Question 1: (a) Prove that the order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

- Let σ be a permutation of a finite set S.
- Let σ be written as a product of disjoint cycles: $\sigma = c_1 c_2 \dots c_k$.
- Since the cycles are disjoint, they commute with each other.
- Let the length of the cycle c_i be l_i. This means that the order of the cycle c_i is l_i.
- For any integer m, $\sigma^m = (c_1 c_2 \dots c_k)^m = c_1^m c_2^m \dots c_k^m$.
- For σ^m to be the identity permutation, each c_i^m must be the identity permutation.
- This implies that m must be a multiple of the order of each cycle c_i, i.e., m must be a multiple of l_i for all $i = 1,2, \dots, k$.
- The smallest positive integer m for which this holds is the least common multiple (LCM) of the lengths of the cycles.
- Therefore, the order of σ is lcm$(l_1, l_2, \dots, l_k)$.

(b) (i) Let S_3 denote the symmetric group of degree n. In S_3, find elements α and β such that |α| = 2, |β| = 2 and |αβ| = 3.

- In S_3, elements of order 2 are transpositions (cycles of length 2).
- Let $\alpha = (1\ 2)$. Its order is 2.
- Let $\beta = (1\ 3)$. Its order is 2.
- Now, let's find the product $\alpha\beta$: $\alpha\beta = (1\ 2)(1\ 3)$. To compute this, start with 1: $1 \xrightarrow{3} 3 \to 3$. So 1 goes to 3. Now 3: $3 \xrightarrow{1} 1 \xrightarrow{2} 2$. So 3 goes to 2. Now 2: $2 \to 2 \xrightarrow{1} 1$. So 2 goes to 1.
- Thus, $\alpha\beta = (1\ 3\ 2)$.

- The order of $(1\ 3\ 2)$ is 3, which is the length of the cycle.
- Therefore, $\alpha = (1\ 2)$ and $\beta = (1\ 3)$ satisfy the given conditions.

(ii) Let β ∈ S_7 and β^4 = (2 1 4 3 5 6 7). Then find β.

- Let $\gamma = (2\ 1\ 4\ 3\ 5\ 6\ 7)$.
- The length of γ is 7. So, $|\gamma| = 7$.
- We are given $\beta^4 = \gamma$.
- Since the order of γ is 7, we know that $(\beta^4)^7 = \beta^{28} = e$ (identity).
- Also, since $\beta^4 = \gamma$, then $\beta = \gamma^k$ for some integer k such that $4k \equiv 1 \pmod 7$.
- We need to find the inverse of 4 modulo 7. $4 \times 1 = 4 \pmod 7$ $4 \times 2 = 8 \equiv 1 \pmod 7$
- So, $k = 2$.
- Therefore, $\beta = \gamma^2$.
- Now, we compute $\gamma^2 = (2\ 1\ 4\ 3\ 5\ 6\ 7)^2$. $2 \xrightarrow{1} 1 \xrightarrow{4} 4$ $1 \xrightarrow{4} 4 \xrightarrow{3} 3$ $4 \xrightarrow{3} 3 \xrightarrow{5} 5$ $3 \xrightarrow{5} 5 \xrightarrow{6} 6$ $5 \xrightarrow{6} 6 \xrightarrow{7} 7$ $6 \xrightarrow{7} 7 \xrightarrow{2} 2$ $7 \xrightarrow{2} 2 \xrightarrow{1} 1$
- So, $\beta = (2\ 4\ 5\ 7\ 1\ 3\ 6)$.

(c) (i) Give two reasons to show that the set of odd permutations in S_n is not a subgroup of S_n.

- Reason 1: A subgroup must contain the identity element. The identity permutation is an even permutation (it can be written as a product of an even number of transpositions, e.g., zero transpositions). The set of odd permutations does not contain the identity element.
- Reason 2: A subgroup must be closed under the group operation. The product of two odd permutations is an even permutation. For example, if σ and τ are odd permutations, then sgn$(\sigma) = -1$ and

sgn(τ) $= -1$. Then sgn($\sigma\tau$) $=$ sgn(σ)sgn(τ) $= (-1)(-1) = 1$. Since the product of two odd permutations is an even permutation, the set of odd permutations is not closed under multiplication.

(ii) Define even and odd permutations and show that the set of even permutations in S_n is a subgroup of S_n.

- **Definition of Even and Odd Permutations:**
  - A permutation $\sigma \in S_n$ is called an **even permutation** if it can be expressed as a product of an even number of transpositions.
  - A permutation $\sigma \in S_n$ is called an **odd permutation** if it can be expressed as a product of an odd number of transpositions.
- **Proof that the set of even permutations in S_n is a subgroup of S_n:** Let A_n be the set of all even permutations in S_n. We need to show that A_n satisfies the three subgroup criteria:
  a. **Non-empty:** The identity permutation e can be written as a product of zero transpositions (which is an even number). Thus, $e \in A_n$, so A_n is non-empty.
  b. **Closure:** Let $\sigma, \tau \in A_n$. This means σ can be written as a product of an even number of transpositions, say k transpositions, and τ can be written as a product of an even number of transpositions, say m transpositions. Then the product $\sigma\tau$ can be written as a product of $k + m$ transpositions. Since k and m are both even, $k + m$ is also even. Therefore, $\sigma\tau$ is an even permutation, so $\sigma\tau \in A_n$.
  c. **Existence of Inverses:** Let $\sigma \in A_n$. This means $\sigma = \tau_1\tau_2 \dots \tau_k$ where k is an even number and τ_i are transpositions. The inverse of σ is $\sigma^{-1} = (\tau_1\tau_2 \dots \tau_k)^{-1} = \tau_k^{-1} \dots \tau_2^{-1}\tau_1^{-1}$. Since each transposition is its own inverse ($\tau_i^{-1} = \tau_i$), we have $\sigma^{-1} = \tau_k \dots \tau_2\tau_1$. This is also a product of k transpositions. Since k is even, σ^{-1} is also an even permutation. Therefore, $\sigma^{-1} \in A_n$.

- Since A_n satisfies all three conditions, it is a subgroup of S_n. This subgroup is called the alternating group of degree n.

Question 2: (a) (i) Let a be an element in a group G such that |a| = 15. Find all left cosets of ⟨a³⟩ in ⟨a⟩.

- Given $|a| = 15$. The cyclic group generated by a is $\langle a \rangle = \{e, a, a^2, \dots, a^{14}\}$. The order of $\langle a \rangle$ is 15.
- Let $H = \langle a^3 \rangle$. The elements of H are powers of a^3. Since $|a| = 15$, the order of a^3 is $15/\gcd(3,15) = 15/3 = 5$. So, $H = \{(a^3)^0, (a^3)^1, (a^3)^2, (a^3)^3, (a^3)^4\} = \{e, a^3, a^6, a^9, a^{12}\}$.
- The index of H in $\langle a \rangle$ is $[\langle a \rangle : H] = |\langle a \rangle|/|H| = 15/5 = 3$.
- This means there will be 3 distinct left cosets.
- The cosets are of the form gH where $g \in \langle a \rangle$.
- The first coset is $eH = H = \{e, a^3, a^6, a^9, a^{12}\}$.
- To find the next coset, pick an element from $\langle a \rangle$ not in H, for example, a. $aH = \{a \cdot e, a \cdot a^3, a \cdot a^6, a \cdot a^9, a \cdot a^{12}\} = \{a, a^4, a^7, a^{10}, a^{13}\}$.
- To find the third coset, pick an element from $\langle a \rangle$ not in H or aH, for example, a^2. $a^2H = \{a^2 \cdot e, a^2 \cdot a^3, a^2 \cdot a^6, a^2 \cdot a^9, a^2 \cdot a^{12}\} = \{a^2, a^5, a^8, a^{11}, a^{14}\}$.
- We have found 3 distinct cosets, which matches the index. These are all the left cosets of $\langle a^3 \rangle$ in $\langle a \rangle$.
- The left cosets are:
  - $H = \{e, a^3, a^6, a^9, a^{12}\}$
  - $aH = \{a, a^4, a^7, a^{10}, a^{13}\}$
  - $a^2H = \{a^2, a^5, a^8, a^{11}, a^{14}\}$

(ii) State and prove Lagrange's theorem.

- **Lagrange's Theorem:** If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. Furthermore, the number of distinct left (or right) cosets of H in G is $|G|/|H|$.
- **Proof:**

d. Let G be a finite group and H be a subgroup of G.

e. Consider the set of all distinct left cosets of H in G. Let these be $a_1H, a_2H, \ldots, a_kH$, where k is the index of H in G, denoted by $[G: H]$.

f. We know that the set of all left cosets of H in G forms a partition of G. This means that every element of G belongs to exactly one left coset.

g. We also know that for any $a \in G$, the mapping $h \mapsto ah$ is a bijection from H to aH. This implies that every left coset has the same number of elements as H. That is, for any i, $|a_iH| = |H|$.

h. Since the distinct left cosets partition G, the sum of the number of elements in each distinct coset must be equal to the total number of elements in G.

i. Therefore, $|G| = |a_1H| + |a_2H| + \cdots + |a_kH|$.

j. Since each coset has $|H|$ elements, we have $|G| = |H| + |H| + \cdots + |H|$ (k times).

k. So, $|G| = k \cdot |H|$.

l. This implies that $k = |G|/|H|$.

m. Since k is an integer (the number of distinct cosets), $|H|$ must divide $|G|$.

(b) Suppose that G is a group with more than one element and G has no proper, non-trivial subgroups. Prove that |G| is prime.

- Let G be a group with more than one element, so $|G| > 1$.

- Assume G has no proper, non-trivial subgroups. This means the only subgroups of G are the trivial subgroup $\{e\}$ and G itself.
- Let a be any element in G such that $a \neq e$.
- Consider the cyclic subgroup generated by a, denoted by $\langle a \rangle$.
- Since $a \neq e$, $\langle a \rangle$ is not the trivial subgroup $\{e\}$.
- Since G has no proper, non-trivial subgroups, $\langle a \rangle$ must be equal to G.
- This means that G is a cyclic group generated by any non-identity element a.
- Now, we need to show that the order of G (which is the order of a) must be a prime number.
- Assume, for the sake of contradiction, that $|G|$ is not prime. Since $|G| > 1$, it must be either 1 (which contradicts $|G| > 1$) or a composite number.
- If $|G|$ is a composite number, then $|G| = mn$ for some integers $m, n > 1$.
- Since $G = \langle a \rangle$ and $|G| = mn$, the order of a is mn.
- Consider the element a^m.
- The order of a^m is $|a|/\gcd(m, |a|) = mn/\gcd(m, mn) = mn/m = n$.
- Since $n > 1$, $a^m \neq e$.
- Consider the subgroup $\langle a^m \rangle$. Its order is n.
- Since $n > 1$, $\langle a^m \rangle$ is not the trivial subgroup.
- Since $m > 1$, $n = |G|/m < |G|$, so $\langle a^m \rangle$ is a proper subgroup of G.
- Thus, $\langle a^m \rangle$ is a proper, non-trivial subgroup of G.

