Übung 6 - Lösung

Ausgabedatum: 20. November 2023
Abgabedatum: 26. November 2023

Hausaufgabe 6.1 (Normalteiler und Faktorgruppe) 5 Punkte

(i) Es sei $m \in \mathbb{N}$. Zeigen Sie, dass die Menge $\mathbb{Z} / m\mathbb{Z}$ mit $\tilde{\cdot}$ definiert durch $[a] \,\tilde{\cdot}\, [b] := [a \cdot b]$ ein kommutatives Monoid mit neutralem Element $[1]$ ergibt, welches isomorph zu dem kommutativen Monoid $(\mathbb{Z}_m, \cdot_m)$ aus Beispiel 7.16 ist.

Beachte: Mit der Menge $\mathbb{Z} / m\mathbb{Z}$ ist die Faktormenge des Normalteilers $(m\mathbb{Z}, +)$ in der Gruppe $(\mathbb{Z}, +)$ gemeint. Diese Faktormenge stimmt mit den Restklassen in $\mathbb{Z} / \overset{m}{\equiv} = \{\{a + m\mathbb{Z}\} \mid a \in \mathbb{Z}\}$ überein. Auf dieser Menge soll jetzt statt der Faktorverknüpfung $\tilde{+}$ (siehe Beispiel 8.15 im Skript) das $\tilde{\cdot}$ untersucht werden.

(ii) Bestimmen Sie für $(\mathbb{R}, +)$ und den Normalteiler $(\mathbb{Z}, +)$ die Elemente von $(\mathbb{R} / \mathbb{Z}, \tilde{+})$ mit endlicher Ordnung.

(iii) Es sei $(G, \star)$ eine Gruppe und $(N, \star)$ einer ihrer Normalteiler. Zeigen Sie, dass G / N genau dann abelsch ist, wenn N die Kommutatorgruppe $K(G) := \langle\{a \star b \star a' \star b' \mid a, b \in G\}\rangle$ enthält. (Diese Aussage erweitert Satz 8.13 (iii) des Skripts).

(iv) Es sei $(G, \star)$ eine Gruppe. Zeigen Sie die Aussage von Bemerkung 8.16 im Skript, also dass die Normalteiler von $(G, \star)$ genau die Kerne geeigneter Homomorphismen sind.

Lösung.

(i) Man kann direkt an der Definition von $\tilde{\cdot}$ ablesen, dass $\mathbb{Z} / m\mathbb{Z}$ der Bildbereich ist, denn die Bilder sind ja genau Klassen aus der Faktormenge. Die Abbildung ist außerdem wohldefiniert (repräsentantenunabhängig), denn für Repräsentanten $a, \tilde{a}$ und $b, \bar{b}$ aus $\mathbb{Z}$ mit $[a] = [\bar{a}]$ und $[b] = [\bar{b}]$ existieren $z_a, z_b \in \mathbb{Z}$, so dass $\bar{a} = a + z_a \cdot m$ und $\bar{b} = b + z_b \cdot m$, also ist

$$[\bar{a}] \,\tilde{\cdot}\, [\bar{b}] = [\bar{a} \cdot \bar{b}] = \bar{a} \cdot \bar{b} + m\mathbb{Z} = (a + z_a \cdot m) \cdot (b + z_b \cdot m) + m\mathbb{Z} = a \cdot b + m\mathbb{Z} = [a \cdot b] = [a] \,\tilde{\cdot}\, [b].$$

Es handelt sich also um eine innere **Verknüpfung** auf $\mathbb{Z}/m\mathbb{Z}$.

Die **Assoziativität** von $\tilde{\cdot}$ wird direkt von der Assoziativität von $\cdot$ in den ganzen Zahlen vererbt, denn

$$([a] \tilde{\cdot} [b]) \tilde{\cdot} [c] = [a \cdot b] \tilde{\cdot} [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \tilde{\cdot} [b \cdot c] = [a] \tilde{\cdot} ([b] \tilde{\cdot} [c]).$$

Analog wird die **Kommutativität** vererbt, denn

$$[a] \tilde{\cdot} [b] = [a \cdot b] = [b \cdot a] = [b] \tilde{\cdot} [a].$$

(0.5 Punkte)

