Kap. II Ringe und Körper

Zur Untersuchung von Gruppen haben wir einige Methoden herangezogen, die für die Algebra typisch sind:

- Bildung von Untergruppen (Unterstrukturen)
- Bildung von Faktorgruppen (Faktorstrukturen)
- Bildung von Produktgruppen (Produktstrukturen)
- Betrachtung von Gruppenhomomorphismen (strukturverträgliche Abbildungen)

Entsprechend werden wir jetzt auch bei der Behandlung von Ringen und Körpern vorgehen.

§13. Ringe

Da die Grundbegriffe aus der Linearen Algebra bekannt sein sollten, wird der Schwerpunkt auf die beiden Punkte "Faktorringe" und "Ringhomomorphismen" gelegt.

(13.1) DEF: R sei eine Menge mit zwei Verknüpfungen $+$ (genannt Addition) und $\cdot$ (genannt Multiplikation).
Das Tripel $(R, +, \cdot)$ heißt ein **Ring**, wenn gilt:

R$_1$) $(R, +)$ ist eine abelsche Gruppe.

R$_2$) Die Multiplikation ist assoziativ und besitzt ein neutrales Element.

R$_3$) Es gelten die distributiven Gesetze

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{und} \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a) \quad (\forall\, a, b, c \in R)\,.$$

Ist zusätzlich die Multiplikation kommutativ, so heißt $(R, +, \cdot)$ ein **kommutativer Ring**.

(13.2) BEM: **a)** Wir benutzen folgende Bezeichnungen:

0_R	neutrales Element bzgl. $+$ (Nullelement)
$-a$	das eindeutig bestimmte Inverse (Negative) von $a \in R$ bzgl. $+$
$a - b$	für bn $a + (-b)$ (Differenz von a und b)
ab	für das Produkt $a \cdot b$
1_R	neutrales Element bzgl. $\cdot$ (Einselement)

b) Vereinbart man noch "Punktrechnung geht vor Strichrechnung", so lassen sich die distributiven Gesetze in der gewohnten Form aufschreiben:

$a(b + c) = ab + ac$ und $(b + c)a = ba + ca$.

Beispiele: **a)** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind kommutative Ringe.

b) Der Matrizenring $\mathrm{M}_n(\mathbb{R})$ ist für $n \geq 2$ nicht kommutativ.

(13.3) SATZ: $(R, +, \cdot)$ sei ein Ring. Dann gelten die folgenden Rechenregeln für beliebige $a, b \in R$:

a) $-(-a) = a$ **b)** $-(a+b) = -a-b$ **c)** $a \cdot 0_R = 0_R = 0_R \cdot a$

d) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$ **e)** $(-a) \cdot (-b) = a \cdot b$.

BEM: $R = \{0_R\}$ (Nullring) $\iff$ $1_R = 0_R$

In einem Ring R ist jedes Element bzgl. der Addition invertierbar, dies muß jedoch bzgl. der Multiplikation nicht gelten.

(13.4) DEF: R sei ein Ring. Ein Element $a \in R$ heißt **Einheit in** R, falls a invertierbar bzgl. $\cdot$ ist (d.h.wenn es ein $b \in R$ gibt mit $ab = 1_R = ba$). Das Inverse einer Einheit $a \in R$ wird mit a^{-1} bezeichnet. Die Menge aller Einheiten von R werde mit $R^\star$ bezeichnet.

(13.5) BEISPIELE: **a)** $\mathbb{Z}^\star = \{1, -1\}$, $\mathbb{Q}^\star = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\star = \mathbb{R} \setminus \{0\}$

b) $\mathrm{M}_n(\mathbb{R})^\star = \mathrm{GL}_n(\mathbb{R})$

c) $(R^\star, \cdot)$ ist eine Gruppe, die sog. Einheitengruppe des Ringes R.

d) Im Falle $1_R \neq 0_R$ ist 0_R **keine** Einheit in R.

(13.6) DEF: $(R, +, \cdot)$ sei ein Ring. Eine Teilmenge $U \subseteq R$ heißt ein **Unterring** von R, wenn gilt:

UR$_1$) $\forall\, a, b \in U \,:\, a - b \in U$ **UR**$_2$) $\forall\, a, b \in U \,:\, a \cdot b \in U$ **UR**$_3$) $1_R \in U$.

