Aufgabe 1

(a) Eine Abbildung $\mathbb{N} \to R$ ist ein Halbringhomomorphismus, falls sie ein Monoidhomomorphismus bezüglich Addition und Multiplikation ist. Mit Aufgabe 4(a) von Blatt 6 gibt es für jedes $r \in R$ genau einen Monoidhomomorphismus $f : (\mathbb{N}, +, 0) \to (R, +, 0)$ mit $f(1) = r$. Damit dieser auch ein Monoidhomomorphismus bezüglich der Multiplikation ist, muss $f(1) = 1$ sein—es gibt also *maximal* einen Halbringhomomorphismus $\mathbb{N} \to R$. Um zu zeigen, dass f auch tatsächlich ein Halbringhomomorphismus ist, müssen wir überprüfen, dass $f(m \cdot n) = f(m) \cdot f(n)$ für $m, n \in \mathbb{N}$ gilt: Dies ist natürlich eine Induktion. Falls $n = 0$ ist, ist $f(m \cdot 0) = f(0) = 0 = f(m) \cdot 0$. Angenommen, dies gilt für ein $n \in \mathbb{N}$: Dann ist

$$\begin{aligned} f(m \cdot (n+1)) &= f(m \cdot n + m) = f(m \cdot n) + f(m) \\ &= f(m) \cdot f(n) + f(m) = f(m) \cdot (f(n) + 1) \\ &= f(m) \cdot (f(n) + f(1)) = f(m) \cdot f(n+1). \end{aligned}$$

Also ist f ein Halbringhomomorphismus, und als solcher eindeutig.

(b) Mit (a) gibt es dann einen eindeutigen Halbringhomomorphismus $f : \mathbb{N} \to R$. Mit Aufgabe 4(b) von Blatt 6 erweitert dieser sich zu einem eindeutig bestimmten Monoidhomomorphismus $(\mathbb{Z}, +, 0) \to (R, +, 0)$ genau dann, wenn $f(1) = 1$ eine Einheit ist. Das ist wiederum mit Aufgabe 2(d) von Blatt 6 genau dann der Fall, wenn R ein Ring ist.

Wenn R ein Ring ist, gibt es insgesamt also wieder *maximal* einen Ringhomomorphismus $\widetilde{f} : \mathbb{Z} \to R$, denn dieser muss eine Erweiterung des eindeutigen Halbringhomomorphismus $f : \mathbb{N} \to R$ sein. Es ist also nur zu prüfen, dass diese Erweiterung auch wieder multiplikativ ist, also dass $\widetilde{f}(x \cdot y) = \widetilde{f}(x) \cdot \widetilde{f}(y)$ für $x, y \in \mathbb{Z}$ ist. Folgende Fälle können auftreten:

- $x, y \in \mathbb{N}$: Dann ist $x \cdot y \in \mathbb{N}$, also $\widetilde{f}(x \cdot y) = f(x \cdot y)$, $\widetilde{(f)}(x) = f(x)$ und $\widetilde{(f)}(y) = f(y)$, somit folgt die Aussage aus (a).
- $x \in \mathbb{N}$, $y \notin \mathbb{N}$. Dann ist $-y \in \mathbb{N}$ und somit

$$\begin{aligned} \widetilde{f}(x \cdot y) &= \widetilde{f}(-(x \cdot (-y))) = -\widetilde{f}(x \cdot (-y)) \\ &= -f(x \cdot (-y)) = -f(x) \cdot f(-y) = -(\widetilde{f}(x) \cdot \widetilde{f}(-y)) \\ &= -(\widetilde{f}(x) \cdot (-\widetilde{f}(y))) = \widetilde{f}(x) \cdot \widetilde{f}(y). \end{aligned}$$