Dass das **neutrale Element** aus der Klasse $[1]$ besteht, wird ebenfalls vererbt, denn es ist

$$[1] \tilde{\cdot} [a] = [1 \cdot a] = [a] = [a \cdot 1] = [a] \tilde{\cdot} [1].$$

Der kanonische Isomorphismus $f\colon (\mathbb{Z}_m, \cdot_m) \to (\mathbb{Z}/m\mathbb{Z}, \tilde{\cdot})$ ist die Abbildung

$$\{0, \ldots, m-1\} \ni m \mapsto [m] \in \mathbb{Z}/m\mathbb{Z}.$$

Die Bijektivität der Abbildung folgt sofort daraus, dass $m \in \{0, \ldots, m-1\}$. Die Homomorphismuseigenschaft zeigt die Gleichungskette

$$f(a \cdot_m b) = f(a \cdot b \mod m) = [a \cdot b \mod m] = [a \cdot b] = f(a) \tilde{\cdot} f(b) \quad \forall a, b \in \{0, \ldots, m-1\}.$$

(0.5 Punkte)

(ii) Die Elemente von $\mathbb{R}/\mathbb{Z}$ besteht aus den Klassen $[a] = a + \mathbb{Z}$ für alle $a \in \mathbb{R}$, also

$$\mathbb{R}/\mathbb{Z} = \{a + \mathbb{Z} \mid a \in \mathbb{R}\} = \{a + \mathbb{Z} \mid a \in [0, 1)\}.$$

Ein Element $[a] \in \mathbb{R}/\mathbb{Z}$ besitzt genau dann endliche Ordnung bezüglich $\tilde{+}$, wenn ein $n \in \mathbb{N}$ existiert, so dass

$$\underbrace{\mathbb{Z} = [0]}_{\text{neutr. Elem. in } \mathbb{R}/\mathbb{Z}} = n[a] = \underbrace{[a] \tilde{+} \cdots \tilde{+} [a]}_{\text{n-mal}} = [na] = na + \mathbb{Z},$$

was genau dann der Fall ist, wenn $na \in \mathbb{Z}$, also wenn ein $m \in \mathbb{Z}$ existiert, so dass

$$na = m$$

also genau dann, wenn $a \in \mathbb{Q}$, also wenn die Klasse $[a]$ einen Repräsentanten aus $\mathbb{Q}$ besitzt (womit dann gleich alle Repräsentanten aus $\mathbb{Q}$ sind). Die Menge von Elementen aus $\mathbb{R}/\mathbb{Z}$ mit endlicher Ordnung ist also genau $\{[a] \mid a \in \mathbb{Q}\}$. (1 Punkt) (*iii*) „$\Rightarrow$" Ist $G\,/\,N$ abelsch, dann gilt für alle $a, b \in G$, dass

$$[a \star b \star a' \star b'] = [a] \mathbin{\tilde\star} [b] \mathbin{\tilde\star} [a'] \mathbin{\tilde\star} [b'] = [a] \mathbin{\tilde\star} [a'] \mathbin{\tilde\star} [b] \mathbin{\tilde\star} [b'] = [e] \mathbin{\tilde\star} [e] = [e] = N.$$

Insbesondere ist damit jeder Kommutator in N. Da N mit $\star$ eine Untergruppe von $(G, \star)$ ist, welche die Mengen der Kommutatoren beinhaltet, ist die von den Kommutatoren erzeugte Gruppe (die bzgl. der Mengeninklusion kleinste Gruppe) eine Teilmenge von N. (1 Punkt)

„$\Leftarrow$" Liegt die Kommutatorengruppe in N, dann ist wegen des Translationsgruppenkriteriums (Lemma 7.18) (konkret der Surjektivität) für beliebige $a, b \in G$, deren Inverse den Kommutator $b' \star a' \star b \star a \in N$ bilden, schon

$$b' \star a' \star b \star a \star N = N$$

und somit gilt

$$[a] \mathbin{\tilde\star} [b] = [a \star b] = a \star b \star N = a \star b \star b' \star a' \star b \star a \star N = b \star a \star N = [b \star a] = [b] \mathbin{\tilde\star} [a].$$

(1 Punkt)

