Prof. Dr. H. Brenner **Osnabrück SS 2020**

Diskrete Mathematik

Vorlesung 4

Vorli mag alle Menschen und achtet nicht auf Äußerlichkeiten. Ihr besonderes Talent ist aber, ...

Verknüpfungen

In den beiden folgenden Vorlesungen werden wir die algebraischen Begrifflichkeiten zusammenstellen, die immer wieder verwendet werden und zu einem Großteil aus den Anfängervorlesungen bekannt sein dürften.

Definition 4.1. Eine *Verknüpfung* $\circ$ auf einer Menge M ist eine Abbildung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto \circ(x,y) = x \circ y.$$

Eine Verknüpfung macht also aus einem Paar

$$(x,y)\ \in\ M \times M$$

ein einziges Element

$$x \circ y\ \in\ M.$$

Eine Vielzahl von mathematischen Konstruktionen fällt unter diesen Begriff: Die Addition, die Differenz, die Multiplikation, die Division von Zahlen, die

Verknüpfung von Abbildungen, der Durchschnitt oder die Vereinigung von Mengen, etc. Als Verknüpfungssymbol kommt eine ganze Reihe in Frage, z.B. $\circ, \cdot, +, -, \oplus, \clubsuit, \heartsuit$ u.s.w.

Wichtige strukturelle Eigenschaften einer Verknüpfung werden in den folgenden Definitionen aufgelistet.

DEFINITION 4.2. Eine Verknüpfung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto x \circ y,$$

auf einer Menge M heißt *kommutativ*, wenn für alle $x, y \in M$ die Gleichheit

$$x \circ y = y \circ x$$

gilt.

DEFINITION 4.3. Eine Verknüpfung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto x \circ y,$$

auf einer Menge M heißt *assoziativ*, wenn für alle $x, y, z \in M$ die Gleichheit

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

gilt.

DEFINITION 4.4. Es sei eine Menge M mit einer Verknüpfung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto x \circ y,$$

gegeben. Dann heißt ein Element $e \in M$ *neutrales Element* der Verknüpfung, wenn für alle $x \in M$ die Gleichheit $x \circ e = x = e \circ x$ gilt.

Im kommutativen Fall muss man natürlich für das neutrale Element nur eine Reihenfolge betrachten.

DEFINITION 4.5. Es sei eine Menge M mit einer Verknüpfung

$$\circ\colon\ M \times M \longrightarrow M,\ (x,y) \longmapsto x \circ y,$$

und einem neutralen Element $e \in M$ gegeben. Dann heißt zu einem Element $x \in M$ ein Element $y \in M$ *inverses Element*, wenn die Gleichheit

$$x \circ y = e = y \circ x$$

gilt.

DEFINITION 4.6. Ein *Monoid* ist eine Menge M zusammen mit einer Verknüpfung

$$\circ\colon\ M \times M \longrightarrow M$$

und einem ausgezeichneten Element $e \in M$ derart, dass folgende beiden Bedingungen erfüllt sind.

(1) Die Verknüpfung ist *assoziativ*, d.h. es gilt

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

für alle $x, y, z \in M$.

(2) e ist *neutrales Element* der Verknüpfung, d.h. es gilt

$$x \circ e = x = e \circ x$$

für alle $x \in M$.

Die natürlichen Zahlen bilden mit der Addition das kommutative Monoid $(\mathbb{N}, +, 0)$ und mit der Multiplikation das kommutative Monoid $(\mathbb{N}, \cdot, 1)$.

Beispiel 4.7. Es sei L eine Menge und

$$M = \text{Abb}\,(L, L)$$

die Menge aller Abbildungen von L in sich. Durch die Hintereinanderschaltung von Abbildungen liegt eine Verknüpfung auf M vor, die aufgrund von Lemma 3.15 (Mathematik für Anwender (Osnabrück 2019-2020)) assoziativ ist. Dagegen ist sie nicht kommutativ. Die Identität auf L ist das neutrale Element. Eine Abbildung $f\colon L \to L$ besitzt genau dann ein inverses Element, wenn sie bijektiv ist; das inverse Element ist einfach die Umkehrabbildung.

Potenzen

Es sei $(M, \cdot, 1)$ ein multiplikativ geschriebenes Monoid. Zu $a \in M$ und eine positive natürliche Zahl $n \in \mathbb{N}_+$ setzt man

$$a^n := \underbrace{a \cdots a}_{n-\text{fach}}$$

und nennt dies die n-te *Potenz* von a. Weiter setzen wir

$$a^0 := 1.$$

Man beachte, dass bei der Potenz a^n die Basis a aus dem Monoid und der Exponent n eine natürliche Zahl ist. Der Ausdruck a^b mit a, b aus dem Monoid hat im Allgemeinen keine Bedeutung.

