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 be a permutation of a finite set .
* Let be written as a product of disjoint cycles: .
* Since the cycles are disjoint, they commute with each other.
* Let the length of the cycle be . This means that the order of the cycle is .
* For any integer , .
* For to be the identity permutation, each must be the identity permutation.
* This implies that must be a multiple of the order of each cycle , i.e., must be a multiple of for all .
* The smallest positive integer for which this holds is the least common multiple (LCM) of the lengths of the cycles.
* Therefore, the order of is .

(b) (i) Let S₃ denote the symmetric group of degree n. In S₃, find elements α and β such that |α| = 2, |β| = 2 and |αβ| = 3.

* In , elements of order 2 are transpositions (cycles of length 2).
* Let . Its order is 2.
* Let . Its order is 2.
* Now, let's find the product : . To compute this, start with 1: . So 1 goes to 3. Now 3: . So 3 goes to 2. Now 2: . So 2 goes to 1.
* Thus, .
* The order of is 3, which is the length of the cycle.
* Therefore, and satisfy the given conditions.

(ii) Let β ∈ S₇ and β⁴ = (2 1 4 3 5 6 7). Then find β.

* Let .
* The length of is 7. So, .
* We are given .
* Since the order of is 7, we know that (identity).
* Also, since , then for some integer such that .
* We need to find the inverse of modulo .
* So, .
* Therefore, .
* Now, we compute .
* So, .

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

* 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 and are odd permutations, then and . Then . 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 Sₙ is a subgroup of Sₙ.

* **Definition of Even and Odd Permutations:**
  + A permutation is called an **even permutation** if it can be expressed as a product of an even number of transpositions.
  + A permutation 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 Sₙ is a subgroup of Sₙ:** Let be the set of all even permutations in . We need to show that satisfies the three subgroup criteria:
  1. **Non-empty:** The identity permutation can be written as a product of zero transpositions (which is an even number). Thus, , so is non-empty.
  2. **Closure:** Let . This means can be written as a product of an even number of transpositions, say transpositions, and can be written as a product of an even number of transpositions, say transpositions. Then the product can be written as a product of transpositions. Since and are both even, is also even. Therefore, is an even permutation, so .
  3. **Existence of Inverses:** Let . This means where is an even number and are transpositions. The inverse of is . Since each transposition is its own inverse (), we have . This is also a product of transpositions. Since is even, is also an even permutation. Therefore, .
  + Since satisfies all three conditions, it is a subgroup of . This subgroup is called the alternating group of degree .

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 . The cyclic group generated by is . The order of is 15.
* Let . The elements of are powers of . Since , the order of is . So, .
* The index of in is .
* This means there will be 3 distinct left cosets.
* The cosets are of the form where .
* The first coset is .
* To find the next coset, pick an element from not in , for example, . .
* To find the third coset, pick an element from not in or , for example, . .
* We have found 3 distinct cosets, which matches the index. These are all the left cosets of in .
* The left cosets are:

(ii) State and prove Lagrange's theorem.

* **Lagrange's Theorem:** If is a finite group and is a subgroup of , then the order of divides the order of . Furthermore, the number of distinct left (or right) cosets of in is .
* **Proof:**
  1. Let be a finite group and be a subgroup of .
  2. Consider the set of all distinct left cosets of in . Let these be , where is the index of in , denoted by .
  3. We know that the set of all left cosets of in forms a partition of . This means that every element of belongs to exactly one left coset.
  4. We also know that for any , the mapping is a bijection from to . This implies that every left coset has the same number of elements as . That is, for any , .
  5. Since the distinct left cosets partition , the sum of the number of elements in each distinct coset must be equal to the total number of elements in .
  6. Therefore, .
  7. Since each coset has elements, we have (k times).
  8. So, .
  9. This implies that .
  10. Since is an integer (the number of distinct cosets), must divide .

