Math 3110 **Test #2** **October 9th, 2015**

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

1. (20 points) Random Group Stuff — Fill out the following table:

$G =$	What is the identity of G?	Is G abelian?	Is G cyclic?	What is the order of ...?	Does G have an element of order 5?
$\mathbb{Z}_{99}$	0	Yes	Yes	$\lvert 15\rvert = \dfrac{99}{\gcd(99,15)} = \dfrac{99}{3} = 33$	No. $5 \nmid 99$
$U(10)$	1	Yes	Yes	$\lvert 3\rvert = 4$	No. $5 \nmid 4 = \lvert U(10)\rvert$
D_{20}	$1 = R_{0^\circ}$	No	No	$\lvert x^6\rvert = \dfrac{20}{\gcd(20,6)} = \dfrac{20}{2} = 10$	Yes. $\lvert x^4\rvert = 5$
S_9	(1)	No	No	$\lvert(123)(4567)(89)\rvert = \operatorname{lcm}(3,4,2) = 12$	Yes. $\lvert(12345)\rvert = 5$

Recall: $D_{20} = \{1, x, \ldots, x^{19}, y, xy, \ldots, x^{19}y\}$ where $x^{20} = 1$, $y^2 = 1$, and $xyxy = 1$.

Scratch Work:

$\mathbb{Z}_{99} = \langle 1\rangle$ so it is cyclic and thus also abelian. Notice that in $U(10)$: $3^1 = 3$, $3^2 = 9$, $3^3 = 27 = 7$, and $3^4 = 81 = 1$. Thus $\lvert 3\rvert = 4$ and $\langle 3\rangle = \{1, 3, 7, 9\} = U(10)$ so $U(10)$ is cyclic and thus also abelian. On the other hand D_{20} and S_9 are not abelian. Thus they cannot be cyclic either.

2. (24 points) Cyclic Stuff

(a) Let G be a finite group and $g \in G$. Suppose that $\lvert g\rvert = 66$.

i. What is the order of g^{55}? List the distinct elements in $\langle g^{55}\rangle$.

$\langle g^{55}\rangle = \{e, g^{55}, g^{110}, g^{165}, \ldots\} = \{e, g^{55}, g^{44}, g^{33}, g^{22}, g^{11}\}$

Alternatively, notice that $\langle g^{55}\rangle = \langle g^{\gcd(66,55)}\rangle = \langle g^{11}\rangle = \{e, g^{11}, \ldots, g^{55}\}$.

ii. Is $g^{22} \in \langle g^{22}\rangle$? **Yes** / **No**

And, yes, this was a very very silly typo on the test.

(b) How many elements of order 6 does $\mathbb{Z}_{120}$ have? What are they?

6 does divide 120 so there are elements of order 6. Recall that we can find the number of elements of various order in *any* cyclic group using our big theorem about the existence and uniqueness of subgroups of every divisor order. As discussed in class, there is 1 element of order 1, $2 - 1 = 1$ element of order 2, $3 - 1 = 2$ elements of order 3, and $6 - 2 - 1 - 1 =$ 2 elements of order 6.

(c) List the orders of elements in $\mathbb{Z}_{55}$. Then determine the number of elements of each order.

Use the same procedure as in part (b). The divisors of 55 are 1, 5, 11, and 55.

Order =	1	5	11	55
Number of elements =	1	$5 - 1 = 4$	$11 - 1 = 10$	$55 - 10 - 4 - 1 = 40$

(d) List the orders of elements in D_{55}. Then determine the number of elements of each order.

Part (c) accounts for the rotations, we just need to add in the reflections (all of which have order 2).

Order =	1	2	5	11	55
Number of elements =	1	55	4	10	40

3. (22 points) Permutations

(a) Let $G = \langle i \rangle = \{1, i, -1, -i\}$ where $i = \sqrt{-1}$. [G is a subgroup of $\mathbb{C}_{\neq 0}$ (nonzero complex numbers).]

