7. Ringe und Körper

In den bisherigen Kapiteln haben wir nur Gruppen, also insbesondere nur Mengen mit lediglich *einer* Verknüpfung, untersucht. In der Praxis gibt es aber natürlich auch viele Mengen, auf denen *zwei* Verknüpfungen gegeben sind, die man sich dann in der Regel als Addition und Multiplikation vorstellen kann: z. B. die Mengen der ganzen Zahlen, reellen Zahlen, reellwertigen Funktionen oder Matrizen. Da Addition und Multiplikation hierbei nicht einfach unabhängige Verknüpfungen sind, sondern in der Regel über ein „Distributivgesetz“ $(a+b)c = ac+bc$ miteinander zusammen hängen, reicht es in diesen Fällen nicht aus, einfach zwei Gruppenstrukturen auf derselben Menge zu betrachten. Stattdessen bilden derartige Mengen eine neue Struktur, die man einen *Ring* nennt und die wir jetzt einführen wollen.

Definition 7.1 (Ringe)**.**

(a) Ein **Ring** ist eine Menge R mit zwei Verknüpfungen $+\colon R\times R\to R$ und $\cdot\colon R\times R\to R$ (genannt „Addition“ und „Multiplikation“ und immer geschrieben als „$+$“ bzw. „$\cdot$“), so dass die folgenden Eigenschaften gelten:

(R1) $(R,+)$ ist eine abelsche Gruppe. (Wie üblich bezeichnen wir das neutrale Element dieser Verknüpfung mit 0 und das zu $a\in R$ inverse Element mit $-a$.)

(R2) Für alle $a,b,c\in R$ gilt $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ (**Assoziativität** der Multiplikation).

(R3) Für alle $a,b,c\in R$ gilt die **Distributivität**

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

Wir schreiben einen solchen Ring als $(R,+,\cdot)$, oder in der Regel auch einfach nur als R, wenn die Verknüpfungen aus dem Zusammenhang klar sind.

(b) Gilt zusätzlich zu (R1), (R2) und (R3) noch

(R4) Es gibt ein $e\in R$ mit $e\cdot a = a\cdot e = a$ für alle $a\in R$ (Existenz eines **neutralen Elements** der Multiplikation),

so heißt R ein **Ring mit Eins**.

(c) Gilt zusätzlich zu (R1), (R2) und (R3)

(R5) Für alle $a,b\in R$ gilt $a\cdot b = b\cdot a$ (**Kommutativität** der Multiplikation),

dann heißt R ein **kommutativer Ring**.

Konvention 7.2. Um unsere Untersuchung von Ringen nicht zu kompliziert werden zu lassen, wollen wir uns in dieser Vorlesung auf den in der Praxis wichtigsten Fall beschränken, in dem alle Eigenschaften (R1), ..., (R5) aus Definition 7.1 gelten. Wir vereinbaren daher:

$$\boxed{\text{Im Folgenden sei ein Ring stets kommutativ mit Eins.}}$$

Fasst man die Eigenschaften (R1), ..., (R5) zusammen, so ist ein Ring für uns also eine Menge mit zwei Verknüpfungen „$+$“ und „$\cdot$“, von denen die Addition eine abelsche Gruppe bildet, die Multiplikation alle Eigenschaften einer abelschen Gruppe mit Ausnahme der Existenz inverser Elemente besitzt, und die das Distributivgesetz erfüllen.

Wenn ihr in die Literatur schaut, werdet ihr feststellen, dass einige Autoren ebenfalls diese Konvention verwenden, während andere unter einem Ring wirklich nur eine Struktur mit den drei Eigenschaften (R1), (R2) und (R3) verstehen. Es bleibt einem also nichts anderes übrig, als bei jedem Buch, in dem man etwas über Ringe liest, erst einmal zu überprüfen, welche Konvention der Autor verwendet.

Bemerkung 7.3. Eine Eins wie in Eigenschaft (R4) von Definition 7.1 ist stets eindeutig: Sind e und $\tilde{e}$ zwei solche Einselemente, so folgt natürlich sofort $e = e \cdot \tilde{e} = \tilde{e}$. Wir schreiben das (eindeutig bestimmte) Einselement eines Ringes daher in der Regel einfach als 1, wenn dadurch keine Verwirrung entstehen kann.

Beispiel 7.4.

(a) $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ (mit der üblichen Addition und Multiplikation) sind natürlich Ringe. Ebenso gilt dies für die Menge $\mathbb{C}$ der komplexen Zahlen, die ihr inzwischen sicher aus den Grundlagen der Mathematik kennt.

