13.2 Solutions to Exercises 2 - Exercises on groups

Solution. (Question 2.5.1) Can prove by induction (which is long), or notice that:

$$\begin{aligned}(g^{-1}hg)^n &= (g^{-1}hg)(g^{-1}hg)(g^{-1}hg)\cdots(g^{-1}hg)(g^{-1}hg)\\ &= g^{-1}h(gg^{-1})h(gg^{-1})h(gg^{-1})\cdots h(gg^{-1})hg\\ &= g^{-1}h^ng.\end{aligned}$$

Solution. (Question 2.5.2)

(a) ($\Rightarrow$) By the Quick Subgroup Test, we know $e_G \in H$. Therefore, if $|H| = 1$, then the unique element of H must be e_G.
($\Leftarrow$) If $H = \langle e_G\rangle$ then obviously $|H| = 1$.

(b) Every element in H lies in G, we can write $G = H \cup S$, where $S \cap H = \varnothing$. Since G is finite and $H \cap S = \varnothing$, we have $|G| = |H| + |S|$.
($\Rightarrow$) If $|G| = |H|$, then $|S| = 0$ and so $S = \varnothing$. Hence $G = H$.
($\Leftarrow$) If $G = H$ then obviously $|G| = |H|$.

(c) No. For example, $(\mathbb{Z}, +) < (\mathbb{Q}, +)$, but $|\mathbb{Z}| = |\mathbb{Q}|$.

Solution. (Question 2.5.3) We use the Quick Subgroup Test.

[Identity] Since H and K are subgroups of G, we know (by the Quick Subgroup Test) that $e_G \in H$ and $e_G \in K$. Hence $e_G \in H \cap K$.

[Closure] If $h, k \in H \cap K$, then $h, k \in H$ and so $hk \in H$. Furthermore, $h, k \in K$ and so $hk \in K$. Hence $hk \in H \cap K$.

[Inverse] Suppose $h \in H \cap K$. Then $h \in H$ so $h^{-1} \in H$. Furthermore, $h \in K$ and so $h^{-1} \in K$. Hence $h^{-1} \in H \cap K$ for all $h \in H \cap K$.

Solution. (Question 2.5.4) Let $n := o(g)$. Now $\{g^0, \ldots, g^{n-1}\} = \{g^1, \ldots, g^n\} \subseteq \langle g\rangle$, so $n \leq |\langle g\rangle|$.
On the other hand, a general element of $\langle g\rangle$ has the form g^m for some $m \in \mathbb{Z}$. We can write $m = an + r$ for some $a \in \mathbb{Z}$ and some $0 \leq r < n$ by the division algorithm. Hence,

$$g^m = g^{an+r} = (g^n)^a * g^r = e_G^a * g^r = g^r \in \{g^0, \ldots, g^{n-1}\}.$$

Hence $|\langle g\rangle| \leq n$. The result is thus proved.

Solution. (Question 2.5.5)

(a) To answer this just calculate $g^0, g^1, g^2, \ldots$ until you get a repeat — then you know you've found every element of $\langle g\rangle$.
$\langle g\rangle = \{e,\ (1\ 3\ 5\ 7)(2\ 4),\ (1\ 5)(3\ 7),\ (1\ 7\ 5\ 3)(2\ 4)\}$

(b) To answer this just calculate $(g^2)^0, (g^2)^1, (g^2)^2, \ldots$ until you get a repeat — then you know you've found every element of $\langle g^2\rangle$.
$\langle g^2\rangle = \{e, (1\ 5)(3\ 7)\}$

Solution. (Question 2.5.6) To prove it is cyclic, we need to find a single element that generates the group. Choose any element in $\mathbb{Z}_n$. It will have the form $[m]_n$ for some $m \in \{0, 1, \ldots, n-1\}$.
Now because $\oplus$ is the group operation we have $([1]_n)^m = [1]_n \oplus \cdots \oplus [1]_n$ (m times) $= [1 + \cdots + 1]_n = [m]_n$. We have shown that every element in $\mathbb{Z}_n$ lies in $\langle [1]_n\rangle$. Hence $\mathbb{Z}_n \subseteq \langle [1]_n\rangle$. On the other hand, we know $\langle [1]_n\rangle \leq \mathbb{Z}_n$. Therefore $\mathbb{Z}_n = \langle [1]_n\rangle$ and $\mathbb{Z}_n$ is thus cyclic.