2.3 Ringhomomorphismen

In der Linearen Algebra beschäftigten wir uns nicht nur mit den dortigen Objekten – den Vektorräumen – sondern auch mit den mit der Vektorraumstruktur verträglichen Abbildungen zwischen diesen – den Vektorraum-Homomorphismen, die auch als Lineare Abbildungen bezeichnet werden. In der Algebra I wird unser Hauptaugenmerk auf Ringen liegen und auf Abbildungen, die diese Struktur respektieren, den Ringhomomorphismen.

Definition 2.3.1 *Seine* $(R, +_R, \cdot_R), (S, +_S, \cdot_S)$ *Ringe. Eine Abbildung* $\phi : R \longrightarrow S$ *heißt* **Ringhomomorphismus**, *falls gilt:*

a) $\forall a, b \in R : \phi(a +_R b) = \phi(a) +_S \phi(b)$

b) $\forall a, b \in R : \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$

c) $\phi(1_R) = 1_S$

Erinnern wir uns hier nochmals an die Generalvoraussetzung, dass alle Ringe ab Abschnitt 2.2 eine 1 haben, so könnte man sich fragen, wie die Definition für allgemeinere Ringe aussehen müsste. Für diese würde einfach Bedingung c) wegfallen. Zu beachten ist, dass Bedingung c) nicht aus den beiden anderen gefolgert werden kann, sondern tatsächlich die Verträglichkeit mit der Struktur des Ringes **mit** 1 erzwingt.

Bemerkung 2.3.2 *Analog zu den bei Vektorraumhomomorphismen eingeführten Begriffsbildungen, verwenden wir bei Ringhomomorphismen die Begriffe* **Ringmonomorphismus** *(oder auch* **Einbettung***) bei Injektivität,* **Ringepimorphismus** *bei Surjektivität sowie* **Ringisomorphismus** *bei Bijektivität. Ist* $R = S$*, so sprechen wir auch von einem* **Ringendomorphismus**. *Einen bijektiven Ringendomorphismus nennen wir* **Ringautomorphismus**.

Satz 2.3.3 *Seien* $(R, +_R, \cdot_R)$ *und* $(S, +_S, \cdot_S)$ *Ringe und* $\phi : R \longrightarrow S$ *ein Ringhomomorphismus. Dann gilt:*

a) $\forall n \in \mathbb{N}, \forall r \in R : \phi(r^n) = (\phi(r))^n$

b) $\forall r \in R^* : \phi(r) \in S^*$

c) $\forall n \in \mathbb{N}, \forall r \in R^* : \phi(r^{-n}) = (\phi(r))^{-n}$

Beweis: Aussage a) folgt direkt aus der n-fachen Anwendung von 2.3.1,b), ebenso wie c) nach Beweis von b).
Zum Beweis von b) seien $r, s \in R^*$ mit $r \cdot_R s = 1_R$. Dann gilt:

$$\phi(r) \cdot_S \phi(s) = \phi(r \cdot_R s) = \phi(1_R) = 1_S,$$

weswegen $\phi(r), \phi(s) \in S^*$.

□

Definition 2.3.4 *Seien $(R, +_R, \cdot_R), (S, +_S, \cdot_S)$ Ringe und sei $\phi : R \longrightarrow S$ ein Ringhomomorphismus. Dann heisst*

$$\ker(\phi) := \{x \in R \mid \phi(x) = 0_S\} = \phi^{-1}(\{0_S\})$$

der **Kern** *von ϕ. Das Bild von ϕ ist definiert als*

$$\mathrm{Im}(\phi) := \{y \in S \mid \exists x \in R : \phi(x) = y\} = \{\phi(x) \mid x \in R\}.$$

Definition 2.3.5 *Sei $(R, +_R, \cdot_R)$ ein Ring und $\emptyset \neq S \subseteq R$ eine Teilmenge. S heißt Unterring von R, kurz $S \leq R$, falls $(S, +_R, \cdot_R)$ ein Ring ist.*

