8. Ideale und Faktorringe

Im letzten Kapitel haben wir Ringe eingeführt und (analog zur Theorie von Gruppen) Unterringe und Ringhomomorphismen untersucht. Es fehlen uns allerdings noch die Faktorstrukturen – d. h. wir müssen noch sehen, wie man aus einem Ring analog zu den Faktorgruppen in Kapitel 6 geeignete Unterstrukturen herausteilen kann. Ein Beispiel dafür haben wir bereits gesehen: In Beispiel 7.4 (b) hatten wir gezeigt, dass $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ein Ring ist. In diesem Fall hatten wir also durch Herausteilen der Untergruppe (bzw. des Normalteilers) $n\mathbb{Z}$ bereits eine Ringstruktur erhalten – insbesondere war also neben der Addition $\overline{a}+\overline{b} := \overline{a+b}$ auch die Multiplikation $\overline{a}\cdot\overline{b} := \overline{ab}$ wohldefiniert.

Wir wollen nun untersuchen, ob dies immer der Fall ist: Es sei R ein Ring und S eine additive Untergruppe von R. Da $(R,+)$ nach der Ringeigenschaft (R1) eine abelsche Gruppe ist, ist $(S,+)$ dann nach Beispiel 6.6 (a) sogar ein Normalteiler von $(R,+)$. Wir können nach Satz 6.13 also in jedem Fall schon einmal die Faktor*gruppe* $(R/S,+)$ bilden, d. h. wir haben auf R/S bereits eine wohldefinierte (und kommutative) Addition.

Leider bedeutet dies jedoch im Allgemeinen nicht, dass wir mit der Vorschrift $\overline{a}\cdot\overline{b} := \overline{ab}$ dann auch eine wohldefinierte Multiplikation auf R/S erhalten: Für $R=\mathbb{R}$ und $S=\mathbb{Z}$ ist z. B. $\overline{1}=\overline{2}$ in $\mathbb{R}/\mathbb{Z}$ wegen $2-1\in\mathbb{Z}$, aber $\overline{\frac{1}{2}\cdot 1} = \overline{\frac{1}{2}} \neq \overline{1} = \overline{\frac{1}{2}\cdot 2}$ wegen $1-\frac{1}{2}\notin\mathbb{Z}$, so dass die Multiplikation von $\overline{\frac{1}{2}}$ mit $\overline{1}=\overline{2}$ also nicht wohldefiniert ist. Da $\mathbb{Z}$ sogar ein Unterring von $\mathbb{R}$ ist, sehen wir an diesem Beispiel auch schon, dass wir Unterringe auch nicht herausteilen können.

Wir müssen an unsere herausgeteilte Menge S also andere Bedingungen stellen. Wie im Fall von Faktorgruppen geben wir auch hier die nötigen Bedingungen zunächst in Form einer Definition an und zeigen später, dass wir damit wirklich das Gewünschte erreichen.

Definition 8.1 (Ideale)**.** Eine Teilmenge I eines Ringes R heißt ein **Ideal**, wenn gilt:

(I1) $0\in I$;

(I2) für alle $a,b\in I$ ist $a+b\in I$;

(I3) für alle $a\in I$ und $x\in R$ ist $a\cdot x\in I$.

Ist I ein Ideal von R, so schreiben wir dies als $I \trianglelefteq R$, sofern keine Verwechslungsgefahr mit dem Begriff des Normalteilers aus Definition 6.3 besteht. (Die gleiche Bezeichnung kommt daher, dass sich Ideale in Ringen analog zu Normalteilern in Untergruppen als diejenigen Teilmengen herausstellen werden, mit denen eine Faktorstruktur definiert werden kann.)

Bemerkung 8.2.

(a) Jedes Ideal I eines Ringes R ist eine additive Untergruppe von R: Die Eigenschaften (U1) und (U2) des Untergruppenkriteriums aus Satz 3.3 sind genau die Bedingungen (I2) und (I1) in Definition 8.1, und die Eigenschaft (U3) folgt aus (I3) mit $x=-1$. Da $(R,+)$ außerdem nach Definition eines Ringes abelsch ist, ist jedes Ideal von R nach Beispiel 6.6 (a) sogar ein Normalteiler bezüglich der Addition in R.

(b) Ähnlich wie beim Untergruppenkriterium in Bemerkung 3.4 (b) kann die Bedingung (I1) durch die scheinbar schwächere Forderung $I\neq\emptyset$ ersetzt werden: Gibt es nämlich ein Element $a\in I$, so folgt mit (I3) sofort auch $0=a\cdot 0\in I$.

