

Math 3560

Fall 2011

Solutions to the Final Exam

December 15, 2011

Problem 1: Answer *True* or *False*. (4 points each)

- a. The product of three cyclic groups cannot be cyclic. **F**
- b. If H and K are subgroups of G , and if H is normal in G , then $HK = KH$. **T**
- c. If G is any group and x and y are any elements of G that commute, then x is conjugate to y . **F**
- d. No two elements of $\mathbb{Z} \times \mathbb{Z}$ are conjugate to one another. **T**
- e. If the finite group G acts transitively on a set X , then $|G| \geq |X|$. **T**
- f. If two regular polygons (centered at the origin) have isomorphic rotational symmetry groups, then the polygons are isometric. **F**
- g. If $A \in O_3$, then $A^2 \in SO_3$. **T**
- h. Conjugate elements of a group have the same order. **T**

Problem 2: (10 points) Suppose that G is a group of order 49 acting on the set $X = \{1, 2, 3, 4, 5, 6, 7\}$. Consider the following assertion: *The action is not trivial and not transitive*. If you believe that this assertion can be true, give an example. If you believe that this assertion must be false, give a proof.

The assertion must be false, and here's why. If the action is not transitive, then no orbit can equal all of X . So, every orbit has size < 7 . If the action is non-trivial, some orbit must have size > 1 . But, by the Orbit-Stabilizer Theorem, the size of every orbit divides the order of G , which is $49 = 7^2$. Therefore, the size of a non-trivial orbit must be 7, which we have ruled out.

Problem 3: State definitions of each of the following (underlined> terms. (5 points each)

- a. the commutator subgroup $[G, G]$ of a group G .

$[G, G]$ is the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$, for a, b ranging over G .

- b. the conjugacy class of an element g in a group G .

The conjugacy class of g in G consists of all elements of the form hgh^{-1} , where h ranges over G .

- c. the centralizer $C(g)$ of an element g in a group G .

$C(g)$ consists of all elements of G that commute with g ; equivalently, it consists of all elements h in G such that $hgh^{-1} = g$.

- d. the axis of symmetry of a rotation $A \in SO_3$.

The axis of symmetry is a line through the origin determined by an eigenvector of A having eigenvalue 1.

Problem 4: State each of the following theorems: (5 points each)

- a. The Orbit-Stabilizer Theorem.

Let G be a group acting on a set X , and choose any $x \in X$. Denoting the orbit of x by $G(x)$ and the stabilizer of x by G_x , as usual, the rule $gG_x \mapsto g(x)$ establishes a bijection between G/G_x and $G(x)$.

- b. The First Isomorphism Theorem.

Let $f : G \rightarrow H$ be a homomorphism of groups. Then $\text{kernel}(f)$ is a normal subgroup of G , and the rule $g\text{kernel}(f) \mapsto f(g)$ establishes an isomorphism between the group $G/\text{kernel}(f)$ and $\text{image}(f)$.

- c. A theorem that describes the structure of groups of order p^2 for an arbitrary prime number p .

A group of order p^2 , for any prime p , is either cyclic or isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Problem 5: (30 points) Let Δ denote an equilateral triangular glass pendant with jewels placed at the vertices and center. The jewels are sapphires and rubies, all perfectly round and of the same size. The pendant is not currently attached to a necklace, so it may be rotated or turned over. The jewels are equally visible from both sides of the pendant. How many distinct pendants of this kind can there be, if we count two as the same when, by rotation and flipping, they can be made to look identical? Use the Counting Theorem of Chapter 18 of the text.

Note that of course the point of this problem is to test your understanding of the Counting Theorem. You may obtain an answer by direct enumeration or by some short-cut counting method that works in this simple case. This might be useful for you for verifying the answer you get via the Counting Theorem. But we will not credit answers that are obtained without using the Counting Theorem.

Solution: We'll first give a quick counting argument to find the answer. The center of the pendant is fixed under all symmetries, so it can be either a ruby or a sapphire. Whatever configuration of jewels on the vertices, it is easy to see that it is completely determined by the number of rubies: any two configurations with the same number of rubies can be transformed to one another by a symmetry. Since the possible number of rubies on the vertices is 4 (i.e., 0, 1, 2, 3) and the number of kinds of jewels at the center is 2, the total number of pendants, up to symmetry, is 8.