Lemma 2.3.6 *Sei $(R, +_R, \cdot_R)$ ein Ring und $\emptyset \neq S \subseteq R$ eine Teilmenge. S ist Unterring von R, falls:*

a) $\forall s_1, s_2 \in S : s_1 +_R (-s_2) \in S$

b) $\forall s_1, s_2 \in S : s_1 \cdot_R s_2, s_2 \cdot_R s_1 \in S$

c) $1_R \in S$

Beweis: Die Voraussetzung $S \neq \emptyset$ zusammen mit Bedingung a) ist gerade das Untergruppenkriterium für S bzgl. der Addition, so dass wir daraus direkt schließen können, dass $(S, +_R)$ abelsche Gruppe ist.
Die Bedingung b) liefert uns die Abgeschlossenheit bzgl. der Multiplikation, bei der wir für zwei gegebene Elemente beide Reihenfolgen betrachten, da wir für R keine Kommutativität vorausgesetzt haben.[1] Daraus folgt bereits, dass $(S, \cdot_R)$ eine Halbgruppe ist, da die Assoziativität dann direkt aus der Assoziativität in R folgt. Weil nun nach Bedingung c) $1_R \in S$, ist diese Halbgruppe auch ein Monoid.
Die beiden Distributivgesetze gelten wiederum wegen der Abgeschlossenheit

[1] Natürlich reicht es, nur eine Reihenfolge zu fordern, da ja die Rollen von s_1 und s_2 bei einer Aussage "für alle s_1, s_2 "vertauscht werden können.

von $+_R$ und $\cdot_R$ in S und der Gültigkeit der Gesetze in R.
Damit wurde gezeigt, dass $(S, +_R, \cdot_R)$ ein Unterring von $(R, +_R, \cdot_R)$ ist.

□

Satz 2.3.7 *Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe und $\phi : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt:*

a) $\mathrm{Im}(\phi)$ *ist Unterring von S.*

b) Ist $R_1 \leq R$ Unterring, so ist $\phi(R_1) = \{\phi(x) \mid x \in R_1\}$ Unterring von S.

c) Ist $S_1 \leq S$ Unterring, so ist $\phi^{-1}(S_1) = \{x \in R \mid \phi(x) \in S_1\}$ Unterring von R.

d) Ist R kommutativ, so auch $\phi(R)$.

e) ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{0\}$.

Beweis: Die Beweise der Aussagen a),b) und c) sind direkte Anwendungen des Unterringkriteriums, weswegen deren Beweis eine gute Übung sein kann. Für den vorletzten Beweisteil d) betrachten wir einen kommutativen Ring R. Dann gilt im Unterring $\phi(R)$:

$$\forall r_1, r_2 \in R : \phi(r_1) \cdot_S \phi(r_2) = \phi(r_1 \cdot_R r_2) = \phi(r_2 \cdot_R r_1) = \phi(r_2) \cdot_S \phi(r_1),$$

was gerade die Kommutativität von $\phi(R)$ ist.
Ein Ringhomomorphismus ist insbesondere auch ein Gruppenhomomorphismus der zugrundeliegenden abelschen Gruppen $(R, +_R)$ und $(S, +_S)$, für den die Äquivalenz bereits in der Linearen Algebra bewiesen wurde. Sie erinnern sich sicher an die Argumente: Haben zwei unterschiedliche Elemente dasselbe Bild, so liegt ihre Differenz im Kern. Liegt zusätzlich zur Null ein weiteres Element im Kern, so haben die beiden Elemente dasselbe Bild.

□

Notation 2.3.8 *Ab jetzt werden wir die unteren Indizes bei den beiden Verknüpfungen in Ringen nur noch dort schreiben, wo eine echte Verwechslungsgefahr besteht.*

2.4 Charakteristik

Studierende, die bei mir im letzten Semester Lineare Algebra gehört haben, haben auf einem der Übungsblätter den Begriff der Charakteristik eines Ringes/Körpers gesehen. Formal eingeführt war er dort jedoch noch nicht. Daher holen wir das nun nach:

Definition 2.4.1 *Sei $(R, +, \cdot)$ ein Ring. Existiert eine positive Zahl $\ell \in \mathbb{N}$ mit*

$$\sum_{i=1}^{\ell} r = 0 \quad \forall r \in R,$$

so heißt die kleinste solche Zahl die **Charakteristik** *von R, kurz* $\mathrm{char}(R)$. *Existiert solch eine Zahl nicht, so definiert man* $\mathrm{char}(R) = 0$.

