnitt oder Vereinigung, also $(\mathbb{P}^X, \cap)$ und $(\mathbb{P}^X, \cup)$;
4. Für eine beliebiges Alphabet X, die Wörter (Listen) über diesem Alphabet zusammen mit der Konkatenation, also $(X^*, \diamond)$;
5. die Menge aller Funktionen einer Menge X in sich zusammen mit der Hintereinanderausführung, $(X \to X, \circ)$.
6. Die Menge aller Relationen auf einer Menge X zusammen mit dem Relationenprodukt.

Keine Halbgruppen

1. Potenzieren (nicht assoziativ)
2. Subtraktion (nicht assoziativ)
3. Logische Implikation (nicht assoziativ)
4. Addition ungerader Zahlen (keine abgeschlossene Operation)
5. Listeneinfügen

Monoid

Definition

Sei $(H, \circ)$ eine Halbgruppe und $e \in H$. Dann heißt e ein neutrales Element wenn für alle $h \in H$ gilt

$$e \circ h = h = h \circ e.$$

Man nennt dann H zusammen mit $\circ$ und e, also $(H, \circ, e)$, ein Monoid.

Satz

In jeder Halbgruppe gibt es höchstens ein neutrales Element.

Beweis.

Seien e_1, e_2 neutral. Dann gilt $e_1 = e_1 \circ e_2 = e_2$. □

Halbgruppen;Beispiele

Example

Alle vorhin erwähnten Beispiele für Halbgruppen besitzen ein neutrales Element und können daher als Monoide betrachtet werden.

Example

Halbgruppen ohne neutrales Element sind:

- die strikt positiven Zahlen mit Addition;
- die geraden Zahlen mit Multiplikation;
- nicht-leere Wörter (Listen) mit Verkettung.

Potenzieren

Definition

In einem Monoid H (mit neutralem Element 1) kann man auch Potenzieren: ist $h \in H$ und $n \in \mathbb{N}$, dann definiert man rekursiv

$$h^0 = 1$$
$$h^{n+1} = h \circ h^n.$$

Satz

Für alle $h \in H$, $n, m \in \mathbb{N}$ gilt

$$h^m \circ h^n = h^{m+n}, \tag{1}$$

Bemerkung

Im allgemeinen gilt aber nicht $(g \circ h)^n = g^n \circ h^n$.
Es gilt aber stets $h^m \circ h^n = h^n \circ h^m$.

Inverse Elemente

Definition

Sei $(G, \circ, 1)$ ein Monoid. Dann heißen $g, h \in G$ zueinander invers, wenn $g \circ h = 1 = h \circ g$ gilt. Besitzt jedes Element ein inverses, dann ist dieses eindeutig bestimmt und wird mit g^{-1} bezeichnet (oder mit $-g$, bei additiver Schreibweise). Das Monoid zusammen mit dieser zusätzlichen (einstelligen) Operation heißt dann eine Gruppe. D.h., $(G, \circ, 1, (^{-1}))$ ist eine Gruppe falls $(G, \circ, 1)$ ein Monoid ist und für alle $g \in G$ gilt

$$g \circ g^{-1} = 1 = g^{-1} \circ g.$$

Bemerkung

Die Notation für das Inverse passt gut zum Potenzieren, da damit tatsächlich die Beziehung in Gleichung (1) auf beliebige ganzzahlige Exponenten erweitert wird.

Gruppen; Beispiele

Example

$(\mathbb{Z}, +, 0, -)$, $(\mathbb{Q}, \cdot, (^{-1}))$, $(\mathbb{R}, \cdot, (^{-1}))$.

Bemerkung

Keine inversen Elemente gibt es dagegen bei der Listenverkettung. Auch die erwähnten logischen Operationen erlauben keine Inversen ($\neg A$ ist nicht invers zu A, denn $A \wedge \neg A = \bot$, neutral ist aber $\top$). Auch $(X \to X, \circ)$ führt zu keiner Gruppe, da Funktionen nur dann ein Inverses haben, wenn sie bijektiv sind.

Example

Allerdings ergibt die Hintereinanderausführung von bijektiven Funktionen wieder eine bijektive Funktion (es gilt konkret: $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$, man beachte die Umkehrung der Reihenfolge), weshalb die Menge der bijektiven Funktionen von $X \to X$, oft auch Permutationen von X genannt und mit $P(X)$ bezeichnet, sehr wohl eine Gruppe bildet. Im Gegensatz zu den erwähnten Gruppen mit Zahlen, ist die Gruppe der Permutationen nicht kommutativ.

Ringe;Distributivgesetze

Definition

Sei $(R, +, 0, -)$ eine kommutative Gruppe und $(R, \cdot, 1)$ ein Monoid, dann heißt $(R, +, 0, -, \cdot, 1)$ ein Ring, falls zusätzlich die Distributivgesetze

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$

gelten.

Bemerkung

Da sich die jeweiligen neutralen Elemente und die Operation für das Inverse eindeutig ergeben, spricht man kürzer vom Ring $(R, +, \cdot)$, oder einfach vom Ring R, falls auch die Operationen aus dem Zusammenhang klar sind.

Kommutative Ringe

Bemerkung

Man beachte, daß man beide Distributivgesetze benötigt, da die Multiplikation nicht immer als kommutativ vorausgesetzt wird.

Bemerkung

Die bekannten Beispiele $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *sind allerdings allsamt kommutative Ringe.*

Bemerkung

Nicht-kommutative Ringe ergeben sich in natürlicher Weise in der Linearen Algebra duch lineare Abbildungen oder Matrizen.

Ringe;Beispiele

Example

Eine weitere wichtige Klasse von kommutativen Ringen bilden die Restklassenringe $\mathbb{Z}_m$, welche im wesentlichen dem Ring $\mathbb{Z}$ entsprechen, allerdings werden zwei Elemente als gleich betrachtet, wenn die modulo m denselben Rest ergeben, d.h.
$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Example

Polynomringe: ist R ein kommutativer Ring, dann bezeichnen wir mit $R[x]$ den Ring aller Polynome in der Variablen x mit Koeffizienten aus R, d.h.

$$R[x] = \{\sum_{k=0}^{n} a_k x^k \mid n \epsilon \mathbb{N},\ a_1\ \ldots, a_n \epsilon R\}.$$

Körper

Definition

Bildet in einem kommutativen Ring $(K, +, \cdot)$ die Menge K^* der von 0 verschiedenen Elemente eine Gruppe, dann nennt man K einen Körper.

Example

$\mathbb{Q}, \mathbb{A}, \mathbb{R}, \mathbb{C}$;

$\mathbb{Z}_p$, wobei p eine Primzahl ist.