Aufgabe 1

Wir nehmen an, dass $\mathcal{P}$ endlich ist. Dann gibt es ein $n \in \mathbb{N}$ mit $\mathcal{P} = \{p_1, \dots, p_n\}$. Wir betrachten dann die Zahl

$$x := \left(\prod_{i=1}^{n} p_i\right) + 1.$$

Dann gilt für jede Primzahl p_l, dass $x-1$ ein Vielfaches von p_i ist, genauer ist

$$x - 1 = p_l \cdot \underbrace{\left(\prod_{i=1}^{l-1} p_i\right) \cdot \left(\prod_{i=l+1}^{n} p_i\right)}_{=:q}.$$

Insbesondere kann also x kein Vielfaches von p_l sein: Für $r \leq q$ ist

$$r \cdot p_l \leq q \cdot p_l < x,$$

und da $p_l \geq 2$ ist, ist für $r > q$

$$r \cdot p_l \geq (q+1) \cdot p_l = q \cdot p_l + q \geq q \cdot p_l + 2 = (x-1) + 2 > x.$$

Es gilt also für alle $p \in \mathcal{P}$, dass p kein Teiler von x ist—also muss x eine Primzahl sein. Allerdings ist x größer als jedes Element von $\mathcal{P}$, und somit $x \notin \mathcal{P}$. Dies ist ein Widerspruch, also ist die Annahme falsch, und die Menge $\mathcal{P}$ aller Primzahlen ist nicht endlich.

Aufgabe 2

Wir rufen in Erinnerung: Ein Element $m \in M$ ist per Definition genau dann eine Einheit, wenn es ein $m' \in M$ gibt, sodass $m * m' = e$ und $m' * m = e$. Dann ist m' eindeutig und wird mit m^{-1} notiert.

(a) Sei $u \in M$ eine Einheit. Dann gibt es $u^{-1} \in M$, sodass

$$u * u^{-1} = e \text{ und } u^{-1} * u.$$

Genau diese Gleichungen bezeugen aber auch, dass u das Inverse von u^{-1} ist (also $u = (u^{-1})^{-1}$), und u^{-1} somit eine Einheit ist.

(b) Wenn u eine Einheit ist, gibt es ein u^{-1} wie oben. Dann ist

$$f(u) * f(u^{-1}) = f(u * u^{-1}) = f(e) = e$$

und genauso

$$f(u^{-1}) * f(u) = f(u^{-1} * u) = f(e) = e,$$

also ist $f(u)$ eine Einheit.

(c) Wenn u und v Einheiten sind, gibt es $u^{-1}, v^{-1} \in M$, sodass die entsprechenden Gleichungen gelten. Dann ist

$$(u * v) * (v^{-1} * u^{-1}) = u * (v * (v^{-1} * u^{-1})) = u * ((v * v^{-1}) * u^{-1}) = u * e * u^{-1} = u * u^{-1} = e,$$

und genauso $(v^{-1} * u^{-1}) * (u * v) = e$. Also ist $u * v$ eine Einheit.

(d) Ein Halbring $(R, +, \times, 0, 1)$ ist ein Ring genau dann, wenn $(R, +, 0)$ eine Gruppe ist, also jedes $r \in R$ eine Einheit bezüglich $+$ ist. Insbesondere ist in einem Ring also 1 eine Einheit bezüglich $+$. Falls umgekehrt 1 eine Einheit ist, so gibt es ein Element $-1 \in R$ mit $1 + (-1) = 0$. Sei $r \in R$ nun beliebig: Dann ist

$$r + (-1 \times r) = (1 \times r) + (-1 \times r) = (1 + (-1)) \times r = 0 \times r = 0.$$

Genauso ist $(-1 \times r) + r = 0$, also ist $-1 \times r$ ein additives Inverses zu r. Da somit jedes $r \in R$ eine Einheit bezüglich $+$ ist, ist R also ein Ring.

Aufgabe 3

(a) Die Abbildung $\tilde{*}\colon M/\sim \times M/\sim \to M/\sim$ ist eindeutig determiniert durch die Eigenschaft $[m]\tilde{*}[n] = [m*n]$, es ist also nur zu zeigen, dass eine solche Abbildung tatsächlich existiert. Da $*\colon M\times M\to M$ existiert, müssen wir nur zeigen, dass $\tilde{*}$ wohldefiniert ist: Falls $m\sim m'$ und $n\sim n'$, so gilt per Annahme $m*n\sim m'*n'$, also $[m*n]=[m'*n']$.

