Math 3110 **Test #1** **February 9th, 2022**

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

1. (20 points) Definition and Basics

(a) Suppose that G is a non-empty set equipped an operation. What 4 things do I need to check to see if G is a group?

1: Closure: $\forall x, y \in G$, we have $xy \in G$
2: Associativity: $\forall x, y, z \in G$, we have $(xy)z = x(yz)$
3: Identity: $\exists e \in G$ such that $\forall x \in G$, $xe = x = ex$
4: Inverses: $\forall x \in G$, $\exists y \in G$ such that $xy = e = yx$

What additional property needs to hold for G to be an **Abelian** group?

5: Commutivity: $\forall x, y \in G$, $xy = yx$

(b) The closed interval $I = [-1, 1] = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ does not form a group under addition. Why? **[BE CONCRETE.]**

While associativity, identity (i.e., 0), and inverses (i.e., negations) all seem to check out, the real problem is that we lack closure. Notice that $1 \in I$ but $1 + 1 = 2 \notin I$. Thus I is not a group under addition because addition is not closed.

(c) This same interval $I = [-1, 1]$ does not form a group under multiplication either. Why? **[BE CONCRETE.]**

Now closure is ok here. Associativity and identity (i.e., 1) also check out. However, inverses give us problems. For example, $0^{-1} = 1/0$ just doesn't exist! Even discarding 0, we still have a problem. Notice that $(1/2)^{-1} = 2 \notin I$, so I is not closed under taking inverses. In any case, this is not a group because we lack closure under (multiplicative) inverses.

(d) Equip $\mathbb{Q}_{\neq 0}$ (the non-zero rational numbers) with the operation of **division**. Is 1 an identity for this set equipped with this operation? Why or why not? **[BE CONCRETE.]**

Once again we fail to have a group. In fact, associativity fails: $1/(2/3) = 3/2$ whereas $(1/2)/3 = 1/6$. However, we are being asked about the identity axiom. Notice that $x/1 = x$ for all $x \in \mathbb{Q}_{\neq 0}$ so 1 is a right identity. However, $1/x \neq x$ unless $x = \pm 1$. In particular, $1/2 \neq 2$. Therefore, 1 is a right identity but it is not a left identity. Thus 1 is not a (two-sided) identity for division.

2. (20 points) Arithmetic mod 12. *Note:* The positive integers divisors of 12 are 1, 2, 3, 4, 6, and 12.

(a) Make a list of all of the cyclic subgroups of $\mathbb{Z}_{12}$ along with their contents (for example: $\langle 0 \rangle = \{0\}$).

As discussed in class, we have one subgroup per divisor of 12. Since there are 6 divisors, we will have 6 distinct (cyclic) subgroups. Although, we were not asked to, I will provide each distinct subgroup *and* display *all* generators.

- $\langle 0 \rangle = \{0\}$
- $\langle 6 \rangle = \{0, 6\}$
- $\langle 4 \rangle = \{0, 4, 8\}$ $(= \langle 8 \rangle)$
- $\langle 3 \rangle = \{0, 3, 6, 9\}$ $(= \langle 9 \rangle)$
- $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ $(= \langle 10 \rangle)$
- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ $(= \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle)$

(b) Fill out the following table referring to the operations of addition and multiplication modulo 12:

Note: Just put an **X** if something is undefined / does not exist.

Element $x =$	0	1	2	3	4	5	6	7	8	9	10	11
Additive Inverse $-x =$	0	11	10	9	8	7	6	5	4	3	2	1
Order (in $\mathbb{Z}_{12}$) $\lvert x \rvert =$	1	12	6	4	3	12	2	12	3	4	6	12
Multiplicative Inverse $x^{-1} =$	**X**	1	**X**	**X**	**X**	5	**X**	7	**X**	**X**	**X**	11
Order (in $U(12)$) $\lvert x \rvert =$	**X**	1	**X**	**X**	**X**	2	**X**	2	**X**	**X**	**X**	2

(c) Compute $5^{-2}(1-4)+8 \bmod 12$ or explain why this is undefined.

Notice that $5^{-1}=5$ and so $5^{-2}=(5^{-1})^2=5^2=1$. Thus $5^{-2}(1-4)+8=1(-3)+8=\boxed{5}$.

(d) Compute $2^{-5}(1-4)-8 \bmod 12$ or explain why this is undefined.

Notice that 2^{-1} does not exist (since $\gcd(2,12)=2\neq 1$). Thus this is $\boxed{\text{undefined}}$.

3. (20 points) More Modular Arithmetic.