- This contradicts our initial assumption that G has no proper, non-trivial subgroups.
- Therefore, our assumption that $|G|$ is not prime must be false.
- Hence, $|G|$ must be a prime number.

(c) Let C be the group of non-zero complex numbers under multiplication and let H = {a + bi ∈ C | $a^2 + b^2 = 1$}. Give a geometrical description of the coset (3 + 4i)H. Give a geometrical description of the coset (c + di)H.

- Let C^* be the group of non-zero complex numbers under multiplication.
- Let $H = \{a + bi \in C^* \mid a^2 + b^2 = 1\}$. Geometrically, H represents the set of all complex numbers with modulus 1. This is the unit circle centered at the origin in the complex plane.
- **Geometrical description of the coset $(3 + 4i)H$:**
  - A coset $(3 + 4i)H$ consists of all elements of the form $(3 + 4i)z$, where $z \in H$.
  - Let $z = x + yi$ with $x^2 + y^2 = 1$.
  - The modulus of $(3 + 4i)$ is $|3 + 4i| = \sqrt{3^2 + 4^2} = \sqrt{9 + 16} = \sqrt{25} = 5$.
  - When we multiply two complex numbers, their moduli multiply and their arguments add.
  - So, for any $w = (3 + 4i)z$, we have $|w| = |3 + 4i| \cdot |z|$.
  - Since $|z| = 1$, we have $|w| = 5 \cdot 1 = 5$.
  - Therefore, every complex number in the coset $(3 + 4i)H$ has a modulus of 5.

- Geometrically, the coset $(3+4i)H$ represents a circle centered at the origin with a radius of 5. This circle passes through the point $3+4i$.

- **Geometrical description of the coset $(c+di)H$:**
    - Let $c+di$ be any non-zero complex number.
    - Let its modulus be $r = |c+di| = \sqrt{c^2+d^2}$. Since $c+di \neq 0$, $r > 0$.
    - A coset $(c+di)H$ consists of all elements of the form $(c+di)z$, where $z \in H$.
    - For any $w = (c+di)z$, we have $|w| = |c+di| \cdot |z|$.
    - Since $|z| = 1$, we have $|w| = r \cdot 1 = r$.
    - Therefore, every complex number in the coset $(c+di)H$ has a modulus of $r = \sqrt{c^2+d^2}$.
    - Geometrically, the coset $(c+di)H$ represents a circle centered at the origin with a radius of $r = \sqrt{c^2+d^2}$. This circle passes through the point $c+di$.

Question 3: (a) (i) Let G be a group and H be its subgroup. Prove that if H has index 2 in G, then H is normal in G.

- **Proof:**
    - Let G be a group and H be a subgroup of G.
    - Given that the index of H in G, denoted by $[G:H]$, is 2.
    - This means there are exactly two distinct left cosets of H in G, and exactly two distinct right cosets of H in G.
    - One of these left cosets is $eH = H$.
    - One of these right cosets is $He = H$.

- Since the cosets partition G, the union of the two left cosets must be G, and the union of the two right cosets must be G.
- So, $G = H \cup xH$ for some $x \in G$ and $x \notin H$.
- And $G = H \cup Hy$ for some $y \in G$ and $y \notin H$.
- Since $x \notin H$, xH must be the other left coset, which is $G \backslash H$.
- Similarly, since $y \notin H$, Hy must be the other right coset, which is $G \backslash H$.
- Therefore, $xH = G \backslash H$ and $Hy = G \backslash H$.
- This implies that $xH = Hy$.
- Now, we need to show that $gH = Hg$ for all $g \in G$ to prove that H is normal.
  - Case 1: If $g \in H$.
    - Then $gH = H$ (since H is a subgroup).
    - And $Hg = H$ (since H is a subgroup).
    - So, $gH = Hg$.
  - Case 2: If $g \notin H$.
    - Since there are only two left cosets, gH must be the other coset, i.e., $gH = G \backslash H$.
    - Similarly, since there are only two right cosets, Hg must be the other coset, i.e., $Hg = G \backslash H$.
    - Therefore, $gH = Hg$.
- Since $gH = Hg$ for all $g \in G$, H is a normal subgroup of G.

(ii) If a group G has a unique subgroup H of some finite order, then show that H is normal in G.

- **Proof:**
  - Let G be a group and H be a unique subgroup of G of some finite order, say $n = |H|$.
  - To prove that H is normal in G, we need to show that for every $g \in G$, $gHg^{-1} = H$.
  - Consider the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ for an arbitrary $g \in G$.
  - We know that gHg^{-1} is a subgroup of G. This is a standard result:
    - Identity: $geg^{-1} = e \in gHg^{-1}$.
    - Closure: Let $x, y \in gHg^{-1}$. Then $x = gh_1g^{-1}$ and $y = gh_2g^{-1}$ for some $h_1, h_2 \in H$. $xy = (gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1}$. Since $h_1h_2 \in H$, $xy \in gHg^{-1}$.
    - Inverse: Let $x \in gHg^{-1}$. Then $x = ghg^{-1}$ for some $h \in H$. $x^{-1} = (ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1}$. Since $h^{-1} \in H$, $x^{-1} \in gHg^{-1}$.
  - Thus, gHg^{-1} is a subgroup of G.
  - Now, let's consider the order of gHg^{-1}.
  - The mapping $\phi: H \to gHg^{-1}$ defined by $\phi(h) = ghg^{-1}$ is an isomorphism.
    - It is a homomorphism: $\phi(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \phi(h_1)\phi(h_2)$.
    - It is injective: If $\phi(h_1) = \phi(h_2)$, then $gh_1g^{-1} = gh_2g^{-1}$. By cancellation, $h_1 = h_2$.
    - It is surjective by definition of gHg^{-1}.
  - Since ϕ is an isomorphism, $|gHg^{-1}| = |H| = n$.

- So, for every $g \in G$, gHg^{-1} is a subgroup of G of order n.
- However, we are given that H is the *unique* subgroup of G of order n.
- Therefore, gHg^{-1} must be equal to H for all $g \in G$.
- This shows that H is a normal subgroup of G.

(b) (i) Prove that a factor group of a cyclic group is cyclic. Is converse true? Justify your answer.

- **Proof that a factor group of a cyclic group is cyclic:**
  - Let G be a cyclic group. This means $G = \langle a \rangle$ for some element $a \in G$.
  - Let N be a normal subgroup of G.
  - Consider the factor group $G/N = \{gN \mid g \in G\}$.
  - We want to show that G/N is cyclic. This means we need to find an element in G/N that generates the entire factor group.
  - Consider the coset aN.
  - Let gN be an arbitrary element in G/N.
  - Since $g \in G$ and $G = \langle a \rangle$, g can be written as a^k for some integer k.
  - Therefore, $gN = a^k N$.
  - By the definition of multiplication in factor groups, $(aN)^k = a^k N$.
  - So, every element gN in G/N can be expressed as a power of aN.
  - Thus, $G/N = \langle aN \rangle$.
  - Therefore, G/N is a cyclic group.

- **Is converse true? Justify your answer.**
    - The converse is **not true**.
    - **Justification:** The converse states that if a factor group of a group G is cyclic, then G must be cyclic. This is false.
    - Consider the group S_3, the symmetric group of degree 3.
        - S_3 is not a cyclic group because its elements have orders 1, 2, or 3, and there is no element of order $|S_3| = 6$. (For example, S_3 is non-abelian, while all cyclic groups are abelian).
    - Consider the alternating group $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$, which is a normal subgroup of S_3.
        - The order of A_3 is 3.
        - The index of A_3 in S_3 is $[S_3 : A_3] = |S_3|/|A_3| = 6/3 = 2$.
    - The factor group S_3/A_3 has order 2.
    - Any group of order 2 is cyclic. For example, $S_3/A_3 \cong Z_2$.
    - So, S_3/A_3 is a cyclic group.
    - However, S_3 itself is not cyclic.
    - This provides a counterexample, showing that the converse is false.

(ii) Let G be a group and let Z(G) be the center of G. If G/Z(G) is cyclic, then show that G is Abelian.

- **Proof:**
    - Let G be a group and $Z(G)$ be its center.
    - Assume that $G/Z(G)$ is cyclic.

- Since $G/Z(G)$ is cyclic, there exists an element $aZ(G) \in G/Z(G)$ such that $G/Z(G) = \langle aZ(G) \rangle$.
- This means that every element in $G/Z(G)$ can be written as a power of $aZ(G)$.
- Let x, y be any two arbitrary elements in G.
- Consider their cosets $xZ(G)$ and $yZ(G)$ in $G/Z(G)$.
- Since $G/Z(G)$ is cyclic and generated by $aZ(G)$, there exist integers k and m such that:
    - $xZ(G) = (aZ(G))^k = a^k Z(G)$
    - $yZ(G) = (aZ(G))^m = a^m Z(G)$
- From $xZ(G) = a^k Z(G)$, it implies that x and a^k belong to the same coset. So, $x = a^k z_1$ for some $z_1 \in Z(G)$.
- Similarly, from $yZ(G) = a^m Z(G)$, it implies that $y = a^m z_2$ for some $z_2 \in Z(G)$.
- Now, we need to show that G is Abelian, i.e., $xy = yx$ for all $x, y \in G$.
- $xy = (a^k z_1)(a^m z_2)$
- Since $z_1 \in Z(G)$, z_1 commutes with all elements in G, including a^m. So, $z_1 a^m = a^m z_1$.
- $xy = a^k (z_1 a^m) z_2 = a^k (a^m z_1) z_2 = a^{k+m} z_1 z_2$.
- Similarly, consider yx:
- $yx = (a^m z_2)(a^k z_1)$
- Since $z_2 \in Z(G)$, z_2 commutes with all elements in G, including a^k. So, $z_2 a^k = a^k z_2$.
- $yx = a^m (z_2 a^k) z_1 = a^m (a^k z_2) z_1 = a^{m+k} z_2 z_1$.