(13.7) BEM: **a)** Ein Unterring $U \subseteq R$ ist für sich betrachtet wieder ein Ring. Seine Verknüpfungen sind die Einschränkungen der Verknüpfungen des Ringes R auf U.

b) Ein Unterring von R ist insbesondere eine Untergruppe von $(R, +)$.

c) $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$ und auch von $\mathbb{R}$.

c) $U := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ ist ein Unterring von $\mathbb{R}$.

d) Für $k \in \mathbb{Z} \setminus \{-1, 1\}$ ist $\mathbb{Z}k$ kein Unterring von $\mathbb{Z}$.

(13.8) DEF: R und S seien Ringe. Eine Abbildung $\alpha : R \longrightarrow S$ heißt ein **Ringhomomorphismus**, wenn gilt:

RH$_1$) $\alpha(a+b) = \alpha(a) + \alpha(b)$ $(\forall\, a, b \in R)$

RH$_2$) $\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b)$ $(\forall\, a, b \in R)$

RH$_3$) $\alpha(1_R) = 1_S$

Ein bijektiver Ringhomomorphismus heißt ein **Ringisomorphismus**.

R heißt **isomorph zu** S (in Zeichen: $R \cong S$), wenn es einen Ringisomorphismus $\alpha : R \longrightarrow S$ gibt.

BEM: **a)** Jeder Ringhomomorphismus $\alpha : R \longrightarrow S$ ist auch ein Gruppenhomomorphismus $\alpha : (R,+) \longrightarrow (S,+)$. Daher gilt immer $\alpha(0_R) = 0_S$ und $\alpha(-a) = -\alpha(a) \quad (a \in R)$.

b) Die Abbildung $\mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \overline{z}$ ist ein bijektiver Ringhomomorphismus, also ein Ringisomorphismus.

(13.9) LEMMA: $\alpha : R \longrightarrow S$ sei ein Ringhomomorphismus. Dann gilt:

a) $\mathrm{Bild}(\alpha)$ ist ein Unterring von S .

b) $\mathrm{Kern}(\alpha)$ Unterring von $R \iff S = O$.

c) $\mathrm{Kern}(\alpha)$ ist eine Untergruppe von $(R,+)$, und es gilt

$$\forall\, x \in R\, \forall\, a \in \mathrm{Kern}(\alpha) \;:\; x \cdot a \in \mathrm{Kern}(\alpha) \quad \text{und} \quad a \cdot x \in \mathrm{Kern}(\alpha)$$

(13.10) DEF: R sei ein Ring. Eine Teilmenge $I \subseteq R$ heißt ein (zweiseitiges) **Ideal von** R , wenn gilt:

$\mathbf{I}_1$) I ist eine Untergruppe von $(R,+)$

$\mathbf{I}_2$) $\forall\, x \in R\, \forall\, a \in I \,:\, x \cdot a \in I$ und $a \cdot x \in I$.

(13.11) BEISPIELE: **a)** Nach (13.9c) sind Kerne von Ringhomomorphismen Ideale.

b) Für jedes $n \in \mathbb{N}_0$ ist $\mathbb{Z}n$ ein Ideal in $\mathbb{Z}$, und dies sind die einzigen Ideale in $\mathbb{Z}$.

c) In einem kommutativen Ring R ist $(a) := Ra = \{xa | x \in R\}$ für jedes $a \in R$ ein Ideal. Es heißt das von a erzeugte **Hauptideal** .

Faktorgruppen wurden nach Normalteilern (d.h. Kernen von Gruppenhomomorphismen) gebildet. Bei Ringen werden Faktorringe nach Idealen gebildet.

Sei $I \subseteq R$ ein Ideal in dem Ring R . Dann ist I Normalteiler in der abelschen Gruppe $(R,+)$, so daß man die Faktorgruppe

$$R/I \;=\; \{\, [a]_I \,|\, a \in R \,\}$$

bilden kann, die aus allen Nebenklassen $[a]_I = a+I$ (Komplexsumme!) besteht. Die Addition auf R/I ist "repräsentantenweise" definiert, d.h.

$$[a]_I + [b]_I \;:=\; [a+b]_I \quad (a,b \in R)$$

Wir wissen, daß $(R/I,+)$ eine abelsche Gruppe ist mit dem neutralen Element $[0_R]_I$. Eine **Multiplikation** auf R/I definieren wir ganz entsprechend:

$$[a]_I \cdot [b]_I \;:=\; [a \cdot b]_I \quad (a,b \in R)$$

Diese Multiplikation ist wohldefiniert, d.h. unabhängig von der Auswahl der Vertreter der Nebenklassen, assoziativ und besitzt $[1_R]_I$ als neutrales Element. Außerdem gelten die Distributivgesetze, was sich alles leicht nachprüfen läßt . Zusammenfassend erhalten wir:

