**Math 3110** **Test #2** **October 9th, 2020**

**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 5? | Is $G$ abelian? | Is $G$ cyclic? |
|---|---|---|---|---|---|
| $\mathbb{Z}_{80}$ | 0 | $\lvert 25\rvert = 80/\gcd(80,25) = 80/5 = 16$ | Yes, $\lvert 80/5\rvert = \lvert 16\rvert = 5$. | Yes. | Yes, it can be generated by 1. |
| $U(9)$ | 1 | $\lvert 2\rvert = 6$ | No, 5 doesn't divide 6. | Yes. | Yes, 2 is a generator. |
| $D_{12}$ | $1 = R_{0^\circ}$ | $\lvert x^8\rvert = 3$ | No, 5 doesn't divide 24. | No, $xy \neq yx$. | No, it's not even Abelian. |
| $S_9$ | (1) | $\lvert(1234)(56)(789)\rvert = \operatorname{lcm}(4,2,3) = 12$ | Yes, $\lvert(12345)\rvert = 5$. | No, $(12)(13) \neq (13)(12)$. | No, it's not even Abelian. |

**Recall:** $D_{12} = \{1, x, \ldots, x^{11}, y, xy, \ldots, x^{11}y\}$ where $x^{12} = 1$, $y^2 = 1$, and $xyxy = 1$.

- $\mathbb{Z}_{80}$ is a group under addition modulo 80 thus its identity is 0. We know $\langle 25\rangle = \langle \gcd(25, 80)\rangle = \langle 5\rangle$, so $\lvert 25\rvert = \lvert 5\rvert = 80/5 = 16$. Notice that for any divisor $k$, $80/k$ is an element of order $k$. So, $80/5 = 16$ has order 5. $\mathbb{Z}_{80}$ is generated by every element in $U(80)$ – in particular, it's generated by 1. Therefore, this is a cyclic group (and thus Abelian).
- $U(9)$ is a group under multiplication modulo 9 thus its identity is 1. $U(9) = \{k \mid \gcd(k, 9) = 1\} = \{1, 2, 4, 5, 7, 8\}$, so this is a group of order 6. Notice that $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 = 7$, $2^5 = 32 = 5$, and $2^6 = 64 = 1$. Thus $\lvert 2\rvert = 6$. This also shows that 2 generates all of $U(6)$. Thus $U(6)$ is cyclic (and thus Abelian). Finally, since $\lvert U(9)\rvert = 6$ and 5 doesn't divide 6, there are no elements of order 5. Alternatively, we could just verify the order of each element (we would see they have orders 1, 2, 3, and 6 but not 5).
- $D_{12}$ is a group under function composition if thought of as a symmetry group. Otherwise, its operation just an abstract generator/relation group multiplication. Thus the identity of $D_{12}$ is denoted by either $R_{0^\circ}$ (the zero degree rotation) or just plain old 1. Note that $\lvert x\rvert = 12$, so $\langle x^8\rangle = \langle x^{\gcd(8,12)}\rangle = \langle x^4\rangle$. Thus $\lvert x^8\rvert = \lvert x^4\rvert = 12/4 = 3$. Alternatively, $(x^8)^1 = x^8$, $(x^8)^2 = x^{16} = x^4$, $(x^8)^3 = x^{24} = 1$, so $\lvert x^8\rvert = 3$. We know that $D_{12}$ has rotations of orders 1, 2, 3, 4, 6, and 12 (i.e., divisors of 12) and its reflections have order 2. Thus it has no elements of order 5. This is not an Abelian group since $xy \neq yx = x^{-1}y = x^{11}y$. Finally, it isn't cyclic since cyclic groups must be Abelian.
- $S_9$ is a group under function composition with the identity transformation, (1), as its identity element. Orders of permutations are just least common multiples of the length of the permutation's cycles if it is written in terms of disjoint cycles. Thus $\lvert(1234)(56)(789)\rvert = \operatorname{lcm}(4, 2, 3) = 12$. Any 5-cycle gives us an element of order 5, so $\lvert(12345)\rvert = 5$. We know that $S_n$ is not Abelian for $n \geq 3$. In particular, we have $(12)(13) = (132) \neq (123) = (13)(12)$. Since $S_9$ isn't Abelian, it cannot be cyclic.