(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 be a group with more than one element, so .
* Assume has no proper, non-trivial subgroups. This means the only subgroups of are the trivial subgroup and itself.
* Let be any element in such that .
* Consider the cyclic subgroup generated by , denoted by .
* Since , is not the trivial subgroup .
* Since has no proper, non-trivial subgroups, must be equal to .
* This means that is a cyclic group generated by any non-identity element .
* Now, we need to show that the order of (which is the order of ) must be a prime number.
* Assume, for the sake of contradiction, that is not prime. Since , it must be either 1 (which contradicts ) or a composite number.
* If is a composite number, then for some integers .
* Since and , the order of is .
* Consider the element .
* The order of is .
* Since , .
* Consider the subgroup . Its order is .
* Since , is not the trivial subgroup.
* Since , , so is a proper subgroup of .
* Thus, is a proper, non-trivial subgroup of .
* This contradicts our initial assumption that has no proper, non-trivial subgroups.
* Therefore, our assumption that is not prime must be false.
* Hence, must be a prime number.

(c) Let C be the group of non-zero complex numbers under multiplication and let H = {a + bi ∈ C | a² + b² = 1}. Give a geometrical description of the coset (3 + 4i)H. Give a geometrical description of the coset (c + di)H.

* Let be the group of non-zero complex numbers under multiplication.
* Let . Geometrically, 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 :**
  + A coset consists of all elements of the form , where .
  + Let with .
  + The modulus of is .
  + When we multiply two complex numbers, their moduli multiply and their arguments add.
  + So, for any , we have .
  + Since , we have .
  + Therefore, every complex number in the coset has a modulus of 5.
  + Geometrically, the coset represents a circle centered at the origin with a radius of 5. This circle passes through the point .
* **Geometrical description of the coset :**
  + Let be any non-zero complex number.
  + Let its modulus be . Since , .
  + A coset consists of all elements of the form , where .
  + For any , we have .
  + Since , we have .
  + Therefore, every complex number in the coset has a modulus of .
  + Geometrically, the coset represents a circle centered at the origin with a radius of . This circle passes through the point .

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 be a group and be a subgroup of .
  + Given that the index of in , denoted by , is 2.
  + This means there are exactly two distinct left cosets of in , and exactly two distinct right cosets of in .
  + One of these left cosets is .
  + One of these right cosets is .
  + Since the cosets partition , the union of the two left cosets must be , and the union of the two right cosets must be .
  + So, for some and .
  + And for some and .
  + Since , must be the other left coset, which is .
  + Similarly, since , must be the other right coset, which is .
  + Therefore, and .
  + This implies that .
  + Now, we need to show that for all to prove that is normal.
    - Case 1: If .
      * Then (since is a subgroup).
      * And (since is a subgroup).
      * So, .
    - Case 2: If .
      * Since there are only two left cosets, must be the other coset, i.e., .
      * Similarly, since there are only two right cosets, must be the other coset, i.e., .
      * Therefore, .
  + Since for all , is a normal subgroup of .

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

* **Proof:**
  + Let be a group and be a unique subgroup of of some finite order, say .
  + To prove that is normal in , we need to show that for every , .
  + Consider the set for an arbitrary .
  + We know that is a subgroup of . This is a standard result:
    - Identity: .
    - Closure: Let . Then and for some . . Since , .
    - Inverse: Let . Then for some . . Since , .
  + Thus, is a subgroup of .
  + Now, let's consider the order of .
  + The mapping defined by is an isomorphism.
    - It is a homomorphism: .
    - It is injective: If , then . By cancellation, .
    - It is surjective by definition of .
  + Since is an isomorphism, .
  + So, for every , is a subgroup of of order .
  + However, we are given that is the *unique* subgroup of of order .
  + Therefore, must be equal to for all .
  + This shows that is a normal subgroup of .

