MATH 301/601: Spring 2025 **Instructor: Nicholas Vlamis**

Wednesday 3/19/2025 Exam 1 110 minutes

Name: Solutions

Instructions.

1. ***Read each problem carefully.*** Make sure you understand what the problem is asking.
2. Proofs can be informal: use of logical symbols and incomplete sentences **are** permitted. However, make sure all statements and logical steps are clear and correct.
3. You are allowed one 8.5" x 11" sheet of notes, written on the front and back. Your sheet may only contain theorem statements and definitions. You must turn in your note sheet with the exam.
4. No devices other than a writing utensil may be used.
5. Feel free to use the back of any sheet. Just make it clear where I am meant to look for your solutions.

Question	Points	Score
1	3	
2	3	
3	3	
4	6	
5	5	
6	4	
7	5	
8	7	
9	7	
10	7	
11	7	
Total:	50	

Part I: Computation and Understanding

1. 3 points Use the Euclidean algorithm to compute $\gcd(54, 120)$.

$120 = 2 \cdot 54 + 12$

$54 = 4 \cdot 12 + \boxed{6}$

$12 = 2 \cdot 6 + 0$

$\Rightarrow \gcd(54, 120) = 6$

2. 3 points Use the fact that $10^n \equiv (-1)^n \pmod{11}$ for each $n \in \mathbb{N}$ to show that 132539 is divisible by 11.

$132539 \equiv 1 \cdot 10^5 + 3 \cdot 10^4 + 2 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10 + 9$

$\equiv 1 \cdot (-1)^5 + 3(-1)^4 + 2 \cdot (-1)^3 + 5(-1)^2 + 3(-1) + 9$

$\equiv -1 + 3 - 2 + 5 - 3 + 9$

$\equiv 11$

$\equiv 0 \mod 11 \Rightarrow 11 \mid 132539$

3. 3 points List all the subgroups of $\mathbb{Z}_6$ and explain how you know that you have them all.

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_6$

$\langle \bar{2} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$

Every subgroup of a cyclic group is cyclic, so the above list is all subgroups of $\mathbb{Z}_6$.

4. $\boxed{\text{6 points}}$ For each of following pairs of sets and binary operations, give **one reason** why the pair is **not** a group.

   (a) the natural numbers with addition, $(\mathbb{N}, +)$

   There is no identity element.

   $a+b \neq a \quad \forall\, a,b \in \mathbb{N}$

   (b) the integers with subtraction, $(\mathbb{Z}, -)$

   Not associative

   $(1-1)-1 \neq 1-(1-1)$

   (c) the rational numbers with multiplication, $(\mathbb{Q}, \cdot)$

   0 has no inverse, $a \cdot 0 \neq 1 \quad \forall a \in \mathbb{Q}$.

5. $\boxed{\text{5 points}}$ In each of the parts, find the inverse of the element in the specified group.

   (a) $\bar{4}$ in $U(9)$ (Recall that, for $n \in \mathbb{N}$, $U(n) = \{\bar{a} \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ is a group under multiplication modulo n.)

   $\bar{7} = \bar{4}^{-1}$, as $\overline{4 \cdot 7} = \overline{28} = \bar{1}$

   (b) $1 + \sqrt{2}$ in the group $(\mathbb{Q}(\sqrt{2}), +)$, where $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

   $-1-\sqrt{2}$

   (I meant this to be about $(\mathbb{Q}(\sqrt{2}) \setminus \{0\}, \cdot)$. oops!)

6. $\boxed{\text{4 points}}$ In each of the parts, find the order of the element in the specified group. In each case, the order is finite.

(a) $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ in $\mathrm{SL}(2, \mathbb{Z})$.

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \left| \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right| = 4$$

(b) $\overline{5}4$ in $\mathbb{Z}_{120}$ (Your answer from Question 1 should be helpful; the order is too big to find by brute force).

$$|\overline{54}| = \frac{120}{\gcd(54, 120)} = \frac{120}{6} = 20$$

7. $\boxed{\text{5 points}}$ Explain why each of the following groups is **not** cyclic.

(a) $U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

$\langle \overline{1} \rangle = \{\overline{1}\}$

$\langle \overline{3} \rangle = \{\overline{1}, \overline{3}\}$

$\langle \overline{5} \rangle = \{\overline{1}, \overline{5}\}$

$\langle \overline{7} \rangle = \{\overline{1}, \overline{7}\}$

None of these are the whole group, so $U(8)$ is not cyclic.

(b) $(\mathbb{Q}, +)$

Let $p/q \in \mathbb{Q}$. As $\langle p/q \rangle = \langle -p/q \rangle$, we can assume $p/q > 0$.

