Exercise 4.29

Abstract Algebra 1
MATH 3140

SEBASTIAN CASALAINA

ABSTRACT. This is Exercise 4.29 from Fraleigh [Fra03, §4]:

Exercise 4.29. Show that if G is a finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a * a = e$.

Proof. For brevity, I am going to drop the $*$ in what follows. For this problem, I want to start by observing two things. First, if $g, h \in G$ with $g \neq h$, then $g^{-1} \neq h^{-1}$. Indeed if $g^{-1} = h^{-1}$, then applying g to the right on each side we would have $e = g^{-1}g = h^{-1}g$, and similarly, applying g on the left to $g^{-1} = h^{-1}$, we would have $e = gh^{-1}$, so that h^{-1} would be an inverse to g. Since inverses are unique (see [Fra03, Theorem 4.17]), this would imply $h = g$, giving a contradiction. Second, since e is its own inverse, we can apply this to conclude that if $e \neq g \in G$, then $g^{-1} \neq e$.

Now let us list the elements of the group G, and for concreteness, let us assume that $|G| = 2n$ for some natural number n. To start, we have the identity element e. Since the order of G is even, and in particular is not equal to 1, there must be another element, $g_1 \in G$, with $g_1 \neq e$. If $g_1 g_1 = e$, then we are done. Otherwise, the inverse $g_1^{-1} \in G$ is not equal to g_1 or e (from the first paragraph), and so we have three distinct elements in the group, namely

$$e, g_1, g_1^{-1}.$$

Since the order G is even, there must be a fourth element $g_2 \in G$, with $g_2 \neq e, g_1, g_1^{-1}$. If $g_2 g_2 = e$ we are done. Otherwise, the inverse $g_2^{-1} \in G$ is not equal to g_2 or e, g_1, g_1^{-1} (from the first paragraph), and so we have five distinct elements in the group

$$e, g_1, g_1^{-1}, g_2, g_2^{-1}.$$

Date: August 8, 2021.

Continuing on in this way, either we find an element $g_k \in G$, with $g_k g_k = e$, and we are done, or we obtain a list of $2n-1$ distinct elements in the group,

$$e, g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_{n-1}, g_{n-1}^{-1}.$$

Let $g_n \in G$ be the last element in the group; i.e., the one not listed above. From the first paragraph above we must have that g_n^{-1} is not equal to any of the other elements of the group listed above, so that $g_n^{-1} = g_n$. In other words, $g_n g_n = e$, and we are done. □

Here is another solution that may be useful in thinking about the more general question of whether, given a finite group G of order divisible by a prime number p, there exists an element $a \in G$ such that $a^p = e$. (Exercise 4.29 answers this question in the case $p = 2$.)

Another solution. Consider the set

$$X := \{(a,b) \in G \times G : ab = e\}.$$

For any $(a,b) \in X$, we have that $b = a^{-1}$, so that $X = \{(a, a^{-1}) : a \in G\}$, and so we can conclude that $|X| = |G| = 2n$.

Let us next consider the subsets

$$X' := \{(a,b) \in X : (a,b) = (b,a)\}, \quad X'' := \{(a,b) \in X : (a,b) \neq (b,a)\}.$$

In particular, since $X = X' \sqcup X''$, we have that

$$|X| = |X'| + |X''|.$$

Note that if $(a,b) \in X$, then $(b,a) \in X$; [1] thus $|X''|$ is even. Since $|X|$ is even, and $|X''|$ is even, it must be that $|X'|$ is even. Since $(e,e) \in X'$, we have that $|X'| \geq 2$; thus there must be some $a \in G$ with $a \neq e$ and $(a,a) \in X'$. In other words, $a^2 = e$. □

[1]When thinking about the question of whether, given a finite group G of order pn for some prime number p, there exists an element $a \in G$ such that $a^p = e$, think of this assertion as saying that we can cyclicly permute the elements in X, where now $X := \{(g_1, \dots, g_p) : g_1 \cdots g_p = e\}$, $X' := \{(g, \cdots, g) \in X\}$, and $X'' = X - X'$.

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