MATH 301/601: Fall 2023 Instructor: Nicholas Vlamis

Wednesday 4/10/2024 Exam 2 110 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	2	
2	4	
3	4	
4	3	
5	6	
6	3	
7	4	
8	3	
9	7	
10	7	
11	7	
12	7	
Total:	50	

Part I: Computation and Understanding

1. $\boxed{\text{2 points}}$ Find the order of $\overline{70}$ in $\mathbb{Z}_{240}$.

$70 = 7 \cdot 10$

$240 = 24 \cdot 10$

$\gcd(70, 240) = 10$

$|\overline{70}| = \frac{240}{\gcd(70,240)} = \frac{240}{10} = 24$

2. $\boxed{\text{4 points}}$ List all the subgroup of $\mathbb{Z}_6$, and explain how you know that you have them all.

$\mathbb{Z}_6$ is cyclic $\Rightarrow$ Every subgroup of $\mathbb{Z}_6$ is cyclic

$\Rightarrow$ every subgroup of $\mathbb{Z}_6$ is of the form $\langle a \rangle$ for some $a \in \mathbb{Z}_6$

$$\Rightarrow \left\{ \begin{array}{l} \langle \bar{0} \rangle = \{0\} \\ \langle \bar{1} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_6 \\ \langle \bar{2} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} \\ \langle \bar{3} \rangle = \{\bar{0}, \bar{3}\} \end{array} \right\} \text{ are all the subgroups of } \mathbb{Z}_6.$$

3. $\boxed{\text{4 points}}$ Recall that $U(n) = \{\bar{a} \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ and is a group when equipped with multiplication modulo n.

(a) Determine if $U(8)$ is cyclic. Explain.

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

$\bar{3}^2 = \bar{9} = \bar{1}$

$\bar{5}^2 = \overline{25} = \bar{1}$ $\Rightarrow U(8)$ not cyclic

$\bar{7}^2 = \overline{49} = \bar{1}$

(b) Determine if $U(10)$ is cyclic. Explain.

$U(10) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

$\bar{3}^2 = \bar{9}$

$\bar{3}^3 = \overline{27} = \bar{7}$ $\Rightarrow U(10) = \langle \bar{3} \rangle$

$\Rightarrow U(10)$ is cyclic.

4. $\boxed{\text{3 points}}$ Find the smallest natural number n for which there exists a group of order n containing an element of order 5 and an element of order 7. Justify your answer.

Let G be a group s.t. $\exists\, a,b \in G$ w/ $|a|=5$, $|b|=7$

$\cdot$ $|a| \mid |G|$ and $|b| \mid |G| \Rightarrow 5 \mid |G|$ and $7 \mid |G|$

$$\left.\begin{array}{l} \Rightarrow 35 \mid |G| \Rightarrow n \geq 35 \\ G = \mathbb{Z}_{35} \text{ is such a group} \Rightarrow n \leq 35 \end{array}\right\} \Rightarrow n = 35.$$

5. $\boxed{\text{6 points}}$ Let $\sigma \in S_7$ be the permutations defined as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 4 & 2 \end{pmatrix}$$

(a) Express σ in cycle notation.

$\sigma = (1\,3)(2\,5\,7)(4\,6)$

(b) Is σ an even or odd permutation? Justify your answer.

$\sigma = (1\,3)(2\,5)(5\,7)(4\,6) \Rightarrow \sigma$ is even

(c) Let $\tau = (3\ 7\ 4\ 2\ 5) \in S_7$. Express τ as a product of 4 transpositions.

$\tau = (3\,7)(7\,4)(4\,2)(2\,5)$

(d) Express the permutation $\sigma\tau$ in cycle notation.

$\sigma\tau = (1\,3)(2\,5\,7)(4\,6)(3\,7\,4\,2\,5)$

$= (1\,3\,2\,7\,6\,4\,5)$

6. $\boxed{\text{3 points}}$ (a) Give an element of order 15 in A_{10}.

$(1\ 2\ 3)(4\ 5\ 6\ 7\ 8)$

(b) Explain why A_{10} does not have an element of order 26.

The order of an element in A_{10} must divide $|A_{10}| = \frac{10!}{2} = 10 \cdot 8 \cdot 7 \cdots 3$

But $13 \mid 26$ and $13 \nmid \frac{10!}{2} \Rightarrow 26 \nmid |A_{10}|$

7. $\boxed{\text{4 points}}$ Let $H = \{\sigma \in S_4 : \sigma(2) = 2\}$.

(a) What is the order of H ?

$|H| = 6$

(b) What is the index of H in S_4?

$|S_4| = [S_4 : H] \cdot |H|$

$\Rightarrow [S_4 : H] = \frac{|S_4|}{|H|} = \frac{24}{6} = 4$

(c) Are the left cosets $(1\ 2\ 3)H$ and $(2\ 3)H$ equal? Justify your answer.

