Math 344 Fall 2025 Exam Two

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) write f in disjoint cycle form,
   (b) write f as a product of transpositions,
   (c) state the parity of f, and
   (d) write $(126) \circ (389) \circ f$ in disjoint cycle form.

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

Solution. (a) (17896)(345),
(b) (17)(78)(89)(96)(34)(45),
(c) even,
(d) (179)(26)(3458).

□

2. Let H be the subgroup of S_5 generated by (12345). In other words, let $H = \langle(12345)\rangle$. Write, in disjoint cycle form,

   (a) all elements of $H(12)$, and

   (b) all elements of $(12)H$.

   Solution. Let's write id for $\mathrm{id}_{\{1,2,3,4,5\}}$.

   (a)

$$\begin{aligned} H(12) &= \{\mathrm{id}(12), (12345)(12), (13524)(12), (14253)(12), (15432)(12)\} \\ &= \{(12), (1345), (14)(235), (153)(24), (2543)\}. \end{aligned}$$

   (b)

$$\begin{aligned} (12)H &= \{(12)\,\mathrm{id}, (12)(12345), (12)(13524), (12)(14253), (12)(15432)\} \\ &= \{(12), (2345), (135)(24), (14)(253), (1543)\}. \end{aligned}$$

□

Proofs

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

Proof. Since G is cyclic, it has a generator $g \in G$, so $G = \langle g \rangle$. I claim that $H = \langle \phi(g) \rangle$—if we can show this, then we will see that H is cyclic with generator $\phi(g)$.

Be definition, we know that $\langle \phi(g) \rangle \subseteq H$. For the reverse inclusion, take any $h \in H$. Since ϕ is surjective, there is some $x \in G$ such that $\phi(x)$. But we also remember that G is cyclic, so there is some $n \in \mathbb{Z}$ with $x = g^n$. Thus, using the fact that ϕ preserves the operations of the groups G, H, we see that

$$h = \phi(x) = \phi(g^n) = \phi(g)^n \in \langle \phi(g) \rangle .$$

□

(II) Suppose that p is a prime number and that G is a group of size p, say with identity e. Prove: for all $g \in G$, if $g \neq e$, then $G = \langle g \rangle$.

Proof. Choose any $g \in G \setminus \{e\}$. Then Lagrange's Theorem tells us that $\operatorname{ord}(g)$ is a divisor of p. But since p is prime, this means $\operatorname{ord}(g)$ is either 1 or p. And since $g \neq e$, we know that $\operatorname{ord}(g) \neq 1$, so

$$|\langle g \rangle| = \operatorname{ord}(g) = p.$$

Since $|G| = p$, we conclude that $\langle g \rangle = G$. ☐

(III) Suppose that G, H are groups and $\phi: G \to H$ is an isomorphism. In particular, we know that ϕ is bijective, so it has an inverse: $\phi^{-1}: H \to G$. Prove that ϕ^{-1} is an isomorphism.

Proof. Since ϕ^{-1} is invertible (with inverse ϕ), we know it is bijective. To show it preserves the operations of H, G, choose any $h_1, h_2 \in H$. Since ϕ is (in particular) surjective, there are $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$.

$$\begin{aligned}
\phi^{-1}(h_1 h_2) &= \phi^{-1}(\phi(g_1)\phi(g_2)) && \text{(substitution)} \\
&= \phi^{-1}(\phi(g_1 g_2)) && \text{(since } \phi \text{ is an isomorphism)} \\
&= g_1 g_2 && \text{(definition of inverse function)} \\
&= \phi^{-1}(h_1)\phi^{-1}(h_2) && \text{(definition of inverse function).}
\end{aligned}$$

□

Extra Credit (if you have extra time)

Suppose that G is a abelian group (ie, the operation of G is commutative) of size 77. Define

$$\begin{aligned} \phi\colon G &\to G \\ g &\mapsto g^3. \end{aligned}$$

Prove that ϕ is an isomorphism.

Proof. Let e be the identity of G. We must show three things. (In fact, as mentioned in class, since G is finite, the injectivity of ϕ implies its surjectivity, and vice-versa. We'll show all three though.)

- For any $g, h \in G$, note that

$$\begin{aligned} \phi(gh) &= (gh)^3 && \text{(definition of } \phi) \\ &= g^3h^3 && \text{(since } G \text{ is abelian)} \\ &= \phi(g)\phi(h) && \text{(definition of } \phi). \end{aligned}$$

- Choose any $g, h \in G$ and suppose that $\phi(g) = \phi(h)$, so that by facts from class:

$$e = e^3 = \phi(e) = \phi(g)\phi(g)^{-1} = \phi(g)\phi(h)^{-1} = \phi\left(gh^{-1}\right) = \left(gh^{-1}\right)^3.$$

  But then $\operatorname{ord}\left(gh^{-1}\right)$ is a divisor of 3, but must also be a divisor of 77 by Lagrange's Theorem. Thus, we see $\operatorname{ord}\left(gh^{-1}\right) = 1$, so that $gh^{-1} = e$; ie, $g = h$.

- Choose any $g \in G$ and note that since $\operatorname{ord} g$ is a divisor of 77 (by Lagrange's Theorem), we know that $g^{77} = e$. Then

$$\phi\left(g^{26}\right) = \left(g^{26}\right)^3 = g^{78} = gg^{77} = ge = g.$$

□