

Solutions to Math 343-471 Final Exam

Question 1: True/False with Justification

(Choose 6 only)

1. The maximum order of an element in S_7 is 7. False. The order of an element in the symmetric group S_n is the least common multiple (LCM) of the lengths of the disjoint cycles in its cycle decomposition. To maximize the order, we look for a partition of $n = 7$ such that the LCM of the summands is maximized. Consider the partition $3 + 4 = 7$. The element $\sigma = (123)(4567) \in S_7$ has order $\text{lcm}(3, 4) = 12$. Since $12 > 7$, the statement is false.

2. If $\alpha, \beta \in S_n$ are conjugates, then they are both even or both odd. True. Two permutations in S_n are conjugates if and only if they have the same cycle structure (i.e., the same number of cycles of each length). The sign (parity) of a permutation is determined solely by its cycle structure. Specifically, a cycle of length k can be decomposed into $k - 1$ transpositions. Therefore, if α and β have the same cycle structure, they have the same number of transpositions modulo 2, meaning they have the same parity.

3. $\text{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_6$. True. The automorphism group of a cyclic group $\mathbb{Z}_n$ is isomorphic to the group of units $U(n)$ (also denoted as $\mathbb{Z}_n^\times$) under multiplication modulo n . The order is $|U(9)| = \phi(9) = 9(1 - 1/3) = 6$. The elements of $U(9)$ are $\{1, 2, 4, 5, 7, 8\}$. To determine the structure, we check if it is cyclic. Let's calculate the powers of 2 modulo 9: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 \equiv 7, 2^5 = 14 \equiv 5, 2^6 = 10 \equiv 1$. Since 2 generates the entire group, $U(9)$ is cyclic of order 6. Thus, $\text{Aut}(\mathbb{Z}_9) \cong U(9) \cong \mathbb{Z}_6$.

4. If n is an odd integer, then $\mathbb{Z}_2 \oplus \mathbb{Z}_n$ is cyclic. True. The direct sum of cyclic groups $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic if and only if $\text{gcd}(m, n) = 1$. Here, $m = 2$. Since n is an odd integer, it is not divisible by 2, so $\text{gcd}(2, n) = 1$. Therefore, $\mathbb{Z}_2 \oplus \mathbb{Z}_n \cong \mathbb{Z}_{2n}$, which is cyclic.

5. A group G is abelian if and only if $|\text{Inn}(G)| = 1$. True. The inner automorphism group, $\text{Inn}(G)$, consists of conjugations by elements of G . There is a known isomorphism $\text{Inn}(G) \cong G/Z(G)$, where $Z(G)$ is the center of G . If G is abelian, then $Z(G) = G$, so $\text{Inn}(G) \cong G/G \cong \{e\}$, which implies $|\text{Inn}(G)| = 1$. Conversely, if $|\text{Inn}(G)| = 1$, then $G/Z(G)$ is the trivial group, implying $G = Z(G)$, which means G is abelian.

6. A group cannot be isomorphic to one of its proper subgroups. False. This statement holds for finite groups but is false for infinite groups. Counterexample: Let $G = \mathbb{Z}$ (the integers under addition). The map $\phi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ defined by $\phi(x) = 2x$ is a bijection and a homomorphism. Thus, $\mathbb{Z} \cong 2\mathbb{Z}$. However, $2\mathbb{Z}$ is a proper subgroup of $\mathbb{Z}$.

7. Let A and B be groups. If $A \times B$ is cyclic then both A and B must be cyclic. True. If a direct product $G = A \times B$ is cyclic, then any subgroup and any homomorphic image of G must be cyclic. There is a natural projection homomorphism $\pi_A : A \times B \rightarrow A$ defined by $\pi_A(a, b) = a$. Since this map is surjective, A is a homomorphic image of a cyclic group, so A is cyclic. Similarly, B is cyclic.

8. A_4 is isomorphic to a subgroup of D_8 . False. The alternating group A_4 has order $|A_4| = 12$. The dihedral group D_8 (symmetries of a regular octagon) has order 16. By Lagrange's Theorem, the order of any subgroup of D_8 must divide the order of D_8 . Since 12 does not divide 16, D_8 cannot contain a subgroup of order 12. Therefore, A_4 cannot be isomorphic to a subgroup of D_8 .

Question 2

(a) Define what it means for a map $\varphi : G \rightarrow G'$ to be a homomorphism. A map $\varphi : G \rightarrow G'$ is a homomorphism if for all $x, y \in G$:

$$\varphi(xy) = \varphi(x)\varphi(y)$$

where the operation on the left is in G and the operation on the right is in G' .