(b) Es sei $n \in \mathbb{N}_{>0}$. Wir haben in Beispiel 6.15 bereits gesehen, dass sich die additive Gruppenstruktur der ganzen Zahlen wohldefiniert auf $\mathbb{Z}_n$ übertragen lässt, wenn man $\overline{a} + \overline{b} := \overline{a+b}$ setzt. Wir wollen nun zeigen, dass sich genauso auch die Multiplikation durch $\overline{a} \cdot \overline{b} := \overline{ab}$ auf $\mathbb{Z}_n$ übertragen lässt und $\mathbb{Z}_n$ damit zusammen mit der Addition zu einem Ring macht. Dazu rechnen wir zunächst analog zu Satz 6.13 (a) nach, dass diese Verknüpfung wohldefiniert ist: Sind $a, b, a', b' \in \mathbb{Z}$ mit $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$ in $\mathbb{Z}_n$, also $a' = a + kn$ und $b' = b + ln$ für gewisse $k, l \in \mathbb{Z}$, so ist auch

$$a'b' = (a+kn)(b+ln) = ab + aln + bkn + kln^2 = ab + n(al + bk + kln) \quad \in ab + n\mathbb{Z}$$

und damit $\overline{ab} = \overline{a'b'}$. Von den Ringeigenschaften aus Definition 7.1 hatten wir (R1) schon gezeigt. Die anderen Eigenschaften übertragen sich nun genau wie in Satz 6.13 (a) von $\mathbb{Z}$ auf $\mathbb{Z}_n$; wir zeigen hier exemplarisch (R2): Für alle $a, b, c \in \mathbb{Z}$ gilt

$$\left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right)$$

in $\mathbb{Z}_n$. Also ist $\mathbb{Z}_n$ ein Ring.

Wir werden in Kapitel 8 noch genauer untersuchen, in welchen Fällen sich Ringe durch Herausteilen einer additiven Untergruppe wieder zu neuen Ringen machen lassen.

(c) Sind R und S Ringe, so ist auch ihr Produkt $R \times S$ mit der komponentenweise definierten Addition und Multiplikation

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2) \quad \text{und} \quad (a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot b_1, a_2 \cdot b_2)$$

ein Ring (mit Nullelement $(0,0)$ und Einselement $(1,1)$). Der Beweis dieser Aussage verläuft natürlich völlig analog zum Fall von Gruppen in Konstruktion 1.5.

(d) Ist M eine beliebige Menge und R ein Ring, so rechnet man sofort nach, dass auch die Menge

$$S = \{f \colon M \to R \text{ Abbildung}\}$$

aller Abbildungen von M nach R mit der punktweise definierten Addition und Multiplikation

$$(f+g)(x) := f(x) + g(x) \qquad \text{und} \quad (f \cdot g)(x) := f(x) \cdot g(x)$$

ein Ring ist. Das Nullelement 0 in S ist dabei die konstante Funktion mit Wert $0 \in R$, das Einselement 1 die konstante Funktion mit Wert $1 \in R$.

(e) Die einelementige Menge $R = \{0\}$ (mit den trivialen Verknüpfungen) ist ein Ring, wenn man $e = 0$ setzt (d. h. es gilt hier $1 = 0$ im Sinne von Bemerkung 7.3). Man bezeichnet diesen (eher uninteressanten) Ring als den **Nullring**. Wir werden gleich in Lemma 7.5 (c) sehen, dass dies der einzige Ring ist, in dem $1 = 0$ gilt – wir müssen uns also über diese etwas merkwürdig aussehende Gleichung nicht allzu viele Gedanken machen.

Wie im Fall von Gruppen sollten wir als Erstes die wichtigsten Rechenregeln in Ringen auflisten. Einige davon ergeben sich sofort daraus, dass ein Ring R mit der Addition eine abelsche Gruppe ist – so ist z. B. $-(-a) = a$ für alle $a \in R$, und aus $x + a = x + b$ (für $x, a, b \in R$) folgt $a = b$ (siehe Lemma 1.10). Derartige Regeln brauchen wir natürlich hier nicht noch einmal zu beweisen. Neu sind hingegen die Rechenregeln, die die additive Struktur eines Ringes mit der multiplikativen verknüpfen:

Lemma 7.5 (Rechenregeln in Ringen)**.** *In jedem Ring R gilt:*

(a) *Für alle $a \in R$ ist $0 \cdot a = 0$.*

(b) *Für alle* $a, b \in R$ *ist* $(-a) \cdot b = -(a \cdot b)$.

(c) *Ist* R *nicht der Nullring, so ist* $1 \neq 0$.

Beweis.

(a) Für alle $a \in R$ gilt zunächst $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Subtrahieren wir nun $0 \cdot a$ von beiden Seiten dieser Gleichung, so erhalten wir wie behauptet $0 = 0 \cdot a$.

(b) Für alle $a, b \in R$ ist $(-a) \cdot b + a \cdot b = (-a+a) \cdot b = 0 \cdot b \overset{\text{(a)}}{=} 0$. Also ist $(-a) \cdot b$ das additive Inverse zu $a \cdot b$, d. h. es ist $(-a) \cdot b = -(a \cdot b)$.