(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 be a cyclic group. This means for some element .
  + Let be a normal subgroup of .
  + Consider the factor group .
  + We want to show that is cyclic. This means we need to find an element in that generates the entire factor group.
  + Consider the coset .
  + Let be an arbitrary element in .
  + Since and , can be written as for some integer .
  + Therefore, .
  + By the definition of multiplication in factor groups, .
  + So, every element in can be expressed as a power of .
  + Thus, .
  + Therefore, 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 is cyclic, then must be cyclic. This is false.
  + Consider the group , the symmetric group of degree 3.
    - is not a cyclic group because its elements have orders 1, 2, or 3, and there is no element of order . (For example, is non-abelian, while all cyclic groups are abelian).
  + Consider the alternating group , which is a normal subgroup of .
    - The order of is 3.
    - The index of in is .
  + The factor group has order 2.
  + Any group of order 2 is cyclic. For example, .
  + So, is a cyclic group.
  + However, 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 be a group and be its center.
  + Assume that is cyclic.
  + Since is cyclic, there exists an element such that .
  + This means that every element in can be written as a power of .
  + Let be any two arbitrary elements in .
  + Consider their cosets and in .
  + Since is cyclic and generated by , there exist integers and such that:
  + From , it implies that and belong to the same coset. So, for some .
  + Similarly, from , it implies that for some .
  + Now, we need to show that is Abelian, i.e., for all .
  + Since , commutes with all elements in , including . So, .
  + .
  + Similarly, consider :
  + Since , commutes with all elements in , including . So, .
  + .
  + Since and are elements of , they commute with each other ().
  + Therefore, .
  + Since and were arbitrary elements of , this proves that is Abelian.

(c) (i) Let ϕ be a group homomorphism from group G₁ to group G₂ and H be a subgroup of G₁. Show that if H is cyclic, then ϕ(H) is cyclic.

* **Proof:**
  + Let be a group homomorphism.
  + Let be a subgroup of .
  + Assume is cyclic. This means for some element .
  + We need to show that is cyclic. This means we need to find an element in that generates it.
  + Consider the element . We will show that .
  + Let be an arbitrary element in .
  + By definition of , there exists an element such that .
  + Since is cyclic and generated by , can be written as for some integer .
  + So, .
  + Since is a homomorphism, .
  + Therefore, .
  + This shows that every element in can be expressed as a power of .
  + Thus, .
  + Hence, is a cyclic group.

(ii) How many homomorphisms are there from Z₂₀ to Z₈? How many are there onto Z₈?

* **Number of homomorphisms from Z₂₀ to Z₈:**
  + Let be a homomorphism.
  + A homomorphism from a cyclic group is completely determined by the image of its generator.
  + Let the generator of be (under addition modulo 20).
  + Let , where .
  + For a homomorphism , the order of must divide the order of . So, must divide .
  + Also, , so must divide .
  + Therefore, must divide both 20 and 8. So, must divide .
  + The possible orders for are 1, 2, 4, 8.
  + We need to find elements whose order divides 4.
    - Elements of order 1: (since )
    - Elements of order 2: (since )
    - Elements of order 4: (since and )
    - Elements of order 8: (their orders do not divide 4, so they are not valid choices for ).
  + The possible values for are .
  + Each of these choices for uniquely defines a homomorphism.
  + Therefore, there are **4** homomorphisms from to .
* **Number of homomorphisms from Z₂₀ onto Z₈:**
  + For a homomorphism to be onto , its image must be equal to .
  + This means the generator must generate .
  + The elements that generate are those whose order is 8. These are the elements such that .
  + The generators of are .
  + From the previous part, we found that must divide .
  + The possible orders for are 1, 2, 4.
  + Since none of these orders is 8, it is impossible for to generate .
  + Therefore, there are **0** homomorphisms from onto .

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):**
  + is the group of units modulo 30.
  + .
  + The elements are: .
  + .
* **Using properties of homomorphisms:**
  + We are given is a homomorphism.
  + .
  + We are given .
  + We need to find all such that .
  + By a property of homomorphisms, if and , then . More generally, the set of all elements that map to a specific image is given by , where is any element such that .
  + Here, and we know one element that maps to 7 is .
  + So, the set of all elements such that is .
  + .
  + .
  + .
  + .
  + Therefore, the elements of that map to 7 are **{7, 17}**.