Um zu sehen, dass $M/\sim$ ein Monoid ist, müssen wir also nur noch Assoziativität und Neutralität überprüfen: Seien $m,n,o\in M$. Dann ist

$$[m]\tilde{*}([n]\tilde{*}[o]) = [m]\tilde{*}[m*o] = [m*(m*o)] = [(m*n)*o] = [m*n]\tilde{*}[o] = ([m]\tilde{*}[n])\tilde{*}[o],$$

sowie

$$[m]\tilde{*}[e] = [m*e] = [m] = [e*m] = [e]\tilde{*}[m].$$

(b_1) Seien $(r,w)\sim(r',w')$ und $(s,v)\sim(s',v')$, also gilt $r+w'=r'+w$ und $s+v'=s'+v$. Dann ist

$$rs+wv+w's+r'v = (r+w')s+(r'+w)v = (r'+w)s+(r+w')v = r's+w'v+ws+rv,$$

und somit $(r,w)\times(s,v)\sim(r',w')\times(s,v)$, und genauso

$$r's+w'v+w's'+r'v' = r'(s+v')+w'(s'+v) = r'(s'+v)+w'(s+v') = r's'+w'v'+w's+r'v,$$

und somit $(r',w')\times(s,v)\sim(r',w')\times(s',v')$. Mit Transitivität ist dann $(r,w)\times(s,v)\sim(r',w')\times(s',v')$.

(b_2) Zunächst ist zu bemerken, dass für Konstruktion 10.7 der Halbring R notwendigerweise kommutativ ist, wir werden das hier benutzen (müssen).

Seien $(r,w)\sim(r',w')$ und $(s,v)\sim(s',v')$, also gilt $r\times w'=r'\times w$ und $s\times v'=s'\times v$. Dann ist

$$\begin{aligned}(rv+ws)(w'v') &= rvw'v'+wsw'v' = rw'vv'+ww's v'\\ &= r'wvv'+ww's'v = r'v'wv+w's'wv = (r'v'+w's')(wv),\end{aligned}$$

wobei im zweiten und vierten Schritt die Kommutativität und im dritten Schritt die Voraussetzung benutzt werden. Somit ist $(r,w)\times(s,v)\sim(r',w')\times(s',v')$.

(b_3) Sei $m\equiv_b m'$ und $n\equiv_b n'$, also $\mathrm{rem}_b(m)=\mathrm{rem}_b(m')=:r$ und $\mathrm{rem}_b(n)=\mathrm{rem}_b(n')=:s$. Laut Definition von rem_b (Satz 8.1) gibt es also $q_m,q_{m'},q_n,q_{n'}\in\mathbb{N}$ mit

$$q_m\cdot b+r=m,\qquad q_{m'}\cdot b+r=m',\qquad q_n\cdot b+s=n,\qquad q_{n'}\cdot b+s=n'.$$

Auch mit Satz 8.1 gibt es ein $q_+\in\mathbb{N}$ und $0\le t<b$, sodass $(r+s)=q\cdot b+t$ ist (tatsächlich ist $q_+\le 1$, aber das ist egal). Dann ist

$$\begin{aligned}m+n &= q_m\cdot b+r+q_n\cdot b+s = (q_m+q_n+\tilde{q})\cdot b+t,\\ m'+n' &= q_{m'}\cdot b+r+q_{n'}\cdot b+s = (q_{m'}+q_{n'}+\tilde{q})\cdot b+t,\end{aligned}$$

also $\mathrm{rem}_b(m+n)=t=\mathrm{rem}_b(m'+n')$ und somit $m+n\equiv_b m'+n'$.

