

Name: **Solution Key**

Math 343

May 4, 2026

## Midterm Exam 2

Time: 90 minutes

Student ID #: \_\_\_\_\_

| Question # | 1 | 2 | 3 | 4 | 5 | Total |
|------------|---|---|---|---|---|-------|
| Score      |   |   |   |   |   |       |

1. Justify answers and show all work for full credit.
2. Answer the questions in the space provided. If you run out of room continue on the back of the page.

---

[4 pts] **Q1: Determine whether each statement is true or false and justify your answer. (Choose 4 only)**

**1. The set of odd permutations in  $S_n$  forms a subgroup.**

**Solution: FALSE.** A subgroup must contain the identity element. The identity permutation is always an even permutation, so it is not in the set of odd permutations. Additionally, the set is not closed under the group operation (the product of two odd permutations is an even permutation).

**2. The group  $\mathbb{Z} \oplus \mathbb{Z}$  is cyclic.**

**Solution: FALSE.** If it were cyclic, it would be generated by a single element  $(a, b)$ . This means every element in  $\mathbb{Z} \oplus \mathbb{Z}$  would take the form  $(ka, kb)$  for some integer  $k$ . To generate  $(1, 0)$  and  $(0, 1)$ , we would need integers  $k_1, k_2$  such that  $k_1a = 1, k_1b = 0$  and  $k_2a = 0, k_2b = 1$ . The first implies  $b = 0$ , but if  $b = 0$ , we cannot satisfy  $k_2b = 1$ . Thus, no single generator exists.

**3. The group  $\mathbb{Z}_{16} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{999}$  is cyclic.**

**Solution: TRUE.** A finite external direct product of cyclic groups  $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$  is cyclic if and only if the moduli are pairwise relatively prime. Since  $16 = 2^4$ ,  $25 = 5^2$ , and neither 2 nor 5 divide 999. We have  $(\gcd(16, 25) = 1, \gcd(16, 999) = 1, \gcd(25, 999) = 1)$ . Therefore, the group is cyclic.

**4. If  $H, K \leq G$  with  $|H| = 12$  and  $|K| = 35$ , then we must have  $H \cap K = \{e\}$ .**

**Solution: TRUE.**  $H \cap K$  is a subgroup of both  $H$  and  $K$ . By Lagrange's Theorem, the order of  $H \cap K$  must divide both  $|H| = 12$  and  $|K| = 35$ . The only positive integer that divides both 12 and 35 is 1. Since  $|H \cap K| = 1$ , the intersection contains only the identity element.

**5. If  $H, K \leq G$  with  $|G| = 180$ ,  $|H| = 10$ , and  $|K| = 20$  then we must have  $H \cap K = \{e\}$ .**

**Solution: FALSE.** Assume by way of contradiction that  $H \cap K = \{e\}$ , meaning  $|H \cap K| = 1$ . We use the formula for the size of the product of two subgroups:  $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{10 \times 20}{1} = 200$ . However,  $HK$  is a subset of  $G$ , so  $|HK|$  cannot exceed  $|G| = 180$ . Since  $200 \leq 180$  is a contradiction, the intersection  $H \cap K$  must have an order strictly greater than 1.

**6. The element  $(2, 4, 6)$  in  $\mathbb{Z}_6 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{12}$  has the largest possible order.**

**Solution: FALSE.** The maximum possible order of any element in this group is  $\text{lcm}(6, 5, 12) = 60$  (achieved by the element  $(1, 1, 1)$ ). The order of  $(2, 4, 6)$  is the lcm of the orders of its components:

- $|2|$  in  $\mathbb{Z}_6$  is  $6/\gcd(2, 6) = 3$ .
- $|4|$  in  $\mathbb{Z}_5$  is  $5/\gcd(4, 5) = 5$ .
- $|6|$  in  $\mathbb{Z}_{12}$  is  $12/\gcd(6, 12) = 2$ .

The order of  $(2, 4, 6)$  is  $\text{lcm}(3, 5, 2) = 30$ . Since  $30 < 60$ , it does not have the largest possible order.

