

Grundkurs Mathematik I

Vorlesung 11

Kultur ist Reichtum an
Problemen.

Egon Friedell

Axiomatik

Wir haben schon für die intuitiv bekannten natürlichen Zahlen ein Axiomensystem eingeführt, das speziell auf die natürlichen Zahlen zugeschnitten war und das sogar die Eigenschaft besitzt, dass es die natürlichen Zahlen in dem Sinne charakterisiert, dass je zwei Strukturen (je zwei Modelle), die dieses Axiomensystem erfüllen, zueinander in eine eindeutige Beziehung gebracht werden können, also im Wesentlichen gleich sind (siehe Satz 7.2).

In dieser Vorlesung werden wir eine andere Art von *Axiomensystem* kennenlernen, wie sie in der Mathematik typisch ist. Man fasst verschiedene strukturelle Eigenschaften, die in einem bestimmten Kontext immer wieder auftauchen, in einen neuen Begriff zusammen. Das Ziel ist dabei, weitere Eigenschaften aus einigen wenigen Grundeigenschaften logisch zu erschließen. Man argumentiert dann nicht auf der Ebene vertrauter Beispiele, wie der natürlichen Zahlen, sondern auf der Ebene der Eigenschaften. Der Gewinn ist dabei, dass man mathematische Schlüsse nur einmal auf der abstrakten Ebene der Eigenschaften durchführen muss und diese dann für alle Modelle gelten, die die jeweiligen Grundeigenschaften erfüllen, also unter den Begriff fallen. Zugleich erkennt man logische Abhängigkeiten und Hierarchien zwischen Eigenschaften, die häufig auch im Lernprozess versteckt vorliegen und auch eine gewisse Orientierung für die Didaktik geben, selbst wenn nicht axiomatisch argumentiert wird.

In diesem Sinne werden wir im Laufe der Vorlesung die Begriffe Halbringe, Ringe, Gruppen und Körper kennen lernen (auch der Ordnungsbegriff ist ein axiomatischer Begriff).

Kommutative Halbringe

Wir fassen die bisher etablierten algebraischen Eigenschaften der natürlichen Zahlen in einem eigenen Begriff zusammen.

DEFINITION 11.1. Ein *kommutativer Halbring* R ist eine Menge mit zwei 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 11.2. Die natürlichen Zahlen \mathbb{N} bilden einen kommutativen Halbring.

Beweis. Dies folgt unmittelbar aus Lemma 8.10 und aus Lemma 9.2. □

Neben den natürlichen Zahlen gibt es viele weitere Halbringe, beispielsweise die ganzen Zahlen \mathbb{Z} , die rationalen Zahlen \mathbb{Q} oder die reellen Zahlen \mathbb{R} . Wenn man eine Eigenschaft aus den Gesetzen eines Halbringes erschließen kann, so gilt diese Eigenschaft in jedem Halbring. Sobald man also für eine Struktur gezeigt hat, dass ein Halbring vorliegt, so hat man damit auch automatisch gezeigt, dass diese neue Eigenschaft gilt. Dies ist letztlich ein sehr ökonomisches Vorgehen! Der Preis ist, dass man zusätzliche Begriffe einführen muss und dass man sehr abstrakt argumentieren muss.

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 für ein Halbringelement $a \in R$ und eine positive natürliche Zahl $n \in \mathbb{N}_+$ die Schreibweisen $na = a + \cdots + a$ (n Summanden) und $a^n = a \cdots a$ (n Faktoren). Hier muss man also richtig die Anzahl der Summanden bzw. die Anzahl der Faktoren zählen. 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 dieser Bezeichnung gilt 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, \dots, a_k aus R ist also

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

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 11.3. 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 der zweitkleinste Halbring.

BEISPIEL 11.4. 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 11.5 muss

$$0 \cdot 0 = 0$$

gelten. Ferner legen wir

$$1 + 1 = 0$$

fest. Die Operationstabellen sehen somit wie folgt aus.

+	0	1
0	0	1
1	1	0

und

·	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.¹

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 11.5. *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 Eigenschaft, die im derzeit hauptsächlich interessierenden Zahlenbereich (also derzeit die natürlichen Zahlen) aus dem Begriff eines kommutativen Halbringes ableiten kann.