(b) Show that if $H' \leq G'$ then $\varphi^{-1}(H') \leq G$. Let $K = \varphi^{-1}(H') = \{g \in G \mid \varphi(g) \in H'\}$. We check the subgroup criteria:

1. **Identity:** Since $\varphi(e_G) = e_{G'}$ and $e_{G'} \in H'$ (since $H' \leq G'$), we have $e_G \in K$.
2. **Closure:** Let $x, y \in K$. Then $\varphi(x) \in H'$ and $\varphi(y) \in H'$. Since φ is a homomorphism, $\varphi(xy) = \varphi(x)\varphi(y)$. Since H' is a subgroup, the product of two elements in H' is in H' . Thus $\varphi(xy) \in H'$, so $xy \in K$.
3. **Inverses:** Let $x \in K$. Then $\varphi(x) \in H'$. Since φ is a homomorphism, $\varphi(x^{-1}) = (\varphi(x))^{-1}$. Since H' is a subgroup, it contains the inverse of $\varphi(x)$. Thus $\varphi(x^{-1}) \in H'$, so $x^{-1} \in K$. Therefore, $\varphi^{-1}(H') \leq G$.

(c) Show that if $H' \triangleleft G'$, then $\varphi^{-1}(H') \triangleleft G$. Let $K = \varphi^{-1}(H')$. We know $K \leq G$ from part (b). To show normality, let $k \in K$ and $g \in G$. We must show $gkg^{-1} \in K$. Apply φ :

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1}$$

Since $k \in K$, $\varphi(k) \in H'$. Let $h' = \varphi(k)$. Then $\varphi(gkg^{-1}) = \varphi(g)h'\varphi(g)^{-1}$. Since H' is a normal subgroup of G' , the conjugate of any element in H' by any element in G' remains in H' . Thus, $\varphi(g)h'\varphi(g)^{-1} \in H'$. Since $\varphi(gkg^{-1}) \in H'$, it follows by definition that $gkg^{-1} \in \varphi^{-1}(H') = K$. Thus, $K \triangleleft G$.

(d) **State the First Isomorphism Theorem, then use it to show that there is no surjective homomorphism from A_4 onto D_4 .** **First Isomorphism Theorem:** Let $\varphi : G \rightarrow G'$ be a homomorphism. Then $G/\ker(\varphi) \cong \text{Im}(\varphi)$.

Proof: Assume there exists a surjective homomorphism $\varphi : A_4 \rightarrow D_4$. By the First Isomorphism Theorem, $A_4/\ker(\varphi) \cong D_4$. Taking the orders of the groups:

$$\frac{|A_4|}{|\ker(\varphi)|} = |D_4|$$

Substitute the known orders ($|A_4| = 12$ and $|D_4| = 8$):

$$\frac{12}{|\ker(\varphi)|} = 8$$

$$|\ker(\varphi)| = \frac{12}{8} = 1.5$$

The order of a subgroup (the kernel) must be an integer (Lagrange's Theorem). Since 1.5 is not an integer, no such kernel exists. Therefore, there is no surjective homomorphism from A_4 onto D_4 .

Question 3

(a) **Let $\alpha \in S_{10}$ be an element of order 6. What are the possible cycle decompositions of α ? Give an example for each possibility and determine if it is even or odd.**

The order of a permutation is the LCM of its cycle lengths. We need partitions of $n \leq 10$ such that the LCM of the parts is 6. Parity rule: A cycle of length k is Even if k is odd, and Odd if k is even. (Alternatively, parity is determined by $\sum(\text{length} - 1)$).

Possible Cycle Structures (sum of lengths ≤ 10 , LCM = 6):

1. 6-cycle

- *Structure:* (6)
- *Example:* (123456)
- *Parity:* Length 6 is even, so permutation is **Odd**.

2. 6-cycle + 2-cycle

- *Structure:* (6)(2)
- *Example:* (123456)(78)
- *Parity:* Odd $\times$ Odd = **Even**.

3. **6-cycle + 3-cycle**

- Structure: $(6)(3)$
- Example: $(123456)(789)$
- Parity: $\text{Odd} \times \text{Even} = \text{Odd}$.

4. **6-cycle + 2-cycle + 2-cycle**

- Structure: $(6)(2)(2)$
- Example: $(123456)(78)(9\ 10)$
- Parity: $\text{Odd} \times \text{Odd} \times \text{Odd} = \text{Odd}$.

5. **3-cycle + 2-cycle**

- Structure: $(3)(2)$
- Example: $(123)(45)$
- Parity: $\text{Even} \times \text{Odd} = \text{Odd}$.

6. **3-cycle + 2-cycle + 2-cycle**

- Structure: $(3)(2)(2)$
- Example: $(123)(45)(67)$
- Parity: $\text{Even} \times \text{Odd} \times \text{Odd} = \text{Even}$.

