HANSER

Leseprobe

Rolf Socher

Algebra für Informatiker

Mit Anwendungen in der Kryptografie und Codierungstheorie

ISBN (Buch): 978-3-446-43257-4

ISBN (E-Book): 978-3-446-43312-0

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-43257-4

sowie im Buchhandel.

2 Ringe, Körper und Polynome

2.1 Ringe

Grundlegende Definitionen

Ein Ring ist eine algebraische Struktur mit zwei Operationen, von denen eine additiv, die andere multiplikativ geschrieben wird.

Der Prototyp eine Rings ist der Ring der ganzen Zahlen mit der Addition und Multiplikation. In dieser Struktur gelten die Assoziativgesetze für die Addition und Multiplikation, es gilt das Distributivgesetz, das Addition und Multiplikation verbindet, die 0 ist das neutrale Element der Addition und es gibt additive Inverse. Außer den Zahlen 1 und -1 hat jedoch keine ganze Zahl eine multiplikative Inverse.

Definition
Ring,
Integritätsbereich

Die Struktur $(R, +, \cdot)$ heißt *Ring*, falls folgende Bedingungen (die Ringaxiome) erfüllt sind:

(R1) $(R,+)$ ist eine abelsche Gruppe, deren neutrales Element mit 0 bezeichnet wird.

(R2) Die Multiplikation in R ist assoziativ und hat ein neutrales Element, das mit 1 bezeichnet wird.

(R3) Es gelten die Distributivgesetze, das heißt für alle $a, b, c \in R$ ist

$$a \cdot (b+c) = a \cdot b + a \cdot c \text{ und } (b+c) \cdot a = b \cdot a + c \cdot a.$$

Ein Ring mit kommutativer Multiplikation heißt *kommutativer Ring*.

Ein Ring R heißt *nullteilerfrei*, falls aus $a \cdot b = 0$ folgt, dass $a = 0$ oder $b = 0$ ist. Ein kommutativer nullteilerfreier Ring wird auch *Integritätsbereich* genannt.

Wie in Kapitel 1 lässt sich leicht zeigen, dass das neutrale Element der Multiplikation eindeutig bestimmt ist.

Die Terminologie ist in der Literatur nicht ganz einheitlich. Manchmal wird von einem Ring nicht die Existenz des Einselements verlangt.

Wie üblich lassen wir im Folgenden den Malpunkt der Multiplikation weg.

Beispiel 2.1

a) Die Struktur $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich.

b) Die rationalen, reellen sowie komplexen Zahlen mit Addition und Multiplikation sind ebenfalls Integritätsbereiche.

c) Für jedes $m \in \mathbb{N}$ ist die Struktur $(\mathbb{Z}_m, +, \cdot)$ ebenfalls ein kommutativer Ring. Dieser Ring ist genau dann ein Integritätsbereich, wenn m eine Primzahl ist. Beispielsweise gilt im Ring $\mathbb{Z}_4$ die Gleichung $2 \cdot 2 = 0$.

d) Ist K ein Körper und ist $n \in \mathbb{N}$, so ist die Menge $M_n(K)$ der $n \times n$-Matrizen mit Koeffizienten aus K mit der Matrizenaddition und -multiplikation ein Ring. Das neutrale Element der Addition ist die Nullmatrix, die additive Inverse der Matrix (a_{ij}) ist $(-a_{ij})$. Das neutrale Element der Multiplikation ist die $n \times n$-Einheitsmatrix E_n. Das folgende Beispiel mit $n = 2$ zeigt, dass $M_n(K)$ weder kommutativ noch nullteilerfrei ist.

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\ AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ BA = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \blacksquare$$

Aus den Ringaxiomen lassen sich folgende Rechenregeln ableiten:

Satz 2.1

Sei R ein Ring. Dann gilt für alle $a, b \in R$:

a) $a0 = 0a = 0$

b) $(-1)a = a(-1) = -a$

c) $(-a)b = a(-b) = -(ab)$.

