Math 3110 **Test #2** **March 4th, 2022**

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?	What is the order of ...?	Does G have an element of order 6?	Is G abelian?	Is G cyclic?
$\mathbb{Z}_{55}$	0	$\lvert 33\rvert = \dfrac{55}{\gcd(33,55)} = \dfrac{55}{11} = 5$	No, 6 does not divide 55.	Yes.	Yes, $\mathbb{Z}_{55} = \langle 1\rangle$
$U(9)$	1	$\lvert 5\rvert = 6$ since: $5^1 = 5$, $5^2 = 7$, $5^3 = 8$, $5^4 = 4$, $5^5 = 2$, $5^6 = 1$	Yes, $\lvert 5\rvert = 6$.	Yes.	Yes, $U(9) = \langle 5\rangle$
D_{10}	1 (or R_{0°)	$\lvert x^4\rvert = \dfrac{10}{\gcd(4,10)} = \dfrac{10}{2} = 5$	No, 6 does not divide 10.	No.	No, not even Abelian.
S_7	(1)	$\lvert(1234)(56)\rvert = \operatorname{lcm}(4,2) = 4$	Yes, the order of (123456) is 6.	No.	No, not even Abelian.

Recall: $D_{10} = \{1, x, \ldots, x^9, y, xy, \ldots, x^9y\}$ where $x^{10} = 1$, $y^2 = 1$, and $xyxy = 1$.

Notes: Recall that $\langle g^k\rangle = \langle g^{\gcd(k,n)}\rangle$ when $\lvert g\rvert = n$ (so in $\mathbb{Z}_n$, $\langle k\rangle = \langle \gcd(k,n)\rangle$). Thus $\langle 33\rangle = \langle \gcd(33,55)\rangle = \langle 11\rangle$ and the order of 11 in $\mathbb{Z}_{55}$ is $55/11 = 5$. Likewise, in D_{10}, $\langle x^4\rangle = \langle x^{\gcd(4,10)}\rangle = \langle x^2\rangle = \{1, x^2, x^4, x^6, x^8\}$ has order 5.

Next, the orders of the elements in $\mathbb{Z}_n$ are precisely the (positive) divisors of n, so $\mathbb{Z}_{55}$ only has elements of orders 1, 5, 11, and 55. Also, we know that the rotations in D_n form a subgroup isomorphic to $\mathbb{Z}_n$ (so they have orders k where k divides n) and all reflections have order 2. Consequently, D_n has elements of order 6 if and only if 6 divides n.

Next, $\mathbb{Z}_n$ is always cyclic (and thus Abelian) whereas $U(n)$ is sometimes cyclic but always Abelian (since multiplication mod n is commutative). Notice that $U(9) = \{1,2,4,5,7,8\} = \langle 5\rangle$ (and also $= \langle 2\rangle$). Thus $U(9)$ is cyclic. On the other hand, D_n (for $n \geq 2$) and S_n (for $n \geq 3$) are non-Abelian. Finally, since cyclic implies Abelian, these last groups cannot be cyclic.

2. (20 points) Cyclic Stuff

(a) Let G be a finite group and $g \in G$. Suppose that $\lvert g\rvert = 120 = 2^3 \cdot 3 \cdot 5$.

i. What is the order of g^{100}? List the distinct elements in $\langle g^{100}\rangle$.

We have $\langle g^{100}\rangle = \langle g^{\gcd(100,120)}\rangle = \langle g^{20}\rangle = \{1, g^{20}, g^{40}, g^{60}, g^{80}, g^{100}\}$. Thus $\lvert g^{100}\rvert = \lvert g^{20}\rvert = 120/20 = 6$.

ii. Is $g^{31} \in \langle g^{77}\rangle$? **Yes** / **No**

We have $\langle g^{77}\rangle = \langle g^{\gcd(77,120)}\rangle = \langle g^1\rangle$. Thus every power of g belongs to this cyclic subgroup!

(b) How many elements of order 10 does $\mathbb{Z}_{40}$ have? What are they?

