HW 5 Due: 14 May 2025

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 $\operatorname{ord}(gh)$ 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. □

(II) Suppose that G is a finite cyclic group of order n, 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. Let e be the identity of G. Since $\langle g^j \rangle \subseteq G$, we need only show that $G \subseteq \langle g^j \rangle$. And since $G = \langle g \rangle$, this means we must show $g \in \langle g^j \rangle$. Since G is cyclic of order n, we know $g^n = e$. Thus, we use [Pin10, Chapter 10, Theorem 1] to note that

$$(g^j)^b = g^{bj} = e^a g^{bj} = (g^n)^a g^{bj} = g^{an} g^{bj} = g^{an+bj} = g^1 = g,$$

so $g \in \langle g^j \rangle$, as desired. □

(III) Let $m \in \mathbb{Z}_{>0}$ and let J be any subgroup of $\mathbb{Z}_m$. Prove that if j is the smallest positive integer in J, then $J = \langle j \rangle$. (In particular: all subgroups of $\mathbb{Z}_m$ are cyclic.)

Proof. Suppose that $k \in J$, and perform long division to obtain $q, r \in \mathbb{Z}_{\geq 0}$ such that

- $k = qj + r$ and
- $r < j$.

Since J is a subgroup, we know $-j \in J$; hence $r = k + q(-j) \in J$. But j was the smallest *positive* integer in J, so the fact that $r < j$ tells us that $r = 0$. That is, $k = qj \in J$, as desired. □

(IV) Suppose that G, H are groups and $\phi: G \to H$ 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 $g^j = e_G$. 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