(*iv*) Es sei $(N, \star)$ ein Normalteiler von der Gruppe $(G, \star)$, deren neutrales Element wir e_G nennen werden. Wir suchen eine Gruppe $(\tilde G, \square)$ (mit einem neutralen Element $e_{\tilde G}$) und einen Homomorphismus $f\colon (G, \star) \to (\tilde G, \square)$ mit $\mathrm{Kern}(f) = N$. Naheliegend ist, hier als $(\tilde G, \square)$ gerade $(G\,/\,N, \tilde\star)$ zu wählen, denn hier ist das dazugehörige neutrale Element gerade $e_{\tilde G} = [e_G] = N$ und die kanonische Surjektion

$$a \to [a] = a \star N$$

ist gerade ein surjektiver Gruppenhomomorphismus mit dem entsprechenden Kern, siehe Satz 8.13. (1 Punkt)

Hausaufgabe 6.2 (Homomorphiesatz für Gruppen) 2 Punkte

Es seien $(G_1, \star)$ und $(G_2, \square)$ zwei Gruppen und G_1 endlich. Zeigen Sie:

(*i*) Ist auch G_2 endlich und $\#G_1$ und $\#G_2$ teilerfremd, dann existiert zwischen $(G_1, \star)$ und $(G_2, \square)$ nur der triviale Gruppenhomomorphismus.

Hinweis: Nutzen Sie den Satz von Lagrange (Satz 7.43 im Skript).

(*ii*) Ist $\#G_1$ eine Primzahl, dann ist jeder Gruppenhomomorphismus von $(G_1, \star)$ nach $(G_2, \square)$ trivial oder injektiv.

Lösung.

(i) Es sei $f\colon (G_1, \star) \to (G_2, \square)$ ein Gruppenhomomorphismus. Dann ist nach den Eigenschaften von Bild und Kern von Gruppenhomomorphismen in Lemma 8.7 des Skripts

$$\begin{aligned} \operatorname{Bild}(f) &= f(G_1) \quad \text{mit } \square \text{ eine Untergruppe von } (G_2, \square) \\ \operatorname{Kern}(f) &= f^{-1}(e_2) \text{ mit } \star \text{ eine Untergruppe von } (G_1, \star) \end{aligned}$$

Aus dem Satz 7.43 von Lagrange folgt die Teilereigenschaft $\# \operatorname{Bild}(f) \mid \# G_2$. (0.5 Punkte)

Der Homomorphiesatz für Gruppen (Satz 8.17 des Skripts) besagt nun weiter, dass $G_1 / \operatorname{Kern}(f) \cong \operatorname{Bild}(f)$ ist. Alle Nebenklassen bzgl. $\operatorname{Kern}(f)$ sind aber zu $\operatorname{Kern}(f)$ gleichmächtig, es ist also

$$\# G_1 = \underbrace{\#(G_1 / \operatorname{Kern}(f))}_{\text{Anzahl der Nebenklassen}} \cdot \# \operatorname{Kern}(f) = \# \operatorname{Bild}(f) \cdot \# \operatorname{Kern}(f) \tag{0.1}$$

Das liefert die Teilereigenschaft $\# \operatorname{Bild}(f) \mid \# G_1$. (0.5 Punkte)

Zusammen haben wir also $\# \operatorname{Bild}(f) \mid \# G_1$ und $\# \operatorname{Bild}(f) \mid \# G_2$ sowie die Teilerfreiheit von $\# G_1$ und $\# G_2$, also muss $\# \operatorname{Bild}(f) = 1$ sein. Da f nach Annahme ein Gruppenhomomorphismus ist, muss $f(e_1) = e_2$ gelten, also $e_2 \in \operatorname{Bild}(f)$ und damit $\{e_2\} = \operatorname{Bild}(f)$, f muss also der triviale Gruppenhomomorphismus sein. (0.5 Punkte)

(ii) Wie zuvor erhalten wir (0.1) und damit die Teilereigenschaft $\# \operatorname{Bild}(f) \mid \# G_1$, und da G_1 prim ist, muss $\# \operatorname{Bild}(f) = 1$ sein und damit $\operatorname{Bild}(f) = \{e_2\}$, also f trivial, oder es muss $\# \operatorname{Bild}(f) = \# G_1$ sein, und f damit injektiv. (0.5 Punkte)

Hausaufgabe 6.3 (Ringe und Unterringe) 6 Punkte

(i) Es sei X eine nichtleere Menge. Entscheiden Sie, ob die folgenden Beispiele Ringe sind, und falls ja, ob der jeweilige Ring ein Einselement besitzt oder kommutativ, nullteilerfrei bzw. ein Integritätsring ist.