BEISPIEL 11.6. 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

¹Sogar um einen Körper, einen Begriff, den wir später einführen werden.

\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 11.7. *Es sei R ein kommutativer Halbring und es seien $a_1, \dots, a_r, b_1, \dots, b_s$ 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

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

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

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

□

Die binomische Formel

Die Gültigkeit der ersten binomischen Formel ist keine Besonderheit der natürlichen Zahlen, sondern folgt allein aus den im Begriff einer Halbgruppe zusammengefassten Eigenschaften.

KOROLLAR 11.8. *In einem kommutativen Halbring R gilt die erste binomische Formel, also die Beziehung*

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Beweis. Unter mehrfacher Verwendung des Distributivgesetzes und der Kommutativgesetze ist

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) \\ &= a(a + b) + b(a + b) \\ &= a \cdot a + a \cdot b + b \cdot a + b \cdot b \\ &= a^2 + a \cdot b + a \cdot b + b^2 \\ &= a^2 + 2a \cdot b + b^2. \end{aligned}$$

□

Die zweite und die dritte binomische Formel lässt sich nicht in einem beliebigen Halbring formulieren, da in ihnen das Minuszeichen bzw. die Subtraktion vorkommt, die es in einem beliebigen kommutativen Halbring nicht gibt und die innerhalb der natürlichen Zahlen auch nur eingeschränkt ausführbar ist. Stattdessen werden wir uns den höheren Potenzen von Summen zuwenden. Die *erste binomische Formel* besagt wie eben formuliert

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Für die dritte Potenz einer Summe gilt

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

und für die vierte Potenz

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Worauf beruht dieser Zusammenhang und wo kommen diese Vorfaktoren her? Betrachten wir die dritte Potenz. Es ist (wieder in einem beliebigen kommutativen Halbring)

$$\begin{aligned} (a + b)^3 &= (a + b)(a + b)^2 \\ &= (a + b)(a^2 + 2ab + b^2) \\ &= a(a^2 + 2ab + b^2) + b(a^2 + 2ab + b^2) \\ &= a^3 + 2a^2b + ab^2 + a^2b + 2ab^2 + b^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3. \end{aligned}$$

Für die vierte Potenz siehe Aufgabe 11.20. In dieser Weise kann man jede Potenz einer Summe als Summe von Produkten ausdrücken, wobei die auftretenden Koeffizienten *Binomialkoeffizienten* heißen. Um diese einzuführen,

müssen wir uns mit elementarer Kombinatorik beschäftigen, was wir in der übernächsten Vorlesung tun werden.

Die Potenzmenge

Wir schließen mit einem Objekt ab, das ein eher ungewöhnliches Beispiel für einen kommutativen Halbring und auch ein Beispiel für eine geordnete, aber nicht total geordnete Menge ist, die Potenzmenge. Sie ist auch wichtig im Rahmen der elementaren Kombinatorik.

DEFINITION 11.9. Zu einer Menge M nennt man die Menge aller Teilmengen von M die *Potenzmenge* von M . Sie wird mit

$$\mathfrak{P}(M)$$

bezeichnet.

Wenn M die Menge der Leute im Kurs sind, so kann man $\mathfrak{P}(M)$ als die Menge aller Parties auffassen, die diese Leute feiern können, wenn man eine Party mit der Menge der anwesenden Leute identifiziert.

BEISPIEL 11.10. Sei M eine beliebige Menge und

$$R = \mathfrak{P}(M)$$

die Potenzmenge davon. Dann sind die Elemente aus $R = \mathfrak{P}(M)$ - also die Teilmengen von M - durch die Inklusionsbeziehung \subseteq geordnet. Die Reflexivität bedeutet einfach, dass eine jede Menge in sich selbst enthalten ist und die Transitivität bedeutet, dass aus $T_1 \subseteq T_2$ und $T_2 \subseteq T_3$ die Inklusion $T_1 \subseteq T_3$ folgt. Die Antisymmetrie ist dabei ein wichtiges Beweisprinzip für die Gleichheit von Mengen: Zwei Mengen T_1, T_2 sind genau dann gleich, wenn $T_1 \subseteq T_2$ und umgekehrt $T_2 \subseteq T_1$ gilt.

LEMMA 11.11. 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 $A \cap (B \cup C)$. \square

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.