12.1

Note that: $r = (1\ 2 \cdots n)$ is even $\iff$ n odd

$s = (2\ n)(3\ n-1)\cdots$ is even $\iff$ $n \equiv 1 \bmod 4$ or $n \equiv 2 \bmod 4$

Thus: if...

$n \equiv 0 \bmod 4$

$\ker\{s\} = \{e, sr, r^2, sr^3, \dots\}$

$n \equiv 1 \bmod 4$

$\ker(s) = \{e, r, r^2, \dots, s, sr, sr^2, \dots\}$

$n \equiv 2 \bmod 4$

$\ker\{s\} = \{e, s, r^2, sr^2, r^4, sr^4, \dots\}$

$n \equiv 3 \bmod 4$

$\ker(s) = \{e, r, r^2, \dots\}$

12.2

($\Rightarrow$) Let $N \trianglelefteq G$. Fix $g \in G$.

($\subseteq$) Let $n \in N$. Notice $gng^{-1} \in N$ since N normal.

($\supseteq$) Let $n \in N$. By Lemma 12.8, $\exists n' \in N$ such that $ng = gn'$. Thus $n = gn'g^{-1} \in gNg^{-1}$.

($\Leftarrow$) Let $N \subseteq G$ and $gNg^{-1} = N$ $\forall g \in G$. Then if $n \in N$, $g \in G$, $gng^{-1} \in gNg^{-1} \Rightarrow gng^{-1} \in N$. ☒

12.3

Let $f: G \to H$ be a surjective group homomorphism with $N = \ker(f) = \{g \in G \mid f(g) = e\}$.

Define $w: G/N \to H$ by $w(Ng) = f(g)$.

- Suppose $Ng_0 = Ng_1$, where $g_0, g_1 \in G$. Then $g_1 g_0^{-1} \in N$, and thus

$$\begin{aligned} w(Ng_1) &= f(g_1) \\ &= f(g_1 g_0^{-1} g_0) \\ &= f(g_1 g_0^{-1}) f(g_0) && (f \text{ is homomorphism}) \\ &= e \cdot w(Ng_0) && (g_1 g_0^{-1} \in N = \ker(f)) \\ &= w(Ng_0). \end{aligned}$$

So w is well defined.

- Notice

$$\begin{aligned} w(Ng_0 Ng_1) &= w(Ng_0 g_1) && (\text{Lemma } 12.9) \\ &= f(g_0 g_1) \\ &= f(g_0) f(g_1) && (f \text{ is homomorphism}) \\ &= w(Ng_0)\, w(Ng_1) \end{aligned}$$

So w is a homomorphism.

- Let $h \in H$. Then $\exists g \in G$ such that $h = f(g) = w(Ng)$. So w is surjective.
- Suppose $w(Ng_0) = w(Ng_1)$. Then $f(g_0) = f(g_1)$. It follows from f being a homomorphism that

$$e = f(g_1) f(g_0)^{-1} = f(g_1) f(g_0^{-1}) = f(g_1 g_0^{-1})$$

So $g_1 g_0^{-1} \in N$, and thus $Ng_0 = Ng_1$ (Lemma 11.5). ☒

Lemma If G abelian, then every subgroup of G is normal. Pf Let $N \leq G$, $n \in N$, $g \in G$. Since G abelian, $gng^{-1} = gg^{-1}n = n \in N$. ☒

12.4

($\Leftarrow$) Let $N \geq 2$ be prime. Note that $|\mathbb{Z}/N| = N$ is prime, so by Lagrange, every subgroup of $\mathbb{Z}/N$ must be of order 1 or N. Since the only possible subgroups of order 1 or N are $\{e\}$ and $\mathbb{Z}/N$, $\mathbb{Z}/N$ is simple.

($\Rightarrow$) Let $N \geq 2$ and $\mathbb{Z}/N$ be simple. Consider $g \in \mathbb{Z}/N$, $g \neq e$. Then $\{g, g^2, \dots\} = \mathbb{Z}/N$ since $\mathbb{Z}/N$ simple. Suppose for contradiction that $N = pq$, where $p > 1$, $q > 1$ are integers. Then $(g^m)^n = g^{mn} = e$ so $\{g^m, (g^m)^2, \dots\}$ is a normal (Lemma) subgroup of $\mathbb{Z}/N$ with order M, $1 < M \leq n < N$, a contradiction! Thus N prime. ☒

12.5

Let A be a non-trivial abelian group.

($\Rightarrow$) Let A be simple. If $g \in A$ then $\{g, g^2, \dots\} \trianglelefteq A$ since A is abelian (Lemma). Furthermore, $\{g, g^2, \dots\} = A$ since A simple. If $|A|$ not finite, $\{g^2, (g^2)^2, \dots\} \trianglelefteq A$ is a proper normal subgroup of A, which is impossible since A simple. Thus $|A| = N$, where $N < \infty$. Since $A = \{g, g^2, \dots, g^{N-1}, e\}$, consider the map $\varphi : A \to \mathbb{Z}/N$ defined by $\varphi(g^i) = i$. (This is clearly an isomorphism). Then $\mathbb{Z}/N \cong A$ is simple, so N must be prime by (12.4).

($\Leftarrow$) Let $A \cong \mathbb{Z}/p$, p prime. By (12.4), $\mathbb{Z}/p$ is simple. Let $\phi : \mathbb{Z}/p \to A$ be an isomorphism, $N \trianglelefteq A$, $N \neq A$. Then $\phi^{-1}(N) \trianglelefteq \mathbb{Z}/p$, and thus $\phi^{-1}(N) = \{e\}$. Now, let $x \in N$. Then $\phi^{-1}(x) \in \phi^{-1}(N) = \{e\}$, so $\phi^{-1}(x) = e$. Thus $x = e$, and so $N = \{e\}$. ☒