Math 3110 **Test #2** **October 26th, 2011**

Name: ANSWER KEY **Be sure to show your work!**

1. (20 points) Cyclic

(a) Let $G = \langle g \rangle$ where g has order 20.

Don't forger g has order 20, so its exponents can be reduced modulo 20.

$\langle g^8 \rangle = \{g^8, g^{16}, g^{24}, \dots\} = \{g^8, g^{16}, g^4, g^{12}, e\} = \langle g^4 \rangle$

Is $g^{102} \in \langle g^8 \rangle$? Why or why not?

No. 102 mod 20 is 2. But $g^{102} = g^2 \notin \langle g^8 \rangle$. OR $g^{102} \notin \langle g^8 \rangle$ because $\gcd(8, 20) = 4$ does not divide 102.

(b) Suppose G is a cyclic group with at least one element of order 6.

What can you say about the order of G?

Since G has an element of order 6, it's order must be a multiple of 6. G could be a group of order 6, 12, 18, etc.

How many elements of order 6 can G have? Is there more than one possibility?

If $g \in G$ is an element of order 6, then $\langle g \rangle$ is a subgroup of order 6. However, G is cyclic. Therefore, it has a **unique** subgroup of order 6. This subgroup in turn has unique subgroups of orders 1, 2, 3, and 6. Its subgroup of order 1 just contains the identity. Its subgroup of order 2 has elements of order 1 and 2, but there is only 1 element of order 1. Therefore, there are exactly $2 - 1 = 1$ element of order 2. Next, the subgroup of order 3 has elements of order 1 and 3 (the divisors of 3). There is only 1 element of order 1, thus there are $3 - 1 = 2$ elements of order 3. Finally, the subgroup of order 6 has elements of order 1, 2, 3, and 6. There is 1 element of order 1, 1 element of order 2, and 2 elements of order 3. Thus there are $6 - 2 - 1 - 1 = 2$ elements of order 6.

Any **cyclic** group whose order is divisible by 6 will have **exactly** 2 elements of order 6 (and 2 of order 3, 1 of order 2, and 1 of order 1).

This essentially follows from the fact that subgroups of cyclic groups are cyclic and there is a unique subgroup corresponding to each divisor of the order of that group.

Note: This is not true of non-cyclic groups. For example. In $U(8) = \{1, 3, 5, 7\}$, all non-identity elements: 3, 5, and 7 have order 2. In S_5 there are many elements of order 6: (12)(345), (12)(354), (13)(245), etc. On the other hand, A_4 has order 12 (which is divisible by 6), but it has ZERO elements of order 6. In fact, it doesn't even have a subgroup of order 6.

(c) List the possible orders of elements in $\mathbb{Z}_{33}$. Then determine the number of elements of each order.

$\mathbb{Z}_{33}$ is cyclic, the divisors of 33 are 1, 3, 11, and 33, so there are elements of orders 1, 3, 11, and 33. There is 1 element of order 1 (the identity is the only element of order 1 in any group). There are $3 - 1 = 2$ elements of order 3. Next, 11 is divisible by 1 and 11 so the (unique) cyclic subgroup of order 11 (which contains all of the elements of order 11) there are $11 - 1 = 10$ elements of order 11. Finally after knocking out the elements of orders 1, 3, and 11 we are left with $33 - 10 - 2 - 1 = 20$ elements of order 33.

We also need to count the number of elements of various orders for D_n. D_n's subgroup of rotations is a cyclic subgroup of order n, thus isomorphic to $\mathbb{Z}_n$. So the orders of various rotations can be counted just like we count orders for $\mathbb{Z}_n$. In addition D_n has n reflections. A reflection is its own inverse, so its order is 2. Thus the only difference in the tables for $\mathbb{Z}_n$ and D_n is that D_n has an additional n elements of order 2.

For $\mathbb{Z}_{33}$:

Order =	1	3	11	33
Number of elements =	1	2	10	20

For D_{33}:

Order =	1	2	3	11	33
Number of elements =	1	33	2	10	20

2. (20 points) The following pairs of groups are **not** isomorphic. Prove this is the case.

(a) $\mathrm{GL}_3(\mathbb{R}) \ncong A_{500}$

$\mathrm{GL}_3(\mathbb{R})$ (2×2 invertible matrices over the reals) is an infinite group. A_{500} is finite (although, it's order is quite large: 500!/2). Isormophic groups must have the same size. Thus these groups are not isomorphic.

(b) $U(8) = \{1, 3, 5, 7\} \ncong \mathbb{Z}_4$

Notice that $3^2 = 9 = 1$, $5^2 = 25 = 1$, and $7^2 = 49 = 1 \pmod 8$. Thus $U(8)$ has 3 elements of order 2 while $\mathbb{Z}_4$ only has 1 element of order 2. Therefore, they cannot be isormophic. Alternatively, $U(8)$ has no elements of order 4. Thus $U(8)$ is not cyclic. However, $\mathbb{Z}_4$ is cyclic. Therefore, they cannot be isomorphic.