(b_4) Sei wieder $m\equiv_b m'$ und $n\equiv_b n'$, und $r,s,q_m,q_{m'},q_n,q_{n'}\in\mathbb{N}$ wie oben. Dann gibt es ein $q_\times\in\mathbb{N}$ und $0\le u<b$ mit $(r\cdot s)=q_\times\cdot b+u$, und es ist

$$\begin{aligned}m\cdot n &= (q_m\cdot b+r)\cdot(q_n\cdot b+s) = (q_m\cdot q_n\cdot b+q_m\cdot s+q_n\cdot r)b+r\cdot s\\ &= (q_m\cdot q_n\cdot b+q_m\cdot s+q_n\cdot r+q_\times)b+u,\\ m'\cdot n' &= (q_{m'}\cdot b+r)\cdot(q_{n'}\cdot b+s) = (q_{m'}\cdot q_{n'}\cdot b+q_{m'}\cdot s+q_{n'}\cdot r)b+r\cdot s\\ &= (q_{m'}\cdot q_{n'}\cdot b+q_{m'}\cdot s+q_{n'}\cdot r+q_\times)b+u,\end{aligned}$$

also $\mathrm{rem}_b(m\cdot n)=u=\mathrm{rem}_b(m'\cdot n')$ und somit $m\cdot n\equiv_b m'\cdot n'$.

Aufgabe 4

(a) Angenommen, es existiert ein Monoidhomomorphismus $f : \mathbb{N} \to M$ mit $f(1) = m$. Da f ein Homomorphismus ist, ist $f(0) = 0$. Für jedes $n \in \mathbb{N}$ muss ebenfalls

$$f(s(n)) = f(n+1) = f(n) \star f(1) = f(n) \star m.$$

Aber nach dem Rekursionsprinzip gibt es eine eindeutige Abbildung (von Mengen) $g : \mathbb{N} \to M$ mit $g(0) = e$ und $g(s(n)) = g(n) \star m$ für alle $n \in \mathbb{N}$, das heißt: Falls f existiert, ist es eindeutig bestimmt.

Auf der anderen Seite zeigen wir, dass die Abbildung g ein Monoidhomomorphismus ist, also ein solches f existiert: Es ist $g(0) = e$ nach Konstruktion, und für $n, n' \in \mathbb{N}$ ist $g(n+n') = g(n) \star g(n')$: Das gilt für $n' = 0$ mit

$$g(n+0) = g(n) = g(n) \star e = g(n) \star g(0).$$

Angenommen, es gilt für ein $n' \in \mathbb{N}$, so ist

$$\begin{aligned} g(n+(n'+1)) &= g((n+n')+1) = g(n+n') \star m = (g(n) \star g(n')) \star m \\ &= g(n) \star (g(n') \star m) = g(n) \star g(n'+1). \end{aligned}$$

Somit ist g ein Monoidhomomorphismus, insbesondere ist damit Existenz gezeigt.

(b) Eine Erweiterung/Fortsetzung von $f : \mathbb{N} \to M$ zu einem Homomorphismus $\widetilde{f} : \mathbb{N} \to M$ bedeutet, dass $\widetilde{f} \circ \iota = f$ ist, wobei $\iota : \mathbb{N} \to \mathbb{Z}$ der Homomorphismus ist, der $\mathbb{Z}$ als Gruppenvervollständigung von $\mathbb{N}$ ausweist.

Sei zuerst angenommen, eine solche Erweiterung $\widetilde{f}$ existiert: Insbesondere ist dann

$$e = \widetilde{f}(0) = \widetilde{f}((-1)+1) = \widetilde{f}(-1) \star \widetilde{f}(1) = \widetilde{f}(-1) \star \widetilde{f}(\iota(1)) = \widetilde{f}(-1) \star f(1) = \widetilde{f}(-1) \star m$$

und genauso

$$e = \widetilde{f}(0) = \widetilde{f}(1+(-1)) = \widetilde{f}(1) \star \widetilde{f}(-1) = \widetilde{f}(\iota(1)) \star \widetilde{f}(-1) = f(1) \star \widetilde{f}(-1) = m \star \widetilde{f}(-1),$$

also ist m eine Einheit mit Inversem $\widetilde{f}(-1)$.

Sei nun umgekehrt $f(1) = m$ eine Einheit. Dann ist mit einer kleinen Induktion auch jedes Element von $\mathrm{Im}(f)$ eine Einheit: Es ist $f(0) = e$ eine Einheit, und falls $f(n)$ eine Einheit ist, so auch (mit Aufgabe 2(c))

$$f(n+1) = f(n) \star f(1) = f(n) \star m.$$

Da nach Definition $\mathbb{Z} = \mathbb{N}^{\mathrm{grp}} = K(\mathbb{N}, \mathbb{N})$ ist, gibt es dann laut Satz 9.10 genau eine Erweiterung $\widetilde{f} : \mathbb{Z} \to M$ von f.