(c) Angenommen, es wäre $1 = 0$. Dann wäre für alle $a \in R$

$$a = 1 \cdot a = 0 \cdot a \overset{\text{(a)}}{=} 0.$$

Also wäre R dann der Nullring, im Widerspruch zur Voraussetzung. □

Wir hatten schon bemerkt, dass die Eigenschaften (R1), ..., (R5) aus Definition 7.1 über die Multiplikation in einem Ring besagen, dass sie alle Eigenschaften einer abelschen Gruppe bis auf evtl. die Existenz von Inversen erfüllt. Diese Existenz von multiplikativen Inversen, die also für manche Ringelemente gegeben sein wird und für manche nicht, müssen wir daher jetzt genauer untersuchen.

Definition 7.6 (Einheiten und Nullteiler)**.** Es sei $R \neq \{0\}$ ein Ring.

(a) Ein Element $a \in R$ heißt **invertierbar** bzw. eine **Einheit**, wenn es ein $a' \in R$ gibt mit $a' \cdot a = 1$. Die Menge aller Einheiten von R wird mit R^* bezeichnet.

(b) Nach Lemma 7.5 (a) ist 0 nie eine Einheit. Sind aber alle Elemente außer 0 Einheiten, also gilt $R^* = R \backslash \{0\}$, dann heißt R ein **Körper**.

(c) Ein Element $a \in R$ heißt **Nullteiler**, wenn es ein $b \in R$ mit $b \neq 0$ gibt, so dass $ab = 0$.

(d) Offensichtlich ist 0 immer ein Nullteiler. Der Ring R heißt ein **Integritätsring**, wenn kein Element außer 0 ein Nullteiler ist, also wenn für alle $a, b \in R$ aus der Gleichung $ab = 0$ bereits folgt, dass $a = 0$ oder $b = 0$.

Bemerkung 7.7.

(a) Mit exakt derselben Rechnung wie in Satz 1.7 (c) zeigt man, dass ein multiplikatives inverses Element a' zu einer Einheit $a \in R^*$ wie in Definition 7.6 (a) eindeutig ist. Wir bezeichnen es daher wie bei multiplikativ geschriebenen Gruppen mit a^{-1}. Da die Multiplikation in einem Ring kommutativ ist, können wir hier für eine Einheit $a \in R^*$ auch problemlos die Schreibweise $\frac{b}{a}$ für ba^{-1} bzw. $a^{-1}b$ verwenden (siehe Notation 1.9 (b)).

(b) Fassen wir die Definitionen 7.1 (mit Konvention 7.2) und 7.6 (b) zusammen, so sehen wir, dass eine Menge K mit zwei Verknüpfungen „+“ und „$\cdot$“ genau dann ein Körper ist, wenn gilt:

(K1) $(K, +)$ ist eine abelsche Gruppe (deren neutrales Element wir mit 0 bezeichnen);

(K2) $(K \backslash \{0\}, \cdot)$ ist ebenfalls eine abelsche Gruppe (deren neutrales Element wir mit 1 bezeichnen);

(K3) für alle $a, b, c \in K$ gilt die Distributivität $(a+b)c = ac + bc$.

Das folgende Lemma fasst die wichtigsten Eigenschaften von Einheiten und Nullteilern zusammen.

Lemma 7.8. *Es sei* $R \neq \{0\}$ *ein Ring.*

(a) *Die Menge* R^* *aller Einheiten von* R *bildet mit der Multiplikation eine Gruppe. Sie wird daher auch die* ***Einheitengruppe*** *von* R *genannt.*

(b) *Ist* $a \in R$ *eine Einheit, so ist* a *kein Nullteiler. Insbesondere ist also jeder Körper ein Integritätsring.*

(c) *(**Kürzungsregel**) Es seien $a,b,c \in R$ und c kein Nullteiler. Dann gilt*

$$ac = bc \;\Leftrightarrow\; a = b.$$

Insbesondere gilt diese Kürzungsregel in einem Integritätsring also für alle $c \neq 0$.

Beweis.

(a) Zunächst einmal ist die Multiplikation wirklich eine Verknüpfung auf R^*, denn ist a invertierbar mit Inversem a^{-1} und b invertierbar mit Inversem b^{-1}, so ist auch ab invertierbar mit Inversem $a^{-1}b^{-1}$. Weiterhin erfüllt $(R^*, \cdot)$ die Gruppenaxiome aus Definition 1.1 (a):

(G1) Dies folgt aus Teil (R2) der Definition 7.1 (a).

(G2) Das Element 1 ist natürlich immer eine Einheit und damit das neutrale Element in R^*.

(G3) Ist $a \in R^*$ und damit $a^{-1} \cdot a = 1$, so besagt dieselbe Gleichung, dass auch $a^{-1} \in R^*$ gilt.

