CHAPTER 2 — INTRODUCING GROUPS

1 What is a Group?

One of the goals of modern algebra is to study the properties of systems in which certain types of algebraic equations can be solved. The simplest of all such systems is called a *group*. A group is a set endowed with a binary operation $*$ which has just enough properties to make it possible to solve the equations $a * x = b$ and $x * a = b$ for the variable x. Here is the fundamental definition.

Definition 1 *A **group** is a set G endowed with a binary operation $*$ which satisfies the following conditions:*

1. *The operation is associative; that is, $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.*
2. *The set G has an **identity element** under the operation $*$; that is, there exists an element $e \in G$ such that $e * a = a = a * e$ for all $a \in G$.*
3. *Every member of G has an **inverse** under $*$; that is, for all $a \in G$, there exist $b \in G$ such that $a * b = e = b * a$.*

The set G is called the *universe* of the group; it is common to write $\mathcal{G} = (G, *)$ to indicate a group, especially when we need to give a symbol for the operation and the universe. It is common to call the binary operation a *multiplication* on the set G; and, when no confusion will result, we often simply write ab instead of $a * b$. Notice that the binary operation for a group is not required to be commutative. A group endowed with a commutative binary operation is called a *commutative* group or an *abelian* group. (The term "abelian" refers to Niels Abel, a Norwegian mathematician who was a pioneer in group theory in the nineteenth century.) You are actually familiar with a number of abelian groups. For example,

- The pair $\mathcal{Z} = (\mathbb{Z}, +)$ of integers under integer addition is an abelian group. The number 0 serves as an identity element; and, for each $m \in \mathbb{Z}$, the number $-m$ serves as an inverse.
- Likewise, the pairs $\mathcal{Q} = (\mathbb{Q}, +)$ and $\mathcal{R} = (\mathbb{R}, +)$ of rational and real numbers under addition, respectively, are abelian groups. In both, the number 0 serves as an identity element, and for each m in $\mathbb{Q}$ or $\mathbb{R}$, the number $-m$ serves as an inverse.
- The pairs $\mathcal{Q}^* = (\mathbb{Q}^*, \cdot)$ and $\mathcal{R}^* = (\mathbb{R}^*, \cdot)$ of *nonzero* rational and real numbers under multiplication, respectively, are abelian groups. In both, the number 1 serves as an identity element, and for each m in $\mathbb{Q}^*$ or $\mathbb{R}^*$, the number $1/m$ serves as an inverse.

Nonabelian groups abound as well, and you have already had exposure to some of these.

Example 2 *Let X be any nonempty set and show that $(\wp_X, \circ)$ is a group, where $\circ$ denotes function composition.*

Solution. Recall that $\wp_X$ is the family of permutations on X (see Definition 1.56 and the examples which follow it). Theorem 1.44 and Exercises 1.5.12 and 1.5.13 together show that function composition is an associative binary operation on $\wp_X$. To see that $(\wp_X, \circ)$ is a group, we need to show that Group Axioms 2 and 3 are met. Exercise 1.5.10 tells us that the identity function ϵ_X serves as an identity element for $\wp_X$. Theorem 1.47 tells us that every member of $\wp_X$ has a full inverse which is necessarily also a member of $\wp_X$. If $\alpha \in \wp_X$, then let α^{-1} denote its full inverse and observe that

$$\alpha \circ \alpha^{-1} = \epsilon_X = \alpha^{-1} \circ \alpha$$

Consequently, we know that Groups Axioms 2 and 3 are met; and we may conclude that $(\wp_X, \circ)$ is a group.

Example 1.57 shows that function composition is not commutative on $\wp_X$ whenever X contains at least three elements; consequently, nonabelian groups are very abundant. Consider, for example, the group $\mathcal{P}_3 = (\wp_3, \circ)$ of permutations on the three-element set $X = \{1, 2, 3\}$. We examined this group closely in Example 1.58, where we constructed its operation table. Let's take a closer look at this table.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$	$\boldsymbol{\delta}$	$\boldsymbol{\zeta}$
$\boldsymbol{\epsilon}$	ϵ	α	β	γ	δ	ζ
$\boldsymbol{\alpha}$	α	ϵ	δ	ζ	β	γ
$\boldsymbol{\beta}$	β	ζ	ϵ	δ	γ	α
$\boldsymbol{\gamma}$	γ	δ	ζ	ϵ	α	β
$\boldsymbol{\delta}$	δ	γ	α	β	ζ	ϵ
$\boldsymbol{\zeta}$	ζ	β	γ	α	ϵ	δ

The symbols in the table represent the six the permutations on X and are defined in Example 1.58. When confronted with an operation table, it is easy to see whether or not the operation it summarizes is a group operation. (Once you have established that the operation is associative.) An identity element is particularly easy to spot — just look for an element whose row and column exactly reproduce the Zero Row and the Zero Column. In the table above, the element ϵ has this property and hence serves as an identity element for $\wp_3$ under $\circ$. (Of course, we already know that the identity function serves as an identity element for this set.) To see if a particular element x has an inverse, look for an identity in the x-row. If you find one, look to see if that identiy is paired with the same element in the x-column. If so, then that element serves as an inverse for x. For example, checking the table we see that ϵ, α, β and γ serve as their own inverses, while ζ is an inverse for δ and vice-versa.

The operation table for $\mathcal{P}_3 = (\wp_3, \circ)$ shows us directly that ϵ is the *only* identity for $\wp_3$ under function composition. The table also shows us that every element of $\wp_3$ has *only one* inverse under function composition. The table also shows us something more subtle — every member of $\wp_3$ appears *exactly once* in each row and column of the operation table, if we don't count the Zero Row and Zero Column. (In other words, each row and column of the table is a permutation on $\wp_3$.) All of these features turn out to be properties of groups in general, as the following result shows.

Theorem 3 *If $\mathcal{G} = (G, *)$ is a group, then the following statements are true:*

1. *The group has exactly one identity element.*
2. *Every element has exactly one inverse.*
3. *For every fixed $a \in G$, the functions $f : G \longrightarrow G$ and $g : G \longrightarrow G$ defined by $f(x) = a * x$ and $g(x) = x * a$ are bijections.*

Proof. To prove Claim (1), suppose that u and v are identity elements for G under this operation. We will prove that $u = v$. To this end, observe that since v is an identity element, we know $v * u = u$. However, since u is also an identity element, we know that $v * u = v$. Consequently, we know

$$u = v * u = v$$

To prove Claim (2), let $a \in G$ and suppose that u and v are inverses for a under the operation $*$. We will prove that $u = v$. To this end, suppose that e is the identity element. It follows that $a * u = e$ and it follows that $v * a = e$. With this in mind, observe that

$$\begin{aligned} a * u = e &\implies v * (a * u) = v * e \\ &\implies (v * a) * u = v * e \\ &\implies e * u = v * e \\ &\implies u = v \end{aligned}$$

It remains to prove Claim (3). We will show that f is a bijection and leave verification for g as an exercise. Suppose $b \in G$. Since G is a group, we know that the inverse for a exists; call it α. Since G is closed under $*$, we know that the element $x = \alpha * b$ exists in G. Therefore, since $*$ is assumed to be associative, we see that

$$f(x) = a * (\alpha * b) = (a * \alpha) * b = e * b = b$$

Consequently, we may conclude that f is onto. Now, suppose that $x, y \in G$ are such that $f(x) = f(y)$. This tells us that $a * x = a * y$. Once again, since $*$ is assumed to be associative, we see that

$$\begin{aligned} a * x = a * y &\implies \alpha * (a * x) = \alpha * (a * y) \\ &\implies (\alpha * a) * x = (\alpha * a) * y \\ &\implies e * x = e * y \\ &\implies x = y \end{aligned}$$

Consequently, we may conclude that f is one-to-one.

QED

Since the inverse of any group element is unique, we are justified in denoting it by a special symbol. Borrowing the full inverse notation from functions, if $\mathcal{G} = (G, *)$ is a group and $a \in G$, it is customary to let a^{-1} represent its inverse *regardless of what the operation may be.* It is important to keep the underlying group operation in mind when working with inverses, because the nature of the inverse can change dramatically. For example, the integer 2 is a member of the groups $\mathcal{Q}^* = (\mathbb{Q}^*, \cdot)$ and $\mathcal{Z} = (\mathbb{Z}, +)$. However, the inverse of 2 is completely different in these groups.

- In $\mathcal{Q}^* = (\mathbb{Q}^*, \cdot)$, we have $2^{-1} = 1/2$.
- In $\mathcal{Z} = (\mathbb{Z}, +)$, we have $2^{-1} = -2$.

Claim (3) in the theorem above is what tells us that every element of a finite group appears exactly once in each row and column of its operation table. (The Claim holds true for infinite groups as well, but we obviously do not construct operation tables for infinite groups.) The reason Claim (3) tells us this is simply because the bijections f and g represent the a-row and the a-column, respectively, in the operation table. Claim (3) has deeper consequences that we will explore later.

The group axioms appearing in Definition 1 above are sufficient to solve equations of the form $a * x = b$ and $x * a = b$ for the variable x. For example, observe that

$$\begin{aligned} a * x = b &\implies a^{-1} * (a * x) = a^{-1} * b && \\ &\implies (a^{-1} * a) * x = a^{-1} * b && \text{Operation is associative} \\ &\implies e * x = a^{-1} * b && a^{-1} * a = e \\ &\implies x = a^{-1} * b && e * x = x \end{aligned}$$

The solution to the equation $x * a = b$ is the element $x = b * a^{-1}$. The solutions to $a * x = b$ and $x * a = b$ may not be the same if the group is nonabelian. As an example, consider the equations $\delta \circ x = \alpha$ and $x \circ \delta = \alpha$ in the group $\mathcal{P}_3 = (\wp_3, \circ)$. Using the operaton table above, we see that

$$\begin{aligned} \delta \circ x = \alpha &\implies x = \delta^{-1} \circ \alpha \implies x = \zeta \circ \alpha \implies x = \beta \\ x \circ \delta = \alpha &\implies x = \alpha \circ \delta^{-1} \implies x = \alpha \circ \zeta \implies x = \gamma \end{aligned}$$

Example 4 *Let n be a fixed positive integer and show that the pair $\mathcal{Z}_n = (\mathbb{Z}_n, \boxplus_n)$ is an abelian group, where $\boxplus_n$ denotes addition modulo n.*

Solution. In Exercise 1.6.13, you proved that $\boxplus_n$ is commutative and associative. Consequently, we only need to verify that Group Axioms 2 and 3 hold. Since $0 + a = a$ for any integer a, it should be clear that $[0]_n$ serves as the identity element for $\mathcal{Z}_n$. Suppose that $[a]_n \in \mathbb{Z}_n$ and observe that

$$[a]_n \boxplus_n [-a]_n = [a - a]_n = [0]_n$$

Consequently, we know that $[-a]_n$ serves as the inverse for $[a]_n$.

****

Notice that in the last example we did not check to see if $[-a]_n \boxplus_n [a]_n = [0]_n$. There is no need to check this because the operation $\boxplus_n$ is commutative. When trying to verify that a set is a group under an operation, it is always a good idea to see if the operation is commutative before tackling the group axioms, since commutativity cuts the workload in half. This is especially true if the operation is defined by a table and we are trying to verify associativity using case-by-case analysis.

Consider the operation table for $\mathcal{Z}_4 = (\mathbb{Z}_4, \boxplus_4)$ shown below.

$\boxplus_4$	$[\mathbf{0}]_4$	$[\mathbf{1}]_4$	$[\mathbf{2}]_4$	$[\mathbf{3}]_4$
$[\mathbf{0}]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[\mathbf{1}]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[\mathbf{2}]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[\mathbf{3}]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Notice that once again every element appears exactly once in every row and every column (not counting the Zero Row and Zero Column of course). The table shows us that $[0]_4$ serves as the identity element, as predicted in the previous example. Notice that the table tells us $[1]_4$ is the inverse of $[3]_4$. At first, this might seem out of line with the previous example, which predicts that the inverse of $[3]_4$ is $[-3]_4$. However, since

$$1 \equiv -3 \texttt{MOD}(4)$$

this is not the problem it first seems to be. We see that 1 and -3 are merely different representatives for the same residue class.

Example 5 *Let M_2 denote the set of all 2×2 matrices with real entries and nonzero determinant. In other words, let*

$$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$$

Show that $\mathcal{M}_2 = (M_2, *)$ is a nonabelian group, where $*$ denotes matrix multiplication.

Solution. To see why this is so, first recall that the product of two 2×2 matrices is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} u & v \\ w & x \end{bmatrix} = \begin{bmatrix} au + bw & av + bx \\ cu + dw & cv + dx \end{bmatrix}$$

To see that $*$ is indeed an operation on M_2, we need to show that

$$(au + bw)(cv + dx) - (av + bx)(cu + dw) \neq 0$$

whenever $ad - bc \neq 0$ and $ux - vw \neq 0$. To this end, first observe that

$$\begin{aligned} (au + bw)(cv + dx) - (av + bx)(cu + dw) = 0 &\implies aucv + audx + bwcv + bwdx - avcu - avdw - bxcu - bxdw = 0 \\ &\implies ux(ad - bc) - vw(ad - bc) = 0 \\ &\implies (ad - bc)(ux - vw) = 0 \end{aligned}$$

Therefore, we can have $(au+bw)(cv+dx)-(av+bx)(cu+dw)=0$ only if $ad-bc=0$ or $ux-vw=0$. We may conclude that $*$ is indeed a binary operation on M_2. We next observe that matrix multiplication is unfortunately not a commutative operation on M_2. Indeed, observe that

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} * \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ 20 & 11 \end{bmatrix} \qquad \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 11 & 20 \\ 5 & 8 \end{bmatrix}$$

To see that $\mathcal{M}_2=(M_2,*)$ is a group, we need to verify the three group axioms. First, we note that the so-called *identity matrix*

$$I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

serves as the identity element for M_2 under matrix multiplication, since

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} u & v \\ w & x \end{bmatrix} = \begin{bmatrix} 1(u)+0(w) & 1(v)+0(x) \\ 0(u)+1(w) & 0(v)+1(x) \end{bmatrix} = \begin{bmatrix} u & v \\ w & x \end{bmatrix}$$

$$\begin{bmatrix} u & v \\ w & x \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} u(1)+w(0) & v(1)+x(0) \\ u(0)+w(1) & v(0)+x(1) \end{bmatrix} = \begin{bmatrix} u & v \\ w & x \end{bmatrix}$$

To see that every member of M_2 has an inverse under matrix multiplication, first, let

$$A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

be any member of M_2. We basically solve the equation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} u & v \\ w & x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

for the variables u,v,w,x. Notice that this equation gives us the following system of linear equations:

$$\begin{cases} au & & +bw & & & = 1 \\ & av & & & +bx & = 0 \\ cu & & +dw & & & = 0 \\ & cv & & & +dx & = 1 \end{cases}$$

A bit of algebra shows that there is a unique solution to this system of equations; it is summarized by the matrix

$$B=\begin{bmatrix} \dfrac{d}{ad-bc} & -\dfrac{b}{ad-bc} \\ -\dfrac{c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Solving the system of equations above guarantees that $A*B=I$. We only need to prove that $B\circ A=I$ to establish that B is the inverse of A. Observe that

$$B*A=\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = I$$

The last thing we must do in order to establish that $\mathcal{M}_2=(M_2,\circ)$ is a group is to prove that matrix multiplication is associative. This is a standard exercise in linear algebra, but let's see how it plays out in this limited arena. Let A,B,C be any members of M_2. We need to prove that $A*(B*C)=(A*B)*C$. To this end, let

$$A=\begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad B=\begin{bmatrix} m & n \\ p & q \end{bmatrix} \qquad C=\begin{bmatrix} u & v \\ w & x \end{bmatrix}$$

Taking advantage of the fact that real number addition and multiplication are associative and that addition is commutative, we see that

$$\begin{aligned}
A*(B*C) &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \left(\begin{bmatrix} m & n \\ p & q \end{bmatrix} * \begin{bmatrix} u & v \\ w & x \end{bmatrix} \right) \\
&= \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} mu+nw & mv+nx \\ pu+qw & pv+qx \end{bmatrix} \\
&= \begin{bmatrix} a(mu+nw)+b(pu+qw) & a(mv+nx)+b(pv+qx) \\ c(mu+nw)+d(pu+qw) & c(mv+nx)+d(pv+qx) \end{bmatrix} \\
&= \begin{bmatrix} (am+bp)u+(an+bq)w & (am+bp)v+(an+bq)x \\ (cm+dp)u+(cn+dq)w & (cm+dp)v+(cn+dq)x \end{bmatrix} \\
&= \begin{bmatrix} am+bp & an+bq \\ cm+dp & cn+dq \end{bmatrix} * \begin{bmatrix} u & v \\ w & x \end{bmatrix} \\
&= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} m & n \\ p & q \end{bmatrix} \right) * \begin{bmatrix} u & v \\ w & x \end{bmatrix} = (A*B)*C
\end{aligned}$$

We have now established that $\mathcal{M}_2 = (M_2, \circ)$ is a group. In some branches of mathematics, this system is called the 2×2 *General Linear Group* and is denoted by $GL(2)$. We will simply call it $\mathcal{M}_2$.

****

Example 6 *Explain why the whole numbers* ***do not*** *form a group under integer addition.*

Solution. Integer addition is a binary operation on the set $\mathbb{W}$ of whole numbers, so we can talk about the pair $\mathcal{W} = (\mathbb{W}, +)$. The whole number 0 certainly serves as an indentity; however, the number 1 does not have an inverse. This is because the equation

$$1 + x = 0$$

has no solution in the set $\mathbb{W}$.

****

Example 7 *Let* $\mathbb{I} = (0, 1]$ *and consider the operation on* $\mathbb{I}$ *defined by*

$$a \circledast b = \begin{cases} ab & \text{if} \quad a < b \\ \dfrac{b}{a} & \text{if} \quad b \leq a \end{cases}$$

Example 8 *Is the pair* $(\mathbb{I}, \circledast)$ *a group?*

Solution. First, we need to decide whether $\circledast$ is a binary operation on $\mathbb{I}$. It is clear from the formula that $\circledast$ is a binary function from $\mathbb{I}$ to $\mathbb{R}^+$. However, this is not good enough. We must prove that $\circledast$ is a binary function from $\mathbb{I}$ to $\mathbb{I}$. Let $a, b \in (0, 1]$. If $a < b$, then we know

$$a \circledast b = ab < (1)(1) = 1$$

On the other hand, if $b \leq a$, then we know that $1/a \leq 1/b$, and this tells us that

$$a \circledast b = \frac{b}{a} = \left(\frac{1}{a}\right)(b) \leq \left(\frac{1}{b}\right)(b) = 1$$

Consequently, we see that $0 < a \circledast b \leq 1$; and we may conclude that $a \circledast b \in (0, 1]$. (We say that $\mathbb{I}$ is *closed under* $\circledast$.) We are therefore justified in considering the pair $(\mathbb{I}, \circledast)$. The number 1 serves as an identity element for $\mathbb{I}$ under $\circledast$. To see why, let $x \in \mathbb{I}$. Note that we always have $x \leq 1$. If $x = 1$, then we know that $x \circledast 1 = 1 \circledast 1 = 1/1 = 1 = x$. On the other hand, if $x < 1$, then we know

$$x \circledast 1 = x(1) = x \qquad\qquad 1 \circledast x = \frac{x}{1} = x$$

Consequently, we know that 1 serves as an identity element. Furthermore, every member of $\mathbb{I}$ has an inverse under $\circledast$. To see why, note that for all $a \in (0, 1]$, it is clear that $a \leq a$; consequently, we know that $a \circledast a = a/a = 1$. Therefore, every element is its own inverse.

We have shown that $\circledast$ is a binary operation on $\mathbb{I}$; and we have proven that Group Axioms 2 and 3 hold for $\mathbb{I}$ under $\circledast$. However, this is not enough to prove that $(\mathbb{I}, \circledast)$ is a group. It turns out that the operation $\circledast$ is *not* associative. Observe that

$$\left[\frac{1}{3} \circledast \frac{1}{2}\right] \circledast \frac{1}{4} = \frac{1}{24} \qquad\qquad \frac{1}{3} \circledast \left[\frac{1}{2} \circledast \frac{1}{4}\right] = \frac{1}{6}$$

Consequently, we are forced to conclude that $(\mathbb{I}, \circledast)$ is not a group.

****

Example 9 *Consider the operation $\sqcap$ defined on $\mathbb{R}^*$ by the formula $x \sqcap y = \dfrac{xy}{4}$. Is the pair $(\mathbb{R}^*, \sqcap)$ a group?*

Solution. First, we must verify that $\sqcap$ is a binary operation on $\mathbb{R}^*$. This is much easier than in the last example, however since the output of the arithmetic formula clearly produces a unique nonzero real number. Consequently, we know that $\sqcap$ is a binary operation on $\mathbb{R}^*$; and we are justified in considering the pair $(\mathbb{R}^*, \sqcap)$. Since associativity was the achilles' heel of the last example, we will start with this issue. Is $\sqcap$ associative? Let $a, b, c \in \mathbb{R}^*$ and observe that

$$a \sqcap (b \sqcap c) = a \sqcap \frac{bc}{4} = \frac{a(bc)}{16} = \frac{(ab)c}{16} = \frac{ab}{4} \sqcap c = (a \sqcap b) \sqcap c$$

The associativity of real number multiplication allows us to prove that $\sqcap$ is associative. Hence, the first group axiom is satisfied. Before continuing, it is a good idea to check for commutativity. Observe that

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

We may conclude that $\sqcap$ is a commutative operation, and this helps us in checking Group Axioms 2 and 3. Is there an identity element for $\mathbb{R}^*$ under $\sqcap$? Observe that since $a \neq 0$, we know

$$a \sqcap x = a \Longrightarrow \frac{ax}{4} = a \Longrightarrow x = 4$$

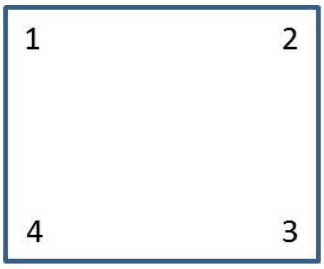
Commutativity allows us to conclude that $x = 4$ is the identity element for $\mathbb{R}^*$ under $\sqcap$ based on this solution. Notice that the assumption $a \in \mathbb{R}^*$ is critical for the existence of the identity, since the above equation has no *unique* solution if we allow $a = 0$. The identity element for a group must be unique. It remains to determine whether every element of $\mathbb{R}^*$ has an inverse under $\sqcap$. Since $a \neq 0$, we know

$$a \sqcap x = 4 \Longrightarrow \frac{ax}{4} = 4 \Longrightarrow x = \frac{4}{a}$$

Commutativity allows us to conclude that $x = 4/a$ is the inverse for a under $\sqcap$ based on this solution. The pair $(\mathbb{R}^*, \sqcap)$ is indeed an (abelian) group.

****

We conclude this section by introducing a family of finite groups which have many applications in the natural sciences and in art. Many geometric objects in two or three dimensions display certain *symmetries*; that is, it is possible to rotate the object through certain fixed angles, or to reflect the object about certain lines or planes and thereby obtain an object which occupies the same space as the original. To keep things simple, let's consider a square.Label the vertices of a square 1,2,3, and 4, clockwise starting at the upper left-hand corner.



There are eight basic movements that can be performed on the square which preserve its position in space:

- You can rotate the square clockwise through any angle coterminal with 0°, 90°, 180°, or 270°.
- You can flip the square around one of its four diagonals (two transverse diagonals, one horizontal, and one vertical).

It seems reasonable that every symmetry of the square results from some combination of these basic movements. Each of these motions permutes the numbered vertices of the square. Consequently, every basic motion corresponds to a permutation on the set $X = \{1, 2, 3, 4\}$. In particular, we have

$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ — rotation through 0° $\qquad R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ — rotation through 90°

$R_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ — rotation through 180° $\qquad R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ — rotation through 270°

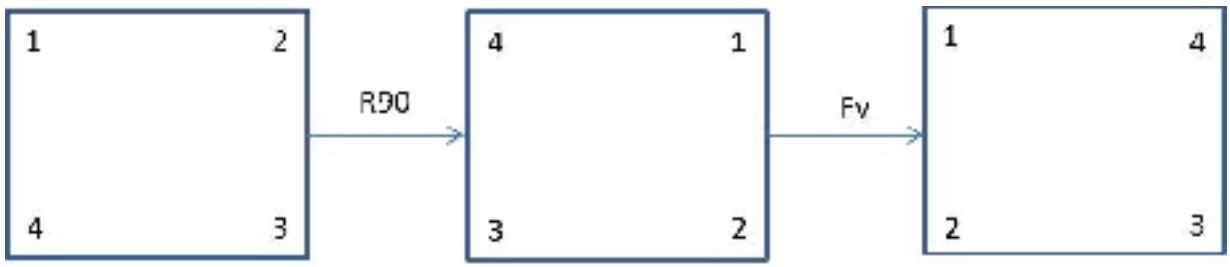
$F_{13} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ — flip around 1−3 diagonal $\qquad F_{24} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ — flip around 2−4 diagonal

$F_v = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ — flip vertical diagonal $\qquad F_h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ — flip horizontal diagonal

Let $\mathbb{O} = \{R_0, R_{90}, R_{180}, R_{270}, F_{13}, F_{24}, F_v, F_h\}$ and define a binary operation $\circ$ on this set by the rule

$$x \circ y \quad \text{means "perform motion } x \text{ after performing motion } y\text{"}$$

The first question you should ask is "Does $\circ$ actually define a binary operation on $\mathbb{O}$?" The answer is "yes"; and to see why, let's consider an example. Consider the motion $F_v \circ R_{90}$. According to our definition, this represents the motion "Flip about the vertical diagonal after rotating 90°clockwise." Here is a diagram showing this motion.



From this diagram, we can see that $F_v \circ R_{90}$ is another member of $\wp_4$; in fact,

$$F_v \circ R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = F_{13}$$

Our definition is nothing more than function composition in $\wp_4$. Therefore, to see that it is indeed an operation on $\mathbb{O}$, we simply need to determine whether or not $\mathbb{O}$ is closed under function composition. Here is the composition table for $\mathbb{O}$.