(a) $(\mathcal{P}(X), \triangle, \cup)$
(b) $(\mathcal{P}(X), \triangle, \cap)$
(c) $(\mathbb{Z}, +, \max(\cdot, \cdot))$
(d) $(\mathbb{R}^X, +, \cdot)$

(ii) Es sei $(G, +)$ eine abelsche Gruppe. Zeigen Sie, dass der Endomorphismenring $(\operatorname{End}(G), +, \circ)$ (Beispiel 9.2 des Skripts) tatsächlich ein Ring ist.

(iii) Es seien $(R, +, \cdot)$ ein Ring und $((R_i, +, \cdot))_{i \in I}$ eine nichtleere Familie von Unterringen. Zeigen Sie, dass $\bigcap_{i \in I} R_i$ mit $+$ und $\cdot$ ein Unterring von $(R, +, \cdot)$ ist.

(iv) Es sei $(R, +, \cdot)$ ein Integritätsring. Zeigen Sie, dass dann $\operatorname{char}(R)$ eine Primzahl oder 0 ist.

Lösung.

(i) (a) Wir wissen aus Hausaufgabe 4.1, dass $(\mathcal{P}(X), \triangle)$ eine abelsche Gruppe mit neutralem Element $\emptyset$ und $(\mathcal{P}(X), \cup)$ ein kommutatives Monoid mit neutralem Element $\emptyset$ ist. Auf Grund der Kommutativität müssen wir nur eines der beiden Distributivgesetze prüfen. Die Distributivgesetze gelten allerdings nicht. In unserem konkreten Fall schreibt sich für alle $a, b, c \in \mathcal{P}(X)$ das Distributivgesetz

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{9.1a}$$

als

$$a \cup (b \triangle c) = (a \cup b) \triangle (a \cup c).$$

Während a immer Teilmenge des linken Ausdrucks ist, ist a nie Teilmenge des rechten Ausdrucks, ein einfaches Gegenbeispiel liefert also $a = X, b = c = \emptyset$, denn dann ist

$$a \cup (b \triangle c) = X \cup (\emptyset \triangle \emptyset) = X \neq \emptyset = (X \cup \emptyset) \triangle (X \cup \emptyset) = (a \cup b) \triangle (a \cup c).$$

Es handelt sich also um **keinen Ring**. (0.5 Punkte)

(b) Wir wissen aus Hausaufgabe 4.1, dass $(\mathcal{P}(X), \triangle)$ eine abelsche Gruppe mit neutralem Element $\emptyset$ und $(\mathcal{P}(X), \cap)$ ein kommutatives Monoid mit neutralem Element X ist. Auf Grund der Kommutativität müssen wir nur eines der beiden Distributivgesetze prüfen. In diesem Fall erhalten wir für alle $a, b, c \in \mathcal{P}(X)$ das Distributivgesetz

$$\begin{aligned} a \cap (b \triangle c) &= a \cap (b \setminus c \cup c \setminus b) \\ &= \big(a \cap (b \setminus c)\big) \cup \big(a \cap (c \setminus b)\big) \\ &= \big((a \cap b) \setminus c\big) \cup \big((a \cap c) \setminus b\big) \\ &= \big((a \cap b) \setminus (a \cap c)\big) \cup \big((a \cap c) \setminus (a \cap b)\big) \\ &= (a \cap b) \triangle (a \cap c). \end{aligned}$$

Hier liegt als ein **kommutativer Ring** mit **Eins** vor (nämlich das Element X). Tatsächlich ist $A \cap B = \emptyset$ genau dann, wenn die Mengen in dem Komplement der jeweils anderen liegen, die Mengen also disjunkt sind. I. A. ist dieser Ring also **nicht nullteilerfrei** und damit **kein Integritätsring**. Nullteilerfrei ist ist der Ring genau dann, wenn X nur kein, oder nur ein Element enthält. Ist X leer, dann handelt es sich um den **Nullring** (dieser Fall war auch ausgeschlossen in der Voraussetzung). Besteht X aus genau einem Element, dann handelt es sich sogar um einen **Integritätsring** (1 Punkt)