(b) Es sei a eine Einheit, d. h. es existiert ein multiplikatives Inverses $a^{-1} \in R$. Ist nun $b \in R$ mit $ab = 0$, so ergibt sich durch Multiplikation mit a^{-1} sofort $b = 0$. Also kann a kein Nullteiler sein.

Ist R ein Körper, sind also alle Elemente außer 0 Einheiten, so kann damit keines dieser Elemente ein Nullteiler sein. Also ist R dann ein Integritätsring.

(c) Die Richtung „$\Leftarrow$“ ist offensichtlich. Für die andere Richtung „$\Rightarrow$“ gelte nun $ac = bc$. Dann ist aber $(a-b)c = 0$, und da c kein Nullteiler ist, folgt daraus sofort $a - b = 0$, also $a = b$. □

Beispiel 7.9.

(a) Offensichtlich ist $\mathbb{Z}^* = \{1,-1\}$, der Ring $\mathbb{Z}$ ist also kein Körper. Die 0 ist aber der einzige Nullteiler in $\mathbb{Z}$, d. h. $\mathbb{Z}$ ist ein Integritätsring.

(b) $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind Körper, da alle Elemente $a \neq 0$ ein multiplikatives Inverses $\frac{1}{a}$ besitzen. Wie in Lemma 7.8 (b) sind sie damit auch Integritätsringe.

(c) Im $\mathbb{Z}_6$ (wie in Beispiel 7.4 (b)) ist $\overline{2}$ ein Nullteiler, denn es ist $\overline{3} \neq \overline{0}$, aber $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$. Also ist $\mathbb{Z}_6$ kein Integritätsring, und damit nach Lemma 7.8 (b) auch kein Körper. In der Tat sieht man auch schnell direkt, dass es kein $\overline{n} \in \mathbb{Z}_6$ mit $\overline{2} \cdot \overline{n} = \overline{1}$ gibt, und $\overline{2}$ somit keine Einheit in $\mathbb{Z}_6$ ist.

Die Gleichung $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0} = \overline{2} \cdot \overline{0}$ zeigt auch, dass die Kürzungsregel für den Nullteiler $\overline{2}$ hier nicht gilt, denn es ist ja $\overline{3} \neq \overline{0}$.

08

Wie man an diesem Beispiel vielleicht schon erahnen kann, können wir sogar exakt angeben, für welche n der Ring $\mathbb{Z}_n$ ein Integritätsring bzw. ein Körper ist:

Satz 7.10. *Es sei $n \in \mathbb{N}_{>1}$. Dann sind die folgenden Aussagen äquivalent:*

(a) *$\mathbb{Z}_n$ ist ein Körper.*

(b) *$\mathbb{Z}_n$ ist ein Integritätsring.*

(c) *n ist eine Primzahl.*

Beweis.

(a) $\Rightarrow$ (b): Dies folgt sofort aus Lemma 7.8 (b).

(b) $\Rightarrow$ (c): Angenommen, n wäre keine Primzahl. Dann gäbe es eine Faktorisierung $n = p \cdot q$ für gewisse $1 < p,q < n$, und es wäre in $\mathbb{Z}_n$

$$\overline{p} \cdot \overline{q} = \overline{n} = \overline{0},$$

obwohl $\overline{p}$ und $\overline{q}$ nicht gleich $\overline{0}$ sind. Dies ist ein Widerspruch zur Annahme, dass $\mathbb{Z}_n$ ein Integritätsring ist.

(c) $\Rightarrow$(a): Es seien n eine Primzahl und $a \in \{1,\dots,n-1\}$; wir müssen zeigen, dass $\overline{a}$ eine Einheit in $\mathbb{Z}_n$ ist.

Nach Folgerung 5.12 (a) ist $\operatorname{ord}\overline{a}$ in $(\mathbb{Z}_n,+)$ ein Teiler von n. Da n eine Primzahl ist, ist also $\operatorname{ord}\overline{a}=1$ oder $\operatorname{ord}\overline{a}=n$. Wegen $\overline{a}\neq\overline{0}$ ist hierbei aber nur $\operatorname{ord}\overline{a}=n$ möglich, d. h. es ist $|\langle\overline{a}\rangle| \overset{5.11}{=} \operatorname{ord}\overline{a}=n$, und damit

$$\mathbb{Z}_n=\langle\overline{a}\rangle=\left\{k\cdot\overline{a}:k\in\mathbb{Z}\right\}=\left\{\overline{k}\cdot\overline{a}:k\in\mathbb{Z}\right\}.$$

Insbesondere ist also $\overline{1}\in\langle\overline{a}\rangle$, d. h. es gibt ein $k\in\mathbb{Z}$ mit $\overline{k}\cdot\overline{a}=\overline{1}$. □

Notation 7.11. Ist p eine Primzahl, so ist für den Körper $\mathbb{Z}_p$ in der Literatur auch die Bezeichnung $\mathbb{F}_p$ üblich – die Bezeichnung kommt vom englischen Wort „field", das in der Mathematik „Körper" bedeutet. Wir werden in diesem Skript jedoch weiterhin die Bezeichnung $\mathbb{Z}_p$ verwenden.