$\circ$	R_0	R_{90}	R_{180}	R_{270}	F_{13}	F_{24}	F_v	F_h
R_0	R_0	R_{90}	R_{180}	R_{270}	F_{13}	F_{24}	F_v	F_h
R_{90}	R_{90}	R_{180}	R_{270}	R_0	F_v	F_h	F_{24}	F_{13}
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_{24}	F_{13}	F_h	F_v
R_{270}	R_{270}	R_0	R_{90}	R_{180}	F_h	F_v	F_{13}	F_{24}
F_{13}	F_{13}	F_h	F_{24}	F_v	R_0	R_{180}	R_{270}	R_{90}
F_{24}	F_{24}	F_v	F_{13}	F_h	R_{180}	R_0	R_{90}	R_{270}
F_v	F_v	F_{13}	F_h	F_{24}	R_{90}	R_{270}	R_0	R_{180}
F_h	F_h	F_{24}	F_v	F_{13}	R_{270}	R_{90}	R_{180}	R_0

Since no new permutations appear in the table, we know that $\mathbb{O}$ is closed under function composition. Is the pair $(\mathbb{O}, \circ)$ a group? We already know that function composition is asscociative, so Group Axiom 1 is satisfied. It is easy to see from the table that R_0 serves as the identity element. (This should be no surprise since R_0 is really the identity permutation.) Hence, Group Axiom 2 is satisfied. Finally, we can see from the table that every element has an inverse under $\circ$; consequently, $\mathcal{O} = (\mathbb{O}, \circ)$ is indeed a group. It is traditonally called the *octic group*. Notice that the octic group is not abelian.

Any regular geometric object in two or three dimensions has a so-called *group of symmetries* associated with it. The octic group is the group of symmetries for the square. When the object is an n-gon, then the group of symmetries for that object can be constructed in the same way we built the octic group — it will be the subset of $\wp_n$ whose members represent all permutations of the n vertices that result from rotations or reflections about diagonals.

EXERCISES FOR SECTION 1

1. Let $\boldsymbol{i} = \sqrt{-1}$ and let $F = \{1, -1, \boldsymbol{i}, -\boldsymbol{i}\}$. Show that F forms an abelian group under complex multiplication. You may assume that complex multiplication is commutative and associative.

2. For a fixed positive integer n, let $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ denote the set of all integer multiples of n. Show that $n\mathbb{Z}$ is an abelian group under integer addition.

3. Is the set of odd integers a group under integer addition?

4. Show that the set $S = \{[5]_{40}, [15]_{40}, [25]_{40}, [35]_{40}\}$ forms a group under multiplication modulo 40 (see Exercise 1.6.16).

5. Explain why the set $\mathbb{Q}^*$ of nonzero rational numbers is not a group under division.

6. Let X be any nonempty set and let $\texttt{Sub}(X)$ denote the family of all subsets of X. Show that the pair $(\texttt{Sub}(X), \ominus)$ is an abelian group, where

$$A \ominus B = (A \cup B) - (A \cap B)$$

for all $A, B \in \texttt{Sub}(X)$. (This operation is called the *symmetric difference on* $\texttt{Sub}(X)$.) You will need to prove associativity.

7. Construct the operation table for $(\texttt{Sub}(X), \ominus)$ when $X = \{a, b, c\}$.

8. Show that the set $X = \mathbb{R} - \{-1\}$ is an abelian group under the operation $a \curlywedge b = a + b + ab$.

9. Is the set $\mathbb{R}$ of real numbers a group under the binary operation $a \circledcirc b = a^2 + 2ab + b^2$?

10. Is the set $S = \{x \in \mathbb{R} : -1 < x < 1\}$ a group under the binary operation

$$x \ltimes y = \frac{x + y}{1 + xy}$$

11. Verify that Row 3 of the operation table for the octic group is correct.

12. Verify that Column 5 of the operation table for the octic group is correct.

13. Construct the group of symmetries for an equliateral triangle.

14. Construct the group of symmetries for a rectangle.

15. Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. Explain why $(a^{-1})^{-1} = a$.

16. Let $\mathcal{G} = (G, *)$ be any group and let $a, b, c \in G$. Use the group axioms to solve the following equations for x.

    (a) $a * x * b = c$

    (b) $a^{-1} * x * a = b$

17. Use the formula for x you obtained in Exercise 16 to solve $a^{-1} * x * a = b$ in the following groups.

    (a) In the octic group, when $a = F_{24}$ and $b = R_{90}$

    (b) In the group $\mathcal{M}_2$, where $a = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$ and $b = \begin{bmatrix} 2 & 5 \\ 3 & 1 \end{bmatrix}$

18. Give a counterexample from the group $\mathcal{M}_2$ to show the equation $a * b * a^{-1} = b$ is not always true.

19. Explain why $\mathbb{Z}_n$ is not a group under mulitplication modulo n (see Exercises 1.6.16 and 1.6.17).

20. Let n be a fixed positive integer and let $\mathbb{U}_n = \{[a]_n \in \mathbb{Z}_n : \texttt{GCF}(a, n) = 1\}$. Show that $\mathcal{U}_n = (\mathbb{U}_n, \boxtimes_n)$ is an abelian group. (This is called the group of *units* modulo n.) Theorem 1.10 is very helpful here.

21. Construct the operation table for $\mathcal{U}_{12} = (\mathbb{U}_{12}, \boxtimes_{12})$.

22. Construct the operation table for $\mathcal{U}_{15} = (\mathbb{U}_{15}, \boxtimes_{15})$.

23. Consider the real-valued functions $f : \mathbb{R} - \{0, 1\} \longrightarrow \mathbb{R} - \{0, 1\}$ defined by the following formulas

$$\epsilon(x) = x \qquad q(x) = 1 - x \qquad r(x) = \frac{1}{x}$$

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

Let $F = \{\epsilon, q, r, s, t, u\}$ and construct the operation table for F under function composition. Explain why $(F, \circ)$ is a nonabelian group. (This group is traditonally called the *cross ratio group*.)

24. Let $\mathcal{G} = (G, *)$ be any group and let $a, b, c \in G$. Prove that $a * c = b * c$ implies $a = b$ and prove that $c * a = c * b$ implies $a = b$. (These are called the right and left *cancellation* laws.)

25. Give an example from the octic group to show that in a group $\mathcal{G} = (G, *)$, the equation $a * c = c * b$ does not necessarily imply that $a = b$.

26. Let $\mathcal{G} = (G, *)$ be any group and let $a, b \in G$. Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$. Hint: Show that $b^{-1} * a^{-1}$ is an inverse for $a * b$ by direct computation, then invoke Theorem 3.

27. Let $\mathcal{G} = (G, *)$ be any group and let $a_1, ...a_n \in G$. Use the previous exercise and mathematical induction to prove that $(a_1 * ... * a_n)^{-1} = a_n^{-1} * ... * a_1^{-1}$.

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

2 Order of Group Elements

In this section, we will explore some of the algebra that is possible in groups. We begin with a definition.

Definition 10 *Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. If n is any positive integer, then we define*

$$a^n = \underbrace{a * a * a * ... * a}_{n \text{ times}} \qquad a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} * ... * a^{-1}}_{n \text{ times}} \qquad a^0 = e$$

Under this convention, the way "powers" of a group element are computed depends on the group operation. Consider the following examples:

- In the permutation group $\mathcal{P}_5$, the operation is function composition; thus

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} \end{aligned}$$

- In the group $\mathcal{Z}_6$, the operation is addition modulo 6 ; thus

$$\begin{aligned} [4]_6^{-3} &= ([4]_6^{-1})^3 \\ &= [2]_6^3 \\ &= [2]_6 \boxplus_6 [2]_6 \boxplus_6 [2]_6 \\ &= [2 + 2 + 2]_6 \\ &= [0]_6 \end{aligned}$$

The following few results establish that "powers" of elements in a group satisfy some of the familiar laws of exponents.

Lemma 11 *Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. If m is any integer and n is any positive integer, then $a^m * a^n = a^{m+n}$.*

Proof. If $m = 0$ then there is nothing to show, since $a^0 = e$ by definition; so let's assume that $m \neq 0$. We will accomplish this proof by induction on the integer n. If $m > 0$, then by definition, we know

$$a^m * a^1 = \underbrace{a * a * a * ... * a}_{m+1 \text{ times}} = a^{m+1}$$

On the other hand, if $m < 0$, then we know that $-m > 0$; hence, the associativity of the group operations tells us

$$\begin{aligned} a^m * a^1 &= (a^{-1})^{-m} * a \\ &= \left(\underbrace{a^{-1} * a^{-1} * a^{-1} * ... * a^{-1}}_{-m \text{ times}} \right) * a \\ &= \left(\underbrace{a^{-1} * a^{-1} * a^{-1} * ... * a^{-1}}_{-m-1 \text{ times}} \right) (a^{-1} * a) \\ &= \left(\underbrace{a^{-1} * a^{-1} * a^{-1} * ... * a^{-1}}_{-m-1 \text{ times}} \right) = (a^{-1})^{-m-1} = a^{m+1} \end{aligned}$$

Consequently, the formula holds for any integer m when $n = 1$. Now suppose that $a^m * a^n = a^{m+n}$ for any integer m and some positive integer n and consider the product $a^m * a^{n+1}$. We therefore know that

$$\begin{aligned} a^m * a^{n+1} &= a^m * (a^n * a) \\ &= (a^m * a^n) * a \\ &= a^{m+n} * a && \text{Induction Hypothesis} \\ &= a^{m+n+1} && \text{Established formula} \end{aligned}$$

We may now conclude by induction that the $a^m * a^n = a^{m+n}$ for any integer m and any positive integer n.

QED

Theorem 12 *Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. If m and n are any integers, then $a^m * a^n = a^{m+n}$.*

Proof. If $n = 0$, then there is nothing to show; and it $n > 0$, then $a^m * a^n = a^{m+n}$ by Lemma 1. Suppose that $n < 0$. In this case, we know that $-n > 0$; hence, Lemma 1 tells us

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

QED

Corollary 13 *Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. If m is any integer, then $(a^m)^{-1} = (a^{-1})^m$.*

Proof. Theorem 2 tells us that for all $b \in G$ we have

$$b^m * b^{-m} = b^{m-m} = b^0 = e$$

The fact that elements of a group have unique inverses now tells us that $(b^m)^{-1} = b^{-m}$. Let $a \in G$. Now, if $m > 0$, we know by definition that $a^{-m} = (a^{-1})^m$. If $m = 0$, then $a^{-m} = a^0 = e$, and $(e^{-1})^m = (e)^0 = e$; hence, we know that $a^{-m} = (a^{-1})^m$ when $m = 0$. If $m < 0$, then we know that $-m > 0$; and we know

$$\begin{aligned} (a^m)^{-1} &= (a^{-(-m)})^{-1} \\ &= ([a^{-1}]^{-m})^{-1} && \text{Definition} \\ &= (a^{-1})^{-(-m)} && \text{Since } (b^k)^{-1} = b^{-k} \\ &= (a^{-1})^m \end{aligned}$$

We may therefore conclude that $(a^m)^{-1} = (a^{-1})^m$ for all integers m.

QED

Corollary 14 *Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. If m and n are any integers, then $(a^m)^n = a^{nm}$.*

Proof. This result is really a direct consequence of Theorem 2 and Corollary 3. We only need to consider three cases. If n is a positive integer, then we know that

$$(a^m)^n = \underbrace{a^m * a^m * a^m * ... * a^m}_{n \text{ times}} = a^{\underbrace{m+m+...+m}_{n \text{ times}}} = a^{nm}$$

Suppose instead that n is a negative integer. This means that $-n > 0$; and we know by Corollary 3 and our last result that

$$\begin{aligned} (a^m)^n &= ([a^m]^{-1})^{-n} \\ &= ([a^{-1}]^m)^{-n} = (a^{-1})^{(-n)m} \end{aligned}$$

However, we also know by definition that $(a^{-1})^{(-n)m} = a^{-(-n)m} = a^{nm}$. The final case to consider is when $n = 0$. However, this case is trivial since we know

$$e = (a^m)^0 \quad \text{and} \quad e = a^0 = a^{0(m)}$$

We may conclude that $(a^m)^n = a^{nm}$ for all integers m and n.

QED

We have established that "powers" of group elements satisfy some of the familiar laws of exponents. However, there are some laws of exponents which *do not* hold for all groups.

Example 15 *Compare $(a \circ b)^2$ and $a^2 \circ b^2$ in the permutation group $\mathcal{P}_5$, where*

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$$

Solution. Observe that

$$a \circ b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

$$(a \circ b)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$$

$$a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$b^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$$

$$a^2 \circ b^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$$

From these computations, we see that $(a \circ b)^2 \neq a^2 \circ b^2$.

****

The reason that $(a \circ b)^2 \neq a^2 \circ b^2$ in the previous example is because the elements a and b do not commute in the permutation group $\mathcal{P}_5$. A moment's thought suggests the following conjecture:

In a group $G = (G, *)$, we have $a * b = b * a$ if and only if $(a * b)^n = a^n * b^n$ for all integers n.

Proving this conjecture is a bit trickier than that moment's thought would suggest, however. You will have an opportunity to prove this conjecture in the exercises. In the meantime, we will assume that it is true.

Corollary 16 *Let $\mathcal{G} = (G, *)$ be any group with identity e, let $a \in G$, and let n be a positive integer. If $a^k \neq e$ for all integers $0 < k \leq n$, then $a^j \neq a^k$ for all distinct integers $0 < j < k \leq n$.*

Proof. Suppose by way of contradiction that there exist positive integers $j < k \leq n$ such that $a^j = a^k$. This tells us

$$a^j = a^k \quad \Longrightarrow \quad e = a^k * a^{-j} = e \quad \Longrightarrow \quad e = a^{k-j}$$

However, this is impossible since $k - j$ is a positive integer less than or equal to n.

QED

Corollary 17 *Let $\mathcal{G} = (G, *)$ be any group with identity e and let $a \in G$. If there exists a nonzero integer n such that $a^n = e$, then there is a smallest positive integer k such that $a^k = e$. Furthermore, we have $a^r \neq a^s$ for all integers $0 < r < s \leq k$.*

Proof. First, we will prove that there is a *positive* integer m such that $a^m = e$. Obviously if $n > 0$ then there is noting to show in this regard. Suppose that $n < 0$ and let $m = -n$. It follows that $m > 0$, and we know by definiiton that

$$e = a^n = a^{-m} = (a^{-1})^m$$

The fact that $e = a^{-m}$ coupled with Theorem 2 tells us

$$\begin{aligned} a^m &= a^m * (a^{-1})^m \\ &= (a^{-1})^{-m} * (a^{-1})^m \\ &= (a^{-1})^{-m+m} = (a^{-1})^0 = e \end{aligned}$$

Now that we know there is a positive integer m such that $a^m = e$, let P be the set of all positive integers q such that $a^q = e$. Since P is a nonempty set of positive integers, the well-ordering property tells us that P has a smallest member k. This is the positive integer that we seek.

To complete the proof, observe that since k is the *smallest* positive integer such that $a^k = e$, we know that $a^s \neq e$ for all positive integers $s < k$. Corollary 6 now tells us that $a^r \neq a^s$ for all $0 < r < s < k$. Since $a^k = e$ and $a^s \neq e$ for all positive integers $s < k$, we may conclude that $a^r \neq a^s$ for all $0 < r < s \leq k$ as desired.

QED

Definition 18 *Let $\mathcal{G} = (G, *)$ be any group with identity e and let $a \in G$. The smallest positive integer k such that $a^k = e$ (when it exists) is called the **order** of a in the group $\mathcal{G}$. If there is no such integer k, then it follows that $a^n \neq e$ for all positive integers n; and we say that a has **infinite order** in the group $\mathcal{G}$.*

Theorem 19 *Every element of a finite group $\mathcal{G} = (G, *)$ has finite order.*

Proof. Let $x \in G$ and consider the set $S = \{x^j : j \in \mathbb{Z}\}$. Since $\mathcal{G}$ is a group, we know that $S \subseteq G$; therefore, since G is finite, the elements of S cannot all be distinct. In other words, there must exist integers $j \neq k$ such that $x^j = x^k$. Consequently, we know that $e = x^{k-j}$ and we may conclude that x has finite order by the previous Corollary.

QED

Theorem 20 *Let $\mathcal{G} = (G, *)$ be any group with identity e, and let $a \in G$ have finite order n. We have $a^k = e$ if and only if k is a multiple of n.*

Proof. This result is an immediate consequence of the division algorithm. For any integer k, we know that there exist unique integers p and r such that $0 \leq r < n$ and $k = pn + r$. With this in mind, we know that

$$\begin{aligned} a^k &= a^{pn+r} \\ &= a^{pn} * a^r \\ &= (a^n)^p * a^r = e^p * a^r = a^r \end{aligned}$$

If k is a multiple of n, then $r = 0$; and we see that $a^k = e$. Conversely, if $a^k = e$, then we know that $a^r = e$. Since we also know that $0 \leq r < n$, that assumption that n is the *order* of a forces us to conclude that $r = 0$. Hence, we know that k is a multiple of n.

QED

Example 21 *Show that every nonzero element of the group $\mathcal{Z} = (\mathbb{Z}, +)$ of integers has infinite order.*

Solution. Let n be any nonzero integer. To show that n has infinite order in $\mathcal{Z}$, we need to prove that $n^k \neq 0$ for any positive integer k. This, however, is obvious, since by definition,

$$n^k = \underbrace{n + n + n + ... + n}_{k \text{ times}} = k(n)$$

Now, since $k > 0$, the properties of integers tell us that $k(n) = 0$ if and only if $n = 0$. Therefore, n must have infinite order.

****

Example 22 *In the group $\mathcal{M}_2$, what is the order of*

$$A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \qquad B = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$$

Solution. First, observe that

$$A^2 = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} * \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Consequently, the matrix A has order 2 in the group $\mathcal{M}_2$. On the other hand, observe that

$$B^2 = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} * \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 0 & 9 \end{bmatrix}$$

$$B^3 = B^2 * B = \begin{bmatrix} 4 & 0 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 8 & 0 \\ 0 & 27 \end{bmatrix}$$

$$B^4 = B^3 * B = \begin{bmatrix} 8 & 0 \\ 0 & 27 \end{bmatrix} * \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 16 & 0 \\ 0 & 81 \end{bmatrix}$$

It should be clear that raising B to positive integer powers will never produce the identity matrix. Indeed, you can use mathematical induction to prove that

$$B^n = \begin{bmatrix} 2^n & 0 \\ 0 & 3^n \end{bmatrix}$$

for any positive integer n (where, of course, 2^n and 3^n are understood in the usual multiplicative sense). Therefore, the the matrix B has infinite order in the group $\mathcal{M}_2$.

****

The following result provides a simple way of computing the order of elements in the groups $\mathcal{Z}_n = (\mathbb{Z}_n, \boxplus_n)$. It will have other uses in the next section.

Theorem 23 *Let $\mathcal{G} = (G, *)$ be a group with identity e, and let $a \in G$ have finite order n. If $m \in \mathbb{Z}^*$ and $d = \texttt{GCF}(m, n)$, then the order of a^m is n/d.*

Proof. First, note that $q = m/d \in \mathbb{Z}^+$; consequently, we know

$$(a^m)^{n/d} = a^{mn/d} = a^{qn} = e$$

It follows that, a^m has finite order t; and we know that $t \leq n/d$. We need to show that $t = n/d$. We know that

$$\left(a^d\right)^{n/d} = a^n = e$$

It follows that a^d has finite order $p \leq n/d$. However, if $p < n/d$, then $dp < n$ and we have $a^{dp} = e$ — contrary to Corollary 16. Thus, we may conclude that a^d has order n/d. There exist integers x and y such that $d = xm + yn$. Consequently, we know that

$$a^d = a^{xm+yn} = a^{xm} * a^{yn} = (a^m)^x * (a^n)^y = (a^m)^x * e = (a^m)^x$$

Since the order of a^d is n/d, we know that the order of a^{mx} is n/d as well. Furthermore, since

$$\left(a^{mx}\right)^t = \left(a^{mt}\right)^x = e^x = e$$

we know that the order of a^{mx} must be less than or equal to t. Therefore, we know that $n/d \leq t$ Thus, we have shown that $n/d \leq t \leq n/d$; and we are forced to conclude that $t = n/d$, as desired.

QED

Corollary 24 *If* $[m]_n \in \mathbb{Z}_n$*, then the order of* $[m]_n$ *in the group* $\mathcal{Z}_n = (\mathbb{Z}_n, \boxplus_n)$ *is* n/d*, where* $d = \texttt{GCF}(m, n)$*.*

Proof. First, note that $[1]_n$ has order n in $\mathcal{Z}_n$. Since $[m]_n = ([1]_n)^m$, the desired result is a direct consequence of the previous theorem.

QED

Example 25 *What is the order of* $[45]_{100}$ *in* $\mathcal{Z}_{100}$*?*

Solution. Since $5 = \texttt{GCF}(45, 100)$, we know that $[45]_{100}$ has order $100/5 = 20$ in this group.

****

Example 26 *What is the order of* $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$ *in the permutation group* $\mathcal{P}_6$*?*

Solution. Since this is a finite group, we know that a has finite order. Hence, we simply compute successive "powers" of a until we reach the identity permutation. Observe that

$$\left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 3 & 6 \end{pmatrix}$$

$$\begin{aligned} \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^3 &= \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^2 \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 3 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^4 &= \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^3 \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^5 &= \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^4 \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 2 & 3 & 6 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^6 &= \left[\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}\right]^5 \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 2 & 3 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \end{aligned}$$

We see that a has order 6 in this group.

****

There is a convenient notation often used to simplify writing permutations. It is especially helpful when trying to determine the order of a permutation and is based on a simple observation — the top row of the tabular notation is not needed. We can describe the permutation fully simply by indicating how it "moves" one element of the set to another. This can be done very efficiently using *cycle notation.*

Definition 27 *Let $X = \{1, 2, ..., n\}$ and let $\alpha \in \wp_n$. We say that α **moves** j provided $\alpha(j) \neq j$. We say that α **fixes** j provided $\alpha(j) = j$. A **cycle** in α is a subset $M = \{c_1, ..., c_k\} \subseteq X$ such that*

$$c_1 \quad \underrightarrow{\alpha} \quad c_2 \quad \underrightarrow{\alpha} \quad ... \quad \underrightarrow{\alpha} \quad c_k \quad \underrightarrow{\alpha} \quad c_1$$

We use the notation $(c_1 c_2 ... c_k)$ to denote this cycle.

The permutation $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$ in the previous example isnot a cycle but contains three cycles, namley

$$(135) \qquad (24) \qquad (6)$$

We can think of these cycles as members of $\wp_6$ in their own right. To do this, we simply assume that any number not appearing in the cycle is fixed by the permutation. Using this convention, we have

$$(135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix} \qquad (24) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 5 & 6 \end{pmatrix} \qquad (6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Notice that the cycle (6) corresponds to the identity permutation. All one-element cycles must fix every element and therefore represent the identity permutation. Because of this, we typically do not consider one-element cycles.

When working with cycles, it does not matter which number from the cycle you start with, as long as you do not change the sequence. For example,

$$(24) = (42) \qquad (135) = (513) = (351)$$

We can think of a cycle as being a permutation on any set containing at least as many elements as the largest number the cycle moves. For example,

In $\wp_5$, we have $(135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ In $\wp_7$, we have $(135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix}$

Example 28 *What is the order of the cycle* (135) *in the permutation group $\mathcal{P}_5$?*

Solution. Observe that

$$(135)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} = (153)$$

$$(135)^3 = (135)^2 \circ (135) = (153) \circ (135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

We see that (135) has order 3 in $\mathcal{P}_5$.

****

In the previous example, notice that composing (135) with itself does not affect the fixed elements. This observation leads us to the following important fact

In particular, the cycle (135) has order 3 in $\mathcal{P}_5$, in $\mathcal{P}_6$, in $\mathcal{P}_7$, and in every permutation group $\mathcal{P}_n$ where $n \geq 5$.

Theorem 29 *If a cycle in the permutation group $\mathcal{P}_n$ moves exactly k elements, then the cycle has order k.*

Proof. Let θ be a cycle in $\mathcal{P}_n$ that moves exactly k elements, and let $\theta = (a_1 ... \ a_k)$. We want to prove that $\theta^k = \epsilon$, and we want to prove that $\theta^m \neq \epsilon$ for any positive integer $m < k$. To begin, note that $\theta(a_m) = a_{m+1}$ for $1 \leq m < k$ and note that $\theta(a_k) = a_1$. If we compose θ with itself, it follows that $\theta^2(a_1) = \theta(\theta(a_1)) = a_3$; likewise, $\theta^3(a_1) = \theta(\theta^2(a_1)) = a_4$. Indeed, it is easy to see that for positive integers $1 \leq m < k$ we must have

$$\theta^m(a_1) = a_{m+1}$$

It follows that $\theta^m \neq \epsilon$ for any positive integer $m < k$, since θ^m must move both a_1 and a_{m+1}. Consider the permutation θ^k. We want to show that $\theta^k(a_m) = a_m$ for all positive integers $1 \leq m \leq k$. To this end, first observe that $\theta^{k-1}(a_1) = a_k$; hence, it follows that

$$\theta^k(a_1) = \theta(\theta^{k-1}(a_1)) = \theta(a_k) = a_1$$

What can we say about $\theta^k(a_2)$? We know that $\theta^2(a_2) = \theta(\theta(a_2)) = a_4$ and $\theta^3(a_2) = \theta(\theta^2(a_2)) = a_5$. In fact, we see that

$$\theta^m(a_2) = \begin{cases} a_{m+2} & \text{if} \quad 1 \leq m \leq k-2 \\ a_1 & \text{if} \quad m = k-1 \\ a_2 & \text{if} \quad m = k \end{cases}$$

Thus, we see that $\theta^k(a_2) = a_2$ as well. In fact, proceeding in like fashion, we can see that, for $1 \leq j \leq k$, we must have

$$\theta^m(a_j) = \begin{cases} a_{m+j} & \text{if} \quad 1 \leq m \leq k-j \\ a_1 & \text{if} \quad m = k+1-j \\ a_2 & \text{if} \quad m = k+2-j \\ \vdots & \vdots \quad \vdots \\ a_j & \text{if} \quad m = k \end{cases}$$

Therefore, we know that $\theta^k = \epsilon$, as desired.

