Math 3110 **Test #2** **March 31st, 2010**

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 4?
$\mathbb{Z}_{40}$	0	Yes	Yes	$\|30\| = 4$	Yes, 30
$U(8)$	1	Yes	No	$\|5\| = 2$	No, not cyclic
D_7	1 or R_0	No	No	$\|x^4y\| = 2$	No, 4 does not divide $7 \cdot 2 = 14$
S_4	(1)	No	No	$\|(12)(34)\| = 2$	Yes, (1234)

Recall: $D_7 = \{1, x, \ldots, x^6, y, xy, \ldots, x^6y\}$ where $x^7 = 1$, $y^2 = 1$, and $xyxy = 1$.

Scratch Work:

$\mathbb{Z}_n$ is cyclic (generated by 1) and thus abelian for all n. The operation is addition (mod n) so the (additive) identity is 0. $30 + 30 = 60 = 20 \bmod 40$, $30 + 30 + 30 = 90 = 10 \bmod 40$, $30 + 30 + 30 + 30 = 120 = 0 \bmod 40$. So $|30| = 4$ in $\mathbb{Z}_{40}$.

$U(n)$ is abelian for all n. Its operation is multiplication (mod n) so the (multiplicative) identity is 1. $U(8) = \{k \in \mathbb{Z}_8 \mid (k, 8) = 1\} = \{1, 3, 5, 7\}$. Notice that $3^2 = 5^2 = 7^2 = 1 \bmod 8$, so $U(8)$ has no elements of order 4 and thus is not cyclic.

D_n is the dihedral group of order $2n$ ($n \geq 3$). These groups are never abelian. The identity of D_n is the rotation of zero degrees. Since D_n is not abelian, it cannot be cyclic (recall cyclic imples abelian). x^4 is a rotation and y is a reflection, so x^4y is a reflection (a rotation times a reflection is a reflection). Thus $|x^4y| = 2$ (all reflections have order 2). Alternatively, $(x^4y)^2 = x^4yx^4y = x^4x^{-4}yy = x^0y^2 = y^2 = 1$ thus order 2. Finally, the order of an element divides the order of the group, so since $|D_7| = 14$ and 4 does not divide 14, D_7 cannot have any elements of order 4. Actually more can be said, D_7 has 1 element of order 1 (the identity), 6 elements of order 7 (the non-identity rotations), and 7 elements of order 2 (the reflections).

The permutation groups S_n are non-abelian (and thus not cyclic) for $n > 2$. The identity permutation is denoted (1). The order of a permutation written as a product of disjoint cycles is just the least common multiple of the lengths of the cycles. Thus $|(12)(34)| = \text{lcm}(2, 2) = 2$. Finally, any 4-cycle has order 4, so S_4 has pleanty of elements of order 4.

2. (20 points) Group or not? Are the following sets with operations groups or not? If G is a group, prove it — you may use a subgroup test if it applies. If G fails to be a group, explain what property fails.

(a) Let $G = [-1, 1] = \{r \in \mathbb{R} \mid -1 \leq r \leq 1\}$ with the operation "+" (addition).

If you start checking, the operation is associative, has an identity: 0, there are inverses (in G) for each element, but G is not a group – the operation is **not closed**. So to show G is not a group, we simply need to give a counterexample showing the operation is not closed.

G is not a group because $1, 1 \in G$ but $1 + 1 = 2 \notin G$.

(b) Let $G = \left\{ \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix} \middle| \, r \in \mathbb{R} \right\}$ with the operation of matrix multiplication.

Notice that for all $A = \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix} \in G$, $\det(A) = 1 \neq 0$. Thus $G \subseteq \text{GL}_2(\mathbb{R})$ (the general linear group – that is – the group of 2×2 invertible matrices). Thus to show G is a group we merely need to go through the subgroup test.

It is easy to see that G is non-empty.

Suppose $A = \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix} \in G$. Then $AB = \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ r+s & 1 \end{bmatrix} \in G$. Thus G is closed under matrix multiplication. Next, recall that the inverse of an invertible 2×2 matrix is given by $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Therefore, $A^{-1} = \begin{bmatrix} 1 & 0 \\ -r & 1 \end{bmatrix} \in G$. Thus G is closed under inversion.

Therefore, G is a subgroup of $\text{GL}_2(\mathbb{R})$ and so G is a group.

3. (15 points) Cayley's Theorem and Permutations.
Recall that $D_n = \{1, x, x^2, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\}$ where $x^n = 1$, $y^2 = 1$, and $xyxy = 1$.