(a) List the elements of $U(9)=\{x\in\mathbb{Z}_9 \mid \gcd(x,9)=1\}=\{1,2,4,5,7,8\}$

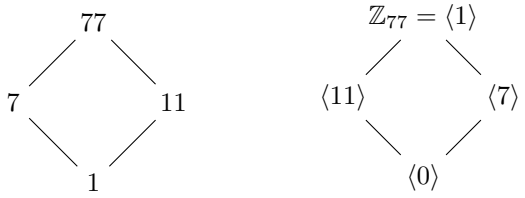
Notice that $1^1=1$; $2^1=2$, $2^2=4$, $2^3=8$, $2^4=7$, $2^5=5$, $2^6=1$; $4^1=4$, $4^2=7$, $4^3=1$; $5^1=5$, $5^2=7$, $5^3=8$, $5^4=4$, $5^5=2$, $5^6=1$; $7^1=7$, $7^2=4$, $7^3=1$; $8^1=8$, $8^2=1$. Of course, we could save time by noting that the identity (i.e., 1) always has order 1; inverses have the same order $6=|2|=|2^{-1}|=|5|$ and $3=|4|=|4^{-1}|=|7|$; Arithmetic is easier when we swap out for smaller representatives like $8=-1$ so $8^2=(-1)^2=1$.

List each element's order: $\underline{|1|=1,\ |2|=6,\ |4|=3,\ |5|=6,\ |7|=3,\text{ and }|8|=2}$

Is $U(9)$ cyclic (circle the correct answer)? $\boxed{\text{Yes}}$ since $\langle 2\rangle=\{1,2,4,8,7,5\}=U(9)$ (also $=\langle 5\rangle$).

Alternatively, we could just note that there are elements of order $|U(9)|=6$, so our group must be cyclic.

(b) Draw the subgroup lattice for $\mathbb{Z}_{77}$. $[77=7\cdot 11]$



(c) Find $10^{-1} \bmod 47$ using the extended Euclidean algorithm [Don't just guess and check].

Divide 47 by 10 and get $47=(4)10+7$ so $7=(1)47+(-4)10$. Next, divide 10 by 7 and get $10=(1)7+3$ so $3=(1)10+(-1)7$. Next, divide 7 by 3 and get $7=(2)3+1$ so $1=(1)7+(-2)3$. Finally, divide 3 by 1 and get $3=(3)1+0$. Thus the last non-zero remainder is 1 (i.e., $\gcd(47,10)=1$ so $10^{-1} \bmod 47$ does in fact exist).

Now run through our facts backwards. We have $1=(1)7+(-2)3$. Substitute in $3=(1)10+(-1)7$ for 3 and get $1=(1)7+(-2)[(1)10+(-1)7]=(3)7+(-2)10$. Finally, substitute $7=(1)47+(-4)10$ for 7 and get $1=(3)[(1)47+(-4)10]+(-2)10=(3)47+(-14)10$. Therefore, $10^{-1}=-14=\boxed{33}$ working mod 47.

4. (20 points) Recall $D_n=\{1,x,\ldots,x^{n-1},y,xy,\ldots,x^{n-1}y\}=\langle x,y \mid x^n=1,y^2=1,(xy)^2=1\rangle$.

(a) Use the relations for D_9 to simplify $y^{-3}x^{14}y^{22}x^{-2}yx$.

Keep in mind that exponents of x work mod 9 and exponents of y work mod 2, so we immediately have: $yx^5\cdot 1\cdot x^{-2}yx$. This is $yx^3yx=x^{-3}yyx=x^6y^2x=x^6\cdot 1\cdot x=\boxed{x^7}$.

(b) Fill out the following table for D_4.

Element $g=$	1	x	x^2	x^3	y	xy	x^2y	x^3y
Inverse $g^{-1}=$	1	x^3	x^2	x	y	xy	x^2y	x^3y
Order $\lvert g\rvert=$	1	4	2	4	2	2	2	2

(c) What is $\langle x^8\rangle$ in D_{10}?

Remember that exponents of x work mod 10 in D_{10}. We compute powers of x^8 and find: $(x^8)^2=x^{16}=x^6$, $(x^8)^3=x^{24}=x^4$, $(x^8)^4=x^{32}=x^2$, and $(x^8)^5=x^{40}=1$. Thus $\boxed{\langle x^8\rangle=\{1,x^2,x^4,x^6,x^8\}}$. Alternatively, if we noticed $\langle x^8\rangle=\langle (x^8)^{-1}\rangle=\langle x^2\rangle$ (since elements and their inverses generate the same cyclic subgroup), this would have been an easier computation.

