In this investigation, we will introduce the central concept that we will be studying in this course.

Group

Suppose that X is a any nonempty set endowed with a binary operation *. We say that the algebra $\boldsymbol{\mathcal{X}} = (X,*)$ is a *group* provided it is a Sudoku algebra whose operation is associative.

$\bowtie$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$
$\boldsymbol{a}$	a	b	c	d	e
$\boldsymbol{b}$	b	a	d	e	c
$\boldsymbol{c}$	c	e	a	b	d
$\boldsymbol{d}$	d	c	e	a	b
$\boldsymbol{e}$	e	d	b	c	a

$\Cap$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$
$\boldsymbol{a}$	b	b	a	d	e
$\boldsymbol{b}$	a	b	c	d	e
$\boldsymbol{c}$	d	e	e	b	b
$\boldsymbol{d}$	d	c	a	a	b
$\boldsymbol{e}$	a	d	c	c	a

$\diamond$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$
$\boldsymbol{a}$	b	d	e	a	c
$\boldsymbol{b}$	d	a	c	e	b
$\boldsymbol{c}$	c	e	a	b	d
$\boldsymbol{d}$	a	b	d	c	e
$\boldsymbol{e}$	e	c	b	d	a

Consider the algebras $\boldsymbol{\mathcal{X}}_1 = (X, \bowtie)$, $\boldsymbol{\mathcal{X}}_2 = (X,\Cap)$, and $\boldsymbol{\mathcal{X}}_3 = (X,\diamond)$ defined by the tables above. You explored these algebras in the previous investigation. In particular, we know that $\boldsymbol{\mathcal{X}}_1$ and $\boldsymbol{\mathcal{X}}_3$ are Sudoku algebras, while $\boldsymbol{\mathcal{X}}_2$ is not. However, we also know that neither $\bowtie$ nor $\diamond$ is associative; hence neither of these algebras is a group.

On the other hand, the symmetry algebras $\boldsymbol{\mathcal{S}}_\Delta = (S_\Delta,*)$ and $\boldsymbol{\mathcal{S}}_\times = (S_\times,*)$ are both groups.

Problem 1. In the homework for Investigation 2, you constructed the operation tables for the algebras $\boldsymbol{\mathcal{Z}}_8 = (\mathbb{Z}_8,\boxplus_8)$ and $\boldsymbol{\mathcal{Z}}_8^m = (\mathbb{Z}_8,\boxtimes_8)$. Is either of these a group? Explain your reasoning.

Problem 2. Two integers are *relatively prime* provided their greatest common divisor is 1. Let $\mathbb{U}_{20}$ represent the subset of $\mathbb{Z}_{20}$ containing those integers relatively prime to 20. Is $\mathbb{U}_{20}$ a group under multiplication modulo 20? Justify your answer.

Identity Elements and Inverses

Suppose that X is any nonempty set endowed with a binary operation *. An element $\varepsilon \in X$ is called an *identity element* for the algebra $\boldsymbol{\mathcal{X}} = (X,*)$ provided $\varepsilon * a = a$ and $a * \varepsilon = a$ for all $a \in X$.

Suppose that X is any nonempty set endowed with a binary operation * and equipped with an identity element ε. An element $a \in X$ has an *inverse* in the algebra $\boldsymbol{\mathcal{X}} = (X,*)$ provided there exists an element $b \in X$ such that $b * a = \varepsilon$ and $a * b = \varepsilon$.

Problem 3. Consider the algebras $\boldsymbol{\mathcal{X}}_1 = (X, \bowtie)$, $\boldsymbol{\mathcal{X}}_2 = (X,\Cap)$, and $\boldsymbol{\mathcal{X}}_3 = (X,\diamond)$ defined by the tables above.

Part (a). Do any of these algebras possess an identity element? How did you decide?

Part (b). Consider each algebra that has an identity element. In that algebra, are there any elements that possess an inverse? How did you decide?

