Math 3110 **Midterm Exam — In Class** **October 14th, 2013**

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

1. (12 points) Basics

(a) Let $S = (0, 1] = \{x \mid 0 < x \leq 1\}$. Then S is **not** a group under multiplication. List the group axioms which hold and then using **concrete** counterexamples, show the other axioms fail.

Axioms that hold:

- Closure: It is true that if $0 < x, y \leq 1$, then $0 < xy \leq 1$ (positive times positive is positive & a number of magnitude less than 1 scaled by a number of magnitude less than 1 will have an even smaller magnitude – less than 1).
- Associativity: Real multiplication is associative. Since this works for *all* real numbers, it certainly holds for *some* real numbers (i.e. those in S).
- Identity: We know that 1 is the multiplicative identity (so it acts as a multiplicative identity on S). Notice that in fact $1 \in S$ since $0 < 1 \leq 1$.

Axioms that fail:

- Inverses – counter-example: $0.5 \in S$ but $0.5^{-1} = 2 \notin S$ since $2 > 1$.
  Notice that given $x \in S$, $x^{-1} = 1/x$ does in fact exist (as a real number). However, we do not necessarily have $1/x < 1$. In other words, the inverse *exists* in some sense, but it does not necessarily belong to our set. In fact, for $1 \neq x \in S$, x^{-1} is never in S – any element of S other than 1 gives a counter-example!

(b) Let $\mathbb{E}$ be the set of even integers. Show $\mathbb{E}$ is a subgroup of $\mathbb{Z}$ using a subgroup test.

First, recall that x is *even* if and only if there is some integer k such that $x = 2k$. Also, keep in mind that the group operation here is *addition* – the integers are an abelian (in fact, cyclic) group under addition. The integers do *not* form a group under multiplication ($2^{-1} = 1/2 \notin \mathbb{Z}$). We'll just run the standard subgroup test:

Non-empty 0 is even since $0 = 2 \cdot 0$, so $\mathbb{E} \neq \emptyset$.

Closure Let $x, y \in \mathbb{E}$, so $x = 2k$ and $y = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Therefore, $x + y = 2k + 2\ell = 2(k + \ell) \in \mathbb{E}$ since $k + \ell \in \mathbb{Z}$.

Inverses Let $x \in \mathbb{E}$, so $x = 2k$ for some $k \in \mathbb{Z}$. Therefore, $-x = -2k = 2(-k) \in \mathbb{E}$ since $-k \in \mathbb{Z}$.

Or more briefly (using just words): The even integers form a subgroup of the integers because it is a non-empty set, even plus even is even, and the negative of an even number is an even number.

2. (14 points) Cyclic Stuff

(a) Let G be a finite group and $g \in G$. Suppose that $|g| = 30$.

i. What is the order of g^{25}? List the distinct elements in $\langle g^{25} \rangle$.

Keep in mind that since $|g| = 30$, the exponents of g work "mod 30". One approach here is to go by brute force: $(g^{25})^1 = g^{25}$, $(g^{25})^2 = g^{25+25} = g^{20}$, $(g^{25})^3 = (g^{25})^2 g^{25} = g^{20+25} = g^{45} = g^{15}$, $(g^{25})^4 = (g^{25})^3 g^{25} = g^{15+25} = g^{40} = g^{10}$, $(g^{25})^5 = (g^{25})^4 g^{25} = g^{10+25} = g^{35} = g^5$, and $(g^{25})^6 = (g^{25})^5 g^{25} = g^{5+25} = g^{30} = e$ (we've looped back to the identity). [You might notice the powers counting down by 5. This is because $g^{25} = g^{-5}$.] Therefore, $\langle g^{25} \rangle = \{g^{25}, g^{20}, g^{15}, g^{10}, g^5, e\}$.

