Exercise on the order of an element in a group

Abstract Algebra 1
MATH 3140

SEBASTIAN CASALAINA

ABSTRACT. This is an Exercise on the order of an element in a group from Fraleigh [Fra03, §6]:

In [Fra03, p.59], Fraleigh defines the order of an element of a group: Given a group G and an element $a \in G$, if the order of the cyclic subgroup $\langle a \rangle$ of G is finite, then the **order of** a is defined to be $|\langle a \rangle|$; i.e., the number of elements in the cyclic subgroup of G generated by a. Otherwise, the order of a is said to be infinite. A common notation for the order of an element a in a group G is $|a|$; unfortunately, this notation is not used in Fraleigh.

In [Fra03, p.59], Fraleigh states without proof that if $a \in G$ is of finite order m, then m is the smallest positive integer such that $a^m = e$. One can deduce this from what is in the rest of [Fra03, §6], but I want to explain this here.

Exercise on the order of an element in a group. Suppose G is a group. Show that $a \in G$ *is of finite order if and only if there exists a positive natural number n such that $a^n = e$*. Moreover, show that for an element $a \in G$ of finite order, *the order of a is equal to m if and only if m is the smallest positive integer such that $a^m = e$*.

Solution. Suppose first that a is of finite order m; i.e., $|\langle a \rangle| = m$. Then from [Fra03, Theorem 6.10], there is an isomorphism of groups

$$\phi : \mathbb{Z}_m \longrightarrow \langle a \rangle$$
$$s \mapsto a^s$$

Using this, we have that $a^m = \phi(1)^m = \phi(\underbrace{1 + \cdots + 1}_{m \text{ times}}) = \phi(0) = a^0 = e$, where in the second equality we are using the fact that ϕ is an isomorphism of binary structures. In particular, we see that there exists a positive natural number m such that $a^m = e$. Moreover, m is the smallest such

Date: August 12, 2021.

positive number, since if there were a positive integer r with $0 < r < m$ such that $a^r = e$, then $\phi(0) = a^0 = e = a^r = \phi(r)$, contradicting the injectivity of ϕ.

Conversely, suppose that there exists a positive integer n such that $a^n = e$. Then let m be the smallest positive integer such that $a^m = e$. I claim that the order of a is finite and equal to m; i.e., $|\langle a \rangle| = m$. Indeed, I claim first that the containment

$$\{e, a, a^2, \dots, a^{m-1}\} \subseteq \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

is an equality. To show this, we just need to show that given $n \in \mathbb{Z}$, we have $a^n = a^r$ for some $0 \le r < m$. For this, we can use the division algorithm to find integers r, q such that

$$n = qm + r, \quad 0 \le r < m.$$

Then $a^n = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = e^q a^r = a^r$, which is what we needed to prove. Thus $\langle a \rangle = \{e, a, a^2, \dots, a^{m-1}\}$.

Finally, I claim that $|\{e, a, a^2, \dots, a^{m-1}\}| = m$. Indeed, if $a^i = a^j$ for some $0 \le i \le j < m$, then we have $e = a^j a^{-i} = a^{j-i}$. Since $0 \le j - i < m$, and m is the smallest positive integer such that $a^m = e$, it must be that $j - i = 0$, or, in other words, $i = j$. Thus $|\langle a \rangle| = |\{e, a, a^2, \dots, a^{m-1}\}| = m$. $\square$

References

[Fra03] John Fraleigh, *A First Course in Abstract Algebra*, Seventh edition, Addison Wesley, Pearson, 2003.

University of Colorado, Department of Mathematics, Campus Box 395, Boulder, CO 80309

Email address: `casa@math.colorado.edu`