Kapitel 2

Ringe und Ideale

Gruppen, Ringe und Körper sind grundlegende Objekte der Algebra. Sie haben sie bereits in der Linearen Algebra kennengelernt, denn ohne deren Definition und grundlegende Eigenschaften sind selbst die Überlegungen der Theorie der Vektorräume nicht solide aufbaubar. Daher werden wir hier zuerst die Begriffe kurz und ohne Beweise wiederholen, ehe wir uns weiterführenden Begriffen, Eigenschaften und Sätzen zuwenden, die dann den Einstieg in die eigentliche Thematik der Algebra bilden.

2.1 Wiederholung: Gruppen, Ringe, Körper

In diesem Abschnitt wird es wegen des Wiederholungscharakters weder Beweise noch umfangreiche Überleitungstexte geben.

Definition 2.1.1 *Sei G eine nicht-leere Menge und*

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \end{aligned}$$

eine zweistellige Operation auf G.

a) $(G, *)$ *heißt* **Halbgruppe**, *wenn das Assoziativgesetz in G bzgl. $*$ erfüllt ist:*
$(AG) \qquad \forall a, b, c \in G : \quad (a * b) * c = a * (b * c).$

b) $(G, *)$ *heißt* **Monoid**, *wenn $(G, *)$ eine Halbgruppe ist, in der ein neutrales Element existiert:*
$(NE) \qquad \exists e \in G : a * e = a = e * a \ \ \forall a \in G.$

c) $(G, *)$ *heißt* **Gruppe**, *wenn* $(G, *)$ *ein Monoid ist, in dem jedes Element ein inverses Element besitzt:*
$(IE) \qquad \forall a \in G \exists b \in G : a * b = e = b * a.$

d) Eine solche Struktur $(G, *)$ *heißt* **abelsch** *(oder* **kommutativ***), falls das Kommutativgesetz in* G *bzgl.* $*$ *erfüllt ist:*
$(KG) \qquad \forall a, b \in G : a * b = b * a.$

Lemma 2.1.2 *Sei* $(G, *)$ *eine Halbgruppe. Sind zusätzlich sowohl*
$(lNE) \qquad \exists e \in G : e * a = a \forall a \in G \quad$ *als auch*
$(lIE) \qquad \forall a \in G \exists b \in G : b * a = e$
erfüllt, so ist $(G, *)$ *bereits eine Gruppe.*

Lemma 2.1.3 *Sei* $(G, *)$ *eine Halbgruppe. Sind zusätzlich sowohl*
$(rNE) \qquad \exists e \in G : a * e = a \forall a \in G \quad$ *als auch*
$(rIE) \qquad \forall a \in G \exists b \in G : a * b = e$
erfüllt, so ist $(G, *)$ *bereits eine Gruppe.*

Satz 2.1.4 *In einem Monoid ist das neutrale Element eindeutig bestimmt. In einer Gruppe ist das inverse Element zu einem gegebenen Element eindeutig bestimmt.*

Notation 2.1.5 *Sehr häufig werden Gruppen in multiplikativer Notation, also als* $(G, \cdot)$*, mit den üblichen Schreibweisen für die Multiplikation notiert. Vor allem bei abelschen Gruppe ist auch die additive Notation, also* $(G, +)$*, mit den üblichen Schreibweisen der Addition gebräuchlich.*

Definition 2.1.6 *Sei* $(G, *)$ *eine Gruppe. Eine nicht-leere Teilmenge* $U \subseteq G$ *heißt* **Untergruppe** *von* G*, falls* $(U, *)$ *eine Gruppe ist.*

Proposition 2.1.7 *Sei* $(G, *)$ *eine Gruppe. Eine Teilmenge* $U \subseteq G$ *ist genau dann Untergruppe, wenn*

(U1) $U \neq \emptyset$

(U2) $\forall a, b \in U : a * b^{-1} \in U$

Definition 2.1.8 *Sei R eine nicht-leere Menge und seien*

$$\begin{aligned} + : R \times R &\longrightarrow R \\ (a,b) &\longmapsto a+b \\ \cdot : R \times R &\longrightarrow R \\ (a,b) &\longmapsto a \cdot b \end{aligned}$$

zwei zweistellige Operationen auf R.
$(R,+,\cdot)$ heißt **Ring**, *falls*

a) $(R,+)$ *abelsche Gruppe*

b) $(R,\cdot)$ *Halbgruppe*

c) die beiden Distributivgesetze gelten:
$\forall a,b,c \in R : (a+b)\cdot c = a\cdot c + b\cdot c$
$\forall a,b,c \in R : a\cdot(b+c) = a\cdot b + a\cdot c.$

Ein Ring $(R,+,\cdot)$ heißt **Ring mit 1**, *falls $(R,\cdot)$ Monoid ist.*
Ein Ring $(R,+,\cdot)$ heißt **kommutativ**, *falls $(R,\cdot)$ abelsch ist.*

Proposition 2.1.9 *Sei $(R,+,\cdot)$ ein Ring mit 1. Dann gilt:*

a) 0_R *und* 1_R *sind eindeutig bestimmt.*

b) $0_R \cdot a = 0_R = a \cdot 0_R \ \ \forall a \in R$

c) $(-a)\cdot b = -(a\cdot b) = a\cdot(-b) \ \ \forall a,b \in R$

d) $(-a)\cdot(-b) = a\cdot b \ \ \forall a,b \in R$

e) $(n\cdot a)\cdot b = n\cdot(a\cdot b) = a\cdot(n\cdot b) \ \ \forall a,b \in R \forall n \in \mathbb{N}$