Now, we use the Orbit Counting Theorem. Our answer here will be substantially longer than what is expected for an answer on the exam, since I give fairly detailed explanations of the method as I go along.

The symmetry group of the pendant is clearly S_3 (the full symmetry group of the equilateral triangle; each symmetry sends each jewel to another jewel). Call it G . of course $|G| = 6$. Let S be the set of jewel sites on the pendant (four of them), and let X be the set of all bejeweled pendants: $|X| = 2^4 = 16$, since there are four sites, each able to receive one of two jewels. The Orbit Counting Theorem tells us that the number of orbits in X under the action of G is $1/6$ the sum of all $|X^g|$, g ranging over G . So, we need to compute this sum.

We know that $|X^g| = |X^h|$ whenever g and h are conjugate. Therefore, we need only compute one $|X^g|$ for each single representative of a conjugacy class and then multiply that by the number of elements in the conjugacy class.

Now G has exactly 3 conjugacy classes: $\{\varepsilon\}$, $\{(12), (13), (23)\}$, and $\{(123), (132)\}$. This follows from the theorem that says that two permutations are conjugate (in the full permutation group) if and only if they have the same cycle structure. We choose the following representatives from each conjugacy class: ε , (12) , and (123) , and we compute $|X^\varepsilon|$, $|X^{(12)}|$, and $|X^{(123)}|$.

It is not hard to see (and you have done so on the homework exercises) that a typical element of X^g is obtained by assigning a ruby or a sapphire (i.e., a color) to each orbit of $\langle g \rangle$ in the set S (the set of jewel sites). If there are n such orbits, then $|X^g| = 2^n$.

Of course, we see directly that that $|X^\varepsilon| = |X| = 16$, so we proceed to the remaining sets.

To compute $|X^{(12)}|$, we first compute the number of orbits in S under the action of $\langle (12) \rangle$, as indicated. By the Orbit Stabilizer Theorem applied to this action on S , we see that the number of orbits here is exactly $1/o((12)) = 1/2$ the sum $|S^\varepsilon| + |S^{(12)}| = (4 + |S^{(12)}|)/2$, so it remains to

compute $|S^{(12)}|$. But (12) is represented by reflection in some altitude, so it fixes exactly one vertex and the center. Therefore, $|S^{(12)}| = 2$ and the number of orbits in S under the action of $\langle (12) \rangle$ is $4 + 2/2 = 3$. Hence, $|X^{(12)}| = 2^3 = 8$.

A similar argument now applies to computing $|X^{(123)}|$. We apply the Orbit Counting Theorem to the action of $\langle (123) \rangle$ on S . The number of these orbits is $1/3$ the sum $|S^\varepsilon| + |S^{(123)}| + |S^{(123)^2}|$. The first term is just $|S| = 4$. Since the rotation represented by (123) fixes only the center, the second term is equal to 1. Finally, since $(123)^2 = (132)$, also a rotation fixing only the center, the last term also equals 1. So the sum of these terms is 6. Therefore, the number of orbits of S under the action of $\langle (123) \rangle$ equals $6/3=2$, from which it follows that $|X^{(123)}| = 2^2 = 4$.

Finally, we must multiply each of the terms we computed by the number of elements in the corresponding conjugacy subgroup, and then divide the total by 6: the total number of orbits in X under the action of G is then $(16 + 3 \cdot 8 + 2 \cdot 4)/6 = 8$, which is (fortunately :-)) the same answer we got earlier.

Problem 6:(15 points) Let G be a group. Recall that an *automorphism* of G is defined to be a homomorphism $G \rightarrow G$ that is a bijection. For example, the identity map $G \rightarrow G$ is an automorphism of G . Since the composition of two automorphisms is again an automorphism, and the inverse of an automorphism is again an automorphism, the set $Aut(G)$ of all automorphisms forms a group under composition. *Prove:* If $|G| = n$, then $|Aut(G)|$ divides $n!$.

Proof: The group $Aut(G)$ is a subgroup of the group S_G of all bijections $G \rightarrow G$. This last is isomorphic to S_n , by the argument in the proof of Cayley's Theorem and its corollary. Therefore, $Aut(G)$ is isomorphic to a subgroup H of S_n . But $|S_n| = n!$. Therefore, by Lagrange's Theorem, $|Aut(G)| = |H|$ divides $n!$

Problem 7: (10 points each) For each of the following groups, find an element of maximal order. In each case, explain your reasoning. (You need not give a complete, airtight proof, as this could be pretty time-consuming. But you should give an argument in favor of your answer. You'll get half-credit for the correct answer; the rest will depend on your reasoning.)

a. S_{17} .