Beispiel 7.12. Im Körper $\mathbb{Z}_7$ ist $\overline{5}$ das multiplikative Inverse zu $\overline{3}$, also $\overline{3}^{-1}=\overline{5}$, denn $\overline{5}\cdot\overline{3}=\overline{15}=\overline{1}$. Man kann also leicht nachprüfen, dass ein gegebenes Element von $\mathbb{Z}_n$ das multiplikative Inverse eines anderen ist. Beachte aber, dass der Beweis von Satz 7.10 *nicht konstruktiv* ist, d. h. er sichert nur die Existenz von multiplikativ inversen Elementen im Körper $\mathbb{Z}_n$ für eine Primzahl n, sagt aber nicht, wie man dieses Inverse konkret bestimmen kann, wenn man nicht alle möglichen Elemente von $\mathbb{Z}_n$ durchprobieren möchte. Wir werden in Folgerung 10.32 noch ein explizites Verfahren kennenlernen, mit dem man Inverse in $\mathbb{Z}_n$ ohne Ausprobieren berechnen kann.

Bemerkung 7.13. Ist p eine Primzahl und $\mathbb{Z}_p$ damit nach Satz 7.10 ein Körper, so ist die Einheitengruppe dieses Körpers natürlich $(\mathbb{Z}_p^*,\cdot)=(\mathbb{Z}_p\backslash\{0\},\cdot)$. Man kann nun zeigen, dass diese Gruppe zyklisch ist – und damit, da sie ja $p-1$ Elemente besitzt, nach Satz 6.21 (a) isomorph zu $(\mathbb{Z}_{p-1},+)$ sein muss. Der Beweis dieser Aussage ist mit unseren momentanen Mitteln noch nicht möglich; er wird typischerweise in der Vorlesung „Elementare Zahlentheorie" behandelt.

Es gibt also ein $a\in\mathbb{Z}$, so dass

$$\mathbb{Z}_p^*=\langle\overline{a}\rangle=\{\overline{a}^k:k\in\mathbb{Z}\}=\{\overline{a}^k:k=0,\dots,p-2\},$$

und damit dann zu jedem $\overline{b}\in\mathbb{Z}_p^*$ ein eindeutiges $k\in\{0,\dots,p-2\}$ mit $\overline{b}=\overline{a}^k$. Die folgende Tabelle zeigt ein konkretes Beispiel: In $\mathbb{Z}_7$ können wir z. B. $\overline{a}=\overline{3}$ wählen und erhalten dann jedes Element von $\mathbb{Z}_7\backslash\{0\}$ auf eindeutige Art als ein $\overline{3}^k$ für ein $k\in\{0,\dots,5\}$.

k	0	1	2	3	4	5
$\overline{3}^k$	$\overline{1}$	$\overline{3}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{5}$

Im Gegensatz zur Inversenbildung in $\mathbb{Z}_p$ (siehe Beispiel 7.12) gibt es allerdings sowohl zur Bestimmung eines solchen a als auch zur anschließenden Berechnung von k aus $\overline{b}=\overline{a}^k$ in der Regel kein anderes Verfahren als das Ausprobieren aller Möglichkeiten. Wir hatten in Beispiel 0.2 der Einleitung schon gesehen, wie sich diese Tatsache für kryptographische Zwecke ausnutzen lässt.

Aufgabe 7.14.

(a) Zeige, dass $\overline{n-1}$ in $\mathbb{Z}_n$ für alle $n\in\mathbb{N}_{\geq 2}$ eine Einheit ist.

(b) Berechne $\overline{5^{12345}}$ in $\mathbb{Z}_7$.

(c) Es sei $a\in\mathbb{Z}_{11}$. Bestimme (in Abhängigkeit von a) alle $x,y\in\mathbb{Z}_{11}$, die das Gleichungssystem

$$\begin{aligned} &\overline{5}x+\overline{6}y=\overline{4}\\ \text{und}\quad &\overline{8}x+\overline{9}y=a \end{aligned}$$

in $\mathbb{Z}_{11}$ erfüllen.

Aufgabe 7.15. Es seien R und S zwei Ringe. Zeige, dass $(R\times S)^*\cong R^*\times S^*$.

Aufgabe 7.16. Zeige, dass in einem endlichen Ring $R \neq \{0\}$ jedes Element eine Einheit oder ein Nullteiler ist.

Insbesondere ist jeder endliche Integritätsring $R \neq \{0\}$ also bereits ein Körper, so dass zusammen mit Lemma 7.8 (b) für endliche Ringe (ungleich dem Nullring) die Begriffe „Integritätsring“ und „Körper“ übereinstimmen – was wir für den speziellen Fall der Ringe $\mathbb{Z}_n$ ja auch schon in Satz 7.10 gesehen hatten.