Label 1 as 1, i as 2, -1 as 3, and $-i$ as 4. Cayley's theorem says that G is isomorphic to a subgroup of S_4. Find this subgroup [using left multiplication maps and the labels provided].

Carefully listing G in the order prescribed, we have the following Cayley table...

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Notice that the left multiplication maps give...

$$L_1 : 1 \mapsto 1 \cdot 1 = 1, i \mapsto 1 \cdot i = i, -1 \mapsto 1 \cdot (-1) = -1, -i \mapsto 1 \cdot (-i) = -i \quad \Longleftrightarrow \quad (1)(2)(3)(4)$$

$$L_i : 1 \mapsto i \cdot 1 = i, i \mapsto i \cdot i = -1, -1 \mapsto i \cdot (-1) = -i, -i \mapsto i \cdot (-i) = 1 \quad \Longleftrightarrow \quad (1234)$$

$$L_{-1} : 1 \mapsto -1 \cdot 1 = -1, i \mapsto -1 \cdot i = -i, -1 \mapsto -1 \cdot (-1) = 1, -i \mapsto -1 \cdot (-i) = i \quad \Longleftrightarrow \quad (13)(24)$$

$$L_{-i} : 1 \mapsto -i \cdot 1 = -i, i \mapsto -i \cdot i = 1, -1 \mapsto -i \cdot (-1) = i, -i \mapsto -i \cdot (-i) = -1 \quad \Longleftrightarrow \quad (1432)$$

In more detail, for example, L_{-1} maps 1 to -1 and -1 to 1 (that is element 1 maps to element 3 and then element 3 maps to 1). Likewise, L_{-1} sends element 2 to element 4 and then 4 back to 2 (i.e. i and $-i$ are interchanged). This gives us the permutation (13)(24).

$G \cong \boxed{\Big\{(1), (1234), (13)(24), (1432)\Big\}} = \langle (1234) \rangle$

(b) Write $\sigma = (237)(1724)(27563)$ as a product of disjoint cycles. $\boxed{\sigma = (1234)(567)}$

$\sigma^{-1} = (765)(4321) = \boxed{(1432)(576)}$

The order of σ is $|\sigma| =$ $\underline{\quad \text{lcm}(4,3) = 12 \quad}$.

Write σ as a product of transpositions. σ is **Even** / $\boxed{\textbf{Odd}}$

$\sigma = (27)(23)(14)(12)(17)(23)(26)(25)(27)$ OR $\boxed{(14)(13)(12)(57)(56)}$

Compute σ^{30}.

$\sigma^{30} = ((1234)(567))^{30} = (1234)^{30}(567)^{30} = (1234)^2(567)^0 = \boxed{(13)(24)}$ where the second equality holds because disjoint cycles commute and the next equality holds since the order of a 4-cycle is 4 and a 3-cycle is 3 (so exponents can be reduced mod 4 and 3 respectively).

4. (18 points) Explain why the following pairs of groups are not isomorphic.

(a) $\mathbb{Q} \ncong \mathbb{Z}_{123}$ [$\mathbb{Q}$ is the rational numbers.]

Both groups are abelian, but $\mathbb{Q}$ is infinite (countably infinite) whereas $\mathbb{Z}_{123}$ is finite (of order 123). Therefore, they cannot be isomorphic.

Of course, there are other reasons as well. The order of any non-identity element of $\mathbb{Q}$ is infinite (if $nx = 0$ for $n \in \mathbb{Z}_{>0}$ and $x \in \mathbb{Q}$, then $x = 0$) whereas the orders of elements in $\mathbb{Z}_{123}$ are divisors of 123. Or $\mathbb{Z}_{123}$ is cyclic and $\mathbb{Q}$ isn't cyclic (if $\mathbb{Q} = \langle x \rangle$ for some $x \in \mathbb{Q}$, then it can be shown that $x/2 \notin \mathbb{Q}$ – contradiction).

(b) $Q \ncong \text{Aut}(\mathbb{Z}_8)$ [$Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the group of quaternions.]