(c) Ist I ein Ideal in einem Ring R mit $1\in I$, so folgt aus Eigenschaft (I3) von Definition 8.1 mit $a=1$ sofort $x\in I$ für alle $x\in R$, d. h. es ist dann bereits $I=R$. Da jeder Unterring die 1 enthalten muss, schließen sich Unterringe und Ideale also fast vollständig aus: Die einzige Teilmenge von R, die gleichzeitig ein Unterring und ein Ideal von R ist, ist R selbst. Unterringe und Ideale sind in diesem Sinne also „sehr unterschiedliche“ Objekte.

09

Beispiel 8.3.

(a) Im Ring $R = \mathbb{Z}$ ist $I = n\mathbb{Z}$ für $n \in \mathbb{N}$ ein Ideal:

(I1) ist offensichtlich;

(I2) für zwei Zahlen $kn, ln \in n\mathbb{Z}$ (mit $k, l \in \mathbb{Z}$) ist auch $kn + ln = (k+l)n \in n\mathbb{Z}$;

(I3) für $kn \in n\mathbb{Z}$ und $x \in \mathbb{Z}$ (mit $k, x \in \mathbb{Z}$) ist auch $kn \cdot x = (kx) \cdot n \in n\mathbb{Z}$.

Da jedes Ideal eines Ringes nach Bemerkung 8.2 (a) auch eine additive Untergruppe sein muss und diese im Ring $\mathbb{Z}$ nach Satz 3.18 alle von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}$ sind, sind dies auch bereits alle Ideale von $\mathbb{Z}$. Insbesondere stimmen Untergruppen und Ideale im Ring $\mathbb{Z}$ also überein. Dies ist aber nicht in jedem Ring so: So ist z. B. $\mathbb{Z}$ eine additive Untergruppe von $\mathbb{Q}$, aber nach Bemerkung 8.2 (c) kein Ideal (denn es ist ja $1 \in \mathbb{Z}$, aber $\mathbb{Z} \neq \mathbb{Q}$).

(b) In einem Ring R sind $\{0\}$ und R offensichtlich stets Ideale von R. Sie werden die **trivialen Ideale** von R genannt.

(c) Ist K ein Körper, so sind die trivialen Ideale $\{0\}$ und K aus (b) bereits die einzigen Ideale von K: Enthält ein Ideal $I \trianglelefteq K$ nämlich ein beliebiges Element $a \neq 0$, so enthält es nach Eigenschaft (I3) auch $1 = a \cdot a^{-1}$ und ist nach Bemerkung 8.2 (c) damit gleich K.

Wir hatten schon erwähnt, dass Ideale in Ringen in gewissem Sinne analog zu Normalteilern in Gruppen sind. Da Kerne von Gruppenhomomorphismen nach Lemma 6.7 Normalteiler sind, ist es daher nicht weiter erstaunlich, dass Kerne von Ringhomomorphismen Ideale sind:

Lemma 8.4. *Ist $f\colon R \to S$ ein Ringhomomorphismus, so ist* $\operatorname{Ker} f$ *ein Ideal von R.*

Beweis. Wir prüfen die Idealeigenschaften nach:

(I1) Es ist $f(0) = 0$ nach Bemerkung 7.27 und damit $0 \in \operatorname{Ker} f$.

(I2) Für $a, b \in \operatorname{Ker} f$ ist $f(a+b) = f(a) + f(b) = 0 + 0 = 0$ und damit $a + b \in \operatorname{Ker} f$.

(I3) Für $a \in \operatorname{Ker} f$ und $x \in R$ ist $f(ax) = f(a)f(x) = 0 \cdot f(x) = 0$ und damit $ax \in \operatorname{Ker} f$. □

Als wir Untergruppen in Kapitel 3 untersucht haben, haben wir gesehen, dass man zu jeder Teilmenge M einer Gruppe G eine davon erzeugte Untergruppe $\langle M \rangle$ konstruieren kann, die man sich vorstellen kann als die „kleinste Untergruppe von G, die M enthält“. Wir hatten diese von M erzeugte Untergruppe zwar elegant, aber recht abstrakt definiert als Durchschnitt aller Untergruppen, die M enthalten (siehe Definition 3.11). Später hatten wir in Aufgabe 3.15 dann eine Darstellung für $\langle M \rangle$ gesehen, die zwar explizit war, aber dennoch so kompliziert, dass sie insbesondere für nicht-abelsche Gruppen meistens nicht wirklich zur Berechnung von $\langle M \rangle$ geeignet ist.

