Ringhomomorphismen und Ideale

Jan Wiesemann

Wintersemester 2024/25

Dieses Skript wurde für einen Proseminarvortrag in meinem dritten Fachsemester für Mathematik verfasst.

1 Ringe

Definition (asso. Ring)**.** Wir nennen $(R, +, \cdot)$ einen *assoziativen Ring*, wenn gilt:

(i) $(R, +)$ ist abelsche Gruppe.

(ii) $(R, \cdot)$ ist Monoid.

(iii) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$gelten für alle $a, b, c \in R$.

Die eingebettete abelsche Gruppe schreibt man auch oft als R^+.

Definition (komm. Ring)**.** Ist R ein Ring wie oben und $(R, \cdot)$ kommutativ dann nennen wir R einen *kommutativen Ring*.

Anmerkung. Bei kommutativen Ringen reicht es nur eins der Distributivgesetze zu fordern.

Beispiele für Ringe:

- Ring der ganzen Zahlen $\mathbb{Z}$
- Polynomring $R[T]$
- Endliche Ringe $\mathbb{Z}/n\mathbb{Z}$
- Der Nullring
- Alle Körper k
- $(\mathrm{Mat}_{n\times n}(R))$

Im Folgenden benutze ich den Begriff *Ring* immer für einen kommutativen Ring. Dies ist auch in Lehrbüchern und vielen anderen Kontexten gebräuchlich.

Anmerkung. Es ist außerdem noch interessant anzumerken, dass manche Authoren in der Definition nicht einmal, dass multiplikative neutrale Element fordern. Diese Authoren benutzen dann den Begriff *Ring mit Eins*, für das, was wir bereits als einen Ring auffassen.

2 Ringhomomorphismen

Wir wollen eine Abbildung, die die Ringaxiome erhält, sowie Eins- und Nullelement wieder auf dergleichen abbildet. Dafür fordern wir drei Eigenschaften:

Definition (Ringhomomorphismus)**.** Wir nennen $\varphi : R \to R'$ einen *Ringhomomorphismus*, wenn folgende drei Eigenschaften erfüllt sind:

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

(iii) $\varphi(1_R) = 1_{R'}$

Da R^+ eine Gruppe ist, definiert (i) einen Gruppenhomomorphismus. Somit gilt bereits $\varphi(0_R) = 0_{R'}$. Als kleine Wiederholung hier auch noch der Beweis:
Wähle $a = b = 0$.

$$\begin{aligned}\varphi(0+0) &= \varphi(0) + \varphi(0)\\ \varphi(0) &= \varphi(0) + \varphi(0)\\ \varphi(0) - \varphi(0) &= \varphi(0) + \varphi(0) - \varphi(0)\\ 0 &= \varphi(0)\end{aligned}$$

□

Da $(R, \cdot)$ keine Untergruppe bildet, funktioniert dieser Beweis nicht und wir müssen die Abbildung auf das Einselement seperat fordern. Das einfachste Gegenbeispiel ist hierfür die Nullabbildung $\varphi(r) = 0$. Sie erfüllt zwar (i) und (ii), da $0 = 0 + 0 = 0 \times 0$, jedoch gilt (iii) nur, wenn auch $1_{R'} = 0_{R'}$ gilt, wir also im Nullring sind.

Man kann sich schnell dazu überlegen, dass sogar beide Richtugen gelten. Also die Nullabbildung ist genau dann ein Ringhomomorphismus, wenn der Zielring der Nullring ist.

Anmerkung. Einem wird noch öfter auffallen, dass der Nullring immer mal wieder auftaucht. Trotz seines fast schon trivialen Charakters hat er, ähnlich wie die Null selbst, sehr viel Relevanz in der Mathematik. Außerdem führen alle Ringhomomorphismen, die aus dem Nullring rausführen zwangsweise wieder in den Nullring rein. Somit bleibt man in ihm *gefangen*, sobald man einmal in ihm landet.

Definition (Isomorphismen und Automorphismen)**.** Diese Begriffe lassen sich wie gewöhnlich definieren:
Sei $\varphi : R \to R'$ ein Ringhomomorphismus.