(c) Es ist $(\mathbb{Z}, +)$ eine schon bekannte abelsche Gruppe (Beispiel 7.20 des Skripts) und $\big(\mathbb{Z}, \max(\cdot, \cdot)\big)$ eine kommutative Halbgruppe ohne neutrales Element. Die Assoziativität des Maximums auf $\mathbb{Z}$ sieht man daran, dass für drei Elemente unabhängig von der Verknüpfungsreihenfolge immer ein Größtes ausgegeben wird. Nun ist für $a = 1$ und $b = c = 0$ aber

$$\max(a, b + c) = \max(1, 0) = 1 \neq 2 = \max(1, 0) + \max(1, 0) = \max(a, b) + \max(a, c),$$

die Distributivgesetze gelten also nicht und somit liegt **kein Ring** vor. (0.5 Punkte)

(d) Hierbei handelt es sich um einen **kommutativen Ring mit Eins**, nämlich der konstanten Einsfunktion, wobei alle benötigten Eigenschaften von dem Ring $(\mathbb{R}, +, \cdot)$ übertragen werden. Da das neutrale Element bzgl. + die konstante Nullfunktion ist, handelt es sich nicht um den Nullring (denn die Eins und die Null sind verschieden). Sind $f, g \in \mathbb{R}^X$ mit $f \cdot g = 0$ dann gilt $f(x) = 0 \lor g(x) = 0$ für alle $x \in X$. Damit ist der Ring genau dann nullteilerfrei, wenn X ein einziges Element beinhaltet, denn dann muss eine der beiden Funktionen die konstante Nullfunktion sein. Dann handelt es sich auch um einen **Integritätsring**. Sobald X zwei verschiedene Elemente x_1, x_2 enthält, kann man allerdings die Funktionen

$$f(x) \coloneqq \begin{cases} 0 & x = x_1 \\ 1 & \text{sonst} \end{cases} \qquad g(x) \coloneqq \begin{cases} 1 & x = x_1 \\ 0 & \text{sonst} \end{cases}$$

angeben, für die $f \cdot g = 0$ aber $f \neq 0 \neq g$. (0.5 Punkte)

(ii) Laut Skript ist

$$\operatorname{End}(G) \coloneqq \{f \colon G \to G \mid f \text{ ist Endomorphismus}\}, \tag{9.2}$$

wobei die Endomorphismen die Homomorphismen mit dem speziellen Definitions- und Bildbereich sind, und wir statten $\operatorname{End}(G)$ mit den Verknüpfungen

$$+\colon \operatorname{End}(G) \times \operatorname{End}(G) \to \operatorname{End}(G) \quad \text{mit } (f, g) \mapsto f + g, \text{definiert durch } (f+g)(x) \coloneqq f(x) + g(x)$$
$$\circ\colon \operatorname{End}(G) \times \operatorname{End}(G) \to \operatorname{End}(G) \quad \text{mit } (f, g) \mapsto f \circ g, \text{definiert durch } (f \circ g)(x) \coloneqq f(g(x))$$

aus. Wir wissen bereits, dass $(G^G, +)$ **eine abelsche Gruppe** ist, weil die entsprechenden punktweisen Eigenschaften von $+\colon G \times G \to G$ an $+\colon G^G \times G^G \to G^G$ vererbt werden. Ebenso wissen wir aus Hausaufgabe 4.1, dass $(G^G, \circ)$ ein (i. A. nichtkommutativer) **Monoid mit Eins**, nämlich der Identitätsabbildung) ist. Diese Eigenschaften bleiben erhalten, wenn wir uns auf Homomorphismen einschränken, da die punktweise Verknüpfung (hier Summe) und die Komposition von Homomorphismen wieder ein Homomorphismus ist, sowohl für Monoide, als auch für Gruppen, denn in beiden Fällen ist

$$(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b) = (f+g)(a) + (f+g)(b)$$

und wegen der Strukturverträglichkeit

$$(f \circ g)(a+b) = f(g(a+b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = (f \circ g)(a) + (f \circ g)(b).$$

(1 Punkt)