Auch für Ideale gibt es eine ähnliche Konstruktion, mit der man einer Teilmenge M eines Ringes R ein „kleinstes Ideal, das M enthält“ zuordnen kann. Man könnte dies analog zum Fall von Untergruppen als Schnitt über alle Ideale definieren, die M enthalten (siehe Aufgabe 8.7) – im Fall von Idealen ist jedoch die zu Aufgabe 3.15 analoge explizite Formel so einfach und nützlich, dass wir sie hier als Definition verwenden wollen.

Definition 8.5 (Erzeugte Ideale)**.** Es sei M eine beliebige Teilmenge eines Ringes R. Dann heißt

$$\langle M \rangle := \{a_1x_1 + \cdots + a_nx_n : n \in \mathbb{N}; a_1, \ldots, a_n \in M; x_1, \ldots, x_n \in R\},$$

das von M **erzeugte Ideal**. Man sagt auch, dass $\langle M \rangle$ aus den endlichen *Linearkombinationen* von Elementen aus M mit Koeffizienten in R besteht.

Ist $M = \{a_1, \ldots, a_n\}$ eine endliche Menge, so schreibt man statt $\langle M \rangle = \langle \{a_1, \ldots, a_n\} \rangle$ in der Regel auch $\langle a_1, \ldots, a_n \rangle$.

Beachte, dass wir wegen der Analogie der Konstruktion hier die gleiche Bezeichnung wie für die von M erzeugte Untergruppe in Definition 3.11 verwendet haben – genauso wie wir das Symbol „$\leq$“ sowohl für Untergruppen als auch Unterringe benutzt haben. Falls eine Verwechslungsgefahr besteht, ist für das von M erzeugte Ideal in der Literatur statt $\langle M \rangle$ oft auch die Bezeichnung (M) oder $\langle M \rangle_R$ üblich.

Bevor wir Beispiele dieser Konstruktion betrachten, sollten wir uns zunächst davon überzeugen, dass $\langle M \rangle$ wirklich ein Ideal ist, und in der Tat auch interpretiert werden kann als das kleinste Ideal, das M enthält. Wir zeigen dazu für $\langle M \rangle$ die zu Lemma 3.12 analogen Eigenschaften.

Lemma 8.6. *Für jede Teilmenge M eines Ringes R gilt:*

(a) *$\langle M \rangle$ ist ein Ideal, das M enthält.*

(b) *Ist I ein beliebiges Ideal, das M enthält, so gilt bereits $\langle M \rangle \subset I$.*

$\langle M \rangle$ ist damit also das kleinste Ideal, das M enthält.

Beweis.

(a) $\langle M \rangle$ erfüllt (I1), da in Definition 8.5 auch $n = 0$ erlaubt ist und damit die leere Summe, also 0, in $\langle M \rangle$ enthalten ist. Die Eigenschaft (I2) ist offensichtlich. Für (I3) seien $a \in \langle M \rangle$ und $x \in R$, also $a = a_1x_1 + \cdots + a_nx_n$ für gewisse $n \in \mathbb{N}$, $a_1, \ldots, a_n \in M$ und $x_1, \ldots, x_n \in R$. Dann ist auch $ax = a_1(xx_1) + \cdots + a_n(xx_n) \in \langle M \rangle$. Also ist $\langle M \rangle$ ein Ideal. Weiterhin ist M natürlich in $\langle M \rangle$ enthalten, denn für $a \in M$ ist $a = a \cdot 1 \in \langle M \rangle$.

(b) Es seien $n \in \mathbb{N}$, $a_1, \ldots, a_n \in M$ und $x_1, \ldots, x_n \in R$. Ist I ein beliebiges Ideal mit $M \subset I$, so enthält I also $a_1x_1, \ldots, a_nx_n$ nach Eigenschaft (I3), und damit auch $a_1x_1 + \cdots + a_nx_n$ nach (I2) (bzw. nach (I1) im Fall $n = 0$). Also gilt $\langle M \rangle \subset I$. □

Aufgabe 8.7. Es sei M eine Teilmenge eines Ringes R. Zeige, dass für das von M erzeugte Ideal $\langle M \rangle$ die Formel

$$\langle M \rangle = \bigcap_{\substack{I \trianglelefteq R \\ \text{mit } M \subset I}} I$$

gilt, also die analoge Formel zu unserer Definition 3.11 für die von einer Teilmenge einer Gruppe erzeugte Untergruppe.