Beweis:

a) Es gilt:

$$a1 = a(1+0) = a1 + a0.$$

Aus der Kürzungseigenschaft der additiven Gruppe $(R, +)$ folgt $a0 = 0$. Genauso lässt sich $0a = 0$ beweisen.

b) Es gilt:

$$(-1)a + a = (-1)a + 1a = (-1+1)a = 0a = 0.$$

Das heißt, $(-1)a$ ist die additive Inverse von a, also $(-1)a = -a$.

c) Der Beweis verläuft völlig analog zum Beweis von b). ❑

Die Ringaxiome schließen nicht aus, dass das Nullelement und das Einselement zusammenfallen. Dieser Fall tritt jedoch nur für den sogenannten Nullring ein:

Satz 2.2

Sei R ein Ring, in dem $1 = 0$ ist. Dann ist $R = \{0\}$.

Beweis: Sei $a \in R$. Dann ist nach Satz 2.1 $a = 1a = 0a = 0$. ❑

Aus dem Schulunterricht ist bekannt, dass die Nullteilerfreiheit eine angenehme Eigenschaft ist, die hilft, Gleichungen zu lösen. Beispielsweise kann die Gleichung $x^2 - x = 0$ in $\mathbb{Z}$ umgeformt werden zu $x \cdot (x-1) = 0$. Aus der Nullteilerfreiheit von $\mathbb{Z}$ folgt, dass einer der beiden Faktoren 0 sein muss, woraus sich die beiden Lösungen $x = 0$ und $x = 1$ ergeben. In einem Integritätsbereich gilt außerdem die Kürzungsregel der Multiplikation, genauer gesagt:

Satz 2.3

Der Ring R ist genau dann nullteilerfrei, wenn er die (Links-)Kürzungseigenschaft der Multiplikation besitzt, das heißt, wenn für alle $a, b, c \in R$ gilt: Aus $ab = ac$ und $a \neq 0$ folgt $b = c$.

Beweis: Sei R nullteilerfrei und sei $a \neq 0$. Aus $ab = ac$ folgt $ab - ac = 0$. Mit dem Distributivgesetz folgt weiter $a(b-c) = 0$ und da $a \neq 0$ ist, muss $b - c = 0$ sein, also $b = c$.

Gelte umgekehrt die Kürzungsregel und sei $ab = 0 = a0$. Ist $a \neq 0$, so folgt aus der Kürzungsregel $b = 0$. ❑

In dem nicht nullteilerfreien Ring $\mathbb{Z}_6$ etwa gilt $2 \cdot 2 = 2 \cdot 5$. Der Faktor 2 lässt sich jedoch nicht kürzen.

Satz 2.3 gilt *mutatis mutandis* für die Rechtskürzungsregel. Dies zeigt, dass Linkskürzungseigenschaft und Rechtskürzungseigenschaft in einem Ring äquivalente Bedingungen sind.

Ein *Unterring* S eines Rings R ist eine Teilmenge von R, die bezüglich der Ringoperationen von R einen Ring bildet. Um nachzuweisen, dass S ein Unterring von R ist, genügt es zu zeigen, dass die additive Gruppe von S eine Untergruppe der additiven Gruppe von R ist, dass S unter Multiplikation abgeschlossen ist und die 1 von R enthält. Ein nullteilerfreier Ring vererbt diese Eigenschaft offensichtlich auf jeden Unterring.

Die Elemente eines Rings müssen bezüglich der Multiplikation nicht invertierbar sein, aber *einzelne Elemente* können durchaus Inverse besitzen. So ist etwa das Einselement stets invertierbar. Invertierbare Elemente eines Rings werden auch *Einheiten* genannt. Im Ring $\mathbb{Z}$ der ganzen Zahlen sind 1 und –1 die einzigen Einheiten. Ist a invertierbar, so ist die Inverse a^{-1} eindeutig bestimmt (▶ Aufgabe 2.1).

Ein kommutativer Ring, der nicht der Nullring ist und in dem jedes Element außer 0 invertierbar ist, heißt *Körper*. Diese werden in Abschnitt 2.2 eingehender behandelt.