- Since $k + m = m + k$ and z_1, z_2 are elements of $Z(G)$, they commute with each other ($z_1 z_2 = z_2 z_1$).
- Therefore, $xy = a^{k+m} z_1 z_2 = a^{m+k} z_2 z_1 = yx$.
- Since x and y were arbitrary elements of G, this proves that G is Abelian.

(c) (i) Let ϕ be a group homomorphism from group G_1 to group G_2 and H be a subgroup of G_1. Show that if H is cyclic, then ϕ(H) is cyclic.

- **Proof:**
  - Let $\phi: G_1 \rightarrow G_2$ be a group homomorphism.
  - Let H be a subgroup of G_1.
  - Assume H is cyclic. This means $H = \langle h \rangle$ for some element $h \in H$.
  - We need to show that $\phi(H)$ is cyclic. This means we need to find an element in $\phi(H)$ that generates it.
  - Consider the element $\phi(h) \in G_2$. We will show that $\phi(H) = \langle \phi(h) \rangle$.
  - Let y be an arbitrary element in $\phi(H)$.
  - By definition of $\phi(H)$, there exists an element $x \in H$ such that $y = \phi(x)$.
  - Since H is cyclic and generated by h, x can be written as h^k for some integer k.
  - So, $y = \phi(h^k)$.
  - Since ϕ is a homomorphism, $\phi(h^k) = (\phi(h))^k$.
  - Therefore, $y = (\phi(h))^k$.

- This shows that every element y in $\phi(H)$ can be expressed as a power of $\phi(h)$.
- Thus, $\phi(H) = \langle \phi(h) \rangle$.
- Hence, $\phi(H)$ is a cyclic group.

(ii) How many homomorphisms are there from Z_{20} to Z_8? How many are there onto Z_8?

- **Number of homomorphisms from Z_{20} to Z_8:**
  - Let $\phi: Z_{20} \to Z_8$ be a homomorphism.
  - A homomorphism from a cyclic group is completely determined by the image of its generator.
  - Let the generator of Z_{20} be 1 (under addition modulo 20).
  - Let $\phi(1) = k$, where $k \in Z_8$.
  - For a homomorphism ϕ, the order of $\phi(g)$ must divide the order of g. So, $|\phi(1)|$ must divide $|1| = 20$.
  - Also, $\phi(1) = k \in Z_8$, so $|k|$ must divide $|Z_8| = 8$.
  - Therefore, $|k|$ must divide both 20 and 8. So, $|k|$ must divide $\gcd(20,8) = 4$.
  - The possible orders for $k \in Z_8$ are 1, 2, 4, 8.
  - We need to find elements $k \in Z_8$ whose order divides 4.
    - Elements of order 1: 0 (since $|0| = 1$)
    - Elements of order 2: 4 (since $2 \times 4 = 8 \equiv 0 \pmod 8$)
    - Elements of order 4: $2,6$ (since $4 \times 2 = 8 \equiv 0 \pmod 8$ and $4 \times 6 = 24 \equiv 0 \pmod 8$)
    - Elements of order 8: $1,3,5,7$ (their orders do not divide 4, so they are not valid choices for $\phi(1)$).

- The possible values for $\phi(1)$ are $0,2,4,6$.
- Each of these choices for $\phi(1)$ uniquely defines a homomorphism.
- Therefore, there are **4** homomorphisms from Z_{20} to Z_8.

- **Number of homomorphisms from Z_{20} onto Z_8:**
  - For a homomorphism $\phi: Z_{20} \to Z_8$ to be onto Z_8, its image Im(ϕ) must be equal to Z_8.
  - This means the generator $\phi(1)$ must generate Z_8.
  - The elements that generate Z_8 are those whose order is 8. These are the elements $k \in Z_8$ such that $\gcd(k, 8) = 1$.
  - The generators of Z_8 are $1,3,5,7$.
  - From the previous part, we found that $|\phi(1)|$ must divide $\gcd(20,8) = 4$.
  - The possible orders for $\phi(1)$ are 1, 2, 4.
  - Since none of these orders is 8, it is impossible for $\phi(1)$ to generate Z_8.
  - Therefore, there are **0** homomorphisms from Z_{20} onto Z_8.

Question 4: (a) (i) Suppose that ϕ is a homomorphism from U(30) to U(30) and Ker ϕ = {1,11}. If ϕ(7) = 7, find all the elements of U(30) that map to 7.

- **Understanding U(30):**
  - $U(30)$ is the group of units modulo 30.
  - $U(30) = \{n \in \{1,2,\dots,29\} \mid \gcd(n, 30) = 1\}$.
  - The elements are: $U(30) = \{1,7,11,13,17,19,23,29\}$.
  - $|U(30)| = \phi(30) = 30(1 - 1/2)(1 - 1/3)(1 - 1/5) = 30(1/2)(2/3)(4/5) = 8$.

- **Using properties of homomorphisms:**
  - We are given $\phi: U(30) \to U(30)$ is a homomorphism.
  - Ker $\phi = \{1,11\}$.
  - We are given $\phi(7) = 7$.
  - We need to find all $x \in U(30)$ such that $\phi(x) = 7$.
  - By a property of homomorphisms, if $\phi(a) = y$ and $\phi(b) = y$, then aKer $\phi = b$Ker ϕ. More generally, the set of all elements that map to a specific image y is given by aKer ϕ, where a is any element such that $\phi(a) = y$.
  - Here, $y = 7$ and we know one element that maps to 7 is $a = 7$.
  - So, the set of all elements x such that $\phi(x) = 7$ is 7Ker ϕ.
  - 7Ker $\phi = \{7 \cdot k \pmod{30} \mid k \in$ Ker $\phi\}$.
  - 7Ker $\phi = \{7 \cdot 1 \pmod{30}, 7 \cdot 11 \pmod{30}\}$.
  - $7 \cdot 1 = 7$.
  - $7 \cdot 11 = 77 \equiv 77 - 2 \times 30 = 77 - 60 = 17 \pmod{30}$.
  - Therefore, the elements of $U(30)$ that map to 7 are **{7, 17}**.

(ii) Let ϕ be a homomorphism from a group G_1 to group G_2. Show that ϕ(a) = ϕ(b) iff aKer ϕ = bKer ϕ.

- **Proof:**
  - Let $\phi: G_1 \to G_2$ be a homomorphism.
  - Let Ker $\phi = \{g \in G_1 \mid \phi(g) = e_2\}$, where e_2 is the identity element in G_2.
  - **Part 1: Prove $\phi(a) = \phi(b) \Longrightarrow a$Ker $\phi = b$Ker ϕ.**
    - Assume $\phi(a) = \phi(b)$.

- Multiply by $\phi(b)^{-1}$ on the right: $\phi(a)\phi(b)^{-1} = e_2$.
- Since ϕ is a homomorphism, $\phi(ab^{-1}) = e_2$.
- By definition of the kernel, this means $ab^{-1} \in$ Ker ϕ.
- Let $k = ab^{-1}$, so $k \in$ Ker ϕ.
- Multiplying by b on the right, we get $a = kb$.
- Now, consider the left coset aKer ϕ. Any element in aKer ϕ is of the form ax where $x \in$ Ker ϕ.
- Substitute $a = kb$: $ax = (kb)x = k(bx)$. This doesn't directly show equality.
- Let's restart the coset equality:
    - We have $ab^{-1} \in$ Ker ϕ.
    - We know that aKer $\phi = b$Ker ϕ if and only if $b^{-1}a \in$ Ker ϕ (or $ab^{-1} \in$ Ker ϕ, depending on whether we're talking about left or right cosets, but the statement here is about left cosets. Let's use the definition of coset equality: $aH = bH \Leftrightarrow a^{-1}b \in H$).
    - Here, we have $ab^{-1} \in$ Ker ϕ. This means aKer $\phi = b$Ker ϕ is not directly true. The correct property is aKer $\phi = b$Ker ϕ if and only if $a^{-1}b \in$ Ker ϕ.
    - Let's try again using direct membership for aKer $\phi = b$Ker ϕ.
    - Assume $\phi(a) = \phi(b)$. This means $\phi(a)\phi(b)^{-1} = e_2 \Longrightarrow \phi(ab^{-1}) = e_2 \Longrightarrow ab^{-1} \in$ Ker ϕ.
    - Let $k \in$ Ker ϕ. Then $k = ab^{-1}$. So $a = kb$.

- Now we show aKer $\phi \subseteq b$Ker ϕ: Let $x \in a$Ker ϕ. Then $x = ah$ for some $h \in$ Ker ϕ. Since $a = kb$, $x = kbh$. This implies $b^{-1}x = kh$.
- This is not the standard way. Let's use the property that $aH = bH$ iff $a^{-1}b \in H$.
- We have $\phi(a) = \phi(b) \Leftrightarrow \phi(a)^{-1}\phi(b) = e_2 \Leftrightarrow \phi(a^{-1}b) = e_2 \Leftrightarrow a^{-1}b \in$ Ker ϕ.
- And for left cosets, we know that aKer $\phi = b$Ker ϕ if and only if $a^{-1}b \in$ Ker ϕ.
- Combining these two equivalences, we directly get $\phi(a) = \phi(b) \Leftrightarrow a$Ker $\phi = b$Ker ϕ.

  - **Part 2: Prove aKer $\phi = b$Ker $\phi \Longrightarrow \phi(a) = \phi(b)$.**
    - Assume aKer $\phi = b$Ker ϕ.
    - This implies that $a^{-1}b \in$ Ker ϕ. (This is a standard result for coset equality).
    - By definition of Ker ϕ, if $a^{-1}b \in$ Ker ϕ, then $\phi(a^{-1}b) = e_2$.
    - Since ϕ is a homomorphism, $\phi(a^{-1}b) = \phi(a^{-1})\phi(b) = \phi(a)^{-1}\phi(b)$.
    - So, $\phi(a)^{-1}\phi(b) = e_2$.
    - Multiplying by $\phi(a)$ on the left, we get $\phi(b) = \phi(a)$.
    - Thus, $\phi(a) = \phi(b)$.

- Since both implications hold, we have $\phi(a) = \phi(b) \Leftrightarrow a$Ker $\phi = b$Ker ϕ.

(b) (i) Is U(8) isomorphic to U(10)? Justify your answer.

