HOMEWORK REVIEW
FRIDAY JUNE 12

MATH 3140

SEBASTIAN CASALAINA

ABSTRACT. Here are solutions to the following problems:

- Fraleigh [Fra03] Excercises 5 Problem 46
- Fraleigh [Fra03] Excercises 6 Problem 50
- Fraleigh [Fra03] Excercises 8 Problem 30
- Fraleigh [Fra03] Excercises 9 Problem 18
- Fraleigh [Fra03] Excercises 10 Problem 3
- Fraleigh [Fra03] Excercises 10 Problem 40

Date: June 12, 2020.

EXERCISES 5

Exercises 5: Problem 46. Prove that a cyclic group with only one generator can have at most 2 elements.

Solution to Exercises 5: Problem 46. For any cyclic group $G = \langle g \rangle$, we have that both g and g^{-1} are generators. These are distinct if and only if $|G| \geq 3$.

EXERCISES 6

Exercises 6: Problem 50. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the *unique* such element. Show that $ax = xa$ for all $x \in G$. [Hint: Consider $(xax^{-1})^2$.]

Solution to Exercises 6: Problem 50. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the *unique* such element. Let $x \in G$. We will show $xa = ax$.

To do this consider the element $(xax^{-1})^2$. We have

$$\begin{aligned}
(xax^{-1})^2 &= (xax^{-1})(xax^{-1}) \\
&= xa(x^{-1}x)ax^{-1} && \text{Associativity} \\
&= xaax^{-1} \\
&= xx^{-1} && |\langle a \rangle| = 2 \implies a^2 = e \\
&= e
\end{aligned}$$

Since a is the unique element of G that generates a cyclic subgroup of order 2, we must have

$$xax^{-1} = e \quad \text{or} \quad xax^{-1} = a.$$

In the first case, multiplying by x on the right, we have $xa = x$, then then multiplying by x^{-1} on the left, we have $a = e$, which is not possible since a generates a subgroup of order 2.

In the second case, multiplying by x on the right gives us that

$$xa = ax.$$

Exercises 8

Exercises 8: Problem 30. Determine whether the function

$$f_1 : \mathbb{R} \to \mathbb{R}$$

defined by $f_1(x) = x + 1$ is a permutation of $\mathbb{R}$.

Solution to Exercises 8: Problem 30. The function

$$f_1 : \mathbb{R} \to \mathbb{R}$$

defined by $f_1(x) = x + 1$ is a permutation of $\mathbb{R}$. In fact, I claim the inverse function f_1^{-1} is given by $f_1^{-1}(x) = x - 1$. To see this we have

$$(f_1^{-1} \circ f_1)(x) = f_1^{-1}(x + 1) = (x + 1) - 1 = x.$$

Similarly, we have

$$(f_1 \circ f_1^{-1})(x) = f_1(x - 1) = (x - 1) + 1 = x.$$

In other words, $f_1^{-1} \circ f_1 = f_1 \circ f_1^{-1} = \mathrm{Id}_{\mathbb{R}}$.

EXERCISES 9

Exercises 9: Problem 18. Find the maximum possible order for an element of S_{15}.

Solution to Exercises 9: Problem 18. We claim that the maximum possible order for an element of S_{15} is 105.

To see this recall that any element $\sigma \in S_{15}$ can be written as a product of disjoint cycles. If $\sigma_1, \ldots, \sigma_r$ are disjoint cycles, then $|\sigma_1 \cdots \sigma_r| = \mathrm{lcm}(|\sigma_1|, \ldots, |\sigma_r|)$. In addition, any element $\sigma \in S_{15}$ of maximum possible order can be written as a product of disjoint cycles $\sigma_1 \cdots \sigma_r$ where

$$\sum_{i=1}^{r} |\sigma_i| = 15.$$

In other words, among all partitions $(d_1, \ldots, d_r)$ of 15 (i.e., natural numbers $1 \leq d_1 \leq \cdots \leq d_r \leq 15$ with $\sum_{i=1}^r d_i = 15$), we want to know what is the maximum of $\mathrm{lcm}(d_1, \ldots, d_r)$.