- $x \notin \mathbb{N}$, $y \in \mathbb{N}$: geht analog.
- $x, y \notin \mathbb{N}$: Dann ist $x \cdot y = (-x) \cdot (-y) \in \mathbb{N}$, also

$$\begin{aligned} \widetilde{f}(x \cdot y) &= f((-x) \cdot (-y)) = f(-x) \cdot f(-y) \\ &= \widetilde{f}(-x) \cdot \widetilde{f}(-y) = (-\widetilde{f}(x)) \cdot (-\widetilde{f}(y)) \\ &= \widetilde{f}(x) \cdot \widetilde{f}(y). \end{aligned}$$

Falls andererseits R kein Ring ist, ist $1 \in R$ keine Einheit, also lässt sich der Halbringhomomorphismus $f : \mathbb{N} \to R$ nicht auf $\mathbb{Z}$ erweitern. Da aber jeder Halbringhomomorphismus $\widetilde{f} : \mathbb{Z} \to R$ sich auf einen Halbringhomomorphismus $f : \mathbb{N} \to R$ einschränken lässt, kann es kein solches $\widetilde{f}$ geben.

(c) Wenn R ein Körper ist, ist es insbesondere ein Ring, und es gibt einen eindeutigen Halbringhomomorphismus $g : \mathbb{Z} \to R$. Jeder Halbringhomomorphismus $\widetilde{g} : \mathbb{Q} \to R$ muss also auf $\mathbb{Z}$ mit g übereinstimmen. Für ein allgemeines Element von $\mathbb{Q}$ gilt dann

$$\widetilde{g}\left(\frac{p}{q}\right) = \widetilde{g}\left(\frac{p}{1} \cdot \frac{1}{q}\right) = \widetilde{g}\left(\frac{p}{1}\right) \cdot \widetilde{g}\left(\frac{1}{q}\right) = g(p) \cdot g(q)^{-1},$$

somit ist $\widetilde{g}$ bereits eindeutig bestimmt.

Damit wir $\widetilde{g}$ so definieren können (und $\widetilde{g}$ somit existieren kann), ist allerdings notwendig, dass für jedes $q \in \mathbb{Z}$ mit $q \neq 0$ das Element $g(q) \in R$ eine Einheit ist—das ist nicht automatisch gegeben, z.B. ist im Körper $\mathbb{Z}/2$

$$g(2) = g(1+1) = g(1) + g(1) = 1 + 1 = 0,$$

da $2 \equiv_2 0$ ist. Es kann also keinen Halbringhomomorphismus $\mathbb{Q} \to \mathbb{Z}/2$ geben.

Aufgabe 2

(a) Da $2 \cdot 4 = 8 \equiv_8 0$ und $6 \cdot 4 = 24 \equiv_8 0$ sind $[0], [2], [4]$ und $[6]$ Nullteiler und somit keine Einheiten in $\mathbb{Z}/8$. Mit $1 \cdot 1 = 1$ und $3 + \cdot 5 = 15 \equiv_8 1$ folgt, dass $[1], [3]$ und $[5]$ Einheiten sind.

(b) $[1]$ und $[12]$ sind ihre eigenen Inversen, darüber sind jeweils zueinander invers: $[4]$ und $[10]$, $[3]$ und $[9]$, $[7]$ und $[2]$, $[8]$ und $[5]$, $[6]$ und $[11]$, und zwar aus folgenden Gründen:

- Es ist $[1] \cdot [1] = [1]$.
- Da $12 \equiv_{13} -1$, ist $[12]^2 = (-[1])^2 = [1]$.
- Weiterhin ist $2 \cdot 7 = 14 \equiv_{13} 1$ und somit $[2] \cdot [7] = [1]$.
- Quadrieren liefert $1 \equiv_{13} 2^2 \cdot 7^2 = 4 \cdot 49 \equiv_{13} 4 \cdot 10$, also $[4] \cdot [10] = [1]$.
- Nochmal Quadrieren liefert $1 \equiv_{13} 4^2 \cdot 10^2 \equiv_{13} 16 \cdot (-3)^2 \equiv_{13} 3 \cdot 9$, also $[3] \cdot [9] = [1]$.
- Es ist $8 = 2 \cdot 4$, also $[8]^{-1} = [2]^{-1} \cdot [4]^{-1} = [7] \cdot [10] = [70] = [5]$.
- Genauso ist $6 = 2 \cdot 3$ und somit $[6]^{-1} = [2]^{-1} \cdot [3]^{-1} = [7] \cdot [9] = [63] = [11]$.