Definition 2.1.10 *Sei $(R,+,\cdot)$ ein Ring mit 1. Ein Element $a \in R \setminus \{0\}$ heißt* **Nullteiler** *in R, falls*

$$\exists b \in R \setminus \{0\} : a\cdot b = 0 \ \textit{(Linksnullteiler)}$$

oder

$$\exists c \in R \setminus \{0\} : c\cdot a = 0 \ \textit{(Rechtsnullteiler).}$$

R heißt **nullteilerfrei**, *falls*

$$\forall a,b \in R : (a\cdot b = 0 \Longrightarrow (a=0) oder (b=0)).$$

Definition 2.1.11 *Ein nullteilerfreier, kommutativer Ring mit* $1 \neq 0$ *heißt* **Integritätsring** *(oder* **Integritätsbereich***).*

Die seltsame Bedingung $1 \neq 0$ stellt einfach sicher, dass wir es mit einem Monoid $(R \setminus \{0\}, \cdot)$ zu tun haben. Das beinhaltet eben auch, dass $R \setminus \{0\}$ nicht leer ist.

Definition 2.1.12 *Sei* $(R, +, \cdot)$ *ein Ring mit* 1*. Ein Element* $a \in R$ *heißt* **Einheit** *in* R*, falls*

$$\exists b \in R : a \cdot b = 1 = b \cdot a.$$

Die Menge der Einheiten in R *wird bezeichnet mit* R^**.*

Definition 2.1.13 *Ein Ring* $(R, +, \cdot)$ *mit* $1 \neq 0$ *heißt* **Schiefkörper***, falls* $R^* = R \setminus \{0\}$*.*
Ist R *zusätzlich kommutativer Ring, so heißt* R **Körper***.*

Bemerkung 2.1.14 $(R^*, \cdot)$ *ist eine Gruppe und wird als die* **Einheitengruppe** *von* R *bezeichnet.*

Korollar 2.1.15 *Sei* $K \neq \emptyset$ *und seien*

$$\begin{aligned} + : K \times K &\longrightarrow K \\ (a, b) &\longmapsto a + b \\ \cdot : K \times K &\longrightarrow K \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

zwei zweistellige Operationen auf K*.*
$(K, +, \cdot)$ *ist ein Körper genau dann, wenn*

a) $(K, +)$ *abelsche Gruppe*

b) $(K \setminus \{0\}, \cdot)$ *abelsche Gruppe*

c) das Distributivgesetz gilt:
$\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c.$

2.2 Ergänzung: Integritätsring, Schiefkörper, Körper

Da die folgenden Aussagen nicht in der Linearen Algebra behandelt wurden und wir sie daher nicht ohne Beweis einfach zitieren können, grenze ich sie bewusst gegenüber den vorigen Aussagen ab. Thematisch könnten sie leicht in dasselbe Kapitel gepackt werden, aber mit dieser Aufteilung ist es für die Leserinnen und Leser des Skripts hoffentlich leichter, die neuen Inhalte von der Wiederholung abzugrenzen.

Satz 2.2.1 *Jeder Schiefkörper ist nullteilerfrei.*

Beweis: Sei $(R, +, \cdot)$ ein Schiefkörper und seien $a, b \in R$, $a \neq 0$, so daß $a \cdot b = 0$. Ein Nullteiler muss nach Definition selbst von Null verschieden sein ebenso wie der Faktor, mit dem er Null ergibt, so dass wir $a = 0$ nicht betrachten müssen und die Aussage bewiesen haben, sobald wir sehen, dass $b = 0$ gelten muss.
Wegen $a \neq 0$ existiert ein multiplikatives Inverses a^{-1} zu a, so dass gilt:

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot b = b,$$

weswegen a kein Nullteiler ist.

□

Korollar 2.2.2 *Jeder Körper ist ein Integritätsring.*

Beweis: Integritätsringe sind kommutative nullteilerfreie Ringe

□

Satz 2.2.3 *Jeder endliche Integritätsring R mit $1 \neq 0$ ist ein Körper.*

Beweis: Sei $(R, +, \cdot)$ ein endlicher Integritätsring. Wir werden zeigen, dass jedes Element $a \in R \setminus \{0\}$ ein multiplikatives Inverses hat. Anstatt diese Inverse jedoch explizit zu konstruieren, werden wir zeigen, dass es ein Inverses zu a geben muss, ohne dieses explizit anzugeben.

Schritt 1: Zeige $\phi : R \longrightarrow R, x \longmapsto a \cdot x$ injektiv
Seien $y_1, y_2 \in R$ mit $\phi(y_1) = \phi(y_2)$, dann gilt:

$$0 = a \cdot y_1 - a \cdot y_2 \overset{(DG)}{=} a \cdot (y_1 - y_2).$$

Da $a \neq 0$ und R nullteilerfrei ist, gilt damit $y_1 = y_2$.
Schritt 2: Zeige $\exists b \in R : a \cdot b = 1$
Da R endlich ist, ist ϕ wegen Injektivität auch surjektiv. Damit existiert $b \in R$, das auf die 1 abgebildet wird. Dies ist unser gesuchtes Inverses.

□

Generalvoraussetzung ab diesem Punkt:
Alle betrachteten Ringe besitzen eine $1 \neq 0$, sofern nicht ausdrücklich etwas anderes vorausgesetzt wird.