QED

Two members of the permutation group $\mathcal{P}_n$ are said to be *disjoint* provided they do not move any of the same elements. It should be clear that any non-identity permutation on $X = \{1, 2, ..., n\}$ is either a cycle or can be written as a composition of disjoint cycles. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = (135) \circ (24) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix} = (24) \circ (35)$$

Lemma 30 *If α and β are disjoint members of the permutation group $\mathcal{P}_n$, then $\alpha \circ \beta = \beta \circ \alpha$.*

Proof. Let $X = \{1, 2, 3, ..., n\}$ and let M_α be the set of elements in X that are moved by the permutation α. Since α and β are assumed to be disjoint, $X - M_\alpha$ must be the set of elements in X that are moved by β. We need to show that $\alpha \circ \beta = \beta \circ \alpha$; to this end, let $j \in X$. Either $j \in M_\alpha$ or $j \in X - M_\alpha$. First, suppose that $j \in M_\alpha$. This means that $\alpha(j) \neq j$. Now, since α is a bijection, we know that $\alpha(\alpha(j)) \neq \alpha(j)$, either. This means that β must fix both j and $\alpha(j)$. Therefore, we know

$$(\alpha \circ \beta)[j] = \alpha(\beta(j)) = \alpha(j) \qquad (\beta \circ \alpha)[j] = \beta(\alpha(j)) = \alpha(j)$$

We may conclude that $(\alpha \circ \beta)[j] = (\beta \circ \alpha)[j]$ when $j \in M_\alpha$. On the other hand, suppose $j \in X - M_\alpha$. By similar reasoning, this implies that α must fix both j and $\beta(j)$. Consequently, we know that

$$(\alpha \circ \beta)[j] = \alpha(\beta(j)) = \beta(j) \qquad (\beta \circ \alpha)[j] = \beta(\alpha(j)) = \beta(j)$$

We may conclude that $(\alpha \circ \beta)[j] = (\beta \circ \alpha)[j]$ when $j \in X - M_\alpha$. Hence, we know that $(\alpha \circ \beta)[j] = (\beta \circ \alpha)[j]$ for all $j \in X$; and we may conclude that $\alpha \circ \beta = \beta \circ \alpha$.

QED

Theorem 31 *If a non-identity permutation θ in the symmetric group $\mathcal{P}_n$ is not a cycle, then its order is the least common multiple of the orders of the disjoint cycles composing θ.*

Proof. Suppose that $\theta = \theta_1 \circ ... \circ \theta_k$, where each θ_m is a cycle of order p_m, and the cycles θ_m are all disjoint. Since disjoint cycles commute by Lemma 27, we know that for any positive integer r, we must have

$$\theta^r = (\theta_1 \circ ... \circ \theta_k)^r = [\theta_1]^r \circ ... \circ [\theta_k]^r$$

Now, suppose that $r = \texttt{LCM}(p_1, ..., p_k)$. It follows that for each $1 \leq m \leq k$, there exists a positive integer a_m such that $r = a_m p_m$. Therefore, we know that

$$\begin{aligned} \theta^r &= (\theta_1 \circ ... \circ \theta_k)^r \\ &= [\theta_1]^r \circ ... \circ [\theta_k]^r \\ &= [\theta_1]^{a_1 p_1} \circ ... \circ [\theta_k]^{a_k p_k} \\ &= ([\theta_1]^{p_1})^{a_1} \circ ... \circ ([\theta_k]^{p_k})^{a_k} = (\epsilon)^{a_1} \circ ... \circ (\epsilon)^{a_k} = \epsilon \end{aligned}$$

From this we see that $\theta^r = \epsilon$. We need to show that r is the *smallest* positive integer with this property. Suppose that t is a positive integer such that $\theta^t = \epsilon$. Since the cycles composing θ are disjoint it follows that

$$[\theta_1]^t \circ ... \circ [\theta_k]^t = \epsilon$$

Since these cycles are all disjoint, it also follows that $[\theta_m]^t = \epsilon$ for $1 \leq m \leq k$. Theorem 20 tells us that t must be a multiple of the order for each θ_m. Consequently, since r is the *least* common multiple of these orders, we know $r \leq t$; and we may conclude that r is the smallest positive integer such that $\theta^r = \epsilon$.

QED

The proof of the previous theorem relies heavily on the factor cycles being disjoint. The conclusion of the theorem may fail for compositions whose factors are not disjoint. For example, in the symmetric group $\mathcal{P}_5$ we have

$$(134) \circ (23) = (1324) \qquad (134) \circ (125) = (12534)$$

In the first example, the least common multiple of the factor cycle orders is 6 while the order of their composition is 4. In the second case, the least common multiple of the factor cycle orders is 3 while the order of their composition is 5. If elements in a group do not commute, then there is no simple relationship between their orders and the order of their product.

EXERCISES FOR SECTION 2

1. Find two cycles $\alpha, \beta \in \mathcal{P}_3$ that are not disjoint but do commute.

2. Write the following permutations either as cycles or as compositions of disjoint cycles.

   (a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

(b) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 5 & 6 & 2 & 4 & 1 \end{pmatrix}$

(c) $\gamma = (1462) \circ (2563)$

(d) $\delta = (23) \circ (35) \circ (41) \circ (45) \circ (62) \circ (36)$

3. Use Exercise 1.27 to find the inverse of $\alpha = (23) \circ (34) \circ (72) \circ (75) \circ (36)$.

4. Use Theorems 29 and 31 to determine the order of each permutation below.

(a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 2 & 8 & 5 & 3 & 7 & 1 & 4 \end{pmatrix}$

(b) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 9 & 7 & 8 & 5 & 6 & 10 & 1 \end{pmatrix}$

(c) $\gamma = (346) \circ (24)$

(d) $\delta = (562) \circ (314) \circ (24)$

5. Use Theorems 20, 29, and 31 to determine the order of each permutation below.

(a) $\alpha = (346871)^2$

(b) $\beta = [(213) \circ (5874)]^8$

6. What is the order of $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ in the group $\mathcal{M}_2$?

7. Let $\mathcal{U}_{40}$ denote the group of units modulo 40 under multiplication modulo 40. (See Exercise 1.20.) What is the order of the following elements in this group?

(a) $[3]_{40}$

(b) $[17]_{40}$

(c) $[31]_{40}$

8. What is the order of the following elements?

(a) the element $[39]_{90}$ in the group $\mathcal{Z}_{90}$

(b) the element $[60]_{250}$ in the group $\mathcal{Z}_{250}$

9. What is the order of -1 in the group $\mathcal{Z}$?

10. Let $\mathcal{G} = (G, *)$ be any group with identity e and suppose $a \in G$. Use Theorem 20 to answer the following questions.

(a) If we know that $a^{20} = e$, then what are the possible orders of a?

(b) If we know that $a^p = e$ for some prime p, then what are the possible orders of a?

11. Let $\mathcal{G} = (G, *)$ be any group and suppose $a \in G$ has order n.

(a) Show that $a^{-1} = a^{n-1}$.

(b) Explain why n and $1 - n$ are relatively prime.

(c) Use Theorem 23 to prove that a^{-1} also has order n.

12. Let $\mathcal{G} = (G, *)$ be any group with identity e and let $a \in G$ be a non-identity element. Prove that $a = a^{-1}$ if and only if a has order 2.

13. Prove that the order of any element in the group $\mathcal{Z}_n$ is a divisor of n.

14. Prove that an element $[m]_n$ of the group $\mathcal{Z}_n$ has order n if and only if m is relatively prime to n.

15. Let $\mathcal{G} = (G, *)$ be any group and suppose $a \in G$ has order n. Use the division alorithm to prove that for all $m \in \mathbb{Z}$ there exist unique $0 \leq r < n$ such that $a^m = a^r$.

16. Let $\mathcal{G} = (G, *)$ be any group and suppose $a, b \in G$. Use mathematical induction to prove that, if $a * b = b * a$, then $(a * b)^n = a^n * b^n$ for every positive integer n.

17. Let $\mathcal{G} = (G, *)$ be any group and suppose $a, b \in G$ are such that $a * b = b * a$.

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

    (b) Use Part (a) and the previous exercise to explain why $(a * b)^n = a^n * b^n$ for *every* integer n.

18. Let $\mathcal{G} = (G, *)$ be any group and suppose $a, b \in G$. If $(a * b)^2 = a^2 * b^2$, then prove $a * b = b * a$. Hint: $a * b = (a * b) * (a * b) * (a * b)^{-1}$

19. If every non-identity element of a group $\mathcal{G} = (G, *)$ has order 2, then prove that $\mathcal{G}$ is abelian. Hint: Let $a, b \in G$ and consider the product $b * b * a * b * a * a$ with judiciously placed parentheses.

    In the next few exercises, we introduce an important way to create new groups from existing ones. Let $\mathcal{G}_1 = (G_1, \otimes_1)$, ..., $\mathcal{G}_n = (G_n, \otimes_n)$ be groups and consider the pair

    $$\mathcal{G}_1 \times ... \times \mathcal{G}_n = (G_1 \times ... \times G_n, *)$$

    where $(a_1, ..., a_n) * (b_1, ..., b_n) = (a_1 \otimes_1 b_1, ..., a_n \otimes_n b_n)$.

20. Show that $\mathcal{G}_1 \times ... \times \mathcal{G}_n$ is a group. This type of group is called a *product group.*

21. Construct the group table for the product group $\mathcal{Z}_3 \times \mathcal{Z}_3$. What is the largest order for any element in this group?

22. Construct the group table for the product group $\mathcal{Z}_2 \times \mathcal{Z}_2 \times \mathcal{Z}_2$. What is the largest order for any element in this group?

23. Show by example that the group $\mathcal{Z} \times \mathcal{Z}_4$ has elements of infinite order and elements of finite order.

24. What is the order of the element $([3]_9, (134) \circ (23))$ in the product group $\mathcal{Z}_9 \times \mathcal{P}_4$?

3 Subgroups

In this section, we will begin with an example. Let $F = \{\epsilon, \alpha, \beta, \gamma, \delta, \theta\}$, where each member of F is the function $t : \mathbb{R} - \{0, 1\} \longrightarrow \mathbb{R} - \{0, 1\}$ defined by

$$\epsilon(x) = x \qquad q(x) = 1 - x \qquad r(x) = \frac{1}{x}$$

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

You showed that this set forms a group under function compositon in Exercise 1.23. Here is the operation table for F under function composition.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{s}$	$\boldsymbol{t}$	$\boldsymbol{u}$
$\boldsymbol{\epsilon}$	ϵ	q	r	s	t	u
$\boldsymbol{q}$	q	ϵ	u	t	s	r
$\boldsymbol{r}$	r	s	ϵ	q	u	t
$\boldsymbol{s}$	s	r	t	u	q	ϵ
$\boldsymbol{t}$	t	u	s	r	ϵ	q
$\boldsymbol{u}$	u	t	q	ϵ	r	s

Now, consider the subset $H = \{\epsilon, s, u\}$ under the same operation. If we construct the operation table for H, we have

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{s}$	$\boldsymbol{u}$
$\boldsymbol{\epsilon}$	ϵ	s	u
$\boldsymbol{s}$	s	u	ϵ
$\boldsymbol{u}$	u	ϵ	s

Note that the set H is closed under $\circ$; hence, we know that $*$ is also an operation on this set. Furthermore, the element ϵ acts as an identity, and each member of H has an inverse under$\circ$. Therefore, we may conclude that $(H, \circ)$ is a group (we already know that function composition is associative). In fact, it is an abelian group. We call H a *subgroup* of the group $(F, \circ)$.

Definition 32 *Let $\mathcal{G} = (G, *)$ be a group and let $H \subseteq G$ be nonemtpy. We say that H is a **subgroup** of $\mathcal{G}$ provided*

- *The set H is closed under $*$.*
- *Whenever $x \in H$, then $x^{-1} \in H$.*

Example 33 *The conditions of the previous definition are independent. In other words, it is possible to find subsets of a group which satisfy one condition but not the other.*

Indeed, here are two such examples.

- The set $H = \{\epsilon, q, r\}$ of the set F above satisfies Condition (2) of the subgroup definition, since each member of H is its own inverse. However, H does not satisfy Condition (1) since $q \circ r = u$. Therefore, this set is *not* a subgroup of $(F, \circ)$.
- Consider the group $\mathcal{Z} = (\mathbb{Z}, +)$ of integers under addition. The set $H = \{2n : n \in \mathbb{Z}^+\}$ is a subset of $\mathbb{Z}$ which satisfies Condition (1) of the subgroup definition, but it does not satisfy Condition (2), since the inverse of $x = 4$ is the integer $y = -4$; and $y = -4$ is not a member of H. Hence, this set is *not* a subgroup of $\mathcal{Z}$.

****

It stands to reason that a subgroup of a group should be a group in its own right. For this reason, it is important that the set H be nonempty in the definition above. The empty set satisfies both conditions *vacuously* (there are no elements in the empty set to violate the conditions), however, the emptyset cannot possibly form a group because it cannot contain an identity element. As long as H is nonempty, the two conditions in the definition guarantee that H contains the identity element of $\mathcal{G}$, and guarantees that it will also be the identity element of H.

We have already encountered many examples of subgroups. Here are a few examples.

- The group $\mathcal{Q}$ of rational numbers under addition is a subgroup of the group $\mathcal{R}$ of real numbers under addition.
- The group $\mathcal{Z}$ of integers under addition is a subgroup of the group $\mathcal{Q}$.
- The octic group $\mathcal{O}$ is a subgroup of the group $\wp_4$ of permutations on a four-element set.
- The cross ratio group $\mathcal{F} = (F, \circ)$ discussed above is a subgroup of the group $[\mathbb{R} - \{0, 1\} \longrightarrow \mathbb{R} - \{0, 1\}]$ of all functions $t : \mathbb{R} - \{0, 1\} \longrightarrow \mathbb{R} - \{0, 1\}$ under function composition.

If $\mathcal{G} = (G, *)$ is any group, then G is always a subgroup, as is the singleton set $\{e\}$, where e is the identity element for $\mathcal{G}$. Thus, every group containing more than one element will have at least two subgroups. The singleton $\{e\}$ is the only one-element subgroup of any group; we call it the *trivial* subgroup. All other subgroups are called *nontrivial*. The set G is called the *improper* subgroup of $\mathcal{G}$; all other subgroups are called *proper*.

Example 34 *It is common to let $n\mathbb{Z}$ denote the set of all integer multiples of the fixed positive integer n. Show that $n\mathbb{Z}$ is always a subgroup of the group $\mathcal{Z} = (\mathbb{Z}, +)$.*

Solution. First, note that

$$n\mathbb{Z} = \{kn : k \in \mathbb{Z}\} = \{..., -3n, -2n, -n, 0, n, 2n, 3n, ...\}$$

To prove that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$, we need to show two things — we must prove that $n\mathbb{Z}$ is closed under integer addition and we must show that $n\mathbb{Z}$ contains the additive inverse for each of its elements. To prove closure under addition, suppose that $x, y \in n\mathbb{Z}$. This means that $x = kn$ and $y = jn$ for some integers k, j. Therefore, we know that

$$x + y = kn + jn = (k + j)n$$

Since $(k + j)n$ is an integer multiple of n, we may conclude that $x + y \in n\mathbb{Z}$. To prove closure under inverses, note that theinverse of $x = kn$ in $(\mathbb{Z}, +)$ is $-x = (-k)n$. Since $-x$ is an integer multiple of n, we may conclude that $-x \in n\mathbb{Z}$.

****

Example 35 *Let $\mathcal{M}_2 = (M, \circ)$ be the group of all 2×2 invertible matrices under matrix multiplication and let*

$$H = \left\{ \begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix} : x, y \in \mathbb{R}, y \neq 0 \right\}$$

Is the set H a subgroup of $\mathcal{M}_2$?

Solution. We must decide whether the set H satisfies Conditions (1) and (2) of Definition 1. To show closure under matrix multiplication, let

$$A = \begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix} \quad B = \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix}$$

be members of H. Observe that

$$AB = \begin{bmatrix} 1 & ax + by \\ 0 & yb \end{bmatrix}$$

By assumption, we know that $y \neq 0$ and $b \neq 0$; therefore, we also know that $yb \neq 0$. Consequently, AB is a member of H; and we may conclude that H is closed under matrix multiplication. We know that the inverse for the matrix A is given by the formula

$$A^{-1} = \begin{bmatrix} 1 & -x/y \\ 0 & 1/y \end{bmatrix}$$

Since $y \neq 0$, it is clear that $1/y \neq 0$ as well. Hence, the inverse of A is also a member of H; and we may conclude that H is a subgroup of $\mathcal{M}_2$.

****

Example 36 *Let $\mathcal{Z} = (\mathbb{Z}, +)$ be the group of integers under addition and let $\mathcal{Z} \times \mathcal{Z}$ be the corresponding product group. Is the set*

$$H = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y \text{ is odd}\}$$

a subgroup of $\mathcal{Z} \times \mathcal{Z}$?

Solution. We must decide whether the set H satisfies Conditions (1) and (2) of Definition 1. Since the sum of two odd integers is even, it is easy to see that H is not closed under addition. Indeed, if $a = (1, 3)$ and $b = (2, 5)$, then $a + b = (3, 8)$. Since the second coordinate of $a + b$ is even, we know that $a + b \notin H$. Therefore, H is not a subgroup of $\mathcal{Z} \times \mathcal{Z}$.

****

It is interesting to note that the set H given in the previous example is not closed under the operation on $\mathcal{Z} \times \mathcal{Z}$, but *is* closed under the formation of inverses. Indeed, if y is an odd integer, then $-y$ is also an odd integer. Hence, if $(x, y) \in H$, then its inverse $(-x, -y) \in H$ as well.

If H is an infinite subset of an infinite group $\mathcal{G}$, then closure under the operation is not enough to guarantee that H is a subgroup of $\mathcal{G}$. (Consider the subset H of positive even integers in the group $\mathcal{Z} = (\mathbb{Z}, +)$ of integers under addition mentioned above.) However, it is a different story is the subset is *finite*.

Theorem 37 *Suppose that $\mathcal{G} = (G, *)$ is a group. A nonempty finite subset H of G is a subgroup of $\mathcal{G}$ if and only if H is closed under the operation.*

Solution. If H is a subgroup of $\mathcal{G}$, then H is certainly closed under the operation, so there is nothing to show. On the other hand, suppose that H is closed under the operation. This means that H satisfies Condition (1) of Definition 1. We must show that H also satisfies Condition (2). Let $H = \{a_1, ..., a_n\}$, and let b be any fixed element in H. Consider the set

$$bH = \{ba_1, ..., ba_n\}$$

Since H is closed under the operation on G, we know that $bH \subseteq H$. Since the function $f : G \longrightarrow G$ defined by $f(x) = bx$ is a bijection, we know that all of the members of bH are distinct. In other words, there are exactly n elements in the set bH. Therefore, we must conclude that $bH = H$. Consequently, since every element of H must be a member of bH, we know

$$b = ba_j$$

for some integer $1 \leq j \leq n$. However, this tells us that $e = a_j$; hence, we may conclude that $e \in H$. We are now ready to prove that H is closed under the formation of inverses. Since we know that $e \in H$, and since we know that $bH = H$, it follows that

$$e = ba_k$$

for some integer $1 \leq k \leq n$. This, however, tells us that $b^{-1} = a_k$. We may therefore conclude that $b^{-1} \in H$. Since b is an arbitrary fixed element of H, this suffices to prove that H contains the inverse of each of its members.

QED

Example 38 *Determine all of the subgroups of $\mathcal{Z}_4 = (\mathbb{Z}_4, \boxplus_4)$, where $\boxplus_4$ denotes addition modulo 4.*

Solution. Since $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ contains four elements, we know there are sixteen subsets of $\mathbb{Z}_4$. (We are omitting subscripts on the residue classes for simplicity since we are always working modulo 4.) Since all of these subsets are finite, the previous theorem tells us we only need to check each one for closure under addition modulo 4. Still, this is a large task; and we can be smarter. Since any subgroup of $\mathcal{Z}_4$ must contain the identity 0, we can discard any subset which does not contain 0. This means we have only eight subsets to check:

$$H_1 = \{[0]\} \qquad H_2 = \{[0], [1]\} \qquad H_3 = \{[0], [1], [2]\} \qquad H_4 = \{[0], [1], [2], [3]\}$$

$$H_5 = \{[0], [1], [3]\} \qquad H_6 = \{[0], [2]\} \qquad H_7 = \{[0], [3]\} \qquad H_8 = \{[0], [2], [3]\}$$

A quick check shows that of these sets, only H_1, H_6, and H_4 are closed under addition modulo 4; hence these are the only subgroups of $\mathcal{Z}_4$.

****

Definition 39 *Let X be any set and let P_X be its power set. If $F \subseteq P_X$ is a nonempty collection of subsets from X, then we let $\bigcap F$ denote the set of all elements contained in every member of F. In other words,*

$$\bigcap F = \{a \in X : a \in A \text{ for every set } A \in F\}$$

*We call $\bigcap F$ the **intersection** of the family F.*

Example 40 *Suppose that $X = \{a, b, c, d\}$ and let $F = \{\{a, b, c\}, \{b, c\}, \{b, c, d\}\}$. In this case, $\bigcap F = \{b, c\}$ since these are the only two elements contained in every member of F.*

****

Example 41 *If $F = \{2\mathbb{Z}, 3\mathbb{Z}, 8\mathbb{Z}, 12\mathbb{Z}\}$, then what is $\bigcap F$?*

Solution. An integer $k \in \bigcap F$ if and only if k is an integer multiple of $2, 3, 8$, and 12, since it must be an element of every member of F. This means that every member of $\bigcap F$ must be an integer multiple of $n = 24$, since this is the least common multiple of these numbers. Thus,

$$\bigcap F = 24\mathbb{Z} = \{..., -72, -48, -24, 0, 24, 48, 72, ...\}$$

****

Theorem 42 *Let $\mathcal{G} = (G, *)$ be any group. If F is a nonempty collection of subgroups of $\mathcal{G}$, then $\bigcap F$ is also a subgroup of $\mathcal{G}$.*

Proof. Let e be the identity element for $\mathcal{G}$. Since every member of F is a subgroup of $\mathcal{G}$, we know that every member of F contains e. Hence, we know that $e \in \bigcap F$. This tells us that $\bigcap F$ is nonempty. We need to show that $\bigcap F$ is closed under the operation $*$ and show that $\bigcap F$ contains the inverse for each of its elements. Let $x, y \in \bigcap F$. This means that x and y are elements of each member in F; and this tells us that $x * y$ must be an element of each member in F — because they are all subroups of $\mathcal{G}$. Hence, we may conclude that $x * y \in \bigcap F$. Furthermore, since x is an element of each member in F, the fact that all members of F are subgroups tell us that x^{-1} must also be an element of each member in F. Consequently, we may conclude that $x^{-1} \in \bigcap F$. Therefore, $\bigcap F$ is a subgroup of $\mathcal{G}$.

Definition 43 *Let $\mathcal{G} = (G, *)$ be any group, and let $X \subseteq G$ be nonempty. The subgroup of $\mathcal{G}$ **generated** by the set X is defined to be the intersection of all subgroups that contain X. It is denoted by $\langle X \rangle$ and is the smallest subgroup of $\mathcal{G}$ containing the set X.*

Example 44 *What is the subgroup of $\mathcal{Z}_3 \times \mathcal{Z}_6$ generated by the set $X = \{([2]_3, [2]_6), ([2]_3, [4]_6)\}$?*

Solution. We want to construct the subgroup $H = \langle\{([2]_3, [2]_6), ([2]_3, [4]_6)\}\rangle$. By definition, this is the smallest subgroup of $\mathcal{Z}_3 \times \mathcal{Z}_6$ that contains these two elements. Since this group must be finite, we simply take the set X and close it under the group operation. To begin, we know that H must contain the identity $([0]_3, [0]_6)$ and must contain the inverse of $([2]_3, [2]_6)$ and the inverse of $([2]_3, [4]_6)$. Thus, our first attempt at closing X under the operation is

$$H_1 = \{([0]_3, [0]_6), ([2]_3, [2]_6), ([1]_3, [4]_6), ([2]_3, [4]_6), ([1]_3, [2]_6)\}$$

However, a quick check shows that this set is *not* closed under the operation, since $([2]_3, [2]_6) * ([1]_3, [2]_6) = ([0]_3, [4]_6)$. Constructing the operation table tells us what new elements we will have to add. We will omit the usual residue class notation for the sake of readability and work only with the smallest positive representative of each class.

$*$	**(0, 0)**	**(2, 2)**	**(1, 4)**	**(2, 4)**	**(1, 2)**
(0, 0)	(0, 0)	(2, 2)	(1, 4)	(2, 4)	(1, 2)
(2, 2)	(2, 2)	(1, 4)	(0, 0)	(1, 0)	(0, 4)
(1, 4)	(1, 4)	(0, 0)	(2, 2)	(0, 2)	(2, 0)
(2, 4)	(2, 4)	(1, 0)	(0, 2)	(1, 2)	(0, 0)
(1, 2)	(1, 2)	(0, 4)	(2, 0)	(0, 0)	(2, 4)

We can see from this table that several new elements (along with their inverses) will have to be added to our first attempt. Our second attempt is the set

$$H_2 = \{([0]_3, [0]_6), ([2]_3, [2]_6), ([1]_3, [4]_6), ([2]_3, [4]_6), ([1]_3, [2]_6), ([0]_3, [4]_6), ([0]_3, [2]_6), ([1]_3, [0]_6), ([2]_3, [0]_6)\}$$

We now need to check the operation table for this set. If no new elements appear, we have found the subgroup that we seek.

