Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 12

Ringe

Wir beginnen einen neuen Abschnitt dieser Vorlesung, in dem es um Ringe geht.

DEFINITION 1. Ein *Ring* R ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$ und mit zwei ausgezeichneten Elementen 0 und 1 derart, dass folgende Bedingungen erfüllt sind:

(1) $(R, +, 0)$ ist eine abelsche Gruppe.
(2) $(R, \cdot, 1)$ ist ein Monoid.
(3) Es gelten die *Distributivgesetze*, also $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ für alle $a, b, c \in R$.

DEFINITION 2. Ein Ring R heißt *kommutativ*, wenn die Multiplikation kommutativ ist.

In einem kommutativen Ring muss man nicht zwischen den beiden Formen des Distributivgesetzes unterscheiden. Das Basismodell für einen (kommutativen) Ring bildet die Menge der ganzen Zahlen $\mathbb{Z}$ mit der natürlichen Addition und Multiplikation. Die 0 ist das neutrale Element der Addition und die 1 ist das neutrale Element der Multiplikation. Der Nachweis, dass $\mathbb{Z}$ die Axiome eines Ringes, also die oben aufgelisteten Eigenschaften, erfüllt, beruht letztlich auf den Peano-Axiomen für die natürlichen Zahlen $\mathbb{N}$ und ist ziemlich formal. Darauf wollen wir verzichten und stattdessen diese seit langem vertrauten Gesetzmäßigkeiten akzeptieren. Die natürlichen Zahlen bilden keinen Ring, da sie noch nicht einmal eine additive Gruppe bilden. Die Zahlbereiche $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind ebenfalls kommutative Ringe, wobei der Nachweis der Eigenschaften dadurch geschieht, dass man die Konstruktion dieser Zahlbereiche aus den „vorhergehenden“ betrachtet (etwa $\mathbb{R}$ aus $\mathbb{Q}$) und die Gültigkeit (in $\mathbb{R}$) auf die Gültigkeit im „Vorgänger“ ($\mathbb{Q}$) zurückführt.

Wir benutzen allgemein die *Klammerkonvention*, dass Punktrechnung stärker bindet als Strichrechnung, d.h. wir schreiben einfach $ab + cd$ statt $(ab) + (cd)$. Das Inverse zu $a \in R$ bzgl. der Addition, das es ja immer gibt, schreiben wir als $-a$ und nennen es das *Negative* von a. Statt $a + (-b)$ schreiben wir $a - b$. An weiteren Notationen verwenden wir für ein Ringelement $a \in R$ und eine natürliche Zahl $n \in \mathbb{N}$ die Schreibweisen $na = a + \ldots + a$ (n Summanden) und $a^n = a \cdots a$ (n Faktoren). Bei negativen $n \in \mathbb{Z}$ ist $na = (-n)(-a)$ zu interpretieren (dagegen macht a^n mit negativen Exponenten im Allgemeinen keinen Sinn). Statt $n1 = n1_R$ schreiben wir einfach n (bzw. manchmal n_R), d.h. jede ganze Zahl findet sich in jedem Ring wieder.

Beispiel 3. (Der Nullring) Die einelementige Menge $R = \{0\}$ kann man zu einem Ring 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. Diesen Ring nennt man den *Nullring*.

Nach dem Nullring ist der folgende Ring der zweitkleinste Ring.

Beispiel 4. Wir suchen nach einer Ringstruktur 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 alles festgelegt, da $1 + 1 = 0$ sein muss. Die Operationstafeln sehen also 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 Ring handelt (sogar um einen Körper).

Lemma 5. *Sei R ein Ring und seien a, b, c, a_i, b_k Elemente aus R. Dann gelten folgende Aussagen*

(1) $0a = a0 = 0$ *(Annullationsregel),*
(2) $a(-b) = -ab = (-a)b$
(3) $(-a)(-b) = ab$ *(Vorzeichenregel),*
(4) $a(b - c) = ab - ac$ *und* $(b - c)a = ba - ca$,
(5) $(\sum_{i=1}^{r} a_i)(\sum_{k=1}^{s} b_k) = \sum_{1 \le i \le r,\, 1 \le k \le s} a_i b_k$ *(allgemeines Distributivgesetz).*

Beweis. Wir beweisen im nicht kommutativen Fall je nur eine Hälfte.