Beispiel 8.8.

(a) Besteht die Menge M in Definition 8.5 nur aus einem Element a, so ist offensichtlich

$$\langle a \rangle = \{ax : x \in R\}$$

die „Menge aller Vielfachen von a“. Insbesondere gilt in $R = \mathbb{Z}$ also für $n \in \mathbb{N}$

$$\langle n \rangle = \{nx : x \in \mathbb{Z}\} = n\mathbb{Z},$$

d. h. hier stimmt das von einem Element erzeugte Ideal mit der von ihm erzeugten Untergruppe in Beispiel 3.13 (a) überein.

(b) Im Ring $R = \mathbb{Z} \times \mathbb{Z}$ ist das vom Element $(2,2)$ erzeugte Ideal

$$\langle (2,2) \rangle = \{(2,2) \cdot (m,n) : m,n \in \mathbb{Z}\} = \{(2m,2n) : m,n \in \mathbb{Z}\},$$

während die von diesem Element erzeugte (additive) Untergruppe nach Beispiel 3.13 (a) gleich

$$\{n \cdot (2,2) : n \in \mathbb{Z}\} = \{(2n,2n) : n \in \mathbb{Z}\}$$

ist.

(c) Wir wissen aus Beispiel 8.3 (c) bereits, dass ein Körper nur die beiden trivialen Ideale besitzt. In der Tat gilt hiervon auch die Umkehrung: Ist $R \neq \{0\}$ ein Ring, in dem $\{0\}$ und R die einzigen Ideale sind, so muss von jedem Element $a \neq 0$ das erzeugte Ideal $\langle a \rangle$ bereits gleich R sein und damit insbesondere die Eins enthalten. Nach (a) ist dann aber $ax = 1$ für ein $x \in R$, d. h. a ist invertierbar. Also ist R dann ein Körper.

Aufgabe 8.9. Ist I ein Ideal in einem Ring R, so heißt

$$\sqrt{I} := \{a \in R : a^n \in I \text{ für ein } n \in \mathbb{N}\} \quad \subset R$$

das **Radikal** von I.

(a) Zeige, dass $\sqrt{I}$ wieder ein Ideal von R ist.

(b) Man zeige: Ist $a \in \sqrt{\langle 0 \rangle}$, so ist $1+a$ eine Einheit in R.

(c) Berechne das Ideal $\sqrt{180\mathbb{Z}}$ in $\mathbb{Z}$.

Wie bereits angekündigt sind Ideale in Ringen besonders deswegen interessant, weil man mit ihnen analog zu Satz 6.13 Faktorstrukturen definieren kann. Dies wollen wir jetzt zeigen. Ist dazu zunächst einmal I eine additive Untergruppe in einem Ring R, so können wir in jedem Fall die zugehörige Faktorgruppe R/I bilden, d. h. es ist $\overline{a} = a + I$ für $a \in R$ (siehe Lemma 5.6 (b)) und $\overline{a} = \overline{b}$ in R/I genau dann, wenn $b - a \in I$ (siehe Bemerkung 5.7 (a)). Ist I zusätzlich ein Ideal, so lässt sich auch die Multiplikation wohldefiniert von R auf R/I übertragen:

Satz 8.10 (Faktorringe)**.** *Es sei $I \trianglelefteq R$ ein Ideal in einem Ring R. Dann gilt:*

(a) *Auf der Menge R/I ist neben der Addition auch die Multiplikation $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ wohldefiniert und macht R/I zu einem Ring.*

(b) *Die Restklassenabbildung $\pi \colon R \to R/I$, $a \mapsto \overline{a}$ ist ein surjektiver Ringhomomorphismus mit Kern I.*

*Analog zum Fall von Gruppen wird R/I als ein **Faktorring** von R bezeichnet.*

Beweis.

(a) Die Multiplikation ist wohldefiniert: Es seien $a, a', b, b' \in R$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, d. h. es ist $a' = a + u$ und $b' = b + v$ für gewisse $u, v \in I$. Dann gilt

$$a'b' = (a+u)(b+v) = ab + \underbrace{av + bu + uv}_{\in I},$$

wobei die Summe der letzten drei Terme in I liegt, weil jeder einen Faktor aus I (nämlich u oder v) enthält und Ideale bezüglich Summen sowie Produkten mit beliebigen Ringelementen abgeschlossen sind. Also ist $\overline{ab} = \overline{a'b'}$ in R/I.

