Math 3110 **Test #2** **March 12th, 2021**

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

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

$G =$	Identity?	What is the order of ...?	Does G have an element of order 4?	Abelian?	Cyclic?
$\mathbb{Z}_{100}$	0	$\lvert 55\rvert = \frac{100}{\gcd(100,55)} = \frac{100}{5} = 20$	Yes, for example, $\frac{100}{4} = 25$.	Yes.	Yes, $\mathbb{Z}_{100} = \langle 1\rangle$
$U(12)$	1	$\lvert 5\rvert = 2$ since $5^2 = 1 \pmod{12}$	No, $1^1 = 5^2 = 7^2 = 11^2 = 1$.	Yes.	No, nothing of order 4.
D_{15}	1 (or R_{0°)	$\lvert x^9\rvert = \lvert x^{\gcd(9,15)}\rvert = \lvert x^3\rvert = \frac{15}{3} = 5$	No, 4 does not divide 15.	No.	No, not even Abelian.
S_8	(1)	$\lvert(12345)(678)\rvert = \operatorname{lcm}(5,3) = 15$	Yes, for example, (1234).	No.	No, not even Abelian.

Recall: $D_{15} = \{1, x, \ldots, x^{14}, y, xy, \ldots, x^{14}y\}$ where $x^{15} = 1$, $y^2 = 1$, and $xyxy = 1$.

Notes: Remember that in $\mathbb{Z}_n$, $\langle k\rangle = \langle \gcd(k,n)\rangle$ so that $|k| = n/\gcd(k,n)$. Likewise, if $g^n = 1$, then $\langle g\rangle = \langle g^{\gcd(k,n)}\rangle$ and so $|g^k| = n/\gcd(k,n)$. This helps us with order of 55 in $\mathbb{Z}_{100}$ and the order of x^9 in D_{15}.

Recall that $U(12) = \{k \in \mathbb{Z}_{12} \mid \gcd(k,12) = 1\} = \{1,5,7,11\}$. In this group, the order of 1 is 1 and the rest of the elements have order 2 since they square to 1 (working mod 12). Thus, while $U(12)$ is Abelian, we have that $U(12)$ is not cyclic (we'd need an element of order 4 to generate all of $U(12)$).

2. (20 points) Cyclic Stuff

(a) Let G be a finite group and $g \in G$. Suppose that $|g| = 63 = 3^2 \cdot 7$.

i. What is the order of g^{45}? List the distinct elements in $\langle g^{45}\rangle$.

We have $\langle g^{45}\rangle = \langle g^{\gcd(45,63)}\rangle = \langle g^9\rangle = \boxed{\{1, g^9, g^{18}, g^{27}, g^{36}, g^{45}, g^{54}\}}$ and $|g^{45}| = |g^{\gcd(45,63)}| = |g^9| = 63/9 = \boxed{7}$.

ii. Is $g^{13} \in \langle g^{55}\rangle$? **Yes** / **No**

Notice that $\langle g^{55}\rangle = \langle g^{\gcd(55,63)}\rangle = \langle g^1\rangle$, so of course $g^{13} \in \langle g\rangle = \langle g^{55}\rangle$.

(b) How many elements of order 12 does $\mathbb{Z}_{36}$ have? What are they?

Notice that $36/12 = 3$ so we do in fact have an element of order 12 (and one such element is 3). Thus there are a total of $|U(12)| = |\{1,5,7,11\}| = \boxed{4}$ elements of order 12. We compute $3 \cdot 1, 3 \cdot 5, 3 \cdot 7$, and $3 \cdot 11$. The elements of order 12 are $\boxed{3, 15, 21, \text{ and } 33}$.

(c) List the orders of elements in $\mathbb{Z}_{35}$. Then determine the number of elements of each order.

Order =	1	5	7	35
Number of elements =	1	$5-1=4$	$7-1=6$	$35-1-4-6=24$

Recall how this works, for example, a cyclic group whose order is divisible by 35 has a unique subgroup of order 35. This subgroup itself has unique subgroups of order 1, 5, and 7. The only element of the trivial subgroup (of order 1) is the identity – so 1 element of order 1 (always). Next, any element of order 5 must belong to the subgroup of order 5. This subgroup has elements of orders 1 and 5 only. So if we knock out the element(s) of order 1, we are left with $5 - 1 = 4$ elements of order 5. Likewise, there are $7 - 1 = 6$ elements of order 7. Finally, the elements of order 35 must belong to the (unique) subgroup of order 35, the other elements in this subgroup must have orders 1, 5, and 7 (the other divisors). Thus knocking out those elements, we are left with $35 - 1 - 4 - 6 = 24$ elements of order 35.

