1. Prove the unit quaternion group Q_8 is not a semidirect product of its proper subgroups.

   Solution: If G is a semindirect product of its proper subgroups H and K, then it follows $H \cap K = \{1\}$.

   If $|H| = 2$, since -1 is the unique element of order 2, $H = \{1, -1\}$. If $|H| = 4$, then Cauchy's Theorem implies H contains an element of order 2, which again has to be -1, so $-1 \in H$ in any case. Similarly, $-1 \in K$ in any case. This implies $-1 \in H \cap K$, contradiction, so Q_8 is not a semidirect product of its proper subgroups.

2. Classify isomorphic classes of groups of order 28.

   Solution: let G be a group of order 28. By Sylow Theorem, we know G has a Sylow 7-subgroup H and a Sylow 2-subgroup K, and the number of Sylow 7-subgroup is 1, so H is a normal subgroup of G.

   $|H| = 7$ and $|K| = 4$ are relatively prime, so $H \cap K = \{1\}$.

   $|HK| = \frac{|H| \times |K|}{|H \cap K|} = 28 = |G|$, so $G = HK$.

   We conclude $G = H \rtimes K$.

   $|H| = 7$ implies $H \cong \mathbb{Z}/7\mathbb{Z}$, $|K| = 4$ implies $K \cong \mathbb{Z}/4\mathbb{Z}$ or $K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   Case 1. If $K \cong \mathbb{Z}/4\mathbb{Z}$, $G \cong \mathbb{Z}/7\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$ for some $\phi : \mathbb{Z}/4\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. Note that $\bar{6} = \overline{-1}$ is the only element of order 2 in $(\mathbb{Z}/7\mathbb{Z})^*$.

   ϕ is determined by $\phi(\bar{1})$, and $|\bar{1}| = 4$, so $|\phi(\bar{1})|$ divides 4. Also $|\phi(\bar{1})|$ divides $|Aut(\mathbb{Z}/4\mathbb{Z})| = 6$ implies $|\phi(\bar{1})|$ is 1 or 2.

   Case 1.(a): If $|\phi(\bar{1})| = 1$, then ϕ is the trivial map, $G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

   Case 1.(b): If $|\phi(\bar{1})| = 2$, then $\phi(\bar{1}) = \bar{6} = \overline{-1}$. $\phi(\bar{m}) : \mathbb{Z}/7\mathbb{Z} \longrightarrow \mathbb{Z}/7\mathbb{Z}$ is then defined by $\phi(\bar{m})(\bar{k}) = \overline{(-1)^m k}$. In this case we obtain a semidirect product different from direct product.

   Case 2. If $K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $G \cong \mathbb{Z}/7\mathbb{Z} \rtimes_\phi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ for some $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

   Note $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong K_4 = \{1, a, b, c\}$, so we can regard ϕ as a homomorphism $K_4 \longrightarrow (\mathbb{Z}/7\mathbb{Z})^*$. Note $|a| = |b| = |c| = 2$, so $|\phi(a)|, |\phi(b)|, |\phi(c)| \in \{1, 2\}$. By the relations $ab = c$, $\phi(a)\phi(b) = \phi(c)$, it has to be the case $\phi(a) = \phi(b) = \phi(c) = \bar{1}$ or two of $\phi(a), \phi(b), \phi(c)$ is $\overline{-1}$ and the remaining is $\bar{1}$.

Case 2.(a): If $\phi(a) = \phi(b) = \phi(c) = \bar{1}$, we get ϕ is the trivial group. so $G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Case 2.(b): If two of $|\phi(a)|, |\phi(b)|, |\phi(c)|$ is $\overline{-1}$ and the remaining is $\bar{1}$, ϕ is not trivial and we will get a semidirect product that is not isomorphic to direct product.

3. A **short exact sequence** of groups is a sequence of groups and homomorphisms:

$$\{1\} \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \{1\}$$

such that the image of each map equals to the kernel of the next map. For example, $\mathrm{Im}(f) = \ker(g)$. Given the above short exact sequence, prove:

(i). $f : A \longrightarrow B$ is injective

(ii). $g : B \longrightarrow C$ is surjective

(iii). $B/f(A) \cong C$

(iv). Given two groups G and G' and a homomorphism $\phi : G' \longrightarrow Aut(G)$, prove the following is a short exact sequence:

$$\{1\} \longrightarrow G \xrightarrow{i_1} G \rtimes_\phi G' \xrightarrow{\pi_2} G' \longrightarrow \{1\}$$

where $i_1(g) = (g, 1')$ and $\pi_2(g, g') = g'$ for any $g \in G, g' \in G'$

Solution:

(i). $\ker f$ is the image of the map $\{1\} \longrightarrow A$, which is $\{1\}$, so f is injective.