Analog zu Satz 6.13 (a) übertragen sich nun die Ringeigenschaften aus Definition 7.1 sofort von R auf R/I. Wir zeigen exemplarisch die Distributivität (R3): Für alle $a, b, c \in R$ gilt

$$\left(\overline{a} + \overline{b}\right) \cdot \overline{c} = \overline{a+b} \cdot \overline{c} = \overline{(a+b)c} \overset{(*)}{=} \overline{ac + bc} = \overline{ac} + \overline{bc} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c},$$

wobei $(*)$ die Distributivität in R ist und alle anderen Gleichungen einfach nur die Definitionen der Verknüpfungen auf R/I sind.

(b) Wir wissen aus Satz 6.13 (b) bereits, dass die Restklassenabbildung π ein surjektiver additiver Gruppenhomomorphismus mit Kern I ist. Weiterhin ist $\pi(1) = \overline{1}$ das multiplikative neutrale Element des Faktorringes, und es gilt

$$\pi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b)$$

für alle $a, b \in R$. Also ist π sogar ein Ringhomomorphismus. □

Beispiel 8.11. Da $n\mathbb{Z}$ nach Beispiel 8.3 (a) ein Ideal in $\mathbb{Z}$ ist, ist $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ nach Satz 8.10 ein Ring – wie wir vorher schon in Beispiel 7.4 (b) gesehen hatten.

Zum Abschluss dieses Kapitels wollen wir schließlich noch den Homomorphiesatz, den wir in Satz 6.17 für Gruppen gesehen hatten, auf den Fall von Ringen übertragen. Mit unseren Vorbereitungen verläuft diese Übertragung nun genau wie erwartet:

Satz 8.12 (**Homomorphiesatz** für Ringe)**.** *Es sei $f \colon R \to S$ ein Ringhomomorphismus. Dann ist die Abbildung*

$$\begin{aligned} g \colon R/\operatorname{Ker} f &\to \operatorname{Im} f \\ \overline{a} &\mapsto f(a) \end{aligned}$$

zwischen dem Faktorring $R/\operatorname{Ker} f$ von R und dem Unterring $\operatorname{Im} f$ von S ein Ringisomorphismus.

Beweis. Da $\operatorname{Ker} f$ nach Lemma 8.4 ein Ideal von R ist, können wir den Faktorring $R/\operatorname{Ker} f$ bilden. Wenden wir weiterhin den Homomorphiesatz 6.17 für Gruppen auf den zugehörigen Gruppenhomomorphismus $f\colon (R,+) \to (S,+)$ an, so sehen wir, dass g wohldefiniert, mit der Addition verträglich und bijektiv ist. Außerdem ist g auch mit der Multiplikation verträglich: Für alle $a,b \in R/\operatorname{Ker} f$ ist

$$g(\overline{a} \cdot \overline{b}) = g(\overline{ab}) = f(ab) = f(a)\,f(b) = g(\overline{a}) \cdot g(\overline{b}).$$

Wegen $f(1) = 1$ gilt schließlich auch $g(\overline{1}) = f(1) = 1$, und damit ist g ein Ringisomorphismus. □

Aufgabe 8.13. Es seien R ein Integritätsring und $a,b \in R\backslash\{0\}$ keine Einheiten.

Man zeige: Ist $\overline{a}$ ein Nullteiler in $R/\langle b\rangle$, so ist $\overline{b}$ ein Nullteiler in $R/\langle a\rangle$.

Aufgabe 8.14. In einem Ring R heißt ein Element $e \in R$ *idempotent*, wenn $e^2 = e$.

Offensichtlich sind 0 und 1 stets idempotent. Man zeige nun:

(a) Ist $R = S \times T$ ein nicht-triviales Produkt von zwei Ringen (d. h. S und T sind beide nicht der Nullring), so besitzt R ein idempotentes Element $e \notin \{0,1\}$.

(b) Besitzt umgekehrt R ein idempotentes Element $e \notin \{0,1\}$, so ist $R \cong R/\langle e\rangle \times R/\langle 1-e\rangle$ isomorph zu einem nicht-trivialen Produkt von zwei Ringen.

Ist $\mathbb{Z}_8$ bzw. $\mathbb{Z}_{12}$ isomorph zu einem nicht-trivialen Produkt von zwei Ringen?