Wie für die natürlichen Zahlen (siehe Lemma Anhang 1.10) gelten in jedem (kommutativen) Monoid die folgenden *Potenzgesetze*.

Lemma 4.8. *Es sei M ein Monoid, $a, b \in M$ und $m, n \in \mathbb{N}$. Dann gelten die folgenden* Potenzgesetze.

(1)
$$a^{m+n} = a^m \cdot a^n.$$

(2)
$$(a^m)^n = a^{mn}.$$

(3) *Wenn M kommutativ ist, so ist*
$$(a \cdot b)^n = a^n \cdot b^n.$$

Beweis. Siehe Aufgabe 4.11. □

Wenn das Monoid additiv geschrieben wird, so schreibt man na für die n-fache Summe von a mit sich selbst und spricht von Vielfachen statt von Potenzen. Es gelten dann die entsprechenden Vielfachgesetze, nämlich

$$(m+n)a = ma + na,$$
$$n(ma) = (nm)a,$$
$$n(a+b) = na + nb.$$

Kommutative Halbringe

Wir betrachten nun algebraische Strukturen, bei denen es wie bei den natürlichen Zahlen zwei Verknüpfungen gibt.

Definition 4.9. Ein *kommutativer Halbring* R ist eine Menge mit Verknüpfungen $+$ und $\cdot$ (genannt *Addition* und *Multiplikation*) und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) Die Addition ist eine kommutative, assoziative Verknüpfung, für die 0 das neutrale Element ist.
(2) Die Multiplikation ist eine kommutative, assoziative Verknüpfung, für die 1 das neutrale Element ist.
(3) Es gilt das *Distributivgesetz*, also
$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$
für alle $a, b, c \in R$.

Korollar 4.10. *Die natürlichen Zahlen* $\mathbb{N}$ *bilden einen kommutativen Halbring.*

Beweis. Dies folgt unmittelbar aus Lemma Anhang 1.5 und aus Lemma Anhang 1.9. □

Neben den natürlichen Zahlen gibt es viele weitere Halbringe, beispielsweise die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ oder die komplexen Zahlen $\mathbb{C}$.

Wir lassen das Produktzeichen $\cdot$ häufig weg, wenn das nicht zu Missverständnissen führen kann und wir benutzen allgemein die *Klammerkonvention*, dass Punktrechnung stärker bindet als Strichrechnung, d.h. wir schreiben einfach $ab + cd$ statt $(ab) + (cd)$. An weiteren Notationen verwenden wir (gemäß den oben eingeführten Bezeichnungen für Monoide) für ein Halbringelement $a \in R$ und eine positive natürliche Zahl $n \in \mathbb{N}_+$ die Schreibweisen (n-tes *Vielfaches* von a und n-te *Potenz* von a) $na = a + \cdots + a$ (n Summanden) und $a^n = a \cdots a$ (n Faktoren). Statt $n1 = n1_R$ schreiben wir einfach n (bzw.

manchmal n_R), d.h. jede natürliche Zahl findet sich in jedem Halbring wieder. Die Schreibweise na könnte man dann auch als das Produkt

$$(1+1+\cdots+1)\cdot a$$

(mit n Einsen) lesen, was aber aufgrund des Distributivgesetzes mit der n-fachen Summe von a mit sich selbst übereinstimmt. Für

$$n = 0$$

ist dies jedenfalls als $0\cdot a$ im Halbring zu lesen, was nicht ohne weiteres gleich 0 sein muss (aber in allen für uns wichtigen Beispielen gleich 0 ist). Weiter setzen wir

$$a^0 = 1.$$

Mit diesen Bezeichnungen gilt nach Lemma 4.8 beispielsweise

$$(m+n)a = ma + na$$

und

$$(m\cdot n)a = m\cdot(na)$$

für natürliche Zahlen $m, n \in \mathbb{N}_+$ (man mache sich klar, was hier jeweils die Multiplikation bezeichnet).

Wie bei den natürlichen Zahlen verwenden wir das Summenzeichen $\sum$ und das Produktzeichen $\prod$. Für indizierte Elemente $a_1, \ldots, a_k$ aus R ist also

$$\sum_{i=1}^{k} a_i = a_1 + \cdots + a_k$$

und

$$\prod_{i=1}^{k} a_i = a_1 \cdots a_k.$$

Die beiden folgenden extremen Beispiele zeigen, wie verschieden ein Halbring von dem Halbring der natürlichen Zahlen sein kann. Dennoch gelten alle aus den Halbringaxiomen ableitbaren Eigenschaften auch in diesen beiden Beispielen.