$*$	**(0, 0)**	**(2, 2)**	**(1, 4)**	**(2, 4)**	**(1, 2)**	**(0, 4)**	**(0, 2)**	**(1, 0)**	**(2, 0)**
(0, 0)	(0, 0)	(2, 2)	(1, 4)	(2, 4)	(1, 2)	(0, 4)	(0, 2)	(1, 0)	(2, 0)
(2, 2)	(2, 2)	(1, 4)	(0, 0)	(1, 0)	(0, 4)	(2, 0)	(2, 4)	(0, 2)	(1, 2)
(1, 4)	(1, 4)	(0, 0)	(2, 2)	(0, 2)	(2, 0)	(1, 2)	(1, 0)	(2, 4)	(0, 4)
(2, 4)	(2, 4)	(1, 0)	(0, 2)	(1, 2)	(0, 0)	(2, 2)	(2, 0)	(0, 4)	(1, 4)
(1, 2)	(1, 2)	(0, 4)	(2, 0)	(0, 0)	(2, 4)	(1, 0)	(1, 4)	(2, 2)	(0, 2)
(0, 4)	(0, 4)	(2, 0)	(1, 2)	(2, 2)	(1, 0)	(0, 2)	(0, 0)	(1, 4)	(2, 4)
(0, 2)	(0, 2)	(2, 4)	(1, 0)	(2, 0)	(1, 4)	(0, 0)	(0, 4)	(1, 2)	(2, 2)
(1, 0)	(1, 0)	(0, 2)	(2, 4)	(0, 4)	(2, 2)	(1, 4)	(1, 2)	(2, 0)	(0, 0)
(2, 0)	(2, 0)	(1, 2)	(0, 4)	(1, 4)	(0, 2)	(2, 4)	(2, 2)	(0, 0)	(1, 0)

The set H_2 is closed under the operation; hence, we have found the subgroup of $\mathcal{Z}_3 \times \mathcal{Z}_6$ that is generated by $X = \{(2, 2), (2, 4)\}$. In particular, we know

$$\begin{aligned}\langle\{([2]_3, [2]_6), ([2]_3, [4]_6)\}\rangle \quad = \quad & \{([0]_3, [0]_6), ([2]_3, [2]_6), ([1]_3, [4]_6), ([2]_3, [4]_6), \\ & ([1]_3, [2]_6), ([0]_3, [4]_6), ([0]_3, [2]_6), ([1]_3, [0]_6), ([2]_3, [0]_6)\}\end{aligned}$$

****

Example 45 *Let $\mathcal{F} = (\{\epsilon, q, r, s, t, u\}, \circ)$ be the cross ratio group discussed at the beginning of this section. What is $\langle\{s\}\rangle$?*

Solution. We see from the table at the beginning of these notes that u is the inverse of s; hence, we begin by considering the set

$$H_1 = \{\epsilon, s, u\}$$

We have already shown that this set is closed under function composition (see the table at the beginning of this section). Therefore, we know that

$$\langle\{s\}\rangle = \{\epsilon, s, u\}$$

****

There is something special about the subgroup appearing in the last example. Notice from the table that $u = s^2$ and $\epsilon = s^3$. Consequently, we see that

$$\langle\{s\}\rangle = \{s, s^2, s^3\}$$

The subgroup of F generated by the singleton $\{s\}$ consists of positive integer powers of s. This turns out to be true for any subgroup of a group that is generated by a singleton subset.

Theorem 46 *Let $\mathcal{G} = (G, *)$ be any group. If $a \in G$, then $\langle\{a\}\rangle = \{a^n : n \in \mathbb{Z}\}$. In other words, the subgroup of $\mathcal{G}$ that is generated by the single element a is the set of all integer powers of a.*

Proof. Let $A = \{a^n : n \in \mathbb{Z}\}$ and let F denote the family of all subgroups that contain the element a. By definition, we know that $\langle\{a\}\rangle = \bigcap F$. We need to prove that $\bigcap F = A$. Since any subroup is closed with respect to the group operation, we know that A must be a subset of every member of F; hence, we may conclude that $A \subseteq \bigcap F$. We need to prove that $\bigcap F \subseteq A$.

First, we will prove that A is a subgroup of $\mathcal{G}$. Clearly $a \in A$, so we know that A is nonempty. Suppose that $x, y \in A$. It follows that $x = a^j$ and $y = a^k$ for some integers j and k. Consequently, we know that

$$x * y = a^j * a^k = a^{j+k}$$

Since $j + k$ is an integer, we may conclude that $x * y \in A$; therefore, A is closed under the operation. Furthermore, the inverse of x will be the element $x^{-1} = \left(a^j\right)^{-1} = a^{-j}$. Therefore, we know that $x^{-1} \in A$ as well. We may therefore conclude that A is a subgroup of $\mathcal{G}$.

Now, since A is a subgroup of $\mathcal{G}$ that contains the element a, we know that $A \in F$. Consequently, $\bigcap F \subseteq A$, as desired.

QED

Definition 47 *Let $\mathcal{G} = (G, *)$ be any group. A subgroup of $\mathcal{G}$ that is generated by a singleton set is called a **cyclic** subgroup of $\mathcal{G}$. In other words, a subgroup H of $\mathcal{G}$ is cyclic provided $H = \langle\{a\}\rangle$ for some $a \in G$. The element a is called a **generator** for H. It is common to write $\langle a\rangle$ in place of $\langle\{a\}\rangle$ for cyclic subgroups.*

Example 48 *Show that the integers under addition forms a cyclic group.*

Solution. To show that $\mathcal{Z} = (\mathbb{Z}, +)$ is cyclic, we must locate a generator. In other words, we need to find a fixed integer a such that each integer n can be written as a "power" of a. Now, since the operation is addition, we know that

$$a^k = \underbrace{a + a + ... + a}_{k \text{ times}} = ka$$

Therefore, saying that $a^k = n$ means that $n = ka$ in this context. Of course, this equation will be true if we let $a = 1$ and $k = n$. Therefore, we may conclude that $\mathcal{Z}$ is cyclic with $a = 1$ as a generator.

****

Example 49 *Prove that the additive group $\mathcal{Z}_n$ is cyclic for every positive integer $n > 1$. How many generators are there for the additive group $\mathcal{Z}_6$?*

Solution. Remember that the operation on $\mathcal{Z}_n$ is addition modulo n. To prove that $\mathcal{Z}_n$ is cyclic, we need to find an element a of $\mathbb{Z}_n$ such that k can be written as a "power" of a for each $k \in \mathbb{Z}_n$. Once again, the element $a = 1$ fits the bill, since

$$1^k = \underbrace{(1 + 1 + ... + 1)}_{k \text{ times}} \texttt{MOD}(n) = k(1)\texttt{MOD}(n) = k$$

Now, consider the group $\mathcal{Z}_6 = (\{[0], [1], [2], [3], [4], [5]\}, \boxplus)$, where $\boxplus$ is addition modulo 6. We already know that [1] is a generator. To see if there are any other generators, we construct the cyclic subgroup generated by each element. Observe that

- $\langle [0] \rangle = \{[0]\}$
- $\langle [1] \rangle = \{[1], [2], [3], [4], [5], [0]\} = \mathbb{Z}_6$
- $\langle [2] \rangle = \{[2], [4], [0]\}$
- $\langle [3] \rangle = \{[3], [0]\}$
- $\langle [4] \rangle = \{[4], [2], [0]\}$
- $\langle [5] \rangle = \{[5], [4], [3], [2], [1], [0]\} = \mathbb{Z}_6$

  We see that the group$\mathcal{Z}_6$ actually has two generators, namely [1] and [5].

****

Example 50 *Show that the subgroup $H = \langle \{([2]_3, [2]_6), ([2]_3, [4]_6)\} \rangle$ of $\mathcal{Z}_3 \times \mathcal{Z}_6$ is not cyclic.*

Solution. To see why this is true, we construct $\langle a \rangle$ for every element of H. Observe that, since the operation on H is addition modulo 3 in the first coordinate and addition modulo 6 in the second, we know $(x, y)^n = (nx \ \texttt{MOD}(3), ny \ \texttt{MOD}(6))$. For the sake of readability, we will suppress the residue class notation and simply work with the smallest nonnegative representative of each class. Observe that

$$\langle (0,0) \rangle = \{(0,0)\} \qquad \langle (2,2) \rangle = \{(0,0), (2,2), (1,4)\} \qquad \langle (1,4) \rangle = \{(0,0), (2,2), (1,4)\}$$

$$\langle (2,4) \rangle = \{(0,0), (2,4), (1,2)\} \qquad \langle (1,2) \rangle = \{(0,0), (2,4), (1,2)\} \qquad \langle (0,4) \rangle = \{(0,0), (0,4), (0,2)\}$$

$$\langle (0,2) \rangle = \{(0,0), (0,4), (0,2)\} \qquad \langle (1,0) \rangle = \{(0,0), (1,0), (2,0)\} \qquad \langle (2,0) \rangle = \{(0,0), (1,0), (2,0)\}$$

****

You may have noticed in the last two examples that $\langle a \rangle$ is always equal to $\left\langle a^{-1} \right\rangle$. A moment's thought proves that this must be true in any group, since a is an integer power of a^{-1} and vice-versa. Generators for cyclic groups are not necessarily unique.

Example 51 *Construct the subgroup* $\langle \{([2]_3, [2]_4), ([2]_3, [0]_4)\} \rangle$ *in the group* $\mathcal{Z}_3 \times \mathcal{Z}_4$ *and show that it is cyclic.*

Solution. Once again, we will suppress the residue class notation for the sake of readability. In this case, we start with the set

$$H_1 = \{(0,0), (2,2), (1,2), (2,0), (1,0)\}$$

This set contains the elements $(2,2)$ and $(2,0)$, along with their inverses and the identity. Unfortunately, this set is not closed under the operation, since $(1,2) * (2,0) = (0,2)$. Since $(0,2)$ is its own inverse, and since no other products of elements from H_1 yield different elements, it seems like

$$H_2 = \{(0,0), (2,2), (1,2), (2,0), (1,0), (0,2)\}$$

is the set we seek. Constructing the operation table proves that this is the case.

$*$	$\mathbf{(0,0)}$	$\mathbf{(2,2)}$	$\mathbf{(1,2)}$	$\mathbf{(2,0)}$	$\mathbf{(1,0)}$	$\mathbf{(0,2)}$
$\mathbf{(0,0)}$	$(0,0)$	$(2,2)$	$(1,2)$	$(2,0)$	$(1,0)$	$(0,2)$
$\mathbf{(2,2)}$	$(2,2)$	$(1,0)$	$(0,0)$	$(1,2)$	$(0,2)$	$(2,0)$
$\mathbf{(1,2)}$	$(1,2)$	$(0,0)$	$(2,0)$	$(0,0)$	$(2,2)$	$(1,0)$
$\mathbf{(2,0)}$	$(2,0)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$	$(2,2)$
$\mathbf{(1,0)}$	$(1,0)$	$(0,2)$	$(2,2)$	$(0,0)$	$(2,0)$	$(1,2)$
$\mathbf{(0,2)}$	$(0,2)$	$(2,0)$	$(1,0)$	$(2,2)$	$(1,2)$	$(0,0)$

To prove that $H = \langle \{(2,2), (2,0)\} \rangle$ is cyclic, we must find a member a of H such that $H = \langle a \rangle$. Observe that

$$\langle (2,2) \rangle = \{(0,0), (2,2), (1,0), (0,2), (2,0), (1,2)\} = H$$

Therefore, H is indeed cyclic. Both $([2]_3, [2]_4)$ and $([1]_3, [2]_4)$ serve as generators.

****

Theorem 52 *Let* $m > 1$ *be a positive integer. Every subgroup of* $\mathcal{Z}_m$ *is cyclic.*

Proof. Let H be a subgroup of $\mathcal{Z}_m$. Either H contains a single residue class, or it does not. If H contains a single residue class, then we must have $H = \{[0]_m\}$, and it is clear that $H = \langle [0]_m \rangle$. Suppose that H contains more than one residue class. It follows that there exists a smallest positive integer $0 < a < m$ such that $[a]_m \in H$. We will prove that $H = \langle [a]_m \rangle$. To do this, we will need to show that every element of H is a "power" of $[a]_m$. To this end, let $[b]_m \in H$. The Division Algorithm tells us that $b = ka + r$ for some integers k and r such that $0 \leq r < a$. Now, since H is closed under addition modulo m, we know that $[b - ka]_m$ is a member of H. Observe that

$$[b - a^k] \ \texttt{MOD}(m) = [(ka + r) - ka] \ \texttt{MOD}(m) = r \ \texttt{MOD}(m)$$

Thus, we know that $[r]_m \in H$. However, since we have selected a to be the *smallest positive* integer $0 < a < m$ such that $[a]_m \in H$, we must conclude that $r = 0$. Therefore, we know that $[b]_m = [ka]_m = ([a]_m)^k$. We may conclude that every member of H is a "power" of a, as desired.

QED

Virtually the same argument used to prove the last result can also be used to prove that every subgroup of the group $\mathcal{Z}$ of integers is also cyclic (just drop the modulo m component). The fact that every subgroup of a cyclic group is itself cyclic, coupled with the following result, makes finding the subgroups of cyclic groups simple. We begin with a basic consequence of the Division Algorithm which is very important in elementary number theory.

Theorem 53 *Let $m > 1$ be a positive integer. An element $[a]_m$ of $\mathcal{Z}_m$ is a generator for $\mathcal{Z}_m$ if and only if a and m are relatively prime.*

Proof. First, suppose that $[a]_m$ is a generator for $\mathcal{Z}_m$. This means that $[a]_m$ has order m in the group $\mathcal{Z}_m$; and this means that m is the smallest positive integer such that $ma = 0 \ \texttt{MOD}(m)$. Suppose by way of contradiction that a and m have a common factor $b > 1$. This means that $a = kb$ for some integer k and $m = jb$ for some integer j. Clearly we must have $j < m$; however, we also must have

$$ja = j(bk) = (jb)k = mk = 0 \ \texttt{MOD}(m)$$

This is impossible, since we have assumed that m is the smallest positive integer with this property. Consequently, we must conclude that a and m have no common positive factors other than 1.

On the other hand, suppose that a and m are relatively prime. Since this implies that $\texttt{GCF}(a, m) = 1$, there exist integers x and y such that $1 = ax + my$. We need to show that $[a]_m$ has order m in the group $\mathcal{Z}_m$. Since $\mathcal{Z}_m$ is a finite group, we know that $[a]_m$ has finite order. Let k be the order of $[a]_m$. It is clear that $k \leq m$, since we know that $([a]_m)^m = [ma]_m = [0]_m$. Now, we know that

$$k = k(ax + my) \quad \Longrightarrow \quad k = m(x + ky)$$

Consequently, we see that k is a multiple of m. Since $0 < k \leq m$, we must conclude that $k = m$, as desired.

QED

Theorem 54 *Let $m > 1$ be a positive integer. The subgroups of $\mathcal{Z}_m$ are generated by the residue classes whose representatives are positive divisors of m.*

Proof. If r is a positive divisor of m, then clearly $[r]_m \in \mathbb{Z}_m$ and therefore generates a subgroup of $\mathcal{Z}_m$. Suppose that H is a subgroup of $\mathcal{Z}_m$. We need to show that H is generated by a residue class whose representative is a divisor of m. The trivial subgroup $\{[0]_m\}$ is generated by $[m]_m$, so suppose that H is a nontrivial subgroup of $\mathcal{Z}_m$. There exists a smallest positive integer $0 < a < m$ such that $[a]_m \in H$; and we know that $H = \langle [a]_m \rangle$. Let b be the greatest common factor of m and a. Clearly b is a positive divisor of m. We will prove that $a = b$.

Clearly we have $0 < b \leq a$. Since b is the greatest common factor of a and m, we know that there exist integers x and y such that $b = ax + my$. Consequently, we know that $b = ax \ \texttt{MOD}(m)$; and this tells us that $[b]_m = ([a]_m)^x$. Since H is closed under addition modulo m, we may conclude that $[b]_m \in H$. Since a is the *smallest* positive integer such that $[a]_m \in H$, we must conclude that $b = a$, as desired.

QED

Example 55 *Construct all of the subgroups for* $\mathcal{Z}_{30}$.

Solution. The previous result makes this task relatively easy. Note that the positive divisors of $m = 30$ are $1, 2, 3, 5, 6, 10, 15$ and 30. Each of these will generate a distinct subgroup of $\mathcal{Z}_{30}$, and there will be no others. In particular,

$$\langle [1] \rangle = \mathbb{Z}_{30}$$

$$\langle [2] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14], [16], [18], [20], [22], [24], [26], [28]\}$$

$$\langle [3] \rangle = \{[0], [3], [6], [9], [12], [15], [18], [21], [24], [27]\} \qquad \langle [5] \rangle = \{[0] . [5], [10], [15], [20], [25]\}$$

$$\langle [6] \rangle = \{[0], [6], [12], [18], [24]\} \qquad \langle [10] \rangle = \{[0], [10], [20]\} \qquad \langle [15] \rangle = \{[0], [15]\} \qquad \langle [30] \rangle = \{[0]\}$$

****

Theorem 56 *Let* $m > 1$ *be a positive integer and suppose that* j *and* k *are positive divisors of* m. *If* $\langle [j]_m \rangle = \langle [k]_m \rangle$, *then* $j = k$.

Proof. Suppose $\langle [j]_m \rangle = \langle [k]_m \rangle$. This tells us that there exist integers r and s such that $([j]_m)^r = [k]_m$ and $([k]_m)^s = [j]_m$. Of course, this means that

$$j \equiv sk \texttt{MOD}(m) \qquad k \equiv rj \texttt{MOD}(m)$$

Since j and k are divisors of m we know that there exist integers a and b such that $m = aj$ and $m = bk$. Consequently, we know that $j \equiv sk \texttt{MOD}(k)$ and $k \equiv rj \texttt{MOD}(j)$. This tells us that $j \equiv 0 \texttt{MOD}(k)$ and $k \equiv 0 \texttt{MOD}(j)$ which in turn tells us that $j|k$ and $k|j$. Therefore, we must conclude that $j = \pm k$ by Theorem 1.2.7(8). However, since we have assumed that j and k are *positive*, we must now conclude that $j = k$.

QED

Determining the number of subgroups a given group contains is a very difficult task. However, the previous theorem gives us a simple way to count the number of subgroups for $\mathcal{Z}_m$ — the number of subgroups for this group is precisely the number of positive divisors for m.

Lemma 57 *Let* m *and* n *be positive integers larger than* 1. *If* $[a]_m \in \mathbb{Z}_m$ *has order* j *and if* $[b]_n \in \mathbb{Z}_n$ *has order* k, *then the order of* $([a]_m, [b]_n)$ *in* $\mathcal{Z}_m \times \mathcal{Z}_n$ *will be the least common multiple of* j *and* k.

Proof. Suppose that c is the order of $([a]_m, [b]_n)$. This means that $([a]_m, [b]_n)^c = ([0]_m, [0]_n)$; and we know this can happen if and only if c is a multiple of j and c is a multiple of k. Therefore, c must be a common multiple of j and k. Furthermore, since c is the *smallest* positive integer such that $([a]_m, [b]_n)^c = ([0]_m, [0]_n)$, it follows that c is the least common multiple of j and k.

QED

Theorem 58 *Let* m *and* n *be positive integers larger than* 1. *The group* $\mathcal{Z}_m \times \mathcal{Z}_n$ *is cyclic if and only if* m *and* n *are relatively prime.*

Proof. First, suppose that $\mathcal{Z}_m \times \mathcal{Z}_n$ is cyclic. This means that $\mathcal{Z}_m \times \mathcal{Z}_n$ has a generator $([a]_m, [b]_n)$. Clearly the order of $([a]_m, [b]_n)$ must be mn since this is the number of elements in $\mathcal{Z}_m \times \mathcal{Z}_n$. The previous lemma therefore tells us that the least common multiple of the orders for $[a]_m$ and $[b]_n$ must be mn. This occurs only if the greatest common factor of m and n is 1.

On the other hand, suppose that the greatest common factor of m and n is 1. This means that the least common multiple of m and n is mn. Let $[a]_m \in \mathbb{Z}_m$ be a generator for $\mathcal{Z}_m$ and let $[b]_n \in \mathbb{Z}_n$ be a generator for $\mathcal{Z}_n$. It follows that $[a]_m$ has order m and $[b]_n$ has order n. Consequently, we know from the previous lemma that the order of $([a]_m, [b]_n)$ must be mn. It follows that $([a]_m, [b]_n)$ is a generator for $\mathcal{Z}_m \times \mathcal{Z}_n$; and we may conclude that $\mathcal{Z}_m \times \mathcal{Z}_n$ is cyclic.

QED

EXERCISES FOR SECTION 3

1. Construct all of the subgroups for the group $\mathcal{Z}_{25}$.
2. Construct all of the subgroups for the group $\mathcal{Z}_{40}$.
3. How many generators will the group $\mathcal{Z}_{50}$ have?
4. How many subgroups does $\mathcal{Z}_{50}$ have?
5. Without constructing the subgroups, prove that $\mathcal{Z}_{12}$ has the same number of subgroups as $\mathcal{Z}_{20}$.
6. Consider the group $\mathcal{M}_2$ of all 2×2 matrices having real entries and nonzero determinant under matrix multiplication. Show that the set
$$H = \{A \in M_2 : \texttt{Det}(A) = 1\}$$
is a subgroup of $\mathcal{M}_2$.
7. Show that the set $H = \{A \in M_2 : A \text{ is diagonal}\}$ is a subgroup of $\mathcal{M}_2$.
8. Construct the subgroup $\langle\{(35), (12) \circ (35)\}\rangle$ in the group $\mathcal{P}_5$.
9. Construct the subgroup $\langle\{([1]_2, [0]_4), ([0]_2, [2]_4)\}\rangle$ in the group $\mathcal{Z}_2 \times \mathcal{Z}_4$.
10. Construct the subgroup $\langle\{([1]_3, [0]_3), ([0]_3, [1]_3)\}\rangle$ in the group $\mathcal{Z}_3 \times \mathcal{Z}_3$.
11. Construct the subgroups $\langle R_{270}\rangle$ and $\langle\{R_{180}, F_{13}\}\rangle$ in the Octic Group.
12. What is the order of the element $[8]_{100}$ in the group $\mathcal{Z}_{100}$?
13. Is the group $\mathcal{U}_{20}$ of units modulo 20 a cyclic group?
14. Is the group $\mathcal{U}_{19}$ of units modulo 19 a cyclic group?
15. Consider the groups $\mathcal{Z}_2 \times \mathcal{Z}_9$ and $\mathcal{Z}_3 \times \mathcal{Z}_6$.
    (a) Explain why $\mathcal{Z}_2 \times \mathcal{Z}_9$ is cyclic while $\mathcal{Z}_3 \times \mathcal{Z}_6$ is not.
    (b) List all of the generators for $\mathcal{Z}_2 \times \mathcal{Z}_9$. (Consider the order of each element.)
    (c) Which elements in $\mathcal{Z}_3 \times \mathcal{Z}_6$ have the largest order?
16. Let $\mathcal{G} = (G, *)$ be any group and let $a \in G$. Show that the set
$$C_a = \{b \in G : a * b = b * a\}$$
is a subgroup of $\mathcal{G}$. (This subgroup is called the *centralizer* of a — note that it is the set of all elements which commute with a.)

17. Find the centralizer of (13) in the group $\mathcal{P}_3$.

18. Find the centralizer of F_{24} in the Octic Group.

19. Let $\mathcal{G} = (G, *)$ be any group and let $a, b \in G$. The *commutator* of a and b is the element $[a, b] = (a * b) * (b * a)^{-1}$. An element $x \in G$ is a *commutator* provided $x = [a, b]$ for some $a, b \in G$.

    (a) Explain why the identity element is the only commutator in an abelian group.

    (b) Show that $[b, a] = [a, b]^{-1}$.

    (c) Find all of the commutators for the group $\mathcal{P}_3$ and show that they form a subgroup of $\mathcal{P}_3$.

    (d) Find all of the commutators for the Octic Group and show that they form a subgroup of this group.

20. Let $\mathcal{G} = (G, *)$ be a group and let H, K be subgroups of $\mathcal{G}$. Let $HK = \{h * k : h \in H, k \in K\}$.

    (a) If $\mathcal{G}$ is abelian, prove that HK is a subgroup of $\mathcal{G}$.

    (b) Give a counterexample to show that HK may not be a subgroup when $\mathcal{G}$ is nonabelian.

21. Let $\mathcal{G} = (G, *)$ be a group, let $a \in G$, and let H be a subgroup of $\mathcal{G}$. Show that the set $aHa^{-1} = \{a * h * a^{-1} : h \in H\}$ is always a subgroup of $\mathcal{G}$.

22. Let $\mathcal{G} = (G, *)$ be a group, let $a \in G$, and let H be a subgroup of $\mathcal{G}$. If $aHa^{-1} \subseteq H$, prove that $H = aHa^{-1}$.

23. Let $\mathcal{G} = (G, *)$ be a group and let H be a subgroup of $\mathcal{G}$. The set $N_H = \{a \in G : aHa^{-1} = H\}$ is called the *normalizer* of H.

    (a) Show that $H \subseteq N_H$.

    (b) Show that $N_H = G$ when $\mathcal{G}$ is abelian.

    (c) Show that N_H is always a subgroup of $\mathcal{G}$.

24. Find the normalizer for $H = \langle (13) \rangle$ in the group $\mathcal{P}_3$.

25. Find the normalizer for $H = \langle F_{24} \rangle$ in the Octic Group.

26. Find the normalizer for $H = \langle (123) \rangle$ in the group $\mathcal{P}_3$.

4 COSETS

In this section, we explore a way to create equivalence relations on groups. This process leads to useful insights into subgroups and develops powerful tools for better understanding the structure of groups.

