HW 5 Solutions

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 $\operatorname{ord}(f) = 5$, we know from class that $\langle f \rangle$ is isomorphic to $\mathbb{Z}_5$ and $\langle f \rangle = \{\epsilon, f, f^2, f^3, f^4\}$. Moreover, ϵ has order 1, and f, f^2, f^3, f^4 all have order 5. □

Proofs

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

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

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

   so by [Pin10, Chapter 10, Theorem 5] we know that $\operatorname{ord}(gh)$ is a divisor of m. □

2. 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

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

   - 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 $\phi(gh) = (gh, gh) = (g, g)(h, h) = \phi(g)\phi(h)$.

   □

3. Suppose that G, H are groups and $\phi \colon G \to H$ is an isomorphism. Prove: for all $g \in G$,

   $$\operatorname{ord}(g) = \operatorname{ord}(\phi(g)).$$

   Proof. Let e_G, e_H be the identity elements of G, H, respectively. Then by a fact from class, the definition of order, and the definition of isomorphism, we see that

   $$e_H = \phi(e_G) = \phi\left(g^{\operatorname{ord}(g)}\right) = \phi(g)^{\operatorname{ord}(g)},$$

   so $\operatorname{ord}(\phi(g)) \leq \operatorname{ord}(g)$. Now let's suppose $j \in \{0, 1, \ldots, \operatorname{ord}(g) - 1\}$, and $\phi(g)^j = e_H$; we'd like to show that $j = 0$. Well in this case, we see $\phi\left(g^j\right) = \phi(g)^j = e_H = \phi(e_G)$, so by the injectivity of ϕ we deduce that $g^j = e_H$. But hey, we assumed that $j < \operatorname{ord}(g)$! This means that $j = 0$, as desired. □

References

[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.