Aufgabe 3 (4 Punkte)

Sei $k \in \mathbb{N}$. Dann ist $[n] \cdot [k] = [0]$ in $\mathbb{Z}/m$ genau dann, wenn $n \cdot k \equiv_m 0$ ist. Nach Definition heißt das, dass $\mathrm{rem}_m(n \cdot k) = \mathrm{rem}_m(0) = 0$ ist, also dass es ein $q \in \mathbb{N}$ gibt mit

$$\begin{aligned} & n \cdot k = q \cdot m \\ \Leftrightarrow\ & n \cdot k = q \cdot \frac{m}{n} \cdot n \\ \Leftrightarrow\ & k = q \cdot \frac{m}{n}. \end{aligned}$$

Es ist also $[k]$ genau dann eine Lösung für $n \cdot x = 0$, wenn k ein Vielfaches von $\frac{m}{n}$ ist. (Dabei ist $\frac{m}{n} \in \mathbb{N}$, weil n ein Teiler von m ist.) Jedes $x \in \mathbb{Z}/m$ lässt sich eindeutig schreiben als $x = [k]$ für ein $0 \le k < m$, und es gibt genau n solche k, die Vielfache von $\frac{m}{n}$ sind, nämlich

$$0 \cdot \frac{m}{n}, 1 \cdot \frac{m}{n}, \ldots, (n-1) \cdot \frac{m}{n}.$$

Für $p \ge n$ ist

$$p \cdot \frac{m}{n} \ge n \cdot \frac{m}{n} = m.$$

Bonusaufgabe: Wie im Hinweis vorgeschlagen sei $k \in \mathbb{N}$ und $i > 0$, sodass $[k]$ und $[k+i]$ Lösungen in $\mathbb{Z}/m$ sind. Dann existiert wie oben ein $q \in \mathbb{N}$, sodass $n \cdot k = q \cdot m$, und genauso ein $q' \in \mathbb{N}$ mit $n \cdot (k+i) = q' \cdot m$. Nun ist

$$n \cdot i = n \cdot ((k+i) - k) = (q' - q) \cdot m,$$

also ist $n \cdot i$ ein Vielfaches von m. Es ist $i > 0$, also $q - q' > 0$ und somit $n \cdot i \ge m$. Aber dann folgt direkt $i \ge \frac{m}{n}$.

Sei nun $l \in \mathbb{N}$ die Anzahl der Lösungen in $\mathbb{Z}/m$. Dann gibt es $0 < k_1 < \ldots < k_l \le m$, sodass die Lösungen genau $[k_1], \ldots, [k_l]$ sind. Beachte, dass wir $0 < k_i \le m$ statt $0 \le k_i < m$ gewählt haben, wir repräsentieren $[0] = [m]$ also durch m. Insbesondere ist das eine Lösung, also ist $k_l = m$.

Nun wenden wir einen Trick an: Es ist

$$m = k_l = (k_l - k_{l-1}) + k_{l-1} = \cdots = (k_l - k_{l-1}) + (k_{l-1} - k_{l-2}) + \cdots + (k_2 - k_1) + (k_1 - 0).$$

(So etwas nennt sich *Teleskopsumme*, sie lässt sich wie ein Teleskop vollständig zusammenschieben.) Da alle $[k_i]$ sowie $[0]$ Lösungen sind, sind alle diese Summanden die Differenz zwischen zwei Lösungen. Diese haben wir aber oben abgeschätzt, sie ist mindestens $\frac{m}{n}$. Da wir insgesamt l solche Summanden haben, ist also

$$m = (k_l - k_{l-1}) + (k_{l-1} - k_{l-2}) + \cdots + (k_2 - k_1) + (k_1 - 0) \ge l \cdot \frac{m}{n}.$$

Nach Multiplikation mit n und kürzen von m folgt, dass $n \leq l$ ist.