(c) $\mathrm{GL}_2(\mathbb{Z}) \ncong \mathbb{Q}$

$\mathrm{GL}_2(\mathbb{Z})$ (2×2 invertible integer matrices) is a non-abelian group (in general, matrix multiplication is not commutative). However, $\mathbb{Q}$ (rational numbers under addition) is an abelian group. Therefore, they cannot be isomorphic.

(d) $S_4 \ncong D_{12}$

Both groups are non-abelian (and thus also not cyclic) and both are groups of order 24. Let's try looking at the orders of various elements.

D_{12} has a cyclic subgroup of order 12 (i.e. it's subgroup of rotations). Thus D_{12} has at least one element of order 12. On the other hand S_4 does not have an element of order 12. It would take either a 12 cycle or a pair of disjoint 3 and 4 cycles to get an element of order 12 in a permutation group. So while S_7 has elements of order 12 (i.e. (123)(4567)), S_4 does not. Therefore, they cannot be isomorphic.

Alternatively, the elements of order 2 in S_4 are $(12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23)$ (there are 9). On the other hand, D_{12} has 12 reflections and the 180° rotation and no other elements of order 2. So D_{12} has 13 (not 9) elements of order 2. Thus these groups cannot be isomorphic.

Or we could look at elements of order 3. The only elements of order 3 in D_6 are rotations (reflections have order 2). Since the rotations form a cyclic group, there are only $3 - 1 = 2$ elements of order 3. On the other hand, S_4 has many elements of order 3 (there are a lot of 3-cycles: $(123), (132), (124), \dots$). Thus these groups cannot be isomorphic.

One last reason they are not isomorphic. The center of S_n is trivial for all $n \geq 3$, so $Z(S_4) = \{(1)\}$. On the other hand, the center of D_n is trivial for odd n, but contains the 180° rotation for even n, so $Z(D_{12}) = \{R_0, R_{180}\}$. Since the centers are not isomorphic (they have different orders), the groups cannot be isomorphic.

3. (20 points) Isomorphisms

(a) Prove that $U(5) \cong \mathbb{Z}_4$.

Consider $2 \in U(5)$. $\langle 2 \rangle = \{1, 2, 4, 8, \dots\} = \{1, 2, 4, 3\} = U(5)$. Thus $U(5)$ is a cyclic group of order 4. However, $\mathbb{Z}_4$ is a cyclic group of order 4. We proved in class that any two cyclic groups of the same order are isomorphic. Therefore, $U(5) \cong \mathbb{Z}_4$.

(b) Let G be an **Abelian** group. Define the map $\varphi : G \to G$ by $\varphi(g) = g^{-1}$. Prove that φ is an isomorphism (actually φ is an automorphism since its domain and codomain are equal).

First, note that $\varphi \circ \varphi(g) = \varphi(\varphi(g)) = \varphi(g^{-1}) = (g^{-1})^{-1} = g$. Thus $\varphi^{-1} = \varphi$ (φ is its own inverse). Therefore, φ is a bijection (i.e. one-to-one and onto).

Next, $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$ where we know $y^{-1}x^{-1} = x^{-1}y^{-1}$ because G is abelian. Thus φ is a homomorphism.

Therefore, φ is an isomorphism (also, an automorphism since its domain and codomain are both G).

Note: Instead of showing φ is its own inverse. We could prove it is one-to-one and onto directly. This would go something like: Suppose $\varphi(x) = \varphi(y)$ so that $x^{-1} = y^{-1}$ and thus $x = y$. Therefore, φ is one-to-one. Next, $\varphi(x^{-1}) = (x^{-1})^{-1} = x$. Therefore, φ is onto.

Is φ an automorphism if G is not Abelian? Why or why not?

No. Since G is not abelian, there are element $a, b \in G$ such that $ab \neq ba$ and so $a^{-1}b^{-1} \neq b^{-1}a^{-1}$. Thus we have $\varphi(ab) = \varphi(b)\varphi(a) \neq \varphi(a)\varphi(b)$ (the homomorphism property fails).

Note: A bijective mapping for which $\varphi(ab) = \varphi(b)\varphi(a)$ (the order is reversed) is often called an **anti-isomorphism**.

4. (20 points) Zombie Apocalypse! Does anyone actually read the directions to these problems?
[Answer: Apparently, "Yes."]

(a) Let $\sigma = (2453)(1346)(126) \in S_6$
Write σ as a product of disjoint cycles

Think of each cycle as a map. For example:
$$((2453) \circ (1346) \circ (126))[1] = (2453)((1346)((126)[1])) = (2453)((1346)[2]) = (2453)[2] = 4$$
So $\sigma = (1462)(35)$

Find σ^{-1} Simply write the permutation backwards. Then rewrite it with "good manners".
$\sigma^{-1} = (53)(2641) = (35)(1264) = (1264)(35)$.
Note that $(53) = (35)$ (bumping 3 to the front) and $(2641) = (1264)$ (bumping 1 to the front). We can switch the order of the 4-cycle (1264) and the transposition (35) because disjoint cycles commute.

What is the order of σ? $\underline{\text{lcm}(4, 2) = 4}$
[If a permutation is written as a product of disjoint cycles, its order is the least common multiple of the lengths of the cycles.]

