

Definitionen und Aussagen zu Ringen

Michael Hortmann, 11.4.2002

Während wir es bei Gruppen mit nur einer Operation zu tun haben, kennen wir z.B. von den ganzen Zahlen das Zusammenspiel zweier Operationen, Addition und Multiplikation, wobei charakteristisch ist, dass zwar jede ganze Zahl ein Inverses bzgl. der Addition, i.a. jedoch keines bezüglich der Multiplikation besitzt: Die ganzen Zahlen sind ein wichtiges Beispiel für einen **Ring**.

Ein **Ring** ist ein geordnetes Tripel $(R, +, \cdot)$.

Dabei ist R eine Menge, „+“, „ \cdot “ sind Verknüpfungen $R \times R \rightarrow R$, wobei man i.a. „+“ als *Addition*, „ \cdot “ als *Multiplikation* bezeichnet und auch ab statt $a \cdot b$ schreibt.

Bezüglich der Addition ist R eine abelsche Gruppe mit neutralem Element „0“, für die Multiplikation fordert man das Assoziativgesetz.

Addition und Multiplikation werden in Verbindung gebracht durch das **Distributivgesetz**:

$$\forall a, b, c \in R: a(b+c) = ab + ac, (b+c)a = ba + ca$$

Gilt auch für die Multiplikation das **Kommutativgesetz**, so nennt man den Ring *kommutativ*, gibt es ein **Einselement** „1“ bzgl. der Multiplikation, so nennt man ihn „Ring mit Eins“.

In jedem Ring gilt $0a=0$, denn $0a=(0+0)a=0a+0a$; in jedem Ring mit Eins gilt $(-1)a = -a$, denn $0=0a=(1+(-1))a=1a+(-1)a=a+(-1)a$, also ist $(-1)a$ das additiv Inverse von a .
Damit folgt auch $(-1)(-1) = -(-1) = 1$.

In einem kommutativen Ring gilt die **binomische Formel**:

$$(a+b)^n := \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$$

Dies beweist man durch Induktion mit Hilfe der bekannten Rekursionsformeln für die Binomialkoeffizienten $\binom{n}{i}$.

In einem kommutativen Ring R heißt ein Element $a \neq 0$ **Nullteiler**, wenn es ein Element $b \neq 0$ gibt mit $ab=0$.

Ein kommutativer Ring ohne Nullteiler heißt **Integritätsring**.

Die ganzen, rationalen und reellen Zahlen, also $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mit ihrer „eingebauten“ Addition und Multiplikation sind Integritätsringe.

$\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ mit der „modulo n “ definierten Addition und Multiplikation ist ein kommutativer Ring mit 1 und genau dann ein Integritätsring, wenn n eine Primzahl ist. ($3 \cdot 4 = 0$ in \mathbb{Z}_{12} !)

Wie bei den Gruppen geht es nun darum, aus „alten“ Ringen neue zu bauen, Homomorphismen und Quotientenstrukturen zu definieren.

Sind R, S Ringe, so ist der **Produkttring** $R \times S$ mit komponentenweise definierter Addition und Multiplikation ebenfalls ein Ring, analog der Produktkonstruktion bei Gruppen.

Dies lässt sich verallgemeinern: Ist I eine Menge und R ein Ring, so ist die Menge der Abbildungen $R^I := \{f \mid f : I \rightarrow R\}$ ebenfalls ein Ring, wobei die Verknüpfungen definiert werden durch $(f + g)(i) := f(i) + g(i)$, $(fg)(i) := f(i)g(i)$, und man überlegt sich leicht, wie hier das Nullelement und ggf. das Einselement auszusehen haben.

Ebenso definiert man zu einem gegebenen Ring R den **Matrizenring**

$$M_n(R) := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in R \right\}.$$

Die Elemente dieser Menge sind quadratische Schemata von Elementen von R , sogenannte **Matrizen**. a_{ij} ist das Element in der i -ten Zeile und j -ten Spalte der Matrix. Man benutzt

häufig für eine Matrix die Notation $(a_{i,j})_{1 \leq i, j \leq n}$ oder nur (a_{ij}) . Während die Addition von

Matrizen elementweise definiert wird, ist die Multiplikation komplizierter: Sind $A, B \in M_n(R)$ so definiert man die Elemente der **Produktmatrix** $C = AB$ durch

$$c_{ik} := \sum_{j=1}^n a_{ij} b_{jk},$$

d.h. man summiert die Produkte der Elemente der i -ten Zeile der Matrix A und der k -ten Spalte der Matrix B auf. Das Nullelement von $M_n(R)$ ist die **Nullmatrix**, deren Einträge sämtlich das Nullelement von R sind; ist R ein Ring mit Eins, so gibt es auch ein Einselement von $M_n(R)$, die sog. **Einheitsmatrix**, deren Einträge auf der „Hauptdiagonalen“ 1 und 0 sonst sind. Matrizenringe sind i.a. nicht kommutativ und nicht nullteilerfrei.