Alternatively, we could use the Euler φ-function (or totient function). This allows us the compute the number of elements of order d (for a divisor d of n) in $\mathbb{Z}_n$ directly. The number of elements of order d in $\mathbb{Z}_n$ is $|U(d)| = \varphi(d)$. Thus the number of elements of order 35 is $|U(35)| = \varphi(35) = \varphi(5 \cdot 7) = \varphi(5)\varphi(7) = (5^1 - 5^0)(7^1 - 7^0) = 4 \cdot 6 = 24$.

(d) List the orders of elements in D_{35}. Then determine the number of elements of each order.

Order =	1	2	5	7	35
Number of elements =	1	35	4	6	24

Note: We just add in the 35 reflections.

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

(a) Consider $G = \langle i \rangle = \{1, i, -1, -i\}$ where $i = \sqrt{-1}$ so that $i^2 = -1$. 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].

Left multiplying by i yields: $L_i(1) = i \cdot 1 = i$, $L_i(i) = i \cdot i = -1$, $L_i(-1) = i \cdot (-1) = -i$, and $L_i(-i) = i \cdot (-i) = 1$. Numbering the elements, we have $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1$, so i represented by L_i is in turn represented by (1234). We could go through a similar computation for each of the rest of the elements of G or just use the fact that $-1 = i^2$ and $-i = i^3$ will be represented by $(1234)^2 = (13)(24)$ and $(1234)^3 = (1234)^{-1} = (1432)$ respectively. Therefore, $G = \langle i \rangle \cong \langle (1234) \rangle = \boxed{\{(1), (1234), (13)(24), (1432)\}}$.

(b) Write $\sigma = (243)(1523)(364)$ as a product of disjoint cycles.

For example: $\sigma[1] = (243)(1523)(364)[1] = (243)(1523)[1] = (243)[5] = 5$ and then $\sigma[5] = (243)(1523)(364)[5] = (243)(1523)[5] = (243)[2] = 4$. Continuing in this fashion, we get that $\sigma = (154)(2)(36) = \boxed{(154)(36)}$.

$\sigma^{-1} = (63)(451) = \boxed{(145)(36)}$ [Write it backwards and then clean it up.]

The order of σ is $|\sigma| =$ $\underline{\text{lcm}(3, 2) = 6}$. [Make sure you use the disjoint cycle representation to compute this.]

Write σ as a product of transpositions. σ is **Even** / $\boxed{\textbf{Odd}}$ [We use an odd number of transpositions below.]

$\sigma = \boxed{(14)(15)(36)}$ or $\boxed{(23)(24)(13)(12)(15)(34)(36)}$ (among other possible correct answers).

Compute $\sigma^{64} = ((154)(36))^{64} = (154)^{64 \bmod 3}(36)^{64 \bmod 2} = (154)^1(36)^0 = \boxed{(154)}$.

Note: We used $(ab)^k = a^k b^k$. This exponent law requires $ab = ba$. We can apply this rule since disjoint cycles commute.

(c) Does S_{10} have an element of order 30? If not, explain why not. If so, give an example of such an element.

$\boxed{\text{Yes.}}$ Notice that $\text{lcm}(5, 3, 2) = 30$ so $\boxed{(12345)(678)(9, 10)}$ has order 30.

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

(a) $\mathbb{Z}_{12} \ncong U(12)$

Since $\mathbb{Z}_{12}$ has order 12 whereas $U(12) = \{1, 5, 7, 11\}$ is a group of order 4, these cannot be isomorphic groups. Alternatively, on the first page of the test we noted that $U(12)$ is not cyclic. Therefore, $\mathbb{Z}_{12} \ncong U(12)$ because $\mathbb{Z}_{12}$ is cyclic but $U(12)$ is not. Or we could note that $\mathbb{Z}_{12}$ only has 1 element of order 2 while $U(12)$ has 3 elements of order 2. Or we could note that $\mathbb{Z}_{12}$ has elements of order 3, 4, 6, and 12 while $U(12)$ does not.

(b) $S_4 \ncong D_{12}$ $|S_4| = 4! = 24 = 2 \cdot 12 = |D_{12}|$ so both are non-Abelian groups of order 24 (no help here).