Beispiel 4.11. Die einelementige Menge $R = \{0\}$ kann man zu einem kommutativen Halbring machen, indem man sowohl die Addition als auch die Multiplikation auf die einzig mögliche Weise erklärt, nämlich durch $0+0=0$ und $0\cdot 0 = 0$. In diesem Fall ist $1 = 0$, dies ist also ausdrücklich erlaubt. Die Rechengesetze in einem Halbring sind hier trivialerweise erfüllt, da bei jeder zu erfüllenden Gleichung links und rechts sowieso immer 0 herauskommt. Diesen Halbring nennt man den *Nullring*.

Nach dem Nullring ist der folgende Ring (sogar Körper, siehe die nächste Vorlesung) der zweitkleinste Halbring.

Beispiel 4.12. Wir suchen nach einer Halbringstruktur auf der Menge $\{0,1\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element der Multiplikation sein soll, so ist dadurch schon viel festgelegt. Nach Lemma 4.13 muss

$$0 \cdot 0 = 0$$

gelten. Ferner legen wir

$$1 + 1 = 0$$

fest. Die Verknüpfungstabellen (oder Operationstafeln) sehen somit wie folgt aus.

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

Durch etwas aufwändiges Nachrechnen stellt man fest, dass es sich in der Tat um einen kommutativen Halbring handelt.

Eine „natürliche“ Interpretation dieses Halbringes gewinnt man, wenn man sich die geraden natürlichen Zahlen durch 0 und die ungeraden natürlichen Zahlen durch 1 repräsentiert denkt. Beispielsweise ist die Summe zweier ungerader Zahlen stets gerade, was der obigen Gleichung $1 + 1 = 0$ entspricht. Wie oben erwähnt lassen sich in jedem kommutativen Halbring die natürlichen Zahlen eindeutig interpretieren, dabei können aber, wie in den beiden Beispielen, verschiedene Zahlen gleich werden. Im Beispiel wird jede gerade Zahl zu 0 und jede ungerade Zahl zu 1.

Lemma 4.13. *In einem kommutativen Halbring gilt*

$$0 \cdot 0 = 0.$$

Beweis. Dies ergibt sich aus

$$0 \cdot 0 = 0 \cdot 0 + 0 = 0 \cdot 0 + 0 \cdot 1 = 0 \cdot (0 + 1) = 0 \cdot 1 = 0.$$

□

Das folgende Beispiel zeigt, dass in einem kommutativen Halbring im Allgemeinen nicht die Gleichung

$$0x = 0$$

für alle x gilt. Für die natürlichen Zahlen und in jedem kommutativen Ring gilt diese Eigenschaft. Es ist also keineswegs so, dass man jede von den Zahlenbereichen her vertraute Eigenschaft aus dem Begriff eines kommutativen Halbringes ableiten kann.

Beispiel 4.14. Wir suchen nach einer Halbringstruktur auf der dreielementigen Menge $\{0,1,u\}$. Wenn 0 das neutrale Element einer Addition und 1 das neutrale Element der Multiplikation sein soll, so ist dadurch schon viel festgelegt. Wir legen die Verknüpfungen durch die Verknüpfungstabellen

$+$	0	1	u
0	0	1	u
1	1	1	u
u	u	u	u

und

$\cdot$	0	1	u
0	0	0	u
1	0	1	u
u	u	u	u

fest. Durch etwas aufwändiges Nachrechnen stellt man fest, dass es sich in der Tat um einen kommutativen Halbring handelt.

Die folgende Aussage heißt das *allgemeine Distributivgesetz*.

Satz 4.15. *Es sei R ein kommutativer Halbring und es seien $a_1, \ldots, a_r, b_1, \ldots, b_s$ Elemente aus R. Dann gilt das* allgemeine Distributivgesetz

$$\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{k=1}^{s} b_k\right) = \sum_{1 \leq i \leq r,\, 1 \leq k \leq s} a_i b_k.$$

Beweis. Wir machen eine Doppelinduktion nach r und nach s. D.h. wir beweisen die Aussage für jedes feste r durch Induktion nach s (innere Induktion) und erhöhen dann in einem eigenen Induktionsdurchgang r (äußere Induktion). Bei $r = 0$ ist nichts zu zeigen, da dann die Summen links und rechts leer sind, also gleich 0. Sei also $r = 1$, so dass der linke Faktor einfach eine fixierte Zahl $a = a_1$ ist. Wir wollen die Aussage in dieser Situation für beliebiges s zeigen. Bei $s = 0, 1$ ist die Aussage klar. Sei die Aussage nun für ein

$$s \geq 2$$

schon bewiesen. Dann ist

$$\begin{aligned} a \cdot (b_1 + \cdots + b_s + b_{s+1}) &= a \cdot ((b_1 + \cdots + b_s) + b_{s+1}) \\ &= a \cdot (b_1 + \cdots + b_s) + a b_{s+1} \end{aligned}$$

