Aufgabe 1

Die Primfaktorzerlegung von 1260 ist

$$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7.$$

Vermöge des chinesischen Restsatzes sind daher

$$\begin{aligned}
\mathbb{Z}/1260\mathbb{Z} &\cong \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/1260\mathbb{Z} && \text{0 Primfaktoren links} \\
&\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/315\mathbb{Z} \quad \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/252\mathbb{Z} && \text{1 Primfaktor links} \\
&\cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/140\mathbb{Z} && \text{" 3 Primfaktoren rechts} \\
&\cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z} \\
&\cong \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z} && \text{2 Primfaktoren links} \\
&\cong \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/63\mathbb{Z} && \text{" 2 Primfaktoren rechts} \\
&\cong \mathbb{Z}/28\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}
\end{aligned}$$

alle Zerlegungen von $\mathbb{Z}/1260\mathbb{Z}$ in Produkte $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ für positive ganze Zahlen m und n (bis auf Reihenfolge).

Aufgabe 2

$n = 538 = 2 \cdot 269$:

teilerfremd

Somit gibt es nur die Gruppe

$\mathbb{Z}/538\mathbb{Z}$

$n = 539 = 7^2 \cdot 11$:

In diesem Fall gibt es die beiden Gruppen

$\mathbb{Z}/539\mathbb{Z}$

und

$\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/77\mathbb{Z}$

$n = 540 = 2^2 \cdot 3^3 \cdot 5$:

Hier gibt es einige Möglichkeiten:

$\mathbb{Z}/540\mathbb{Z}$,

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/270\mathbb{Z}$,

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$,

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$,

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$,

und

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

Verwenden hier stets die Klassifikation endlich erzeugter abelscher Gruppen mit der Zusatzbedingung an die Teiler $d_1 | d_2 | \ldots | d_n$

$n = 541$:

prim

Gibt also nur die Gruppe

$\mathbb{Z}/541\mathbb{Z}$

Aufgabe 3

(i)

Da $n \cdot 0 = 0$ ist nG nicht leer. Sind nun ng und ng' aus nG, so auch $ng - ng' = n(g-g')$. Somit ist nG eine Untergruppe von G.

(ii)

Sei $\varphi: G \to G_1 \times \dots \times G_r$ ein Isomorphismus.

Wir definieren

$$\psi: nG \to nG_1 \times \dots \times nG_r.$$
$$ng \mapsto n\varphi(g)$$

Dies ist ein Homomorphismus, denn es gilt

$$\begin{aligned}\psi(ng + ng') = \psi(n(g+g')) = n\varphi(g+g') &= n(\varphi(g) + \varphi(g')) \\ &= n\varphi(g) + n\varphi(g') \\ &= \psi(ng) + \psi(ng')\end{aligned}$$

für alle $ng, ng' \in nG$.

Zudem ist ψ bijektiv, da

$$\psi': nG_1 \times \dots \times nG_r \to nG$$
$$(ng_1, \dots, ng_r) \mapsto n\varphi^{-1}(g_1, \dots, g_r)$$

aufgrund von

$$\begin{array}{c} \text{gilt} \\ \text{für} \\ \text{alle} \\ (ng_1,\dots,ng_r) \\ \text{in} \\ nG_1 \times \dots \times nG_r \end{array} \left\{ \begin{aligned} \psi \circ \psi'(ng_1, \dots, ng_r) &= \psi(n\varphi^{-1}(g_1, \dots, g_r)) \\ &= n\,\varphi(\varphi^{-1}(g_1, \dots, g_r)) \\ &= n(g_1, \dots, g_r) \\ &= (ng_1, \dots, ng_r) \end{aligned} \right.$$

und

$$\begin{array}{c} \text{gilt} \\ \text{für} \\ \text{alle} \\ ng \\ \text{in} \\ nG \end{array} \left\{ \begin{aligned} \psi' \circ \psi(ng) = \psi'(n\varphi(g)) &= n\varphi^{-1}(\varphi(g)) \\ &= ng \end{aligned} \right.$$

die Umkehrabbildung von ψ ist.