**2. (20 points)** Cyclic Stuff

(a) Let $G$ be a finite group and $g \in G$. Suppose that $\lvert g\rvert = 49$.

i. What is the order of $g^{28}$? List the distinct elements in $\langle g^{28}\rangle$.

$\lvert g^{28}\rvert = \dfrac{49}{\gcd(28, 49)} = \dfrac{49}{7} = \boxed{7}$. We have $\langle g^{28}\rangle = \langle g^{\gcd(28,49)}\rangle = \langle g^7\rangle = \boxed{\{1, g^7, g^{14}, g^{21}, g^{28}, g^{35}, g^{42}\}}$ (7 elements).

ii. Is $g^6 \in \langle g^{14}\rangle$? **Yes** / **No** $\langle g^{14}\rangle = \langle g^{\gcd(14,49)}\rangle = \langle g^7\rangle$ (as above), so $g^6 \notin \langle g^{14}\rangle$.

(b) How many elements of order 8 does $\mathbb{Z}_{40}$ have? What are they?

Notice that 8 divides 40, so $\mathbb{Z}_{40}$ does in fact have elements of order 8. In any cyclic group whose order is divisible by 8, we have 1 element of order 1, $2 - 1 = 1$ element of order 2, $4 - 1 - 1 = 2$ elements of order 4, and $8 - 2 - 1 - 1 = 4$ elements of order 8.

To get a single element of order 8, we divide: $40/8 = 5$. To get the rest of the elements of order 8, we multiply this element, 5, by elements of $U(8) = \{1, 3, 5, 7\}$. Thus, there are $\boxed{4}$ elements of order 8. In particular, they are $\boxed{5,\ 15,\ 25,\ \text{and } 35}$.

(c) List the orders of elements in $\mathbb{Z}_{77}$. Then determine the number of elements of each order.

There are elements of order $k$ for each divisor $k$ of 77. Also, we use the fact that cyclic subgroups have unique (cyclic) subgroups for each divisor order. Thus, for example, there is exactly one subgroup of order 11. It's elements have orders 1 and 11 (divisors of 11). If we toss out the (only) element of order 1 (i.e., the identity), we are left with $11 - 1 = 10$ elements. Each of these must have order 11. We thus recursively compute the number of elements of each order after first noting that the divisors of 77 are 1, 7, 11, and 77.

| Order = | 1 | 7 | 11 | 77 |
|---|---|---|---|---|
| Number of elements = | 1 | $7 - 1 = 6$ | $11 - 1 = 10$ | $77 - 10 - 6 - 1 = 60$ |

(d) List the orders of elements in $D_{77}$. Then determine the number of elements of each order.

The rotations form a subgroup isomorphic to $\mathbb{Z}_{77}$. Thus we can use the table from part (c) to account for their orders and frequency. We also have 77 reflections. Reflections have order 2.

| Order = | 1 | 2 | 7 | 11 | 77 |
|---|---|---|---|---|---|
| Number of elements = | 1 | 77 | 6 | 10 | 60 |

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

(a) Consider $D_4 = \langle x, y \mid x^4 = 1, y^2 = 1, (xy)^2 = 1\rangle = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$.

Label these elements in the order listed above: 1 as 1, $x$ as 2,... $x^3y$ as 8. Cayley's theorem says that $D_4$ is isomorphic to a subgroup of $S_8$. Using left multiplication maps and the labels provided, what element of $S_8$ represents $y$?

Left multiplication by $y$ sends 1 to $y$ (i.e., 1 to 5), $x$ to $yx = x^{-1}y = x^3y$ (i.e., 2 to 8), $x^2$ to $yx^2 = x^{-2}y = x^2y$ (i.e., 3 to 7), and $x^3$ to $yx^3 = x^{-3}y = xy$ (i.e., 4 to 6). It then sends each of these outputs back to where they came from (since $y$ is its own inverse). Thus $y$'s left multiplication is represented by $\boxed{(15)(28)(37)(46)}$.

Assuming that this correspondence associates $xy$ with (16)(25)(38)(47) and $x$ with (1234)(5678). What permuation is associated with $x^2y$?