Ist K ein Körper, so sind die invertierbaren Elemente des Rings $M_n(K)$ bekanntlicherweise diejenigen quadratischen Matrizen, deren Determinante ungleich 0 ist. Den invertierbaren Matrizen kommt eine besondere Bedeutung zu, etwa bei der Lösung von linearen Gleichungssystemen oder im Kontext von geometrischen Transformationen.

Satz 2.4
Invertierbare Elemente eines Rings

Ist R ein Ring, so heißt $a \in R$ *invertierbar*, wenn es ein $a' \in R$ gibt mit

$$aa' = a'a = 1.$$

Die Menge aller invertierbaren Elemente von R wird mit $R^\times$ bezeichnet.

a) Ist $a \in R^\times$, so ist die Inverse von a eindeutig bestimmt. Sie wird mit a^{-1} bezeichnet.

b) $R^\times$ bildet eine Gruppe bezüglich der Ringmultiplikation, die auch *Einheitengruppe* von R heißt.

Beweis:

a) Übungsaufgabe (▶ Aufgabe 2.1).

b) Wir zeigen zunächst, dass $R^\times$ unter der Ringmultiplikation abgeschlossen ist. Seien $a, b \in R^\times$. Dann ist

$$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aa^{-1} = 1$$

und ebenso $(b^{-1}a^{-1})(ab) = 1$. Daraus folgt $ab \in R^\times$ und $(ab)^{-1} = b^{-1}a^{-1}$.
Das Assoziativgesetz gilt im Ring R. Wegen $1 \cdot 1 = 1$ ist $1 \in R^\times$. Ist a invertierbar, so ist auch a^{-1} invertierbar und es gilt $(a^{-1})^{-1} = a$. ❑

Beispiel 2.2 Der Ring der ganzen gaußschen Zahlen

Der Ring der ganzen gaußschen Zahlen, $\mathbb{Z}[i]$, besteht aus allen komplexen Zahlen der Form $a+bi$ mit $a, b \in \mathbb{Z}$. Man kann sich die ganzen gaußschen Zahlen als Punkte eines quadratischen Gitters in der komplexen Zahlenebene vorstellen. Die Ringeigenschaften von $\mathbb{Z}[i]$ lassen sich leicht nachprüfen. Als Unterring des Körpers $\mathbb{C}$ ist $\mathbb{Z}[i]$ auch nullteilerfrei.

Im Körper $\mathbb{C}$ gilt:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2}.$$

Die Zahl $a+bi \in \mathbb{Z}[i]$ ist also genau dann invertierbar, wenn $a^2+b^2 = 1$ ist und das ist genau dann der Fall, wenn $a = \pm 1$ und $b = 0$ oder $a = 0$ und $b = \pm 1$ gilt. Die Einheitengruppe von $\mathbb{Z}[i]$ ist also $\{1, -1, i, -i\}$. Sie ist zyklisch mit erzeugendem Element i (▶ Abschnitt 1.2). ■

Homomorphismen und Isomorphismen

Definition
Homomorphismus
Isomorphismus

a) Seien R und S Ringe. Eine Abbildung $\varphi : R \to S$ heißt (Ring-)*Homomorphismus*, wenn für alle $a, b \in R$ folgende Gleichungen gelten:

$$\varphi(a+b) = \varphi(a)+\varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$
$$\varphi(1) = 1.$$

b) Ein bijektiver Homomorphismus heißt *Isomorphismus*.

c) Gibt es einen Isomorphismus $\varphi : R \to S$, so heißen R und S *isomorph*. Wir schreiben $R \cong S$.

Beispiel 2.3 Die Abbildung $\varphi: \mathbb{Z} \to \mathbb{Z}_m$ mit $\varphi(a) = [a]_m$ ist ein Ringhomomorphismus. ■

Aus der Verträglichkeit mit der Addition folgt, dass ein Ringhomomorphismus $\varphi : R \to S$ insbesondere ein Gruppenhomomorphismus ist. Als solcher bildet er die 0 von R auf die 0 von S ab, das heißt $\varphi(0) = 0$. Dagegen muss die Eigenschaft $\varphi(1) = 1$ zusätzlich gefordert werden, da R und S keine Gruppen bezüglich der Multiplikation sind.