Alternatively, we know that $|g^{25}| = \dfrac{|g|}{\gcd(25, |g|)} = \dfrac{30}{\gcd(25, 30)} = \dfrac{30}{5} = 6$. Thus g^{25} generates *the* cyclic subgroup of order 6 in $\langle g \rangle$. This subgroup is also generated by $g^{30/6} = g^5$. Therefore, $\langle g^{25} \rangle = \langle g^5 \rangle = \{e, g^5, g^{10}, g^{15}, g^{20}, g^{25}\rangle$. In general, $\langle g^k \rangle = \langle g^{30/\gcd(30,k)} \rangle$.

Answer: $\langle g^{25} \rangle = \langle g^5 \rangle = \{e, g^5, g^{10}, g^{15}, g^{20}, g^{25}\rangle$

ii. Is $g^{904} \in \langle g^{25} \rangle$? **Yes** / **No**

Keep in mind that exponents work "mod 30" since $|g| = 30$. Therefore, $g^{904} = g^4$ because $904 = 4 + 900 = 4 +$ (a multiple of 30). But $g^{904} = g^4 \notin \langle g^{25} \rangle$.

(b) How many elements of order 4 does $\mathbb{Z}_{100}$ have? What are they?

$\mathbb{Z}_{100}$ is a cyclic group of order 100. Since it is cyclic, it has a *unique* subgroup of order k for each k dividing 100. Any element of order 4, generates a subgroup of order 4. Therefore, all of the elements of order 4 must live in the unique subgroup of order 4.

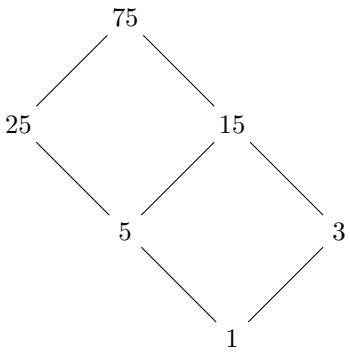
Specifically, $100/4 = 25$ has order 4. We know (by the paragraph above) that all of the elements of order 4 must reside in $\langle 25 \rangle = \{0, 25, 50, 75\}$. Among these elements only 25 and 75 have order 4, so there are exactly 2 elements of order 4 in $\mathbb{Z}_{100}$.

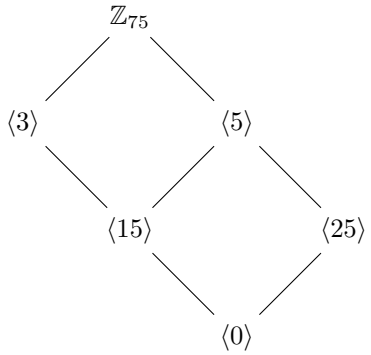
Note: Subgroups of cyclic groups are themselves cyclic and all cyclic groups of the same order are isomorphic. Thus a cyclic group whose order is divisible by 4, must have exactly ONE subgroup of order 4 which is itself cyclic and thus isomorphic to the cyclic group $\mathbb{Z}_4$. Now $\mathbb{Z}_4$ has 2 elements of order 4 (i.e. 1 and 3). Thus *any* cyclic group whose order is divisible by 4, must have exactly 2 elements of order 4.

Answer: There are 2 elements of order 4 in $\mathbb{Z}_{100}$. They are 25 and 75.

(c) Draw the subgroup lattice for $\mathbb{Z}_{75}$. [*Note:* $75 = 3 \cdot 5^2$.]

Keep in mind that the divisors of 75 are 1, 3, 5, 15, 25, and 75. Also, it is helpful to write out a "divisibility lattice" picturing how the divisors of 75 "fit into" each other.





3. (13 points) Permutations

(a) What is the order of $\sigma = (142)(235)(13)(25)$?

Warning: We cannot simply compute $\text{lcm}(3, 3, 2, 2) = 6$ since σ in the problem statement above is not written as a product of *disjoint* cycles. First we need to "simplify" σ.