Problem 4. Consider the symmetry algebras $\boldsymbol{\mathcal{S}}_\Delta = (S_\Delta,*)$ and $\boldsymbol{\mathcal{S}}_\times = (S_\times,*)$.

Part (a). Both of these algebras possess an identity element. In each algebra, what is the identity element?

Part (b). In both of these algebras, each element has exactly one inverse. List each element along with its inverse.

Problem 5. Suppose that $\boldsymbol{\mathcal{X}} = (X,*)$ is an algebra.

Part (a). If ε and δ are both identity elements for the algebra $\boldsymbol{\mathcal{X}}$, prove that $\varepsilon = \delta$. (Hint: Think about $\varepsilon * \delta$.)

Part (b). Suppose $\boldsymbol{\mathcal{X}}$ that possesses an identity element, and suppose that b and c are both inverses for an element $a \in X$. If the operation * is *associative*, prove that $b = c$. (Hint: First explain why we know $b = (c * a) * b$.)

Theorem 5.1

Suppose that X is any nonempty set endowed with an associative binary operation *. The following statements are logically equivalent.

1. The algebra $\boldsymbol{\mathcal{X}} = (X,*)$ is a group.
2. The algebra $\boldsymbol{\mathcal{X}} = (X,*)$ possesses an identity element, and every element of X has an inverse.

Proof of Theorem 5.1

First, let's suppose that the algebra $\boldsymbol{\mathcal{X}} = (X,*)$ possesses an identity element ε and that every member of X has an inverse. We need to show that $\boldsymbol{\mathcal{X}}$ is a Sudoku algebra. Let $m, n \in X$. We need to show that the equations $m * x = n$ and $x * m = n$ have exactly one solution. Let u be an inverse for the element m and observe

$m * x = n \Rightarrow u * (m * x) = u * n$ (Apply u to both sides of the equation.)

$\Rightarrow (u * m) * x = u * n$ (Apply the associative property.)

$\Rightarrow \varepsilon * x = u * n$

$\Rightarrow x = u * n$ (Apply the fact that ε is the identity element.)

Consequently, this equation has *at least one* solution. Now, Problem 5 (b) tells us that the element u is unique --- in other words, u is the only inverse for m. Therefore, we may conclude this equation has *exactly one* solution.

The proof that the equation $x * m = n$ has exactly one solution is similar and will be left as an exercise.

Conversely, suppose that $\boldsymbol{\mathcal{X}}$ is a group. This means that every equation $m * x = n$ and $x * m = n$ has a unique solution. We need to prove that the algebra $\boldsymbol{\mathcal{X}}$ possesses an identity element, and we must prove that every member of the set X has an inverse.

Let $a \in X$. By assumption, we know that the equation $a * x = a$ has a unique solution. Let $x = \partial$ be this solution. Observe that

$a * \partial = a \Rightarrow (a * \partial) * a = a * a$ (Apply a to the right on both sides of the equation.)

$\Rightarrow a * (\partial * a) = a * a$ (Apply the associative property.)

$\Rightarrow \partial * a = a$ (Apply the Cancellation Law.)

(Recall that you proved the Cancellation Laws hold for any Sudoku algebra in the homework for Investigation 4.) Consequently, we may conclude that $\partial * a = a$. Now, suppose that b is any member of the set X. Observe that

$\partial * a = a \Rightarrow b * (\partial * a) = b * a$ (Apply b to the left on both sides of the equation.)

$\Rightarrow (b * \partial) * a = b * a$ (Apply the associative property.)

$\Rightarrow b * \partial = b$ (Apply the Cancellation Laws.)

Now, observe

$b * \partial = b \Rightarrow (b * \partial) * b = b * b$ (Apply a to the right on both sides of the equation.)

$\Rightarrow b * (\partial * b) = b * b$ (Apply the associative property.)

$\Rightarrow \partial * b = b$ (Apply the Cancellation Laws.)

We have shown that for all $b \in X$, we have $\partial * b = b$ and $b * \partial = b$; consequently, the element ∂ serves as an identity for the algebra $\boldsymbol{X}$.