Aufgabe 7.17 (**Satz von Wilson**)**.** Zeige, dass $(p-1)! := \overline{1} \cdot \dots \cdot \overline{p-1} = \overline{-1}$ in $\mathbb{Z}_p$ für jede Primzahl $p > 2$.

Aufgabe 7.18. Es sei K ein Körper. Zeige, dass $(K,+)$ als Gruppe dann niemals isomorph zu $(K \backslash \{0\}, \cdot)$ sein kann.

Aufgabe 7.19. Es sei R ein Ring mit genau 5 Einheiten. Man zeige:

(a) In R gilt $-1 = 1$.

(b) Für jedes $a \in R^*$ gilt $(1+a+a^2)^3 = a^3$.

(c) Für jedes $a \in R^*$ gilt $1+a+a^2 = a$.

(d) Es gibt R gar nicht.

Hinweis: R^* ist bekanntlich eine Gruppe.

Nachdem wir nun Ringe (und Körper) eingeführt haben, wollen wir für diese Strukturen kurz die gleichen Konstruktionen einführen, wie wir sie für Gruppen in den vorangegangenen Kapiteln betrachtet haben: zuerst die Unterstrukturen (also Teilmengen von Ringen, die selbst wieder Ringe sind), dann die Morphismen (als Abbildungen, die die Ringstruktur erhalten), und schließlich im nächsten Kapitel die Faktorstrukturen (also das „Herausteilen“ von Äquivalenzrelationen). Alle diese Konstruktionen verlaufen mehr oder weniger parallel zu denen von Gruppen und sollten euch daher auch helfen, die generelle Vorgehensweise dabei besser zu verstehen.

Beginnen wir also mit den Unterstrukturen. Die Definition eines Unterrings verläuft ganz analog zu der einer Untergruppe in Definition 3.1:

Definition 7.20 (Unterringe)**.** Eine Teilmenge S eines Ringes R heißt **Unterring** von R, wenn S „mit der gleichen 0 und 1 wie in R und denselben Verknüpfungen selbst wieder ein Ring ist“, d. h. wenn gilt:

(a) $1 \in S$;

(b) für alle $a,b \in S$ ist $a+b \in S$ und $ab \in S$ (d. h. die Verknüpfungen „$+$“ und „$\cdot$“ in R lassen sich auf Verknüpfungen in S einschränken);

(c) $(S,+,\cdot)$ ist ein Ring.

Man verwendet hierfür genau wie bei Untergruppen oft die Schreibweise $S \leq R$, muss dabei aber natürlich darauf achten, dass aus dem Zusammenhang klar wird, ob Untergruppen oder Unterringe gemeint sind.

Bemerkung 7.21. Ein Unterring S eines Ringes R ist nach Definition natürlich insbesondere auch eine additive Untergruppe von R. Nach dem Untergruppenkriterium (U2) aus Satz 3.3 muss S dann also automatisch das additive neutrale Element $0 \in R$ enthalten. Wir mussten in Definition 7.20 also nicht explizit auch $0 \in S$ fordern, da dies schon aus den anderen Eigenschaften folgt.

Für das Element $1 \in S$ gilt dies jedoch nicht: Hätten wir in Definition 7.20 nicht explizit $1 \in S$ gefordert, so wäre z. B. der Nullring ein Unterring von $\mathbb{Z}$. Der Nullring besäße dann zwar auch ein Einselement (nämlich 0), dies wäre aber nicht das gleiche wie im Gesamtring $\mathbb{Z}$. Die Forderung (a) in Definition 7.20 schließt solche merkwürdigen Fälle aus.

Beispiel 7.22.

(a) Natürlich ist $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(b) Es sei S ein Unterring von $\mathbb{Z}$. Dann muss S zunächst auch eine additive Untergruppe von $\mathbb{Z}$, also nach Satz 3.18 von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}$ sein. Weiterhin muss S nach Definition 7.20 (a) aber auch das Element 1 enthalten, was nur für $n = 1$ (und somit $S = \mathbb{Z}$) der Fall ist. Also ist der triviale Unterring $\mathbb{Z}$ der einzige Unterring von $\mathbb{Z}$.

Analog zum Untergruppenkriterium aus Satz 3.3 gibt es auch ein Unterringkriterium, an dem man sieht, dass in Definition 7.20 (c) die Überprüfung der meisten Ringaxiome überflüssig ist:

Lemma 7.23 (**Unterringkriterium**). *Eine Teilmenge S eines Ringes R ist genau dann ein Unterring, wenn gilt:*

(1) $1 \in S$;

(2) *für alle $a, b \in S$ ist $a + b \in S$ und $ab \in S$;*

(3) *für alle $a \in S$ ist $-a \in S$.*

Beweis.

„$\Rightarrow$“: Ist S ein Unterring von R, so gelten nach Definition natürlich (1) und (2). Außerdem ist S dann eine additive Untergruppe, also gilt (3) nach dem Untergruppenkriterium (U3).

