MATH3100 Dr. Smith Test # 2, Friday April 4, 2025. Make sure to show all your work. You may not receive full credit if the accompanying work is incomplete or incorrect. If you do scratch work make sure to indicate scratch work - I will not take off points for errors in the scratch work if it is so labeled and will assume that the scratch work is not part of the final answer/proof. **Do 5 of the following 6 problems**; you may do all 6 for extra credit.

1. Let G be a group:

a. Prove that if $g \in G$ then the inverse of g is unique.

Proof. Suppose that $\hat{g}$ is an inverse of the element g. Then

$$\begin{aligned} gg^{-1} &= e \\ g\hat{g} &= e. \end{aligned}$$

So,

$$\begin{aligned} gg^{-1} &= g\hat{g} \\ g^{-1}gg^{-1} &= g^{-1}g\hat{g} \\ eg^{-1} &= e\hat{g} \\ g^{-1} &= \hat{g}. \end{aligned}$$

□

b. Prove that if x, y and z are elements of G, then

$$(xyz)^{-1} = z^{-1}y^{-1}x^{-1}.$$

Proof.

$$\begin{aligned} (xyz)(xyz)^{-1} &= e \\ x^{-1}xyz(xyz)^{-1} &= x^{-1}e \\ eyz(xyz)^{-1} &= x^{-1} \\ y^{-1}yz(xyz)^{-1} &= y^{-1}x^{-1} \\ z^{-1}z(xyz)^{-1} &= z{-}1y^{-1}x^{-1} \\ e(xyz)^{-1} &= z^{-1}y^{-1}x^{-1} \\ (xyz)^{-1} &= z^{-1}y^{-1}x^{-1} \end{aligned}$$

□

2. Consider the multiplication operator for $\mathbb{Z}_7$.

a. Define the multiplication operator $\cdot$ by $[x] \cdot [y] = [xy]$. Prove that $\cdot$ is well defined.

Proof. Most students proved it for n which is fine:

Let

$$\begin{aligned} x \sim a \quad &\text{and} \quad y \sim b \\ a - x = nq \quad &\text{and} \quad b - y = nr \\ a = x + nq \quad &\text{and} \quad b = y + nr. \end{aligned}$$

So

$$\begin{aligned} xy - ab &= xy - (x+nq)(y+nr) \\ &= xy - (xy + nqy + nrx + n^2qr) \\ &= -n(qy + rx + nqr) \\ \therefore ab &\sim xy. \end{aligned}$$

□

b. Construct the multiplication table for $(\mathbb{Z}_7, \cdot_7)$. (Note: use only the integers 0 through 6 in your table.)

Solution. Insert table here.

□

c. Is $Z_7 - \{0\}$ with the operator $\cdot$ a group? Indicate why or why not.

Solution. Yes, because

1. Operation is associative (this follows from the associativity of the integers).

2. Closure: the product of every pair of non-zero elements in the table is in $(\mathbb{Z}_7 - \{0\}, \cdot_7)$.

3. Identity: $[1]_7$ is the identity.

4. Inverse: The identity is in every row and column of $(\mathbb{Z}_7 - \{0\}, \cdot_7)$. □

3. Consider the following element of the permutation group S_5: (13254).

a. Find the subgroup generated by this element.

Solution.

$$\begin{aligned} a &= (13254) \\ a^2 &= (13254)(13254) = (12435) \\ a^3 &= (13254)(12435) = (15342) \\ a^4 &= (13254)(15342) = (14523) \\ a^5 &= e = a^0. \end{aligned}$$

□

b. Show that it is isomorphic to some $\mathbb{Z}_n$.

Solution. It's isomorphic $\mathbb{Z}_5$ with the + operation. I'm willing to accept the observation that they are both cyclic groups of order 5. Or you can give me an isomorphism θ:

$$\theta(a^n) = [n]_5.$$

□

4. Let F be the following function: $F : \mathbb{Z}_{12} \to \mathbb{Z}_6$:

$$F([x]_{12}) = [5x + 2]_6$$

a. Show that F is well defined.

Solution. Suppose $a \sim x$. Then

$$\begin{aligned} x - a &= 12q \\ x &= a + 12q \\ 5x + 2 - (5a + 2) &= 5x - 5a \\ &= 5(a + 12q) - 5a \\ &= 60q = 6(10q) \\ 5x + 2 &= 5a + 2. \end{aligned}$$

So the function is well defined.

□

b. Is F one-to-one? Show why or why not.

Solution. No, because of the pigeon-hole principle: $\mathbb{Z}_{12}$ has more elements than $\mathbb{Z}_6$. □

c. Is F onto? Show why or why not.

Solution. Yes, the easiest way to see this is to list what each element goes to:

$$\begin{array}{ccl} 0 & \to & 2 \\ 1 & \to & 7 = 1 \\ 2 & \to & 12 = 2 \\ 3 & \to & 17 = 5 \\ 4 & \to & 22 = 4 \\ 5 & \to & 27 = 3 \\ 6 & \to & 32 = 2 \\ \vdots & & \end{array}$$

Each element of $\mathbb{Z}_6$ is the image of some element of $\mathbb{Z}_{12}$. Also with the extra row, we show it's not onto. □

d. Is F a homomorphism? Show why or why not.

Solution. No because $F(0) = 2 \neq 0$. □

5. Consider $\mathbb{Z}_n$ with the multiplication operator $\cdot_n$.

a. Argue that $\mathbb{Z}_n$ has a multiplicative identity.

Solution. Since $[x] \cdot [1] = [x]$, then $[1]$ is the multiplicative identity. □

b. Prove that if x and n are relatively prime then $[x]$ has a multiplicative inverse. [Hint: use the theorem about relatively prime numbers stated in class.]

Solution. According to the theorem stated in class, x and n are relatively prime if and only if there are integers p and q so that $1 = xp + nq$. Then:

$$\begin{aligned} 1 &= xp + nq \\ xp &= 1 - nq \\ [xp] &= [1 - nq] \\ [x][p] &= [1] - [n][q] \\ [x][p] &= [1] - [0][q] \\ [x][p] &= [1]. \end{aligned}$$

So $[p]$ is the multiplicative inverse of $[x]$.

□

c. Prove that n and $n - 1$ are relatively prime.

Solution. Again we use the theorem from class:

$$1 = np + (n-1)q,$$

where $p = 1$ and $q = -1$. □

6. Let G be an Abelian group and let $H = \{g^2 | g \in G\}$. Show that H is a subgroup of G.

Solution. Again we use the theorem from class:

1. Associativity: this follows from the associativity G.
2. Closure: if $a = x^2 \in G$ and $b = y^2 \in G$ then

$$\begin{aligned} x^2y^2 &= xxyy \\ &= xyxy \\ &= (xy)^2 \\ \therefore \quad & ab \in G. \end{aligned}$$

Where the Abelian property is used in step 2.

3. Identity: $e^2 = e$ so $e \in G$.

4. Inverse: If $a = x^2 \in G$ then

$$\begin{aligned} a^{-1} &= (x^2)^{-1} \\ &= (x^{-2}) \\ &= (x^{-1})^2. \\ \therefore \quad & a^{-1} \in G. \end{aligned}$$

$\square$