- **U(8):**

- $U(8) = \{n \in \{1,2,\ldots,7\} \mid \gcd(n,8) = 1\} = \{1,3,5,7\}$.
- The order of $U(8)$ is $\phi(8) = 8(1 - 1/2) = 4$.
- Let's find the order of each element:
  - $|1| = 1$
  - $|3|$: $3^1 = 3$, $3^2 = 9 \equiv 1 \pmod 8$. So, $|3| = 2$.
  - $|5|$: $5^1 = 5$, $5^2 = 25 \equiv 1 \pmod 8$. So, $|5| = 2$.
  - $|7|$: $7^1 = 7$, $7^2 = 49 \equiv 1 \pmod 8$. So, $|7| = 2$.
- All non-identity elements in $U(8)$ have order 2. This means $U(8)$ is isomorphic to the Klein four-group $Z_2 \times Z_2$.

- **U(10):**
  - $U(10) = \{n \in \{1,2,\ldots,9\} \mid \gcd(n,10) = 1\} = \{1,3,7,9\}$.
  - The order of $U(10)$ is $\phi(10) = 10(1 - 1/2)(1 - 1/5) = 10(1/2)(4/5) = 4$.
  - Let's find the order of each element:
    - $|1| = 1$
    - $|3|$: $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 7 \pmod{10}$, $3^4 = 81 \equiv 1 \pmod{10}$. So, $|3| = 4$.
    - $|7|$: $7^1 = 7$, $7^2 = 49 \equiv 9 \pmod{10}$, $7^3 = 63 \equiv 3 \pmod{10}$, $7^4 = 21 \equiv 1 \pmod{10}$. So, $|7| = 4$.
    - $|9|$: $9^1 = 9$, $9^2 = 81 \equiv 1 \pmod{10}$. So, $|9| = 2$.
  - $U(10)$ has elements of order 4 (e.g., 3 and 7). This means $U(10)$ is a cyclic group of order 4, isomorphic to Z_4.

- **Conclusion:**
  - No, $U(8)$ is not isomorphic to $U(10)$.

- **Justification:** $U(8)$ is not cyclic (all non-identity elements have order 2), while $U(10)$ is cyclic (it has an element of order 4). Isomorphic groups must have the same algebraic properties, including cyclicity. A non-cyclic group cannot be isomorphic to a cyclic group.

(ii) Show that any infinite cyclic group is isomorphic to the group of integers under addition.

- **Proof:**
  - Let G be an infinite cyclic group. By definition, G is generated by a single element, say a, and its order is infinite. So, $G = \langle a \rangle = \{a^k \mid k \in Z\}$ and all powers a^k are distinct.
  - Let Z be the group of integers under addition, $(Z, +)$.
  - We need to find an isomorphism $\phi: G \to Z$.
  - Define the mapping $\phi(a^k) = k$ for all integers k.
  - **1. ϕ is well-defined:** Since G is an infinite cyclic group generated by a, all powers a^k are distinct. Thus, if $a^k = a^m$, then $k = m$. This ensures that $\phi(a^k)$ maps to a unique value.
  - **2. ϕ is a homomorphism:**
    - Let $x, y \in G$. Then $x = a^k$ and $y = a^m$ for some integers $k, m \in Z$.
    - $\phi(xy) = \phi(a^k a^m) = \phi(a^{k+m})$.
    - By definition of ϕ, $\phi(a^{k+m}) = k + m$.
    - Also, $\phi(x) + \phi(y) = \phi(a^k) + \phi(a^m) = k + m$.
    - Since $\phi(xy) = \phi(x) + \phi(y)$, ϕ is a homomorphism.
  - **3. ϕ is injective (one-to-one):**
    - Assume $\phi(x) = \phi(y)$.

- Then $\phi(a^k) = \phi(a^m)$, which means $k = m$.
- Since $k = m$, $a^k = a^m$, so $x = y$.
- Therefore, ϕ is injective.

- **4. ϕ is surjective (onto):**
  - Let j be any integer in Z.
  - We need to find an element $x \in G$ such that $\phi(x) = j$.
  - Consider $x = a^j \in G$.
  - By definition of ϕ, $\phi(a^j) = j$.
  - Therefore, for every integer in Z, there exists an element in G that maps to it. So, ϕ is surjective.
- Since ϕ is a well-defined, bijective homomorphism, it is an isomorphism.
- Hence, any infinite cyclic group is isomorphic to the group of integers under addition.

(c) (i) If ϕ is an onto homomorphism from group G_1 to group G_2, then prove that G_1/Ker ϕ is isomorphic to G_2. Hence show that if G_1 is finite, then order of G_2 divides the order of G_1.

- **Proof that G_1/Ker ϕ is isomorphic to G_2 (First Isomorphism Theorem):**
  - Let $\phi: G_1 \to G_2$ be an onto (surjective) group homomorphism.
  - Let $K =$ Ker $\phi = \{g \in G_1 \mid \phi(g) = e_2\}$, where e_2 is the identity in G_2.
  - We know that K is a normal subgroup of G_1. (This is a standard result; kernels of homomorphisms are always normal subgroups).

- Consider the factor group $G_1/K = \{gK \mid g \in G_1\}$.
- Define a mapping $\psi: G_1/K \to G_2$ by $\psi(gK) = \phi(g)$.
- **1. ψ is well-defined:**
  - Assume $g_1K = g_2K$ for some $g_1, g_2 \in G_1$.
  - This means $g_1^{-1}g_2 \in K =$ Ker ϕ.
  - By definition of Ker ϕ, $\phi(g_1^{-1}g_2) = e_2$.
  - Since ϕ is a homomorphism, $\phi(g_1^{-1})\phi(g_2) = e_2 \implies \phi(g_1)^{-1}\phi(g_2) = e_2$.
  - Multiplying by $\phi(g_1)$ on the left, we get $\phi(g_2) = \phi(g_1)$.
  - Thus, $\psi(g_1K) = \phi(g_1) = \phi(g_2) = \psi(g_2K)$. So, ψ is well-defined.
- **2. ψ is a homomorphism:**
  - Let $g_1K, g_2K \in G_1/K$.
  - $\psi((g_1K)(g_2K)) = \psi(g_1g_2K)$.
  - By definition of ψ, $\psi(g_1g_2K) = \phi(g_1g_2)$.
  - Since ϕ is a homomorphism, $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$.
  - Also, $\psi(g_1K)\psi(g_2K) = \phi(g_1)\phi(g_2)$.
  - Since $\psi((g_1K)(g_2K)) = \psi(g_1K)\psi(g_2K)$, ψ is a homomorphism.
- **3. ψ is injective (one-to-one):**
  - Assume $\psi(gK) = e_2$ (the identity in G_2).
  - By definition of ψ, $\phi(g) = e_2$.
  - By definition of Ker ϕ, if $\phi(g) = e_2$, then $g \in$ Ker $\phi = K$.

- If $g \in K$, then the coset gK is equal to K (which is the identity element in G_1/K).
- Since the kernel of ψ is trivial (only the identity element), ψ is injective.

- **4. ψ is surjective (onto):**
  - Let $y \in G_2$.
  - Since ϕ is an onto homomorphism from G_1 to G_2, there exists an element $g \in G_1$ such that $\phi(g) = y$.
  - Consider the coset $gK \in G_1/K$.
  - By definition of ψ, $\psi(gK) = \phi(g) = y$.
  - Therefore, for every element $y \in G_2$, there exists a coset in G_1/K that maps to it. So, ψ is surjective.
- Since ψ is a well-defined, bijective homomorphism, it is an isomorphism.
- Thus, $G_1/\text{Ker } \phi \cong G_2$.

- **Hence show that if G_1 is finite, then order of G_2 divides the order of G_1.**
  - If G_1 is a finite group, then its order $|G_1|$ is finite.
  - From the First Isomorphism Theorem, we have $G_1/\text{Ker } \phi \cong G_2$.
  - This means that $|G_1/\text{Ker } \phi| = |G_2|$.
  - By definition of the order of a factor group, $|G_1/\text{Ker } \phi| = |G_1|/|\text{Ker } \phi|$.
  - Therefore, $|G_2| = |G_1|/|\text{Ker } \phi|$.
  - Rearranging this equation, we get $|G_1| = |G_2| \cdot |\text{Ker } \phi|$.

  - Since |Ker ϕ| is an integer (it's the order of a subgroup), this equation clearly shows that the order of G_2 divides the order of G_1. This is also a direct consequence of Lagrange's Theorem applied to G_1 and its subgroup Ker ϕ.

Question 5: (a) Let G be a group and let a ∈ G. Define the inner automorphism of G induced by a. Show that the set of all inner automorphisms of a group G, denoted by Inn(G), forms a subgroup of Aut(G), the group of all automorphisms of G. Find Inn(D_4).

- **Definition of the inner automorphism of G induced by a:**
  - For any element $a \in G$, the **inner automorphism of G induced by a**, denoted by ϕ_a, is a mapping from G to G defined by: $\phi_a(x) = axa^{-1}$ for all $x \in G$.
- **Show that Inn(G) forms a subgroup of Aut(G):**
  - Aut(G) is the group of all automorphisms of G. We need to show that Inn(G) = {ϕ_a | $a \in G$} satisfies the subgroup criteria.
  - **First, show that each ϕ_a is an automorphism:**
    i. **Homomorphism:** $\phi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$ for all $x, y \in G$.
    ii. **Injective:** Assume $\phi_a(x) = \phi_a(y)$. Then $axa^{-1} = aya^{-1}$. By cancellation (multiplying by a^{-1} on the left and a on the right), $x = y$.
    iii. **Surjective:** Let $y \in G$. We need to find $x \in G$ such that $\phi_a(x) = y$. $axa^{-1} = y \Longrightarrow x = a^{-1}ya$. Since $a^{-1}ya \in G$, for any $y \in G$, there exists an x such that $\phi_a(x) = y$.
    - Therefore, each ϕ_a is an automorphism of G, so Inn(G) ⊆ Aut(G).
  - **Now, show that Inn(G) is a subgroup of Aut(G):**

iv. **Non-empty:** The identity automorphism $id_G(x) = x$ is an inner automorphism induced by $e \in G$. $\phi_e(x) = exe^{-1} = x$. So, $id_G = \phi_e \in \text{Inn}(G)$. Thus, $\text{Inn}(G)$ is non-empty.

v. **Closure under composition:** Let $\phi_a, \phi_b \in \text{Inn}(G)$ for some $a, b \in G$. Consider their composition $(\phi_a \circ \phi_b)(x)$. $(\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = \phi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(b^{-1}a^{-1}) = (ab)x(ab)^{-1}$. This is $\phi_{ab}(x)$. Since $ab \in G$, $\phi_{ab} \in \text{Inn}(G)$. Thus, $\text{Inn}(G)$ is closed under composition.

vi. **Existence of inverses:** Let $\phi_a \in \text{Inn}(G)$. We need to find its inverse. Consider $\phi_{a^{-1}}$. Since $a^{-1} \in G$, $\phi_{a^{-1}} \in \text{Inn}(G)$. $(\phi_a \circ \phi_{a^{-1}})(x) = \phi_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = exe = x = id_G(x)$. Similarly, $(\phi_{a^{-1}} \circ \phi_a)(x) = x = id_G(x)$. So, $\phi_a^{-1} = \phi_{a^{-1}} \in \text{Inn}(G)$.

