

# MATH 109 MIDTERM 1

Wednesday, January 26, 2005

Name: \_\_\_\_\_

Numeric Student ID: \_\_\_\_\_

Instructor's Name: \_\_\_\_\_

I agree to abide by the terms of the honor code:

Signature: \_\_\_\_\_

**Instructions:** Print your name, student ID number and instructor's name in the space provided. During the test you may not use notes, books or calculators. Read each question carefully and **show all your work**; full credit cannot be obtained without sufficient justification for your answer unless explicitly stated otherwise. Underline your final answer to each question. There are 7 questions. You have 90 minutes to do all the problems.

Question	Score	Maximum
1		10
2		6
3		10
4		5
5		10
6		10
7		10
Total		61

1. Determine if the following sets  $G$  with the indicated operation form a group by checking the group axioms. If not, point out which of the group axioms fail.

- (a)  $G = \{1, 5\}$  with operation  $*$  multiplication modulo 6.

**Solution:**

Check closure and identity and inverse with a 2x2 group table. Associativity in groups under modular multiplication follows from associativity of integers under multiplication. So  $G$  is a group.

- (b)  $G = \{1, 3, 5, 7, 9\}$  with operation  $*$  multiplication modulo 10.

**Solution:**

This is not a group since 5 doesn't have an inverse. You can show this by either finding the inverses of 1, 3, 7, and 9 (3 is inverse of 7, 9 is own inverse) and showing 5 is not its own inverse. Or you can argue that since 5 is not relatively prime to 10, there is no such  $k$  such that  $5k = 10j + 1$  for some  $j$ .

- (c)  $G = \{\text{functions } f_{a,b} = ax + b \text{ such that } a, b \in \mathbb{R}, a \neq 0\}$ , the set of linear functions of a real variable  $x$  with  $*$  given by composition of functions.

**Solution:**

This is a group under composition of functions.

$$f_{c,d} \circ f_{a,b}(x) = f_{c,d}(ax + b) = c(ax + b) + d$$

which is again a linear function with  $ac \neq 0$  if  $a, c \neq 0$ . The identity function is the linear function which takes  $x \rightarrow x$ , so pick  $a = 1$  and  $b = 0$ . For inverses, looking at the above composition, we need to pick  $c, d$  so that  $(ca)x + cb + d = x$ , the identity element. So choose  $c = 1/a$  and  $d = -b/a$  which is well-defined since  $a \neq 0$ . Associativity follows since composition of functions is always associative.

- (d)  $G = \mathbb{R} - \{0\}$ , the set of non-zero real numbers with operation  $*$  given by  $a * b = a^2b$ . So for example,  $2 * 3 = 2^2(3) = 12$ .

**Solution:**

This fails several of the group axioms. First, there is no identity element, since for any proposed identity  $e$ ,

$$a * e = a^2e \text{ which must equal } a \text{ if } e \text{ is the identity}$$

So then  $e = 1/a$ . Pick any other real number  $b \neq a$  and then  $b * 1/a = b^2/a \neq b$ . If there's no identity element, then there is no way to define inverses. It further fails associativity:

$$(a * b) * c = a^2b * c = a^4b^2c \neq a^2b^2c = a * (b * c)$$

- (e)  $G$  is the set of  $2 \times 2$  matrices with real number entries and trace (i.e. sum of entries on the main diagonal) equal to 0 with operation  $*$  addition of matrices.

**Solution:**

This does form a group under addition. It's closed since the real numbers are closed under addition and matrix addition is done component-wise. It's identity is the matrix

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

which differs from the identity matrix under multiplication, with 1's on the diagonal. Then the inverse of a matrix  $A$  is easily shown to be  $-A$  and associativity follows from associativity of addition of real numbers.

2. Show that  $G = \mathbb{Z}[i] = \{a + bi, \text{ complex numbers such that } a, b \in \mathbb{Z}\}$  forms a group under addition of complex numbers. Then find 2 proper subgroups (i.e. not  $\{e\}$  or the entire group  $G$ ) of this group (that is, check that the 2 proper subsets you choose satisfy the axioms required to be a subgroup).