Since Cayley's theorem gives an isomorphism between $D_4$ and some permutations in $S_8$ and since $x^2y = x \cdot xy$, we should have that $x^2y$ is represented by $x$'s permutation times $xy$'s permutation: (1234)(5678)(16)(25)(38)(47) = $\boxed{(17)(26)(35)(48)}$. Notice also, $y = x^4y = x^2 \cdot x^2y$ so $y$ should be represented by $\Big((1234)(5678)\Big)^2(17)(26)(35)(48)$ = (13)(24)(57)(68)(17)(26)(35)(48) = (15)(28)(37)(46) just like we found in part (a).

(b) Write $\sigma = (1235)(14)(236)$ as a product of disjoint cycles (and compute some stuff).

$\boxed{\sigma = (1425)(36)}$ and so $\sigma^{-1} = (63)(5241) = (5241)(63) = \boxed{(1524)(36)}$. The order of $\sigma$ is $|\sigma| = \text{lcm}(4, 2) = \boxed{4}$.

Write $\sigma$ as a product of transpositions: $\sigma = \boxed{(15)(12)(14)(36)}$ or we could use the original (un-simplified non-disjoint description of $\sigma$) $\sigma = \boxed{(15)(13)(12)(14)(26)(23)}$. Either way there are an $\sigma$ is $\boxed{\textbf{Even}}$ / **Odd** number of transpositions used to write $\sigma$.

Compute $\sigma^{102} = \sigma^{102 \bmod 4} = \sigma^2 = (1425)(36)(1425)(36) = \boxed{(12)(45)}$ (here we use the fact that $|\sigma| = 4$ to reduce the exponent). Alternatively, noting that disjoint cycles commute, we have $\sigma^{102} = \Big((1524)(36)\Big)^{102} = (1524)^{102}(36)^{102} = (1524)^{102 \bmod 4}(36)^{102 \bmod 2} = (1524)^2(36)^0 = (1524)^2 = (12)(45)$.

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

(a) $\mathbb{R}^{2\times 2} \ncong \text{GL}_2(\mathbb{R})$ [$\mathbb{R}^{2\times 2}$ is the $2 \times 2$ matrices under addition.]

Both of these are infinite groups (in fact, continuum in cardinality), so size doesn't help us. However, since matrix multiplication is non-commutative, $\text{GL}_2(\mathbb{R})$ is not Abelian. Therefore, these groups cannot be isomorphic given $\mathbb{R}^{2\times 2}$ is $\boxed{\text{Abelian}}$ (under matrix addition) whereas $\text{GL}_2(\mathbb{R})$ is $\boxed{\text{not Abelian}}$ (under matrix multiplication).

Of course, there are other ways to see that these groups cannot be isomorphic. For example, if $A \neq 0$, then $A+A+\cdots+A \neq 0$. Thus other than the identity (i.e., the zero matrix) every element in $\mathbb{R}^{2\times 2}$ has infinite order. On the other hand, there are elements of every possible order in $\text{GL}_2(\mathbb{R})$. In particular, $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ has order 2 since $B^2 = I_2$.

(b) $D_4 \ncong Q$ $[Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the group of quaternions.]

Both of these are non-Abelian groups of order 8, so no help there. However, notice that $D_4$ has 5 elements of order 2 (it has the 180° rotation and 4 reflections). On the other hand, $Q$'s only element of order 2 is $-1$. Thus $\boxed{D_4 \text{ and } Q \text{ do not have the same number of elements of order 2}}$. Thus they are not isomorphic.

As always, we could see this other ways. For example, $D_4$ only has 2 elements of order 4 whereas $Q$ has 6 elements of order 4.

(c) $A_5 \ncong \mathbb{Z}_{60}$

Notice that $|A_5| = 5!/2 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1/2 = 60$, so both are groups of order 60. However, $A_5$ is $\boxed{\text{not Abelian}}$ whereas $\mathbb{Z}_{60}$ is $\boxed{\text{Abelian}}$ (in fact, it's cyclic). Therefore, these groups cannot be isomorphic.

Again, there are many other ways to see these groups cannot be isomorphic. We could note that 30 is the only element of order 2 in $\mathbb{Z}_{60}$ whereas $A_5$ has many elements of order 2 including (12)(34) and (13)(24). Or notice that the largest order appearing in $S_5$ is 6 (e.g., (123)(45)), but such elements are odd. So the largest order appearing in $A_5$ is 5 (e.g., (12345)). On the other hand, $\mathbb{Z}_{60}$ has elements of higher orders such as 10, 12, 15, 30, and 60.