(ii) Let ϕ be a homomorphism from a group G₁ to group G₂. Show that ϕ(a) = ϕ(b) iff aKer ϕ = bKer ϕ.

* **Proof:**
  + Let be a homomorphism.
  + Let , where is the identity element in .
  + **Part 1: Prove .**
    - Assume .
    - Multiply by on the right: .
    - Since is a homomorphism, .
    - By definition of the kernel, this means .
    - Let , so .
    - Multiplying by on the right, we get .
    - Now, consider the left coset . Any element in is of the form where .
    - Substitute : . This doesn't directly show equality.
    - Let's restart the coset equality:
      * We have .
      * We know that if and only if (or , 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: ).
      * Here, we have . This means is not directly true. The correct property is if and only if .
      * Let's try again using direct membership for .
      * Assume . This means .
      * Let . Then . So .
      * Now we show : Let . Then for some . Since , . This implies .
      * This is not the standard way. Let's use the property that iff .
      * We have .
      * And for left cosets, we know that if and only if .
      * Combining these two equivalences, we directly get .
  + **Part 2: Prove .**
    - Assume .
    - This implies that . (This is a standard result for coset equality).
    - By definition of , if , then .
    - Since is a homomorphism, .
    - So, .
    - Multiplying by on the left, we get .
    - Thus, .
* Since both implications hold, we have .

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

* **U(8):**
  + .
  + The order of is .
  + Let's find the order of each element:
    - : , . So, .
    - : , . So, .
    - : , . So, .
  + All non-identity elements in have order 2. This means is isomorphic to the Klein four-group .
* **U(10):**
  + .
  + The order of is .
  + Let's find the order of each element:
    - : , , , . So, .
    - : , , , . So, .
    - : , . So, .
  + has elements of order 4 (e.g., 3 and 7). This means is a cyclic group of order 4, isomorphic to .
* **Conclusion:**
  + No, is not isomorphic to .
  + **Justification:** is not cyclic (all non-identity elements have order 2), while 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 be an infinite cyclic group. By definition, is generated by a single element, say , and its order is infinite. So, and all powers are distinct.
  + Let be the group of integers under addition, .
  + We need to find an isomorphism .
  + Define the mapping for all integers .
  + **1. is well-defined:** Since is an infinite cyclic group generated by , all powers are distinct. Thus, if , then . This ensures that maps to a unique value.
  + **2. is a homomorphism:**
    - Let . Then and for some integers .
    - .
    - By definition of , .
    - Also, .
    - Since , is a homomorphism.
  + **3. is injective (one-to-one):**
    - Assume .
    - Then , which means .
    - Since , , so .
    - Therefore, is injective.
  + **4. is surjective (onto):**
    - Let be any integer in .
    - We need to find an element such that .
    - Consider .
    - By definition of , .
    - Therefore, for every integer in , there exists an element in that maps to it. So, is surjective.
  + Since 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 G₁ to group G₂, then prove that G₁/Ker ϕ is isomorphic to G₂. Hence show that if G₁ is finite, then order of G₂ divides the order of G₁.

* **Proof that G₁/Ker ϕ is isomorphic to G₂ (First Isomorphism Theorem):**
  + Let be an onto (surjective) group homomorphism.
  + Let , where is the identity in .
  + We know that is a normal subgroup of . (This is a standard result; kernels of homomorphisms are always normal subgroups).
  + Consider the factor group .
  + Define a mapping by .
  + **1. is well-defined:**
    - Assume for some .
    - This means .
    - By definition of Ker , .
    - Since is a homomorphism, .
    - Multiplying by on the left, we get .
    - Thus, . So, is well-defined.
  + **2. is a homomorphism:**
    - Let .
    - .
    - By definition of , .
    - Since is a homomorphism, .
    - Also, .
    - Since , is a homomorphism.
  + **3. is injective (one-to-one):**
    - Assume (the identity in ).
    - By definition of , .
    - By definition of Ker , if , then .
    - If , then the coset is equal to (which is the identity element in ).
    - Since the kernel of is trivial (only the identity element), is injective.
  + **4. is surjective (onto):**
    - Let .
    - Since is an onto homomorphism from to , there exists an element such that .
    - Consider the coset .
    - By definition of , .
    - Therefore, for every element , there exists a coset in that maps to it. So, is surjective.
  + Since is a well-defined, bijective homomorphism, it is an isomorphism.
  + Thus, .
* **Hence show that if G₁ is finite, then order of G₂ divides the order of G₁.**
  + If is a finite group, then its order is finite.
  + From the First Isomorphism Theorem, we have .
  + This means that .
  + By definition of the order of a factor group, .
  + Therefore, .
  + Rearranging this equation, we get .
  + Since is an integer (it's the order of a subgroup), this equation clearly shows that the order of divides the order of . This is also a direct consequence of Lagrange's Theorem applied to and its subgroup .