Recall that $40/10 = 4$ has order 10 in $\mathbb{Z}_{40}$ and thus $4k$ has order 10 for each $k \in U(10) = \{1,3,7,9\}$. Therefore, the elements of $\mathbb{Z}_{40}$ of order 10 are 4, 12, 28, and 36.

(c) List the orders of elements in $\mathbb{Z}_{52}$. Then determine the number of elements of each order.

Note: It might be helpful to know that $52 = 2^2 \cdot 13$ and its positive divisors are 1, 2, 4, 13, 26, and 52.

Order =	1	2	4	13	26	52
Number of elements =	1	$2-1$ $= 1$	$4-1-1$ $= 2$	$13-1$ $= 12$	$26-1-1-12$ $= 12$	$52-1-1-2-12-12$ $= 24$

(d) List the orders of elements in D_{52}. Then determine the number of elements of each order.

Order =	1	2	4	13	26	52
Number of elements =	1	$1+52$ $= 53$	2	12	12	24

(same as $\mathbb{Z}_{52}$ except we add in the 52 reflections of order 2)

3. (22 points) Permutations *Note:* Please give simplified ("good manners") answers.

(a) Consider $G = D_3 = \{1, x, x^2, y, xy, x^2y\} = \langle x, y \mid x^3 = 1, y^2 = 1, (xy)^2 = 1\rangle$. Label 1 as 1, x as 2, x^2 as 3, y as 4, xy as 5, and x^2y as 6. Cayley's theorem says that G is isomorphic to a subgroup of S_6. Write down left multiplication by xy does in D_3: $L_{xy} : D_3 \to D_3$ is...

$$
\begin{array}{rcll}
1 & \mapsto & \underline{\quad xy \cdot 1 = xy \quad} & \Longrightarrow \quad 1 \mapsto 5 \\
x & \mapsto & \underline{\quad xy \cdot x = xx^{-1}y = y \quad} & \Longrightarrow \quad 2 \mapsto 4 \\
x^2 & \mapsto & \underline{\quad xy \cdot x^2 = xx^{-2}y = x^{-1}y = x^2y \quad} & \Longrightarrow \quad 3 \mapsto 6 \\
y & \mapsto & \underline{\quad xy \cdot y = x \quad} & \Longrightarrow \quad 4 \mapsto 2 \\
xy & \mapsto & \underline{\quad xy \cdot xy = xx^{-1}yy = 1 \quad} & \Longrightarrow \quad 5 \mapsto 1 \\
x^2y & \mapsto & \underline{\quad xy \cdot x^2y = xx^{-2}yy = x^{-1} = x^2 \quad} & \Longrightarrow \quad 6 \mapsto 3
\end{array}
$$

The corresponding permutation in S_6 is $\underline{\quad (15)(24)(36) \quad}$.

(b) Suppose that using Cayley's theorem we found the left multiplication operator of x in D_4 corresponds with $(1234)(5678)$ and the left multiplication operator of y corresponds with $(15)(28)(37)(46)$. Find the permutation associated with x^2y. [Your answer should be written in terms of disjoint cycles.]

We are given the x corresponds with $(1234)(5678)$ and y corresponds with $(15)(28)(37)(46)$. Therefore, x^2y should correspond with $[(1234)(5678)]^2(15)(28)(37)(46) = (13)(24)(57)(68)(15)(28)(37)(46) = \boxed{(17)(26)(35)(48)}$.

(c) Write $\sigma = (124)(1326)(34576)$ as a product of disjoint cycles.

We give a little detail: $\sigma[1] = (124)(1326)(34576)[1] = (124)(1326)[1] = (124)[3] = 3$ since (34576) does not change 1, (1326) sends 1 to 3, and (124) does not change 3. Next, $\sigma[3] = (124)(1326)(34576)[3] = (124)(1326)[4] = (124)[4] = 1$. So now we know that σ sends 1 to 3 and then 3 back to 1. This is represented by the 2-cycle (i.e., transposition) (13). Next, we see that $\sigma[2] = 6$ then $\sigma[6] = 4$ then $\sigma[4] = 5$ then $\sigma[5] = 7$ then $\sigma[7] = 2$. This gives us the 5-cycle (26457). Therefore, $\boxed{\sigma = (13)(26457)}$.