We claim that the maximum is 105, corresponding to the partition $(3, 5, 7)$, which for instance would correspond to the element

$$\sigma = (1, 2, 3)(4, 5, 6, 7, 8)(9, 10, 11, 12, 13, 14, 15) \in S_{15}.$$

We will argue by considering the maximal element of the partition, d_r. For instance, if $d_r = 15$, then the partition is (15), and then the least common multiple is 15. If $d_r = 14$, then the partition is $(1, 14)$ and then the least common multiple is 14. If $d_r = 13$, then the partition is either $(2,13)$ or $(1,1,13)$, and then the maximum of the least common multiples is 26. If $d_r = 12$, then the partition is $(3,12)$, or $(1,2,12)$, or $(1,1,1,12)$, and the maximum of the least common multiples is 12. If $d_r = 11$, then we have $(4,11)$, or $(1,3,11)$, or $(1,1,2,11)$, or $(1,1,1,1,11)$, in which case the maximum is 44. If $d_r = 10$, then we have $(5,10)$, or $(1,4,10)$, or $(2,3,10)$, or $(1,1,3,10)$, or, $(1,1,1,2,10)$, or $(1,1,1,1,10)$, in which case the maximum is 30. If $d_r = 9$, then we have $(6,9)$, or $(1,5,9)$, or $(2,4,9)$, or $(1,1,4,9)$, or $(1,2,3,9)$, or $(1,1,1,3,9)$, or $(2,2,2,9)$, or $(1,1,2,2,9)$, or $(1,1,1,1,2,9)$, or $(1,1,1,1,1,1,9)$, in which case the maximum is 45. Arguing similarly for $d_r = 8,7,6,5,4,3,2,1$, gives the assertion.

EXERCISES 10

Exercises 10: Problem 3. Find all cosets of the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_{12}$.

Solution to Exercises 10: Problem 3. There are two cosets of the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_{12}$, namely,

$$\langle 2 \rangle \quad \text{and} \quad 1 + \langle 2 \rangle.$$

To see this, observe that

$$0 + \langle 2 \rangle = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}.$$

$$1 + \langle 2 \rangle = \{1, 3, 5, 7, 9, 11\}.$$

These cosets are distinct, and by Lagrange's theorem,

$$|\mathbb{Z}_{12}/\langle 2 \rangle| = 12/6 = 2,$$

so $\langle 2 \rangle$ and $1 + \langle 2 \rangle$ are the only cosets.

Exercises 10: Problem 40. Let G be a finite group of order n with identity e. Show that for any $a \in G$, we have $a^n = e$.

Solution to Exercises 10: Problem 40. Let G be a finite group. Recall that Lagrange's theorem says that for any subgroup $H \leq G$, we have

$$|G/H| = |G|/|H|.$$

In particular, the order of H divides the order of G. Recall that I am using the notation G/H to denote the set of left cosets of H in G.

Recall that given a group G with identity e, and an element $a \in G$, the order of a, written $|a|$, is the smallest natural number n such that $a^n = e$.

Corollary 0.1 (Corollary to Lagrange's theorem)**.** *If G is a finite group, and $a \in G$, then $|a|$ divides $|G|$.*

Proof. Let G be a finite group. Let $a \in G$. Let $H = \langle a \rangle$. We have $|a| = |\langle a \rangle| = |H|$. Since $|H|$ divides $|G|$, it follows that $|a|$ divides $|G|$. □

With this, we can answer the problem. Let G be a finite group of order n with identity e. Let $a \in G$. We will show $a^n = e$. Let $r = |a|$. We know from the corollary above that $r \mid n$; i.e., $n = rs$ for some natural number s. From this we have

$$a^n = a^{rs} = (a^r)^s = e^s = e.$$

REFERENCES

[Fra03] John B. Fraleigh, *A first course in abstract algebra*, 7 ed., Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 2003.

UNIVERSITY OF COLORADO, DEPARTMENT OF MATHEMATICS, CAMPUS BOX 395, BOULDER, CO 80309-0395

Email address: casa@math.colorado.edu