Weiterhin müsste, damit $n = l$ ist, jede Differenz $(k_{i+1} - k_i)$ genau $\frac{m}{n}$ sein. Aber $(k_{i+1} - k_i)$ ist eine natürliche Zahl, und da n kein Teiler von m ist, ist $\frac{m}{n}$ keine natürliche Zahl. Also folgt, dass die Anzahl der Lösungen l echt kleiner als n ist.

Bemerkung. Allgemein ist die Anzahl der Lösungen gegeben durch den größten gemeinsamen Teiler $l = ggT(m,n)$. Um das zu beweisen benötigen wir den euklidischen Algorithmus, den wir später in der Vorlesung sehen werden.

Aufgabe 4 (5 Punkte)

(a) Das assoziierte Gleichungssystem in den Variablen $x_1, \ldots, x_5$ ist

$$\begin{array}{rrrr} x_2 & +2x_3 & +4x_5 & = b_1 \\ & -1x_4 & +2x_5 & = b_2 \\ & & 0 & = b_3. \end{array}$$

(b) Der Zeilenrang ist 2, also besitzt das Gleichungssystem eine Lösung genau dann, wenn $b_i = 0$ für $i > 2$ ist, also $b_3 = 0$.

(c) Wir gehen vor wie in Beispiel II.1.6: Zunächst bemerken wir, dass die Matrix in strikter Zeilenstufenform ist und Zeilenrang $l = 2$ hat. Die Zeilenzeugenfunktion ist

$$\begin{aligned} r : \{1,2\} &\longrightarrow \{1,\ldots,5\} \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 4. \end{aligned}$$

In anderen Worten: Die 1. Zeile ist zum ersten Mal nicht null in der 2. Spalte, die 2. Zeile ist zum ersten Mal nicht null in der 4. Spalte.

Für das Gleichungssystem bedeutet das: Wir können die Werte für x_i in den übrigen Spalten 1,3 und 5 frei wählen, und es gibt für jede solche Wahl von x_1, x_3 und x_5 eindeutige x_2 und x_4, sodass zusammen eine Lösung gebildet wird. Wir können also unser Gleichungssystem umformen: Die letze Zeile kann gestrichen werden und wir lösen nach x_2 und x_4 auf, indem wir alle anderen Werte auf die rechte Seite bringen:

$$\begin{aligned} x_2 &= b_1 - 2x_3 - 4x_5 \\ x_4 &= -b_2 + 2x_5. \end{aligned}$$

Damit haben wir bereits "die Lösung", wir bringen sie nun noch in die formale Form, die von der Aufgabe gefragt ist: Es ist $k = 5 - l = 3$, und wir definieren:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -4 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{Mat}(5,3,\mathbb{Z}) \qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & -1 \\ 0 & 0 \end{pmatrix} \in \mathrm{Mat}(5,2,\mathbb{Z}).$$

Dann ist mit $b = (b_1, b_2, b_3)$ das Bild der injektiven Funktion

$$\begin{aligned} f_b : \mathbb{Z}^{5-l} &\longrightarrow \mathbb{Z}^5 \\ a &\longmapsto \big(L(A)\big)(a) + \big(L(B)\big)(b) \end{aligned}$$

gerade gegeben durch die Elemente der Form

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} a_1 \\ b_1 - 2a_2 - 4a_3 \\ a_2 \\ -b_2 + 2a_3 \\ a_3 \end{pmatrix}$$

für $a_1, a_2, a_3 \in \mathbb{Z}$: Das ist genau die oben von uns bestimmte Lösungsmenge $L(Z)^{-1}(b)$.