---

[4pts] **Q2: Let  $\alpha = (1\ 3\ 5\ 6\ 8)(2\ 4\ 5\ 8) \in S_8$ .**

**(i) Write  $\alpha$  as a product of disjoint cycles, find its order.**

**Solution:** Evaluating the permutations from right to left, we have:  $\alpha = (1\ 3\ 5)(2\ 4\ 6\ 8)$ .

The order is the least common multiple of the lengths of the disjoint cycles:  $|\alpha| = \text{lcm}(3, 4) = 12$ .

**(ii) Write  $\alpha$  as a product of transpositions and determine if it is even or odd.**

**Solution:** We can break down the disjoint cycles into transpositions:

$$(1\ 3\ 5) = (1\ 5)(1\ 3)$$

$$(2\ 4\ 6\ 8) = (2\ 8)(2\ 6)(2\ 4)$$

$$\text{Thus, } \alpha = (1\ 5)(1\ 3)(2\ 8)(2\ 6)(2\ 4).$$

Because  $\alpha$  is composed of 5 transpositions (an odd number), it is an **odd** permutation.

**(iii) Show that  $\langle \alpha \rangle \cap A_8 = \langle \alpha^2 \rangle$  (Hint: Which powers of  $\alpha$  are even permutations?)**

**Solution:** The alternating group  $A_8$  consists exactly of all the even permutations in  $S_8$ . From part (ii), we know  $\alpha$  is an odd permutation. The product of two odd permutations is even, and the product of an even and an odd permutation is odd. Therefore, the power  $\alpha^k$  is an even permutation if and only if  $k$  is an even integer. This implies that  $\alpha^k \in A_8 \iff k = 2m$  for some integer  $m$ . Thus, the elements in  $\langle \alpha \rangle$  that are also in  $A_8$  are exactly the powers of  $\alpha^2$ , which generates the subgroup  $\langle \alpha^2 \rangle$ . Hence,  $\langle \alpha \rangle \cap A_8 = \langle \alpha^2 \rangle$ .

---

[(1+1.5+1.5)pts] **Q3:**

**(a) Define what it means for a map  $f$  to be an isomorphism from a group  $G$  to a group  $G'$**

**Solution:** A map  $f : G \rightarrow G'$  is an isomorphism if it satisfies two conditions:

1.  $f$  is a bijection (it is both one-to-one/injective and onto/surjective).
2.  $f$  preserves the group operation, meaning  $f(xy) = f(x)f(y)$  for all  $x, y \in G$ .

**(b) Determine with justification if any of the following groups are isomorphic:  $\mathbb{R}^+$ ,  $\mathbb{R}^*$  and  $\mathbb{R}$ .**

**Solution:**

- $\mathbb{R}$  (reals under addition) is isomorphic to  $\mathbb{R}^+$  (positive reals under multiplication). An explicit isomorphism is the exponential function  $f(x) = e^x$ . It is a bijection and preserves the operation:  $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$ .

- $\mathbb{R}^*$  (non-zero reals under multiplication) is **not** isomorphic to either  $\mathbb{R}$  or  $\mathbb{R}^+$ .  $\mathbb{R}^*$  contains an element of order 2 (namely,  $-1$ , since  $(-1)^2 = 1$ ). However, neither  $\mathbb{R}$  nor  $\mathbb{R}^+$  has any elements of order 2. Since isomorphisms preserve element orders,  $\mathbb{R}^*$  cannot be isomorphic to the others.

Conclusion:  $\mathbb{R} \cong \mathbb{R}^+$ , but  $\mathbb{R}^* \not\cong \mathbb{R}$  and  $\mathbb{R}^* \not\cong \mathbb{R}^+$ .

**(c) Determine with justification if any of the following groups are isomorphic:**  $D_6, A_4$ , and  $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ .

**Solution:** None of these groups are isomorphic to each other.

- $\mathbb{Z}_2 \oplus \mathbb{Z}_6$  is an abelian group, whereas both  $D_6$  and  $A_4$  are non-abelian. Therefore, the abelian group cannot be isomorphic to the non-abelian ones.
- To distinguish between  $D_6$  and  $A_4$ , we look at element orders.  $D_6$  contains a rotation of order 6. However,  $A_4$  (even permutations of 4 elements) contains only elements of order 1, 2 (products of disjoint transpositions), and 3 (3-cycles). Because  $A_4$  has no element of order 6,  $D_6 \not\cong A_4$ .