7. **3-cycle + 2-cycle + 2-cycle + 2-cycle**

- Structure: $(3)(2)(2)(2)$
- Example: $(123)(45)(67)(89)$
- Parity: $\text{Even} \times \text{Odd} \times \text{Odd} \times \text{Odd} = \text{Odd}$.

8. **3-cycle + 3-cycle + 2-cycle**

- Structure: $(3)(3)(2)$
- Example: $(123)(456)(78)$
- Parity: $\text{Even} \times \text{Even} \times \text{Odd} = \text{Odd}$.

(b) Let G be a group and $A, B \trianglelefteq G$. Show that $A \cap B \triangleleft G$. Deduce that $A/(A \cap B)$ is a subgroup of $G/(A \cap B)$. Is it also normal? Justify. (Note: The problem text " $A, B \trianglelefteq G$ " is interpreted as A, B being normal subgroups based on the context of the required proof).

Show $A \cap B \triangleleft G$:

1. **Subgroup:** The intersection of two subgroups is always a subgroup.
2. **Normality:** Let $x \in A \cap B$ and $g \in G$. We need to show $gxg^{-1} \in A \cap B$.
 - Since $x \in A$ and $A \trianglelefteq G$, $gxg^{-1} \in A$.

- Since $x \in B$ and $B \trianglelefteq G$, $gxg^{-1} \in B$.
- Therefore, $gxg^{-1} \in A \cap B$.
- Thus, $A \cap B \triangleleft G$.

Deduce $A/(A \cap B)$ is a subgroup of $G/(A \cap B)$: Since $A \leq G$ and $A \cap B \trianglelefteq G$, the set of cosets $A/(A \cap B) = \{a(A \cap B) \mid a \in A\}$ is clearly a subset of the quotient group $G/(A \cap B) = \{g(A \cap B) \mid g \in G\}$. Since A is a subgroup of G , the product of two cosets from A yields a coset represented by an element in A , and inverses form cosets in A . Thus, it forms a subgroup.

Is it also normal? Yes. Since $A \trianglelefteq G$, for any $a \in A$ and $g \in G$, the conjugate $gag^{-1} \in A$. Consider an element $\bar{a} = a(A \cap B)$ in the subgroup and $\bar{g} = g(A \cap B)$ in the larger group.

$$\begin{aligned}\bar{g}\bar{a}\bar{g}^{-1} &= (g(A \cap B))(a(A \cap B))(g^{-1}(A \cap B)) \\ &= (gag^{-1})(A \cap B)\end{aligned}$$

Since $gag^{-1} \in A$, this resulting coset is an element of $A/(A \cap B)$. Therefore, $A/(A \cap B) \trianglelefteq G/(A \cap B)$.

Question 4

(a) Let $G = \mathbb{Z}_8 \oplus \mathbb{Z}_9$. Compute $|(6,6)|$. How many elements of order 6 does G have?

Compute $|(6,6)|$: The order of an element (a,b) in a direct product is $\text{lcm}(|a|, |b|)$.

- In $\mathbb{Z}_8$, the element 6 has order: $6 \cdot 1 = 6 \neq 0$, $6 \cdot 2 = 12 \equiv 4$, $6 \cdot 3 = 18 \equiv 2$, $6 \cdot 4 = 24 \equiv 0$. So $|6| = 4$.
- In $\mathbb{Z}_9$, the element 6 has order: $6 \cdot 1 = 6 \neq 0$, $6 \cdot 2 = 12 \equiv 3$, $6 \cdot 3 = 18 \equiv 0$. So $|6| = 3$.
- Order of $(6,6) = \text{lcm}(4,3) = 12$.

Number of elements of order 6: Note that $\gcd(8,9) = 1$, so $G \cong \mathbb{Z}_{72}$. G is a cyclic group of order 72. In a cyclic group of order n , the number of elements of order d (where $d|n$) is exactly $\phi(d)$ (Euler's totient function). Since 6 divides 72, the number of elements of order 6 is:

$$\phi(6) = \phi(2)\phi(3) = (1)(2) = 2$$

The group has exactly 2 elements of order 6.

(b) Classify all abelian groups of order 225. Show that every abelian group of order 225 must have an element of order 15.

Classification: Order $225 = 3^2 \cdot 5^2$. We use the Fundamental Theorem of Finite Abelian Groups. We find the possible isomorphism types by partitioning the powers of the primes.