(d) Fill in the following rows of the Cayley table for D_5:

	1	x	x^2	x^3	x^4	y	xy	x^2y	x^3y	x^4y
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x^4	x^4	1	x	x^2	x^3	x^4y	y	xy	x^2y	x^3y
y	y	x^4y	x^3y	x^2y	xy	1	x^4	x^3	x^2	x
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

For example, $x^4 \cdot x^3y = x^7y = x^2y$ since exponents of x work mod 5 in D_5. As another example, $y \cdot x^4 = x^{-4}y = xy$.

(e) Is $H = \{1, y, xy\}$ a subgroup of D_3? Why or why not?

Non-empty *finite* subsets are subgroups if and only if they are closed under the operation. Notice that $xy \cdot y = xy^2 = x \notin H$, so **No**, this is not a subgroup.

5. (20 points) Proofs!

(a) Choose one of the following: Assume G is a group under multiplication with identity 1.

I. Suppose that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Prove that G is Abelian.

Let $a, b \in G$. Then by assumption $(a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1}$. By socks-shoes, the left hand side is $(b^{-1})^{-1}(a^{-1})^{-1}$. Therefore, we have $ba = ab$. Thus G is Abelian.

Alternatively, we could take our assumption: $(ab)^{-1} = a^{-1}b^{-1}$ and multiply it on the left by ab and on the right by ba. This gives us: $(ab)(ab)^{-1}ba = (ab)a^{-1}b^{-1}ba$ so that $1 \cdot ba = aba^{-1} \cdot 1 \cdot a$ so $ba = ab \cdot 1$ and thus $ba = ab$. Therefore, G is Abelian.

II. Suppose that $g \in G$. Prove that $|g| = |g^{-1}|$ (elements and their inverses have the same order).

Notice that $g^n = 1$ if and only if $(g^n)^{-1} = 1^{-1}$ which is $(g^{-1})^n = 1$. Therefore, the same powers n take both g and g^{-1} to the identity. Thus (if there is one) the same smallest positive power takes them back to the identity. Therefore, they have the same order.

Alternatively, $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} = \{g^{-\ell} \quad -\ell \in \mathbb{Z}\} = \{(g^{-1})^\ell \mid \ell \in \mathbb{Z}\} = \langle g^{-1} \rangle$ since a number ranging over all integers means its negation ranges over all integers (and vice-versa). Finally, $|g| = |\langle g \rangle| = |\langle g^{-1} \rangle| = |g^{-1}|$.

(b) Choose one of the following: (You **must** use a subgroup test in your proof.)

I. Let G be an Abelian group. Prove that $H = \{g \in G \mid g^2 = e\}$ is a subgroup of G.

Notice that $e^2 = e$ so $e \in H$ (H is a non-empty subset of G). We check closures. Let $a, b \in H$ so that $a^2 = e$ and $b^2 = e$. Notice $(ab)^2 = abab = aabb = a^2b^2 = ee = e$ (we used commutativity – G is Abelian – to get the second equality). Thus $ab \in H$. Notice that since $a^2 = e$, we have $a^{-1} = a \in H$. [Alternatively, $(a^{-1})^2 = (a^2)^{-1} = e^{-1} = e$. Thus $a^{-1} \in H$.] Therefore, H is closed under the operation and inverses. Thus H is a subgroup of G.

We note that if G is not Abelian, H may fail to be a subgroup. For example, in D_3, H would be the set of reflections. These are not closed under the operation.

II. Prove that $K = \left\{ \begin{bmatrix} a & a \\ 0 & 2b \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$ is a subgroup of $\mathbb{R}^{2\times 2}$.

[*Caution:* What operation makes the set of **all** 2×2 matrices a group?]

Notice that the zero matrix belongs to K so it is non-empty. Also, the zero matrix belongs to $\mathbb{R}^{2\times 2}$. This reminds us that our operation is addition of matrices (not multiplication). Let $A, B \in K$. Say $A = \begin{bmatrix} a & a \\ 0 & 2b \end{bmatrix}$ and $B = \begin{bmatrix} x & x \\ 0 & 2y \end{bmatrix}$ for some $a, b, x, y \in \mathbb{R}$. Then $A + B = \begin{bmatrix} a+x & a+x \\ 0 & 2(b+y) \end{bmatrix} \in K$ (since $a + x, b + y \in \mathbb{R}$ and $A + B$ has the right form to belong to K). Likewise, $-A = \begin{bmatrix} -a & -a \\ 0 & 2(-b) \end{bmatrix} \in K$ (again since $-a, -b \in \mathbb{R}$ and $-A$ has the right form to belong to K). Therefore, K is closed under addition and negation (i.e., inverses). Thus K is a subgroup of $\mathbb{R}^{2\times 2}$.