Exercise 1 We show that if $(G, \circ)$ is a group and H is a nonempty subset of G which is closed under $\circ$ then H is a subgroup of G. We assume associativity as per axiom 1.41 and show that there exists a neutral element and inverse elements.

Since H is closed under $\circ$, for arbitrary $a, b \in H$ we have $a \circ b \in H$. It follows that for any $h \in H$ we have that $h, h^2, h^3, \ldots \in H$.

Since H is finite the above sequence must have repeating elements at some point. Thus there must exist $i, k \in \mathbb{Z}$ with $i > k$ such that $h^i = h^k$. By $\circ$-ing h^{-k} to both sides we can transform this to $h^{i-k} = e$. Since $i > k$, $i - k$ is positive which means that e is a positive power of h and thus $e \in H$.

We can restate $h^{i-k} = e$ to $h \circ h^{i-k-1} = e$ and thus the inverse of $h \in H$ is $h^{i-k-1} \in H$.

Exercise 2 There is no such group. Consider $G = H_1 \cup H_2$ with $g_1 \in H_1 \backslash H_2$ and $g_2 \in H_2 \backslash H_1$. Assume $g_1 \circ g_2 \in H_1$, we then have

$$\begin{aligned} g_1 \circ g_2 &\in H_1 \\ g_1^{-1} \circ (g_1 \circ g_2) &\in H_1 \\ (g_1^{-1} \circ g_1) \circ g_2 &\in H_1 \\ e \circ g_2 &\in H_1 \\ g_2 &\in H_1, \end{aligned}$$

which is a contradiction. It follows that the same applies for $g_1 \circ g_2 \in H_2$.

A proper subgroup H of a group G is a subgroup where $H \neq G$. We are given a group G and asked to show if there exist proper subgroups H_1 and H_2 such that $G = H_1 \cup H_2$.

Let us assume that this is the case. We now have $H_1 \not\subset H_2$ and $H_2 \not\subset H_1$ because otherwise $H_1 \cup H_2 = H_1$ and $H_1 \cup H_2 = H_2$, respectively, which would mean that H_1 and H_2 are not proper subgroups. This means that there exist $x \in G \backslash H_1$ and $y \in G \backslash H_2$. (Thus $x \notin H_1$ and $y \notin H_2$.)

Because G is a group we have $xy \in G$. Since we assume $G = H_1 \cup H_2$ we further have $xy \in H_1$ *or* $xy \in H_2$. We can now derive a contradiction through

$$\begin{aligned} xy = xy &\in H_1 & \qquad xy = xy &\in H_2 \\ x = (xy)y^{-1} &\in H_1 & \qquad y = (xy)x^{-1} &\in H_2 \end{aligned}$$

which ultimately shows that $G = H_1 \cup H_2$ cannot exist.

Exercise 3 If we take a cycle c to the power of its length l we get $\mathrm{id} \in S_l$. If we apply it to the power of some multiple of its length this obviously still holds. So we are looking for the smallest common multiple of all cycle lengths, knowing that this will yield id for all respective lengths.

Breaking π down into disjoint cycles gives us (1 3 7)(2)(4 8 5 6), with lengths 3, 1 and 4 respectively. The least common multiple of these cycle lengths is 12, thus the order of the permutation is 12.

Exercise 4 Following the given hint we obtain $\gcd(9, 15) = 3$ and determine that the set of $c \in \mathbb{Z}$ for which $9x + 15y = c$ has a solution is the set of all c which are a multiple of 3. (Since, for a diophantic equation to have an integer solution, the greatest common divisor must divide c.)

We can thus describe G as $3 \cdot \mathbb{Z}$.

Exercise 5 To show that a group G is abelian we show that for arbitrary $a, b \in G$ we have $a \circ b = b \circ a$. Consider

$$\begin{aligned} a \circ b &= b \circ a \quad \text{and after adding } b \text{ to both sides,} \\ a &= b \circ a \circ b, \end{aligned}$$

and, replacing the a on the left hand side and adding $b \circ b = e$ on the right hand side

$$\begin{aligned} a \circ b &= b \circ a \\ b \circ a \circ b \circ b &= b \circ a \circ e \\ b \circ a \circ b \circ b &= b \circ a \circ b \circ b \\ b \circ a &= b \circ a. \end{aligned}$$

Exercise 6 We are given a homomorphism ϕ from a group $(G, \circ)$ to a group $(H, *)$.