To complete the proof, we will need to show that every member of the set X has an inverse in the algebra $\boldsymbol{X}$. To this end, let $a \in X$. We know that the equation $a * x = \partial$ has a unique solution. Let $x = u$ be this solution. We need to show that $u * a = \partial$ as well. Observe that

$a * u = \partial \Rightarrow (a * u) * a = \partial * a$ (Apply a to the right on both sides of the equation.)

$\Rightarrow a * (u * a) = \partial * a$ (Apply the associative property.)

$\Rightarrow a * (u * a) = a * \partial$ (Apply the fact that a and ∂ commute.)

$\Rightarrow u * a = \partial$ (Apply the Cancellation Laws.)

QED

Special Notation for Inverses

Suppose that $\boldsymbol{X} = (X,*)$ is a group. If $a \in X$, then we know that a has exactly one inverse in the algebra $\boldsymbol{X}$. It is traditional to let a^{-1} represent the inverse of a with respect to the operation *.

The usual way to show that an algebra $\boldsymbol{X} = (X,*)$ is a group is to prove that

1. The operation * is associative.
2. The algebra possesses an identity element.
3. Every member of X has an inverse with respect to the operation *.

Problem 6. Consider the set $\mathbb{Z}$ of integers.

Part (a). Is the algebra $\boldsymbol{\mathcal{Z}} = (\mathbb{Z}, +)$ of integers under addition a group? Justify your answer.

Part (b). Is the algebra $\boldsymbol{\mathcal{Z}^m} = (\mathbb{Z}, \cdot)$ of integers under multiplication a group? Justify your answer.

Permutations on a Set

Let X be any nonempty set. A *permutation* on the set X is a member of the family $[X \to X]$ that is both one-to-one and onto. We will let $\mathcal{P}_X$ denote the family of all permutations on the set X.

Problem 7. Let X be any nonempty set.

Part (a). If $f, g \in \mathcal{P}_X$, prove the composition $f \circ g$ is also a member of $\mathcal{P}_X$.

Part (b). Show that the function $\varepsilon: X \to X$ defined by $\varepsilon(x) = x$ serves as an identity element for the algebra $\boldsymbol{\mathcal{P}_X} = (\mathcal{P}_X, \circ)$.

Part (c). For each $f \in \mathcal{P}_X$, let g represent the inverse function for f. (Why do we know that g exists?) Prove that g serves as an inverse for the function f in the algebra $\boldsymbol{\mathcal{P}_X}$.

Homework.

Problem 1. Let $S = \{5, 15, 25, 35\}$.

Part (a). Fill in the table below.

$\boxtimes_{40}$	5	15	25	35
5				
15				
25				
35				

Part (b). Does the set S form a group under multiplication modulo 40? Explain how you decided.

Problem 2. Let $X = \mathbb{R} - \{0,1\}$ and the following members of $[X \to X]$.

$$\varepsilon(x) = x \qquad q(x) = 1 - x \qquad r(x) = \frac{1}{x} \qquad s(x) = \frac{1}{1-x} \qquad t(x) = \frac{x}{x-1} \qquad u(x) = \frac{x-1}{x}$$

Part (a). Fill in the table below. (Here $\circ$ represents function composition.)

$\circ$	ε	q	r	s	t	u
ε						
q						
r						
s						
t						
u						

Part (b). Explain why the set $CR = \{\varepsilon, q, r, s, t, u\}$ forms a group under function composition. (This group is called the *cross-ratio* group.)

Problem 3. Let $X = \{1,2,3,4,5\}$. The functions $f: X \to X$ defined by

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad g: \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

are permutations on the set X.

Part (a). Write the inverse for f and the inverse for g in the group $\boldsymbol{\mathcal{P}_X}$ using tabular notation. How did you determine the formula for the inverses?

Part (b). Use tabular notation to construct the formula for the following permutations on X.

$$f^{-1} \circ g \circ f \qquad \text{and} \qquad g \circ f \circ g^{-1}$$