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(D₄).

* **Definition of the inner automorphism of G induced by a:**
  + For any element , the **inner automorphism of G induced by a**, denoted by , is a mapping from to defined by: for all .
* **Show that Inn(G) forms a subgroup of Aut(G):**
  + is the group of all automorphisms of . We need to show that satisfies the subgroup criteria.
  + **First, show that each is an automorphism:**
    1. **Homomorphism:** for all .
    2. **Injective:** Assume . Then . By cancellation (multiplying by on the left and on the right), .
    3. **Surjective:** Let . We need to find such that . . Since , for any , there exists an such that .
    - Therefore, each is an automorphism of , so .
  + **Now, show that Inn(G) is a subgroup of Aut(G):**
    1. **Non-empty:** The identity automorphism is an inner automorphism induced by . . So, . Thus, is non-empty.
    2. **Closure under composition:** Let for some . Consider their composition . . This is . Since , . Thus, is closed under composition.
    3. **Existence of inverses:** Let . We need to find its inverse. Consider . Since , . . Similarly, . So, .
    - Therefore, is a subgroup of .
* **Find Inn(D₄):**
  + is the dihedral group of order 8, representing the symmetries of a square.
  + Elements of are , where is a rotation by and is a reflection. We have , , and .
  + The group of inner automorphisms is isomorphic to , where is the center of .
  + Let's find .
    - .
    - commutes with all elements.
    - does not commute with ().
    - commutes with and : . So commutes with all elements.
    - does not commute with ().
    - does not commute with .
    - does not commute with (). (Alternatively, and . since ).
    - does not commute with .
    - does not commute with .
    - So, .
  + .
  + The elements of are for . However, if , then .
  + So, and .
  + The distinct inner automorphisms are generated by elements not in the center. We can pick representatives from the cosets of .
  + .
  + So the distinct inner automorphisms are .
  + Let's describe them by their action on the generators and :
    - .
    - . . So .
    - . . So .
    - . . So . (Wait, this is wrong: . This is incorrect. Let's recompute . This is still not right. Let's use the definition: . So .
* Let's re-evaluate the inner automorphisms based on representatives .
  + :
    - .
  + :
    - .
    - .
  + :
    - .
    - . (This is not ) Wait, . . Ah, so conjugation by is identity. . It's not the reflection itself.
* Let's check the group structure. has order 4. has order 1. . So . This means . . So . This means . . So is not correct. . This means maps to , 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 again: . This is correct. Now, : . . . . So . This means . All non-identity elements in have order 2. This means .
* **Inn(D₄) = { }** where:
  + (identity automorphism)
  + , (conjugation by )
  + , (conjugation by )
  + , (conjugation by ). Note that because . (e.g., and , these are not the same cosets).

Let's use the coset representatives as generators for the distinct inner automorphisms: . The distinct cosets are , , , .

* (induced by or )
* : , (induced by or )
* : , (induced by or )
* : , (induced by or )
  + Let's verify .
  + . So is different from .

The four distinct inner automorphisms are:

1. (conjugation by or )
2. (conjugation by or ). Acts as .
3. (conjugation by or ). Acts as .
4. (conjugation by or ). Acts as and .