Recall that $\text{Aut}(\mathbb{Z}_n) \cong U(n)$ (the unit group of $\mathbb{Z}_n$). These groups cannot be isomorphic since Q is not abelian whereas $\text{Aut}(\mathbb{Z}_8) \cong U(8)$ is abelian. OR $|Q| = 8 \neq |\text{Aut}(\mathbb{Z}_8)| = |U(8)| = |\{1, 3, 5, 7\}| = 4$ (they are groups of different orders). Of course, yet again, there are other reasons as well.

(c) $A_4 \ncong D_6$

First, note that $|A_4| = \dfrac{4!}{2} = 12 = 2 \cdot 6 = |D_6|$, so these are both non-abelian groups of order 12 (no help here).

Now $A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$ has elements of orders 1, 2, and 3. On the other hand, D_6 has elements of orders 1, 2, 3, and **6**. So since A_4 has no elements of order 6, these groups cannot be isomorphic.

Another way to see that A_4 and D_6 aren't isomorphic is to count the number of elements of order 2. A_4 has 3 elements of order 2: $(12)(34), (13)(24)$, and $(14)(23)$. On the other hand, D_6 has 7 elements of order 2: the 180° rotation and 6 reflections.

5. (16 points) A few proofs

(a) Explain why $A_3 \cong \mathbb{Z}_3$ but $A_n \ncong \mathbb{Z}_n$ for $n > 3$.

$A_3 = \{(1), (123), (132)\} = \langle(123)\rangle$ is a cyclic group of order 3. Since any two cyclic groups of the same order are isomorphic, $A_3 \cong \mathbb{Z}_3$. On the other hand, A_n is not abelian for $n > 3$. Therefore, A_n (for $n > 3$) isn't cyclic. Thus $A_n \ncong \mathbb{Z}_n$ for $n > 3$.

(b) Pick **ONE** of the following...

I. Let G be an abelian group. Show that $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}$ is an automorphism of G.

First, notice that $\varphi(\varphi(x)) = \varphi(x^{-1}) = (x^{-1})^{-1} = x$. Therefore, $\varphi = \varphi^{-1}$ (φ is its own inverse) and so φ is bijective (one-to-one and onto). [Alternatively, suppose $x, y \in G$ such that $\varphi(x) = \varphi(y)$. Then $x^{-1} = y^{-1}$ so that $x = y$. Thus φ is one-to-one. Also, suppose $x \in G$. Then $\varphi(x^{-1}) = (x^{-1})^{-1} = x$. Therefore, φ is onto.]

Next, let $x, y \in G$. $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$ (the third equality holds because G is abelian). Therefore, φ is a homomorphism.

We have shown that φ is a bijective homomorphism from G to itself. This means that φ is an automorphism.

Note: The converse is also true: If $\varphi(x) = x^{-1}$ is an automorphism, then G is abelian. Why? Suppose φ is an automorphism and let $x, y \in G$. Then $\varphi(x^{-1}y^{-1}) = \varphi(x^{-1})\varphi(y^{-1})$ (φ is operation preserving) so that $(x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$. Therefore, by socks-shoes, $(y^{-1})^{-1}(x^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}$ and so $yx = xy$ (G is abelian).

II. Let φ, ψ be automorphisms of G. Prove that $H = \{x \in G \mid \varphi(x) = \psi(x)\}$ is a subgroup of G.

First, note that $\varphi(e) = e = \psi(e)$. Therefore, $e \in H$. Thus H is a non-empty subset of G.

Next, let $x, y \in H$. Then by definition: $\varphi(x) = \psi(x)$ and $\varphi(y) = \psi(y)$. This implies that $\varphi(xy) = \varphi(x)\varphi(y) = \psi(x)\psi(y) = \psi(xy)$, so $xy \in H$. This also implies that $\varphi(x)^{-1} = \psi(x)^{-1}$ so that $\varphi(x^{-1}) = \psi(x^{-1})$. Therefore, $x^{-1} \in H$.

Thus by the 2-step subgroup test, H is a subgroup of G.