- Wir nennen φ einen Isomorphismus, wenn φ bijektiv ist, bzw. wenn eine Umkehrabbildung $\varphi' : R' \to R$ existiert.
- Wir nennen φ einen Automorphismus, wenn $R = R'$ ist.

Ich war zunächst erstaunt, dass es überhaupt Ringautomorphismen gibt, die nicht die Identität sind. Immerhin sind sind die Bedinungen der Ringhomomorphismus deutlich strikter, als die der Gruppenhomomorphismen oder der linearen Abbildung.
Ein Bespiel für ein Ringautomorphismus wäre jedoch z.B. folgender:

$$\varphi : \mathbb{C} \to \mathbb{C}; \qquad x + iy \longmapsto x - iy$$

Den Nachweis, dass die Axiome für Ringhomomorphismen erfüllt sind, lasse ich als Hausaufgabe für den Leser.

Ich hatte eben angemerkt, dass die Definition des Ringhomomorphismen sehr strikt gewählt ist. Ein Beispiel dafür ist folgender Satz:

Satz. *Es existiert genau ein Ringhomomorphismus $\varphi : \mathbb{Z} \to R$.*
Sei ohne Einschränkungen $n \geq 0$. Dann wird dieser wird definiert durch:

$$\varphi(n) = \sum_{1}^{n} 1_R \qquad \textit{und} \qquad \varphi(-n) = -\varphi(n)$$

Beweis. Beweisen wir zunächst die Eindeutigkeit. Nehme an φ sei ein beliebiger Ringhomomorphismus: Nach Definition gilt $\varphi(1) = 1_R$ und folglich $\varphi(n+1) = \varphi(n) + 1_R$. Das definiert rekursiv bereits die Form für alle Zahlen in $\mathbb{N}_0$. Um $\varphi(n-n) = 0$ zu erfüllen setzt man dazu noch $\varphi(-n) = -\varphi(n)$.

Müssen jetzt noch zeigen, dass φ auch wirklich ein Ringhomomorphismus ist. Dafür nehmen wir die Form, die wir oben aus den Ringhomomorphismus Eigenschaften gefolgert haben, nun als Definition an für unser Abbildung φ. Abbildung auf das Einselement ist nach Definition klar. Müssen zeigen, dass Addition und Multiplikation respektiert werden:
$\varphi(m+1) = \varphi(m) + \varphi(1)$ und $\varphi(m \cdot 1) = \varphi(m)\varphi(1)$. Das nehmen wir als Induktionsstart für folgende Induktionsannahmen: $\varphi(m+n) = \varphi(m) + \varphi(n)$ und $\varphi(mn) = \varphi(m)\varphi(n)$. Induktionsschritt sieht dann, wie folgt aus:

$$\begin{aligned}
\varphi(m+(n+1)) &= \varphi((m+n)+1) && \text{(Assoziativität)} \\
&= \varphi(m+n)+1 && \text{(Definition von } \varphi\text{)} \\
&= \varphi(m)+\varphi(n)+1 && \text{(Induktionsvorautsetzung)} \\
&= \varphi(m)+\varphi(n+1) && \text{(Definition von } \varphi\text{)}
\end{aligned}$$

$$\begin{aligned}
\varphi(m(n+1)) &= \varphi(mn+m) && \text{(Distributivgesetz von } R\text{)} \\
&= \varphi(mn)+\varphi(m) && \text{(Siehe oben)} \\
&= \varphi(m)\varphi(n)+\varphi(m) && \text{(Induktionsvorraussetzung)} \\
&= \varphi(m)(\varphi(n)+1) && \text{(Distributivgesetz von } R'\text{)} \\
&= \varphi(m)\varphi(n+1) && \text{(Definition von } \varphi\text{)}
\end{aligned}$$

□

Der Satz gibt einem auch die Freiheit in beliebigen Ringen mit der Notation von $\mathbb{Z}$ zu arbeiten, da die Bilder in dem Zielring eindeutig bestimmt sind.