Let's check the composition of these to confirm the structure. . . So . This is . All orders are 2. So it must be . where:

(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., |(g₁, g₂, ..., gₙ)| = lcm(|g₁|, |g₂|, ..., |gₙ|). Also, find the number of elements of order 7 in Z₄₉ ⊕ Z₇.

* **Proof:**
  + Let be the external direct product of finite groups .
  + Let be an element in , where .
  + Let be the order of in , and let be the order of in .
  + By definition, is the smallest positive integer such that , where is the identity element in .
  + .
  + So, means that .
  + This implies that for all .
  + For each , means that must be a multiple of .
  + Therefore, must be a common multiple of .
  + Since is the *smallest* such positive integer , it must be the least common multiple (LCM) of the orders of the components.
  + Hence, .
* **Find the number of elements of order 7 in Z₄₉ ⊕ Z₇:**
  + Let , where and .
  + We want to find the number of elements such that .
  + We know that .
  + For , the possible orders for and must be divisors of 7, i.e., 1 or 7.
  + Also, at least one of or must be 7.
* Let's list the possibilities for :
  + Case 1: .
    - Elements of order 1 in : Only . (1 element)
    - Elements of order 7 in : These are the elements such that . These are . ( elements)
    - Number of elements in this case: .
  + Case 2: .
    - Elements of order 7 in : These are the elements such that . These are of the form , where . So . (6 elements)
    - Elements of order 1 in : Only . (1 element)
    - Number of elements in this case: .
  + Case 3: .
    - Elements of order 7 in : 6 elements (as found above).
    - Elements of order 7 in : 6 elements (as found above).
    - Number of elements in this case: .
* Total number of elements of order 7 in is the sum of elements from these cases: Total = .

(c) Without doing any calculations in Aut(Z₁₀₅), determine how many elements of Aut(Z₁₀₅) have order 6.

* **Understanding Aut(Z\_n):**
  + The group of automorphisms of , denoted , is isomorphic to , the group of units modulo .
  + So, .
  + We need to find the number of elements of order 6 in .
* **Structure of U(105):**
  + .
  + Since is a product of distinct odd primes, is isomorphic to the direct product of the groups of its prime factors: .
  + Let's find the structure and orders of these component groups:
    - . This is isomorphic to . The only non-identity element (2) has order 2.
    - . This is isomorphic to . Elements of order 1, 2, 4. (e.g., , )
    - . This is isomorphic to . Elements of order 1, 2, 3, 6. (e.g., , )
* **Finding elements of order 6 in :**
  + An element in corresponds to a triplet .
  + The order of is .
  + We want this LCM to be 6.
  + The possible orders for are based on the orders of elements in respectively.
  + For , 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 such that their LCM is 6. We need . This implies that for each prime factor (2 and 3), the maximum power of that prime in the orders must be and . So, 3 must divide at least one of the orders, and 2 must divide at least one of the orders.
* Let , , .
  + (from )
    - Number of elements for : 1 (element )
    - Number of elements for : 1 (element )
  + (from )
    - Number of elements for : 1 (element )
    - Number of elements for : 1 (element )
    - Number of elements for : 2 (elements )
  + (from )
    - Number of elements for : 1 (element )
    - Number of elements for : 1 (element )
    - Number of elements for : 2 (elements )
    - Number of elements for : 2 (elements )
* Now we analyze the combinations for . We need:
  1. At least one order must be divisible by 3 (so must be 3 or 6).
  2. The maximum power of 2 in the orders is (so cannot be 4).
* Let's count elements based on combinations:
  + **Case A: .** (This automatically satisfies the 'divisible by 3' condition, and also the 'divisible by 2' condition).
    - Number of elements for : 2
    - For : Can be 1 or 2 (2 choices)
    - For : Can be 1 or 2 (2 choices) (Cannot be 4, otherwise lcm would be 12).
    - Number of elements = (choices for ) (choices for ) (choices for )
    - Number of elements = .
  + **Case B: .** (This satisfies the 'divisible by 3' condition). Now we need the 'divisible by 2' condition to be satisfied by or . And cannot be 4.
    - Number of elements for : 2
    - For : Can be 1 or 2. (Cannot be 4).
    - For : Can be 1 or 2.
  + We need . This means . This implies:
    - . (1 choice for , 1 choice for )
    - . (1 choice for , 1 choice for )
    - . (1 choice for , 1 choice for )
    - Total combinations for where :
      * (, ): 1 element of order 2 in , 1 element of order 1 in . (1 \* 1 = 1 combination)
      * (, ): 1 element of order 1 in , 1 element of order 2 in . (1 \* 1 = 1 combination)
      * (, ): 1 element of order 2 in , 1 element of order 2 in . (1 \* 1 = 1 combination)
      * So, 3 combinations for that yield LCM 2.
    - Number of elements = (choices for ) (choices for )
    - Number of elements = .
* Total number of elements of order 6 in is the sum of elements from these cases: Total = .
* So, there are **14** elements of order 6 in .