- Therefore, $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$.

- **Find Inn(D_4):**
  - D_4 is the dihedral group of order 8, representing the symmetries of a square.
  - Elements of D_4 are $\{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, where r is a rotation by $90°$ and s is a reflection. We have $r^4 = e$, $s^2 = e$, and $rs = sr^{-1} = sr^3$.
  - The group of inner automorphisms $\text{Inn}(G)$ is isomorphic to $G/Z(G)$, where $Z(G)$ is the center of G.
  - Let's find $Z(D_4)$.
    - $Z(D_4) = \{g \in D_4 \mid gx = xg$ for all $x \in D_4\}$.
    - e commutes with all elements.
    - r does not commute with s ($rs \neq sr$).

  - r^2 commutes with r and s: $r^2s = sr^{-2} = sr^2$. So r^2 commutes with all elements.
  - r^3 does not commute with s ($r^3s = sr^{-3} = sr \neq sr^3$).
  - s does not commute with r.
  - sr does not commute with r ($srr = srr^{-1}r = sr^{-1}r = s \neq r(sr)$). (Alternatively, $r(sr) = r^2s$ and $sr(r) = sr^2$. $r^2s \neq sr^2$ since $s \neq r^{-2}sr^2 = s$).
  - sr^2 does not commute with r.
  - sr^3 does not commute with r.
  - So, $Z(D_4) = \{e, r^2\}$.
- $|\text{Inn}(D_4)| = |D_4|/|Z(D_4)| = 8/2 = 4$.
- The elements of $\text{Inn}(D_4)$ are ϕ_a for $a \in D_4$. However, if $a \in Z(D_4)$, then $\phi_a = id_G$.
- So, $\phi_e = id_{D_4}$ and $\phi_{r^2} = id_{D_4}$.
- The distinct inner automorphisms are generated by elements not in the center. We can pick representatives from the cosets of $Z(D_4)$.
- $D_4/Z(D_4) = \{Z(D_4), rZ(D_4), sZ(D_4), srZ(D_4)\}$.
- So the distinct inner automorphisms are $\phi_e, \phi_r, \phi_s, \phi_{sr}$.
- Let's describe them by their action on the generators r and s:
  - $\phi_e(x) = exe^{-1} = x$.
  - $\phi_r(r) = rrr^{-1} = r$. $\phi_r(s) = rsr^{-1} = rsr^3 = r^2(rsr^2) = r^2s = sr^2$. So $\phi_r = (s \mapsto sr^2)$.
  - $\phi_s(r) = srs^{-1} = srs = r^{-1}$. $\phi_s(s) = sss^{-1} = s$. So $\phi_s = (r \mapsto r^{-1})$.

- $\phi_{sr}(r) = (sr)r(sr)^{-1} = sr^2r^{-1}s^{-1} = srs = r^{-1}$. $\phi_{sr}(s) = (sr)s(sr)^{-1} = srsr^{-1}s^{-1} = s(srs)r^{-1} = sr(r^{-1})s = s(e)s = s$. So $\phi_{sr} = (r \mapsto r^{-1})$. (Wait, this is wrong: $srsr^{-1}s^{-1} = srsrs = s(rs)rs = s(sr^3)rs = r^3(sr)s = r^3(sr)s = r^3(s)s = r^3$. This is incorrect. Let's recompute $\phi_{sr}(s) = (sr)s(sr)^{-1} = srsr^{-1}s^{-1} = s(rs)r^{-1}s = s(sr^{-1})r^{-1}s = s^2r^{-2}s = r^2s$. This is still not right. Let's use the definition: $(sr)s(sr)^{-1} = srsr^{-1}s^{-1} = srsrs = sr(srs) = sr(r^{-1}) = s$. So $\phi_{sr} = (r \mapsto r^{-1})$.

Let's re-evaluate the inner automorphisms based on representatives e, r, s, sr.

- $\phi_e = id_{D_4}$
- ϕ_r:
  - $\phi_r(r) = rrr^{-1} = r$
  - $\phi_r(s) = rsr^{-1} = sr^{-1}r^{-1} = sr^2$.
- ϕ_s:
  - $\phi_s(r) = srs^{-1} = srs = r^{-1}$.
  - $\phi_s(s) = sss^{-1} = s$.
- ϕ_{sr}:
  - $\phi_{sr}(r) = (sr)r(sr)^{-1} = (sr)r(r^{-1}s^{-1}) = srrr^{-1}s = srs = r^{-1}$.
  - $\phi_{sr}(s) = (sr)s(sr)^{-1} = srsr^{-1}s^{-1} = s(sr^{-1})r^{-1}s = s^2r^{-2}s = r^2s$. (This is r^2s not s) Wait, $(sr)^{-1} = r^{-1}s^{-1} = r^3s$. $\phi_{sr}(s) = (sr)s(r^3s) = srsr^3s = s(rs)r^3s = s(sr^3)r^3s = s^2r^6s = r^2s$. Ah, $r^2 \in Z(D_4)$ so conjugation by r^2 is identity. $r^2s = sr^2$. It's not the reflection itself.

Let's check the group structure. Inn(D_4) has order 4. ϕ_e has order 1. $\phi_r^2(s) = \phi_r(sr^2) = r(sr^2)r^{-1} = r(sr^2)r^3 = r(s)r^2r^3 = r(s)r^5 = r(s)r = r(r^{-1}s)r = s$. So $\phi_r^2 = id_{D_4}$. This means $|\phi_r|$ = 2. $\phi_s^2(r) = \phi_s(r^{-1}) = s(r^{-1})s^{-1} = s(r^{-1})s = (sr^{-1})s = (sr^3)s = s(r^3s) = s(sr^{-3}) = r^{-3} = r$. So $\phi_s^2 = id_{D_4}$. This means $|\phi_s|$ = 2. $\phi_{sr}^2(r) = \phi_{sr}(r^{-1}) = (sr)r^{-1}(sr)^{-1} = (sr)r^{-1}r^3s = sr^4s = ses = s^2 = e$. So r^{-1} is not correct. $\phi_{sr}(r) = (sr)r(sr)^{-1} = srrr^{-1}s^{-1} = s(rr^{-1})s = s(e)s = s^2 = e$. This means (sr) maps r to e, which is incorrect. A homomorphism cannot map a generator to identity if the image of the generator is not identity. Let's check calculation of $\phi_{sr}(r)$ again: $(sr)r(sr)^{-1} = (sr)r(r^{-1}s^{-1}) = sr^2r^{-1}s = srs = r^{-1}$. This is correct. Now, $|\phi_{sr}|$: $\phi_{sr}(r) = r^{-1}$. $\phi_{sr}(s) = s$. $\phi_{sr}^2(r) = \phi_{sr}(r^{-1}) = (sr)r^{-1}(sr)^{-1} = srr^{-1}r^{-1}s = sr^{-1}s = s(sr) = r$. $\phi_{sr}^2(s) = \phi_{sr}(s) = s$. So $\phi_{sr}^2 = id_{D_4}$. This means $|\phi_{sr}|$ = 2. All non-identity elements in Inn(D_4) have order 2. This means Inn$(D_4) \cong Z_2 \times Z_2$.

- **Inn(D$_4$) = {$\phi_e, \phi_r, \phi_s, \phi_{rs}$ }** where:
  - $\phi_e(x) = x$ (identity automorphism)
  - $\phi_r(r) = r$, $\phi_r(s) = sr^2$ (conjugation by r)
  - $\phi_s(r) = r^{-1}$, $\phi_s(s) = s$ (conjugation by s)
  - $\phi_{rs}(r) = r^{-1}$, $\phi_{rs}(s) = s$ (conjugation by rs). Note that $\phi_{rs} = \phi_s$ because $rsZ(D_4) = sZ(D_4)$. (e.g., $rs(r^2) = r^3s$ and $s(r^2) = sr^2$, these are not the same cosets).

Let's use the coset representatives as generators for the distinct inner automorphisms: $Z(D_4) = \{e, r^2\}$. The distinct cosets are $Z(D_4)$, $rZ(D_4)$, $sZ(D_4)$, $srZ(D_4)$.

- $\phi_e = id$ (induced by e or r^2)
- ϕ_r: $r \mapsto r$, $s \mapsto sr^2$ (induced by r or r^3)
- ϕ_s: $r \mapsto r^{-1}$, $s \mapsto s$ (induced by s or sr^2)

- ϕ_{sr}: $r \mapsto r^{-1}$, $s \mapsto sr^2$ (induced by sr or sr^3)
  - Let's verify $\phi_{sr}(r) = (sr)r(sr)^{-1} = sr^2(r^{-1}s^{-1}) = srs^{-1} = srs = r^{-1}$.
  - $\phi_{sr}(s) = (sr)s(sr)^{-1} = srsr^{-1}s^{-1} = s(rs)r^{-1}s^{-1} = s(sr^{-1})r^{-1}s^{-1} = s^2r^{-2}s^{-1} = r^2s^{-1} = r^2s$. So ϕ_{sr} is different from ϕ_s.

The four distinct inner automorphisms are:

2. $\phi_e = id$ (conjugation by e or r^2)
3. ϕ_r (conjugation by r or r^3). Acts as $s \mapsto sr^2$.
4. ϕ_s (conjugation by s or sr^2). Acts as $r \mapsto r^{-1}$.
5. ϕ_{sr} (conjugation by sr or sr^3). Acts as $r \mapsto r^{-1}$ and $s \mapsto sr^2$.

Let's check the composition of these to confirm the $Z_2 \times Z_2$ structure. $\phi_r \circ \phi_s(r) = \phi_r(r^{-1}) = rr^{-1}r^{-1} = r^{-1}$. $\phi_r \circ \phi_s(s) = \phi_r(s) = sr^2$. So $\phi_r \circ \phi_s = \phi_{sr}$. This is $xy = z$. All orders are 2. So it must be $Z_2 \times Z_2$. Inn$(D_4) = \{\phi_e, \phi_r, \phi_s, \phi_{sr}\}$ where:

- $\phi_e(x) = x$
- $\phi_r(x) = rxr^{-1}$
- $\phi_s(x) = sxs^{-1}$
- $\phi_{sr}(x) = (sr)x(sr)^{-1}$

(b) Prove that the order of an element in a direct product of a finite number of finite groups is the lcm of the orders of the components of the element, i.e., $|(g_1, g_2, ..., g_n)| = \text{lcm}(|g_1|, |g_2|, ..., |g_n|)$. Also, find the number of elements of order 7 in $Z_{49} \oplus Z_7$.