For $k \in \mathbb{Z}$, either $k \cdot p/q \geq p/q$ or $k \cdot p/q \leq -p/q$.

Therefore, $\langle p/q \rangle \neq \mathbb{Q}$ as $\frac{p}{2q} \notin \langle p/q \rangle$.

Part II: Proofs

Instructions: Complete any three of the following four problems.

8. $\boxed{\text{7 points}}$ Let $n \in \mathbb{N}$ and $a \in \mathbb{Z} \setminus \{0\}$ be relatively prime. Prove that if $b \equiv a \pmod{n}$, then b and n are relatively prime. (****This is an easier version of a homework problem: do not reference any homework exercises in your proof.*)

As $b \equiv a \bmod n$, $n \mid b-a$. So, $\exists\, q \in \mathbb{Z}$ s.t. $b-a = nq$, or $a = b - nq$. If $d \in \mathbb{N}$ s.t. $d \mid b$ and $d \mid n$, then $d \mid (b-nq)$. Hence, $d \mid a$, implying d is a common divisor of a and n. Thus, $d = 1$. $\square$

9. $\boxed{\text{7 points}}$ Let $p, q \in \mathbb{N}$ be prime numbers. Prove that $\mathbb{Z}_{pq}$ has $pq \cancel{-} 3$ generators.

$pq - p - q + 1$ generators

Let $\bar{a} \in \mathbb{Z}_{pq}$. Then $|\bar{a}| \in \{1, p, q, pq\}$, as $|\bar{a}| \mid pq$.

- $|\bar{a}| = 1 \Leftrightarrow \bar{a} = \bar{0}$
- $|\bar{a}| = p \Leftrightarrow \dfrac{pq}{\gcd(a,pq)} = p \Leftrightarrow \gcd(a,pq) = q \Leftrightarrow a = kq$ for some $k \in \mathbb{Z}$.

  so, $|\bar{a}| = p \Leftrightarrow a \in \langle \bar{q} \rangle = \{\bar{0}, \bar{q}, 2\bar{q}, \dots, (p-1)\bar{q}\}$
- Similarly, $|\bar{a}| = q \Leftrightarrow a \in \langle \bar{p} \rangle = \{\bar{0}, \bar{p}, 2\bar{p}, \dots, (q-1)\bar{p}\}$.

Therefore, $\langle \bar{a} \rangle = \mathbb{Z}_{pq} \Leftrightarrow a \notin \langle \bar{p} \rangle \cup \langle \bar{q} \rangle$

$\Rightarrow$ There are $|\mathbb{Z}_{pq}| - |\langle \bar{p} \rangle| - |\langle \bar{q} \rangle| + |\langle \bar{p} \rangle \cap \langle \bar{q} \rangle| = pq - p - q + 1$ generators. $\square$

10. $\boxed{\text{7 points}}$ Let a and b be nonzero integers, and let $d = \gcd(a, b)$. Prove that an integer c is a linear combination of a and b if and only if $d \mid c$.

($\Rightarrow$) If c is a linear combination of a and b, then $\exists\ s, t \in \mathbb{Z}$ so that $c = as + bt$. As $d|a$ and $d|b$, $d|(as+bt)$.

Hence, $d|c$

($\Leftarrow$) As $d = \gcd(a,b)$, $\exists\ s,t \in \mathbb{Z}$ so that $d = as + bt$.

As $d|c$, $\exists\ q \in \mathbb{Z}$ s.t. $c = dq$

$\Rightarrow c = dq = q(as+bt) = a(qs) + b(sq)$

$\Rightarrow c$ is a linear combination of a and b. $\square$

11. $\boxed{\text{7 points}}$ The *center* of a group G, denoted $Z(G)$, is the set

$$Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}.$$

Prove that $Z(G)$ is a subgroup of G.

We need to show $e \in Z(G)$ and that $Z(G)$ is closed under the group operation and inversion.

$\forall\ g \in G$, $eg = ge$, so $e \in Z(G)$.

Now, let $a, b \in Z(G)$. Then $\forall g \in G$,

$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$

$\Rightarrow ab \in Z(G) \Rightarrow Z(G)$ is closed under the group operation.

Finally, let $a \in Z(G)$. Then $\forall g \in G$, $ag^{-1} = g^{-1}a$

$\Rightarrow (ag^{-1})^{-1} = (g^{-1}a)^{-1} \Rightarrow ga^{-1} = a^{-1}g \Rightarrow a^{-1} \in Z(G)$

$\Rightarrow Z(G)$ is closed under inversion. $\square$