(iii)

Als Untergruppe der zyklischen Gruppe G ist nG zyklisch. Bleibt also nur die Ordnung zu bestimmen.

Ist a ein Erzeuger von G, so ist zudem na ein Erzeuger von nG, sodass $|nG| = \mathrm{ord}(na)$.
Da $\frac{m}{n} \cdot na = ma = 0$ in $G \cong \mathbb{Z}/m\mathbb{Z}$, ist $\mathrm{ord}(na) \leq \frac{m}{n}$. Ist allerdings $k < \frac{m}{n}$, so ist $kn < m$ und somit $k \cdot na \neq 0$ in G. Somit gilt $\mathrm{ord}(na) = \frac{m}{n}$, sodass $nG \cong \mathbb{Z}/\frac{m}{n}\mathbb{Z}$.

(iv)

Nach Lagrange ist $m \cdot g = 0$ für alle $g \in G$ und somit auch $qm \cdot g = 0$ für alle $q \in \mathbb{Z}$.
Da $n = qm$ für ein geeignetes q ist, muss also nG isomorph zu $\{0\}$ sein.

(v)

Die Abb. $\varphi_n : G \xrightarrow{\cdot n} G$, $g \mapsto ng$ ist bijektiv, da $a, b \in \mathbb{Z}$ mit $am + bn = 1$ existieren (m,n sind teilerfremd) und somit $b = n^{-1} \bmod m$ ist und die Multiplikation mit b daher die zu φ_n inverse Abbildung ist.

Aufgabe 4

Da G zyklisch ist, ist ein Homomorphismus $\varphi: G \to H$ bereits durch das Bild eines Erzeugers von G festgelegt, denn ist $G = \langle a \rangle$, so erhalten wir

$$\varphi(\underbrace{a^n}_{\text{beliebiges Element in } G \text{ sieht so aus}}) = \varphi(a)^n$$

für alle $n \in \mathbb{Z}$.

Ist $G \cong \mathbb{Z}$, so liefert auch andersherum jede solche Wahl einen Homomorphismus $\varphi: \mathbb{Z} \to H$ vermöge

$$\varphi(m) = m\varphi(1).$$

Ist $G \cong \mathbb{Z}/n\mathbb{Z}$ für ein $n \geq 1$, und ist $H \cong \mathbb{Z}$, so erhalten wir aufgrund der Gleichung

$$n \cdot \bar{1} = 0$$

in $\mathbb{Z}/n\mathbb{Z}$, dass jeder Homomorphismus $\varphi: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$, welcher $\varphi(\bar{1}) \neq 0$ erfüllt, nicht wohldefiniert sein kann. (denn $\bar{0} = \varphi(\underbrace{n\bar{1}}_{=\bar{0}}) = n\varphi(\bar{1})$). Es gibt also nur den trivialen Homomorphismus (alle Elemente auf 0 abbilden).

Ist $G \cong \mathbb{Z}/n\mathbb{Z}$ und $H \cong \mathbb{Z}/m\mathbb{Z}$, so wird es interessanter und schwieriger. Es muss auch hier $n\underbrace{\varphi(\bar{1})}_{=:\bar{b}} = \bar{0}$ gelten, sodass wir

$qm = nb$ und somit auch $\frac{qm}{g} = \frac{nb}{g}$ erhalten, wobei $g = \mathrm{ggT}(n,m)$. Nun sind $\frac{m}{g}$ und $\frac{n}{g}$ aber teilerfremd. Daher muss $\frac{m}{g}$ ein Teiler von b sein. Von solchen b gibt es nun g viele (mod m), nämlich $k\overline{\frac{m}{g}}$ für $0 \leq k \leq (g-1)$. Diese Wahlen liefern nun allesamt wohldef. Homomorphismen, wie man kurz nachrechnen kann:

Ist $a \in \mathbb{Z}$, so haben $\bar{a}$ und $\overline{a+qn}$ dasselbe Bild, da $qn\overline{\frac{km}{g}} = q \cdot \bar{k}\,\underbrace{\overline{\frac{nm}{g}}}_{=\overline{\pm \mathrm{kgV}(n,m)} = \bar{0}} = \bar{0}$.