A function between two groups that preserves the group operation is called a group *homomorphism*. To be precise, suppose that $\boldsymbol{\mathcal{X}} = (X,*)$ and $\boldsymbol{\mathcal{Y}} = (Y,\odot)$ are groups. A group *homomorphism from* $\boldsymbol{\mathcal{X}}$ *to* $\boldsymbol{\mathcal{Y}}$ is a function $f : X \to Y$ with the property that $f(a * b) = f(a) \odot f(b)$ for all $a, b \in X$.

All isomorphisms are group homomorphisms. However, since we do not require group homomorphisms to be bijections, there exist group homomorphisms which are not isomorphisms.

Problem 1. Let $\boldsymbol{\mathcal{X}} = (X,*)$ and $\boldsymbol{\mathcal{Y}} = (Y,\odot)$ be groups, and consider the product group $\boldsymbol{\mathcal{X}} \times \boldsymbol{\mathcal{Y}}$. Let $\pi_X : X \times Y \to X$ be defined by $\pi_X[(a,b)] = a$. Show that π_X is a group homomorphism from $\boldsymbol{\mathcal{X}} \times \boldsymbol{\mathcal{Y}}$ to $\boldsymbol{\mathcal{X}}$.

Of course, the function $\pi_Y : X \times Y \to Y$ be defined by $\pi_X[(a,b)] = b$ is also a group homomorphism from $\boldsymbol{\mathcal{X}} \times \boldsymbol{\mathcal{Y}}$ to $\boldsymbol{\mathcal{Y}}$. These two functions are called the *projection maps*.

Problem 2. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any group, and let $a \in X$ be fixed. Consider the function $L_a : X \to X$ defined by $L_a(x) = a * x$. What would have to be true in order for L_a to be a group homomorphism from $\boldsymbol{\mathcal{X}}$ to $\boldsymbol{\mathcal{X}}$?

Problem 3. Consider the group $\boldsymbol{\mathcal{Q}}^+ = (\mathbb{Q}^+,\cdot)$ of positive rational numbers under ordinary multiplication. Is the rule $f : \mathbb{Q}^+ \to \mathbb{Q}^+$ defined below a group homomorphism from $\boldsymbol{\mathcal{Q}}^+$ to $\boldsymbol{\mathcal{Q}}^+$? Be careful!

$$f\left(\frac{p}{q}\right) = q$$

Problem 4. In Homework Problem 5 of Investigation 7, you proved that isomorphisms preserve the identity and inverses. Look at your proof of this fact. Could your argument also be used to show that group homomorphisms preserve the identity and inverses? Explain.

Group Homomorphisms Preserve the Identity and Inverses

Theorem 10.1 Suppose that $\boldsymbol{X} = (X,*)$ and $\boldsymbol{Y} = (Y,\odot)$ are groups, and suppose that $h: X \to Y$ is a group homomorphism.

1. If ε is the identity of $\boldsymbol{X}$, then $f(\varepsilon)$ is the identity of $\boldsymbol{Y}$.
2. If $a \in X$, then $f(a^{-1})$ serves as the group inverse for $f(a)$ in $\boldsymbol{Y}$.

Problem 5. Let $\boldsymbol{X} = (X,*)$ be any group, and let $\boldsymbol{Y} = (Y,\diamond)$ be another group such that $f : X \to Y$ is a group homomorphism from $\boldsymbol{X}$ to $\boldsymbol{Y}$. Let ε be the identity for $\boldsymbol{Y}$ and let

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

Prove that $\ker(f)$ is always a subgroup of $\boldsymbol{X}$. (This subgroup is called the *kernel* of the group homomorphism f.)

Problem 6. Let $\boldsymbol{X} = (X,*)$ be any group, and let $\boldsymbol{Y} = (Y,\diamond)$ be another group such that $f : X \to Y$ is a group homomorphism from $\boldsymbol{X}$ to $\boldsymbol{Y}$. Let $a \in X$.

Part (a). Explain why we know $f(a^0) = [f(a)]^0$.

Part (b). Let n be a positive integer. Explain why we know $f(a^{-n}) = [f(a^n)]^{-1}$.

Part (c). Let n be a positive integer. Use the method of induction to prove that $f(a^n) = [f(a)]^n$.