Satz (Einsetzungsprinzip)**.** *Sei $\varphi : R \to R'$ ein Ringhomomorphismus, dann existiert zu jedem $r' \in R'$ eine eindeutig bestimmte Fortsetzung von φ zu $\Phi : R[T] \to R'$, die T auf r' abbildet und auf den konstanten Polynomen gleich ist zu φ.*

Diese Aussage gilt sogar für Multiindizes $R[T_1, ..., T_n]$, wenn man das einzusetzende r', als Vektor $(r'_1, ..., r'_n)$ in $(R')^n$ auffasst.

Beweisskizze. Zunächst möchte ich anmerken, dass der Beweis direkt für Multiindizes funktioniert. Man muss lediglich alle r' und T als Indizevektoren auffassen. Die Beweisidee ist wieder ähnlich, wie bei dem letzten Beweis. Man würde erst annehmen, dass wir einen beliebigen Ringhomomorphismus haben, der dazu T auf r' abbildet und auf den konstanten Polynomen gleich mit φ ist und damit dann die Eindeutigkeit zeigen. Danach nimmt man genau diese Form als Definition und folgert, dass diese Form einen Rinhomomorphismus definiert. Ich möchte hier aus Zeitgründen nur den ersten Teil des Beweis machen:

Wenn man Φ Stück für Stück aufbaut, kann man sich schnell davon überzeugen, dass diese Form die einzige mögliche Form sein muss. Also:

$$\Phi\Big(\sum a_i T^i\Big) = \sum \varphi(a_i)(r')^i$$

Damit haben wir bereits eine eindeutige Form.

Jetzt müsste man noch beweisen, dass Φ einen Ringhomomorphismus definiert. Wen es interessiert, der kann im Buch von Artin oder in meiner alten (und teilweise fehlerhaften) Version des Skripts nachlesen, denn dort ist der Beweis in ausführlicherer Form vorhanden.

Beispiel. Ein Beispiel für das Einsetzungsprinzip, ist der Wechsel des Koeffizientenrings.
Sei $\varphi : R \to R'$ ein Ringhomomorphismus. Nach dem Einsetzungsprinzip existiert folgende Fortsetzung $\Phi : R[T] \to R'$. Und da $R' \subset R'[T]$ ein Unterring ist, können wir den Wertebereich vergrößern und bekommen den Ringhomomorphismus $\Phi : R[T] \to R'[T]$.

Z.B. für $\mathbb{Z} \to \mathbb{F}_p$ erhalten wir:

$$\mathbb{Z}[T] \to \mathbb{F}_p[T]; \qquad \sum_i a_i T^i \longmapsto \sum_i (a_i \bmod p) T^i$$

Beispiel. Ein anderes Andwendungsbeispiel wäre, formal zu zeigen, dass $R[x][y]$ und $R[x, y]$ isomorph sind. Der Beweis ist jedoch etwas länger und deutlich nicht so interessant, wie die Tatsache an sich, dass es geht. Anschaulich kann man sich einfach vorstellen, dass bei $R[x][y] \to R[x, y]$ Polynome ausmultipliziert und bei $R[x, y] \to R[x][y]$ nach y sortiert. Der Beweis spielt dann mit trivialen Inklusionsabbildungen und dem Einsetzungsprinzip, um es rigoros zu zeigen. Das möchte ich hier jedoch auslassen, um mich interessanteren Themen witmen zu können.

Zum Beispiel wollen wir hier noch den Begriff des Kerns, in unserem Kontext der Ringhomomorphismen definieren:

Definition (Kern)**.** $\mathrm{Ker}(\varphi) := \{a \in R \mid \varphi(a) = 0\}$

Anders als der Kern eines Gruppenhomomorphismus, der eine Untergruppe gebildet hat, bildet der Kern eines Ringhomomorphismus in der Regel keinen Unterring. Bei der Definition des Rings, gehört schließlich das Einselement dazu, und wenn dieses im Kern ist, gilt $\varphi(1) = 0$. Somit sind wir entweder im Nullring, wo $1 = 0$ gilt oder unsere Abbildung erfüllt die Erhaltung des multiplikativen neutralen Element nicht.