- **Proof:**
  - Let $G = G_1 \oplus G_2 \oplus ... \oplus G_n$ be the external direct product of finite groups G_i.

- Let $g = (g_1, g_2, \dots, g_n)$ be an element in G, where $g_i \in G_i$.
- Let $|g|$ be the order of g in G, and let $|g_i|$ be the order of g_i in G_i.
- By definition, $|g|$ is the smallest positive integer k such that $g^k = e_G$, where $e_G = (e_1, e_2, \dots, e_n)$ is the identity element in G.
- $g^k = (g_1, g_2, \dots, g_n)^k = (g_1^k, g_2^k, \dots, g_n^k)$.
- So, $g^k = e_G$ means that $(g_1^k, g_2^k, \dots, g_n^k) = (e_1, e_2, \dots, e_n)$.
- This implies that $g_i^k = e_i$ for all $i = 1,2, \dots, n$.
- For each g_i, $g_i^k = e_i$ means that k must be a multiple of $|g_i|$.
- Therefore, k must be a common multiple of $|g_1|, |g_2|, \dots, |g_n|$.
- Since $|g|$ is the *smallest* such positive integer k, it must be the least common multiple (LCM) of the orders of the components.
- Hence, $|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$.

- **Find the number of elements of order 7 in $Z_{49} \oplus Z_7$:**
  - Let $(x, y) \in Z_{49} \oplus Z_7$, where $x \in Z_{49}$ and $y \in Z_7$.
  - We want to find the number of elements (x, y) such that $|(x, y)| = 7$.
  - We know that $|(x, y)| = \text{lcm}(|x|, |y|)$.
  - For $\text{lcm}(|x|, |y|) = 7$, the possible orders for $|x|$ and $|y|$ must be divisors of 7, i.e., 1 or 7.
  - Also, at least one of $|x|$ or $|y|$ must be 7.

  Let's list the possibilities for $(|x|, |y|)$:

  - Case 1: $|x| = 1, |y| = 7$.
    - Elements of order 1 in Z_{49}: Only 0. (1 element)

- Elements of order 7 in Z_7: These are the elements $y \in Z_7$ such that $\gcd(y, 7) = 1$. These are $1,2,3,4,5,6$. ($\phi(7) = 6$ elements)
- Number of elements in this case: $1 \times 6 = 6$.

  - Case 2: $|x| = 7, |y| = 1$.
    - Elements of order 7 in Z_{49}: These are the elements $x \in Z_{49}$ such that $|x| = 7$. These are of the form $k \cdot (49/7) = 7k$, where $\gcd(k, 7) = 1$. So $x \in \{7,14,21,28,35,42\}$. (6 elements)
    - Elements of order 1 in Z_7: Only 0. (1 element)
    - Number of elements in this case: $6 \times 1 = 6$.
  - Case 3: $|x| = 7, |y| = 7$.
    - Elements of order 7 in Z_{49}: 6 elements (as found above).
    - Elements of order 7 in Z_7: 6 elements (as found above).
    - Number of elements in this case: $6 \times 6 = 36$.

  Total number of elements of order 7 in $Z_{49} \oplus Z_7$ is the sum of elements from these cases: Total = $6 + 6 + 36 = 48$.

(c) Without doing any calculations in Aut(Z_{105}), determine how many elements of Aut(Z_{105}) have order 6.

- **Understanding Aut(Z_n):**
  - The group of automorphisms of Z_n, denoted Aut(Z_n), is isomorphic to $U(n)$, the group of units modulo n.
  - So, Aut$(Z_{105}) \cong U(105)$.
  - We need to find the number of elements of order 6 in $U(105)$.
- **Structure of U(105):**

- $105 = 3 \times 5 \times 7$.
- Since 105 is a product of distinct odd primes, $U(105)$ is isomorphic to the direct product of the U groups of its prime factors: $U(105) \cong U(3) \oplus U(5) \oplus U(7)$.
- Let's find the structure and orders of these component groups:
  - $U(3) = \{1,2\}$. This is isomorphic to Z_2. The only non-identity element (2) has order 2.
  - $U(5) = \{1,2,3,4\}$. This is isomorphic to Z_4. Elements of order 1, 2, 4. (e.g., $|2| = 4$, $|4| = 2$)
  - $U(7) = \{1,2,3,4,5,6\}$. This is isomorphic to Z_6. Elements of order 1, 2, 3, 6. (e.g., $|3| = 6$, $|6| = 2$)

- **Finding elements of order 6 in $U(105)$:**
  - An element in $U(105)$ corresponds to a triplet $(u_1, u_2, u_3) \in U(3) \oplus U(5) \oplus U(7)$.
  - The order of (u_1, u_2, u_3) is lcm$(|u_1|, |u_2|, |u_3|)$.
  - We want this LCM to be 6.
  - The possible orders for u_1, u_2, u_3 are based on the orders of elements in Z_2, Z_4, Z_6 respectively.
    - $|u_1| \in \{1,2\}$
    - $|u_2| \in \{1,2,4\}$
    - $|u_3| \in \{1,2,3,6\}$
  - For lcm$(|u_1|, |u_2|, |u_3|) = 6$, at least one of the orders must be a multiple of 3 (so 3 or 6) AND at least one must be a multiple of 2 (so 2, 4 or 6).

Let's enumerate the possibilities for $(|u_1|, |u_2|, |u_3|)$ such that their LCM is 6. We need lcm$(|u_1|, |u_2|, |u_3|) = 2 \times 3$. This implies that for each prime factor (2 and 3), the maximum power of that prime in the orders must be 2^1 and 3^1. So, 3 must divide at least one of the orders, and 2 must divide at least one of the orders.

Let $o_1 = |u_1|$, $o_2 = |u_2|$, $o_3 = |u_3|$.

- $o_1 \in \{1,2\}$ (from Z_2)
  - Number of elements for $o_1 = 1$: 1 (element $1 \in U(3)$)
  - Number of elements for $o_1 = 2$: 1 (element $2 \in U(3)$)
- $o_2 \in \{1,2,4\}$ (from Z_4)
  - Number of elements for $o_2 = 1$: 1 (element $1 \in U(5)$)
  - Number of elements for $o_2 = 2$: 1 (element $4 \in U(5)$)
  - Number of elements for $o_2 = 4$: 2 (elements $2,3 \in U(5)$)
- $o_3 \in \{1,2,3,6\}$ (from Z_6)
  - Number of elements for $o_3 = 1$: 1 (element $1 \in U(7)$)
  - Number of elements for $o_3 = 2$: 1 (element $6 \in U(7)$)
  - Number of elements for $o_3 = 3$: 2 (elements $2,4 \in U(7)$)
  - Number of elements for $o_3 = 6$: 2 (elements $3,5 \in U(7)$)

Now we analyze the combinations for lcm$(o_1, o_2, o_3) = 6$. We need:

a. At least one order must be divisible by 3 (so o_3 must be 3 or 6).
b. The maximum power of 2 in the orders is 2^1 (so o_2 cannot be 4).

Let's count elements based on (o_1, o_2, o_3) combinations:

- **Case A: $o_3 = 6$.** (This automatically satisfies the 'divisible by 3' condition, and also the 'divisible by 2' condition).
  - Number of elements for $o_3 = 6$: 2

- For o_1: Can be 1 or 2 (2 choices)
- For o_2: Can be 1 or 2 (2 choices) (Cannot be 4, otherwise lcm would be 12).
- Number of elements = (choices for o_1) $\times$ (choices for o_2) $\times$ (choices for $o_3 = 6$)
- Number of elements = $2 \times 2 \times 2 = 8$.

◦ **Case B:** $o_3 = 3$**.** (This satisfies the 'divisible by 3' condition). Now we need the 'divisible by 2' condition to be satisfied by o_1 or o_2. And o_2 cannot be 4.

- Number of elements for $o_3 = 3$: 2
- For o_2: Can be 1 or 2. (Cannot be 4).
- For o_1: Can be 1 or 2.

We need lcm$(o_1, o_2, 3) = 6$. This means lcm$(o_1, o_2) = 2$. This implies:

- $o_1 = 2, o_2 = 1$. (1 choice for o_1, 1 choice for o_2)
- $o_1 = 1, o_2 = 2$. (1 choice for o_1, 1 choice for o_2)
- $o_1 = 2, o_2 = 2$. (1 choice for o_1, 1 choice for o_2)
- Total combinations for (o_1, o_2) where lcm$(o_1, o_2) = 2$:
  - ($|u_1| = 2$, $|u_2| = 1$): 1 element of order 2 in $U(3)$, 1 element of order 1 in $U(5)$. (1 * 1 = 1 combination)
  - ($|u_1| = 1$, $|u_2| = 2$): 1 element of order 1 in $U(3)$, 1 element of order 2 in $U(5)$. (1 * 1 = 1 combination)
  - ($|u_1| = 2$, $|u_2| = 2$): 1 element of order 2 in $U(3)$, 1 element of order 2 in $U(5)$. (1 * 1 = 1 combination)
  - So, 3 combinations for (o_1, o_2) that yield LCM 2.

- Number of elements = (choices for lcm$(o_1, o_2) = 2$) $\times$ (choices for $o_3 = 3$)
- Number of elements = $3 \times 2 = 6$.

Total number of elements of order 6 in $U(105)$ is the sum of elements from these cases: Total = $8 + 6 = 14$.

So, there are **14** elements of order 6 in Aut(Z_{105}).

Question 6: (a) For any group G, prove that G/Z(G) ≅ Inn(G).

