(Q1) Consider the group $(\mathbb{Z}/p\mathbb{Z})^\times$. The only subgroups of $(\mathbb{Z}/p\mathbb{Z})^\times$ have an order of that divides $p-1$ (the order of the group $(\mathbb{Z}/p\mathbb{Z})^\times$).

Note that since $p \nmid a$, it is congruent mod p to some element $b \in (\mathbb{Z}/p\mathbb{Z})^\times$.

$$a \equiv b \pmod{p}.$$

Now the order of b must divide $p-1$. Let o be the order of b:

$$b^o \equiv 1 \pmod{p}$$

Since $o \mid p-1 \Rightarrow \exists m \in \mathbb{Z}^+ : om = p-1$

$b^o \equiv 1 \pmod{p}$

$(b^o)^m = (1)^m \pmod{p}$

$b^{p-1} \equiv 1 \pmod{p}$

Thus, $a^{p-1} \equiv 1 \pmod{p}$ ∎

(Q3) To show that H is a normal subgroup, we have to show that for any $g \in G_1$ and $h \in H$, $(ghg^{-1}) \in H$.

$$ghg^{-1} = gg^{-1}h \quad \text{(since } G_1 \text{ is abelian)}$$

$$= e_{G_2}h = h$$

$h \in H$ (by assumption). Thus, $H \trianglelefteq G_1$ for any subgroup of an abelian group.

Note: Equivalent definitions of normal subgroups.

(i) · For every $g \in G_1$, we have that $gN = Ng$.

(ii) · For every $g \in G_1$ and $n \in N$, $gng^{-1} \in N$.

i → ii Since $gN = Ng$, every element of gN is also an element Ng. For all $g \in G_1$ and $n \in N$, we can find an $n' \in N$ such that $gn = n'g$. Thus, $gn \cdot g^{-1} = n' \cdot g \cdot (g^{-1}) \Rightarrow gng^{-1} = n'$. Since $n' \in N$, $gng^{-1} \in N$.

ii → i For every $g \in G_1$ and $n \in N$, $gng^{-1} = n'$ for some $n' \in N$. Thus, $gng^{-1} \cdot (g) = n' \cdot g \Rightarrow gn = n'g$ and finally $gN = Ng$.

A subgroup H in G_1 is said to be normal if for all $h \in H$ and $g \in G_1$, we have that $(ghg^{-1}) \in H$.

(Q5) Consider a homomorphism $\varphi : G_1 \longrightarrow G_{12}$. We have to show $\text{Ker}(\varphi) \leq G_1$ is a normal subgroup of G_1.

Let $x \in G_1$ and $R \in \text{Ker}(\varphi)$. Now consider $\varphi(x \cdot R \cdot x^{-1})$.

$$\begin{aligned} \varphi(x \cdot R \cdot x^{-1}) &= \varphi(x) \cdot \varphi(R) \cdot \varphi(x^{-1}) \\ &= \varphi(x) \cdot e_{G_{12}} \cdot [\varphi(x)]^{-1} \\ &= \varphi(x) \cdot [\varphi(x)]^{-1} \\ &= e_{G_{12}}. \end{aligned}$$

$\therefore$

Thus, $xRx^{-1} \in \text{Ker}(\varphi)$, and $\text{Ker}(\varphi) \trianglelefteq G_1$.

(Q7)

- If a subgroup $K \leq G_1$ is normal in G_1, then there exists a homomorphism $\varphi : G_1 \to H$ such that $K = \ker(\varphi)$.
- Consider the function $\varphi : G_1 \to G_1 \backslash K$ (Since K is normal $G_1 \backslash K$ is a well-defined group), such that $\varphi(g) = gK$.

First, $\varphi(g_1 \cdot g_2) = (g_1 \cdot g_2)K = (g_1 K) \oplus (g_2 K)$

$= \varphi(g_1) \oplus \varphi(g_2)$

Thus φ is a homomaphism.

- $\ker(\varphi) = ?$.

$\varphi(g) = eK \Rightarrow gK = eK \Rightarrow (e^{-1})(g) \in K$

$\Rightarrow g \in K$.

Thus, $K = \ker(\varphi)$

- The backward direction is as a result of Problem 5 (The kernel is a normal subgroup).

(Q8) Part I:

- First, we prove that $Z(G_1)$ is a subgroup of G_1.