**Solution:**

The addition in the complex numbers is given by

$$a + bi + c + di = (a + c) + (b + d)i$$

so all of the group axioms essentially follow from those of the integers. It's closed since the sum of any two integers is an integer, hence  $(a + c)$  and  $(b + d)$  are both integers. The identity element is just  $0 = 0 + 0i$  and inverses are  $-a - bi$  for any element  $a + bi$ . Associativity follows since the addition in the integers is associative. To find proper subgroups, there are many approaches. In particular, pick any element  $g$  and consider the subgroup generated by  $g$ , denoted  $\langle g \rangle$ . This will always be a proper subgroup since  $G$  is not cyclic. Here are some examples of that:

- (a) The integers form a group under addition, and are contained in  $\mathbb{Z}[i]$  so they form a subgroup (generated by  $(1)$ ).
- (b) The subgroup of all even integers, generated by the element  $(2)$ .
- (c) The subgroup of all  $a + bi$  such that  $a = b$ , generated by the element  $(1+i)$
- (d) The subgroup of all  $a + bi$  such that  $a$  is even and  $b$  is a multiple of 3. This is an example of a proper subgroup not generated by a single element. It is generated by  $2$  and  $3i$ .

3. (a) Find the order of the following elements of  $S_7$ , the symmetric group on the set  $\{1, 2, \dots, 7\}$ .

i.  $(1\ 7)(6\ 4\ 5)(2)(3)$

**Solution:**

The least common multiple of cycle lengths is 6 and the permutation is written as a product of disjoint cycles, so the order of the element is 6.

ii.  $(1\ 3)(2\ 3)(4\ 1\ 5\ 7)$

**Solution:**

This permutation is not composed of disjoint cycles. We need to rewrite it as a product of disjoint ones. Doing this we find the above is equal to

$$(1\ 5\ 7\ 4\ 3\ 2)$$

which has order 6.

iii.  $(2\ 1\ 3\ 4\ 5\ 7\ 6)(2\ 1\ 3\ 4\ 5\ 7\ 6)$

**Solution:**

The cycle  $(2\ 1\ 3\ 4\ 5\ 7\ 6)$  is of length 7, so this element, call it  $x$  has order 7. But the permutation above is  $x^2$ . Since 2 and 7 are relatively prime, no smaller power of  $x^2$  is taken to the identity, so the order of  $x^2$  is also 7. (Note  $(x^2)^7 = x^{14} = e$ .) One could also just rewrite the above as a product of disjoint cycles:

$$(2\ 3\ 5\ 6\ 1\ 4\ 7)$$

which is of order 7.

- (b) Find a subgroup of order 6 and a subgroup of order 12 in  $S_7$ .

**Solution:**

There are lots of ways to find such subgroups. One is to consider the subgroup generated by a single element of order 6, like either of the ones you found in part (a) or (b) above. Then the order of the subgroup is just the number of distinct powers of the generating element, so also equal to 6. Similarly,

$$(1\ 2\ 3\ 4)\ (5\ 6\ 7)$$

is an element of order 12 according to the lcm of 4 and 3, so it generates a subgroup of order 12. There are other subgroups of orders 6 and 12 as well, like  $S_3$ , which permutes just 1,2,3. These permutations are a subset of those that permute 1,2,3,4,5,6,7. They fix 4 through 7. So this is a subgroup of order 6. Similarly,  $A_4$  is a subgroup of  $S_n$  for any  $n \geq 4$  and has order 12.

- (c) What is the smallest  $n$  for which  $S_n$  contains a subgroup of order 11? Explain your reasoning.

**Solution:**

Answer:  $n=11$ . Since the subgroup would necessarily be cyclic (by Lagrange's theorem), so would have to contain an element of order 11.