Proposition. *Ist $a \in \mathrm{Ker}(\varphi)$ und $r \in R$, dann $ra \in \mathrm{Ker}(\varphi)$.*

Beweis. Da a im Kern, gilt $\varphi(a) = 0$. Es folgt:

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$$

□

Man kann sich den Kern auf eine gewisse Weise *magnetisch* vorstellen, da er Ringelemente bei Multiplikation in den Kern zieht.

Betrachten wir als Beispiel für einen Kern mal, den der Abbildung $\varphi : R[T] \to R$, die wir durch einsetzen von r erhalten. Dieser besteht dann offensichtlich aus den Polynomen die r als Nullstelle haben, also lässt sich der Kern definieren, durch alle Polynome, die durch $(T - r)$ teilbar sind. Somit:

$$\mathrm{Ker}(\varphi) = (T - r)R[T]$$

3 Ideale

Diese *magnetische* Eigenschaft, die wir gerade beim Kern beobachtet haben, lässt sich mit dem Begriff des Ideals abstrahieren.

Bevor wir das tun, hier jedoch noch kurz ein paar wissenswerte Kleinigkeiten. Der Begriff des *Ideals* kommt ursprünglich aus der Zahlentheorie, da man dort Zahlen gesucht hat, die *ideal* dafür wären, die Eindeutigkeit von irreduziblen Elementen wiederherzustellen. Sie wurden auch *ideales Element* oder *ideale Zahlen* genannt. Was sich dann später zu dem Begriff des *Ideals* entswickelt hat. Wen das genauer interessiert, der kann im elften Kapitel im Buch von Artin oder auf Wikipedia nachlesen.

Wollen nun das Ideal, wie man es heute kennt definieren:

Definition. (Ideal) Wir nennen die Teilmenge $\mathfrak{a}$ ein Ideal, wenn gilt:

(i) $\mathfrak{a}$ ist Untergruppe von R^+.

(ii) Ist $a \in \mathfrak{a}$ und $r \in R$, dann $ra \in \mathfrak{a}$.

Anmerkung. Durch die Überlappung der Definition mit der Proposition, die wir gerade zum Kern hatten, kann man schnell feststellen, dass der Kern immer ein Ideal des Wertebereichs ist.

Aus (i) folgt, dass das $\mathfrak{a}$ nicht leer und abgeschlossen unter Addition ist. Aus (ii) folgt, dass $\mathfrak{a}$ auch unter Multiplikation abgeschlossen ist und das sogar mit einem beliebigen Ringelement $r \in R$.

Mit dem wissen kann man eine äquivalente Definition definieren, die auch oft sehr von Nutzen sein kann:

Definition. $\mathfrak{a}$ ist nicht leer, und jede Linearkombination $\sum r_i a_i$ von elementen $a_i \in \mathfrak{a}$ und $r_i \in R$ liegt wieder in $\mathfrak{a}$.

Diese Definition ist besonders nützlich, da man Ideale *erzeugen* kann. Dafür ist die folgende Schreibweise sehr üblich:

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

Kann man ein Ideal mit einem einzigen Erzeuger ausdrücken, nennt man es auch *Hauptideal*. Zum Beispiel ist $(2, 4)$ ein Hauptideal, da man es auch als (2) schreiben kann.

Beispiele.

- triviale Ideale (0) und (1). Diese sind im Nullring identisch.
- die ganzen Zahlen $\mathbb{Z}$: gerade Zahlen. Also (2) in der Schreibweise.
- die Gaußschen Zahlen $\mathbb{Z}[i]$ haben ähnliche Ideale: (2), $(2i)$, $(2, 2i)$
- Körper k: Hier ist jeder Erzeuger $a \in k^\times$ *übereifrig* und erzeugt direkt komplett k. Da a^{-1} für alle a existiert können wir mit komposition von $r = a^{-1}b$ direkt jedes beliebige $b \in k$ generieren.

Anmerkung. Es ist immer sinnvoll den Ring zu erwähnen über den man gerade redet, da es aus der kompakten Schreibweise nicht direkt klar wird. Manche Authoren bevorzugen deshalb die Schreibweise Ra, aR oder RaR.

