Math 344 Fall 2025 Exam One

Name:_____

- Put your name in the "_____" above.
- Answer all questions.
- Proofs are graded for clarity, rigor, neatness, and style.
- Good luck!

Computations

1. For the following element f of S_9, do the following:
   (a) compute $f \circ f \circ f \circ f(9)$,
   (b) write the smallest positive integer n such that

$$\overbrace{f \circ \cdots \circ f}^{n \text{ times}}(9) = 9,$$

   and
   (c) write down an element m in $\{1,2,3,4,5,6,7,8,9\}$ with the property that $f \circ f \circ f(m) = m$.

$$\begin{gathered} f\colon \{1,2,3,4,5,6,7,8,9\} \to \{1,2,3,4,5,6,7,8,9\} \\ 1 \mapsto 7 \\ 2 \mapsto 2 \\ 3 \mapsto 4 \\ 4 \mapsto 5 \\ 5 \mapsto 3 \\ 6 \mapsto 1 \\ 7 \mapsto 8 \\ 8 \mapsto 9 \\ 9 \mapsto 6 \end{gathered}$$

Solution. (a) 8
(b) 5
(c) 2.

□

2. Suppose that G is a group with a subgroup H. For any $g \in G$, define $gH = \{gh \mid h \in H\}$.

   (a) Write down two elements A of D_4 such that $F \in A\langle R\rangle$. (For example, we see that $A = I$ does not work since $I\langle R\rangle = \{I, R, R^2, R^3\}$ does not contain F.)

   (b) Write down three distinct subgroups of D_4 of size 2.

   (c) Write down three elements B in D_5 such that $\langle B\rangle = \langle R\rangle$.

Proof. (a) Elements that work are F, FR, FR^2, FR^3.

(b) Subgroups of size 2 are $\{I, R^2\}, \{I, F\}, \{I, FR\}, \{I, FR^2\}, \{I, FR^3\}$.

(c) Elements that work are R, R^2, R^3, R^4.

□

Proofs

(I) Let $H = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ both } m \text{ and } n \text{ are even}\}$. Prove that H is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

Proof. We must prove three things.

- Since $(0,0) = (2 \cdot 0, 2 \cdot 0)$, we see that $(0,0) \in H$, so that $H \neq \varnothing$.
- Suppose that $m_1, n_1, m_2, n_2 \in \mathbb{Z}$, so that $(2m_1, 2n_1), (2m_2, 2n_2)$ are arbtirary in H. Then

$$\begin{aligned} (2m_1, 2n_1) + (2m_2, 2n_2) &= (2m_1 + 2m_2, 2n_1 + 2n_2) && \text{(this is the operation on } \mathbb{Z} \times \mathbb{Z}) \\ &= (2(m_1 + m_2), 2(n_1 + n_2)) && \text{(how integers work)}, \end{aligned}$$

  so we see that $(2m_1, 2n_1) + (2m_2, 2n_2) \in H$ by the definition of H.
- Finally, choose any $m, n \in \mathbb{Z}$, so that $(2m, 2n)$ is arbitrary in H. Then we see that

$$-(2m, 2n) = (-2m, -2n) = (2(-m), 2(-n)),$$

  so $-(2m, 2n) \in H$ by the definition of H.

□

(II) Suppose that G is a group and write

$$H = \left\{ g^{130} \mid g \in G \right\}.$$

Prove: if G is commutative, then H is a subgroup of G.

Proof. To show H is a subgroup of G, there are three steps. As usual, let e be the identity of G.

- Note that $e = e^{130}$, by the definition of the identity 129 times. Hence, we see $e \in H$, so $H \neq \varnothing$.
- Suppose that $a, b \in G$, so that a^{130} and b^{130} are arbitrary elements of H. Note that

$$\begin{aligned} a^{130}b^{130} &= \underbrace{a \cdots a}_{130 \text{ times}} \cdot \underbrace{b \cdots b}_{130 \text{ times}} && \text{(definition of exponents)} \\ &= \underbrace{(ab) \cdots (ab)}_{130 \text{ times}} && \text{(since } G \text{ is commutative)}, \end{aligned}$$

  so $a^{130}b^{130} \in H$ by the definition of H.
- Finally suppose that $c \in G$, so that c^{130} is arbitrary in H, and note that

$$\begin{aligned} c^{130}\left(c^{-1}\right)^{130} &= \underbrace{c \cdots c}_{130 \text{ times}} \cdot \underbrace{c^{-1} \cdots c^{-1}}_{130 \text{ times}} && \text{(definition of exponents)} \\ &= \underbrace{\left(cc^{-1}\right) \cdots \left(cc^{-1}\right)}_{130 \text{ times}} && \text{(since } G \text{ is commutative)} \\ &= e^{130} && \text{(definition of inverses)} \\ &= e && \text{(definition of identity 129 times)}. \end{aligned}$$

  That is, we know by fact from class that $\left(c^{130}\right)^{-1} = \left(c^{-1}\right)^{130} \in H$.

□

(III) Define the operation $\star$ on $\mathbb{R}$ by setting $x \star y = x^2 + y^2$. Either prove that $(\mathbb{R}, \star)$ is a group or prove that it is not a group.

Proof. Let's prove that there is no identity element in $(\mathbb{R}, \star)$, thereby showing that $(\mathbb{R}, \star)$ is *not* a group. To do this, choose an arbitrary $z \in \mathbb{R}$ and note that since z^2 is positive:

$$2 \star z = 2^2 + z^2 = 4 + z^2 > 2.$$

So z is not the identity of $(\mathbb{R}, \star)$; and since z was arbitrary, we conclude that $(\mathbb{R}, \star)$ has no identity. $\square$

Extra Credit (if you have extra time)

Suppose that G is a group with two subgroups I and J. Prove that

$$I \cup J \text{ is a subgroup of } G \qquad \text{if and only if} \qquad \text{either } I \subseteq J \text{ or } J \subseteq I.$$

Proof.

- If $I \subseteq J$, then $I \cup J = J$ is a subgroup of G by hypothesis. Likewise, if $J \subseteq I$, then $I \cup J = I$ is a subgroup of G by hypothesis.
- Conversely, suppose that $I \cup J$ is a subgroup of G. If $I \subseteq J$, we are done! So we suppose that $I \not\subseteq J$; that is, there is some $i \in I$ with $i \notin J$. We must show that $J \subseteq I$, so take an arbitrary $j \in J$. Since $I \cup J$ is a subgroup, we know that $ij \in I \cup J$. There are two cases:
  - Suppose $ij \in J$. Since J is a subgroup, we know $j^{-1} \in J$. Closure of J now implies $i = (ij)j^{-1} \in J$—but this is not the case by our choice of i, so we see $ij \notin J$.
  - Suppose $ij \in I$. Since I is a subgroup, we know $i^{-1} \in I$. Closure of I now implies $j = i^{-1}(ij) \in I$, as desired.

□