Neben Matrizenringen sind in der Mathematik **Polynomringe** von Bedeutung. Man geht

wieder aus von einem Ring R und definiert $R[X] := \left\{ \sum_{i=1}^n a_i X^i \mid n \in \mathbb{N}_0, a_i \in R \text{ für } 0 \leq i \leq n \right\}$.

Ein Element $f = \sum_{i=0}^n a_i X^i = a_0 + a_1 X + \dots + a_n X^n$ heißt **Polynom**, die Elemente a_i heißen

Koeffizienten des Polynoms, das „Symbol“ X heißt **Unbestimmte**. Beim Rechnen mit der

„Unbestimmten“ setzt man $X^0 := 1$ und $X^i X^j := X^{i+j}$. Ist $a_n \neq 0$, so heißt $n =: \text{grad}(f)$ der **Grad** des Polynoms. Der Grad des Nullpolynoms, dessen sämtliche Koeffizienten Null sind, ist undefiniert.

Ein Polynom ist durch seine Koeffizienten eindeutig bestimmt; man könnte statt

$$f = \sum_{i=0}^n a_i X^i = a_0 + a_1 X + \dots + a_n X^n \quad \text{auch einfach } f = (a_n, \dots, a_1, a_0) \text{ schreiben; die}$$

Schreibweise mit der „Unbestimmten“ ist aber häufig ganz sinnvoll. Während die Addition von Polynomen koeffizientenweise geschieht, wobei das Nullpolynom das neutrale Element der Addition ist, setzt man für die Multiplikation

$$\left(\sum_{i=0}^n a_i X^i \right) \left(\sum_{j=0}^m b_j X^j \right) := \sum_{i=0}^n \sum_{j=0}^m a_i b_j X^{i+j} = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^k .$$

Hat also das Polynom f die Koeffizienten a_i und das Polynom g die Koeffizienten b_j , so besitzt das Produktpolynom $h=fg$ die Koeffizienten $c_k = \sum_{i+j=k} a_i b_j$.

Ist $\text{grad}(f)=n$ und $\text{grad}(g)=m$, so ist im Produkt fg der „höchstmögliche“ Koeffizient ungleich Null $c_{m+n} = a_n b_m$. Ist also R ein Integritätsring, so ist $c_{m+n} = a_n b_m \neq 0$, also gilt die

$$\textbf{Gradformel} \quad \text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$$

Im übrigen ist ein Polynomring kommutativ, wenn der Grundring kommutativ ist; besitzt letzterer das Einselement 1, so ist das Polynom $f=1$ das Einselement des Polynomringes. Man kann grundsätzlich die Elemente des „Grundringes“ als Polynome vom Grad 0 auffassen (mit Ausnahme des Nullelements, welchem kein Grad zugeordnet ist), hat also eine natürliche Inklusion $R \subset R[X]$.

Im allgemeinen besitzt ein Ringelement in einem Ring mit Eins kein Inverses bzgl. der Multiplikation. Man nennt nun die Menge $R^* := \{a \in R \mid \exists a' \in R : aa' = 1\}$ der Elemente, die ein Inverses besitzen, die **Einheitengruppe** von R ; da jedenfalls $1 \in R^*$, ist diese Menge nicht leer, und sie bildet bzgl. der Multiplikation eine Gruppe. Es ist z.B. $\mathbb{Z}^* = \{1, -1\}$ und $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ und $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \text{ggT}(k, n) = 1\}$, insbesondere z.B. $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.

Unterringe und Ideale

Sei R ein Ring, $S \subset R$ eine Teilmenge.

S heißt **Unterring** von R , wenn S Untergruppe von R bezüglich der additiven Struktur ist und abgeschlossen bzgl. der Multiplikation, d.h. das Produkt zweier Elemente von S ist selbst Element von S .

Besitzt ein Unterring $I \subset R$ sogar die Eigenschaft dass $RI := \{rx \mid r \in R, x \in I\} \subset I$ und $IR := \{xr \mid r \in R, x \in I\} \subset I$ also $\forall r \in R \forall x \in I: rx \in I, xr \in I$, so heißt I ein **Ideal** von R .

Multipliziert man also ein Ideal-Element mit einem beliebigen Ringelement, so erhält man wieder ein Idealelement.