(a) Write down what the left multiplication operator of y does in D_3. Then write down the corresponding permutation if we label 1 as 1, x as 2, x^2 as 3, y as 4, xy as 5, x^2y as 6.

$L_y : D_3 \to D_3$

$$\begin{array}{rcl} 1 & \mapsto & \underline{y1 = y} \\ x & \mapsto & \underline{yx = x^{-1}y = x^2y} \\ x^2 & \mapsto & \underline{yx^2 = x^{-2}y = xy} \\ y & \mapsto & \underline{yy = 1} \\ xy & \mapsto & \underline{xyy = x^{-1}yy = x^21 = x^2} \\ x^2y & \mapsto & \underline{yx^2y = x^{-2}yy = x1 = x} \end{array}$$

$L_y : \{1, 2, \ldots, 6\} \to \{1, 2, \ldots, 6\}$

$$\begin{array}{rcl} 1 & \mapsto & 4 \\ 2 & \mapsto & 6 \\ 3 & \mapsto & 5 \\ 4 & \mapsto & 1 \\ 5 & \mapsto & 3 \\ 6 & \mapsto & 2 \end{array}$$

The corresponding permutation is...?

L_y is represented by (14)(26)(35)

(b) Suppose that using Cayley's theorem we found the left multiplication operator of x in D_4 corresponds to (1234)(5678) and y corresponds to (15)(28)(37)(46). What would the left multiplication operator of x^2y correspond to? [Your answer should be a permutation written as a product of disjoint cycles.]

$x^2y \mapsto [(1234)(5678)]^2(15)(28)(37)(46) = (13)(24)(57)(68)\,(15)(28)(37)(46) = \boxed{(17)(26)(35)(48)}$

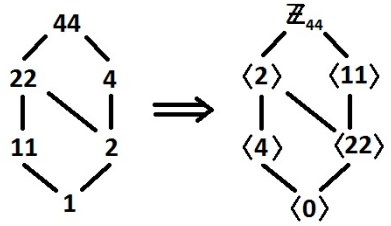
Now write your answer as a product of transpositions. Is this permutation even or odd?

It's already written as a product of transpositions: (17)(26)(35)(48). There are 4 transpositions, so this permutation is even.

4. (25 points) Mod stuff.

(a) Draw the subgroup lattice of $\mathbb{Z}_{44}$. *Note:* $44 = 2^2 \cdot 11$.

First, note that the divisors of 44 are 1, 2, 4, 11, 22, and 44. We first write the lattice of divisors, then make the corresponding lattice of subgroups.



(b) List the possible orders of elements in $\mathbb{Z}_{44}$. Then determine the number of elements of each order.

Order =	1	2	4	11	22	44
Number of elements =	1	1	2	10	10	20

Briefly, this is because there is only 1 element of order 1 (the identity) in any group and then $2 - 1 = 1$, $4 - 1 - 1 = 2$, $11 - 1 = 10$, $22 - 1 - 1 - 10 = 10$, and $44 - 1 - 1 - 2 - 10 - 10 = 20$.

A bit more detail, consider for example the divisor 22: $\mathbb{Z}_{44}$ is a cyclic group. Thus every subgroup is cyclic and also there is a unique subgroup of every order dividing 44. Thus there is exactly 1 subgroup of order 22. Any element of order 22 must generate a subgroup of order 22, so (since there is only 1 subgroup of order 22) all elements of order 22 must belong to this *unique* subgroup. Next, because 1, 2, and 11 divide 22 and this subgroup is cyclic, it must have elements of orders 1, 2, and 11. Because of uniqueness of subgroups all of the elements of orders 1, 2, and 11 must be in their repective subgroups and thus be contained in the subgroup of order 22. Hence the $1 + 1 + 10 = 12$ elements of orders 1, 2, and 11 belong to the subgroup of order 22. This leaves $22 - 12 = 10$ elements. Since we've exhausted all of the

elements of orders 1, 2, and 11 and orders of elements must divide the order of the subgroup, it must be the case that the remaining 10 elements all have order 22.

(c) Show that $f : \mathbb{Z}_6 \to \mathbb{Z}_4$ defined by $f(x) = 2x$ is a **well-defined** homomorphism.

Suppose $x = y$ in $\mathbb{Z}_6$. Therefore, there exits some $k \in \mathbb{Z}$ such that $x = y + 6k$. Thus $2x = 2y + 12k$. Therefore, $2x = 2y + 4(3k)$ so that $2x = 2y$ in $\mathbb{Z}_4$. Thus $f(x) = f(y)$. So f is well-defined (equal inputs give equal outputs).

$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$ thus f is a homomorphism.