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

* **Proof:**
  + Let be a group and be its center. We know is a normal subgroup of .
  + Let be the set of all inner automorphisms of . We have already shown in Q5(a) that is a subgroup of .
  + Define a mapping by , where for all .
  + **1. is a homomorphism:**
    - Let . We need to show .
    - .
    - .
    - .
    - Since for all , we have .
    - Therefore, , so is a homomorphism.
  + **2. is surjective (onto):**
    - By definition, is the set of all for .
    - For any , there exists an element such that .
    - Thus, is surjective.
  + **3. Find the Kernel of (Ker ):**
    - , where is the identity automorphism.
    - , so .
    - This means for all .
    - for all .
    - Multiplying by on the right, for all .
    - By definition, the set of all elements that commute with every element in is the center of , .
    - Therefore, .
  + **4. Apply the First Isomorphism Theorem:**
    - Since is an onto homomorphism with , by the First Isomorphism Theorem (as proved in Q4(c)(i)), we have: .
    - Since is surjective, .
    - Substituting , we get .

(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 is the **internal direct product** of its subgroups if the following three conditions are met:
    1. Each is a normal subgroup of .
    2. (every element can be written as a product where ).
    3. For each , (the intersection of each subgroup with the product of the other subgroups is the identity element).
  + Alternatively, for two subgroups and of , is the internal direct product of and if:
    1. and are normal subgroups of .
    2. .
    3. .
  + (And for two subgroups, (1) can be relaxed to just for all if and because this implies normality for and within .)
* **Prove that R is the internal direct product of R⁺ and the subgroup {1, -1}:**
  + Let be the group of all non-zero real numbers under multiplication.
  + Let be the group of all positive real numbers under multiplication.
  + Let be a subgroup of under multiplication.
  + We need to verify the three conditions for internal direct product:
  + **1. H and K are normal subgroups of G:**
    - **H = R⁺:**
      * is a subgroup of (closed under multiplication, contains 1, has inverses for every element).
      * To show is normal in , we need to show for all and .
      * Let and . Then . Since , .
      * Alternatively, consider . Since , . The product of any two positive numbers is positive. If , then , . If , then , . So is always positive.
      * Therefore, is a normal subgroup of .
    - **K = {1, -1}:**
      * is a subgroup of (closed under multiplication: , , ; contains 1; inverses exist: ).
      * To show is normal in , we need to show for all and .
      * If , .
      * If , .
      * Therefore, is a normal subgroup of .
  + **2. G = HK:** (Every element in can be written as a product of an element from and an element from ).
    - Let .
    - If , then . We can write , where and .
    - If , then . So . We can write , where and .
    - Therefore, every element in can be expressed as a product of an element from and an element from . So .
  + **3. H ∩ K = {e}:** (The intersection of and is the identity element).
    - (set of positive real numbers).
    - .
    - The common element in both sets is only .
    - Therefore, .
  + Since all three conditions are satisfied, is the internal direct product of and .