$\sigma = (15342)$ so $|\sigma| = 5$

(b) Let $\sigma = (134)(24)(12)$. Find σ^{-1}.

$\sigma = (234)$ so $\sigma^{-1} = (432) = (243)$. Alternatively, $\sigma^{-1} = (21)(42)(431) = (243)$.

(c) Write $\sigma = (1572)(2345)(12)$ as a product of transpositions. σ is **Even** / **Odd**

$\sigma = (12)(17)(15)(25)(24)(23)(12)$ or alternatively $\sigma = (134725) = (15)(12)(17)(14)(13)$ – of course there are many other possible correct answers. In any case, there are an odd number of transpositions, so σ is odd.

(d) Let $\sigma = (12345)(67)$. Compute σ^{995}.

Notice that σ is written as a product of disjoint cycles, so since disjoint cycles commute, we have: $\sigma^{995} = ((12345)(67))^{995} = (12345)^{995}(67)^{995} = (12345)^0(67)^1 = \boxed{(67)}$ since $95 \equiv 0 \bmod |(12345)| = 5$ and $95 \equiv 1 \bmod |(67)| = 2$.

(e) Does S_9 have an element of order 14? If so, give an example. If not, explain why not.

We need to cook up an element whose lengths of (disjoint) cycles have least common multiple 14. To get 14 we could use 2 and 7. Helpfully, $2 + 7 = 9$ so there is enough "room" in S_9 to cook up such a permutation.

Answer: Yes, for example, $(1234567)(89)$ has order $\text{lcm}(7, 2) = 14$.

4. (12 points) Explain why the following pairs of groups are not isomorphic.

(a) $\mathrm{GL}_2(\mathbb{R}) \ncong \mathbb{C}$

The simplest way to see these groups are not isomorphic is to note that $\boxed{\mathrm{GL}_2(\mathbb{R}) \text{ is not abelian}}$ (2×2 matrix multiplication is not commutative) while $\boxed{\mathbb{C} \text{ is abelian}}$ (complex multiplication is commutative).

Note: These groups cannot be distinguished by sizes (both are uncountably infinite with cardinalities equal to that of the real numbers), cyclic (both are not cyclic), or element orders (both have elements of all possible orders – finite and infinite).

(b) $U(8) \ncong \mathbb{Z}_4$

Both of these groups are abelian groups of order 4. However, $\boxed{U(8) = \{1,3,5,7\} \text{ is not cyclic}}$ ($|1| = 1$ and $|3| = |5| = |7| = 2$) while $\boxed{\mathbb{Z}_4 \text{ is cyclic}}$. Equivalently, $U(8)$ has no elements of order 4 while $\mathbb{Z}_4$ has 2 elements of order 4. Or alternatively, $U(8)$ has 3 elements of order 2 while $\mathbb{Z}_4$ only has 1 element of order 2.

Note: $U(8)$ is a group under multiplication mod 8 and $\mathbb{Z}_4$ is a group under addition mod 4. From this alone we **cannot** conclude that they fail to be isomorphic. We can have groups with all sorts of different operations be isomorphic. When it comes to isomorphism, the type of operation is not important. Instead the *group* properties of the operation matter – "addition" and "multiplication" are themselves not group properties. They are more or less just different types of notations.

(c) $A_4 \ncong D_6$

Notice that $|A_4| = 4!/2 = 12$ and $|D_6| = 2 \cdot 6 = 12$. So these are both non-abelian groups of order 12 (no help here). However, D_6 has elements of order 6 (for example the rotation of $360/6 = 60°$) while A_4 has no elements of order 6. Alternatively, D_6 has 7 elements of order 2 (the 180° rotation plus all 6 reflections) while A_4 only has 3 elements of order 2 (specifically (12)(34), (13)(24), and (14)(23)). Or D_6 has 2 elements of order 3 while A_4 has 8 elements of order 3. Anyone of these mismatched properties will do.

