Math 344 Winter 2026 Exam Two

Name:_____

- Put your name in the "_____" above.
- Answer all questions.
- Proofs are graded for clarity, rigor, neatness, and style.
- You may choose **two** of the three proofs for me to grade; write your choices below:

  Proof one: _____ Proof two: _____.

  (If you leave this blank, I will grade the first two proofs.)
- Good luck!

Computations

1. (a) Write down three subgroups of S_6 that have size 3.
   (b) Write down three elements of S_6 of order 4.
   (c) Write down a group of size 32 with no elements of order 16.

   Solution. (a) $\langle (123), (124), (125) \rangle$,
   (b) $(1234), (1235), (1236)$,
   (c) $\mathbb{Z}_8 \times \mathbb{Z}_4$.

□

2. Let $G = \mathbb{Z}_{20}$ and let H be the subgroup of G generated by 5.

   (a) Write down all elements of all right cosets of H.

   (b) What is $(G : H)$?

Solution. (a)
- $H + 0 = \{0, 5, 10, 15\}$,
- $H + 1 = \{1, 6, 11, 16\}$,
- $H + 2 = \{2, 7, 12, 17\}$,
- $H + 3 = \{3, 8, 13, 18\}$,
- $H + 4 = \{4, 9, 14, 19\}$.

(b) $(G : H) = 5$.

□

Proofs

(I) Suppose that G, H are groups with identities e_g, e_H. Now assume that $G \times H$ is cyclic, so there are some $g_0 \in G$ and $h_0 \in H$ such that $G \times H = \langle (g_0, h_0) \rangle$. Prove that $G = \langle g_0 \rangle$.

Proof. Choose any $g \in G$. Since $G \times H = \langle (g_0, h_0) \rangle$, there is some $j \in \mathbb{Z}$ such that

$$(g, e_H) = (g_0, h_0)^j = \left((g_0)^j, (h_0)^j \right),$$

so we see that $g = (g_0)^j \in \langle g_0 \rangle$. □

(II) Suppose G, H are groups and $\phi: G \to H$ is an isomorphism. Prove: if H is cyclic, then G is cyclic.

Proof. Since H is cyclic, there is some $h \in H$ with $H = \langle h_0 \rangle$, and since ϕ is surjective, there is some $g_0 \in G$ such that $\phi(g_0) = h_0$. Let's show that $G = \langle g_0 \rangle$. Of course, we know $\langle g_0 \rangle \subseteq G$, so choose an arbitrary $g \in G$. Since $H = \langle h_0 \rangle$, there is some $j \in \mathbb{Z}$ such that $\phi(g) = (h_0)^j$. But then

$$\begin{aligned} \phi\left((g_0)^j\right) &= \phi(g_0)^j && \text{(since } \phi \text{ is an isomorphism)} \\ &= (h_0)^j && \text{(this is how we chose } g_0\text{)}. \end{aligned}$$

Since ϕ is injective, we see that $g = (g_0)^j \in \langle g_0 \rangle$. □

(III) Let G be a group and define a relation $\sim$ on G by: for all $g, h \in G$

$$g \sim h \qquad \text{if and only if} \qquad \text{there exists } j \in \mathbb{Z} \text{ such that } g^j = h^j.$$

Prove that $\sim$ is an equivalence relation.

Proof.

- To see that $\sim$ is reflexive, choose any $g \in G$ and note that $g^1 = g = g^1$, so $g \sim g$.
- To see that $\sim$ is symmetric, choose any $g, h \in G$ and assume that $g \sim h$. Thus, there is some $j \in \mathbb{Z}$ such that $g^j = h^j$. But then $h^j = g^j$, so that $h \sim g$.
- , Finally, to prove that $\sim$ is transitive, we choose any $g, h, i \in G$ and assume $g \sim h$ and $h \sim i$. Then there are $j, k \in \mathbb{Z}$ such that $g^j = h^j$ and $h^k = i^k$. Note that

$$\begin{aligned}
g^{jk} &= (g^j)^k && \text{(exponent rules)} \\
&= (h^j)^k && \text{(this is what } j \text{ does)} \\
&= (h^k)^j && \text{(exponent rules)} \\
&= (i^k)^j && \text{(this is what } k \text{ does)} \\
&= i^{jk} && \text{(exponent rules)},
\end{aligned}$$

so $g \sim i$.

□

Extra Credit (if you have extra time)

Suppose that G is an abelian group of size 64. Define the function

$$\begin{aligned} \phi: G &\to G \\ g &\mapsto g^2 \end{aligned}$$

Either prove that ϕ is an isomorphism or prove it is not an isomorphism.

Proof. Let's write e for the identity of G. Since $|G| > 1$, we know there exists some $g \in G$ with $g \neq e$. Since $|G| = 2^6$ and $\operatorname{ord}(g) \neq 1$, Lagrange's Theorem tells us that there exists $j \in \{1, 2, 3, 4, 5, 6\}$ such that $\operatorname{ord}(g) = 2^j$. But then

$$\begin{aligned} \phi(g)^{(2^{j-1})} &= \left(g^2\right)^{(2^{j-1})} && \text{(definition of } \phi\text{)} \\ &= g^{(2^j)} && \text{(exponent rules)} \\ &= e && \left(\text{since } \operatorname{ord}(g) = 2^j\right) \end{aligned}$$

But this means that $\operatorname{ord}(\phi(g))$ is a divisor of 2^{j-1}, by fact from class. In particular, we see that $\operatorname{ord}(\phi(g)) < \operatorname{ord}(g)$. But in class, we proved that isomorphisms preserve orders of elements, so we conclude that ϕ is not an isomorphism. □