- **Proof:**
  - Let G be a group and $Z(G)$ be its center. We know $Z(G)$ is a normal subgroup of G.
  - Let Inn(G) be the set of all inner automorphisms of G. We have already shown in Q5(a) that Inn(G) is a subgroup of Aut(G).
  - Define a mapping $\psi: G \to$ Inn(G) by $\psi(a) = \phi_a$, where $\phi_a(x) = axa^{-1}$ for all $x \in G$.
  - **1. ψ is a homomorphism:**
    - Let $a, b \in G$. We need to show $\psi(ab) = \psi(a) \circ \psi(b)$.
    - $\psi(ab) = \phi_{ab}$.
    - $(\phi_{ab})(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1}$.
    - $(\psi(a) \circ \psi(b))(x) = (\phi_a \circ \phi_b)(x) = \phi_a(\phi_b(x)) = \phi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = abxb^{-1}a^{-1}$.
    - Since $\phi_{ab}(x) = (\phi_a \circ \phi_b)(x)$ for all $x \in G$, we have $\phi_{ab} = \phi_a \circ \phi_b$.
    - Therefore, $\psi(ab) = \psi(a) \circ \psi(b)$, so ψ is a homomorphism.
  - **2. ψ is surjective (onto):**

  - By definition, $\text{Inn}(G)$ is the set of all ϕ_a for $a \in G$.
  - For any $\phi_a \in \text{Inn}(G)$, there exists an element $a \in G$ such that $\psi(a) = \phi_a$.
  - Thus, ψ is surjective.

- **3. Find the Kernel of ψ (Ker ψ):**
  - $\text{Ker}\ \psi = \{a \in G \mid \psi(a) = \text{id}_G\}$, where id_G is the identity automorphism.
  - $\psi(a) = \phi_a$, so $\phi_a = \text{id}_G$.
  - This means $\phi_a(x) = x$ for all $x \in G$.
  - $axa^{-1} = x$ for all $x \in G$.
  - Multiplying by a on the right, $ax = xa$ for all $x \in G$.
  - By definition, the set of all elements that commute with every element in G is the center of G, $Z(G)$.
  - Therefore, $\text{Ker}\ \psi = Z(G)$.

- **4. Apply the First Isomorphism Theorem:**
  - Since $\psi: G \to \text{Inn}(G)$ is an onto homomorphism with $\text{Ker}\ \psi = Z(G)$, by the First Isomorphism Theorem (as proved in Q4(c)(i)), we have: $G/\text{Ker}\ \psi \cong \text{Im}(\psi)$.
  - Since ψ is surjective, $\text{Im}(\psi) = \text{Inn}(G)$.
  - Substituting $\text{Ker}\ \psi = Z(G)$, we get $G/Z(G) \cong \text{Inn}(G)$.

(b) Define the internal direct product of a collection of subgroups of a group G. Let R denote the group of all nonzero real numbers under multiplication. Let R^+ denote the group of all positive real numbers under multiplication. Prove that R is the internal direct product of R^+ and the subgroup {1, -1}.

- **Definition of Internal Direct Product:**

- A group G is the **internal direct product** of its subgroups $H_1, H_2, \dots, H_n$ if the following three conditions are met:
    i. Each H_i is a normal subgroup of G.
    ii. $G = H_1 H_2 \dots H_n$ (every element $g \in G$ can be written as a product $h_1 h_2 \dots h_n$ where $h_i \in H_i$).
    iii. For each i, $H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n) = \{e\}$ (the intersection of each subgroup with the product of the other subgroups is the identity element).
- Alternatively, for two subgroups H and K of G, G is the internal direct product of H and K if:
    iv. H and K are normal subgroups of G.
    v. $G = HK$.
    vi. $H \cap K = \{e\}$.
- (And for two subgroups, (1) can be relaxed to just $hk = kh$ for all $h \in H, k \in K$ if $G = HK$ and $H \cap K = \{e\}$ because this implies normality for H and K within $G = HK$.)

- **Prove that R is the internal direct product of R⁺ and the subgroup {1, -1}:**
    - Let $G = R^*$ be the group of all non-zero real numbers under multiplication.
    - Let $H = R^+$ be the group of all positive real numbers under multiplication.
    - Let $K = \{1, -1\}$ be a subgroup of R^* under multiplication.
    - We need to verify the three conditions for internal direct product:
    - **1. H and K are normal subgroups of G:**

- **H = R⁺:**
  - R^+ is a subgroup of R^* (closed under multiplication, contains 1, has inverses for every element).
  - To show R^+ is normal in R^*, we need to show $gxg^{-1} \in R^+$ for all $g \in R^*$ and $x \in R^+$.
  - Let $g \in R^*$ and $x \in R^+$. Then $gxg^{-1} = x(gg^{-1}) = x \cdot 1 = x$. Since $x \in R^+$, $gxg^{-1} \in R^+$.
  - Alternatively, consider gxg^{-1}. Since $x > 0$, $gxg^{-1} = (g^2)(x/g^2)$. The product of any two positive numbers is positive. If $g > 0$, then $g^{-1} > 0$, $gxg^{-1} > 0$. If $g < 0$, then $g^{-1} < 0$, $gxg^{-1} > 0$. So gxg^{-1} is always positive.
  - Therefore, R^+ is a normal subgroup of R^*.

- **K = {1, -1}:**
  - K is a subgroup of R^* (closed under multiplication: $1 \cdot 1 = 1$, $1 \cdot (-1) = -1$, $(-1) \cdot (-1) = 1$; contains 1; inverses exist: $1^{-1} = 1, (-1)^{-1} = -1$).
  - To show K is normal in R^*, we need to show $gxg^{-1} \in K$ for all $g \in R^*$ and $x \in K$.
  - If $x = 1$, $g \cdot 1 \cdot g^{-1} = 1 \in K$.
  - If $x = -1$, $g \cdot (-1) \cdot g^{-1} = -gg^{-1} = -1 \in K$.
  - Therefore, K is a normal subgroup of R^*.

- **2. G = HK:** (Every element in R^* can be written as a product of an element from R^+ and an element from K).
  - Let $x \in R^*$.

- If $x > 0$, then $x \in R^+$. We can write $x = x \cdot 1$, where $x \in R^+$ and $1 \in K$.
- If $x < 0$, then $-x > 0$. So $-x \in R^+$. We can write $x = (-x) \cdot (-1)$, where $-x \in R^+$ and $-1 \in K$.
- Therefore, every element in R^* can be expressed as a product of an element from R^+ and an element from K. So $R^* = R^+K$.

- **3. H ∩ K = {e}:** (The intersection of R^+ and K is the identity element).
  - $R^+ = (0, \infty)$ (set of positive real numbers).
  - $K = \{1, -1\}$.
  - The common element in both sets is only 1.
  - Therefore, $R^+ \cap \{1, -1\} = \{1\}$.
- Since all three conditions are satisfied, R^* is the internal direct product of R^+ and $\{1, -1\}$.

(c) The set G = {1,4,11,14,16,19,26,29,31,34,41,44} is a group under multiplication modulo 45. Write G as an external and an internal direct product of cyclic groups of prime-power order.

- **Understanding the group G:**
  - The group is $U(45)$ because its elements are precisely those integers relatively prime to 45.
  - $45 = 9 \times 5 = 3^2 \times 5$.
  - The order of $U(45)$ is $\phi(45) = 45(1 - 1/3)(1 - 1/5) = 45(2/3)(4/5) = 2 \times 3 \times 4 = 24$.
  - The given set G has 12 elements. Let's list them and compare with $U(45)$. $U(45) = \{1,2,4,7,8,11,13,14,16,17,19,22,23,26,28,29,31,32,34,37,38,41,43,44\}$

. The provided set G is a subset of $U(45)$. This implies that G is a subgroup of $U(45)$.

- Let's check the elements: $G = \{1,4,11,14,16,19,26,29,31,34,41,44\}$. $|G| = 12$. $U(45)$ has order 24. So G is a subgroup of $U(45)$.
- The prime-power factorization of the order of G is $12 = 2^2 \times 3$.
- We need to write G as an external and internal direct product of cyclic groups of prime-power order.
- The structure of $U(n)$ groups: $U(45) \cong U(9) \oplus U(5)$. $U(9) = \{1,2,4,5,7,8\}$. This is cyclic of order $\phi(9) = 6$, so $U(9) \cong Z_6$. (Generator e.g., 2: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 \equiv 7, 2^5 = 14 \equiv 5, 2^6 = 10 \equiv 1 \pmod 9$). $U(5) = \{1,2,3,4\}$. This is cyclic of order $\phi(5) = 4$, so $U(5) \cong Z_4$. (Generator e.g., 2: $2^1 = 2, 2^2 = 4, 2^3 = 8 \equiv 3, 2^4 = 16 \equiv 1 \pmod 5$).
- So, $U(45) \cong Z_6 \oplus Z_4$.
- The elements of G are: $\{1,4,11,14,16,19,26,29,31,34,41,44\}$.
- Let's consider elements modulo 9 and modulo 5 for elements in G.
  - $1 \pmod 9 \equiv 1$, $1 \pmod 5 \equiv 1$. $(1,1)$
  - $4 \pmod 9 \equiv 4$, $4 \pmod 5 \equiv 4$. $(4,4)$
  - $11 \pmod 9 \equiv 2$, $11 \pmod 5 \equiv 1$. $(2,1)$
  - $14 \pmod 9 \equiv 5$, $14 \pmod 5 \equiv 4$. $(5,4)$
  - $16 \pmod 9 \equiv 7$, $16 \pmod 5 \equiv 1$. $(7,1)$
  - $19 \pmod 9 \equiv 1$, $19 \pmod 5 \equiv 4$. $(1,4)$
  - $26 \pmod 9 \equiv 8$, $26 \pmod 5 \equiv 1$. $(8,1)$
  - $29 \pmod 9 \equiv 2$, $29 \pmod 5 \equiv 4$. $(2,4)$

        - $31 \pmod 9 \equiv 4$, $31 \pmod 5 \equiv 1$. $(4,1)$
        - $34 \pmod 9 \equiv 7$, $34 \pmod 5 \equiv 4$. $(7,4)$
        - $41 \pmod 9 \equiv 5$, $41 \pmod 5 \equiv 1$. $(5,1)$
        - $44 \pmod 9 \equiv 8$, $44 \pmod 5 \equiv 4$. $(8,4)$
    - Mapping these to $U(9) \oplus U(5)$: $G' = \{(1,1),(4,4),(2,1),(5,4),(7,1),(1,4),(8,1),(2,4),(4,1),(7,4),(5,1),(8,4)\}$.
    - Let $H_{1'} = \{(x,1) \mid x \in U(9)\} = \{(1,1),(2,1),(4,1),(5,1),(7,1),(8,1)\}$. This is $U(9) \oplus \{1\}$. It is isomorphic to Z_6.
    - Let $H_{2'} = \{(1,y) \mid y \in U(5)\} = \{(1,1),(1,2),(1,3),(1,4)\}$. This is $\{1\} \oplus U(5)$. It is isomorphic to Z_4.
    - The group G consists of elements where the second component (modulo 5) is either 1 or 4.
    - The elements of $U(5)$ with second component 1 or 4 are $\{1,4\}$. This subgroup of $U(5)$ has order 2 and is isomorphic to Z_2.
    - So, $G \cong U(9) \oplus \{1,4\} \pmod 5$.
    - This means $G \cong U(9) \oplus \langle 4 \rangle_{U(5)}$.
    - $G \cong Z_6 \oplus Z_2$.
    - Since $Z_6 \cong Z_2 \oplus Z_3$, we have $G \cong Z_2 \oplus Z_3 \oplus Z_2$.
    - Rearranging, $G \cong Z_2 \oplus Z_2 \oplus Z_3$.
- **External Direct Product of Cyclic Groups of Prime-Power Order:**
    - $G \cong Z_2 \oplus Z_2 \oplus Z_3$.
- **Internal Direct Product of Cyclic Groups of Prime-Power Order:**