Definition 59 *Let $\mathcal{G} = (G, *)$ be any group and let $H \subseteq G$ be a subgroup of $\mathcal{G}$. For each $a \in G$, let*

$$aH = \{a * x : x \in H\} \qquad Ha = \{x * a : x \in H\}$$

*We call aH the **left coset** of H generated by a, and we call Ha the **right coset** of H generated by a.*

Example 60 *In the symmetric group $\mathcal{P}_4$ of permutations on a six-element set, construct the cosets $(12)H$ and $H(12)$ for the subgroup*

$$H = \langle (1234) \rangle = \{\epsilon, (1234), (13)(24), (1432)\}$$

Solution. We have

$$(12)H = \{(12)\circ\epsilon, (12)\circ(1234), (12)\circ(13)(24), (12)\circ(1432)\} = \{(12), (234), (1324), (143)\}$$

$$H(12) = \{\epsilon\circ(12), (1234)\circ(12), (13)(24)\circ(12), (1432)\circ(12)\} = \{(12), (134), (1423), (243)\}$$

****

Notice that $(12)H \neq H(12)$ in the previous example. The two cosets do have the same number of elements, however. This always turns out to be the case.

Theorem 61 *Let $\mathcal{G} = (G, *)$ be any group and let $H \subseteq G$ be a subgroup of $\mathcal{G}$. For each $a \in G$, there is a bijection between H and Ha and between H and aH.*

Proof. We already know that the function $\varphi : G \longrightarrow G$ defined by $\varphi_a(x) = x * a$ is a bijection for any fixed $a \in G$. Consequently, the restriction of this function to H provides a bijection between H and Ha. Likewise, the restriction to H of the function $\psi : G \longrightarrow G$ defined by $\psi_a(x) = a * x$ provides a bijection between H and aH.

QED

Corollary 62 *Let $\mathcal{G} = (G, *)$ be any group and let $H \subseteq G$ be a subgroup of $\mathcal{G}$. There is a bijection between aH and Hb for any $a, b \in G$.*

Proof. The function $f : aH \longrightarrow Hb$ defined by $f = \psi_a^{-1} \circ \varphi_b$ provides the desired bijection.

QED

The previous result gives us a key fact about left and right cosets: If H is a finite subgroup of a group $\mathcal{G} = (G, *)$, then the left and right cosets of H all have the same number of elements as H.

Theorem 63 *Let $\mathcal{G} = (G, *)$ be any group and let $H \subseteq G$ be a subgroup of $\mathcal{G}$. The set $L_H = \{aH : a \in G\}$ forms a partition of the set G. The equivalence relation induced by L_H is defined by $(x, y) \in \theta \Longleftrightarrow y^{-1} * x \in H$.*

Proof. To prove that L_H is a partition of G, we must show that every member of G is contained in exactly one member of L_H. Since H is a subgroup of $\mathcal{G}$, we know that the identity e of $\mathcal{G}$ is a member of H. Consequently, we know that $a \in aH$ for every $a \in G$. Thus, every member of G is contained in *at least* one member of L_H. Suppose now that $a \in bH$ for some $b \in G$. We need to show that $aH = bH$. To this end, suppose that $u \in aH$. This means that $u = a * y$ for some $y \in H$; to prove that $aH \subseteq bH$, we need to show that $u = a * z$ for some $z \in H$. Now, since $a \in bH$, we know that $a = b * x$ for some $x \in H$; and this tells us that $x = b^{-1} * a$. Consequently, since $x \in H$, we may conclude that $b^{-1} * a \in H$. Therefore, since H is closed under the operation, we know that $z = b^{-1} * a * y \in H$. Thus, we know that

$$u = a * y \quad \Longrightarrow \quad u = (b * b^{-1}) * (a * y) \quad \Longrightarrow \quad u = b * (b^{-1} * a * z) \quad \Longrightarrow \quad u = b * z$$

We may conclude that $aH \subseteq bH$. On the other hand, suppose that $v \in bH$. To prove that $bH \subseteq aH$, we must show that $v = a * t$ for some $t \in H$. Since we know $b^{-1} * a \in H$ and since H is closed under the

formation of inverses, we know that $a^{-1} * b = (b^{-1} * a)^{-1} \in H$. Since $v \in bH$, we know that $v = b * s$ for some $s \in H$. Now, we know that $t = a^{-1} * b * s \in H$; therefore

$$v = b * s \quad \Longrightarrow \quad v = (a * a^{-1}) * (b * s) \quad \Longrightarrow \quad v = a * (a^{-1} * b * s) \quad \Longrightarrow \quad u = a * t$$

We may conclude that $aH \subseteq bH$; therefore, we know that $aH = bH$.

To complete the proof, we need to describe the equivalence relation defined by this partition. We know that

$$\begin{aligned}
(x, y) \in \theta &\iff x, y \in aH \text{ for some } a \in G \\
&\iff x = a * h \text{ and } y = a * j \text{ for some } a \in G \text{ and } h, j \in H \\
&\iff x * h^{-1} = y * j^{-1} \text{ for some } h, j \in H \\
&\iff y^{-1} * x = j^{-1} * h \text{ for some } h, j \in H \\
&\iff y^{-1} * x \in H
\end{aligned}$$

QED

Of course, this theorem could also be stated using right cosets instead of left cosets. If $\mathcal{G} = (G, *)$ is any group and H is any subgroup of $\mathcal{G}$, then $R_H = \{Ha : a \in G\}$ forms a parition of G; and the equivalence relation induced by this partition is defined by $(x, y) \in \theta \iff x * y^{-1} \in H$. The proof of this result is left as an exercise.

Example 64 *Construct the partition L_H of the group $\mathcal{P}_4$ created by the subgroup $H = \langle(1234)\rangle$.*

Proof. We know that every member of L_H will contain exactly four elements since H contains exactly four elements. Since every element of the twenty-four element set $\wp_4$ must appear in exactly one of the members of L_H, we may conclude that L_H comtains exactly six sets. We have already found two of them. One member of the partition L_H must be the set H itself, since $aH = H$ whenever $a \in H$. We also know that

$$(12)H = \{\{(12), (234), (1324), (143)\}\}$$

is a member of L_H by our previous example. There are four more cosets left to find. We can construct another simply by choosing any permutation from P_4 that does not appear in H or $(12)H$ and using it to form a left coset. For example, (13) does not appear in either coset; hence it will generate a third coset. Observe

$$(13)H = \{(13) \circ \epsilon, (13) \circ (1234), (13) \circ (13)(24), (13) \circ (1432)\} = \{(13), (12)(34), (24), (14)(32)\}$$

None of the elements appearing in $(13)H$ will appear in any other left coset generated by H. One thing this tells us is that $(13)H = (13)(34)H = (24)H = (14)(32)H$ — all of these are just different names for the same left coset. To construct the fourth left coset, select any permutation that does not appear in H, $(12)H$, or $(13)H$. For example, (34) does not appear in any of these cosets. Observe

$$(34)H = \{(34) \circ \epsilon, (34) \circ (1234), (34) \circ (13)(24), (34) \circ (1432)\} = \{(34), (124), (1423), (132)\}$$

The remaining two left cosets can be found using the same strategy. Observe

$$(14)H = \{(14) \circ \epsilon, (14) \circ (1234), (14) \circ (13)(24), (14) \circ (1432)\} = \{(14), (123), (1342), (243)\}$$

$$(134)H = \{(134) \circ \epsilon, (134) \circ (1234), (134) \circ (13)(24), (134) \circ (1432)\} = \{(134), (1243), (142), (23)\}$$

****

Example 65 *The set $\mathbb{Z}$ of integers is a subgroup of $\mathcal{Q} = (\mathbb{Q}, +)$. Describe the members of $L_{\mathbb{Z}}$ and the equivalence relation induced by it.*

Solution. We can construct the equivalence relation even without knowing what the members of $L_{\mathbb{Z}}$ are. According to the previous theorem, we know that

$$(x, y) \in \theta \iff y^{-1} * x \in \mathbb{Z} \iff x - y \in \mathbb{Z}$$

In other words, a pair of rational numbers is a member of θ if and only if their difference is an integer. Now, let's describe the members of $L_{\mathbb{Z}}$. For each fixed $a \in \mathbb{Q}$, the coset $a\mathbb{Z}$ has the form

$$a\mathbb{Z} = \{a + m : m \in \mathbb{Z}\}$$

This is a perfectly good description of the left cosets, but we can use the special properties of rational numbers to clarify it. Suppose that $a = p/q$, where p and q are integers. The Division Algorithm tells us that there exist unique integers m and r such that $0 \leq r < q$ and $p = mq + r$. It follows that

$$a = \frac{p}{q} \implies a = m + \frac{r}{q}$$

If we call the fraction r/q the *proper part of* a, then we can say that *two rational numbers are in the same left coset if and only if they have the same proper part.* Now, the proper part of any rational number is a member of $\mathbb{Q} \cap [0, 1)$. Consequently, the members of $L_{\mathbb{Z}}$ have the form

$$u\mathbb{Z} = \{u + m : m \in \mathbb{Z}\}$$

where $u \in \mathbb{Q} \cap [0, 1)$.

****

The notion of left or right coset gives us a simple proof of one of the most important results in group theory. This result, known as *Lagrange's Theorem*, provides a powerful tool for determining when a subset of a group is actually a subgroup of that group.

Theorem 66 *Let $\mathcal{G} = (G, *)$ be any finite group. If H is a subgroup of $\mathcal{G}$, then the number of elements in H must be a divisor of the number of elements in G.*

Proof. Suppose that G contains exactly n elements and suppose that H contains exactly m elements. Consider the partition $L_H = \{aH : a \in G\}$. This partition contains exactly k members for some positive integer k. Every member of L_H must contain exactly m elements, and every element of G must appear in exactly one member of L_H. Consequently, we must have $n = km$; and it follows that m is a divisor of n.

QED

Definition 67 *Let $\mathcal{G} = (G, *)$ be any finite group and let H be any subgroup of G. The number of elements in G is called the **order** of the group $\mathcal{G}$; it is often denoted by $|G|$. The number of left (or right) cosets generated by H is called the **index** of H in the group $\mathcal{G}$; it is often denoted by $[G : H]$.*

Example 68 *The order of a certain group $\mathcal{G}$ is* 168. *If a subgroup H of $\mathcal{G}$ has index* 24, *then what must be the order of H?*

Solution. Lagrange's Theorem tells us that $|H| = |G|/[G : H]$. Consequently, we know that $|H| = 168/24 = 7$.

****

Corollary 69 *Every group of prime order must be cyclic.*

Proof. Suppose that $\mathcal{G} = (G, *)$ has prime order p. Since p is prime, we know that the only positive divisors of p are one and p. Consequently, we know by Lagrange's Theorem that $\mathcal{G}$ can have only two subgroups, namely the trivial subgroup $\{e\}$ and the set G itself. Since G has order greater than 1, we know that G must contain some element $a \neq e$. We know that $\langle a \rangle \neq \{e\}$; hence, it must be the case that $\langle a \rangle = G$. We may therefore conclude that G is cyclic, as desired.

QED

Lagrange's Theorem is helpful when we are trying to construct subgroups of a finite group. If a group has order n, we can easily find the positive divisors of n; these divisors are the only possibilities for the orders of subgroups for the group.

Example 70 *The operation table for the Octic Group is given below. Construct the subgroup generated by* $X = \{R_{90}, F_v, F_{13}\}$.

$\circ$	R_0	R_{90}	R_{180}	R_{270}	F_{13}	F_{24}	F_v	F_h
R_0	R_0	R_{90}	R_{180}	R_{270}	F_{13}	F_{24}	F_v	F_h
R_{90}	R_{90}	R_{180}	R_{270}	R_0	F_v	F_h	F_{24}	F_{13}
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_{24}	F_{13}	F_h	F_v
R_{270}	R_{270}	R_0	R_{90}	R_{180}	F_h	F_v	F_{13}	F_{24}
F_{13}	F_{13}	F_h	F_{24}	F_v	R_0	R_{180}	R_{270}	R_{90}
F_{24}	F_{24}	F_v	F_{13}	F_h	R_{180}	R_0	R_{90}	R_{270}
F_v	F_v	F_{13}	F_h	F_{24}	R_{90}	R_{270}	R_0	R_{180}
F_h	F_h	F_{24}	F_v	F_{13}	R_{270}	R_{90}	R_{180}	R_0

Solution. We begin by adding in the identity element and the inverse of each element in X to create the set

$$H = \{R_0, R_{90}, R_{270}, F_v, F_{13}\}$$

The set H contains five elements. Since the Octic Group contains eight elements, the only possible orders for $\langle X \rangle$ are 1, 2, 4, and 8. We see that $\langle X \rangle$ must contain at least five elements; hence, LaGrange's Theorem allows us to conclue that $\langle X \rangle$ must be the Octic Group itself. No additional work is necessary.

****

We will conclude this section by taking a closer look at Theorem 63. This result tells us that whenver H is a subgroup of a group $\mathcal{G} = (G, *)$, then the set $\theta_H = \{(x, y) \in G \times G : y^{-1} * x \in H\}$ is an equivalence relation. We know that there is a natural way to place a group structure on the set $G \times G$, namely the product group structure defined by

$$(a, b) \otimes (c, d) = (a * c, b * d)$$

Is it ever true that θ_H is a *subgroup* of the product group $\mathcal{G} \times \mathcal{G}$?

Theorem 71 *If $\mathcal{G} = (G, *)$ is an abelian group and H is a subgroup of $\mathcal{G}$, then θ_H is always a subgroup of $\mathcal{G} \times \mathcal{G}$.*

Proof. We need to show that θ_H is closed under the operation $\otimes$ and closed with respect to the formation of inverses. To this end, suppose that $(a, b), (c, d) \in \theta_H$. We need to prove that $(a * c, b * d) \in \theta_H$ and we need to prove that $(a^{-1}, b^{-1}) \in \theta_H$. Now, $(a, b), (c, d) \in \theta_H$ tells us that $b^{-1} * a \in H$ and $d^{-1} * c \in H$. Since we have assumed that $\mathcal{G}$ is abelian, the fact that H is closed under the operation $*$ tells us

$$(b * d)^{-1} * (a * c) = (b^{-1} * a) * (d^{-1} * c) \in H$$

Consequently, we may conclude that $(a * c, b * d) \in \theta_H$. Furthermore, since H is closed under the formation of inverses, the fact that $b^{-1} * a \in H$ tells us

$$\left[b^{-1} * a\right]^{-1} = a^{-1} * b \in H$$

Since we have assumed that $\mathcal{G}$ is abelian, this implies that $b * a^{-1} \in H$; and this allows us to conclude that $(a^{-1}, b^{-1}) \in \theta_H$, as desired.

QED

The proof of the previous theorem relies heavily on the assumption that the group $\mathcal{G}$ is abelian. The story gets much more interesting when we drop the assumption that our group is abelian.

Example 72 *Consider the subgroup $H = \langle(1234)\rangle$ in the group $\mathcal{P}_4$. Is the equivalence relation θ_H a subgroup of $\mathcal{P}_4 \times \mathcal{P}_4$?*

Solution. The equivalence relation θ_H will be quite a large set, so it is not practical to construct it directly. Observe that

$$H = \langle(1234)\rangle = \{\epsilon, (1234), (13)(24), (1432)\}$$

Now, observe that

$$(234) = (12) \circ (1234) \quad \Longrightarrow \quad (12) \circ (234) = (1234) \quad \Longrightarrow \quad (12) \circ (234) \in H \quad \Longrightarrow \quad [(234), (12)] \in \theta_H$$

However, observe that $[(234), (12)]^{-1} = [(243), (12)]$, and this pair is *not* a member of θ_H since $(12) \circ (243) = (1243) \notin H$. Consequently, θ_H is not a subgroup of $\mathcal{P}_4 \times \mathcal{P}_4$.

****

At this point, you would have a right to cry "foul" since it is not at all obvious where the counterexample came from that we just used. In truth, the counterexample is motivated by the fact that $(12)H \neq H(12)$ as we showed in Example 60 along with the following powerful theorem.

Theorem 73 *For any group $\mathcal{G} = (G, *)$ and subgroup H of $\mathcal{G}$ the following statements are equivalent.*

1. *The equivalence relation θ_H is a subgroup of $\mathcal{G} \times \mathcal{G}$.*
2. *For all $a \in G$ and all $h \in H$, we have $a * h * a^{-1} \in H$.*
3. *For all $a \in G$, we have $aH = Ha$.*

Proof. We will prove that Claim (1) implies Claim (2), Claim (2) implies Claim (3), and Claim (3) implies Claim (1). This logic "loop" will establish that these three statements are interchangeable. We begin by proving Claim (1) implies Claim (2). To this end, suppose that θ_H is a subgroup of $\mathcal{G} \times \mathcal{G}$ and let $a \in G$ and $h \in H$. We need to prove that $a * h * a^{-1} \in H$, and this is equivalent to proving $(h * a^{-1}, a^{-1}) \in \theta_H$. We know that $(a^{-1}, a^{-1}) \in \theta_H$ since θ_H is reflexive. We know that $e * h \in H$, and this tells us that $(h, e) \in \theta_H$. Since θ_H is closed under the operation $\otimes$ defined on $\mathcal{G} \times \mathcal{G}$, we therefore know

$$(h, e) \otimes (a^{-1}, a^{-1}) = (h * a^{-1}, a^{-1}) \in \theta_H$$

We now prove that Claim (2) implies Claim (3). To this end, suppose that for all $a \in G$ and all $h \in H$, we have $a * h * a^{-1} \in H$. We need to show that $aH = Ha$, and we will do this by showing $aH \subseteq Ha$ and $Ha \subseteq aH$. Suppose that $x \in aH$. This means there exist $h \in H$ such that $x = a * h$. To prove that $x \in Ha$, we need to find some $j \in H$ such that $x = j * a$. Now, $x = a * h$ certainly implies that $x * a^{-1} = a * h * a^{-1}$. If we let $j = a * h * a^{-1}$, then we know that $j \in H$; and we know $x = j * a$. Consequently, $x \in Ha$; and we may conclude that $aH \subseteq Ha$. On the other hand, suppose that $y \in Ha$. This means there exist $j \in H$ such that $y = j * a$. To prove that $y \in aH$, we need to find some $h \in H$ such that $y = a * h$. Of course, $y = j * a$ implies that $a^{-1} * y = a^{-1} * j * a$. Now, if $j \in H$, then we know $j^{-1} \in H$ as well since H is a subgroup of $\mathcal{G}$. Therefore, by assumption, we know that $a * j^{-1} * a^{-1} \in H$; and, since H is a subgroup of $\mathcal{G}$, we may conclude that $h = \left(a * j^{-1} * a^{-1}\right)^{-1} = a^{-1} * j * a$ is also a member of H. Since $y = a * h$, we may conclude that $y \in aH$; and this allows us to conclude that $Ha \subseteq aH$.

Finally, we prove that Claim (3) implies Claim (1). To this end, suppose that $aH = Ha$ for all $a \in G$. We need to show that θ_H is closed under the operation $\otimes$ and closed with respect to the formation of inverses. To this end, let $(a, b), (c, d) \in \theta_H$. This means that $b^{-1} * a \in H$ and $d^{-1} * c \in H$. Let's first consider $(a, b)^{-1}$. To prove that this element is a member of θ_H, we need to show that $b * a^{-1} \in H$. Since $b^{-1} * a \in H$ by assumption, we know that $a^{-1} * b \in H$ because H is closed with respect to the formation of inverses. Consequently, we know that $b * (a^{-1} * b) \in bH$. Since $bH = Hb$ by assumption, we know that $(b * a^{-1}) * b \in Hb$; and this allows us to conclude that $b * a^{-1} \in H$. Thus, we know that θ_H is closed with respect to the formation of inverses. To complete the proof, we must show that θ_H is closed under the operation $\otimes$. To show that $(a, b) \otimes (c, d) \in \theta_H$, we must prove that $(a * c, b * d) \in \theta_H$; and it will suffice to prove $(b * d)^{-1} * (a * c) \in H$. Now, we know that $b^{-1} * a \in H$. This implies that $d^{-1} * b^{-1} * a \in d^{-1}H$. Since we have assumed $d^{-1}H = Hd^{-1}$, we know that there exist $j \in H$ such that $d^{-1} * b^{-1} * a = j * d^{-1}$. This fact allows us to conclude that $(b * d)^{-1} * (a * d) \in H$. We also know that $d^{-1} * c \in H$. Since H is a subgroup of $\mathcal{G}$, it follows that

$$(b * d)^{-1} * (a * c) = (b * d)^{-1} * a * (d * d^{-1}) * c = (b * d)^{-1} * (a * d) * (d^{-1} * c) \in H$$

QED

Definition 74 *Let $\mathcal{G} = (G, *)$ be a group. A subgroup H of $\mathcal{G}$ is **normal** provided $aH = Ha$ for all $a \in G$. The equivalence relation it induces on G (which is necessarily a subgroup of $\mathcal{G} \times \mathcal{G}$) is called a **congruence** on the group $\mathcal{G}$.*

Notice that the subgroup $H = \langle(1234)\rangle$ in the group $\mathcal{P}_4$ is not normal since $(12)H \neq H(12)$. In light of the previous theorem, this tells us at once that θ_H is not a subgroup of $\mathcal{G} \times \mathcal{G}$. Of course, every subgroup of an abelian group is normal; and this is consistent with the conclusion of Theorem 71. Normal subgroups do exist in nonabelian groups, as the following example shows.

Example 75 *Show that the subgroup $H = \langle(123)\rangle$ is normal in the group $\mathcal{P}_3$ but is not normal in the group $\mathcal{P}_4$.*

Solution. When checking for normality, it is generally easiest to compare left and right cosets. We begin with an observation which will save us a lot of time:

If $x \in aH$, *then* $xH = aH$.

The reason this statement is true is simply that the left cosets of H form a partition of G, which means that the left cosets must be pairwise disjoint. It should be clear that $x \in xH$ (see the exercises for this section). Consequently, if $x \in aH$ it follows that $xH \cap aH \neq \varnothing$; and this forces us to conclude that $xH = aH$. Of course, the same statement is true for right cosets. The left cosets for H in the group $\mathcal{P}_3$ are

$$H = \{\epsilon, (123), (132)\} = \epsilon H = (123)H = (132)H$$

$$(12)H = \{(12), (23), (13)\} = (23)H = (13)H$$

The right cosets for H in the group $\mathcal{P}_3$ are

$$H = \{\epsilon, (123), (132)\} = H\epsilon = H(123) = H(132)$$

$$H(12) = \{(12), (13), (23)\} = H(23) = H(13)$$

It is now easy to see directly that $aH = Ha$ for all $a \in \wp_3$; hence, this subgroup is normal.

When checking for normality, it is a good idea to compute the left coset aH and the right coset Ha side by side. If the subgroup is not normal, then this approach will detect this property more quickly, since it only takes $aH \neq Ha$ for a single coset to disprove normality. We will use this approach to show that $H = \langle(1234)\rangle$ is not normal in the group $\wp_4$. Since H contains three elements and $\wp_4$ contains 24 elements, we know that H will create eight left and eight right cosets. Now, notice that if a fixes the number 4, then $aH = Ha$ by our previous computations; so we will move on to elements which do not fix 4. Observe that

$$(14)H = \{(14), (1234), (1324)\} \qquad H(14) = \{(14), (1423), (1432)\}$$

Since $(14)H \neq H(14)$, this is sufficient to prove that H is not normal in $\mathcal{P}_4$.

****

EXERCISES FOR SECTION 4

Exercises 1 - 5 deal with an interesting subgroup of $\mathcal{P}_4$ which we will call the "alphabet group." (It is an example of an important type of subgroup found in all finite permutation groups.) Let

$$E = \epsilon \qquad G = (123) \qquad H = (132) \qquad I = (12)(34) \qquad J = (243) \qquad K = (143)$$

$$L = (13)(24) \qquad M = (142) \qquad N = (234) \qquad O = (14)(23) \qquad P = (134) \qquad Q = (124)$$

The set $A_4 = \{E, G, H, I, J, K, L, M, N, O, P, Q\}$ is closed under function composition and is therefore a subgroup of $\mathcal{P}_4$. Its operation table is given below.

$\circ$	$\boldsymbol{E}$	$\boldsymbol{G}$	$\boldsymbol{H}$	$\boldsymbol{I}$	$\boldsymbol{J}$	$\boldsymbol{K}$	$\boldsymbol{L}$	$\boldsymbol{M}$	$\boldsymbol{N}$	$\boldsymbol{O}$	$\boldsymbol{P}$	$\boldsymbol{Q}$
$\boldsymbol{E}$	E	G	H	I	J	K	L	M	N	O	P	Q
$\boldsymbol{G}$	G	H	E	J	K	I	M	N	L	P	Q	O
$\boldsymbol{H}$	H	E	G	K	I	J	N	L	M	Q	O	P
$\boldsymbol{I}$	I	P	N	E	M	Q	O	J	H	L	G	K
$\boldsymbol{J}$	J	Q	L	G	N	O	P	K	E	M	H	I
$\boldsymbol{K}$	K	O	M	H	L	P	Q	I	G	N	E	J
$\boldsymbol{L}$	L	J	Q	O	G	N	E	P	K	I	M	H
$\boldsymbol{M}$	M	K	O	P	H	L	G	Q	I	J	N	E
$\boldsymbol{N}$	N	I	P	Q	E	M	H	O	J	K	L	G
$\boldsymbol{O}$	O	M	K	L	P	H	I	G	Q	E	J	N
$\boldsymbol{P}$	P	N	I	M	Q	E	J	H	O	G	K	L
$\boldsymbol{Q}$	Q	L	J	N	O	G	K	E	P	H	I	M

1. Identify all subgroups of the alphabet group. (There are ten — use Lagrange's Theorem to help you.)

2. Suppose $\mathcal{G}$ is a group of order n. Lagrange's Theorem tells us that every subgroup of $\mathcal{G}$ corresponds to a divisor of n. Explain why your answer to Exercise 1 shows that not all divisors of n necessarily correspond to a subgroup of $\mathcal{G}$.

3. Identify the commutators of the alphabet group. (See Exercise 3.19.)

4. Construct the left and right cosets for the subgroup $S = \langle M \rangle$ of the alphabet group. Is this subgroup normal in the alphabet group?

5. Construct the left and right cosets for the subgroup $T = \langle \{I, L\} \rangle$ in the alphabet group. Is this subgroup normal in the alphabet group?

6. Suppose that a group $\mathcal{G} = (G, *)$ contains exactly 200 elements and suppose that H is a subgroup of $\mathcal{G}$. If J is a subgroup of H that has order 10, what are the possible orders for H?