$Z(G_1) = [z \in G_1 : zg = gz, \forall g \in G_1]$

1. Now, $e \in Z(G_1)$ since $e \cdot g = g = g \cdot e$
2. Given $g_1 \in Z(G_1) \Rightarrow g_1 g = g g_1 \quad \forall g \in G_1$
   and $g_2 \in Z(G_1) \Rightarrow g_2 g' = g g_2 \quad \forall g' \in G_1$

- $g_1 g = g g_1 \Rightarrow g = g_1^{-1} g g_1$
- $g_2 g = g g_2 \Rightarrow$

] OMIT

$(g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot (x \cdot g_2)$

$= (g_1 \cdot x) \cdot g_2$

$= (x \cdot g_1) \cdot g_2$

Thus, $(g_1 \cdot g_2) \cdot x = x \cdot (g_1 \cdot g_2)$

$= x \cdot g_1 \cdot g_2$

3. Given $g \in Z(G_1) \Rightarrow gg' = g'g \quad \forall g' \in G_1$
   Now,

- Now we show that $Z(G_1)$ is a normal subgroup.
- That is, for any $g \in G_1$ and $z \in Z(G_1)$ we have to show that $g \cdot z \cdot g^{-1} \in Z(G_1)$

$$g \cdot z \cdot g^{-1} = g \cdot (z \cdot g^{-1}) = g \cdot (g^{-1} \cdot z)$$

$$= (g \cdot g^{-1}) \cdot z = e \cdot z = z \in Z(G_1).$$

Thus $Z(G_1) \trianglelefteq G_1$.

- Part II:

If $G_1 \backslash Z(G_1)$ is cyclic, then there exists $x \in G_1$ such that $G_1 \backslash Z(G_1) = \langle x Z(G_1) \rangle$. Thus for any $g \in G_1$, there exists $m \in \mathbb{Z}$ such that $gZ(G_1) = x^m Z(G_1) \Rightarrow (x^m)^{-1}(g) \in Z(G_1)$

$(x^{-m})(g) \in Z(G_1) \Rightarrow \forall n \in G_1$, we have:

$(x^{-m})(g)(n) = (n)(g)(x^{-m})$.

Now, let $g = (x^m)(a) = (a)(x^m)$ Substitute $n = e$ in the above equation.

$(x^{-m})(x^m)(a)(n) = (n)(a)(x^m)(x^{-m})$

$(a)(n) = (n)(a) \Rightarrow G_1$ is abelian.

(Q10) In our proof, we use the following result: In a group G_1, if $|G_1| = p^n$ where p is a prime and $n \in \mathbb{Z}^+$, then the center of G_1 is nontrivial.

Proof.

- Since $|G_1| = p^2$, and $Z(G_1)$ is nontrivial, we have two options:

1. $|Z(G_1)| = p^2$. But since $|G_1| = p^2$, $Z(G_1) = G_1 \Rightarrow G_1$ is abelian.
2. $|Z(G_1)| = p$. Thus, by lagranges theorem, $[G_1 : Z(G_1)] = |G_1 \setminus Z(G_1)| = p$. Since the order of the group $G_1 \setminus Z(G_1)$ is cyclic. Thus, by applying the theorem proved in (Q8), we get G_1 is abelian.

(Q9) Lemma 3.1 may be rephrased as:
Let G_1 be a group and H be a subgroup of G_1. If aH and bH are two cosets of H in G_1, and if $(aH) \cap (bH) \neq \emptyset$, then we have that $aH = bH$.

If $(aH) \cap (bH) \neq \emptyset$, then there exists at least one $s \in (aH)$ and $s \in (bH)$.
Since $s \in (aH)$, $aH = sH$. Similarly, since $s \in (bH)$, $bH = sH$. Thus, $aH = sH = bH$ and $aH = bH$. Q.E.D.

The above proof uses the following lemma:
Let G_1 be a group and H be a subgroup of G_1. For any $a' \in aH$ $(a \in G_1)$, we have that $a'H = aH$.
Proof: Since $a' \in aH$, there exists $h' \in H$ such that $a' = ah'$. $aH = [ah : h \in H]$ and $a'H = [a'h : h \in H] = [(ah')(h) : h \in H]$ $= [a(h'h) : h \in H] = [ag : g \in H]$. Note that $(h'h) \in H$ since H is a subgroup and is closed under multiplication.

Note: $|aH| = |H| = |a'H|$ for any $a \in G_1$ and $a' \in G_1$.

Define a function $\varphi : H \to aH$ $(a \in G)$, such that $\varphi(h) = ah$. We will show φ is a bijection.

- $\varphi(h_2) = \varphi(h_1)$
  $\Rightarrow ah_2 = ah_1$
  $\Rightarrow a^{-1}(ah_2) = a^{-1}(ah_1)$
  $\Rightarrow (a^{-1}a)h_2 = (a^{-1}a)h_1$
  $\Rightarrow eh_2 = eh_1$
  $\Rightarrow h_2 = h_1$.
  Thus φ is injective.
- Given any $\alpha \in aH$ such that, $\alpha = ah'$ for a $h' \in H$. Note that $h' \in H$ is such that $\varphi(h') = \alpha = ah'$. Thus φ is surjective.

Since there exists a bijection between the sets H and aH, they must be of the same size.