Wenn in diesem Kapitel von einem Homomorphismus die Rede ist, so ist stets ein Ringhomomorphismus gemeint, falls nicht explizit anders vermerkt.

Ähnlich wie bei Gruppen kann man auch das direkte Produkt von Ringen bilden.

Satz 2.5
Produktring

Seien R_1 und R_2 Ringe. Dann wird das kartesische Produkt $R_1 \times R_2$ zu einem Ring vermöge der Definitionen

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Dieser Ring heißt *Produktring* von R_1 und R_2.

Beweis: Dass mit dieser Konstruktion tatsächlich ein Ring entsteht, lässt sich einfach nachrechnen. Neutrales Element der Addition ist (0,0), neutrales Element der Multiplikation ist (1,1). ❑

Ideale und Faktorringe

In diesem Abschnitt betrachten wir ausschließlich kommutative Ringe.

Ähnlich wie bei Gruppen kann man auch in Ringen bestimmte Unterstrukturen auszeichnen. Was bei den Gruppen die Normalteiler sind, sind bei Ringen die Ideale.

Definition
Ideal

Sei R ein kommutativer Ring. Eine Teilmenge I von R heißt *Ideal*, falls folgende Bedingungen erfüllt sind:

(I1) Sind $x, y \in I$, so ist auch $x + y \in I$.

(I2) Ist $r \in R$ und $x \in I$, so ist $rx \in I$.

Beachten Sie dabei den wesentlichen Unterschied zwischen (I1) und (I2). In (I1) wird nur die Abgeschlossenheit von I unter der Addition verlangt. In (I2) dagegen wird die Abgeschlossenheit unter der Multiplikation mit beliebigen Elementen aus dem Ring R verlangt.

Beispiel 2.4

a) In jedem Ring R sind $\{0\}$ und R selbst Ideale, die sogenannten *trivialen* Ideale.

b) Im Ring der ganzen Zahlen ist die Menge $2\mathbb{Z}$ der geraden Zahlen ein Ideal, denn die Summe zweier gerader Zahlen ist wieder gerade und das Produkt einer geraden Zahl mit einer beliebigen ganzen Zahl ist ebenfalls gerade.

c) Dasselbe gilt für die Menge $3\mathbb{Z}$ der durch 3 teilbaren ganzen Zahlen usw. Allgemein ist für jedes $m \in \mathbb{N}$ die Menge $m\mathbb{Z}$ ein Ideal von $\mathbb{Z}$. ■

Aus dieser Definition folgt unmittelbar, dass $(I, +)$ eine Untergruppe von $(R, +)$ ist (▶ Aufgabe 2.12) und da die Addition in Ringen kommutativ ist, sogar ein Normalteiler. Ein Ideal ist jedoch im Allgemeinen kein Unterring, denn es wird nicht verlangt, dass es das Einselement enthält. Es ist sogar so, dass das triviale Ideal R das einzige Ideal von R ist, das das Einselement enthält, denn ist I ein Ideal, das die Eins enthält, so gilt für jedes $r \in R$: $r = r1 \in I$.

Dem Begriff des Ideals kommt in der Ringtheorie eine größere Bedeutung zu als dem Begriff des Unterrings. Das liegt daran, dass Ideale für Ringe die Rolle spielen, die Normalteiler für Gruppen spielen.

Satz 2.6

Ist $\varphi: R \to S$ ein Ringhomomorphismus, so ist $\operatorname{Kern}\varphi$ ein Ideal von R.