5. (12 points) Prove that the following pairs of groups are isomorphic.

(a) $U(5) \cong \mathbb{Z}_4$

$U(5) = \{1,2,3,4\}$. Notice that $\langle 2 \rangle = \{1, 2, 2^2, 2^3, \dots\} = \{1,2,4,3\} = U(5)$. Therefore, $U(5)$ is cyclic. Hence $U(5) \cong \mathbb{Z}_4$ since they are both cyclic groups of order 4 and any 2 cyclic groups of the same order are isomorphic.

(b) Consider $\mathbb{R}_{>0}$ (positive reals under multiplication) and $\mathbb{R}$ (under addition). Show $\mathbb{R}_{>0} \cong \mathbb{R}$.
[*Hint:* Consider $\varphi(x) = \ln(x)$.]

Consider $\varphi : \mathbb{R}_{>0} \to \mathbb{R}$ defined by $\varphi(x) = \ln(x)$. Notice that $\varphi(xy) = \ln(xy) = \ln(x) + \ln(y) = \varphi(x) + \varphi(y)$ so φ is a homomorphism. Next, $e^{\ln(x)} = x$ for any $x > 0$ and $\ln(e^x) = x$ for any x. Therefore, $\varphi^{-1}(x)$ exists (we have $\varphi^{-1}(x) = e^x$). Therefore, $\varphi(x)$ is a bijection (1-1 and onto) so φ is an isomorphism and thus $\mathbb{R}_{>0} \cong \mathbb{R}$.

If you prefer to show φ is 1-1 and onto separately, that is fine as well. Such arguments would go something like: Suppose $\varphi(x) = \varphi(y)$ so that $\ln(x) = \ln(y)$ and so $x = e^{\ln(x)} = e^{\ln(y)} = y$. Therefore, injective (i.e. 1-1). Next, suppose that $y \in \mathbb{R}$. Then consider $e^y \in \mathbb{R}$. Note that $e^y > 0$ so $e^y \in \mathbb{R}_{>0}$ and $\varphi(e^y) = \ln(e^y) = y$. Therefore, surjective (i.e. onto).

- This portion of the exam must be turned in **no later** than 4:30pm on Wednesday, October 16th, 2013.
- You may use notes, textbooks, and existent online resources to complete these problem.
- You may **not** ask anyone (except me and Dr. Vicky Klima) for help.

6. (5 points) Explain why $111 \in U(997)$. Then compute 111^{-1}.

We run the Euclidean algorithm: $997 = 111 \cdot 8 + 109$ then $111 = 109 \cdot 1 + 2$ then $109 = 2 \cdot 54 + 1$ then $2 = 1 \cdot 2 + 0$. Thus $\gcd(997, 111) = 1$ which means that $111 \in U(997)$.

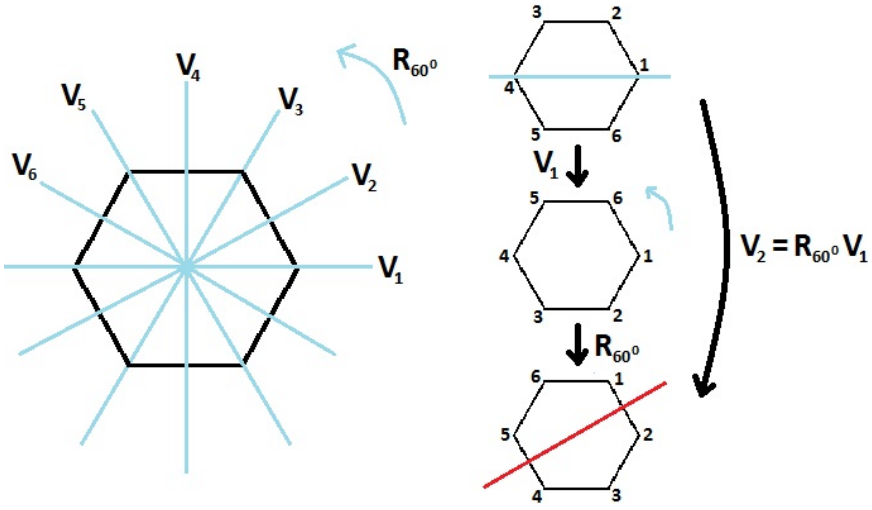
Next, we use the information from the Euclidean algorithm to cook up an inverse. Working backwards:

- $1 = 109 + (-54)2$
- $2 = 111 + (-1)109$ so $1 = 109 + (-54)[111 + (-1)109]$ and so $1 = (55)109 + (-54)111$.
- $109 = 997 + (-8)111$ so $1 = (55)[997 + (-8)111] + (-54)111$ and so $1 = (-494)111 + (55)997$

Therefore, we have found that $111(-494) \equiv 1 \bmod 997$. Therefore, $111^{-1} = -494 = \boxed{503} \pmod{997}$.

7. (9 points) Dihedral Problem.

(a) Draw a regular hexagon and label the reflective symmetries: $V_1, V_2, \ldots, V_6$ (moving around the hexagon in the counter-clockwise direction). Also, let R_{60° be the counter-clockwise rotation of 60°. Draw a few pictures to compute $R_{60^\circ} V_1$.



(b) Recall that $D_{10} = \langle x, y \mid x^{10} = 1, y^2 = 1, (xy)^2 = 1 \rangle = \{1, x, x^2, \ldots, x^9, y, xy, x^2y, \ldots, x^9y\}$.

Simplify $\alpha = x^4yx^2x^{-3}y^3xy^{-7}$.

Remember that $1 = xyxy$ and so $(1)yx^{-1} = (xyxy)yx^{-1}$ so $yx^{-1} = xyxy^2x^{-1} = xyxx^{-1} = xy$. Likewise $yx = x^{-1}y$.

$\alpha = x^4yx^2x^{-3}y^3xy^{-7} = x^4yx^{2-3}yxy = x^4yx^{-1}x^{-1}yy = x^4yx^{-2} = x^4x^2y = \boxed{x^6y}$

(c) Make a table listing the orders of the elements of D_{24} as well as how many elements there are of each order.

Recall that D_{24} has 24 reflections (these have order 2) and then the rotations form a cyclic subgroup of order 24. Thus the subgroup of rotations contributes the number of elements of various orders appearing in $\mathbb{Z}_{24}$.

In turn $\mathbb{Z}_{24}$ has elements of orders 1, 2, 3, 4, 6, 8, 12, 24 (the divisors of 24). We count these as follows (this follows from property that cyclic groups have a unique subgroup of order k for each divisor k): There is 1 identity (element of order 1). In the subgroup of order 2 we have the identity and then everything else must have order 2 – that is – there are $2 - 1 = 1$ elements of order 2. Next, consider 4. There are elements of orders 1, 2, and 4 in the unique subgroup of order 4. We already know there is 1 element of order 1 and 1 of order 2. Thus the remaining $4 - 1 - 1 = 2$ elements have order 4. Next, consider 8. Here we knock out the elements of orders 1, 2, and 4. This leaves $8 - 1 - 1 - 2 = 4$ elements of order 8. etc.

In $\mathbb{Z}_{24}$ we have...

order	1	2	3	4	6	8	12	24
number of elements	1	1	2	2	2	4	4	8

Therefore, in D_{24} (add in the reflections) we have...

order	1	2	3	4	6	8	12	24
number of elements	1	25	2	2	2	4	4	8

8. (8 points) Show x and gxg^{-1} have the same order (in a finite group). Can $x = gxg^{-1}$? If so, what does this say about g and x? If not, why not?

