In the previous investigation, we devised a strategy that can be used to determine when two groups are mathematically indistinguishable. In this section, we introduce a way to determine when one group is *part* of another group, but not necessarily identical to it.

Subgroup of a Group

Suppose that $\boldsymbol{\mathcal{X}} = (X,*)$ is a group. We say that a subset H of the universe X is a *subgroup* of the group $\boldsymbol{\mathcal{X}}$ provided the set H is a group in its own right under the operation *. In other words,

1. The set H is closed under the binary rule *.
2. There is an identity element for the set H under the operation *.
3. Every member of H has an inverse (relative to the identity for H) under the operation *.

Problem 1. Consider the group $\boldsymbol{\mathcal{Z}} = (\mathbb{Z}, +)$ of integers under addition. Is the set $\mathbb{Z}^+$ of positive integers a subgroup of the group $\boldsymbol{\mathcal{Z}}$? Justify your answer.

Problem 2. Let n be a fixed positive integer. Is the set $n\mathbb{Z}$ of multiples of n a subgroup of $\boldsymbol{\mathcal{Z}}$? Justify your answer.

Problem 3. Identify all of the subgroups of the group $\boldsymbol{\mathcal{S}}_\Delta$ of triangle symmetries. Are any of these subgroups cyclic?

Problem 4. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and suppose that $H \subseteq X$ is a subgroup of $\boldsymbol{\mathcal{X}}$. Let ε be the identity for X under $*$, and let δ be the identity for H under $*$.

Part (a). Prove that we must have $\varepsilon = \delta$. (Hint: Let $a \in H$ and carefully consider the equation $a * x = a$.)

Part (b). Let $a \in H$, and suppose that a^{-1} represents the inverse for a in the group $\boldsymbol{\mathcal{X}}$. Prove that $a^{-1} \in H$ as well.

Problem 5. Complete the proof of the following result.

Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and suppose that $H \subseteq X$ is nonempty. If $a * b^{-1} \in H$ for all $a, b \in H$, then H is a subgroup of $\boldsymbol{\mathcal{X}}$.

Proof. Let ε represent the identity for the group $\boldsymbol{\mathcal{X}}$. We will first prove that $\varepsilon \in H$. We know that H is nonempty, so let $a \in H$.

[Fill this in]

Therefore, we may conclude that $\varepsilon \in H$.

Next, we will prove that if $a \in H$, then $a^{-1} \in H$ as well. To this end, suppose $a \in H$. Since $\varepsilon \in H$, we know by assumption that…

[Fill this in.]

Therefore, we may conclude that $a^{-1} \in H$.

Finally, we prove that H is closed under the binary rule $*$. To this end, let $a, b \in H$. We need to show that $a * b \in H$.

[Fill this in.]

Problem 6. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and let $a \in X$. Use Problem 5 to prove that $H = \{a^n : n \in \mathbb{Z}\}$ is always a subgroup of $\boldsymbol{\mathcal{X}}$.

Problem 7. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and let $\boldsymbol{\mathcal{Y}} = (Y,\diamond)$ be another group such that $f : X \to Y$ is a homomorphism from $\boldsymbol{\mathcal{X}}$ to $\boldsymbol{\mathcal{Y}}$. Let ε be the identity for $\boldsymbol{\mathcal{Y}}$ and let

$$\mathrm{Ker}(f) = \{a \in X : f(a) = \varepsilon\}$$

Use Problem 5 and the properties of homomorphisms to show that $\mathrm{Ker}(f)$ is always a subgroup of $\boldsymbol{\mathcal{X}}$. (This subgroup is called the *kernel* of the homomorphism f.)

Problem 8. A subset A of a set X is *proper* provided $A \neq X$. Suppose that $\boldsymbol{\mathcal{X}} = (X,*)$ is a finite group. Is it possible for $\boldsymbol{\mathcal{X}}$ to be isomorphic to a proper subgroup of itself? Justify your answer.

Homework.

Problem 1. Construct all of the subgroups of the group $\boldsymbol{\mathcal{Z}_{12}} = (\mathbb{Z}_{12}, \boxplus_{12})$.

Problem 2. There are ten subgroups of the group $\boldsymbol{\mathcal{S}}_{\times}$ of cross symmetries. Construct all ten of these subgroups.

Problem 3. Let n be any fixed nonnegative integer. Show that the set $n\mathbb{Z}$ of all integer multiples of n is always a subgroup of the group $\boldsymbol{\mathcal{Z}} = (\mathbb{Z}, +)$.

Let $U_{2,2}$ represent the set of all nonsingular (invertible) 2×2 matrices with real number entries. In linear algebra, you showed that matrix multiplication is associative. If we let $*$ represent 2×2 matrix multiplication, then $\boldsymbol{GL_2} = (U_{2\times 2}, *)$ forms a group (called the *General Linear Group*). The identity for this group is the 2×2 identity matrix, and for each $A \in U_{2\times 2}$, we have

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \Rightarrow \quad A^{-1} = \left(\frac{1}{ad - bc}\right)\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

The real number $ad - bc$ is called the *determinant* of the matrix A and is often denoted by $\mathrm{Det}(A)$.

Problem 4. Consider the following collection of matrices from the universe $U_{2\times 2}$.

$$H = \{A \in U_{2\times 2} : \mathrm{Det}(A) = 1\}$$

Prove that H is a subgroup of the General Linear Group. (You may consult a linear algebra text to refresh your memory on the properties of determinants. Be careful to indicate which properties you use.)

Problem 5. Prove that the group $\boldsymbol{\mathcal{Z}} = (\mathbb{Z}, +)$ is isomorphic to its subgroup $n\mathbb{Z}$ for any fixed *positive* integer n. (Compare to Problem 8 in this investigation.)

Problem 6. Complete the proof of the following result.

If H is any subgroup of the group $\boldsymbol{\mathcal{Z}} = (\mathbb{Z}, +)$ that contains at least two elements, then $H = n\mathbb{Z}$ for some positive integer n.

Proof. We are assuming that H contains at least two elements; hence, we know there exist nonzero $a \in H$. It follows that either $a > 0$ or $-a > 0$. Consequently, we know that H must contain positive elements.

[Why can we conclude this?]

Since the set of positive members of H is nonempty, we know that H contains a *smallest* positive member. Call this member n.

Since $n \in H$, we know that $ny \in H$ for every integer y.

[Why do we know this?]

Consequently, we may conclude that $n\mathbb{Z} \subseteq H$. We must prove that $H \subseteq n\mathbb{Z}$. To this end, let $x \in H$. The Division Algorithm tells us there exist unique integers q, r such that $0 \leq r < n$ and $x = nq + r$.

We know that $r \in H$.

[Why do we know this?]

However, since $r < n$, it follows that we must conclude $r = 0$.

[Why must we conclude this?]

Thus, we know that $x = nq$, and we may conclude that $x \in n\mathbb{Z}$. We have proven that $H \subseteq n\mathbb{Z}$, as desired.