## 5. (20 points) A few proofs

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

Prove that $G \cong U(10)$.

Notice that $G = \langle i \rangle$ is cyclic of order 4. Likewise, since $3^1 = 3$, $3^2 = 9$, $3^3 = 27 = 7$, and $3^4 = 81 = 1 \pmod{10}$, we have $U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle$ is also cyclic of order 4. Therefore, since we know that cyclic groups of the same order must be isomorphic, we have that $G \cong U(10)$.

(b) We know $A_n$ is not abelian for $n > 3$. Show this.

The usual counterexample: $(12)(13) = (132) \neq (123) = (13)(12)$ that shows $S_n$ is non-Abelian for $n \geq 3$ does not work here since $(12), (13) \notin A_n$ (they're odd).

However, notice that $(123), (234) \in A_n$ as along as $n \geq 4$ (odd length cycles are even permutations). Now notice that $(123)(234) = (12)(34) \neq (13)(24) = (234)(123)$. Therefore, $A_n$ is not Abelian (as long as $n > 3$).

*Note:* $A_1$ doesn't really make sense since we need at least 2 things to form transpositions. Notice that $A_2 = \{(1)\}$, so $A_2$ – the trivial group – is Abelian and even cyclic. Also, $A_3 = \{(1), (123), (132)\} = \langle (123) \rangle$, so again $A_3$ is not only Abelian, it's cyclic!

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

I. Define $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_9$ by $\varphi(x) = 4x$. Show $\varphi$ is an automorphism of $\mathbb{Z}_9$. What is its inverse? Why is $\psi : \mathbb{Z}_8 \to \mathbb{Z}_8$ defined by $\psi(x) = 4x$ **not** an automorphism of $\mathbb{Z}_8$?

Let $x, y \in \mathbb{Z}_9$. Notice that $4 \cdot 7 = 28 = 1 \pmod{9}$. Thus $\varphi^{-1}(x) = 7x$: $\varphi^{-1}(\varphi(x)) = \varphi^{-1}(4x) = 7(4x) = 28x = x$ and $\varphi(\varphi^{-1}(x)) = \varphi(7x) = 4(7x) = 28x = x$. This means $\varphi$ is invertible (i.e., one-to-one and onto). Next, $\varphi(x+y) = 4(x+y) = 4x + 4y = \varphi(x) + \varphi(y)$. Thus $\varphi$ is operation preserving. Therefore, $\varphi$ is an isomorphism from $\mathbb{Z}_9$ to itself (i.e., it's an automorphism).

On the other hand, 4 has no multiplicative inverse modulo 8 (i.e., $4 \notin U(8)$), so $\psi$ doesn't have an inverse. In particular, notice $\psi(2) = 4(2) = 0 = 4(0) = \psi(0)$ (working mod 8). Thus $\psi$ isn't one-to-one. Therefore, $\psi$ is not an automorphism of $\mathbb{Z}_8$. On the other hand, it is an homomorphism from $\mathbb{Z}_8$ to itself: $\psi(x+y) = 4(x+y) = 4x + 4y = \psi(x) + \psi(y)$ (for any $x, y \in \mathbb{Z}_8$), so $\psi$ is an *endomorphism* of $\mathbb{Z}_8$.

II. Show that if $G$ is cyclic, then it must also be abelian. Is the converse also true? Why or why not? Justify your answer(s).

Suppose $G$ is cyclic. Then there exists some $g \in G$ such that $G = \langle g \rangle$. Now suppose $x, y \in G$. Then since $x, y \in \langle g \rangle$, there exists $k, \ell \in \mathbb{Z}$ such that $x = g^k$ and $y = g^\ell$. We have $xy = g^k g^\ell = g^{k+\ell} = g^{\ell+k} = g^\ell g^k = yx$. Thus $G$ is Abelian.

The converse is false. Note that $U(12) = \{1, 5, 7, 11\}$ is an Abelian group (under multiplication mod 12). But $5^2 = 25 = 1$, $7^2 = 49 = 1$, $11^2 = 121 = 1 \pmod{12}$. Thus the elements in $U(12)$ have orders 1 (i.e., the identity) and 2 (i.e., $5, 7, 11$). Since $U(12)$ has no element of order 4, it has no generator. Thus $U(12)$ is *not* cyclic – even though it is Abelian.