**[(1+1.5+1.5) pts] Q4: How many elements of order 2 and 4 in each of the following groups:**  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,  $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ , and  $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ ?

**Solution:**

**Group 1:**  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$  (Total 4 elements)

**Order 2:** The identity element  $(0,0)$  has order 1. The remaining 3 elements  $(1,0), (0,1), (1,1)$  all have order 2. So, there are **3 elements of order 2**.

**Order 4:** The maximum element order in this group is  $\text{lcm}(2,2) = 2$ . Therefore, there are **0 elements of order 4**.

**Group 2:**  $\mathbb{Z}_2 \oplus \mathbb{Z}_4$  (Total 8 elements)

**Order 2:** An element  $(a,b)$  has an order dividing 2 if  $2a \equiv 0 \pmod{2}$  and  $2b \equiv 0 \pmod{4}$ . This means  $a \in \{0,1\}$  (2 choices) and  $b \in \{0,2\}$  (2 choices). There are  $2 \times 2 = 4$  such elements. Subtracting the identity element leaves  $4 - 1 =$  **3 elements of order 2**.

**Order 4:** An element  $(a,b)$  has order 4 iff its order does not divide 2. Since the maximum order is  $\text{lcm}(2,4) = 4$ , all remaining elements must have order 4. So,  $8 - 4 =$  **4 elements of order 4**.

(Alternatively,  $|b|$  must be 4, so  $b \in \{1,3\}$  (2 choices) and  $a \in \{0,1\}$  (2 choices), giving  $2 \times 2 = 4$  elements).

**Group 3:**  $\mathbb{Z}_4 \oplus \mathbb{Z}_4$  (Total 16 elements)

**Order 2:** Similar to above, elements whose order divides 2 require  $2a \equiv 0 \pmod{4}$  and  $2b \equiv 0 \pmod{4}$ , meaning  $a \in \{0,2\}$  and  $b \in \{0,2\}$ . There are  $2 \times 2 = 4$  such elements. Subtracting the identity gives  $4 - 1 =$  **3 elements of order 2**.

**Order 4:** Every element in this group has an order dividing 4. The elements of order 4 are exactly those whose order does not divide 2. So,  $16 - 4 =$  **12 elements of order 4**.

**[4pts] Q5: Compute the order of each of the following groups and determine if it is cyclic or not:**  $\text{Aut}(\mathbb{Z})$ ,  $\text{Aut}(\mathbb{Z}_9)$ ,  $\text{Aut}(\mathbb{Z}_{20})$  and  $\text{Inn}(\mathbb{Z}_{20})$ .

**Solution:**

**1.  $\text{Aut}(\mathbb{Z})$**

An automorphism of  $\mathbb{Z}$  must map the generator 1 to another generator. The only generators of  $\mathbb{Z}$  are 1 and  $-1$ . Thus, there are only 2 automorphisms: the identity map and the negation map.

$\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$ .

**Order = 2. It IS cyclic.**

**2.  $\text{Aut}(\mathbb{Z}_9)$**

For finite cyclic groups,  $\text{Aut}(\mathbb{Z}_n) \cong U(n)$ . Here,  $U(9)$  has an order of  $\phi(9) = 9(1 - 1/3) = 6$ . Gauss's theorem tells us that  $U(3^2)$  is isomorphic to  $\mathbb{Z}_6$ .

**Order = 6. It IS cyclic.**

**3.  $\text{Aut}(\mathbb{Z}_{20})$**

$\text{Aut}(\mathbb{Z}_{20}) \cong U(20)$ . The order is  $\phi(20) = \phi(4)\phi(5) = 2 \times 4 = 8$ .

We can decompose  $U(20)$  as  $U(4) \oplus U(5) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$ . An external direct product of cyclic groups is cyclic if and only if the moduli are coprime. Since  $\gcd(2, 4) = 2 \neq 1$ , the group is not cyclic.

**Order = 8. It is NOT cyclic.**

**4.  $\text{Inn}(\mathbb{Z}_{20})$**

Since  $\mathbb{Z}_{20}$  is abelian, conjugation by any element is the identity map. So it is the trivial group containing only the identity automorphism.

**Order = 1. It IS cyclic** (the trivial group is cyclic, generated by the identity).