In diesem Sinne ist $n\mathbb{Z}$ ein Ideal von \mathbb{Z} und \mathbb{Z} ein Unterring, aber kein Ideal von \mathbb{Q} . $\{0\}$ (das Nullideal) und R (der gesamte Ring selbst) sind „trivialen Ideale“ jedes Ringes R .

Ideale erweisen sich als viel interessanter als bloße Unterringe. Wir werden weiter unten sehen, dass Ideale gerade diejenigen Unterobjekte von Ringen sind, die – analog den Normalteilern bei Gruppen – die Definition von Quotientenstrukturen erlauben.

In der Idealtheorie stellt man zunächst die Frage, wie man alle Ideale eines gegebenen Ringes bestimmen kann. Es stellt sich heraus, dass es z.B. in \mathbb{Q} und \mathbb{R} nur die trivialen Ideale gibt: dafür ist die Existenz der multiplikativen Inversen aller Elemente ungleich 0 verantwortlich. In \mathbb{Z} haben alle Ideale die Form $n\mathbb{Z}$; dahinter steckt die Existenz einer „Division mit Rest“ in \mathbb{Z} . Kompliziertere Ringe haben kompliziertere Idealstrukturen. Wir werden später im Zusammenhang mit „endlichen Körpern“ auf dieses Thema zurückkommen.

Ringhomomorphismen

Seien R und S Ringe, $\varphi: R \rightarrow S$ eine Abbildung. φ heißt **Ringhomomorphismus**, wenn φ ein Gruppenhomomorphismus bzgl. der additiven Strukturen von R und S ist und auch „verträglich“ mit der Multiplikation ist, also $\forall a, b \in R: \varphi(ab) = \varphi(a)\varphi(b)$.

Ist φ injektiv, so spricht man von einem (**Ring-**)**monomorphismus**, ist φ surjektiv, von einem **Epimorphismus**, und ist φ bijektiv, von einem **Isomorphismus**. Gibt es einen Isomorphismus zwischen zwei Ringen R und S , so nennt man diese **isomorph** und schreibt $R \cong S$.

Im $\varphi = \varphi(R)$ ist ein Unterring von H , $\ker \varphi := \{x \in R \mid \varphi(x) = 0_H\}$ heißt **Kern** von φ und ist ein Ideal von R . Allgemeiner ist sogar die Urbildmenge jedes Ideals in S unter einem Ringhomomorphismus ein Ideal in R . Ein Homomorphismus $\varphi: G \rightarrow H$ ist genau dann ein Monomorphismus, wenn $\ker \varphi = \{0_H\}$ ist.

Quotientenbildung in Ringen

Analog der Quotientendefinition bei Gruppen mit Hilfe von Nebenklassen möchte man bei Ringen vorgehen und auch auf dem Quotienten eine Ringstruktur definieren. Bei Gruppen hatten wir gesehen, dass die zur Quotientenbildung geeigneten Unterobjekte einer Gruppe

nicht irgendwelche Untergruppen sein durften, sondern dass man dazu „Normalteiler“ brauchte. In der Ringtheorie erweisen sich die Ideale als zur Bildung von Quotientenstrukturen geeignet.

Sei also R ein Ring und $I \subset R$ ein Ideal. Zu $x \in R$ bilden wir die (additive) Nebenklasse $x + I := \{x + a \mid a \in I\} =: \bar{x}$ und bilden die Menge aller Nebenklassen $R/I := \{x + I \mid x \in R\}$.

Aus der Gruppentheorie wissen wir, dass die Addition $\bar{x} + \bar{y} := \overline{x + y}$ „wohldefiniert“ (also unabhängig vom Repräsentanten) ist, und dass damit R/I bezüglich dieser Addition eine

abelsche Gruppe ist. Natürlich möchte man auch die Multiplikation durch $\bar{x} \cdot \bar{y} := \overline{x \cdot y}$ erklären; beim Nachweis der Wohldefiniertheit gehen wir wie bei den Gruppen vor, jedoch in „additiver Schreibweise“, und wir benötigen, dass I ein Ideal ist: Wenn nämlich $\bar{x} = \bar{x}'$ und $\bar{y} = \bar{y}'$ gilt, so folgt $x - x' =: a \in I$ und $y - y' =: b \in I$. Also hat man

$xy = (x' + a)(y' + b) = x'y' + ab + ay' + x'b$ und damit $xy - x'y' = ab + ay' + x'b \in I$, denn die Elemente die auf der rechten Seite der Gleichung addiert werden, gehören als Produkte, an denen Elemente von I beteiligt sind, selbst zu I . Damit ist aber $\overline{xy} = \overline{x'y'}$.