$g_1 H = g_2 H \Leftrightarrow g_2^{-1} g_1 \in H$

$(2\ 3)^{-1}(1\ 2\ 3) = (2\ 3)(1\ 2\ 3) = (1\ 3) \in H$

$\Rightarrow (1\ 2\ 3)H = (2\ 3)H$

8. $\boxed{\text{3 points}}$ Consider the following statement:

Let G be a group, and let $H = \{g \in G : g^2 = e\}$, where e is the identity of G. Then H is a subgroup of G.

(a) Use the group D_3 to show that the statement above is **false**.

Let F_1 and F_2 be two distinct reflections.
Then $F_1^2 = F_2^2 = id$. But F_1F_2 is a rotation, all of which have order 3.
$\Rightarrow (F_1F_2)^2 \neq id$

(b) The following is a proof of the above statement given by ChatGPT (with GPT version 3.5). Find and explain the error.

ChatGPT Proof. The identity element is in H, so we need to check that H is closed under the group operation and closed under taking inverses. First, we show that H is closed under the group operation. Let $a, b \in H$, so $a^2 = b^2 = e$. Then,

Not true

$$\boxed{(ab)^2 = a^2b^2} = e \cdot e = e,$$

so H is closed under the group operation. Next, we show that H is closed under taking inverses. Let $a \in H$, so $a^2 = e$. Then, we have

$$(a^{-1})^2 = (a^2)^{-1} = e^{-1} = e.$$

Therefore, $a^{-1} \in H$, and H is closed under taking inverses. As H contains the identity, is closed under the group operation, and is closed under taking inverses, H is a subgroup of G. □

$(ab)^2 = abab \neq a^2b^2$

(c) Add one word to the statement above that makes the statement true and the ChatGPT proof correct.

The statement and proof are correct if G is abelian.

Part II: Proofs

Instructions: Complete any three of the following four problems.

9. $\boxed{\text{7 points}}$ Let H_1 and H_2 be subgroups of a group G. Prove that $H_1 \cap H_2$ is a subgroup of G.

As $e \in H_1$ and $e \in H_2$, $e \in H_1 \cap H_2$.

If $a, b \in H_1 \cap H_2$, then
- $a, b \in H_1 \Rightarrow ab \in H_1$
- $a, b \in H_2 \Rightarrow ab \in H_2$

$\Rightarrow ab \in H_1 \cap H_2$

If $a \in H_1 \cap H_2$, then
- $a \in H_1 \Rightarrow a^{-1} \in H_1$
- $a \in H_2 \Rightarrow a^{-1} \in H_2$

$\Rightarrow a^{-1} \in H_1 \cap H_2$. $\square$

10. $\boxed{\text{7 points}}$ Let G be a group. The *center* of G is the set

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}.$$

Prove that $Z(G)$ is closed under taking inverses.

Let $g \in G$. If $x \in Z(G)$, then

$$g = x^{-1}xg$$
$$= x^{-1}gx \text{ as } x \in Z(G)$$
$$\Rightarrow gx^{-1} = x^{-1}gxx^{-1}$$
$$\Rightarrow gx^{-1} = x^{-1}g$$
$$\Rightarrow x^{-1} \in Z(G), \text{ as } g \in G \text{ was arbitrary.}$$

Alternate Solution (there are several):

Fix $x \in Z(G)$. Let $g \in G$.

As $x \in Z(G)$,
$$g^{-1}x = xg^{-1}$$
$$\Rightarrow (g^{-1}x)^{-1} = (xg^{-1})^{-1}$$
$$\Rightarrow x^{-1}g = gx^{-1}$$
$$\Rightarrow x^{-1} \in Z(G), \text{ as } g \in G \text{ was arbitrary.}$$

11. $\boxed{\text{7 points}}$ Use Fermat's Little Theorem to show that if $p = 4n + 3$ is prime, then there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

Suppose $\exists\, x \in \mathbb{Z}$ s.t. $x^2 \equiv -1 \pmod{p}$

By Fermat's Little thm, $x^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow x^{4n+2} \equiv 1 \pmod{p}$

$\Rightarrow (x^2)^{2n+1} \equiv 1 \pmod{p}$

But $(x^2)^{2n+1} \equiv (-1)^{2n+1} \pmod{p}$

$\equiv -1 \pmod{p}$

$\Rightarrow 1 \equiv -1 \pmod{p}$

$\Rightarrow p \mid 2 \Rightarrow p = 2$, a contradiction since $p = 4n+3$ is odd.

$\Rightarrow x^2 \equiv -1 \pmod{p}$ has no solution

12. $\boxed{\text{7 points}}$ Suppose that $[G : H] = 2$. Prove that if a and b are not in H, then $ab \in H$.

If $a \notin H$, then $a^{-1} \notin H$, since H is closed under inversion.

We know $G = H \cup bH$ and $H \cap bH = \emptyset$ since $b \notin H$. and $[G:H] = 2$.

$\Rightarrow a^{-1} \in bH$ as $a^{-1} \notin H$.

$\Rightarrow \exists\, h \in H$ s.t. $a^{-1} = bh$

$\Rightarrow h^{-1} = ab$

$\Rightarrow ab \in H$. $\square$