Notice that element orders don't match up. The symmetric group S_4 has elements of orders 1, 2, 3, and 4 whereas D_{12} has elements of orders 1, 2, 3, 4, 6, and 12. Therefore, since for example D_{12} has an element of order 12 but S_4 does not, these groups cannot be isomorphic. Alternatively, we could count elements of various orders and get a proof from that data. For example, D_{12} has $12 + 1 = 13$ elements of order 2 (i.e., 12 reflections plus the rotation of 180°) but S_4 only has 9 elements of order 2 (i.e., $(12), (13), (14), (23), (24), (34), (12)(34), (13)(24)$, and $(14)(23)$).

(c) $A_5 \ncong \mathbb{Z}_{60}$ Both are groups of order 60 since $|A_5| = 5!/2 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1/2 = 120/2 = 60$.

The alternating group, A_5, of even permutations on 5 characters is not Abelian whereas $\mathbb{Z}_{60}$ is Abelian. Therefore, they cannot be isomorphic. Of course, many other properties could give us a proof as well. For example, $\mathbb{Z}_{60}$ only has 1 element of order 2 (i.e., $60/2 = 30$) but A_5 has a bunch of elements of order 2 (e.g., $(12)(34)$ and $(13)(24)$ etc.). Thus they cannot be isomorphic.

5. (20 points) A few proofs

(a) Explain why $S_2 \cong \mathbb{Z}_2$ but $S_n \ncong \mathbb{Z}_{n!}$ for any $n > 2$.

Notice that $S_2 = \{(1), (12)\} = \langle (12) \rangle$ is a cyclic group of order 2. Thus since cyclic groups of the same order are isomorphic, $S_2 \cong \mathbb{Z}_2$. On the other hand, while S_n and $\mathbb{Z}_{n!}$ are groups of order $n!$, S_n is not Abelian (example: $(12)(13) = (132) \neq (123) = (13)(12)$) whereas $\mathbb{Z}_{n!}$ is Abelian. Thus they cannot be isomorphic.

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

I. Let G be a group and $g \in G$. Show that $\varphi : G \to G$ defined by $\varphi(x) = gxg^{-1}$ is an automorphism.

Let G be a group, $g \in G$, and define $\varphi : G \to G$ by $\varphi(x) = gxg^{-1}$ for all $x \in G$. Let us show the φ is an isomorphism (i.e., it is one-to-one, onto, and operation preserving).

- Suppose that $\varphi(x) = \varphi(y)$ for some $x, y \in G$. Then $gxg^{-1} = gyg^{-1}$. Multiplying this equation on the left by g^{-1} and on the right by g yields: $g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$ so that $x = y$. Therefore, φ is one-to-one.
- Suppose $y \in G$. Consider $g^{-1}yg \in G$. We have $\varphi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y$. Therefore, y is in the range of φ. Thus φ is onto.
- Suppose $x, y \in G$. Then $\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y)$ so φ is operation preserving.

Therefore, φ is an isomorphism. Since φ has the same domain and codomain, we call it an automorphism.

Note: We could have shown φ is one-to-one and onto by exhibiting an inverse. For example, consider $\psi : G \to G$ defined by $\psi(x) = g^{-1}xg$. Then $\varphi(\psi(x)) = \varphi(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$ so $\varphi \circ \psi = \mathrm{id}_G$. Likewise, $\psi \circ \varphi = \mathrm{id}_G$. Thus $\varphi^{-1} = \psi$ exists and so φ is one-to-one and onto (because it is invertible).

II. Let $\psi : G_1 \to G_2$ be an isomorphism and suppose G_1 is Abelian. Show G_2 is Abelian.

Suppose $\psi : G_1 \to G_2$ is an isomorphism and that G_1 is Abelian. Let $a, b \in G_2$. Now ψ is onto (since it is an isomorphism). Thus there exists $x, y \in G_1$ such that $\psi(x) = a$ and $\psi(y) = b$. Therefore, $ab = \psi(x)\psi(y) = \psi(xy) = \psi(yx) = \psi(y)\psi(x) = ba$ where the second and fourth equalities follow since ψ is operation preserving and the third equality used our assumption that G_1 is Abelian (so $xy = yx$). Therefore, since $ab = ba$ for all $a, b \in G_2$, we have that G_2 is Abelian.