Ich habe ja vohin schonmal angemerkt, dass jeder Körper ein Ring ist. Diese Aussage, kann man mit dem Begriff des Ideals präzisieren:

Satz. *Ein Ring R ist genau dann ein Körper, wenn er exakt zwei Ideale besitzt.*

Beweis. " $\Rightarrow$ " : Sei R ein Körper. Die Existenz des Nullideals (0) und des Einsideals (1) ist trivial, da R nicht der Nullring ist. Nehmen wir an, dass es ein weiteres Ideal gibt, dann können wir, wie oben mit dem *übereifrigen* Erzeuger argumentieren, der die ganze Menge erzeugt, welche das Einsideal ist.

" $\Leftarrow$ " : Sei R ein Ring mit genau zwei Idealen. Zu zeigen seien $0 \neq 1$ und a^{-1} existiert für alle $a \in R \setminus 0$. $0 = 1$ tritt nur im Nullring auf. Da wir jedoch zwei Ideale haben, können wir nicht im Nullring sein. Unsere zwei Ideale müssen offensichtlich die trivialen Ideale sein. Da $a \neq 0$ gilt auch $(a) \neq (0)$. Da wir nur zwei Ideale haben, gilt nach dem Ausschlussprinzip $(a) = (1)$. Nach Definition des Ideals gibt uns das $aR = (1)$. Haben also gezeigt, dass aR jedes Element der Menge annehmen kann, und somit auch 1. In dem Fall haben wir unser Inverses gefunden, denn $ar = 1$ ist genau, dass was wir gesucht haben. □

Korollar. *Sei k Körper und R Ring, dann ist jeder Ringhomomorphismus $\varphi : k \to R$ entweder injektiv oder die Nullabbildung.*

Beweis. Wissen, dass der Kern ein Ideal von k sein muss. Da k ein Körper ist, gilt also $\mathrm{Ker}(\varphi) = (0)$ oder $\mathrm{Ker}(\varphi) = (1)$. Ist $\mathrm{Kern}(\varphi) = (0)$ folgt Injektivität. Ist $\mathrm{Kern}(\varphi) = (1)$, haben wir die Nullabbildung und R *muss* der Nullring sein. □

Satz. *Jedes Ideal im Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptideal.*

Beweis. Allen Untergruppen von $\mathbb{Z}^+$ nehmen die Form $n\mathbb{Z}$ an. Das sind bereits die Ideale. □

Anmerkung. Versucht man ein Ideal mit einer beliebigen Menge an Zahlen I zu generieren, lässt sich dieses Ideal durch $(\mathrm{ggT}(I))$ als Hauptideal ausdrücken.

Als letztes möchte ich noch zeigen, wie man den Begriff der *Charakteristik* formal mit Ringhomomorphismen definieren kann.

Definition (Charakteristik)**.** Sei $\varphi : \mathbb{Z} \to R$ der eindeutig bestimmte Ringhomomorphismus in einen Ring R. Wir definieren die *Charakteristik* $p \in \mathbb{N}_0$ von R als

$$\begin{cases} 0, & \text{falls } \mathrm{Kern}(\varphi) = (0); \\ \min\left(\{a \in \mathrm{Ker}(\varphi) \mid a \in \mathbb{N}\}\right), & \text{sonst.} \end{cases}$$

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben alle die Charakteristik $p = 0$. Der Nullring hat Charakterstik $p = 1$. Die Primkörper $\mathbb{F}_p$ und ihre Körpererweiterungen haben die Charakteristik p. Das nur so als kleine beispielhafte Liste.

Abschließende Worte. Ideale haben eine sehr große Relevanz in der Mathematik. Sie ermöglichen einem die Konstruktion der Restklassenringe und Quotientenkörper, sind also daher ein unverzichtbarer Teil des Werkzeugkasten der reinen Mathematik. Dieses Thema wird jedoch im nächsten Vortrag angesprochen, deshalb möchte ich da nicht zu viel davon vorwegnehmen. Vielen Dank, für's Lesen und der Freude am Mathematisieren!