(13.12) SATZ: R sei ein Ring und I ein Ideal von R. Dann gilt:

a) Die Menge R/I der Nebenklassen nach I wird bzgl. der Verknüpfungen

$$[a]_I + [b]_I \;=\; [a+b]_I \quad , \quad [a]_I \cdot [b]_I \;=\; [a \cdot b]_I \quad (a, b \in R)$$

zu einem Ring, dem sog. **Faktorring von** R **nach** I.

b) Die natürliche Abbildung $\nu_I : R \longrightarrow R/I$, $a \longmapsto [a]_I$, ist ein surjektiver Ringhomomorphismus mit $\mathrm{Kern}(\nu_I) = I$.

c) R kommutativ $\Longrightarrow$ R/I kommutativ.

BEM: Die Ideale eines Ringes R sind genau die Kerne von Ringhomomorphismen $R \longrightarrow S$.

(13.13) BEISPIEL: Als Beispiel betrachten wir den Faktorring des Ringes $\mathbb{Z}$ nach dem Ideal $\mathbb{Z}\,n$ für $n \in \mathbb{N}_0$. Hier werden die Restklassen modulo n repräsentantenweise addiert und multipliziert:

$$[a]_n + [b]_n = [a+b]_n \quad , \quad [a]_n \cdot [b]_n = [a \cdot b]_n$$

$\mathbb{Z}_n = \mathbb{Z}/\mathbb{Z}\,n$ ist ein kommutativer Ring, der n Elemente besitzt. Nach Aufg. 61 gilt für $a \in \mathbb{Z}$

$$[a]_n \in \mathbb{Z}_n^\star \iff \mathrm{ggT}(a, n) = 1\,.$$

Folglich $\;|\,\mathbb{Z}_n^\star\,| = \varphi(n)$ (s. (5.8)).

(13.14) SATZ: **Homomorphiesatz für Ringe**

$\alpha : R \longrightarrow S$ sei ein Ringhomomorphismus und $I \subseteq R$ ein Ideal mit $I \subseteq \mathrm{Kern}(\alpha)$. Dann gilt:

a) Es gibt genau einen Ringhomomorphismus $\alpha^\star : R/I \longrightarrow S$ mit der Eigenschaft $\alpha^\star \circ \nu_I \;=\; \alpha$.

$\alpha^\star$ heißt der durch α induzierte Ringhomomorphismus.

Er ist definiert durch die Vorschrift $\alpha^\star([a]_I) := \alpha(a)$ für alle $a \in R$.

$$\begin{tikzcd}
R \arrow[r, "\alpha"] \arrow[d, "\nu_I"'] & S \\
R/I \arrow[ur, "\alpha^\star"'] &
\end{tikzcd}$$

$$\boxed{\alpha^\star \circ \nu_I = \alpha}$$

b) $\alpha^\star$ surjektiv $\iff$ α surjektiv

c) $\alpha^\star$ injektiv $\iff$ $I = \mathrm{Kern}(\alpha)$.

(13.15) SATZ: R und S seien Ringe. Dann ist das kartesische Produkt $R \times S$ bzgl. der komponentenweise erklärten Addition und Multiplikation ein Ring, der sog. **Produktring** von R und S.

Es ist $(a,b)+(a',b') := (a+a', b+b')$ und $(a,b)\cdot(a',b') := (a\cdot a', b\cdot b')$

(13.16) DEF: **a)** Ein Ring R heißt **nullteilerfrei** wenn gilt:

$$\forall\, a,b \in R \,:\, a\cdot b = 0_R \implies a = 0_R \,\vee\, b = 0_R\,.$$

b) Ein kommutativer nullteilerfreier Ring R mit $1_R \neq 0_R$ heißt ein **Integritätsbereich (IB)**.

(13.17) BEISPIELE: **a)** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Integritätsbereiche.

b) Die Ringe $\mathbb{R}\times\mathbb{R}$ und $\mathbb{Z}_4$ sind keine Integritätsbereiche.

c) Der Matrixring $\mathrm{M}_n(\mathbb{R})$ ist für $n \geq 2$ nicht nullteilerfrei.

(13.18) DEF: Ein R heißt ein **Hauptidealbereich (HIB)**, wenn gilt:

1) R ist ein Integritätsbereich

2) Jedes Ideal von R ist ein Hauptideal.

(13.19) BEISPIEL: $\mathbb{Z}$ ist ein HIB.

Dies gilt nach (13.11b).