„$\Leftarrow$“: Erfüllt umgekehrt S die Bedingungen (1), (2) und (3) des Unterringkriteriums, so gelten natürlich auch die Eigenschaften (a) und (b) der Definition 7.20. Außerdem erfüllt S bezüglich der Addition alle Bedingungen des Untergruppenkriteriums (beachte, dass $1 \in S$, also $S \neq \emptyset$, nach Bemerkung 3.4 (b) für (U2) ausreicht) und ist somit eine Untergruppe von R, erfüllt also (R1). Weiterhin gilt (R4) für S nach (1). Die anderen drei Bedingungen (R2), (R3) und (R5) gelten natürlich in S, weil sie auch in R gelten. Damit ist $(S, +, \cdot)$ ein Ring, nach Definition 7.20 also auch ein Unterring von $(R, +, \cdot)$. □

Ein wichtiges Beispiel von Unterringen, das uns im Folgenden noch häufiger begegnen wird, ist durch die folgende Konstruktion gegeben.

Konstruktion 7.24 (Adjunktion einer Quadratwurzel zu $\mathbb{Z}$). Zu einer fest gegebenen Zahl $x \in \mathbb{C}$ mit $x^2 \in \mathbb{Z}$ (also z. B. $x = \sqrt{2}$ oder $x = \mathrm{i}$) setzen wir

$$\mathbb{Z}[x] := \{a + bx : a, b \in \mathbb{Z}\} \quad \subset \mathbb{C}$$

(gesprochen: „$\mathbb{Z}$ *adjungiert* x“). Nach Lemma 7.23 ist $\mathbb{Z}[x]$ dann ein Unterring von $\mathbb{C}$, denn es gilt:

(1) $1 = 1 + 0x \in \mathbb{Z}[x]$.

(2) Für zwei Elemente $a + bx, c + dx \in \mathbb{Z}[x]$ (mit $a, b, c, d \in \mathbb{Z}$) gilt

$$(a + bx) + (c + dx) = (a + c) + (b + d)x \in \mathbb{Z}[x]$$

$$\text{und} \qquad (a + bx) \cdot (c + dx) = \underbrace{(ac + bdx^2)}_{\in \mathbb{Z} \text{ wegen } x^2 \in \mathbb{Z}} + (ad + bc)x \in \mathbb{Z}[x].$$

(3) Für alle $a + bx \in \mathbb{Z}[x]$ ist auch $-(a + bx) = (-a) + (-b)x \in \mathbb{Z}[x]$.

Aufgabe 7.25.

(a) Bestimme alle Einheiten von $\mathbb{Z}[\mathrm{i}]$ und $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$.

(Hinweis: Für eine komplexe Zahl $z \in \mathbb{Z}[x]$ betrachte man das Betragsquadrat $|z|^2$. Aus den Grundlagen der Mathematik dürft ihr verwenden, dass $|zw|^2 = |z|^2\,|w|^2$ für alle $z, w \in \mathbb{C}$ gilt.)

(b) Zeige, dass der Ring $\mathbb{Z}[\sqrt{5}]$ unendlich viele Einheiten besitzt.

Nach den Unterstrukturen wollen wir – wie bei Gruppen – als Nächstes die Morphismen betrachten. Wie erwartet sollen dies einfach die Abbildungen zwischen Ringen sein, die alle Strukturen (also die 0, die 1, die Addition und die Multiplikation) erhalten. Wir definieren die Konzepte von Kern und Bild eines solchen Morphismus sowie von Isomorphismen gleich mit – die Definitionen sind hier völlig analog zu denen von Gruppen.

Definition 7.26 (Morphismen von Ringen)**.**

(a) Eine Abbildung $f\colon R \to S$ zwischen zwei Ringen heißt ein **Morphismus** (oder **Homomorphismus** oder **Ringhomomorphismus**), wenn $f(1) = 1$ ist und für alle $a,b \in R$

$$f(a+b) = f(a) + f(b) \quad \text{und} \quad f(a \cdot b) = f(a) \cdot f(b)$$

gilt. Sind R und S Körper, so heißt ein solches f auch **Körperhomomorphismus**.

(b) Ein bijektiver Morphismus heißt **Isomorphismus** (bzw. auch **Ringisomorphismus** oder **Körperisomorphismus**). Zwei Ringe (bzw. Körper) heißen **isomorph**, wenn es einen Isomorphismus zwischen ihnen gibt.

(c) Ist $f\colon R \to S$ ein Ringhomomorphismus, so heißt

$$\operatorname{Im} f = f(R) = \{f(a) : a \in R\} \subset S \quad \text{das } \textbf{Bild} \text{ von } f$$
$$\text{und} \quad \operatorname{Ker} f = f^{-1}(\{0\}) = \{a \in R : f(a) = 0\} \subset R \quad \text{der } \textbf{Kern} \text{ von } f$$

(die Definitionen sind also exakt dieselben wie bei Gruppen, wenn man f als Gruppenhomomorphismus bezüglich der Addition auffasst).