7. Suppose that a group $\mathcal{G} = (G, *)$ contains exactly 1000 elements and suppose that H is a subgroup of $\mathcal{G}$. If H has order 50, then what is $[G : H]$?

8. If a group $\mathcal{G} = (G, *)$ has prime order, explain why $\mathcal{G}$ is abelian.

9. Suppose that $\mathcal{G} = (G, *)$ is a subgroup of order pq where p and q are prime numbers. Use Lagrange's Theorem to prove that every proper subgroup of $\mathcal{G}$ is cyclic.

10. Let $\mathcal{G} = (G, *)$ be any group and let H be a subgroup of $\mathcal{G}$. Prove that $a \in aH$ and $a \in Ha$ for all $a \in G$.

11. Let $\mathcal{G} = (G, *)$ be any group, let $a \in G$, and let H be a subgroup of $\mathcal{G}$. Prove that $aH = H$ if and only if $a \in H$.

12. Let $\mathcal{G} = (G, *)$ be any group, let $a \in G$, and let H be a subgroup of $\mathcal{G}$. Prove that $(a * h)H = aH$ and $H(h * a) = Ha$ for all $h \in H$.

13. Let $\mathcal{G} = (G, *)$ be any group, let $a \in G$, and let H be a subgroup of $\mathcal{G}$. Prove that $aH = Ha$ if and only if $H = aHa^{-1}$.

14. Let $\mathcal{G} = (G, *)$ be any group, let $a \in G$, and let H be a subgroup of $\mathcal{G}$. Prove that $a \in Hb$ if and only if $b^{-1} * a \in H$.

15. Let $\mathcal{G} = (G, *)$ be any group of order n and let $a \in G$.

    (a) Use Lagrange's Theorem to explain why the order of the element a must be a divisor of n.

    (b) Prove that $a^n = e$, where e is the group identity.

16. Let p be any prime number. If a is an integer, use the previous exercise to prove that $a^p \equiv a \texttt{MOD}(p)$, where powers in this context refer to integer multiplication. (Consider $[a]_p$ in the group $\mathcal{U}_p$ of units modulo p.) This is an important result from number theory called *Fermat's Little Theorem*.

17. Prove Theorem 63 for right cosets.

18. Let n be a fixed positive integer and consider the subroup $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ of the group $\mathcal{Z} = (\mathbb{Z}, +)$. Prove that the left (and right) cosets of $n\mathbb{Z}$ in $\mathcal{Z}$ are the sets $A_r = \{r + nk : k \in \mathbb{Z}\}$, where $0 \leq r < n$. (Use the Division Alogrithm.)

19. Show that every group is a normal subgroup of itself.

20. Let $\mathcal{G} = (G, *)$ be any group and let H be a subgroup of $\mathcal{G}$. Prove that H is normal if and only if its normalizer is G. (See Exercise 3.22.)

21. Let $\mathcal{G} = (G, *)$ be any group and let H be a subgroup of $\mathcal{G}$. If H has index 2, prove that H must be normal in $\mathcal{G}$.

22. Consider the group $\mathcal{M}_2$. Is the subgroup $H = \{A \in M_2 : \texttt{Det}(A) = 1\}$ normal in $\mathcal{M}_2$?

23. Let $\mathcal{G} = (G, *)$ be any group and let $\mathcal{N}$ be a family of normal subgroups in $\mathcal{G}$. Prove that $\bigcap \mathcal{N} = \bigcap \{H : H \in \mathcal{N}\}$ is a normal subgroup of $\mathcal{G}$.

24. Let $\mathcal{G} = (G, *)$ be any group and let $Z(\mathcal{G}) = \{a \in G : a * g = g * a \text{ for all } g \in G\}$. (This set is called the *center* of $\mathcal{G}$.)

    (a) Show that $Z(\mathcal{G}) = \bigcap \{C_g : g \in G\}$ and is therefore a subgroup of $\mathcal{G}$. (See Exercise 3.16.)

    (b) Show that $Z(\mathcal{G})$ is always a normal subgroup of $\mathcal{G}$.

25. In this exercise, we prove that the center of $\mathcal{M}_2$ is the set of all nonzero scalar multiples of the identity matrix.

    (a) To begin, let $a \in \mathbb{R}^*$ and let I_2 be the 2×2 identity matrix. Explain why $(aI_2)M = M(aI_2)$ for all $M \in M_2$. This shows that $\{aI_2 : a \in \mathbb{R}^*\} \subseteq Z(\mathcal{M}_2)$.

    (b) Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(\mathcal{M}_2)$.

        i. Use the matrix $M = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ to show that we must have $b = c$.

        ii. Use the matrix $N = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$ to show that we must have $a = d$ and $b = 2c$.

        iii. Use Parts (i) and (ii) to explain why $Z(\mathcal{M}_2) \subseteq \{aI_2 : a \in \mathbb{R}^*\}$

26. Let $\mathcal{G} = (G, *)$ be any group. If H and K are normal subgroups of $\mathcal{G}$ such that $H \cap K = \{e\}$, then prove that $h * k = k * h$ for all $h \in H$ and $k \in K$.

27. Let $\mathcal{G} = (G, *)$ be any group and suppose that K is any subgroup of $\mathcal{G}$. Suppose further that H is a normal subgroup of $\mathcal{G}$.

    (a) Prove that $H \cap K$ is a normal subgroup of $(K, *)$ (where $*$ is restricted to K, of course).

    (b) Prove that $HK = \{h * k : h \in H, k \in K\}$ is a subgroup of $\mathcal{G}$.

    (c) Prove that H is a normal subgroup of $(HK, *)$ (where $*$ is restricted to HK, of course).

28. Let $\mathcal{G} = (G, *)$ be any group and suppose that K is a normal subgroup of $\mathcal{G}$. If H is also a normal subgroup of $\mathcal{G}$, then prove that $HK = \{h * k : h \in H, k \in K\}$ is a normal subgroup of $\mathcal{G}$.

29. The set $\mathbb{Z}$ of integers is a subgroup of $\mathcal{Q} = (\mathbb{Q}, +)$. We described the members of $L_{\mathbb{Z}}$ in this section. In this exercise, we will prove that the set $L_{\mathbb{Z}}$ is infinite. To this end, let $m \neq n$ in $\mathbb{Z}^+$ and consider the cosets

$$A = \frac{1}{m} + \mathbb{Z} \qquad B = \frac{1}{n} + \mathbb{Z}$$

    (a) If $A = B$, then prove that there must exist an integer k such that $n = m(nk + 1)$.

    (b) Explain why it is not possible to have $k > 0$ or $k = 0$.

    (c) If $k < 0$, prove that $nk > -1$ and explain why this is impossible.

    (d) Explain why Parts a-c together proves $L_{\mathbb{Z}}$ is infinite.

5 Isomorphisms

At this point in the course, you have encountered many examples of groups; and, you have probably noticed that some of these groups "act" very much alike. For example, compare the symmetric group S_3 of symmetries on the triangle and the cross-ratio group we introduced at the beginning of this course. Recall that the cross-ratio group is the group $\mathcal{F} = (\{\epsilon, q, r, s, t, u\}, \circ)$, where $\circ$ denotes function composition, and each member is a real-valued function $t : (0, 1) \longrightarrow \mathbb{R}$ defined by

$$\epsilon(x) = x \qquad q(x) = 1 - x \qquad r(x) = \frac{1}{x}$$

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

On the other hand, the group S_3 of triangle symmetries consists of the six-element set $\{R_0, R_{120}, R_{240}, F_1, F_2, F_3\}$, where R_θ denotes a clockwise rotation through angle θ, and F_j denotes a flip around the line bisecting vertex j. This set forms a group under the operation $x * y$ taken to mean "perform action x after action y." Here are the operation tables for both groups.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{s}$	$\boldsymbol{t}$	$\boldsymbol{u}$
$\boldsymbol{\epsilon}$	ϵ	q	r	s	t	u
$\boldsymbol{q}$	q	ϵ	u	t	s	r
$\boldsymbol{r}$	r	s	ϵ	q	u	t
$\boldsymbol{s}$	s	r	t	u	q	ϵ
$\boldsymbol{t}$	t	u	s	r	ϵ	q
$\boldsymbol{u}$	u	t	q	ϵ	r	s

$*$	$\boldsymbol{R}_0$	$\boldsymbol{R}_{120}$	$\boldsymbol{R}_{240}$	$\boldsymbol{F}_1$	$\boldsymbol{F}_2$	$\boldsymbol{F}_3$
$\boldsymbol{R}_0$	R_0	R_{120}	R_{240}	F_1	F_2	F_3
$\boldsymbol{R}_{120}$	R_{120}	R_{240}	R_0	F_3	F_1	F_2
$\boldsymbol{R}_{240}$	R_{240}	R_0	R_{120}	F_2	F_3	F_1
$\boldsymbol{F}_1$	F_1	F_2	F_3	R_0	R_{120}	R_{240}
$\boldsymbol{F}_2$	F_2	F_3	F_1	R_{240}	R_0	R_{120}
$\boldsymbol{F}_3$	F_3	F_1	F_2	R_{120}	R_{240}	R_0

At first glance, these tables do not look very much alike. However, if we look deeper, a number of similarities appear. For example,

- Both groups are nonabelian.
- Both groups have exactly two elements of order 3.
- Both groups have exactly three elements or order 2.
- In both groups, the product of any two distinct elements or order 2 is an element of order 3.
- In both groups, the elements of order 3 generate the same cyclic subgroup.
- In both groups, every proper subgroup is abelian.

The more we compare these two groups, the more they look like the same group with different lables applied to the elements. In particular, it doesn't seem to matter what the *lable* we give to the group elements — the *relationship* between specific elements remains the same. Compare the following tables, where the elements of the cross-ratio group have been rearranged.

$\circ$	$\boldsymbol{\epsilon}$	$\boldsymbol{s}$	$\boldsymbol{u}$	$\boldsymbol{t}$	$\boldsymbol{r}$	$\boldsymbol{q}$
$\boldsymbol{\epsilon}$	ϵ	s	u	t	r	q
$\boldsymbol{s}$	s	u	ϵ	q	t	r
$\boldsymbol{u}$	u	ϵ	s	r	q	t
$\boldsymbol{t}$	t	r	q	ϵ	s	u
$\boldsymbol{r}$	r	q	t	u	ϵ	s
$\boldsymbol{q}$	q	t	r	s	u	ϵ

$*$	$\boldsymbol{R}_0$	$\boldsymbol{R}_{120}$	$\boldsymbol{R}_{240}$	$\boldsymbol{F}_1$	$\boldsymbol{F}_2$	$\boldsymbol{F}_3$
$\boldsymbol{R}_0$	R_0	R_{120}	R_{240}	F_1	F_2	F_3
$\boldsymbol{R}_{120}$	R_{120}	R_{240}	R_0	F_3	F_1	F_2
$\boldsymbol{R}_{240}$	R_{240}	R_0	R_{120}	F_2	F_3	F_1
$\boldsymbol{F}_1$	F_1	F_2	F_3	R_0	R_{120}	R_{240}
$\boldsymbol{F}_2$	F_2	F_3	F_1	R_{240}	R_0	R_{120}
$\boldsymbol{F}_3$	F_3	F_1	F_2	R_{120}	R_{240}	R_0

Careful examination shows that these two tables display exactly the same pattern — in both tables, the product of the jth and kth elements in one table corresponds to the jth and kth elements in the other table.

We say that two groups are *isomorphic* provided they have exactly the same structure. This means that, although the elements of the groups may be different, the elements are related through the group operations in exactly the same way. If the groups are finite, isomorphism means

- The two groups have exactly the same number of elements
- The operation table of one group can be rearranged to look exactly like the operation table of the other group.

Since we can arrange the elements so that both operation tables look exactly the same, we say that the cross-ratio goup and the symmetries of the triangle are isomorphic. Although the two groups contain different elements and have a different operation, they are effectively *the same group.*

Of course, rearranging elements in an attempt to make operation tables display the same patterns is not an easy or even a practical way to decide whether two groups are isomorphic. (It is not even possible when the groups are infinite.) There is a more systematic approach. Each listing of the cross-ratio group can be thought of as a *bijection* between it and the group of triangle symmetries. For example, the first and second listings correspond to the following assignments written in tabular form

$$f : \begin{pmatrix} R_0 & R_{120} & R_{240} & F_1 & F_2 & F_3 \\ \epsilon & q & r & s & t & u \end{pmatrix} \qquad g : \begin{pmatrix} R_0 & R_{120} & R_{240} & F_1 & F_2 & F_3 \\ \epsilon & s & u & t & q & r \end{pmatrix}$$

The first assignment is basically random; however, there was some planning put into the second assignment. Note that both groups contain exactly four elements which are their own inverses, namely ϵ, t, q, r in the cross-ratio group and R_0, F_1, F_2, and F_3 in the triangle symmetries group. The assignment g is careful to match up these elements. The elements s and u are inverses of each other in the cross-ratio group, as are the elements R_{120} and R_{240} in the triangle symmetries group. The assignment g is careful to match up these elements as well. In other words, the assignment g is careful to match elements in the cross-ratio group with elements that *behave the same way* in the triangle symmetries group.

The particulars of the assignment don't matter beyond this one goal — *assign elements in one group to distinct elements in the other which behave exactly the same way under the other group operation.* If it is possible to do this, then the two groups are isomorphic; if it is not, then the two groups are not isomorphic. If two groups are not isomorphic, then one group will have a property that the other group does not have.

For example, the group $\mathcal{Z}_6$ is not isomorphic to the group S_3 of triangle symmetries. Both contain exactly six elements, so there are many bijections between them (exactly $6! = 720$ to be exact). However, S_3 contains only one element which commutes with everything, while $\mathcal{Z}_6$ contains six such elements (because it is abelian). Consequently, we cannot match every element in S_3 with a *distinct* element in $\mathcal{Z}_6$ that behaves exactly the same way. (The group S_3 also contains four elements which are their own inverses while $\mathcal{Z}_6$ contains only two.)

We can think of our assignment as a labeling function — it takes the elements of one group and assigns them labels from the other. Two groups $\mathcal{G}$ and $\mathcal{H}$ are isomorphic provided we can construct an assignment in which

- every element in $\mathcal{G}$ is assigned exactly one label from $\mathcal{H}$, and every element in $\mathcal{H}$ is used exactly once as a label for some element in $\mathcal{G}$
- the label of any product in $\mathcal{G}$ is the product of the corresponding labels in $\mathcal{H}$.

Definition 76 *Let $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ be groups. We say that $\mathcal{G}$ and $\mathcal{H}$ are **isomorphic** provided there exists a function $f : G \longrightarrow H$ such that*

1. *f is a bijection*

2. *for all* $x, y \in G$, *we have* $f(x * y) = f(x) \times f(y)$

The function f, *when it exists, is called an* ***isomorphism*** *from* $\mathcal{G}$ *to* $\mathcal{H}$.

Example 77 *Let* $V = \{E, A, B, C\}$ *be endowed with the binary operation* $*$ *defined by the table below.*

$*$	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

The group $\mathcal{V} = (V, *)$ *is called the Klein Four-Group (or Viergruppe). Show that* $\mathcal{V}$ *is isomorphic to* $\mathcal{Z}_2 \times \mathcal{Z}_2$.

Solution. Both groups contain exactly four elements, so there are bijections between them. (In fact, there are $4! = 24$ bijections between them.) If these groups are isomorphic, then at least one of these bijections satisfies Condition (2) of the definition for isomorphisms. We could check each of the twenty-four bijections by brute force. For example, consider the random bijection

$$f : \begin{pmatrix} E & A & B & C \\ (1,1) & (1,0) & (0,1) & (0,0) \end{pmatrix}$$

Does this function satisfy Condition (2)? We check on a case-by-case basis to see if $f(x * y) = f(x) \oplus f(y)$ for all $x, y \in V$. (Here the operation "$\oplus$" denotes addition mod 2 in each coordinate.) For example,

$$f(A * B) = f(C) = (0,0) \qquad f(A) \oplus f(B) = (1,0) \oplus (0,1) = (1,1)$$

Since these two computations do not yield the same result, we know that f does not satisfy Condition 2 and therefore does not represent an isomorphism between these groups.

Just because our first choice of bijection is not an isomorphism does not mean the groups fail to be isomorphic. It simply means our choice was unfortunate. Rather than checking all twenty-four possible bijections, we can be smarter in our choice. Isomorphic groups must have the same structure. This means that elements which behave a certain way in the group $\mathcal{V}$ must be assigned to elements which behave the same way in the group $\mathcal{Z}_2 \times \mathcal{Z}_2$. This tells us one important fact about isomorphisms:

Isomorphisms must assign the identity of one group to the identity of the other.

This fact allows us to eliminate any bijection between V and $\mathbb{Z}_2 \times \mathbb{Z}_2$ which does not assign E to $(0,0)$. Let's consider the bijection

$$g : \begin{pmatrix} E & A & B & C \\ (0,0) & (1,0) & (0,1) & (1,1) \end{pmatrix}$$

We will check to see if this bijection satisfies Condition 2. Observe that

$$g(A * B) = g(C) = (1,1) \qquad g(A) \oplus g(B) = (1,0) \oplus (0,1) = (1,1)$$
$$g(A * C) = g(B) = (0,1) \qquad g(A) \oplus g(C) = (1,0) \oplus (1,1) = (0,1)$$
$$g(A * E) = g(A) = (1,0) \qquad g(A) \oplus g(E) = (1,0) \oplus (0,0) = (1,0)$$
$$g(B * C) = g(A) = (1,0) \qquad g(B) \oplus g(C) = (0,1) \oplus (1,1) = (1,0)$$
$$g(B * E) = g(B) = (0,1) \qquad g(B) \oplus g(E) = (0,1) \oplus (0,0) = (0,1)$$
$$g(C * E) = g(C) = (1,1) \qquad g(C) \oplus g(E) = (1,1) \oplus (0,0) = (1,1)$$
$$g(B * B) = g(E) = (0,0) \qquad g(B) \oplus g(B) = (0,1) \oplus (0,1) = (0,0)$$

$$g(A*A) = g(E) = (0,0) \qquad g(A) \oplus g(A) = (1,0) \oplus (1,0) = (0,0)$$
$$g(C*C) = g(E) = (0,0) \qquad g(C) \oplus g(C) = (1,1) \oplus (1,1) = (0,0)$$
$$g(E*E) = g(E) = (0,0) \qquad g(E) \oplus g(E) = (0,1) \oplus (0,0) = (0,0)$$

Since both groups are commutative, we do not have to check the effect of reversing the order of the factors in each "product" (we would if the groups were not commutative). Thus, the computations above show that g satisfies Condition 2 and is therefore an isomorphism.

****

Example 78 *Show that the group $\mathcal{Z}_{12}$ is isomorphic to the group $\mathcal{Z}_3 \times \mathcal{Z}_4$.*

Solution. Theorem 58 tells us that $\mathcal{Z}_3 \times \mathcal{Z}_4$ is cyclic, so it should not be surprising that this group is isomorphic to $\mathcal{Z}_{12}$. However, it is not obvious how we should construct the desired isomorphism. Both groups contain the same number of elements, and both are commutative. We start by looking for elements in one group with peculiar characteristics and use these as a starting point. We know that $\mathcal{Z}_{12}$ is cyclic — it is generated by the element 1 (among others). It stands to reason that we should match this element with a generator for $\mathcal{Z}_3 \times \mathcal{Z}_4$. Consider the element $([1]_3, [1]_4)$. Observe that

$$([1]_3, [1]_4)^n = ([n]_3, [n]_4\ )$$

If we suppress the bracket notation for readability, we know that

$$(1,1)^2 = (2,2) \quad (1,1)^3 = (0,3) \quad (1,1)^4 = (1,0) \quad (1,1)^5 = (2,1) \quad (1,1)^6 = (0,2)$$
$$(1,1)^7 = (1,3) \quad (1,1)^8 = (2,0) \quad (1,1)^9 = (0,1) \quad (1,1)^{10} = (1,2) \quad (1,1)^{11} = (2,3) \quad (1,1)^{12} = (0,0)$$

Since every element of $\mathcal{Z}_3 \times \mathcal{Z}_4$ is a "power" of the element $([1]_3, [1]_4)$, we know that $\mathcal{Z}_3 \times \mathcal{Z}_4$ is gemerated by this pair. The "powers" above also suggest a possible bijection from the set $\mathbb{Z}_{12}$ to the set $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$$f : \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ (0,0) & (1,1) & (2,2) & (0,3) & (1,0) & (2,1) & (0,2) & (1,3) & (2,0) & (0,1) & (1,2) & (2,3) \end{pmatrix}$$

The question we must answer is whether or not "the label of the product is the product of the labels" for this function. That is, we must prove that for all $[x]_{12}, [y]_{12} \in \mathbb{Z}_{12}$, we have

$$f([x]_{12} \boxplus_{12} [y]_{12}) = f([x]_{12}) \oplus f([y]_{12})$$

where the "$\oplus$" symbol denotes addition modulo 3 in the first coordinate and addition modulo 4 in the second. We could check this case-by-case. For example, if $[x]_{12} = [5]_{12}$ and $[y]_{12} = [9]_{12}$, then

$$f([x]_{12} \boxplus_{12} [y]_{12}) = f([5+9]_{12}) = f([2]_{12}) = ([2]_3, [2]_4)$$

$$f([x]_{12}) \oplus f([y]\,12) = f([5]_{12}) \oplus f([9]_{12}) = ([2]_3, [1]_4) \oplus ([0]_3, [1]_4) = ([2]_3, [2]_4)$$

However, this approach will force us to wade through dozens of computations. We can be smarter in this case. We are taking the set $[k]_{12}$ in $\mathcal{Z}_{12}$ and assigning it the ordered pair $([k]_3, [k]_4)$. Consequently, we know that

$$\begin{aligned} f([x]_{12} \boxplus_{12} [y]_{12}) &= f([x+y]_{12}) \\ &= ([x+y]_3, [x+y]_4) \\ &= ([x]_3 \boxplus_3 [y]_3, [x]_4 \boxplus_4 [y]_4) \\ &= ([x]_3, [x]_4) \oplus ([y]_3, [y]_4) \\ &= f(x) \oplus f(y) \end{aligned}$$

****

The following result lists a number of properties that must be shared by isomorphic groups and the isomorphisms between them. The proofs for many of these claims will be left as exercises.

Theorem 79 *Suppose that $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ are isomorphic groups and suppose that $f : G \longrightarrow H$ is an isormorphism.*

1. *The function $f^{-1} : H \longrightarrow G$ is also an isomorphism.*
2. *If e is the identity for $\mathcal{G}$, then $f(e)$ is the identity for $\mathcal{H}$.*
3. *If $a \in G$, then $f(a^{-1}) = [f(a)]^{-1}$.*
4. *If $n \in \mathbb{Z}$, then $f(a^n) = [f(a)]^n$.*
5. *The group $\mathcal{G}$ is abelian if and only if the group $\mathcal{H}$ is abelian.*
6. *The group $\mathcal{G}$ is cyclic if and only if the group $\mathcal{H}$ is cyclic.*
7. *A subset X of G is a subgroup of $\mathcal{G}$ if and only if $f(X) = \{f(x) : x \in X\}$ is a subgroup of $\mathcal{H}$.*
8. *A subset Y of H is a subgroup of $\mathcal{H}$ if and only if $f^{-1}(Y) = \{f^{-1}(y) : y \in Y\}$ is a subgroup of $\mathcal{G}$.*

Solution. Note that Claim (3) is a special case of Claim (4), and also note that Claim (8) follows from Claim (1) and Claim (7). We will prove Claims (1), (2), and (7) and leave the rest as exercises. To prove Claim (1), first note that $f^{-1} : H \longrightarrow G$ is certainly a bijection. We only need to show that f^{-1} "preserves the operation." That is, we need to show that, for all $u, v \in H$, we have $f^{-1}(u \times v) = f^{-1}(u) * f^{-1}(v)$. To this end, let $u, v \in H$. Since f is a bijection, we know that $\texttt{Pre}_f(u) = \{a\}$ and $\texttt{Pre}_f(v) = \{b\}$ for some $a, b \in G$. Consequently, we know

$$u \times v = f(a) \times f(b) = f(a * b)$$

since f is assumed to "preserve the operation." Therefore, we know

$$f^{-1}(u \times v) = f^{-1}(f(a * b)) = a * b = f^{-1}(u) * f^{-1}(v)$$

We may conclude that f^{-1} is an isomorphism, as desired.

Since a group can have only one identity element, to prove Claim (2), we need only show that $f(e) \times u = u$ and $u \times f(e) = u$ for all $u \in H$. To this end, let $u \in H$. We know that $\texttt{Pre}_f(u) = \{a\}$ for some $a \in G$. Since we have assumed that f "preserves the operation," we know that

$$f(e) \times u = f(e) \times f(a) = f(e * a) = f(a) = u \qquad u \times f(e) = f(a) \times f(e) = f(a * e) = f(a) = u$$

We may therefore conclude that $f(e)$ is the identity element for $\mathcal{H}$, as desired.

To prove Claim (7), let $X \subseteq G$. First, suppose that X is a subgroup of $\mathcal{G}$. We need to show that $f(X)$ is closed under the operation on H and closed with respect to the formation of inverses in $\mathcal{H}$. To this end, let $u, v \in f(X)$. Since f is a bijection, there exist $a, b \in X$ such that $\texttt{Pre}_f(u) = \{a\}$ and $\texttt{Pre}_f(v) = \{b\}$. Since X is a subgroup of $\mathcal{G}$, we know that $a * b \in X$; consequently, we know that $f(a * b) \in f(X)$. Since we have assumed f "preserves the operation," we know that

$$u \times v = f(a) \times f(b) = f(a * b) \in f(X)$$

Thus, $f(X)$ is closed under the operation on H. To see that $f(X)$ is closed with respect to the formation of inverses, consider u. Since X is a subgroup of $\mathcal{G}$, we know that $a^{-1} \in X$; hence, we know that $f(a^{-1}) \in f(X)$. Therefore, according to Claim (3), we know

$$u^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(X)$$

We may now conclude that $f(X)$ is a subgroup of $\mathcal{H}$, as desired.