(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 because its elements are precisely those integers relatively prime to 45.
  + .
  + The order of is .
  + The given set has 12 elements. Let's list them and compare with . . The provided set is a subset of . This implies that is a subgroup of .
  + Let's check the elements: . . has order 24. So is a subgroup of .
  + The prime-power factorization of the order of is .
  + We need to write as an external and internal direct product of cyclic groups of prime-power order.
  + The structure of groups: . . This is cyclic of order , so . (Generator e.g., 2: ). . This is cyclic of order , so . (Generator e.g., 2: ).
  + So, .
  + The elements of are: .
  + Let's consider elements modulo 9 and modulo 5 for elements in G.
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
    - , .
  + Mapping these to : .
  + Let . This is . It is isomorphic to .
  + Let . This is . It is isomorphic to .
  + The group consists of elements where the second component (modulo 5) is either 1 or 4.
  + The elements of with second component 1 or 4 are . This subgroup of has order 2 and is isomorphic to .
  + So, .
  + This means .
  + .
  + Since , we have .
  + Rearranging, .
* **External Direct Product of Cyclic Groups of Prime-Power Order:**
  + .
* **Internal Direct Product of Cyclic Groups of Prime-Power Order:**
  + Let's find the subgroups in corresponding to these cyclic groups.
  + In , elements of order 2 are those such that .
    - (order 2, not 1 in ).
    - (order 2, not 1 in ).
    - By CRT:
      * (order 1)
      * (order 2)
      * (order 2)
      * (order 2)
    - So, contains elements of order 2: .
  + Elements of order 3:
    - , . From , the elements of order 3 are .
    - , . From , there are no elements of order 3.
    - So, an element of order 3 in must have its 5-component of order 1.
    - gives 31. Order of is 3. (, , ).
    - gives 16. Order of is 3. (, , ).
  + The elements of order 2 are .
  + The elements of order 3 are .
  + The elements of order 4 (lcm(order in , order in ) is 4):
    - Order 4 can come from where .
    - where has order 4 in (i.e. ).
      * in corresponds to . . No, , order 6. , order 1. So . So 11 has order 6.
      * in corresponds to . should have order . . Let's solve . . So . . . Is ? No.
    - where .
      * gives . . . . .
* Let's reconsider the elements of G.
  + .
  + .
  + .
  + Let . This is .
  + Let . This is .
  + The elements of are precisely .
  + So, .
  + .
  + Now, decompose into prime-power order cyclic groups: .
  + Therefore, .
  + This is the **external direct product of cyclic groups of prime-power order.**
* **Internal Direct Product:**
  + We need to find subgroups within such that , , , and with trivial intersections.
  + We can use elements that correspond to the decomposition.
  + Let .
    - Elements of with : . This is a subgroup of order 2. Let . (, ).
  + Let .
    - Elements of with : . This is the subgroup projected onto .
    - This subgroup is isomorphic to . We need to split this further.
    - Subgroup of order 2: . , . . Let .
    - Subgroup of order 3: . , . . Let .
  + Let's check elements for the first (from the component of ). Let of order 2, . Let of order 1, . This corresponds to which is . So . This is .
  + Let's check elements for the second (from itself). Let of order 1, . Let of order 2, . This corresponds to which is . So . This is .
  + Let's check elements for the . Let of order 3, . Let of order 1, . This corresponds to which is . So . This is . (Note: , ).
  + Now, we need to check the internal direct product conditions for , , .
    1. **Normality:** All these subgroups are cyclic, and is abelian (as it is isomorphic to , which is abelian). In an abelian group, every subgroup is normal. So, this condition is satisfied.
    2. **Product spans G:** . This means will be if the intersections are trivial.
    3. **Trivial intersections:**
       - .
       - .
       - .
       - More generally, we need .
         * . Note . This is a group of order 4, isomorphic to .
         * .
  + Therefore, is the internal direct product of , , and .
  + **Internal Direct Product:** .
  + **External Direct Product:** .