Math 3110 **Test #1** **February 17th, 2021**

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 positive real numbers $\mathbb{R}_{>0} = \{r \in \mathbb{R} \mid r > 0\}$ do not form a group under division. Why not?

Notice that $1/(2/3) = 3/2$ whereas $(1/2)/3 = 1/6$. Therefore, division is not associative. Thus $\mathbb{R}_{>0}$ does not form a group under division. Alternatively, we could also see that the identity axiom fails: Suppose $x/e = x = e/x$ for all $x \in \mathbb{R}_{\neq 0}$. Then, $x/e = x$ implies $x = ex$ so that $e = 1$. But $1/x \neq x$ for most $x \neq 1$. So there is a right identity but not a two sided identity.

(c) On the other hand, the positive real numbers $\mathbb{R}_{>0} = \{r \in \mathbb{R} \mid r > 0\}$ do form a group if we select the right operation. Which operation turns this collection of numbers into a group: Addition or $\boxed{\text{Multiplication}}$? Then explain why the other operation does not yield a group.

We have that $\mathbb{R}_{>0}$ is a group under multiplication (in fact, an abelian group): positive times positive is positive, multiplication is associative, 1 is a positive number and acts as the multiplicative identity, if $x > 0$ then $x^{-1} > 0$ is too, (and multiplication is commutative). On the other hand, positive real numbers cannot form a group under addition since they lack 0 (the additive identity). Alternatively, we can see that they fail to form a group under addition since the additive inverse of a positive number is a negative number (i.e., they are not closed under inverses).

(d) The non-zero rational numbers $\mathbb{Q}_{\neq 0}$ form a group under multiplication. On the other hand, the (non-zero) irrational numbers $\mathbb{I} = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$ do not. Why?

The irrational numbers do not form a group under multiplication since closure fails: $\sqrt{2} \in \mathbb{I}$, but $(\sqrt{2})^2 = 2 \notin \mathbb{I}$ (i.e., $\sqrt{2}$ is irrational but $(\sqrt{2})^2 = 2$ is rational). Alternatively, they do not form a group since they do not have a multiplicative identity (1 is rational and so $1 \notin \mathbb{I}$).

2. (20 points) Some modular arithmetic.

(a) Make a list of all of the cyclic subgroups of $\mathbb{Z}_{10}$ along with their contents (for example: $\langle 0 \rangle = \{0\}$).

$\boxed{\langle 0 \rangle = \{0\}}$, $\boxed{\langle 1 \rangle = \{0, 1, \ldots, 9\}}$ $(= \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle)$, $\boxed{\langle 2 \rangle = \{0, 2, 4, 6, 8\}}$ $(= \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle)$, and $\boxed{\langle 5 \rangle = \{0, 5\}}$.

(b) Fill out the following table referring to the operations of addition and multiplication modulo 10:

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

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

Briefly, additive inverses are just negatives and additive orders match the sizes the cyclic subgroups found in part (a) or, for example, $4 \neq 0$, $4 + 4 = 8 \neq 0$, $4 + 4 + 4 = 2 \neq 0$, $4 + 4 + 4 + 4 = 6 \neq 0$, but $4 + 4 + 4 + 4 + 4 = 0$ so the additive order of 4 is 5. Only things relatively prime to 10 have a multiplicative inverse. Notice $1 \cdot 1 = 1$, $3 \cdot 7 = 1$, and $9 \cdot 9 = 1$ so $1^{-1} = 1$, $3^{-1} = 7$, $7^{-1} = 3$, and $9^{-1} = 9$. Finally, multiplicative orders are computed by looking at successive powers. For example, $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^3 = 7 \neq 1$, but $3^4 = 1$ so its multiplicative order is 4.

(c) Compute $2^{-1}(3-8)+7 \bmod 10$ or explain why this is undefined.

$\boxed{\text{Undefined}}$ since 2^{-1} does not exist (because $\gcd(2,10)=2\neq 1$).

(d) Compute $3^{-1}(7-3)-11 \bmod 10$ or explain why this is undefined.

$3^{-1}(7-3)-11 = 7(4)-11 = 28-11 = 17 = \boxed{7} \pmod{10}$.

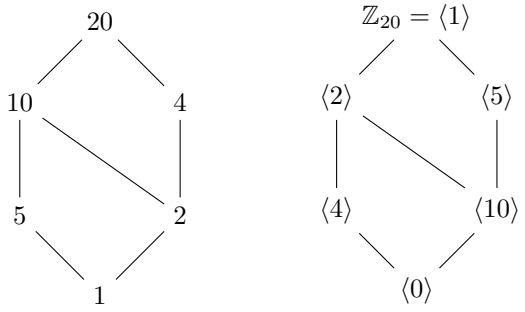
3. (20 points) More Modular Arithmetic.

(a) Write down a Cayley table for $U(8)$. Is $U(8)$ cyclic (circle the correct answer)? Yes / $\boxed{\text{No}}$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(8) = \{k \mid \gcd(k,8)=1\} = \{1,3,5,7\}$ is not cyclic since $\langle 1\rangle = \{1\}$, $\langle 3\rangle = \{1,3\}$, $\langle 5\rangle = \{1,5\}$, and $\langle 7\rangle = \{1,7\}$ (thus nothing generates the whole group).

(b) Draw the subgroup lattice for $\mathbb{Z}_{20}$. $[20 = 2^2 \cdot 5]$



(c) Find $10^{-1} \bmod 77$ using the extended Euclidean algorithm [Don't just guess and check].

