HW 5 Due: 18 February 2026

As always, your answer will be graded on the quality of presentation as well as the correct answer. To get a good score: write your answer neatly, use complete sentences, and *justify your work*.

Computations

1. Write down all the orders of all the elements of D_4.

   Solution.
   - I has order 1,
   - R has order 4,
   - R^2 has order 2,
   - R^3 has order 1,
   - F has order 2,
   - FR has order 2,
   - FR^2 has order 2, and
   - FR^3 has order 2.

   ☐

2. Write down all the orders of all the elements of $S_3 \times \mathbb{Z}_2$.

   Solution. Let $\epsilon = \mathrm{id}_{\{1,2,3\}}$.
   - $(\epsilon, 0)$ has order 1,
   - $(\epsilon, 1)$ has order 2,
   - $((12), 0)$ has order 2,
   - $((12), 1)$ has order 2,
   - $((13), 0)$ has order 2,
   - $((13), 1)$ has order 2,
   - $((23), 0)$ has order 2,
   - $((23), 1)$ has order 2,
   - $((123), 0)$ has order 3,
   - $((123), 1)$ has order 6,
   - $((132), 0)$ has order 3, and
   - $((132), 1)$ has order 6.

   ☐

3. Let $f = (14563) \in S_9$. Write down all the orders of all the elements of $\langle f \rangle$.

   Solution. Let's write $\epsilon = \mathrm{id}_{\{1,2,3,4,5,6,7,8,9\}}$. Since $\mathrm{ord}(f) = 5$, we know from class that $\langle f \rangle$ is isomorphic to $\mathbb{Z}_5$ and $\langle f \rangle = \left\{\epsilon, f, f^2, f^3, f^4\right\}$. Moreover, ϵ has order 1, and f, f^2, f^3, f^4 all have order 5. ☐

Proofs

(I) Let G be a group and suppose $g, h \in G$ have finite order. Prove: if $gh = hg$, then $\mathrm{ord}(gh)$ is a divisor of $\mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h))$.

Proof. Let e be the identity of G and let $m = \mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h))$, so there are $a, b \in \mathbb{Z}$ such that $m = a\,\mathrm{ord}(g)$ and $m = b\,\mathrm{ord}(h)$. Now we use the fact that $gh = hg$ to see that

$$(gh)^m = g^m h^m = g^{a\,\mathrm{ord}(g)} h^{b\,\mathrm{ord}(h)} = \left(g^{\mathrm{ord}(g)}\right)^a \left(h^{\mathrm{ord}(h)}\right)^b = e^a e^b = e,$$

so by [Pin10, Chapter 10, Theorem 5] (or "by fact from class") we know $\mathrm{ord}(gh)$ is a divisor of m. ☐

(II) Suppose that 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; that is, some $g_0 \in G$ such that $G = \langle g_0 \rangle$. Let's prove that $H = \langle \phi(g_0) \rangle$. We know by definition that $\langle \phi(g_0) \rangle \subseteq H$, so let's begin proving the reverse inclusion by choosing any $h \in H$. Since ϕ is surjective, there exists some $g \in G$ with $\phi(g) = h$; and since $G = \langle g_0 \rangle$, there exists some $j \in \mathbb{Z}$ such that $g = (g_0)^j$. Then

$$\begin{aligned} h &= \phi(g) && \text{(as above)} \\ &= \phi\left((g_0)^j\right) && \text{(as above)} \\ &= \phi(g_0)^j && \text{(definition of isomorphism)} \\ &\in \langle \phi(g_0) \rangle && \text{(definition of subgroup generation).} \end{aligned}$$

□

(III) Let G be a group, and define
$$D = \{(g, g) \mid g \in G\}.$$
Assume that D is a subgroup of $G \times G$.[1] Prove that G is isomorphic to D.

Proof. Define
$$\begin{aligned} \phi: G &\to D \\ g &\mapsto (g, g). \end{aligned}$$

- To see that ϕ is surjective, choose any $g \in G$, so that $(g, g) \in D$ is arbitrary. But then we see $\phi(g) = (g, g)$.
- To see that ϕ is injective, choose any $g, h \in G$ and assume that $\phi(g) = \phi(h)$. But then $(g, g) = \phi(g) = \phi(h) = (h, h)$, so that $g = h$.
- To see that ϕ respects the operations of G, D, choose any $g, h \in G$ and note that $\phi(gh) = (gh, gh) = (g, g)(h, h) = \phi(g)\phi(h)$.

□

(IV) Suppose that G is a finite cyclic group of order $n \in \mathbb{Z}_{\geq 1}$, with generator $g \in G$. Let $j \in \mathbb{Z}_{>0}$. Prove: if there exist $a, b \in \mathbb{Z}$ with $an + bj = 1$, then $G = \langle g^j \rangle$.

Proof. We know by definition of subgroup generation that $\langle g^j \rangle \subseteq G$. To show the reverse inclusion, we will show that $g \in \langle g^j \rangle$. Then [Cla, Remark 3.11] will tell us that $G = \langle g \rangle \subseteq \langle g^j \rangle$. To see that $g \in \langle g^j \rangle$, note that

$$\begin{aligned} g &= g^1 && \text{(definition of exponent 1)} \\ &= g^{an+bj} && \text{(hypothesis)} \\ &= (g^n)^a \left(g^j\right)^b && \text{(exponent rules)} \\ &= \left(g^j\right)^b && \text{(definition of order)} \\ &\in \langle g^j \rangle && \text{(definition of subgroup generation).} \end{aligned}$$

□

References

[Cla] Our Group Theory Class, *Our Definition Sheet*.

[Pin10] Charles C. Pinter, *A book of abstract algebra*, Dover Publications, Inc., Mineola, NY, 2010, Reprint of the second (1990) edition [of MR0644983]. MR 2850284

[1] This is always true and in principle, we could prove it. However, I'm not requiring a proof. At this time.