Q1

a) $(1\,7\,6\,4\,5)(2\,3)$

$(1\,7)(7\,6)(6\,4)(4\,5)(2\,3)$

b) • the order of $(1\,7\,6\,4\,5)$ is 5 so $(1\,7\,6\,4\,5)^5 = e$

$(1\,7\,6\,4\,5)^6 = (1\,7\,6\,4\,5)^{5+1} = e \cdot (1\,7\,6\,4\,5)^1 = (1\,7\,6\,4\,5)$

• the order of $(2\,3)$ is 2, and $2|6$, so $(2\,3)^6 = (2\,3)^2(2\,3)^2(2\,3)^2$
$= e$

so $((1\,7\,6\,4\,5)(2\,3))^6 = (1\,7\,6\,4\,5)$

Q2

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z}_m \quad \text{(7.2 from notes)}$$

I'll just restate this first, in words:

the cross product of two cyclic groups $\mathbb{Z}_m, \mathbb{Z}_n$
is isomorphic to cyclic group $\mathbb{Z}_{mn}$
iff. m, n are relatively prime

($\Rightarrow$) suppose that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ such
that $\gcd(m,n) > 1$

Goal: proof by contradiction

let $\gcd(m,n) = d$, so $d > 1$
take $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$
• note that $(a,b) \in \mathbb{Z}_{mn}$ so this is
cyclic and must have order mn.

$d \mid mn$ (due to the gcd statement)

then $\frac{mn}{d} \in \mathbb{Z}$

in $\mathbb{Z}_{mn}$

consider $\frac{mn}{d}(a,b) = \left(\frac{mna}{d}, \frac{mnb}{d}\right)$

$= \left(m\left(\frac{n}{d}a\right), n\left(\frac{m}{d}b\right)\right)$

m is the order of $\mathbb{Z}_m$, so $m\left(\frac{n}{d}a\right) = e \in \mathbb{Z}_m$

n is the order of $\mathbb{Z}_n$, so $n\left(\frac{m}{d}b\right) = e \in \mathbb{Z}_n$

But this implies (by homomorphism) that the order of $\mathbb{Z}_{mn}$ is $\frac{mn}{d}$

Since $\frac{mn}{d} < mn$, then $|\mathbb{Z}_{mn}| \neq mn$

This is a contradiction

Since $d > 1$ is false, then $d = \gcd(m,n) = 1$

($\Leftarrow$) Assume $\gcd(m,n) = 1$

Note that $\langle \bar{1} \rangle$ generates $\mathbb{Z}_m$, and $\mathbb{Z}_n$

$|\langle \bar{1} \rangle| = m$, for $\mathbb{Z}_m$

$|\langle \bar{1} \rangle| = n$, for $\mathbb{Z}_n$

$(\bar{1}, \bar{1}) \in \mathbb{Z}_m \times \mathbb{Z}_n$

We can use that $\gcd(m,n) \cdot \text{lcm}(m,n) = m \cdot n$
so $\text{lcm}(m,n) = m \cdot n$

$|\langle(\bar{1},\bar{1})\rangle| = \text{lcm}(m,n) = mn$

So, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(\bar{1},\bar{1})\rangle$, and it has order mn, as does $\mathbb{Z}_{mn}$

If two cyclic groups have the same order then they are isomorphic

since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Q3

a) take $g_1, g_2 \in G$, and note the binary operator on G is composition

$$\begin{aligned} \text{inn}_{g_1} \circ \text{inn}_{g_2} &= \text{inn}_{g_1}(\text{inn}_{g_2}) \\ &= \text{inn}_{g_1}(g_2 x g_2^{-1}) \\ &= g_1 g_2 x g_2^{-1} g_1^{-1} \\ &= g_1 g_2 x (g_1 g_2)^{-1} \\ &= \text{inn}_{g_1 g_2} \end{aligned}$$

This satisfies the definition of homomorphism dfn 4.2

b) $\mathrm{Inn} : G \to \cancel{\mathrm{Aut}(G)} \cancel{\to} G$

$g \mapsto \cancel{\varphi_g} \cancel{\mapsto} gxg^{-1} = x$

$\mathrm{Inn} : G \to G$

$g \mapsto gxg^{-1} = x$ (forall $x \in G$)

$\underbrace{gx = xg \quad \forall x \in G}$

this is the definition of the $C(G)$

c) the centre of G, $C(G) := \{g \in G : xg = gx \ \forall x \in G\}$

- $e \in C(G)$, so $C(G) \neq \emptyset$
- take $x \in C(G)$, $\forall g \in G$:

$$gx^{-1} = x^{-1}xgx^{-1}$$
$$= x^{-1}gxx^{-1}$$
$$= x^{-1}g$$

so, x^{-1} commutes with g.

by prop 5.3, $C(G) \leqslant G$