MATH 109 SAMPLE MIDTERM

Friday, January 21, 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 6 questions. You have 80 minutes to do all the problems.

Question	Score	Maximum
1		10
2		10
3		10
4		10
5		10
6		10
Total		60

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) $G =$ set of all integers $\mathbb{Z}$, with $a * b = a - b$.

   Solution:

   Associativity fails, so not a group. For example

   $$(5-4)-1=0 \qquad \text{but} \qquad 5-(4-1)=2$$

   (b) $G =$ set of all integers $\mathbb{Z}$, with $a * b = a + b + ab$.

   Solution:

   It is not a group. 0 is an identity since

   $$a * 0 = a + 0 + 0 = a = 0 * a,$$

   so if it is a group, this must be the unique identity. So to find inverses for any $a \in G$, we must be able to solve the equation

   $$a + b + ab = 0.$$

   Solving, we find

   $$b = \frac{-a}{1+a}$$

   so we have no inverse for $a = -1$.

   (c) $G =$ set of all rational numbers $\mathbb{Q} \neq -1$, with $a * b = a + b + ab$.

   Solution:

   By the above arguments, we have an identity element and inverses for every element in the set. Associativity holds because multiplication of real numbers and addition of real numbers are both associative. Clearly any two rationals give a rational under this operation. We must check that no two rationals $a * b = -1$. That is, we must check

   $$a + b + ab = -1$$

   has no solution in the rationals $a, b \neq -1$. This is true! Suppose $a + b + ab = -1$ for some a, b. Then solving for b gives $b = (-1-a)/(1+a) = -1$.

   (d) $G =$ set of all integers modulo 47, $\mathbb{Z}/47\mathbb{Z}$, with $a * b = ab \pmod{47}$.

   Solution:

   It is not a group, since 0 has no multiplicative inverse. However, the set without 0 is a group (check this) since 47 is prime.

2. Prove that every cyclic group G is abelian.

Solution:

We must show that for every $x, y \in G$,

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

But every element in the group G is of the form g^a for some integer a and a generator g. So for any x and y in G, we may write $x = g^a$ for some $a \in \mathbb{Z}$ and $y = g^b$ for some $b \in \mathbb{Z}$. Then

$$x * y = g^a * g^b = \overbrace{g * \cdots * g}^{a} * \overbrace{g * \cdots * g}^{b} = g^{a+b} = g^{b+a} = g^b * g^a = y * x,$$

so G is abelian.

3. (a) Express the following elements of S_8, the symmetric group of order 8!, as a product of transpositions.

   i. $(\,1 \quad 4 \quad 3)$

   Solution:
   $(1 \quad 3)(1 \quad 4)$

   ii. $(\,2 \quad 8)(6 \quad 5 \quad 4)(4 \quad 5)$

   Solution:
   $(6 \quad 5 \quad 4) = (6 \quad 4)(6 \quad 5)$, so one possible solution is

$$(2\ 8)(6\ 4)(6\ 5)(4\ 5)$$

(b) Express the following elements of S_{11}, the symmetric group of order 11!, as a product of disjoint cycles.

   i. $(7 \quad 4 \quad 3 \quad 8)(6 \quad 5 \quad 3)(2 \quad 1)(1 \quad 4 \quad 2)$

   Solution:
   $(1 \quad 3 \quad 6 \quad 5 \quad 8 \quad 7 \quad 4)\ (2)$

   ii. $(6 \quad 5)(5 \quad 7)(8 \quad 4)(3 \quad 1 \quad 2)(3 \quad 5 \quad 11)$

   Solution:
   $(3 \quad 7 \quad 6 \quad 5 \quad 11 \quad 1 \quad 2)\ (8 \quad 4)\ (9)\ (10)$

4. Suppose that for a group G,

$$(ab)^3 = a^3b^3 \quad \text{and} \quad (ab)^5 = a^5b^5 \quad \text{for any } a, b \in G.$$

Prove that G is abelian.

Solution:

There are many ways to show this by various manipulations using the above identities. Here is one.

$$(ab)^3 = a * b * a * b * a * b = a^3b^3$$

The first equality is the definition of the exponential notation, and the second follows by assumption. Cancelling an a on the left and a b on the right leaves:

$$(ba)^2 = a^2b^2$$

Now

$$(ab)^5 = (ab)^3 * (ab)^2 = a^3b^3 * (ab)^2$$

using the first assumption. But

$$(ab)^5 = a^5b^5$$

using the second assumption. So putting these together

$$a^3b^3abab = a^5b^5.$$

Cancelling a^3 on the left and b on the right leaves

$$b^3aba = a^2b^4,$$

but as we showed above $baba = a^2b^2$, so $b^3aba = b^2(a^2b^2)$. Hence

$$b^2a^2 = a^2b^2 = baba$$

and cancelling a b on the left and an a on the right gives the result. I'm sure there are more elegant proofs. This is just the first one I stumbled upon. Try for example, using the fact that $baba = a^2b^2$ and replacing $babababa$ in $(ab)^5$ with $a^2b^2a^2b^2$. This implies $a^3b^2a^2b^3 = a^5b^5$ and after cancellation the result is a bit shorter from this point.

5. (a) Prove that for any finite group G, given any element $a \in G$, there is a positive integer n depending on a such that $a^n = e$.

Solution:

G is a finite group, so given any a in G, the set $\{a, a^2, a^3, \ldots\}$ consisting of all powers of a must be finite (as all these powers must be in G according to closure). But this means that the sequence must eventually repeat itself. That is, there is an i and $j \in \mathbb{Z}$ with say $i < j$ so that

$$a^i = a^j.$$

Multiplying by a^{-i} on both sides gives $e = a^{j-i}$ so $(j - i)$ is the required integer n.

(b) Use the result above to show that for a finite group G, there is a positive integer m such that $a^m = e$ for all $a \in G$.

Solution:

We list the elements of the finite group G as $a_1, a_2, \ldots, a_k$ for some positive integer k. Then by the above argument, to each element a_i $(1 \leq i \leq k)$, there is an integer n_i so that $a_i^{n_i} = e$. Let $m = n_1 n_2 \cdots n_k$, the product of all such exponents. It is finite, since k is finite. And for each element $a_i \in G$,

$$a_i^m = (a_i^{n_i})^{n_1 \cdots n_{i-1} n_{i+1} \cdots n_k} = e^{n_1 \cdots n_{i-1} n_{i+1} \cdots n_k} = e,$$

since $a_i^{n_i} = e$. This proves the claim.

6. Find a shuffle of a deck of 52 cards that requires 42 repeats to return the cards to their original order.

Solution:

A shuffle of a deck of cards is nothing more than a permutation of the original list of cards. We seek, then, a permutation of order 42. Recalling that the order of a permutation, written as a product of DISJOINT cycles, is just the least common multiple of the cycle lengths, then writing down a cycle of lengths 2, 3, and 7 will do the trick. So here's one solution:

$$(1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10\ 11\ 12)$$

The other 41 cards are fixed. A less inspired choice is the cycle

$$(1\ 2\ 3\ \cdots\ 42).$$

This corresponds to cutting the deck 11 cards from the bottom and placing the next card on the top of the original deck.