4. Given any positive integer  $n$ , let  $D_n$  be the dihedral group of  $2n$  elements (the group of symmetries of the regular  $n$ -gon). If  $n$  is even, find all elements  $x$  of  $D_n$  for which

$$x * y = y * x \quad \text{for all } y \in D_n.$$

Be sure to explain why your list is complete.

**Solution:**

To satisfy the above condition, an element  $x$  of  $D_n$  must commute with EVERY other element in  $D_n$  and this is a restrictive condition for elements in a non-abelian group to satisfy. We know that the  $2n$  elements of  $D_n$  can be written:

$$\{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

Let's see if any element of the form  $r^k$  could satisfy this condition (which we now know means that  $r^k$  is in the center  $Z(G)$ .) If so

$$r^l r^k = r^k r^l, \quad sr^l r^k = r^k sr^l \quad \text{for any choice of } l \in \{0, 1, \dots, n-1\}.$$

The first equality is clearly true since both sides are  $r^{k+l}$  with  $k+l$  chosen mod  $n$ . For the second required equality, we must check that they are the same element in our list of  $2n$  elements by applying the relation  $sr = r^{n-1}s$  and rewriting both sides as an element of the form  $r^j$  or  $sr^j$ . Doing this we see the left hand side is still  $sr^{k+l}$  for  $k+l$  mod  $n$  and the right hand side is  $sr^{n-k+l}$ . So the two sides are equal FOR EVERY  $l$  if  $k \equiv n-k$  mod  $n$ . That is,  $k = 0$ , or  $k = n/2$  (which is an integer since  $k$  even). Checking the same for an element of the form  $r^k s$  shows that no such element commutes with all other elements of  $D_n$ . So the complete list is  $\{e, r^{n/2}\}$ .

5. Prove or find a counterexample to the following statement: The elements of order  $\leq 3$  in a group  $G$  form a subgroup.

**Solution:**

You can prove every subgroup axiom except closure, and this is the real problem. An element of order 2 and an element of order 3 typically have a product whose order is 6. (Unless the group has order 6, in which case the product may be the identity as in  $D_3$ .) There are lots of counterexamples that you can suggest.  $D_n$  for  $n > 3$  works, as does  $S_n$  for  $n > 3$ . Or even  $\mathbb{Z}/6\mathbb{Z}$  under addition. There, 2 has order 3 and 3 has order 2, but  $2+3 = 5$  has order 6.

6. If  $G$  is a group such that  $x^2 = e$  for all  $x$  in  $G$ , prove that  $G$  is abelian.

**Solution:**

There are many ways to get from  $x^2 = e$  for all  $x \in G$  to showing  $xy = yx$  for all pairs  $x, y$  in  $G$ . The key observation is that any element is its own inverse according to this assumption. Here's one proof: For any  $x, y$  in  $G$

$$(x * y)^2 = x * y * x * y = e \quad \text{since } x * y \in G \text{ by closure}$$

But

$$x * y * y * x = x * (y * y) * x = x * e * x = e$$

using associativity, and the  $x^2 = e$  assumption. So putting these together

$$x * y * x * y = x * y * y * x$$

Cancelling  $x$  and  $y$  on the left by multiplying by inverses gives the result.

7. If  $G$  is a group with an even number of elements, show that the number of elements with order exactly equal to 2 is odd. (Hint: first show that an element of order 2 always exists for such a group.)

**Solution:**

To show that an element of order 2 exists, note that the order of the group is even and the identity is one of these. This leaves an odd number of non-identity elements. Now  $G$  is a group so every element has a unique inverse. Pairing these odd number of elements up, at least one element in the group must be its own inverse. That is  $x * x = e$ . So this  $x$  is of order 2. Note that there could never be an even number of non-identity elements which are their own inverse since this would leave an odd number of remaining non-identity elements, which all must be uniquely paired with other elements. Hence, the number of non-identity elements which are their own inverse is odd. These are the elements of order 2 in  $G$ .