I get the answer 210 via the following reasoning. The order of any permutation is the least common multiple (lcm) of the lengths of the cycles appearing in the cyclic decomposition of the permutation (i.e., the cycles appearing when the permutation is written as a product of disjoint cycles). If one of the cycles that appears has length ℓ that involves two primes, we may write $\ell = rs$ where both r and s are > 1 and are coprime. Then, we may break up the cycle into one of length r and a disjoint one of length s , obtaining a permutation with the same order. However, the sum of the lengths of the cycles in this new permutation is $rs - r - s$

shorter than that in the former permutation (strictly shorter when r or s is > 2). So the new permutation has the same lcm as the first but we have eliminated the composite ℓ in favor of r and s . We can continue this process until each cycle length involves only powers of one prime. Further reduction along these lines is possible so that the powers that occur are small. But now, in this case, we have enough information to do a trial and error. We attempt to get prime powers that add up to 17 (or as close as possible). And then we check the lcm of these. For example $2^3 + 3^2 = 17$ and lcm of 2^3 and 3^2 is 72. So, there is at least one permutation of order 72 in S_{17} . However, we can do much better with cycle lengths $(2, 3, 5, 7)$ which add up to 17. The lcm of these is 210. Other reasonable possibilities are $(2, 3, 11)$, $(2^2, 5, 7)$, which have smaller lcm's. Similarly for other combinations.

b. D_{150} .

The dihedral group D_{150} has an element of order 150, by definition. Since the group has order 300 and every element in the group has order dividing 300, the only possibility for an element of order > 150 would be an element of order 300. But D_{150} would then be cyclic, and it is known to be non-commutative. Therefore, 150 is the maximal order.

c. $\mathbb{Z}_{18} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}$.

The lcm of 18, 12, 10 is 180, and we claim that this is the maximal order of an element in $\mathbb{Z}_{18} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}$. To see this, first compute $180(a, b, c)$ for any $a \in \mathbb{Z}_{18}, b \in \mathbb{Z}_{12}, c \in \mathbb{Z}_{10}$: so $180(a, b, c) = (180a, 180b, 180c) = (0, 0, 0)$. This shows that every element $(a, b, c) \in \mathbb{Z}_{18} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}$ has order that divides 180. Now suppose that d is any divisor of 180 that is strictly less than 180 and compute $d(1, 1, 1) = (d, d, d) \in \mathbb{Z}_{18} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}$. If this equals $(0, 0, 0)$, we must have $d = 0$ in each of the cyclic groups $\mathbb{Z}_{18}, \mathbb{Z}_{12}, \mathbb{Z}_{10}$, respectively, implying that 18, 12, and 10 all divide d . But then 180 must divide d , which is impossible. So $(1, 1, 1)$ has order 180, and this is the maximal order.

Problem 8: (7 points each) The following parts of this problem will prove the following: *If a group G has order 12, then G has a subgroup of order 4.* This is a special case of a general theorem known as The First Sylow Theorem, which can be stated as follows: *If a group G has order divisible by p^k , for some prime p , but not by p^{k+1} , then G has a subgroup of order p^k .*

Assume G is a group of order 12, and let S be the set of all subsets A of G such that $|A| = 4$. The number of such subsets is well known to equal “12 choose 4” $= {}_{12}C_4 = 12!/4!8!$, which equals 495. For our purposes, it is important to notice that 495 is coprime to 4. In other words, $|S|$ is coprime to 4. Given any $A \in S$ and any $g \in G$, the set $gA = \{ga | a \in A\}$ again has 4 elements, and so it is a member of S . Therefore, the rule $A \mapsto gA$ defines an action of G on S . We use this

action in (a) and (b) below.

- a. *Prove:* There exists an $A_0 \in S$ such that the orbit $|G(A_0)|$ is coprime to 4. (Hint: Use the fact that $|S|$ is coprime to 4, together with any related theorems.)

Proof: S is a disjoint union of orbits under the action of G . Suppose none of the orbits has order coprime to 4. This means that each contains an even number of elements. It follows that $|S|$ is even, which we have seen is not the case. Therefore, at least one orbit has order coprime to 4.