Nun ist zudem wieder wegen der Strukturverträglichkeit von f für alle $a \in G$:

$$(f \circ (g+h))(a) = f((g+h)(a)) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) = (f \circ g + f \circ h)(a),$$

und

$$((g+h)\circ f)(a) = (g+h)(f(a)) = g(f(a)) + h(f(a)) = ((g\circ f + h\circ f))(a)$$

es gelten also die Distributivgesetzte und es liegt ein **Ring mit Eins** vor. (1 Punkt)

(iii) Aus Hausaufgabe 5.1 wissen wir, dass $\bigcap_{i\in I} R_i$ mit $+$ eine (abelsche) Untergruppe von $(R,+)$ bildet. Für $a,b \in \bigcap_{i\in I} R_i$ ist also $a,b \in R_i$ für alle $i \in I$ und wegen der Unterringeigenschaft jedes R_i sind diese bzgl. $\cdot$ auch abgeschlossen, also $a\cdot b \in R_i$ für alle $i \in I$. Also ist auch $\bigcap_{i\in I} R_i$ bzgl. $\cdot$ abgeschlossen und damit $(\bigcap_{i\in I} R_i, +, \cdot)$ ein Unterring von $(R,+,\cdot)$. Die Distributivgesetze gelten für alle Kombinationen von Elementen im Oberring und damit auch für jede beliebige Teilmenge. (0.5 Punkte)

(iv) Per Definition ist ein Integritätsring ein kommutativer, nullteilerfreier Ring mit Einselement ungleich dem Nullring. In einem Integritätsring ist $0_R \neq 1_R$ also $\mathrm{char}(R) \neq 1$. Angenommen es wäre $\mathrm{char}(R)$ nun eine nicht prime Zahl ungleich 1. Dann gibt es $n,m \in [\![2, \mathrm{char}(R)-1]\!]$ mit $\mathrm{char}(R) = nm$, und somit wegen der Distributivgesetze

$$(n1_R)\cdot(m1_R) = (nm)1_R = 0_R.$$

Da der Integritätsring nullteilerfrei ist, muss $n1_R$ oder $m1_R$ mit 0_R übereinstimmen, im Widerspruch dazu, dass $n,m < \mathrm{char}(R)$. (1 Punkt)

Hausaufgabe 6.4 (Ringhomomorphismen) 4 Punkte

(i) Es seien $(R_1,+_1,\cdot_1)$ und $(R_2,+_2,\cdot_2)$ zwei Ringe und $f\colon R_1 \to R_2$ ein Ringhomomorphismus. Zeigen Sie jeweils im Kontext von Ringen ohne Einselement:

(a) $\mathrm{Bild}(f)$ ist mit $+_2$ und $\cdot_2$ ein Unterring von $(R_2,+_2,\cdot_2)$;

(b) $\mathrm{Kern}(f)$ ist mit $+_1$ und $\cdot_1$ ein Unterring von $(R_1,+_1,\cdot_1)$.

(ii) Es seien $(R_1,+_1,\cdot_1)$ und $(R_2,+_2,\cdot_2)$ zwei Ringe und $f\colon R_1 \to R_2$ ein Ringhomomorphismus. Wenn $(R_1,+_1,\cdot_1)$ und $(R_2,+_2,\cdot_2)$ Ringe mit Eins sind, dann fordern wir zusätzlich die Bedingung $f(1_{R_1}) = 1_{R_2}$ um f einen Ringhomomorphismus im Kontext von Ringen mit Eins nennen zu können. Zeigen Sie, dass die Bedingung $f(1_{R_1}) = 1_{R_2}$ äquivalent zu $1_{R_2} \in \mathrm{Bild}(f)$ ist.

(iii) Zeigen Sie, dass es für jeden Ring $(R,+,\cdot)$ mit 1_R genau einen Ringhomomorphismus $f\colon (\mathbb{Z},+,\cdot) \to (R,+,\cdot)$ gibt, der $f(1) = 1_R$ erfüllt.

Lösung.

(*i*) Die Distributivgesetze gelten für alle Kombinationen von Elementen in den Oberringen und damit auch für jede beliebige Teilmenge.