To get an inverse, we just write the permutation backwards and then simplify: $\sigma^{-1} = (75462)(31) = \boxed{(13)(27546)}$.

The order of σ is $|\sigma| = \underline{\quad \text{lcm}(|(13)|, |(26457)|) = \text{lcm}(2, 5) = \boxed{10} \quad}$.

Write σ as a product of transpositions: $\underline{\quad (13)(27)(25)(24)(26) \quad}$. σ is **Even** / $\boxed{\textbf{Odd}}$

Note: We used the trick $(a_1a_2\cdots a_k) = (a_1a_k)(a_1a_{k-1})\cdots(a_1a_2)$. Also, our permutation is odd since we needed 5, an odd number of, transpositions to represent σ. By the way, there are *many* correct answers that could go in the blank above. For example, we could have pulled our trick on the unsimplified version of σ and got $\sigma = (14)(12)(16)(12)(13)(36)(37)(35)(34)$.

$\sigma^{62} = \sigma^{62 \bmod 10} = \sigma^2 = (13)^2(26457)^2 = \boxed{(24765)}$.

(d) Does S_6 have an element of order 8? If not, explain why not. If so, give an example of such an element.

No. In S_n, to get an element of order 8 we need to have a permutation (written in terms of disjoint cycles of lengths $\ell_1, \ldots, \ell_m$) where $\text{lcm}(\ell_1, \ldots, \ell_m) = 8$. But this requires $\ell_1, \ldots, \ell_m$ to be divisors of 8 and *at least* one of them must be 8 itself – otherwise the least common multiple would be 4 or 2 or 1! Therefore to get an element of order 8, we need an 8-cycle. This requires $n \geq 8$. In summary, S_n has an element of order 8 if and only if $n \geq 8$.

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

(a) $Q \ncong \mathbb{Z}_8$ where $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group so $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, etc.

Both are groups of order 8. However, they cannot be isomorphic since Q is not Abelian (e.g., $ij = k \neq -k = ji$) whereas $\mathbb{Z}_8$ is Abelian. Alternatively, we could see that they are not isomorphic since Q's elements have orders 1, 2, and 4 whereas $\mathbb{Z}_8$ has elements of order 8 too (i.e., it's cyclic).

(b) $\mathbb{Z}_9 \ncong U(9)$

Both of these groups are Abelian. In fact, both are even cyclic: $\mathbb{Z}_9 = \langle 1 \rangle$ and $U(9) = \langle 2 \rangle$. However, they cannot be isomorphic since they aren't even the same size: $|\mathbb{Z}_9| = 9 \neq 6 = |U(9)| = |\{1, 2, 4, 5, 7, 8\}|$. Other things don't match either. For example, $U(9)$ has elements of order 6 (like 2 and 5) whereas $\mathbb{Z}_9$ only has elements of orders 1, 3, and 9.

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

Notice that $|S_4| = 4! = 24 = 2 \cdot 12 = |D_{12}|$ and both are non-Abelian (thus non-cyclic) groups. However, D_{12} has elements of order 12 (for example the rotation by $360°/12 = 30°$) whereas S_4 only has elements of orders 1, 2, 3, and 4. We could also see that these groups are not isomorphic by counting the number of elements of various orders and seeing these counts don't match. For example, D_{12} has $12 + 1 = 13$ elements of order 2 (i.e, 12 reflections and the 180° rotation) whereas S_4 has 9 elements of order 2 (i.e., (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), and (14)(23)).

5. (20 points) A few proofs

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

First, $S_3 = \{(1), (123), (132), (12), (13), (23)\}$ so $A_3 = \{(1), (123), (132)\}$ (the even permutations). Notice that $A_3 = \langle (123) \rangle$ so A_3 is a cyclic group of order 3. But $\mathbb{Z}_3 = \langle 1 \rangle = \{0, 1, 2\}$ is also a cyclic group of order 3. Therefore, since any two cyclic groups of the same order are isomorphic, we have $A_3 \cong \mathbb{Z}_3$.