Note: $gx^0g^{-1} = geg^{-1} = gg^{-1} = e = (gxg^{-1})^0$. Suppose that $gx^kg^{-1} = (gxg^{-1})^k$. Then $gx^{k+1}g^{-1} = gx^kxg^{-1} = gx^kg^{-1}gxg^{-1} = (gxg^{-1})^kgxg^{-1} = (gxg^{-1})^{k+1}$. Thus by induction $gx^kg^{-1} = (gxg^{-1})^k$ for all $k = 0, 1, 2, \ldots$. Also, suppose that $gx^kg^{-1} = (gxg^{-1})^k$. Then $gx^{k-1}g^{-1} = gx^kx^{-1}g^{-1} = gx^kg^{-1}gx^{-1}g^{-1} = (gxg^{-1})^k(gxg^{-1})^{-1} = (gxg^{-1})^{k-1}$. Thus by induction $gx^kg^{-1} = (gxg^{-1})^k$ for all $k = 0, -1, -2, \ldots$. Hence $gx^kg^{-1} = (gxg^{-1})^k$ for all $k \in \mathbb{Z}$.

With that fact out of the way (which we might have taken for granted). Notice that $x^n = e$ iff $gx^ng^{-1} = gg^{-1} = e$ iff $(gxg^{-1})^n = e$. Therefore, any power which sends x to the identity will send gxg^{-1} to the identity as well and vice-versa. Therefore, these elements must have the same order.

Next, can $x = gxg^{-1}$ happen? Sure. This simply means that $xg = gxg^{-1}g = gx$. That is $x = gxg^{-1}$ iff $xg = gx$ (i.e. the conjugate of x by g is x itself if and only if x and g commute).

9. (5 points) Suppose that $\sigma = (13)(24765)$ and your classmate claims that $\tau\sigma\tau^{-1} = (142)(3765)$. Is this possible? If so, what might τ be? If not, why not?

This is **not possible**. Why? Recall that conjugation preserves *cycle structure*. Notice that $(13)(24765)$ is the product of a transposition and a 5-cycle (disjoint product) while $(142)(3765)$ is the product of a 3-cycle and a 4-cycle (again disjoint product). These permutations cannot be conjugates because their cycle structures don't match.

10. (10 points) Matrices.

(a) Let $H = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \text{ and } a, b \text{ not both } 0 \right\}$.

Using a subgroup test, show that H is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Certainly, H is non-empty. Consider $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in H$. Then $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \in H$ [if both $ac - bd = 0$ and $ad + bc = 0$ then $(ac - bd)(ac - bd) - (ad + bc)(-(ad + bc)) = (ac-bd)^2 + (ad+bc)^2 = (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = 0$. But this can only happen if $a = b = 0$ or if $c = d = 0$ which contradicts the matrices belonging to H.]

Next, notice that $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} X & Y \\ -Y & X \end{bmatrix} \in H$ where $X = a/(a^2 + b^2)$ and $Y = -b/(a^2 + b^2)$ [since not both a and b zero implies that $a^2 + b^2 \neq 0$ and that not both $X = a/(a^2 + b^2)$ and $Y = -b/(a^2 + b^2)$ are zero.]

(b) Prove that $\mathbb{C}_{\neq 0} = \{x + yi \mid x, y \in \mathbb{R} \text{ and } x, y \text{ not both } 0\} \cong H$

Let $\varphi : \mathbb{C}_{\neq 0} \to H$ be defined by $\varphi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. This is obviously a bijection. We can see that its inverse is $\varphi^{-1}\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + bi$ because

$$\varphi\left(\varphi^{-1}\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right)\right) = \varphi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \text{ and } \varphi^{-1}(\varphi(a + bi)) = \varphi^{-1}\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + bi.$$

We need to check that it is also a homomorphism: $\varphi(a + bi)\varphi(c + di) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} = \varphi((ac - bd) + (ad + bc)i) = \varphi((a + bi)(c + di))$. Therefore, φ is an isomorphism. Thus we have that $\mathbb{C}_{\neq 0} \cong H$.