In this investigation, you will practice working with groups and some of their properties.

Problem 1. Let $\mathbb{R}^*$ denote the set of nonzero real numbers, and consider the binary rule $\sqcap$ defined by

$$a \sqcap b = \frac{ab}{4}$$

Part (a). Explain why $\sqcap$ is a binary operation on the set $\mathbb{R}^*$.

Part (b). Prove that $\sqcap$ is associative and commutative.

Part (c). Show that the set $\mathbb{R}^*$ has an identity element under the operation $\sqcap$.

Part (d). Show that every element in the set $\mathbb{R}^*$ has an inverse under the operation $\sqcap$.

Problem 2. Let $n > 0$ be fixed and let $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a commutative group under integer addition.

Problem 3. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and let $a, b \in X$.

Part (a). What can you say about $(b^{-1} * a^{-1}) * (a * b)$? Justify your answer using the properties of groups.

Part (b). How is $(a * b)^{-1}$ related to a^{-1} and b^{-1}? Justify your answer using the properties of groups.

Problem 4. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and let $a, b \in X$. Prove that $(a * b)^{-1} = a^{-1} * b^{-1}$ if and only if $a * b = b * a$.

Powers of Group Elements

Let $\mathcal{X} = (X,*)$ be any group, let $a \in X$, and let n be a positive integer. We define the element a^n to be the result of applying a to itself n times under the operation $*$. In the spirit of this definition, we let $a^{-n} = (a^{-1})^n$ and let a^0 be the identity element.

Problem 5. What is the value of 3^4 in each of the following groups?

Part (a). The group $\mathcal{Z}$ of integers under addition

Part (b). The group $\mathcal{Q}^*$ of nonzero rational numbers under multiplication

Part (c). The group $\mathcal{Z}_4 = (\mathbb{Z}_4, \boxplus_4)$

Part (d). The group $\mathcal{U}_{20} = (\mathbb{U}_{20}, \boxtimes_{20})$ (See Investigation 5 Problem 2.)

Problem 6. If $X = \{1,2,3 \ldots, n\}$ then it is common to let $\mathcal{P}_n$ denote the set of permutations on the set X and let $\boldsymbol{\mathcal{P}_n} = (\mathcal{P}_n, \circ)$ represent the group of permutations on X under function composition. Consider the permutation group $\boldsymbol{\mathcal{P}_4}$ and the permutation

$$\alpha: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Part (a). Compute the powers α^1 through α^6. What patterns do you notice?

Part (b). Compute the powers α^{-1} through α^{-6}. What patterns do you notice?

> ***Theorem 6.1***
>
> Let $\boldsymbol{X} = (X,*)$ be any group with identity element ε, let $a \in X$, and let n be a positive integer. It is always the case that
> $$a^n * a^{-n} = \varepsilon$$

Proof of Theorem 6.1

We will accomplish this proof by induction. First, note that if $n = 1$, the claim reduces to

$$a^1 * a^{-1} = \varepsilon$$

and since $a^1 = a$, this claim is true by definition of the inverse for a. Now, suppose that the claim holds for any positive integer n. We must show that this supposition allows us to prove that the claim also holds for $m = n + 1$. To this end, observe

$a^m * a^{-m} = a^{n+1} * (a^{-1})^{n+1}$ (Apply the definition of $a^{-(n+1)}$.)

$= (a * a^n) * ((a^{-1})^n * (a^{-1})^1)$ (Apply the definition of a^k for any positive integer k.)

$= (a * a^n) * (a^{-n} * a^{-1})$ (Apply the definition of $(a^{-1})^k$ for any positive integer k.)

$= a * (a^n * a^{-n}) * a^{-1}$ (Apply the associative property.)

$= a * \varepsilon * a^{-1}$ (Apply the induction hypothesis.)

$= a * a^{-1}$ (Apply the definition of the identity element.)

$= \varepsilon$ (Apply the definition of the inverse for a.)

QED

Homework.

Problem 1. Prove that the set $X = \mathbb{R} - \{-1\}$ forms a commutative group under the binary rule

$$a \boxminus b = a + ab + b$$

Problem 2. Consider the group $\boldsymbol{S}_{\times} = (S_{\times}, *)$ of cross symmetries. Is it true that $(F * R)^2 = F^2 * R^2$ in this group?

Problem 3. Let $\boldsymbol{X} = (X, *)$ be any group and let $a, b \in X$.

Part (a). Explain why $a * b = (a * b) * (a * b) * (a * b)^{-1}$.

Part (b). Use Part (a) to help you prove that $(a * b)^2 = a^2 * b^2$ always implies that $a * b = b * a$.

Problem 4. Let $\boldsymbol{X} = (X, *)$ be any group and let $a \in X$. If m, n are nonnegative integers, carefully explain why it is true that $a^m * a^n = a^{m+n}$.

Problem 5. Let $\boldsymbol{X} = (X, *)$ be any group and let $a \in X$. Complete the proof of the following result:

If m and n are positive integers then it is always the case that $a^m * a^{-n} = a^{m-n}$.

Proof. Suppose that $n \geq m$, and let $n = m + k$ (so that $k = n - m$). By definition, we know that $a^{-n} = (a^{-1})^{m+k}$. By Problem 4, we also know that

$$(a^{-1})^{m+k} = (a^{-1})^m * (a^{-1})^k = a^{-m} * a^{-k}$$

[Fill this in]

Therefore, we may conclude that $a^m * a^{-n} = a^{m-n}$.

On the other hand, suppose that $n < m$, and let $m = n + j$. By definition, we know $a^m = a^j * a^n$.

[Fill this in]

Therefore, we may conclude that $a^m * a^{-n} = a^{m-n}$.

Problem 6. Let $\boldsymbol{X} = (X, *)$ be any group and let $a \in X$. Prove that the set $\{a^n : n \in \mathbb{Z}\}$ always forms a commutative group under the binary operation $*$.