Conversely, suppose that $f(X)$ is a subgroup of $\mathcal{H}$. We need to prove that X is a subgroup of $\mathcal{G}$. However, this fact is now a direct consequence of Claim (1), since $f^{-1} : H \longrightarrow G$ is also an isomorphism and $X = f^{-1}[f(X)]$.

Example 80 *Show that the Klein Four-Group is not isomorphic to $\mathcal{Z}_4$.*

Solution. To show that two groups are not isomorphic, we must either show that no bijection exists between them, or we must find some property one group possesses that the other does not. In this case, both groups have the same number of elements, so bijections certainly exist between them. Every element in the Klein Four-Group is its own inverse — this is not the case for $\mathcal{Z}_4$. In fact, only 0 and 2 are their own inverses in $\mathcal{Z}_4$; consequently, the Klein Four-Group has a property that $\mathcal{Z}_4$ does not. Hence, the two groups cannot be isomorphic. (We could also note that $\mathcal{Z}_4$ is cyclic while the Klein Four-Group is not.)

****

Although every example we have looked at involves finite groups, there is nothing in the formal definition which requires this. It is possible to compare infinite groups; however, the process of creating and verifying the isomorphism becomes more challenging.

Example 81 *Let $\mathcal{G} = (\mathbb{R}^*, \cdot)$ denote the group of nonzero real numbers under multiplication and let $\mathcal{H} = (\mathbb{R}^*, \triangleleft)$ denote the group of nonzero real numbers under the operation $x \triangleleft y = (x \cdot y)/2$. Prove that these groups are isomorphic.*

Solution. It is straightforward to prove that $\mathcal{H}$ is indeed a (commutative) group. The identity element for $\mathcal{H}$ is $e_1 = 2$, and for each nonzero real number x, we find that $x^{-1} = 4/x$. Since the underlying sets are the same for both groups, we know that bijections exist between these groups; however, it is not immediately clear *which* bijection we should choose. We know the identity for $\mathcal{G}$ is $e_2 = 1$; and we know that the inverse for each nonzero real number x in $\mathcal{G}$ is $x^{-1} = 1/x$. We also know that an isomorphism must assign the identity of one group to the identity of the other. Therefore, let's start by considering a simple function which accomplishes this, namely $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by

$$f(x) = 2 \cdot x$$

We need to prove first that f is a bijection. To see that f is one-to-one, suppose $x, y \in \mathbb{R}^*$ and suppose that $f(x) = f(y)$. This tells us that

$$2 \cdot x = 2 \cdot y \quad \Longrightarrow \quad x = y$$

To see that f is onto, simply note that if $x \in \mathbb{R}^*$, then $f(x/2) = x$. Thus, every nonzero real number x has a preimage under f (namely $x/2$). We may conclude that f is a bijection.

We now need to decide whether or not f satisfies Condition 2. In this case, since the underlying sets of $\mathcal{G}$ and $\mathcal{H}$ are the same, we can consider f as an assignment from $\mathcal{G}$ to $\mathcal{H}$ or vice-versa. (This would not be an option if the groups had different underlying sets.) The assignment might satisfy Condition 2 in one direction but not in the other. We only need for the condition to be satisfied in one direction. Let's start by assuming that f is an assignment from $\mathcal{G}$ to $\mathcal{H}$.

Let $x, y \in \mathbb{R}^*$. Starting from the group $\mathcal{G}$, (so that we have the dot operation inside f and the triangle operation outside f) observe that

$$f(x \cdot y) = 2 \cdot (x \cdot y) \qquad f(x) \triangleleft f(y) = (2 \cdot x) \triangleleft (2 \cdot y) = \frac{4 \cdot (x \cdot y)}{2} = 2 \cdot (x \cdot y)$$

Since these computations are the same, we know that f is an isomorphism from $\mathcal{G}$ to $\mathcal{H}$.

In the example above, we showed that the function f serves as an isomorphism from $\mathcal{G}$ to $\mathcal{H}$. This example is unusual in that the function f can be considered as assignment from $\mathcal{G}$ to $\mathcal{H}$ or as an assignment from $\mathcal{H}$ to $\mathcal{G}$. (This was not the case in any of our previous examples, since the underlying sets of the groups were different.) This leads to the obvious question — Is f also an isomorphism from $\mathcal{H}$ to $\mathcal{G}$? It is certainly a bijection. It does not, however, satisfy Condition 2. Indeed, starting from the group $\mathcal{H}$, observe that

$$f(x \triangleleft y) = f\left(\frac{x \cdot y}{2}\right) = 2 \cdot \left(\frac{x \cdot y}{2}\right) = x \cdot y$$

$$f(x) \cdot f(y) = (2 \cdot x) \cdot (2 \cdot y) = 4 \cdot (x \cdot y)$$

These two expressions will never be equal in $\mathbb{R}^*$; hence, f does not serve as an isomorphism when viewed as an assignment from $\mathcal{H}$ to $\mathcal{G}$.

Of course, if $\mathcal{G}$ is isomorphic to $\mathcal{H}$, then we would expect that $\mathcal{H}$ is also isomorphic to $\mathcal{G}$. Consequently, we would expect that there exists at least one isomorphism g from $\mathcal{H}$ to $\mathcal{G}$; and Claim (1) of the previous theorem tells us this is the case. The key is to consider the *inverse* of f. Since f is a bijection, we know that f has an inverse, namely the function $g : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by

$$g(y) = \frac{y}{2}$$

Claim (1) of the previous theorem tells us that g is an isomorphism from $\mathcal{H}$ to $\mathcal{G}$. To see that g really is an isomorphism from $\mathcal{H}$ to $\mathcal{G}$, let $a, b \in \mathbb{R}^*$, and observe that

$$g(a \triangleleft b) = g\left(\frac{a \cdot b}{2}\right) = \frac{a \cdot b}{4} \qquad g(a) \cdot g(b) = \left(\frac{a}{2}\right) \cdot \left(\frac{b}{2}\right) = \frac{a \cdot b}{4}$$

Since g satisfies Condition 2 and since g is clearly a bijection (because it is the inverse of a bijection), we see that g is indeed an isomorphism from $\mathcal{H}$ to $\mathcal{G}$.

The following result tells us something that you have probably already suspected. There are, up to isomorphism, only two kinds of cyclic groups — namely the finite groups $\mathcal{Z}_n$ and the group $\mathcal{Z}$ of integers under addition.

Theorem 82 *Let $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ be groups. The following statements are true for any $a \in G$ and $b \in H$.*

1. *If a has order n in $\mathcal{G}$ and b has order n in $\mathcal{H}$, then $\langle a \rangle$ is isomorphic to $\langle b \rangle$.*
2. *If a has infinite order in $\mathcal{G}$ and b has infinite order in $\mathcal{H}$, then $\langle a \rangle$ is isomorphic to $\langle b \rangle$.*

Proof. The proofs of these two claims are very similar. Suppose that a and b have finite order n. In light of Corollary 16, we know that the sequences $a, a^2, a^3, ..., a^{n-1}, e_G$ and $b, b^2, b^3, ..., b^{n-1}, e_H$ consist of distinct elements, and we know

$$\langle a \rangle = \{a, a^2, a^3, ..., a^{n-1}, e_G\} \qquad \langle b \rangle = \{b, b^2, b^3, ..., b^{n-1}, e_H\}$$

There is a natural bijection between these sets, namely the function $f : \langle a \rangle \longrightarrow \langle b \rangle$ defined by $f(a^j) = b^j$ for $0 \leq j < n$. All we need to do is demonstrate that f "preserves the operation." This is a direct consequence of the group laws of exponents and the Division Algorithm. For all $0 \leq j, k < n$ there exist unique integers

m and r such that $j+k = mn+r$ and $0 \leq r < n$. Now, it follows that $a^{j+k} = a^{nm} * a^r = a^r$ and likewise that $b^{j+k} = b^r$. With this in mind, observe

$$f(a^j * a^k) = f(a^{j+k}) = f(a^r) = b^r = b^{j+k} = b^j \times b^k = f(a^j) \times f(a^k)$$

Thus, f is an isomorphism from $\langle a \rangle$ to $\langle b \rangle$, as desired.

When a and b have infinite order, the proof is even simpler. In light of Corollary 16, we know that the sequences $a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, ...$ and $b^{\pm 1}, b^{\pm 2}, b^{\pm 3}, ...$ consist of distinct elements, and we know

$$\langle a \rangle = \{a^j : j \in \mathbb{Z}\} \qquad \langle b \rangle = \{b^j : j \in \mathbb{Z}\}$$

There is a natural bijection between these sets, namely the function $f : \langle a \rangle \longrightarrow \langle b \rangle$ defined by $f(a^j) = b^j$ for $j \in \mathbb{Z}$. All we need to do is demonstrate that f "preserves the operation." Observe that

$$f(a^j * a^k) = f(a^{j+k}) = b^{j+k} = b^j \times b^k = f(a^j) \times f(a^k)$$

Thus, f is an isomorphism from $\langle a \rangle$ to $\langle b \rangle$, as desired.

QED

EXERCISES FOR SECTION 5

1. Let n be a fixed positive integer. Define $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $f(x) = [x]_n$. Show that f "preserves the operation" between the groups $\mathcal{Z}$ and $\mathcal{Z}_n$ but is not an isomorphism.

2. Define $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$ by $f([a]_2, [b]_2) = [2a + 2b]_4$. Show that f "preserves the operation" between the groups $\mathcal{Z}_2 \times \mathcal{Z}_2$ and $\mathcal{Z}_4$ but is not an isomorphism.

3. Consider the subgroup $H = \{I, A, B, C, D, K\}$ of $\mathcal{M}_2$ where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$C = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \qquad D = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}$$

   The operation table for $(H, *)$ is given below. By rearranging this table, show that $(H, *)$ is isomorphic to the group $(S_3, \circ)$ of symmetries for the equilateral triangle whose table appears at the beginning of this section.

$*$	$\boldsymbol{I}$	$\boldsymbol{A}$	$\boldsymbol{B}$	$\boldsymbol{C}$	$\boldsymbol{D}$	$\boldsymbol{K}$
$\boldsymbol{I}$	I	A	B	C	D	K
$\boldsymbol{A}$	A	I	C	B	K	D
$\boldsymbol{B}$	B	K	D	A	I	C
$\boldsymbol{C}$	C	D	K	I	A	B
$\boldsymbol{D}$	D	C	I	K	B	A
$\boldsymbol{K}$	K	B	A	D	C	I

4. Let $Q_8 = \{1, -1, I, -I, J, -J, K, -K\}$ and let $\triangleright$ be a binary operation on Q_8 defined by the following table.

$\triangleright$	$\boldsymbol{1}$	$\boldsymbol{-1}$	$\boldsymbol{I}$	$\boldsymbol{-I}$	$\boldsymbol{J}$	$\boldsymbol{-J}$	$\boldsymbol{K}$	$\boldsymbol{-K}$
$\boldsymbol{1}$	1	-1	I	$-I$	J	$-J$	K	$-K$
$\boldsymbol{-1}$	-1	1	$-I$	I	$-J$	J	$-K$	K
$\boldsymbol{I}$	I	$-I$	-1	1	K	$-K$	$-J$	J
$\boldsymbol{-I}$	$-I$	I	1	-1	$-K$	K	J	$-J$
$\boldsymbol{J}$	J	$-J$	$-K$	K	-1	1	I	$-I$
$\boldsymbol{-J}$	$-J$	J	K	$-K$	1	-1	$-I$	I
$\boldsymbol{K}$	K	$-K$	J	$-J$	$-I$	I	-1	1
$\boldsymbol{-K}$	$-K$	K	$-J$	J	I	$-I$	1	-1

The pair $(Q_8, \triangleright)$ forms a group (you do not need to show this) called the *Quaternion Group*. Is the Quaternion Group isomorphic to the Octic Group?

5. Show that the group $\mathcal{U}_8$ of units modulo 8 is not isomorphic to $\mathcal{U}_{10}$.

6. By comparing operation tables, show that $\mathcal{U}_8$ is isomorphic to $\mathcal{U}_{12}$.

7. Let $\mathcal{R} = (\mathbb{R}, +)$ be the real numbers under addition and let $\mathcal{R}^+ = (\mathbb{R}^+, \cdot)$ be the positive real numbers under multiplication. Show that $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ defined by $f(x) = \texttt{exp}(x)$ (the natural exponential function) is an isomorphism from $\mathcal{R}$ to $\mathcal{R}^+$. What is the corresponding isomorphism from $\mathcal{R}^+$ to $\mathcal{R}$?

8. Let n be a fixed positive integer. Prove that $\mathcal{Z}$ is isomorphic to $n\mathcal{Z}$. (Here $n\mathcal{Z}$ is the subgroup of $\mathcal{Z}$ consisting of all multiples of n.)

9. The previous exercise shows that an infinite group can be isomorphic to a proper subgroup of itself. Is this possible for finite groups?

10. Let $\breve{\mathcal{R}} = (\mathbb{R}, \sqcup)$, where $x \sqcup y = x + y + 1$.

    (a) Show that $\breve{\mathcal{R}}$ is an abelian group.

    (b) Show that $\mathcal{R}$ is isomorphic to $\breve{\mathcal{R}}$. (Create your function by considering formulas which assign the identity of $\mathcal{R}$ to the identity of $\breve{\mathcal{R}}$.)

11. Let $\ddot{\mathcal{R}} = (\mathbb{R}^*, \sqcap)$, where $x \sqcap y = \dfrac{xy}{4}$ and $\mathbb{R}^*$ denotes the nonzero real numbers. (We showed this pair is a group in Example 9.) Show that $\mathcal{R}^* = (\mathbb{R}^*, \cdot)$ is isomorphic to $\ddot{\mathcal{R}}$.

12. Show that $\mathcal{Z}$ is not isomorphic to $\mathcal{Q}$.

13. Show that $\mathcal{Q}$ is not isomorphic to $\mathcal{Q}^+$, the group of positive rational numbers under multiplication.

14. Let $\mathcal{G} = (G, *)$, $\mathcal{H} = (H, \cdot)$ and $\mathcal{J} = (J, \star)$ be groups and suppose that $f : G \longrightarrow H$ and $g : H \longrightarrow J$ are isomorphisms. Prove that $\mathcal{G}$ is isomorphic to $\mathcal{J}$.

15. Suppose that $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ are isomorphic groups and suppose that $f : G \longrightarrow H$ is an isormorphism. Prove that $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$.

16. Suppose that $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ are isomorphic groups and suppose that $f : G \longrightarrow H$ is an isormorphism.

    (a) Use mathematical induction to prove that $f(a^n) = [f(a)]^n$ for every positive integer n.

    (b) Use Part (a), the previous exercise, and Claim (2) of Theorem 79 to prove that $f(a^n) = [f(a)]^n$ for every integer n.

17. Suppose that $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ are isomorphic groups and suppose that $f : G \longrightarrow H$ is an isormorphism.

    (a) Let $a, b \in G$ and prove that $a * b = b * a$ if and only if $f(a) \times f(b) = f(b) \times f(a)$.

    (b) Prove that $\mathcal{G}$ is abelian if and only if $\mathcal{H}$ is abelian.

18. Suppose that $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ are isomorphic groups and suppose that $f : G \longrightarrow H$ is an isormorphism. Let n be a positive integer and prove that $a \in G$ has order n if and only if $f(a)$ has order n.

19. Suppose that $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \times)$ are isomorphic groups and suppose that $f : G \longrightarrow H$ is an isormorphism. Prove that $\mathcal{G}$ is cyclic with generator a if and only if $\mathcal{H}$ is cyclic with generator $f(a)$.

20. For each positive integer n, show that $\mathcal{P}_n$ is isomorphic to a subgroup of $\mathcal{P}_{n+1}$.

21. Let $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \cdot)$ be groups.

(a) Show that $\mathcal{G} \times \mathcal{H}$ is isomorphic to $\mathcal{H} \times \mathcal{G}$.

(b) Show that $\mathcal{G}$ is isomorphic to a subgroup of $\mathcal{G} \times \mathcal{H}$.

22. Let $\mathcal{G} = (G, *)$, $\mathcal{H} = (H, \cdot)$ and $\mathcal{J} = (J, \star)$ be groups. Show that $\mathcal{G} \times (\mathcal{H} \times \mathcal{J})$ is isomorphic to $(\mathcal{G} \times \mathcal{H}) \times \mathcal{J}$.

23. Let $\mathcal{G} = (G, *)$ be a group. An isomorphism $f : G \longrightarrow G$ is called an *automorphism*. Show that the set $\mathtt{AUT}(\mathcal{G})$ of automorphisms on $\mathcal{G}$ is a group under function composition. We will denote this group the *automorphism group of* $\mathcal{G}$ and denote it by $\mathcal{A}_{\mathcal{G}}$.

24. Let $\mathcal{G} = (G, *)$ be a group.

(a) For any fixed $a \in G$, show that $\varphi_a : G \longrightarrow G$ defined by $\varphi_a(x) = a * x * a^{-1}$ is an automorphism. Functions of this form are called *inner* automorphisms on $\mathcal{G}$.

(b) For fixed $a, b \in G$, show that $\varphi_a \circ \varphi_b = \varphi_{a*b}$ and that $\varphi_{a^{-1}} = [\varphi_a]^{-1}$.

(c) Explain why the set $\mathtt{INN}(\mathcal{G})$ of inner automorphisms on $\mathcal{G}$ is a subgroup of $\mathcal{A}_{\mathcal{G}}$.

25. Let $\mathcal{G} = (G, *)$ be a group.

(a) For each $a \in G$ and each automorphism $f : G \longrightarrow G$, prove that $f \circ \varphi_a \circ f^{-1} = \varphi_{f(a)}$. Hint: $a = f^{-1}(f(a))$.

(b) Prove that $\mathtt{INN}(\mathcal{G})$ is a normal subgroup of $\mathcal{A}_{\mathcal{G}}$. (Use Exercise 4.13.)

26. Let n be a positive integer and consider the group $\mathcal{Z}_n$.

(a) If $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ is an automorphism, explain why we must have $f([1]_n) = [b]_n$, where b is relatively prime to n. (Use Theorem 53 and Exercise 17.)

(b) Prove that every automorphism $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ has the form $f([k]_n) = [kb]_n$ for some fixed b relatively prime to n.

27. Construct the group $\mathcal{A}_{\mathcal{Z}_{10}}$ and show that it is isomorphic to the group $\mathcal{U}_{10}$ of units modulo 10. (Compare the operation tables.)

28. If n is a positive integer, prove that $\mathcal{A}_{\mathcal{Z}_n}$ is always isomorphic to $\mathcal{U}_n$. Hint: Consider the function $\tau : \mathtt{AUT}(\mathcal{Z}_n) \longrightarrow U_n$ defined by $\tau(f) = f([1]_n)$.

6 Quotient Groups

In this, the closing section of this chapter, we will consider a question with important consequences in advanced group theory — Is it possible to extend the notion of "modular arithmetic" to general groups? The answer to this question is "yes" and the resulting construction plays an important role in *decomposition theory* — an arena of mathematics which provides ways to break complicated structures into simpler ones. (The fact that every integer may be written as a product of prime numbers is an ancient example of a decomposition process, and the notion of divisibility is another.) We begin by taking a closer look at the groups $\mathcal{Z}_n$.

For any fixed positive integer n, we know that $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ is a subroup of $\mathcal{Z}$. In fact, since every subgroup of $\mathcal{Z}$ must be cyclic, these sets, along with $\{0\}$, are the *only* subgroups of $\mathcal{Z}$. In Exercise 4.17, you proved that the left (and right) cosets of $n\mathbb{Z}$ in $\mathcal{Z}$ are the sets $A_r = \{r + nk : k \in \mathbb{Z}\}$, where $0 \leq r < n$. Let $L_n = \{A_r : 0 \leq r < n\}$.

Example 83 *For a fixed positive integer n, show that L_n forms an abelian group under the binary operation $A_r \oplus A_s = A_t$, where t is the smallest nonnegative integer such that $t \equiv (r+s)\texttt{MOD}(n)$.*

Solution. As defined, the relation $\oplus$ is clearly a commutative binary operation. We need to show that $\oplus$ is associative. To this end, let x, y, z be integers such that $0 \leq x, y, z < r$. We need to show that $A_x \oplus (A_y \oplus A_z) = (A_x \oplus A_y) \oplus A_z$. By definition, $A_x \oplus (A_y \oplus A_z) = A_t$ and $(A_x \oplus A_y) \oplus A_z = A_u$, where t is the smallest nonnegative integer such that $t \equiv [x + (y + z)]\texttt{MOD}(n)$ and u is the smallest nonnegative integer such that $u \equiv [(x + y) + z]\texttt{MOD}(n)$. Of course, since integer addition is associative, we know that $u = t$. Hence, $A_x \oplus (A_y \oplus A_z) = (A_x \oplus A_y) \oplus A_z$, as desired. The set A_0 clearly serves as the identity for L_n under $\oplus$. If $0 \leq r < n$, then let $s = n - r$. It follows that $0 \leq s < n$, and it follows that $r + s \equiv 0\texttt{MOD}(n)$. Hence, $A_r \oplus A_s = A_0$, and the set A_s serves as the inverse for A_r under $\oplus$.

****

Theorem 84 *For a fixed positive integer n, the group $(L_n, \oplus)$ is isomorphic to $\mathcal{Z}_n$.*

Proof. Consider the function $f : L_n \longrightarrow \mathbb{Z}_n$ defined by $f(A_r) = [r]_n$. If $[b]_n \in \mathbb{Z}_n$, then the Division Algorithm tells us there is a unique integer $0 \leq r < n$ such that $[b]_n = [r]_n$; hence, the function f is onto. Suppose that $A_r, A_s \in L_n$ are such that $f(A_r) = f(A_s)$. This means that $[r]_n = [s]_n$. This tells us that $r \equiv s$ $\texttt{MOD}(n)$; and, since $0 \leq r, s < n$, this tells us that $r = s$. Consequently, f is one-to-one. It remains to show that f "preserves the operation." To this end, observe that

$$f(A_r) \boxplus_n f(A_s) = [r]_n \boxplus_n [s]_n = [r + s]_n$$

We also know that $f(A_r \oplus A_s) = f(A_t) = [t]_n$, where t is the smallest nonnegative integer such that $t \equiv (r + s)\texttt{MOD}(n)$. Of course, the fact that $t \equiv (r + s)\texttt{MOD}(n)$ tells us that $t \in [r + s]_n$. Since the members of $\mathbb{Z}_n$ are pairwise disjoint (they are the cells of an equivalence relation), this tells us that $[t]_n = [r + s]_n$. Consequently, we have $f(A_r \oplus A_s) = f(A_r) \boxplus_n f(A_s)$, as desired.

QED

The previous result tells us that it is possible to endow the family of left cosets for $n\mathbb{Z}$ with a binary operation which makes this set mimic the group $\mathcal{Z}_n$. This fact is the first step in extending the notion of modular arithmetic to general groups. The definition of the binary operation $\oplus$ on the family L_n relies heavily on the special properties of the integers. These properties are certainly not available to us in general groups; however, it is possible to define the operation $\oplus$ in a way which is less explicitly dependent on the unique properties of the integers. To begin, we can retool the description of the sets in L_n to bring it in line with our usual description of left cosets. Under our usual definition, $L_n = \{a(n\mathbb{Z}) : a \in \mathbb{Z}\}$, where

$$a(n\mathbb{Z}) = \{a + nx : x \in \mathbb{Z}\}$$

The gyst of Exercise 4.17 was to show that there are really only n *distinct* members of this family, since the Division Algorithm tells us that $a = qn + r$ for unique integers q and $0 \leq r < n$. For the moment, let's forget about Exercise 4.17 and work with the generic definition of the members in L_n. Consider the binary relation $\circledcirc$ on L_n defined by

$$a(n\mathbb{Z}) \circledcirc b(n\mathbb{Z}) = (a + b)(n\mathbb{Z})$$

It turns out that $\circledcirc = \oplus$; however, it takes a bit of work to prove this. It is not so clear that $\circledcirc$ is a binary *operation* on $\mathcal{L}_n$ since there are many different ways to represent the same left coset under our generic definition. (For example, since $9 \equiv 13\texttt{MOD}(4)$, we know that $9(4\mathbb{Z}) = 13(4\mathbb{Z})$.) If $\circledcirc$ is a binary operation, these different representations should not make a difference in the outcome; and it turns out that they don't. The reason why is the key to extending modular arithmetic to general groups.

Suppose that $a(n\mathbb{Z}) = b(n\mathbb{Z})$ and $c(n\mathbb{Z}) = d(n\mathbb{Z})$. We want to show that $a(n\mathbb{Z}) \circledcirc c(n\mathbb{Z}) = b(n\mathbb{Z}) \circledcirc d(n\mathbb{Z})$. Now, we know by definition that

$$a(n\mathbb{Z}) \circledcirc c(n\mathbb{Z}) = (a+c)(n\mathbb{Z}) = \{(a+c)+nx : x \in \mathbb{Z}\} \qquad b(n\mathbb{Z}) \circledcirc d(n\mathbb{Z}) = (b+d)(n\mathbb{Z}) = \{(b+d)+nx : x \in \mathbb{Z}\}$$

We could invoke the Division Algorthim to establish equality, but instead let's take a look at what the coset structure tells us. We have assumed that $a(n\mathbb{Z}) = b(n\mathbb{Z})$, and this means there exist $x \in \mathbb{Z}$ such that $a = b + nx$. Likewise, there exist $y \in \mathbb{Z}$ such that $c = d + ny$. Consequently, we know that

$$a + c = (b + nx) + (d + ny) = (b + d) + nz$$

where $z = x + y \in \mathbb{Z}$. This tells us that $a + c \in b(n\mathbb{Z}) \circledcirc d(n\mathbb{Z})$; and since the left cosets of $n\mathbb{Z}$ are pairwise disjoint, this forces us to conclude that $a(n\mathbb{Z}) \circledcirc c(n\mathbb{Z}) = b(n\mathbb{Z}) \circledcirc d(n\mathbb{Z})$.