- b. With A_0 as in (a), let G_{A_0} be the stabilizer of A_0 .

Prove: $|G_{A_0}|$ is divisible by 4.

Proof: By the Orbit-Stabilizer Theorem, $|G_{A_0}||G(A_0)| = |G|$. Since 4 divides $|G|$, it follows that 4 divides the product $|G_{A_0}||G(A_0)|$. Since $|G(A_0)|$ is coprime to 4 (i.e., it is odd), it follows that 4 divides $|G_{A_0}|$.

Therefore, $|G_{A_0}| \geq 4$. We continue to refer to the same A_0 .

Notice that, for any $x \in A_0$ and $g \in G_{A_0}$, we have $gx \in A_0$, by definition of the concept of stabilizer. This means that G_{A_0} acts on A_0 by left multiplication. We use this action in (c) below.

- c. *Prove:* For any $x_0 \in A_0$, the rule $g \mapsto gx_0$ determines a bijection between G_{A_0} and the orbit $G_{A_0}(x_0)$.

Proof: Note that A_0 is, by definition, a subset of the group G . So, $x_0 \in G$. We know that right multiplication by x_0 is a bijection $G \rightarrow G$; in particular, it is injective. Therefore, right-multiplication by x_0 defines an injection $G_{A_0} \rightarrow G$. By definition the image of this map is the orbit $G_{A_0}(x_0)$. So the map defines an bijection $G_{A_0} \rightarrow G_{A_0}(x_0)$, as desired.

- d. *Conclude:* $|G_{A_0}| \leq 4$.

Conclusion: The orbit $G_{A_0}(x_0)$ is a subset of A_0 , as commented above, so $|G_{A_0}(x_0)| \leq |A_0| = 4$. Then (c) implies that $|G_{A_0}| \leq 4$.

When (b) and (d) are combined, we get $|G_{A_0}| = 4$, so G_{A_0} is the sought-after subgroup of G that has order 4.

Math 3560

Fall 2011

Addendum to Solutions to the Final Exam

December 15, 2011

In the solutions that I presented, I gave a solution to Problem 5 patterned after the general model for solving coloring problems. This was more complicated than warranted by Problem 5. In checking over the solutions submitted for the exam, I saw that most of you used a simpler approach which was correct, so I'll present that here (without repeating the problem).

Solution to Problem 5: The group of symmetries for Δ is either the symmetric group S_3 (which I used in the other solution) or the dihedral group D_3 — of course these two groups are isomorphic. We may take as elements of D_3 , the symmetries, $\varepsilon, r, r^2, s, sr, sr^2$, where ε denotes the identity and r denotes, say, counterclockwise rotation through $2\pi/3$ radians (it being assumed that the pendant is positioned in \mathbb{R}^2 with center at the origin and base parallel to the X -axis). Accordingly, r^2 is the rotation by $4\pi/3$ radians, s is the reflection through one of the altitudes (say the one parallel to the Y -axis), and accordingly sr and sr^2 are the two further reflections through altitudes. The conjugacy classes of D_3 are known to be $\{\varepsilon\}$, $\{r, r^2\}$, and $\{s, sr, sr^2\}$.

Let $G = D_3$, and let X be the set of all bejeweled pendants. $|G| = 6$ and $|X| = 2^4 = 16$. G acts on X , and the Orbit Counting Theorem tells us that the number of distinct orbit is $1/6$ the sum of the quantities $|X^g|$ as g ranges over G . Since $|X^g| = |X^h|$ whenever h and g are conjugate, we need only compute these numbers once for each representative of a conjugacy class and then multiply by the number of elements in that conjugacy class.

Of course $|X^\varepsilon| = |X| = 16$. Since the rotation r fixes only the center and maps the vertices counterclockwise to the next vertices, and since there are 2 possible jewels, $|X^r| = 2^2 = 4$. Since s fixes only the vertical altitude, it fixes one vertex and the center and exchanges the other two vertices. Therefore, the center and one vertex can each receive one of the two jewels, and the two base vertices can both receive one of two jewels (the same for each) , making a possible number of $2^3 = 8$ jeweled pendants counted by $|X^s|$.

Therefore the total number is $(16 + 2 \cdot 4 + 3 \cdot 8)/6 = 48/6 = 8$ possible pendants, up to symmetry.

Most students did very well on this problem.