Math 103A Fall 2007 Exam 2

November 19, 2007

NAME: Solutions

Problem 1 /25	
Problem 2 /25	
Problem 3 /20	
Problem 4 /30	
Total /100	

Problem 1 (25 points)

(a) (**5 pts**). Clearly state Lagrange's theorem.

Theorem 0.1 *Let G be a finite group, and let H be a subgroup of G. Then the order of H divides the order of G.*

(b) (20 pts) Let p be a prime number. Let G be a group with $|G| = p^n$ for some $n \geq 1$ (such a group is called a *p-group*.) Prove that G has at least one element of order p. (Hint: if you don't know how to start, consider first the special case where $|G| = 9$.)

Since G has more than one element, we can pick some element $a \in G$ which is not the identity. Then a has order bigger than 1, and by Lagrange's theorem, in fact order(a) is a divisor of p^n which means it is some power p^i where $0 < i \leq n$.

But if a has order p^i, then $a^{p^{i-1}}$ has order p. So we have found an element of order p.

(The argument here is exactly the same as in Exercise 7.26: "Let $|G| = 8$. Show that G must have an element of order 2." But I think even some people that had gotten that exercise were confused by the extra generality in this problem.)

3

Problem 2 (25 points)

(a) (10 pts) Let G and $\overline{G}$ be two groups. Define what it means for a function $\phi : G \to \overline{G}$ to be an isomorphism of groups.

The function ϕ is an isomorphism if it satisfies the following 2 conditions: (1) ϕ is one-to-one and onto; and (2) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

(b) (15 pts) Define the following set of matrices:

$$G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \middle| a \in \mathbb{Z} \right\}.$$

The set G is a group under matrix *multiplication* (you can assume this.)

Prove that $G \cong \mathbb{Z}$, in other words that G is isomorphic to the group of integers with the operation of *addition*. Hint: you need to find a function ϕ which gives the isomorphism—try something simple.

We define the function $\phi : \mathbb{Z} \to G$ by the formula

$$a \mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

It is easy to see that this function is one-to-one and onto and so this doesn't really require additional argument.

To check the other condition in the definition of an isomorphism, we calculate

$$\phi(a + b) = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \phi(a)\phi(b)$$

(Remember that the operation in $\mathbb{Z}$ is $+$ while the operation in G is matrix multiplication).

Problem 3 (20 points)

In this problem, we consider the group S_7 of permutations of $\{1, 2, 3, \ldots, 7\}$.

(a) (10 pts). Write the permutation $\alpha = (156)(3547)$ in *disjoint* cycle form. What is the order of this permutation in the group S_7?

$\alpha = (156)(3547) = (154736)$ by direct calculation. Since this is a 6-cycle, it has order 6.

(b) (10 pts). Explain why the permutation α in part (a) is an odd permutation. Then find a permutation $\beta \in S_7$ which is an *even* permutation but which has the same order in S_7 as the element α. Again briefly explain your answer.

An m-cycle is an even permutation if m is an odd number, and is an odd permutation if m is an even number. So α is odd. We can also see α is odd directly by expressing α as a product of 5 transpositions:

$$\alpha = (154736) = (15)(54)(47)(73)(36).$$

We need an element of S_7 which, when written in disjoint cycle form, has order 6, but is instead an even permutation. These are conditions only on the cycle shape of the permutation when written in disjoint cycle form, and essentially one cycle shape works: 2 2-cycles and a 3-cycle.

So one answer is $\beta = (123)(45)(67)$. It is even since $\beta = (12)(23)(45)(67)$ and has order $\mathrm{lcm}(3, 2, 2) = 6$.

Problem 4 (30 points)

In this problem, consider the following four groups: A_4, $\mathbb{Z}_{12}$, $U(21)$, D_6. These groups all have order 12 (you don't have to prove this.) (Note that D_6 is the group of all symmetries of a regular hexagon so it contains six rotations and six reflections.)

(a) (10 pts) For each of the four groups, decide if it is Abelian or non-Abelian and list your answers below. *Prove* your answer only for the alternating group A_4.

Z_n and $U(21)$ are Abelian and D_6 is non-Abelian. Though you weren't asked to prove these facts, it follows directly from the definition of the groups Z_n and $U(21)$, and we have studied the groups D_n enough by now to know that composition of symmetries depends on the order of composition.

For A_4, one suspects from experience working with permutations that the group is non-Abelian. But one has to play a bit to find an example that proves this for sure. One example that works is $(123)(234) = (12)(34) \neq (13)(24) = (234)(123)$. Note that (123) and (234) are in A_4 since they are even permutations. Thus A_4 is non-Abelian. (Many students forgot to pick elements that were actually in the group A_4 and so instead only ended up proving that S_4 is non-Abelian, which is weaker.)

(b) (20 pts) Prove that no two of the four groups A_4, $\mathbb{Z}_{12}$, $U(21)$, D_6 are isomorphic. You can assume without proof all of the basic properties of isomorphisms. (Starting hint: look for some elements of order 2 in $U(21)$.)

Using part (a), since a non-Abelian group can never be isomorphic to an Abelian group, we see right away that we only have left to prove that $A_4 \not\cong D_6$ and $\mathbb{Z}_{12} \not\cong U(21)$.

There are multiple ways of doing this, but the easiest involve showing the groups cannot have the same number of elements of some order.

To tell the Abelian groups apart, the hint suggests to look for elements of order 2. The theory of cyclic groups tells us that $\mathbb{Z}_{12}$ has precisely one element of order 2, namely $[6]$. For $U(21)$, trying some elements we find $[8]^2 = [1]$ and so $[8]$ is an element of order 2. But $[-1] = [n-1]$ is an element of order 2 in any $U(n)$ (since $[-1]^2 = [1]$: you once had an exercise about this). So $[20]$ is also an element of order 2 in U_{21}. Since U_{21} has at least two elements of order 2 and Z_{12} has only 1, $\mathbb{Z}_{12} \not\cong U(21)$. (As it turns out, $U(21)$ has precisely 3 elements of order 2, $\{[8], [13], [20]\}$, though it was enough to find two of them.)

To tell the non-Abelian groups apart, looking at elements of order 2 also works. Instead I will look at elements of order 6, which I think is a bit simpler. D_6 has an element of order 6, the rotation R_{60} by 60 degrees, since performing this rotation 6 times is the same as the identity symmetry.

On the other hand, A_4 has no elements of order 6. This is because every element of A_4 has the same disjoint cycle shape as one of the following permutations: ϵ, $(12)(34)$, (123). Thus every element of A_4 has order 1, 2, or 3. So $A_4 \not\cong D_6$.

(more space for problem 4)

(blank page)