Is σ even or odd? $\underline{\sigma \text{ is even.}}$

To see that σ is even we can note that any even length cycle is odd and any odd length cycle is even. σ is made up of two even length cycles. So σ is odd with odd = even. Alternatively, $\sigma = (1462)(35) = (12)(16)(14)(35)$ (four transpositions = even).

(b) For convenience: $A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$
Consider the subgroup $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4.

Since $|A_4| = 12$ and $|H| = 4$ we must have $[A_4 : H] = |A_4|/|H| = 12/4 = 3$ cosets.

- $H = \{(1), (12)(34), (13)(24), (14)(23)\}$
- $(123)H = \{(123)(1), (123)(12)(34), (123)(13)(24), (123)(14)(23)\} = \{(123), (134), (243), (142)\}$
- $(132)H = \{\text{left} - \text{overs}\} = \{(132), (143), (234), (124)\}$

Notice that a careful student only needed to perform **3** (non-trivial) permutation multiplications to get the correct answer!

(c) Let $\sigma = (14)(23) \in S_4$. What is the order of σ? $\underline{\text{lcm}(2, 2) = 2}$

Compute $\sigma^{999} = \sigma = (14)(23)$ (since $999 \equiv 1 \pmod 2$ and the fact that exponents operate "mod" the order of the element).

(d) Find an element of order 15 in S_8.

We need lcm(???) = 15 and ??? adds up to 8 or less. 3 and 5 do the trick. So $(123)(45678) \in S_8$ has order $\text{lcm}(3, 5) = 15$.

5. (20 points)

(a) Let G be a group, H be a subgroup of G, and $a, b \in G$. Prove $aH = bH$ implies that $a^{-1}b \in H$. [You may **not** use any theorems about cosets.]

I'll give two similar proofs. The second is a little cleaner but involves a bit more forethought.

Proof 1: Since $aH = bH$ they share all elements, pick one: $x \in aH = bH$. Now since $x \in aH$, there exists some $h \in H$ such that $x = ah$. Likewise since $x \in bH$, there exists some $h' \in H$ such that $x = bh'$. Thus we have $ah = x = bh'$. Multiply on the left by a^{-1} and on the right by $(h')^{-1}$ and get: $a^{-1}ah(h')^{-1} = a^{-1}bh'(h')^{-1}$ so that $h(h')^{-1} = a^{-1}b$. Now $h, h' \in H$ thus $h(h')^{-1} \in H$. Therefore, we have that $a^{-1}b \in H$.

Proof 2: Let $e \in G$ be the identity. Then $e \in H$ (the identity belongs to every subgroup) so $b = be \in bH$. Thus $b \in aH$ (since $aH = bH$). Therefore, there is some $h \in H$ such that $b = ah$. Thus $a^{-1}b = h \in H$.

(b) My friend is computing some cosets of K which is a subgroup of S_4. He claims has found a left coset $L = \{(243), (142), (123), (134)\}$.

Assuming my friend didn't make a mistake, what is the order of K? $\underline{|L| = 4}$ since all cosets have the same size and the subgroup itself is a coset.

How many cosets will K have in S_4? $\underline{[S_4 : K] = |S_4|/|K| = 24/4 = 6}$ by Lagrange's theorem.

My friend then starts computing right cosets and finds a coset $R = \{(1234), (24), (1432), (13), (1324)\}$.

I know he must have made a mistake. Why?

$|R| = 5$ but all cosets (left and right) must have the same size. Assuming the original coset is ok, this one has one too many elements.

Note R is still definitely wrong even if we don't know about the other coset's size. Why? The size of a coset must divide is order of the group (since coset size = subgroup size = divisor of the group's order). But $5 = |R|$ does not divide $|S_4| = 4! = 24$.

(c) H and K are subgroups of G such that $H \subsetneq K \subsetneq G$ (they are proper subsets of each other).

G has order 50. K has order 5. What are the possible orders for H?

Note: This problem as stated contains a typo. First, I will work it as it is written.

We have that H and K are subgroups of G. So their orders must divide $|G| = 50$. Thus $|H|, |K|$ could be $1, 2, 5, 10, 25$, or 50.

Next, $|K| = 5$. So $|H|$ must divide 5. Thus $|H| = 1$ or 5. But we are also told that $H \neq K$ and $K \neq G$. Thus $|H| \neq |K| = 5$. Therefore, $|H| = 1$. [So H must be the trivial subgroup: $H = \{e\}$.]

The Intended Problem: Suppose $H \subsetneq K \subsetneq G$, G has order 50. H has order 5. What are the possible orders for K? (I mixed up H and K when typing the original test.)

In this case, we must have $|K| = 1, 2, 5, 10, 25$, or 50 since it's a subgroup of G. Then $|K| \neq 50$ because $K \neq G$. Next, H is a subgroup of K so $5 = |H|$ must divide $|K|$. This rules out 1 and 2. Finally, $H \neq K$ so $|K| \neq |H| = 5$. Therefore, $|K|$ is either 10 or 25.