Repeated division gives: $77 = (7)10+7$, $10 = (1)7+3$, $7 = (2)3+1$, $3 = (3)1+0$. Thus $\gcd(77,10) = \gcd(10,7) = \gcd(7,3) = \gcd(3,1) = \gcd(1,0) = 1$. We now run the extended portion of the algorithm using our division facts: $(1)7+(-2)3 = 1$, $(1)10+(-1)7 = 3$, and $(1)77+(-7)10 = 7$.

Plugging, $(1)10+(-1)7 = 3$ into 3 in $(1)7+(-2)3 = 1$ yields $(1)7+(-2)[(1)10+(-1)7] = 1$ which gives $(-2)10+(3)7 = 1$. Next, we plug $(1)77+(-7)10 = 7$ into 7 in our previously obtained fact and get $(-2)10+(3)[(1)77+(-7)10] = 1$. Simplifying yields, $(3)77+(-23)10 = 1$. [*Note:* See my Euclidean Algorithm Sage interactive webpage to automate this computation.] Therefore, this equation says $(-23)10 = 1 \pmod{77}$. Thus $10^{-1} = -23 = -23+77 = \boxed{54}$ in $U(77)$.

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_8 to simplify $x^{13}y^3x^{-2}y^{888}x$

Recall that x's exponents work mod 8 and y's exponents work mod 2 – odd powers of y are just y and even powers of y are just the identity $y^0 = 1$. Finally, remember that $yx^\ell = x^{-\ell}y$ and then the computation follows: $x^{13}y^3x^{-2}y^{888}x = x^5yx^61x = x^5yx^7 = x^5x^{-7}y = x^{-2}y = \boxed{x^6y}$

(b) Make a table listing the elements of D_8, their inverses, and their orders.

$g =$	1	x	x^2	x^3	x^4	x^5	x^6	x^7	y	xy	x^2y	x^3y	x^4y	x^5y	x^6y	x^7y
$g^{-1} =$	1	x^7	x^6	x^5	x^4	x^3	x^2	x	y	xy	x^2y	x^3y	x^4y	x^5y	x^6y	x^7y
$\lvert g\rvert =$	1	8	4	8	2	8	4	8	2	2	2	2	2	2	2	2

(c) What is $\langle x^6\rangle$ in D_8?

Notice $(x^6)^1 = x^6$, $(x^6)^2 = x^{12} = x^4$, $(x^6)^3 = x^{18} = x^2$, $(x^6)^4 = x^{24} = 1$ so $\boxed{\langle x^6\rangle = \{1, x^2, x^4, x^6\}}$.

(d) Fill in the following rows of the Cayley table for D_4:

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

(e) Is $H = \{1, y, x^2y\}$ a subgroup of D_4? Why or why not?

No. This is not a subgroup since closure fails. Notice that $x^2y \cdot y = x^2y^2 = x^2 \cdot 1 = x^2 \notin H$.

5. (20 points) Proofs!

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

I. Suppose that $g = g^{-1}$ for all $g \in G$. Prove that G is abelian.

Suppose $a, b \in G$. Then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ where $ab = (ab)^{-1}$, $b^{-1} = b$, and $a^{-1} = a$ follow from our hypothesis that every element is its own inverse and $(ab)^{-1} = b^{-1}a^{-1}$ by the so-called socks shoes principle. Since $ab = ba$ for all $a, b \in G$, we have that G is abelian.

II. Suppose that $G = \langle g \rangle$ is a cyclic group. Prove that G is abelian.

Suppose $a, b \in G = \langle g \rangle$. Then there exists $k, \ell \in \mathbb{Z}$ such that $a = g^k$ and $b = g^\ell$. Therefore, $ab = g^k g^\ell = g^{k+\ell} = g^{\ell+k} = g^\ell g^k = ba$. Thus G is abelian.

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

I. Prove that $H = 8\mathbb{Z} = \{8k \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

That H is a non-empty subset is obvious (8 times an integer is an integer and for example, $0 = 8(0) \in H$). We need to show closure and closure under inverses. Suppose $x, y \in H$. Then there exists $k, \ell \in \mathbb{Z}$ such that $x = 8k$ and $y = 8\ell$. Notice that $x + y = 8k + 8\ell = 8(k + \ell) \in H$ since $k + \ell \in \mathbb{Z}$. Also, $-x = -8k = 8(-k) \in H$ since $-k \in \mathbb{Z}$. Therefore, H is closed under addition and under (additive) inverses. Thus H is a subgroup of $\mathbb{Z}$.
Alternatively, we could have just check closure under subtraction (i.e., the one step test): $x - y = 8k - 8\ell = 8(k - \ell) \in H$ since $k - \ell \in \mathbb{Z}$.

II. Prove that $K = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \;\middle|\; a, b \in \mathbb{R}_{\neq 0} \right\}$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

Let $A \in K$ then $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ where $a, b \in \mathbb{R}_{\neq 0}$. Notice that $\det(A) = ab \neq 0$ since $a, b \neq 0$. Therefore, A is invertible and so $A \in \mathrm{GL}_2(\mathbb{R})$. This shows that K is a subset of $\mathrm{GL}_2(\mathbb{R})$. Obviously, K is not empty. For example, the identity matrix belongs to K.
We need to check if K is closed under matrix multiplication and inverses. Let $A, B \in K$. Then there are $a, b, x, y \in \mathbb{R}_{\neq 0}$ such that $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ and $B = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$. We have that $AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} = \begin{bmatrix} ax & 0 \\ 0 & by \end{bmatrix} \in K$ since $ax \neq 0$ and $by \neq 0$ (and AB is diagonal). Also, $A^{-1} = \begin{bmatrix} 1/a & 0 \\ 0 & 1/b \end{bmatrix} \in K$ since $1/a \neq 0$ and $1/b \neq 0$ (and A^{-1} is diagonal). Therefore, K is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.