(1) Es ist $a0{=}a(0 + 0){=}a0 + a0$. Durch beidseitiges Abziehen von $a0$ ergibt sich die Behauptung.
(2)
$$(-a)b + ab{=}(-a + a)b{=}0b{=}0$$
nach Teil (1). Daher ist $(-a)b$ das (eindeutig bestimmte) Negative von ab.
(3) Nach (2) ist $(-a)(-b) = (-(-a))b$ und wegen $-(-a) = a$ (dies gilt in jeder Gruppe) folgt die Behauptung.
(4) Dies folgt auch aus dem bisher Bewiesenen.
(5) Dies folgt aus einer einfachen Doppelinduktion.

□

Die Binomialkoeffizienten

DEFINITION 6. Es seien k und n natürliche Zahlen mit $k \leq n$. Dann nennt man

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

den *Binomialkoeffizienten* „n über k“.

Wenn $k > n$ ist oder wenn k negativ ist so setzt man den Binomialkoeffizienten gleich null.

SATZ 7. *(Binomischer Lehrsatz) Es sei R ein kommutativer Ring 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 $a^0 b^0 = 1$. Bei $n = 1$ hat man einerseits $(a+b)^1 = a+b$ und andererseits $a^1 b^0 + a^0 b^1 = a+b$. Sei die Aussage bereits für n bewiesen. Dann ist

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

□

Nichtnullteiler und Integritätsbereiche

DEFINITION 8. Ein Element a in einem kommutativen Ring R heißt *Nullteiler*, wenn es ein von null verschiedenes Element b gibt mit $ab = 0$. Andernfalls heißt es ein *Nichtnullteiler*.

Im nicht kommutativen Fall hat man zwischen Links- und Rechtsnullteilern zu unterscheiden. Die Eins ist stets ein Nichtnullteiler, da aus $1b = 0$ sofort $b = 0$ folgt. Andererseits ist das Nullelement stets ein Nullteiler, es sei denn, der Nullring liegt vor.

LEMMA 9. *Es sei R ein kommutativer Ring und sei $f \in R$ ein Nichtnullteiler. Dann folgt aus einer Gleichung*

$$fx = fy\,,$$

dass $x = y$ sein muss.

Beweis. Man kann die Gleichung umschreiben als

$$0{=}fx - fy{=}f(x - y).$$

Da f ein Nichtnullteiler ist, ist $x - y = 0$, also $x = y$. □

Ein Ring, bei dem es außer der Null keine Nullteiler gibt, heißt *nullteilerfrei*.

DEFINITION 10. Ein kommutativer, nullteilerfreier, von null verschiedener Ring heißt *Integritätsbereich*.

Die Eigenschaft, dass jedes Element $\neq 0$ ein Nichtnullteiler ist, kann man auch so ausdrücken, dass aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt, bzw., dass mit $a \neq 0$ und $b \neq 0$ auch $ab \neq 0$ ist.

Unterringe

DEFINITION 11. Eine Teilmenge $S \subseteq R$ eines Ringes nennt man einen *Unterring*, wenn sowohl $(S, +, 0)$ eine Untergruppe von $(R, +, 0)$ als auch $(S, \cdot, 1)$ ein Untermonoid von $(R, \cdot, 1)$ ist.

Diese Bedingung besagt insbesondere, dass sich die Addition und die Multiplikation von R auf S einschränken lässt. Ein Unterring ist selbst ein Ring. Zum Nachweis, dass eine gegebene Teilmenge $S \subseteq R$ ein Unterring ist, hat man Folgendes zu zeigen.

(1) $0, 1 \in S$.
(2) S ist abgeschlossen unter der Addition und der Multiplikation.
(3) Mit $f \in S$ ist auch $-f \in S$.