Die Beschreibung der Charakteristik in der obigen Definition ist offensichtlich etwas unhandlich. Statt alle $r \in R$ zu betrachten, reicht es völlig aus das kleinste ℓ zu wählen, für das

$$\sum_{i=1}^{\ell} 1 = 0.$$

(Klammern Sie einfach in der Summe der Definition r mittels Distributivgesetz aus.)
Aber auch nach dieser Vereinfachung erscheint insbesondere die Wahl von 0 im Falle der Nicht-Existenz eines ℓ noch nicht natürlich. Woher diese kommt, erklärt die folgende Interpretation der Charakteristik:

Bemerkung 2.4.2 *Betrachte die Abbildung*

$$\begin{aligned} \chi : \mathbb{Z} &\longrightarrow R \\ m &\longmapsto \chi(m) = m \cdot 1_R = \varepsilon(m) \cdot \sum_{i=1}^{|m|} 1_R, \end{aligned}$$

wobei die ad hoc Notation $\varepsilon(m)$ gerade das Vorzeichen von m codiert:

$$\varepsilon(m) = \begin{cases} 1_R & \text{für } m \geq 0 \\ -1_R & \text{für } m < 0 \end{cases}.$$

χ ist ein Ringhomomorphismus, wie sich direkt nachrechnen läßt. Das sollten Sie sich beim Nacharbeiten klarmachen und im Falle von Problemen nachfragen. Denken Sie daran, dass eine leere Summe $\sum_{i=1}^{0} 1_R$ gleich dem neutralen Element der Addition ist.
Offensichtlich existiert ein $\ell \in \mathbb{N}$ mit $\sum_{i=1}^{\ell} 1_R = 0$ genau dann, wenn $\ell \in \ker(\chi)$, was bedeutet:

$$\ker(\chi) = \{0\} \iff \operatorname{char}(R) = 0.$$

Gilt für zwei Zahlen $s, t \in \mathbb{Z}$

$$\chi(s) = \varepsilon(s) \cdot \sum_{i=1}^{|s|} 1_R = 0_R \text{ und } \chi(t) = \varepsilon(t) \cdot \sum_{i=1}^{|t|} 1_R = 0_R,$$

so gilt auch für jede $\mathbb{Z}$-Linearkombination von s und t:

$$\chi(as + bt) = \chi(a) \cdot_R \chi(s) +_R \chi(b) \cdot_R \chi(t) = \chi(a) \cdot_R 0_R +_R \chi(b) \cdot_R 0_R = 0_R.$$

Damit ist $\ker(\chi)$, welches wegen $0_R \in \ker(\chi)$ nicht leer ist, ein Ideal in $\mathbb{Z}$ und damit, wie wir aus dem vorigen Kapitel wissen, ein Hauptideal, erzeugt von seinem kleinsten positiven Element. Es gilt also:

$$\ker(\chi) = \langle m \rangle \iff \operatorname{char}(R) = m.$$

Satz 2.4.3 *Sei R ein Integritätsring. Dann ist R entweder von Charakteristik Null oder $\operatorname{char}(R)$ ist eine Primzahl.*

Beweis: Wir führen einen Widerspruchsbeweis:
Nehmen wir also an, dass die Charakteristik von R ein zusammengesetzte Zahl ist. Es ist daher $\operatorname{char}(R) = n_1 \cdot n_2$ für $n_1, n_2 \in \mathbb{N} \setminus \{1\}$. Da $n_1 \cdot n_2$ als Charakteristik nach Definition das kleinste Element ℓ ist, für das gilt $\chi(\ell) = 0_R$, wissen wir, dass gilt:

$$\chi(n_1) \neq 0_R \neq \chi(n_2), \text{ aber } \chi(n_1) \cdot_R \chi(n_2) = \chi(n_1 \cdot n_2) = 0_R.$$

Damit sind $\chi(n_1), \chi(n_2)$ Nullteiler in R im Widerspruch zu der Voraussetzung, dass R Integritätsring ist.

□