- To show that $\ker(\phi)$ is a subgroup of G we show that the statement

  $$\forall\, a, b \in \ker(\phi) : a \circ b^{-1} \in \ker(\phi)$$

  holds. Let $a, b \in \ker(\phi)$ so we have $\phi(a) = \phi(b) = e_H$. Then

  $$\begin{aligned} \phi(a \circ b^{-1}) &= \phi(a) * \phi(b^{-1}) \\ &= \phi(a) * \phi(b)^{-1} \\ &= e_H * e_H^{-1} \\ &= e_H \end{aligned}$$

  and thus $a \circ b^{-1} \in \ker(\phi)$. (Since $\ker(\phi)$ is defined to contain all $g \in G$ such that $\phi(g) = e_H$.)

- To show that $\phi(G)$ is a subgroup of H we show that the statement

  $$\forall\, a, b \in \phi(G) : a * b^{-1} \in \phi(G)$$

  holds. Choose $x, y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$. We now have

  $$\begin{aligned} \phi(x \circ y^{-1}) &= \phi(x) * \phi(y^{-1}) \\ \phi(x \circ y^{-1}) &= a * b^{-1} \end{aligned}$$

  since G is a group we have $x \circ y^{-1} \in G$ and thus $\phi(x \circ y^{-1}) \in \phi(G)$. (Meaning that $a * b^{-1} \in \phi(G)$.)

Exercise 7 As an example, for $n = 3$ we have

$$p(x) = b_1 \frac{(x - a_2)(x - a_3)}{(a_1 - a_2)(a_1 - a_3)} + b_2 \frac{(x - a_1)(x - a_3)}{(a_2 - a_1)(a_2 - a_3)} + b_3 \frac{(x - a_1)(x - a_2)}{(a_3 - a_1)(a_3 - a_2)}$$

The expression

$$\frac{(x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n)}{(a_i - a_1) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)}$$

will always evaluate to zero (0) unless $x = a_i$ because the dividend would be zero otherwise. In the case where $x = a_i$ it is clear that it will evaluate to one (1) since there are n matching pairs of $(a_i - a_1), (a_i - a_2), \cdots$ in both divisor and dividend.

This means that

$$p(x) = \sum_{i=1}^{n} b_i \frac{(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} = \sum_{i=1}^{n} b_i \cdot \begin{cases} 0 & \text{for } x \neq a_i \\ 1 & \text{for } x = a_i \end{cases}$$

can be restated as $p(a_i) = b_i$.

Consider $a_1 = -1$, $a_2 = 0$, $a_3 = 1$ and $a_4 = 2$ and $b_1 = -1$, $b_2 = 0$, $b_3 = 1$ and b_4. We now have

$$\begin{aligned} p(x) &= -\frac{(x-0)(x-1)(x-2)}{(-1-0)(-1-1)(-1-2)} + \frac{x-(-1)(x-0)(x-2)}{(1-(-1)(1-0)(1-2))} + 5\frac{(x-(-1)(x-0))(x-0)(x-1)}{(2-(-1))(2-0)(2-1)} \\ &= \frac{x^3}{2} + \frac{x}{2} \end{aligned}$$

with $p(-1) = -1$, $p(0) = 0$, $p(1) = 1$ and $p(2) = 5$.

Exercise 8 Of the given structures,

$$\overset{3}{A}, \quad \overset{4}{B}, \quad \overset{5}{C}, \quad \overset{6}{D}, \quad \overset{4}{E}, \quad \overset{4}{G} \quad \text{and} \quad \overset{6}{H}$$

are groups. An isomorphism is a bijective function and thus we need only consider sets of equal length. This leaves (B, E), (B, G) and (D, H) as candidates. (B, G) and (B, E) (exchange 3 and 4) are isomorphic.