- For $p = 3$ (3^2):
 1. $\mathbb{Z}_9$
 2. $\mathbb{Z}_3 \oplus \mathbb{Z}_3$
- For $p = 5$ (5^2):
 1. $\mathbb{Z}_{25}$
 2. $\mathbb{Z}_5 \oplus \mathbb{Z}_5$

Possible combinations (isomorphism classes):

1. $\mathbb{Z}_9 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{225}$
2. $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{75}$
3. $\mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{45}$
4. $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{15}$

Proof of element of order 15: We must show that each of these groups contains an element of order 15. Note that for an abelian group $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ where $n_1 | n_2 | \cdots | n_k$, the largest order of an element is n_k . Alternatively, the exponent of the group is lcm of the orders of the components. Let's check the exponent (max order) for each case:

1. $\mathbb{Z}_{225}$: Contains element of order 225. Since $15 | 225$, there is a subgroup of order 15, hence an element of order 15.
2. $\mathbb{Z}_3 \oplus \mathbb{Z}_{75}$: Max order is $\text{lcm}(3, 75) = 75$. Since $15 | 75$, there is an element of order 15.
3. $\mathbb{Z}_5 \oplus \mathbb{Z}_{45}$: Max order is $\text{lcm}(5, 45) = 45$. Since $15 | 45$, there is an element of order 15.
4. $\mathbb{Z}_{15} \oplus \mathbb{Z}_{15}$: Max order is $\text{lcm}(15, 15) = 15$. There is clearly an element of order 15 (e.g., $(1, 0)$).

Since the maximum order (exponent) in every case is a multiple of 15, and the groups are abelian, an element of order 15 always exists.

Question 5

(a) Define what it means for a subgroup of a finite group to be a Sylow p -subgroup. Let G be a finite group of order $|G| = p^n m$, where p is a prime number and $\gcd(p, m) = 1$. A subgroup P of G is called a **Sylow p -subgroup** if $|P| = p^n$. (Equivalently, it is a maximal p -subgroup of G).

(b) Classify all Sylow p -subgroups of S_4 and decide whether each normal or not. Order of S_4 : $|S_4| = 4! = 24 = 2^3 \cdot 3$. The prime factors are 2 and 3.

Sylow 2-subgroups: Order: $2^3 = 8$. Number of subgroups (n_2): $n_2 \equiv 1 \pmod{2}$ and $n_2 | 3$. Possibilities: 1, 3. In S_4 , the Sylow 2-subgroups are isomorphic to D_4 (the dihedral group of order 8). We can generate them by looking for copies of D_4 . One such group is generated by (1234) and (13) . Since there are multiple such subgroups (specifically, there are 3: corresponding to the 3 ways to pair up the 4 elements into orthogonal axes, or simply by counting n_2), $n_2 = 3$. Since $n_2 \neq 1$, the Sylow 2-subgroups are **not normal**.

Sylow 3-subgroups: Order: $3^1 = 3$. Number of subgroups (n_3): $n_3 \equiv 1 \pmod{3}$ and $n_3 | 8$. Possibilities: 1, 4. Elements of order 3 in S_4 are 3-cycles (abc) . There are $\frac{4 \times 3 \times 2}{3} = 8$ distinct 3-cycles. Each subgroup of order 3 contains 2 distinct 3-cycles. Total number of subgroups = $8/2 = 4$. So $n_3 = 4$. Since $n_3 \neq 1$, the Sylow 3-subgroups are **not normal**.

(c) Prove that a group of order pq is cyclic, where p and q are odd primes. (Note: This statement is true under the condition that $p < q$ and p does not divide $q - 1$. If $p | q - 1$, non-abelian groups exist. Assuming the standard conditions for this theorem).

Assumption: Let p and q be primes such that $p < q$ and $p \nmid (q - 1)$. **Proof:**

1. **Sylow q -subgroup:** Let n_q be the number of Sylow q -subgroups. By Sylow's Theorems: $n_q \equiv 1 \pmod{q}$ and $n_q | p$. Since p is prime and $p < q$, the only divisor of p that is congruent to 1 mod q is 1. Thus, $n_q = 1$. Let Q be the unique Sylow q -subgroup. Since it is unique, $Q \triangleleft G$.
2. **Sylow p -subgroup:** Let n_p be the number of Sylow p -subgroups. By Sylow's Theorems: $n_p \equiv 1 \pmod{p}$ and $n_p | q$. The divisors of q are 1 and q . If $n_p = q$, then $q \equiv 1 \pmod{p}$, which implies $p | (q - 1)$. By our assumption that $p \nmid (q - 1)$, we must have $n_p = 1$. Let P be the unique Sylow p -subgroup. Thus, $P \triangleleft G$.
3. **Cyclic Structure:** Since $P \triangleleft G$ and $Q \triangleleft G$ with $P \cap Q = \{e\}$ (orders are coprime), G is isomorphic to the direct product $P \times Q$. P is cyclic of order p (prime order). Q is cyclic of order q (prime order). $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Since $\gcd(p, q) = 1$, $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. Therefore, G is cyclic.