Die natürlichen Zahlen $\mathbb{N}$ erfüllen in $\mathbb{Z}$ die ersten beiden Bedingungen, aber nicht die dritte. Die Menge aller geraden Zahlen erfüllen alle Bedingungen außer der, dass 1 dazugehört. Ebenso ist $\{0\}$ kein Unterring, da darin die 1 fehlt (obwohl im Nullring für sich betrachtet $0 = 1$ ist, das ist aber nicht die 1 von $\mathbb{Z}$). Die Menge $\{-1, 0, 1\}$ erfüllt die erste und die dritte Bedingung und ist abgeschlossen unter der Multiplikation, aber nicht unter der Addition. Die ganzen Zahlen $\mathbb{Z}$ haben überhaupt nur sich selbst als Unterring. Wir haben die Kette von Unterringen

$$\mathbb{Z} \subset \mathbb{Q} \subseteq \mathbb{R} \subset \mathbb{C}\,.$$

Endomorphismenringe

Definition 12. Es sei $(G, 0, +)$ eine kommutative Gruppe. Dann nennt man

$$\operatorname{End} G = \{\varphi : G \to G : \varphi \text{ ist ein Gruppenhomomorphismus}\}$$

den *Endomorphismenring* zu G. Er wird mit der *Addition*

$$(\varphi + \psi)(x) := \varphi(x) + \psi(x)$$

und der Hintereinanderschaltung als *Multiplikation*

$$\varphi\psi := \varphi \circ \psi$$

versehen.

Der Endomorphismenring zu einer Gruppe ist mit den angegebenen Verknüpfungen in der Tat ein Ring. Dabei folgt die kommutative Gruppenstruktur für die Addition aus einer direkten Rechnung. Die Hintereinanderschaltung von zwei Gruppenhomomorphismen ergibt nach Lemma 5.3 wieder einen Gruppenhomomorphismus. Die Assoziativität der Multiplikation und dass die Identität das neutrale Element ist, gilt allgemeiner für die Verknüpfung von Abbildungen. Für die Distributivität seien Gruppenhomomorphismen φ, ψ, θ gegeben. Dann gilt für jedes $x \in G$

$$((\psi + \theta) \circ \varphi)(x) = (\psi + \theta)(\varphi(x)) = \psi(\varphi(x)) + \theta(\varphi(x)) = (\psi \circ \varphi)(x) + (\theta \circ \varphi)(x).$$

Beispiel 13. (Matrizenring) Es sei R ein kommutativer Ring und $n \in \mathbb{N}$. Wie aus der linearen Algebra bekannt (zumindest für den Fall $R = \mathbb{R}$) beschreiben $n \times n$-Matrizen lineare Abbildungen von R^n nach R^n. Die Matrizenverknüpfung (gemäß der Regel „Zeile mal Spalte“) definiert dabei die Hintereinanderschaltung von linearen Abbildungen. Die Addition von Matrizen, die komponentenweise für jeden Eintrag erklärt ist, beschreibt die Summe von linearen Abbildungen. Mit diesen zwei Verknüpfungen und mit der Nullmatrix als Nullelement und der Einheitsmatrix als Einselement bildet die Menge der Matrizen einen (nicht-kommutativen) Ring, den sogenannten *Matrizenring* über R. Er wird mit $\operatorname{Mat}_n(R)$ bezeichnet.

Zu einem (sagen wir reellen) Vektorraum V der Dimension n hängen der Endomorphismenring zur additiven Gruppe $(V, +, 0)$ und der Matrizenring $\mathrm{Mat}_n(\mathbb{R})$ in folgender Weise zusammen. Nach Wahl einer Basis von V entsprechen die $\mathbb{R}$-linearen Endomorphismen $V \longrightarrow V$ den Matrizen, wobei sich die Additionen entsprechen und die Matrizenmultiplikation der Hintereinanderschaltung von linearen Abbildungen entspricht. Andererseits ist jede lineare Abbildung insbesondere ein Gruppenhomomorphismus von V nach V, so dass sich die Situation

$$\mathrm{Mat}_n(\mathbb{R}) \cong \mathrm{End}_{\mathbb{R}-\mathrm{lin}}(V) \subseteq \mathrm{End}(V)$$

ergibt, wobei hier ein Unterring vorliegt.