Part (d). Use Part (b) and Part (c) to explain why $f(a^m) = [f(a)]^m$ for any *negative* integer m.

Recall that a group $\boldsymbol{\mathcal{X}} = (X,*)$ is *cyclic* provided $X = \text{Pow}[a]$ for some $a \in X$. We call a a *generator* for the group $\boldsymbol{\mathcal{X}}$.

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 group homomorphism from $\boldsymbol{\mathcal{X}}$ to $\boldsymbol{\mathcal{Y}}$. Suppose that H is a subgroup of $\boldsymbol{\mathcal{X}}$ and let

$$f(H) = \{f(a) : a \in H\}$$

Part (a). Prove that $f(H)$ is a subgroup of $\boldsymbol{\mathcal{Y}}$.

Part (b). If H is cyclic with generator a, prove that $f(H)$ is cyclic with generator $f(a)$.

Homework.

Problem 1. Consider the group $\boldsymbol{\mathcal{R}}^* = (\mathbb{R}^*,\cdot)$ of nonzero real numbers under ordinary multiplication, and let $\boldsymbol{\mathcal{R}}^+ = (\mathbb{R}^+,\cdot)$ be the group of positive real numbers under ordinary multiplication. Let m be any even integer, let n be any odd integer, and consider the function $f : \mathbb{R}^* \to \mathbb{R}^+$ defined by $f(x) = x^{m/n}$. Prove that f is a group homomorphism from $\boldsymbol{\mathcal{R}}^*$ to $\boldsymbol{\mathcal{R}}^+$.

Problem 2. Let $\boldsymbol{\mathcal{X}} = (X,*)$ be any commutative group. Prove that the function $f : X \to X$ defined by $f(a) = a^{-1}$ is a group homomorphism. Is this an isomorphism?

Problem 3. Let n be a fixed positive integer and consider the function $R : \mathbb{Z} \to \mathbb{Z}_n$ defined by the formula $R(a) = r$, where r is the remainder for a relative to n. In this exercise, we will use results from Investigation 4 to prove that that f is a group homomorphism from $\boldsymbol{\mathcal{Z}}$ to $\boldsymbol{\mathcal{Z}}_n$.

Part (a). Let $a, b \in \mathbb{Z}$, and let $R(a) = r$, $R(b) = s$. Use Problems 3 and 5 from Investigation 4 to explain why we know $r \boxplus_n s \equiv [a + b] \text{mod}(n)$.

Part (b). Use Part (a) and Problems 3 and 4 from Investigation 4 to explain why $r \boxplus_n s = R(a+b)$.

Part (c). Complete the proof that R is a group homomorphism from $\boldsymbol{\mathcal{Z}}$ to $\boldsymbol{\mathcal{Z}}_n$.

Problem 4. . 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 group homomorphism from $\boldsymbol{\mathcal{X}}$ to $\boldsymbol{\mathcal{Y}}$. Suppose H is a subgroup of $\boldsymbol{\mathcal{Y}}$, and let

$$\text{Pre}_f(H) = \{a \in X : f(a) \in H\}$$

Prove that $\text{Pre}_f(H)$ is a subgroup of $\boldsymbol{\mathcal{X}}$.

Problem 5. Let n be a fixed positive integer. We know the function $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by the formula $f(a) = a \bmod(n)$ is a group homomorphism from $\boldsymbol{\mathcal{Z}}$ to $\boldsymbol{\mathcal{Z}}_n$. This function is clearly a surjection. (Surjective group homomorphisms are called group *epimorphisms*.)

Part (a). Suppose H is any subgroup of $\boldsymbol{\mathcal{Z}}_n$. Use Problem 4 and Homework Problem 7 of Investigation 9 to explain why $\text{Pre}_f(H)$ is cyclic.

Part (b). Explain why we must conclude that every subgroup of $\boldsymbol{\mathcal{Z}}_n$ is cyclic.

Part (c). Use Part (b) and Homework Problem 7 of Investigation 7 to help prove the following result.

- If $\boldsymbol{\mathcal{X}} = (X,*)$ is any finite cyclic group, then every subgroup of $\boldsymbol{\mathcal{X}}$ is also cyclic.