Beweis: Übungsaufgabe (▶ Aufgabe 2.14). ❑

Aus (I1) und (I2) folgt, dass jede Linearkombination $r_1x_1 + \ldots + r_nx_n$ mit $r_i \in R$ und $x_i \in I$ wieder in I liegt. Es gilt:

Satz 2.7

Eine nicht leere Teilmenge I eines Rings R ist genau dann ein Ideal, wenn jede Linearkombination $r_1x_1 + \ldots + r_nx_n$ mit $r_i \in R$ und $x_i \in I$ wieder in I liegt.

Beweis: Übungsaufgabe (▶ Aufgabe 2.5). ❑

Ist R ein Ring und ist $a \in R$, so ist die Menge $Ra = \{ra \mid r \in R\}$ ein Ideal. Ein Ideal dieser Form heißt (das von a erzeugte) *Hauptideal*. Das Hauptideal Ra wird auch oft (a) geschrieben, was jedoch nur dann sinnvoll ist, wenn der zugehörige Ring eindeutig ist.

In jedem Ring R gibt es die beiden trivialen Ideale $(0) = \{0\}$ und $(1) = R$. Es gilt:

Satz 2.8

Der Ring R mit $0 \neq 1$ ist genau dann ein Körper, wenn (0) und (1) die einzigen Ideale von R sind.

Beweis: Sei R ein Körper und $I \neq (0)$ ein Ideal von R. Sei ferner $a \in I$, $a \neq 0$. Da R ein Körper ist, ist $a^{-1} \in R$. Damit ist auch $a^{-1}a = 1 \in I$. Daraus folgt $I = (1)$.

Seien umgekehrt (0) und (1) die einzigen Ideale von R und sei $a \in R$, $a \neq 0$. Dann ist $(a) \neq (0)$, also muss $(a) = (1)$ sein. Daraus folgt $1 \in (a)$, also gibt es ein $r \in R$ mit $1 = ra$. Das bedeutet, dass a invertierbar ist. Wir haben gezeigt, dass jedes Element $a \in R$, $a \neq 0$ invertierbar ist, also ist R ein Körper. ❑

Aufgabe Zeigen Sie, dass jedes Ideal in $\mathbb{Z}$ ein Hauptideal ist.

Lösung Die beiden trivialen Ideale sind von der Form (0) bzw. (1). Sei I ein nicht triviales Ideal in $\mathbb{Z}$ und sei $a \in I$, $a \neq 0$.

Wenn Sie sich einige Ideale von $\mathbb{Z}$ anschauen, etwa (2), (3), (4), dann werden Sie feststellen, dass das erzeugende Element jeweils das kleinste positive Element des Ideals ist. Beispielsweise enthält (4) keine positive Zahl kleiner als 4. Zunächst ist klar, dass I mindestens eine positive Zahl enthält, denn mit a ist auch $(-1)a = -a \in I$ und eine der beiden Zahlen a und $-a$ ist positiv. Sei k die kleinste positive Zahl in I. Dann enthält I alle Vielfachen von k. Es bleibt nur noch zu zeigen, dass I keine weiteren Zahlen enthält. Ist $m \in I$, so gibt es Zahlen q und r mit $m = qk + r$ und $0 \leq r < k$. Dann ist $r = m - qk \in I$. Da jedoch k die kleinste positive Zahl in I ist, muss $r = 0$ sein, das heißt, m ist ein Vielfaches von k. Damit ist gezeigt, dass I von k erzeugt wird. ■

Definition
Hauptidealring

Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*.

Ist R ein Ring und sind $a_1, \ldots, a_n \in R$, so ist die Menge aller Linearkombinationen von $a_1, \ldots, a_n$ ein Ideal. Wir schreiben:

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \ldots + r_n a_n \mid r_i \in R\}.$$

Wir können nun genauso wie bei Gruppen auf der Menge der Nebenklassen eines Ideals eine Addition und darüber hinaus eine Multiplikation definieren.

Satz 2.9
Faktorring

Sei R ein kommutativer Ring und I ein Ideal von R. Mit R/I bezeichnen wir die Menge der Nebenklassen von I bezüglich der additiven Gruppe von R. Wir schreiben die Nebenklassen in der Form $r + I$ mit $r \in R$.