- Let's find the subgroups in G corresponding to these cyclic groups.
- In Z_{45}, elements of order 2 are those x such that $x^2 \equiv 1 \pmod{45}$.
  - $x^2 \equiv 1 \pmod 9 \Longrightarrow x \in \{1,8\}$ (order 2, not 1 in Z_9).
  - $x^2 \equiv 1 \pmod 5 \Longrightarrow x \in \{1,4\}$ (order 2, not 1 in Z_5).
  - By CRT:
    - $x \equiv 1 \pmod 9, x \equiv 1 \pmod 5 \Longrightarrow x = 1$ (order 1)
    - $x \equiv 1 \pmod 9, x \equiv 4 \pmod 5 \Longrightarrow x = 19$ (order 2)
    - $x \equiv 8 \pmod 9, x \equiv 1 \pmod 5 \Longrightarrow x = 26$ (order 2)
    - $x \equiv 8 \pmod 9, x \equiv 4 \pmod 5 \Longrightarrow x = 44$ (order 2)
  - So, G contains elements of order 2: $19,26,44$.
- Elements of order 3:
  - $x^3 \equiv 1 \pmod 9$, $x \neq 1$. From $U(9) \cong Z_6$, the elements of order 3 are $4,7$.
  - $x^3 \equiv 1 \pmod 5$, $x \neq 1$. From $U(5) \cong Z_4$, there are no elements of order 3.
  - So, an element of order 3 in G must have its 5-component of order 1.
  - $(4,1)$ gives 31. Order of $31 \pmod{45}$ is 3. ($31^1 = 31$, $31^2 = 961 \equiv 16 \pmod{45}$, $31^3 \equiv 16 \times 31 = 496 \equiv 1 \pmod{45}$).
  - $(7,1)$ gives 16. Order of $16 \pmod{45}$ is 3. ($16^1 = 16$, $16^2 = 256 \equiv 31 \pmod{45}$, $16^3 \equiv 31 \times 16 = 496 \equiv 1 \pmod{45}$).

- The elements of order 2 are $19, 26, 44$.
- The elements of order 3 are $16, 31$.
- The elements of order 4 (lcm(order in $U(9)$, order in $U(5)$) is 4):
  - Order 4 can come from (o_1, o_2) where $o_2 = 4$.
  - $o_1 \in \{1,2\}$
  - $(1, y)$ where y has order 4 in $U(5)$ (i.e. $y = 2,3$).
    - (1,2) in $U(9) \oplus U(5)$ corresponds to $11 \pmod{45}$. $11^1 = 11, 11^2 = 121 \equiv 31, 11^3 \equiv 31 \times 11 = 341 \equiv 26 \pmod{45}, 11^4 \equiv 26 \times 11 = 286 \equiv 1 \pmod{45}$. No, $11 \pmod 9 \equiv 2$, order 6. $11 \pmod 5 \equiv 1$, order 1. So $|(2,1)| = \text{lcm}(6,1) = 6$. So 11 has order 6.
    - (1,3) in $U(9) \oplus U(5)$ corresponds to $1 \pmod 9, 3 \pmod 5$. (1,3) should have order $1 \times 4 = 4$. $1 \pmod 9, 3 \pmod 5$. Let's solve $x \equiv 1 \pmod 9, x \equiv 3 \pmod 5$. $x = 9k + 1 \equiv 3 \pmod 5 \Longrightarrow 4k + 1 \equiv 3 \pmod 5 \Longrightarrow 4k \equiv 2 \pmod 5 \Longrightarrow -k \equiv 2 \pmod 5 \Longrightarrow k \equiv -2 \equiv 3 \pmod 5$. So $k = 3$. $x = 9(3) + 1 = 28$. $28 \in U(45)$. Is $28 \in G$? No.
  - (x, y) where $|x| = 2, |y| = 4$.
    - (8,2) gives $x \equiv 8 \pmod 9, x \equiv 2 \pmod 5$. $x = 9k + 8 \equiv 2 \pmod 5 \Longrightarrow 4k + 3 \equiv 2 \pmod 5 \Longrightarrow 4k \equiv -1 \equiv 4 \pmod 5 \Longrightarrow k \equiv 1 \pmod 5$. $k = 1$. $x = 17$. $17 \notin G$.

- Let's reconsider the elements of G.
  - $U(45) \cong Z_6 \oplus Z_4$.
  - $G = \{(x \pmod 9, y \pmod 5) \mid x \in G\}$.

- $G = \{(1,1),(4,4),(2,1),(5,4),(7,1),(1,4),(8,1),(2,4),(4,1),(7,4),(5,1),(8,4)\}$.
- Let $A = \{1,2,4,5,7,8\} \subset U(9)$. This is $U(9) \cong Z_6$.
- Let $B = \{1,4\} \subset U(5)$. This is $\langle 4 \rangle_{U(5)} \cong Z_2$.
- The elements of G are precisely $A \times B$.
- So, $G \cong U(9) \oplus \langle 4 \rangle_{U(5)}$.
- $G \cong Z_6 \oplus Z_2$.
- Now, decompose Z_6 into prime-power order cyclic groups: $Z_6 \cong Z_2 \oplus Z_3$.
- Therefore, $G \cong Z_2 \oplus Z_3 \oplus Z_2$.
- This is the **external direct product of cyclic groups of prime-power order.**

- **Internal Direct Product:**
  - We need to find subgroups H_1, H_2, H_3 within G such that $H_1 \cong Z_2$, $H_2 \cong Z_2$, $H_3 \cong Z_3$, and $G = H_1H_2H_3$ with trivial intersections.
  - We can use elements that correspond to the decomposition.
  - Let $H_a = \{x \in G \mid x \equiv 1 \pmod 9\}$.
    - Elements of G with $x \pmod 9 = 1$: $1,19$. This is a subgroup $\{1,19\}$ of order 2. Let $H_a = \langle 19 \rangle \cong Z_2$. ($19 \pmod 9 \equiv 1$, $19 \pmod 5 \equiv 4$).
  - Let $H_b = \{x \in G \mid x \equiv 1 \pmod 5\}$.
    - Elements of G with $x \pmod 5 = 1$: $1,11,16,26,31,41$. This is the subgroup $U(9)$ projected onto G.

- This subgroup is isomorphic to Z_6. We need to split this further.
- Subgroup of order 2: $\{1,26\}$. $26 \pmod 9 \equiv 8$, $26 \pmod 5 \equiv 1$. $26^2 = 676 = 15 \times 45 + 1 \equiv 1 \pmod{45}$. Let $H_{b'} = \langle 26 \rangle \cong Z_2$.
- Subgroup of order 3: $\{1,16,31\}$. $16 \pmod 9 \equiv 7$, $16 \pmod 5 \equiv 1$. $16^3 \equiv 1 \pmod{45}$. Let $H_c = \langle 16 \rangle \cong Z_3$.

- Let's check elements for the first Z_2 (from the Z_2 component of Z_6). Let $g_1 \in U(9)$ of order 2, $g_1 = 8$. Let $g_2 \in U(5)$ of order 1, $g_2 = 1$. This corresponds to $(8,1) \pmod{9,5}$ which is $26 \in G$. So $H_1 = \langle 26 \rangle = \{1,26\}$. This is Z_2.
- Let's check elements for the second Z_2 (from Z_2 itself). Let $g_1 \in U(9)$ of order 1, $g_1 = 1$. Let $g_2 \in U(5)$ of order 2, $g_2 = 4$. This corresponds to $(1,4) \pmod{9,5}$ which is $19 \in G$. So $H_2 = \langle 19 \rangle = \{1,19\}$. This is Z_2.
- Let's check elements for the Z_3. Let $g_1 \in U(9)$ of order 3, $g_1 = 4$. Let $g_2 \in U(5)$ of order 1, $g_2 = 1$. This corresponds to $(4,1) \pmod{9,5}$ which is $31 \in G$. So $H_3 = \langle 31 \rangle = \{1,31,16\}$. This is Z_3. (Note: $31^2 = 16$, $31^3 = 1$).
- Now, we need to check the internal direct product conditions for $H_1 = \langle 26 \rangle$, $H_2 = \langle 19 \rangle$, $H_3 = \langle 31 \rangle$.

vii. **Normality:** All these subgroups are cyclic, and G is abelian (as it is isomorphic to $Z_2 \oplus Z_2 \oplus Z_3$, which is abelian). In an abelian group, every subgroup is normal. So, this condition is satisfied.

viii. **Product spans G:** $|H_1||H_2||H_3| = 2 \times 2 \times 3 = 12 = |G|$. This means $H_1H_2H_3$ will be G if the intersections are trivial.

ix. **Trivial intersections:**

- $H_1 \cap H_2 = \{1,26\} \cap \{1,19\} = \{1\}$.
- $H_1 \cap H_3 = \{1,26\} \cap \{1,16,31\} = \{1\}$.
- $H_2 \cap H_3 = \{1,19\} \cap \{1,16,31\} = \{1\}$.
- More generally, we need $H_i \cap (H_j H_k) = \{1\}$.
    - $H_1 H_2 = \{1,19,26,44\}$. Note $19 \times 26 = 494 \equiv 44 \pmod{45}$. This is a group of order 4, isomorphic to $Z_2 \oplus Z_2$.
    - $H_1 H_2 \cap H_3 = \{1,19,26,44\} \cap \{1,16,31\} = \{1\}$.

- Therefore, G is the internal direct product of $H_1 = \langle 26 \rangle$, $H_2 = \langle 19 \rangle$, and $H_3 = \langle 31 \rangle$.
- **Internal Direct Product:** $G = \langle 26 \rangle \times \langle 19 \rangle \times \langle 31 \rangle$.
- **External Direct Product:** $G \cong Z_2 \oplus Z_2 \oplus Z_3$.