(ii). $\mathrm{Im}(g)$ is the kernel of $C \longrightarrow \{1\}$, which is C, so g is surjective.

(iii). $f(A) = \mathrm{Im}(A) = \ker(g)$, and g is surjective, so by the First Isomorphism Theorem:

$$B/f(A) = B/\ker(g) \cong C$$

(iv). The image of $\{1\} \longrightarrow G$ is $\{1\}$, and $\ker(i_1) = \{(g, 1') \in G \rtimes_\phi G' | i_1(g, 1') = (1, 1')\} = \{1\}$.

$\mathrm{Im}(i_1) = \{(g, 1') \in G \rtimes_\phi G' | g \in G\}$ and $\ker(\pi_2) = \{(g, g') \in G \rtimes_\phi G' | \pi_2(G \rtimes_\phi G') = 1'\} = \{(g, 1') \in G \rtimes_\phi G' | g \in G\}$

$\mathrm{Im}(\pi_2) = G'$ since π_2 is surjective, and $\ker(G' \longrightarrow \{1\}) = G'$

4. R is a ring with the property that $x^2 = x$ for any $x \in R$. Prove $x = -x$ for all $x \in R$.

   Solution:

$$
\begin{aligned}
(x+x)^2 &= x + x \\
x^2 + x^2 + x^2 + x^2 &= x + x \\
x + x + x + x &= x + x \\
x + x &= 0 \\
x &= -x
\end{aligned}
$$

5. X is a nonempty set. Let $\mathcal{P}(X)$ be the set of all subsets of X. Define two compositions on $\mathcal{P}(X)$ by:

$$A + B = (A - B) \cup (B - A), A \times B = A \cap B$$

   Prove $\mathcal{P}(X)$ with the above two compositions is a commutative ring.

   Solution:

   First verify $(\mathcal{P}(X), +)$ is an abelian group:

   - Associativity: For any $S \in \mathcal{P}(X)$, denote $\overline{S} = X - S$. Then for any $A, B, C \in \mathcal{P}(X)$:

$$
\begin{aligned}
(A+B)+C &= ((A+B) \cap \overline{C}) \cup (C \cap \overline{A+B}) \\
&= (((A \cap \overline{B}) \cup (\overline{A} \cap B)) \cap \overline{C}) \cup (C \cap \overline{(A \cap \overline{B}) \cup (\overline{A} \cap B)}) \\
&= (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (C \cap ((\overline{A} \cap \overline{B}) \cup (A \cap B))) \\
&= (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)
\end{aligned}
$$

     Similarly, we can also get

$$A + (B + C) = (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C)$$

     So we conclude $(A + B) + C = A + (B + C)$.

   - The zero element is $\emptyset$: For any $A\mathcal{P}(X)$

$$
\begin{aligned}
A + \emptyset &= (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A \\
\emptyset + A &= (\emptyset - A) \cup (A - \emptyset) = \emptyset \cup A = A
\end{aligned}
$$

- The additive inverse of $A \in \mathcal{P}(X)$ is A:

$$A + A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$$

- Commutativity: For any $A, B \in \mathcal{P}(X)$:

$$A + B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B + A$$

Next we verify $\times$ is associative, commutative and the existence of unit element:

- Associativity: For any $A, B, C \in \mathcal{P}(X)$:

$$(A \times B) \times C = (A \cap B) \cap C = A \cap (B \cap C) = A \times (B \times C)$$

- The unit element is $X \in \mathcal{P}(X)$: For any $A \in \mathcal{P}(X)$,

$$\begin{aligned} A \times X &= A \cap X = A \\ X \times A &= X \cap A = A \end{aligned}$$

- Commutativity: For any $A, B \in \mathcal{P}(X)$,

$$A \times B = A \cap B = B \cap A = B \times A$$

Eventually we verify the distributive law:

- For any $A, B, C \in \mathcal{P}(X)$,

$$\begin{aligned} A \times (B + C) &= A \cap ((B - C) \cup (C - B)) \\ &= (A \cap (B - C)) \cup (A \cap (C - B)) \\ &= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\ &= (A \cap B) + (A \cap C) \\ &= A \times B + A \times C \end{aligned}$$

  By commutitivity,
  $(B + C) \times A = A \times (B + C) = A \times B + A \times C = B \times A + C \times A.$