Auf der Menge R/I definieren wir eine Addition und eine Multiplikation vermöge

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)(b+I) = ab+I.$$

Dann ist R/I mit diesen beiden Operationen ein Ring, der als *Faktorring* von R nach I bezeichnet wird.

Beweis: Die Addition auf R/I ist wohldefiniert, das heißt, unabhängig von der Wahl der Repräsentanten der Nebenklassen, denn I ist ein Normalteiler in der additiven Gruppe von R. Aus Satz 1.12 folgt, dass R/I eine abelsche Gruppe ist.

Wir zeigen, dass die Multiplikation wohldefiniert ist: Seien a' und b' in derselben Nebenklasse wie a bzw. b. Dann ist $a - a' \in I$ und $b - b' \in I$ und

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b')$$

ist eine Linearkombination von Elementen aus I und als solche selbst in I. Daher sind auch ab und $a'b'$ in derselben Nebenklasse.

Die Rechengesetze (beide Assoziativgesetze, Distributivgesetz) vererben sich direkt vom Ring R. Das neutrale Element der Addition ist $0 + I$, das additiv inverse Element von $a + I$ ist $-a + I$, das neutrale Element der Multiplikation ist $1 + I$. ❑

Offensichtlich ist die Konstruktion des Rings $\mathbb{Z}_m$ ein Spezialfall der obigen Konstruktion: Es ist $\mathbb{Z}_m = \mathbb{Z}/(m)$.

In Analogie zu Satz 1.13 gilt der erste Isomorphiesatz auch für Ringe.

Satz 2.10
Erster Isomorphiesatz für Ringe

Sei $\varphi: R \to S$ ein Homomorphismus. Dann ist $R/\text{Kern}\,\varphi \cong \text{Bild}\,\varphi$.
Ist insbesondere φ surjektiv, so ist $R/\text{Kern}\,\varphi \cong S$.

Beweis: Wie im Beweis von Satz 1.13 definieren wir eine Abbildung

$$\theta : R/\text{Kern}\,\varphi \to \text{Bild}\,\varphi$$

durch

$$\theta(a + \text{Kern}\,\varphi) = \varphi(a).$$

Die Abbildung ist wohldefiniert und ein Isomorphismus der additiven Gruppe von $R/\text{Kern}\,\varphi$ auf die additive Gruppe von Bild φ. Es bleibt nur noch zu zeigen, dass θ mit der Multiplikation verträglich ist. Es ist

$$\begin{aligned}\theta((a + \text{Kern}\,\varphi)(b + \text{Kern}\,\varphi)) &= \theta(ab + \text{Kern}\,\varphi) = \varphi(ab) \\ &= \varphi(a)\varphi(b) = \theta(a + \text{Kern}\,\varphi)\theta(b + \text{Kern}\,\varphi).\end{aligned}$$ ❑

Aufgaben zu 2.1

2.1 Zeigen Sie: Ist $a \in R^\times$, so ist die Inverse von a eindeutig bestimmt.

2.2 Sei M eine Menge. Wir definieren zwei Verknüpfungen + und · auf der Potenzmenge $\mathcal{P}(M)$ wie folgt (▶ Aufgabe 1.4):

$$A + B = (A \cup B) - (A \cap B) = (A \cup B) \cap (A^C \cup B^C)$$

$$A \cdot B = A \cap B.$$

Zeigen Sie, dass $(\mathcal{P}(M), +, \cdot)$ ein kommutativer Ring ist.

2.3 Sei M eine endliche Menge mit $n = |M|$. Zeigen Sie, dass dann der Ring aus Aufgabe 2.2 isomorph zum n-fachen Produktring $\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ ist.

2.4 Die Elemente a, b eines Rings R heißen *Nullteiler*, wenn $a \neq 0$ und $b \neq 0$ und $ab = 0$ ist. Zeigen Sie, dass Nullteiler nicht invertierbar sind.

2.5 Beweisen Sie Satz 2.7.