To do the next part it is convenient to compute all of the values of f:

$f(0) = 0$, $f(1) = 2$, $f(2) = 4 = 0$, $f(3) = 6 = 2$, $f(4) = 8 = 0$, $f(5) = 10 = 2$. Thus $\{0, 2, 4\} = \langle 2 \rangle$ map to 0 and $\{0, 2\} = \langle 2 \rangle$ are the only elements in the range.

(d) $\text{Ker}(f) = \underline{\{0, 2, 4\}}$

$f(\mathbb{Z}_6) = \underline{\{0, 2\}}$

Is f 1-1? No, the kernel contains more than just the identity [OR: No, $f(1) = 2 = f(3)$ but $1 \neq 3$].

Is f onto? No, the image (i.e. range) is not all of $\mathbb{Z}_4$ [OR: No, 1 is not in the range].

Is f an isomorphism? No, φ is not one-to-one and onto – in fact – it's not one-to-one and it's not onto!

5. (20 points) POOF! ...I mean... PROOFS! [No magic please.]

(a) Let G be a group and let $a, b \in G$ such that $(ab)^2 = a^2b^2$. Show that $ab = ba$.

$(ab)^2 = a^2b^2 \implies abab = aabb \implies a^{-1}abab = a^{-1}aabb \implies bab = abb \implies babb^{-1} = abbb^{-1} \implies ba = ab$

(b) Let G be a group and let $g \in G$. Define the map $\varphi : G \to G$ by $\varphi(x) = gxg^{-1}$.
Prove that φ is an isomorphism.

Suppose $x, y \in G$. Then $\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y)$. Thus φ is a homomorphism.

Suppose $x \in G$ and $\varphi(x) = e$. Thus $gxg^{-1} = e$ so that $g^{-1}gxg^{-1}g = g^{-1}eg$. Therefore, $x = e$. This shows that $\text{Ker}(\varphi) = \{e\}$ and so φ is one-to-one. [Alternatively, we could have shown $\varphi(x) = \varphi(y) \implies gxg^{-1} = gyg^{-1} \implies \cdots \implies x = y$].

Supose $y \in G$. [Scratch work: $\varphi(x) = y$ so that $gxg^{-1} = y$ and so $x = g^{-1}yg$] Then $\varphi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = gg^{-1}ygg^{-1} = y$. Thus φ is onto.

Thus φ is an isormorphism [Actually, this is an automorphism since both the domain and codomain of φ are G].

Note: As an alternative to showing φ is one-to-one and onto, we could have shown that the map: $\psi(x) = g^{-1}xg$ is the inverse of φ: $\psi(\varphi(x)) = \psi(gxg^{-1}) = g^{-1}gxg^{-1}g = x$ and $\varphi(\psi(x)) = \varphi(g^{-1}xg) = gg^{-1}xgg^{-1} = x$. Since φ has an inverse it must be bijective (i.e. one-to-one and onto).

(c) Let G and G' be groups and let $\psi : G \to G'$ be a homomorphism. Suppose that G is cyclic. Show that $\psi(G)$ is abelian. [Extra Credit: Show that $\psi(G)$ is cyclic.]

Proof #1: Since G is cyclic, it is abelian. Suppose $x, y \in \psi(G)$. Then there exists $a, b \in G$ such that $\psi(a) = x$ and $\psi(b) = y$. $xy = \psi(a)\psi(b) = \psi(ab) = \psi(ba) = \psi(b)\psi(a) = yx$ where the middle equality holds because $ab = ba$ (since G is abelian). Therefore, $\psi(G)$ is abelian.

Proof #2: Since G is cyclic, there exists some $g \in G$ such that $G = \langle g \rangle$. We will show that $\psi(g)$ generates $\psi(G)$. First, $\psi(g)^k = \psi(g^k) \in \psi(G)$ for all $k \in \mathbb{Z}$. Thus $\langle \psi(g) \rangle \subseteq \psi(G)$. Next, suppose $y \in \psi(G)$. Then there exists some $x \in G$ such that $\psi(x) = y$. But $x \in G = \langle g \rangle$ so there exists some $\ell \in \mathbb{Z}$ such that $x = g^\ell$. Therefore, $y = \psi(x) = \psi(g^\ell) = \psi(g)^\ell \in \langle \psi(g) \rangle$. Therefore, $\psi(G) \subseteq \langle \psi(g) \rangle$. Thus we have shown $\psi(G) = \langle \psi(g) \rangle$ so that $\psi(g)$ generates $\psi(G)$. Therefore, $\psi(G)$ is cyclic [Extra Credit!]. Since $\psi(G)$ is cyclic, it is also abelian.