Bemerkung 7.27. Jeder Ringhomomorphismus ist nach Definition auch ein Gruppenhomomorphismus bezüglich der Addition. Aus Lemma 4.4 (a) folgt also sofort, dass ein Ringhomomorphismus $f\colon R \to S$ stets $f(0) = 0$ erfüllen muss.

Im Gegensatz dazu gibt es bei der Bedingung $f(1) = 1$ wie schon bei der Definition von Ringen und Unterringen in der Literatur zwei Varianten: In manchen Büchern wird diese Bedingung unserer Definition 7.26 (a) weggelassen. Die Nullabbildung $f\colon R \to S$, $a \mapsto 0$ wäre dann ein Morphismus; nach unserer Definition ist sie keiner.

Beispiel 7.28. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $f(n) = (n,n)$ ist offensichtlich ein Ringhomomorphismus. In der Tat ist dies sogar der einzige Ringhomomorphismus von $\mathbb{Z}$ nach $\mathbb{Z} \times \mathbb{Z}$: Nach Beispiel 4.8 sind die einzigen *Gruppenhomomorphismen* bezüglich der Addition die Abbildungen $f(n) = (an, bn)$ für gewisse $a,b \in \mathbb{Z}$ – und für einen *Ringhomomorphismus* muss dann wegen $f(1) = (1,1)$ natürlich zusätzlich $a = b = 1$ gelten.

Bemerkung 7.29 (Eigenschaften von Ringhomomorphismen)**.** Genau wie im Fall von Gruppen zeigt man die folgenden beiden einfachen Eigenschaften von Ringhomomorphismen:

(a) Ist $f\colon R \to S$ ein Ringisomorphismus, so ist auch die Umkehrabbildung $f^{-1}\colon S \to R$ ein Ringisomorphismus (vgl. Lemma 4.4 (c)). Isomorphismen spielen in der Theorie der Ringe dieselbe anschauliche Bedeutung wie bei den Gruppen: Ringe, zwischen denen ein Isomorphismus existiert, können als „gleichwertig“ angesehen und miteinander identifiziert werden.

(b) Sind $f\colon R \to S$ und $g\colon S \to T$ Ringhomomorphismen, so ist auch die Verkettung $g \circ f\colon R \to T$ ein Ringhomomorphismus (vgl. Lemma 4.4 (d)).

Aufgabe 7.30. Beweise explizit die Aussagen von Bemerkung 7.29.

Bemerkung 7.31 (Bilder und Kerne von Ringhomomorphismen)**.** Für einen Gruppenhomomorphismus $f\colon G \to H$ hatten wir in Definition 4.17 gesehen, dass $\operatorname{Ker} f$ und $\operatorname{Im} f$ Untergruppen von G bzw. H sind. Für einen Ringhomomorphismus $f\colon R \to S$ ist die Situation etwas anders:

(a) Das Bild $\operatorname{Im} f$ ist ein Unterring von S, wie wir einfach anhand der Unterringkriterien aus Lemma 7.23 nachprüfen können:

(1) Nach Definition 7.26 (a) ist $f(1) = 1$ und damit $1 \in \operatorname{Im} f$.

(2) Für alle $a,b \in \operatorname{Im} f$, also $a = f(u)$ und $b = f(v)$ für gewisse $u,v \in R$, gilt sowohl $a+b = f(u)+f(v) = f(u+v) \in \operatorname{Im} f$ als auch $ab = f(u)f(v) = f(uv) \in \operatorname{Im} f$.

(3) Für $a \in \operatorname{Im} f$, also $a = f(u)$ für ein $u \in R$, gilt $-a = -f(u) = f(-u) \in \operatorname{Im} f$.

(b) Der Kern $\operatorname{Ker} f$ ist hingegen (falls S nicht der Nullring ist) *nie* ein Unterring von R, denn es gilt ja $f(1) = 1$ nach Definition 7.26 (a) und damit $1 \notin \operatorname{Ker} f$. In der Tat bildet der Kern eines Ringhomomorphismus eine andere Art von Unterstruktur – ein sogenanntes *Ideal*. Diesen Begriff werden wir im nächsten Kapitel kennenlernen (siehe Definition 8.1 und Lemma 8.4).

Aufgabe 7.32. Man zeige:

(a) Ist $f\colon K \to R$ ein Ringhomomorphismus von einem Körper K in einen Ring $R \neq \{0\}$, so ist f injektiv.

(b) Von den drei Ringen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ sind keine zwei isomorph zueinander.

Aufgabe 7.33. Bestimme alle Ringhomomorphismen von $\mathbb{Z}_{12}$ nach $\mathbb{Z}_8$ und von $\mathbb{Z}_{12}$ nach $\mathbb{Z}_6$.