Dass $f: R_1 \to R_2$ ein Ringhomomorphismus ist, bedeutet insbesondere, dass f auch ein entsprechender Gruppenhomomorphismus für die Mengen mit der additive Verknüpfung ist. Aus Lemma 8.7 wissen wir dann, dass $\mathrm{Bild}(f)$ mit $+_2$ eine Untergruppe von $(R_2, +_2)$ und $\mathrm{Kern}(f)$ mit $+_1$ eine Untergruppe von $(R_1, +_1)$ ist, beide sind damit abelsch. (1 Punkt)

Wegen der multiplikativen Strukturverträglichkeit des Ringhomomorphismus ist für $a, b \in R_1$

$$f(a) \cdot_2 f(b) = f(\underbrace{a \cdot_1 b}_{\in R_1})$$

und damit $\mathrm{Bild}(f)$ abgeschlossen unter $\square$, also $\mathrm{Bild}(f)$ mit $+_2, \cdot_2$ ein Unterring von $(R_2, +_2, \cdot_2)$ im Kontext von Ringen ohne Einselement. (0.5 Punkte)

Außerdem ist für $a, b \in \mathrm{Kern}(f)$

$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) = 0_{R_2} \cdot_2 0_{R_2} = 0_{R_2}$$

und damit $\mathrm{Kern}(f)$ bzgl. $\cdot_1$ abgeschlossen, also mit $+_1, \cdot_1$ ein Unterring von $(R_2, +_1, \cdot_1)$ im Kontext von Ringen ohne Einselement. (0.5 Punkte)

(*ii*) Klar ist, dass $f(1_{R_1}) = 1_{R_2}$ auch $1_{R_2} \in \mathrm{Bild}(f) = f(R_1)$ bedeutet. Ist andererseits nur $1_{R_2} \in \mathrm{Bild}(f) = f(R_1)$, dann gibt es ein $r \in R_1$ mit $f(r) = 1_{R_2}$ und es ist

$$1_{R_2} = f(r) = f(r \cdot_1 1_{R_1}) = f(r) \cdot_2 f(1_{R_1}) = 1_{R_2} \cdot_2 f(1_{R_1}) = f(1_{R_1}).$$

(1 Punkt)

(*iii*) Zur Erinnerung, in einer Gruppe $(G, +)$ können wir für beliebige Elemente a die Abkürzung $\underbrace{a + \cdots + a}_{z\text{-mal}} = za$ schreiben, dabei ist $z \in \mathbb{Z}$. Dabei taucht also eine ganze Zahl aus dem Zählbereich auf, die angibt, wie oft summiert wurde. In dieser Teilaufgabe sind die ganzen Zahlen, die dem Zählbereich entspringen, rot markiert. Für einen Ringhomomorphismus erhält man durch mehrfache Anwendung der Strukturerhaltung auch

$$f(za) = f(a + \cdots + a) = \underbrace{f(a) + \cdots + f(a)}_{z\text{-mal}} = zf(a).$$

Der Knackpunkt dieser Aufgabe ist jetzt, dass $\mathbb{Z}$ zyklisch ist und von der 1 additiv erzeugt wird, was die Funktionswerte von Ringhomomorphismen schon eindeutig festlegt. Sei nämlich

$f\colon (\mathbb{Z}, +, \cdot) \longrightarrow (R, +, \cdot)$ ein Ringhomomorphismus, für den nach Definition $f(1) = 1_R$ gilt, und $z \in \mathbb{Z}$. Dann muss

$$f(z) \overset{\text{zyklisch erz.}}{=} f(z1) = zf(1) = z1_R$$

gelten, was f eindeutig festgelegt.

Tatsächlich ist diese Abbildung auch ein Ringhomomorphismus, denn für $y, z \in \mathbb{Z}$ ist

$$\begin{aligned} f(y+z) &= (y+z)1_R = y1_R + z1_R &&= f(y) + f(z) \\ f(y \cdot z) &= (y \cdot z)1_R \overset{\text{Distrib.}}{=} (y1_R) \cdot (z1_R) &&= f(y) \cdot f(z), \end{aligned}$$

wobei in der letzten Zeile die Distributivgesetze eingeflossen sind, und natürlich ist $f(1) = 1_R$. (1 Punkt)

Bitte reichen Sie Ihre Lösungen als ein PDF auf Mampf ein.