nach dem Distributivgesetz und mit der Induktionsvoraussetzung folgt die Aussage. Sei die Aussage nun für ein festes r und jedes s bewiesen. Dann ist wieder mit dem Distributivgesetz und der Induktionsvoraussetzung

$$\left(\sum_{i=1}^{r+1} a_i\right) \cdot \left(\sum_{k=1}^{s} b_k\right) = \left(\left(\sum_{i=1}^{r} a_i\right) + a_{r+1}\right) \cdot \left(\sum_{k=1}^{s} b_k\right)$$

$$\begin{aligned} &= \left(\sum_{i=1}^{r} a_i\right) \cdot \left(\sum_{k=1}^{s} b_k\right) + a_{r+1} \cdot \left(\sum_{k=1}^{s} b_k\right) \\ &= \sum_{1 \leq i \leq r,\, 1 \leq k \leq s} a_i b_k + \sum_{k=1}^{s} a_{r+1} b_k \\ &= \sum_{1 \leq i \leq r+1,\, 1 \leq k \leq s} a_i b_k. \end{aligned}$$

□

Das allgemeine Distributivgesetz gilt auch für mehr als zwei Faktoren, siehe Aufgabe 4.21.

Die Potenzmenge als kommutativer Halbring

LEMMA 4.16. *Zu einer Menge M sei $R = \mathfrak{P}(M)$ die Potenzmenge zu M. Dann ist R mit der Vereinigung $\cup$ als Addition und der leeren Menge als 0 und mit dem Durchschnitt $\cap$ als Multiplikation und der Gesamtmenge M als 1 ein kommutativer Halbring.*

Beweis. Die Eigenschaften sind allenfalls bis auf das Distributivgesetz klar. Letzteres besagt die Identität

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Wenn ein Element x links dazugehört, so gehört es zu A und es gehört zu $B \cup C$. Somit gehört es zu B oder zu C und damit auch zu $A \cap B$ oder zu $A \cap C$, also jedenfalls zur rechten Seite. Wenn es rechts dazu gehört, sagen wir zu $A \cap B$, was wir wegen der Symmetrie der Situation annehmen können, so gehört es erst recht zu $A \cap (B \cup C)$. □

Im vorstehenden Beispiel kann man die Rollen der Addition und der Multiplikation vertauschen, da das Distributivgesetz auch in der Form

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

gilt.

Der binomische Lehrsatz

Die folgende *allgemeine binomische Formel* oder *binomischer Lehrsatz* bringt die Addition, die Multiplikation und die Potenzierung in einem kommutativen Halbring und insbesondere für die natürlichen Zahlen miteinander in Beziehung.

SATZ 4.17. *Es sei R ein kommutativer Halbring und $a, b \in R$. Ferner sei n eine natürliche Zahl. Dann gilt*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\,.$$

Beweis. Wir führen Induktion nach n. Für $n = 0$ steht einerseits $(a+b)^0 = 1$ und andererseits $a^0 b^0 = 1$. Sei die Aussage bereits für n bewiesen. Dann ist

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&= a\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) + b\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{k=1}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=1}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
\end{aligned}$$

□

Den vorstehenden Satz kann man sich auf folgendermaßen klar machen. Beim Ausmultiplizieren von

$$(a+b)^n = \underbrace{(a+b)\cdot(a+b)\cdots(a+b)}_{n\text{-fach}}$$

muss jeder Summand gemäß dem allgemeinen Distributivgesetz (in jedem Faktor) mit jedem Summanden multipliziert werden. Für jedes Teilprodukt muss man sich bei jedem Faktor entscheiden, ob man den vorderen Summanden a oder den hinteren Summanden b nimmt. Die einzelnen Produkte haben die Form $a^k b^{n-k}$, wobei k die Anzahl der Faktoren ist, bei denen a gewählt wurde und $n-k$ die Anzahl der Faktoren ist, bei denen b gewählt wurde. Wenn man k fixiert, so kann man sich fragen, auf wie viele Arten das Produkt $a^k b^{n-k}$ zustande kommen kann. Eine solche Möglichkeit ist dadurch gegeben, dass man unter den n Faktoren bestimmt, an welchen von

ihnen a gewählt wird. Die Anzahl der Möglichkeiten ist also die Anzahl der k-elementigen Teilmengen von $\{1, \ldots, n\}$, also gleich $\binom{n}{k}$.

Abbildungsverzeichnis

Quelle = Waeller27.jpg , Autor = Benutzer Odatrulle auf Commons, Lizenz = CC-by-sa 4.0 1

Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von http://commons.wikimedia.org) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 11

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 11