On the other hand, $|A_n| = n!/2 > n = |\mathbb{Z}_n|$ for $n > 3$. [I would accept that inequality as "obvious". But in case you wanted a proof: $4!/2 = 12 > 4$ (base case). Assume $n > 3$ and $n!/2 > n$. Then $(n+1)!/2 = (n+1) \cdot n!/2 > (n+1)n$ using the inductive hypothesis $n!/2 > n$. But $(n+1)n = n^2 + n \geq n$. Therefore, by induction, $n!/2 > n$ for all $n > 3$.] Therefore, since for any $n > 3$, A_n and $\mathbb{Z}_n$ have different sizes, they cannot be isomorphic.

Alternatively, note that $(123)(124) = (13)(24) \neq (14)(23) = (124)(123)$ so that A_n is not Abelian for any $n > 3$ whereas $\mathbb{Z}_n$ is Abelian for all n. Therefore, $A_n \ncong \mathbb{Z}_n$ for $n > 3$.

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

I. Show that every cyclic group is Abelian. Then explain why the converse is not true.

Suppose $G = \langle g \rangle$ (i.e., suppose G is cyclic). Let $x, y \in G$ so there exists $k, \ell \in \mathbb{Z}$ such that $x = g^k$ and $y = g^\ell$. Therefore, $xy = g^k g^\ell = g^{k+\ell} = g^{\ell+k} = g^\ell g^k = yx$. Thus G is Abelian.

To see that the converse fails, consider the Abelian group $U(8) = \{1, 3, 5, 7\}$. Notice that $1 = 3^2 = 5^2 = 7^2$ so $U(8)$ has no element of order 4. Thus $U(8)$ is Abelian, but it is not cyclic.

II. Show that $\mathbb{R} \cong \mathbb{R}_{>0}$. *Hint:* Consider an exponential function for φ.
Note: $\mathbb{R}_{>0} = (0, \infty)$ is the group of positive real numbers.

First, keep in mind that $\mathbb{R}$ is a group under addition (notice $0 \in \mathbb{R}$) whereas $\mathbb{R}_{>0}$ is a group under multiplication (notice $0 \notin \mathbb{R}_{>0}$). We need to turn additions into multiplications – exponentiation should do the job.

Let $\varphi : \mathbb{R} \to \mathbb{R}_{>0}$ be defined by $\varphi(x) = e^x$ (we will use the natural log base e, but any positive constant would do). Let $a, b \in \mathbb{R}$. Then $\varphi(a + b) = e^{a+b} = e^a e^b = \varphi(a)\varphi(b)$, so φ is a "homomorphism" (i.e., it is operation preserving). *Note:* The operation in the domain is addition. Thus the "$a + b$" in φ's argument. And the operation is multiplication in the codomain. Thus we should have $\varphi(a) \cdot \varphi(b)$ when combining outputs.

We also need to show that φ is an invertible map. This can be done by showing it is one-to-one and onto or by exhibiting an inverse. We will do this both ways.

We have that $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ and $\ln(\varphi(x)) = \ln(e^x) = x$ for all x and $\varphi(\ln(x)) = e^{\ln(x)} = x$ for all $x > 0$. Therefore, $\varphi^{-1} = \ln$ exists (so φ is invertible). Alternatively, suppose $\varphi(a) = \varphi(b)$ for some $a, b \in \mathbb{R}$. Then $e^a = e^b$ so that $a = \ln(e^a) = \ln(e^b) = b$. Thus φ is one-to-one. Finally, suppose $y \in \mathbb{R}_{>0}$ and consider $x = \ln(y) \in \mathbb{R}$. Notice that $\varphi(x) = \varphi(\ln(y)) = e^{\ln(y)} = y$ so that φ is onto.

We have shown that φ is an operation preserving, invertible map. Therefore, φ is an isomorphism (between $\mathbb{R}$ and $\mathbb{R}_{>0}$). Thus $\mathbb{R} \cong \mathbb{R}_{>0}$.