Now that we know $\circledcirc$ is a binary operation on L_n, it is easy to show that $\circledcirc$ and $\oplus$ produce the same output when applied to the same left cosets. Indeed, let $a(n\mathbb{Z}), b(n\mathbb{Z}) \in L_n$. Of course, we know that $a(n\mathbb{Z}) = A_r$ and $b(n\mathbb{Z}) = A_s$, where r and s are the smallest nonnegative integers such that $r \equiv a\texttt{MOD}(n)$ and $s \equiv b\texttt{MOD}(n)$. Let t be the smallest nonnegative integer such that $t \equiv (a + b)\texttt{MOD}(n)$. We know that $t \equiv (r + s)\texttt{MOD}(n)$ as well by Corollary 1.2.14. Therefore,

$$a(n\mathbb{Z}) \circledcirc b(n\mathbb{Z}) = (a + b)(n\mathbb{Z}) = A_t = A_r \oplus A_s$$

We now have the tools necessary to create versions of "modular arithmetic", at least in *abelian* groups.

Theorem 85 *Let $\mathcal{G} = (G, *)$ be any abelian group and let H be a subgroup of $\mathcal{G}$. The pair $(L_H, \circledast)$ is always a group, where $\circledast$ is defined by $aH \circledast bH = (a * b)H$.*

The proof of this result is virtually identical to the argument presented above for $(L_n, \circledcirc)$, so we will omit it. (We will prove a more general version of this theorem shortly.) The group $(L_H, \circledast)$ is often called the *quotient group* "$\mathcal{G}$ MOD H" and is commonly denoted by the symbol $\mathcal{G}/\mathcal{H}$.

Example 86 *Construct the quotient group for $\mathcal{G} = \mathcal{Z}_6 \times \mathcal{Z}_2 \times \mathcal{Z}_2$ when*

$$H = \{([0]_3, [0]_2, [0]_2), ([3]_3, [0]_2, [0]_2), ([3]_3, [1]_2, [1]_2), ([0]_3, [1]_2, [1]_2)\}$$

Solution. First, note that since G contains 24 elements, $[G : H] = 6$; hence, L_H will contain six members. Our first task is to construct these members. Suppressing the equivalence class notation for readability, we find that the distinct left cosets for H will be

$$H = (0,0,0)H = \{(0,0,0), (3,0,0), (3,1,1), (0,1,1)\} \qquad (1,1,1)H = \{(1,1,1), (4,1,1), (4,0,0), (1,0,0)\}$$

$$(2,1,1)H = \{(2,1,1), (5,1,1), (5,0,0), (2,0,0)\} \qquad (1,0,1)H = \{(1,0,1), (4,0,1), (4,1,0), (1,0,1)\}$$

$$(2,0,1)H = \{(2,0,1), (5,0,1), (5,1,0), (2,1,0)\} \qquad (3,0,1)H = \{(3,0,1), (0,0,1), (0,1,0), (3,1,0)\}$$

We now construct the operation table for this group by applying the definition of $\circledast$ given in the previous theorem. For example, $(2,0,1)H \circledast (3,0,1)H = (5,0,0)H = (2,1,1)H$. (Note that we always use the same representative for the coset that we start with.)

$\circledast$	$\boldsymbol{H}$	$\boldsymbol{(1,1,1)H}$	$\boldsymbol{(2,1,1)H}$	$\boldsymbol{(1,0,1)H}$	$\boldsymbol{(2,0,1)H}$	$\boldsymbol{(3,0,1)H}$
$\boldsymbol{H}$	H	$(1,1,1)H$	$(2,1,1)H$	$(1,0,1)H$	$(2,0,1)H$	$(3,0,1)H$
$\boldsymbol{(1,1,1)H}$	$(1,1,1)H$	$(2,1,1)H$	$(1,1,1)H$	$(2,0,1)H$	$(3,0,1)H$	$(1,0,1)H$
$\boldsymbol{(2,1,1)H}$	$(2,1,1)H$	H	$(1,1,1)H$	$(3,0,1)H$	$(1,0,1)H$	$(2,0,1)H$
$\boldsymbol{(1,0,1)H}$	$(1,0,1)H$	$(2,0,1)H$	$(3,0,1)H$	$(2,1,1)H$	H	$(1,1,1)H$
$\boldsymbol{(2,0,1)H}$	$(2,0,1)H$	$(3,0,1)H$	$(1,0,1)H$	H	$(1,1,1)H$	$(2,1,1)H$
$\boldsymbol{(3,0,1)H}$	$(3,0,1)H$	$(1,0,1)H$	$(2,0,1)H$	$(1,1,1)H$	$(2,1,1)H$	H

****

The quotient group in the previous example happens to be isomorphic to $\mathcal{Z}_6$ (we leave verification as an exercise). There is no guarantee that a quotient group will be cyclic. In fact, quotient groups can display some very strange structure.

Example 87 *Show that every element of the quotient group $\mathcal{Q}/\mathcal{Z}$ has finite order.*

Solution. We described the left cosets of $\mathbb{Z}$ in the group $\mathcal{Q}$ in Example 65. In particular, we know $L_{\mathbb{Z}} = \{u\mathbb{Z} : u \in \mathbb{Q}\cap[0,1)\}$. We also know that for all $u, v \in \mathbb{Q}\cap[0,1)$ there exist unique $w \in \mathbb{Q}\cap[0,1)$ and $m \in \mathbb{Z}$ such that $u + v = m + w$ (see Example 65). Therefore,

$$u\mathbb{Z}\circledast v\mathbb{Z} = (u+v)\mathbb{Z} = w\mathbb{Z}$$

(Compare this to our discussion on $\mathcal{Z}/n\mathcal{Z}$ above.) Now, since $u \in \mathbb{Q}\cap[0,1)$, we know there exist integers p, q such that $u = p/q$. Consequently, we know that

$$(u\mathbb{Z})^q = \left(\underbrace{u+u+u+...+u}_{q \text{ times}}\right)\mathbb{Z} = p\mathbb{Z} = \mathbb{Z}$$

The coset $\mathbb{Z} = 0\mathbb{Z}$ serves as the identity for this group. Therefore, each element of $L_{\mathbb{Z}}$ has finite order.

****

The quotient group $\mathcal{Q}/\mathcal{Z}$ is an infinite group in which every element has finite order. We have not described a group like this before; in particular, $\mathcal{Q}/\mathcal{Z}$ is not cyclic and is not isomorphic to any group we have so far encountered.

As you might expect, things get more complicated when we consider nonabelian groups. If $\mathcal{G} = (G, *)$ is a nonabelian group and H is a subgroup of $\mathcal{G}$, then it is still true that L_H forms a partition of G; unfortunately, the binary relation $\circledast$ is not always a binary *operation*. Consider for example, the subgroup $H = \langle(1234)\rangle$ of the permutation group $\mathcal{P}_4$. The left cosets of H are

$$H = \{\epsilon, (1234), (13)(24), (1432)\} \qquad (34)H = \{(34), (124), (1423), (132)\}$$

$$(12)H = \{\{(12), (234), (1324), (143)\}\} \qquad (13)H = \{(13), (12)(34), (24), (14)(32)\}$$

$$(14)H = \{(14), (123), (1342), (243)\} \qquad (134)H = \{(134), (1243), (142), (23)\}$$

Now, if we define $\circledast$ the same way we did for abelian groups, we find that

$$(13)H \circledast (12)H = [(13)\circ(12)]\,H = (14)H \qquad (24)H \circledast (12)H = [(24)\circ(12)]\,H = (134)H$$

At first glance, nothing may seem wrong with these computations; however, $(13)H$ and $(24)H$ *are the same coset.* Since the outcome of these computations is different, we must conclude that $\circledast$ is not a binary operation in this case. We know from Example 60 that H is not a normal subgroup of $\mathcal{P}_4$. The fact that $\circledast$ is also not a binary operation is more than coincidence.

Theorem 88 *Let $\mathcal{G} = (G, *)$ be any group and let H be a subgroup of $\mathcal{G}$. The binary relation $\circledast$ defined on L_H by $aH \circledast bH = (a * b)H$ is an operation if and only if H is normal.*

Proof. Suppose that H is a normal subgroup of $\mathcal{G}$ and suppose $a, b, c, d \in G$ are such that $aH = cH$ and $bH = dH$. We need to prove that $aH \circledast bH = cH \circledast dH$. Since $a * b \in aH \circledast bH$ and since the left cosets are pairwise disjoint, it will suffice to prove that $a * b \in cH \circledast dH$. We have assumed that $aH = cH$ and $bH = dH$. This means there exist $u, v \in H$ such that $a = c * u$ and $b = d * v$. Therefore, we know that $a * b = (c * u) * (d * v)$.

We have also assumed that H is normal; this means that $cH = Hc$ and $dH = Hd$. The fact that $dH = Hd$ tells us there exist $k \in H$ such that $d*v = k*d$. Thus, we know $a*b = (c*u)*(k*d) = c*(u*k)*d$. Since H is a subgroup, we know that $u*k \in H$; hence, we also know that $c*(u*k) \in cH$. Now, since $cH = Hc$, we know there exist $h \in H$ such that $c*(u*k) = h*c$. Therefore, we know $a*b = c*(u*k)*d = (h*c)*d$. We have shown that $a * b = h * (c * d)$; and this allows us to conclude that $a * b \in H(c * d)$. Since H is normal, we know that $H(c * d) = (c * d)H$; consequently, we know that $a * b \in (c * d)H = cH \circledast dH$.

On the other hand, suppose that $\circledast$ defined on L_H is a binary operation. We need to show that H is a normal subgroup. According to Claim (2) of Theorem 73, it will suffice to show that $a * h * a^{-1} \in H$ for all $a \in G$ and $h \in H$. By Exercise 4.12, we know that $(a * h)H = aH$. Since $\circledast$ is a binary operation, we therefore know that $(a * h)H \circledast yH = aH \circledast yH$ for any $y \in G$. Consequently, we also know

$$\left[a * h * a^{-1}\right] H = (a * h)H \circledast a^{-1}H = aH \circledast a^{-1}H = (a \circledast a^{-1})H = eH = H$$

Exercise 4.11 tells us that $yH = H$ if and only if $y \in H$; hence, we may conclude that $a * h * a^{-1} \in H$, as desired.

QED

Corollary 89 *Let $\mathcal{G} = (G, *)$ be any group and let H be a subgroup of $\mathcal{G}$. The family L_H is a group under the relation $\circledast$ defined on L_H by $aH \circledast bH = (a * b)H$ if and only if H is normal.*

Proof. If $(L_H, \circledast)$ is a group, then clearly $\circledast$ is a binary operation on L_H; hence, H is normal by the previous theorem. Conversely, suppose that H is normal. The previous theorem tells us that $\circledast$ is a binary operation on L_H. We need to verify that the group axioms hold. Associativity is a direct consequence of the associativity for the operation $*$ and the fact that $\circledast$ is a binary operation on L_H. Indeed, let $a, b, c \in G$ and observe that

$$\begin{aligned} aH \circledast (bH \circledast cH) &= aH \circledast (b * c)H = [a * (b * c)]\, H \\ &= [(a * b) * c]\, H = (a * b)H \circledast cH = (aH \circledast bH) \circledast cH \end{aligned}$$

The fact that $\circledast$ is a binary operation on L_H is used several times in the computation, although in a subtle way. (For example, knowing that $bH \circledast cH = (b*c)H$ allows us to conclude $aH \circledast (bH \circledast cH) = aH \circledast (b*c)H$ only because $\circledast$ is a binary operation on L_H.) The set H serves as the identity element for L_H. To see why, observe that $H = aH$ for all $a \in H$ by Exercise 4.11; in particular, $H = eH$. Therefore, for all $a \in G$ we know

$$aH \circledast H = aH \circledast eH = (a * e)H = aH \qquad H \circledast aH = eH \circledast aH = (e * a)H = aH$$

Finally, if $a \in G$, then the set $a^{-1}H$ serves as the inverse for the set aH under the operation $\circledast$. To see why, observe that

$$aH \circledast a^{-1}H = (a * a^{-1})H = eH = H \qquad a^{-1}H \circledast aH = (a^{-1} * a)H = eH = H$$

We may now conclude that $(L_H, \circledast)$ is a group, as desired.

QED

Whenever H is a normal subgroup of a group $\mathcal{G} = (G, *)$, we know that the pair $(L_H, \circledast)$ is a group. Whether $\mathcal{G}$ is abelian or not, we refer to $(L_H, \circledast)$ as the *quotient group* of $\mathcal{G}$ by H and denote it by the symbol $\mathcal{G}/\mathcal{H}$. This group is often called "$\mathcal{G}$ `MOD` H."

Example 90 *Construct the quotient group $\mathcal{A}_4/\mathcal{U}$, where $\mathcal{A}_4$ is the Alphabet Group and $U = \{E, I, L, O\}$.*

Solution. The Alphabet Group is introduced in the exercises for Section 4; you showed that H is normal in the Alphabet Group in Exercise 4.5. The left cosets of H are

$$U = \{E, I, L, O\} \qquad MU = \{M, P, G, J\} \qquad HU = \{H, K, N, Q\}$$

Since L_U contains three elements, we know by Corollary 69 that $\mathcal{A}_4/\mathcal{U}$ will be isomorphic to $\mathcal{Z}_3$. We can see this directly if we construct its operation table.

$\circledast$	$\boldsymbol{U}$	$\boldsymbol{MU}$	$\boldsymbol{HU}$
$\boldsymbol{U}$	U	MU	HU
$\boldsymbol{MU}$	MU	HU	U
$\boldsymbol{HU}$	HU	U	MU

Using this table as a guide, one isomorphism from $\mathcal{A}_4/\mathcal{U}$ to $\mathcal{Z}_3$ would be the assignment

$$f : \begin{pmatrix} U & MU & HU \\ [0]_3 & [1]_3 & [2]_3 \end{pmatrix}$$

****

Example 91 *The set $H = \{A \in M_2 : \texttt{Det}(A) = 1\}$ is a normal subgroup of $\mathcal{M}_2$. Describe the elements of $\mathcal{M}_2/\mathcal{H}$. To what group is this quotient isomorphic?*

Solution. You showed this set is a normal subgroup in Exercise 4.22. We know that a left coset of this subgroup has the form

$$XH = \{XA : A \in H\} = \{B \in M_2 : \texttt{Det}(B) = \texttt{Det}(X)\}$$

For any nonzero real number a, we can construct a member X_a of M_2 such that $\texttt{Det}(X_a) = a$ (try this yourself). Consequently, there will be exactly one left coset for each nonzero real number, and we know that the left cosets have the form

$$H_a = \{B \in M_2 : \texttt{Det}(B) = a\}$$

. where a is any nonzero real number. It stands to reason then that $\mathcal{M}_2/\mathcal{H}$ is probably isomorphic to $\mathcal{R}^*$, the group of nonzero real numbers under multiplication. Is this really true? Consider the function $f : L_H \longrightarrow \mathbb{R}^*$ defined by $f(H_a) = a$. The function is clearly onto, since there is a left coset for every nonzero real number. Since the members of L_H are pairwise disjoint, it is also clear that f is one-to-one. (This is also the reason why f is a function at all.) Recall from linear algebra that

$$\texttt{Det}(AB) = \texttt{Det}(A)\texttt{Det}(B) = \texttt{Det}(BA)$$

for all $n \times n$ matrices A and B. (Since we are only working with 2×2 matrices, you can easily prove this directly for M_2.) Consequently, we know that

$$H_a \circledast H_b = H_{ab} = H_b \circledast H_a$$

This tells us that the quotient group $\mathcal{M}_2/\mathcal{H}$ is abelian (in keeping with our suspicion that it is isomorphic to $\mathcal{R}^*$), and it also tells us that

$$f\left(H_a \circledast H_b\right) = f\left(H_{ab}\right) = ab = f(H_a)f(H_b)$$

Therefore, the function f preserves the operation and is an isomorphism.

The previous examples show that quotient groups are often isomorphic to familiar groups which are simpler is some respects than the "parent" groups they originate from — noncylic groups can give rise to cyclic quotients, nonabelain groups can give rise to abelian quotients, *etc.* We can think of quotient groups as simpler "approximations" to their parent groups. The structure of a quotient group must be related in some way to the structure of its parent group. We conclude this section by developing a way to explore the relationship between the structure of a quotient group and the structure of its parent group.

Let $\mathcal{G} = (G, *)$ be a group, let H be a normal subgroup of $\mathcal{G}$, and suppose that the quotient group $\mathcal{G}/\mathcal{H}$ is isomorphic to another group $\mathcal{J} = (J, \times)$. We can think of $\mathcal{J}$ as an "approximation" to the group $\mathcal{G}$ — it carries some of the structure from $\mathcal{G}$ but has, in a sense, "forgotten" part of that structure. How is $\mathcal{G}$ related to $\mathcal{J}$? When we want to show two groups have the same structure, we try to create an isomorphism between them (the term acually means "same structure.") What kind of function could we create between $\mathcal{G}$ and $\mathcal{J}$? Since they have similar structure, we would expect that some kind of "structure preserving" function exists between them.

The members of $\mathcal{G}/\mathcal{H}$ are the left cosets of $\mathcal{G}$ generated by the subgroup H. Since the family of left cosets L_H is a partition of the universe G, we can think of its members as equivalence classes. In other words, we are declaring all elements of the same left coset to be "equal." This suggests a way to build a function from G to J. First, suppose that $f : L_H \longrightarrow J$ is an isomorphism from $\mathcal{G}/\mathcal{H}$ to $\mathcal{J}$. The function f assigns each left coset X to unique member $y \in J$. Define a mapping $\psi_H : G \longrightarrow J$ by the following rule: For each $a \in G$, let $\psi_H(a) = f(aH)$. In other words, take all of the elements in G that are "equal" (reside in the same left coset) and send them to the member of J assigned that coset.

Is this assignment acutally a function? Since the members of L_H are pairwise disjoint, we know that a element $a \in G$ cannot reside in two different left cosets. Hence, ψ cannot assign a to more than one element of J and is therefore a function. Unless $H = \{e\}$ is the trivial subgroup, the left cosets of H all contain more than one element; hence, the ψ_H is not one-to-one in general. It will, however, be onto since the function f is onto. Curiously, the function ψ_H "preserves the operation" in the same sense that f does. To see why, suppose that $a, b \in G$ and observe that, since f is an isomorphism,

$$\psi_H(a * b) = f((a * b)H) = f(aH \circledast bH) = f(aH) \times f(bH) = \psi_H(a) \times \psi_H(b)$$

Definition 92 *Let $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \times)$ be groups. A **homomorphism** from $\mathcal{G}$ to $\mathcal{J}$ is a function $\psi : G \longrightarrow J$ with the property that $\psi(a * b) = \psi(a) \times \psi(b)$ for all $a, b \in G$. A homomorphism which is one-to-one is called an **endomorphism**, and one which is onto is called an **epimorphism**.*

The term "homomorphism" means "similar structure." An isomorphism is actually a bijective homomorphism. In the exercises for Section 5, you showed that the function $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$ defined by $f([a]_2, [b]_2) = [2a + 2b]_4$ is a homomorphism. It is not an endomorphism since $f([1]_2, [0]_2) = f([0]_2, [1]_2)$. It is also not an epimorphism since $[3]_4$ has no preimage under f.

Example 93 *Let n be a positive integer and show that the function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = nx$ is an endomorphism from $\mathcal{Z}$ to $\mathcal{Z}$ but not an epimorphism if $n > 1$.*

Solution. First, note that the function is one-to-one since $f(x) = f(y) \Longrightarrow nx = ny \Longrightarrow x = y$. If $n > 1$, then 1 has no preimage under f since the equation $1 = nx$ has no integer solution. Consequently, f is not onto when $n > 1$. The function f is a homomorphism since

$$f(x + y) = n(x + y) = nx + ny = f(x) + f(y)$$

We may therefore conclude that f is an endomorphism from $\mathcal{Z}$ to $\mathcal{Z}$ but is not an epimorphism when $n > 1$.

****

Example 94 *Construct an epimorphism from the Alphabet Group $\mathcal{A}_4$ to $\mathcal{Z}_3$.*

Solution. Consider the subgroup $U = \{E, I, L, O\}$. In Example 90, we showed that $\mathcal{A}_4/\mathcal{U}$ is isomorphic to $\mathcal{Z}_3$ via the function

$$f : \begin{pmatrix} U & MU & HU \\ [0]_3 & [1]_3 & [2]_3 \end{pmatrix}$$

We also determined that $MU = \{M, P, G, J\}$ and $HU = \{H, K, N, Q\}$. Based on this information, we know how to construct an epimorphism $\psi_U : A_4 \longrightarrow \mathbb{Z}_3$. We simply let

$$\psi_U(E) = \psi_U(I) = \psi_U(L) = \psi_U(O) = [0]_3$$

$$\psi_U(M) = \psi_U(P) = \psi_U(G) = \psi_U(J) = [1]_3$$

$$\psi_U(H) = \psi_U(K) = \psi_U(N) = \psi_U(Q) = [2]_3$$

****

The following theorem summarizes some important properties that homomoprhisms possess. Compare these properties to those enjoyed by isomorphisms. Many are the same, but some key isomorphism properties are missing. In addition, some of the proofs below are slightly more challenging since we are not necessarily working with bijections when dealing with homomorphisms.

Theorem 95 *Let $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \times)$ be groups and suppose that $f : G \longrightarrow J$ is a homomorphism. The following statements are true.*

1. *If e is the identity element for $\mathcal{G}$, then $f(e)$ is the identity element for J.*
2. *If $a \in G$, then $f(a^{-1}) = [f(a)]^{-1}$.*
3. *If H is a subgroup of $\mathcal{G}$, then $f(H) = \{f(a) : a \in H\}$ is a subgroup of $\mathcal{J}$.*
4. *If X is a subgroup of $\mathcal{J}$, then $\mathtt{Pre}_f(X) = \{a \in G : f(a) \in X\}$ is a subgroup of $\mathcal{G}$.*

Proof. To establish Claim (1), suppose that e is the identity element of $\mathcal{G}$ and suppose that ϵ is the identity element of $\mathcal{J}$. It is certainly the case that $\epsilon \times f(e) = f(e)$. Observe that

$$f(e) \times f(e) = f(e * e) = f(e) \quad \Longrightarrow \quad f(e) \times f(e) = \epsilon \times f(e)$$

The Cancellation Laws for groups now tell us that $f(e) = \epsilon$, as desired.

Once we know that $f(e) = \epsilon$, the proof that $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$ proceeds in the same way that it did for isomorphisms. Let $a \in G$. We know that

$$f(a) \times f(a^{-1}) = f(a * a^{-1}) = f(e) = \epsilon \qquad f(a^{-1}) \times f(a) = f(a^{-1} * a) = f(e) = \epsilon$$

The uniqueness of inverses in a group now tells us that $f(a^{-1}) = [f(a)]^{-1}$, as desired.

To prove Claim (3), let $H \subseteq G$ be a subgroup of $\mathcal{G}$. We need to show that $f(H)$ is closed under the operation on J and closed with respect to the formation of inverses in $\mathcal{J}$. To this end, let $u, v \in f(H)$. There exist $a, b \in H$ such that $a \in \mathtt{Pre}_f(u)$ and $b \in \mathtt{Pre}_f(v)$. Since H is a subgroup of $\mathcal{G}$, we know that

$a * b \in H$; consequently, we know that $f(a * b) \in f(H)$. Since we have assumed f "preserves the operation," we know that

$$u \times v = f(a) \times f(b) = f(a * b) \in f(H)$$

Thus, $f(H)$ is closed under the operation on J. To see that $f(H)$ is closed with respect to the formation of inverses, consider u. Since H is a subgroup of $\mathcal{G}$, we know that $a^{-1} \in H$; hence, we know that $f(a^{-1}) \in f(H)$. Therefore, according to Claim (2), we know

$$u^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(H)$$

We may now conclude that $f(H)$ is a subgroup of $\mathcal{J}$, as desired.

To prove Claim (4), suppose that X is a subgroup of $\mathcal{J}$; and for simplicity, let $H = \mathtt{Pre}_f(X) = \{a \in G : f(a) \in X\}$. Since $f(e) = \epsilon$, we know that $e \in H$; hence, we know that H is nonempty. We need to show that H is closed under the operation on G and closed with respect to the formation of inverses in $\mathcal{G}$. To this end, suppose that $a, b \in H$. This tells us that $f(a), f(b) \in X$. Now, since X is a subgroup of $\mathcal{J}$, we know that $f(a) \times f(b) \in X$. Consequently, we know that

$$f(a * b) = f(a) \times f(b) \in X$$

and this tells us that $a * b \in H$. Since X is a subgroup of $\mathcal{J}$, we know that $[f(a)]^{-1} \in X$. Thus, by Claim (2) we know that $f(a^{-1}) \in X$; and this tells us that $a^{-1} \in H$, as desired.

QED

Corollary 96 *Let $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \times)$ be groups and suppose that $f : G \longrightarrow J$ is a homomorphism. If f is an endomorphism, then $\mathcal{G}$ is isomorphic to $(f(G), \times)$.*

Proof. We know that $f(G)$ is a subgroup of $\mathcal{J}$ by the previous theorem. Clearly $f : G \longrightarrow f(G)$ is onto. By assuming that f is an endomorphism, we are assuming that f is one-to-one as well. Hence, f is an isomorphism from $\mathcal{G}$ to $(f(G), \times)$.

QED

The following result, called the *Fundamental Homomorphism Theorem*, tells us that all homomorphisms are intimately connected to quotient groups. It also tells us that all homomorphisms can be created by following the steps outlined in the discussion preceding Definition 92.

Theorem 97 *Let $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \times)$ be groups and suppose that $f : G \longrightarrow J$ is a homomorphism. The following statements are true.*

1. *If ϵ is the identity element for $\mathcal{J}$, then the set $H = \mathtt{Pre}_f(\{\epsilon\}) = \{a \in G : f(a) = \epsilon\}$ is always a normal subgroup of $\mathcal{G}$.*
2. *The quotient group $\mathcal{G}/\mathcal{H}$ is isomorphic to $(f(G), \times)$, where $H = \mathtt{Pre}_f(\{\epsilon\})$.*

Proof. To prove Claim (1), we first note that $H = \mathtt{Pre}_f(\{\epsilon\})$ is a subgroup of $\mathcal{G}$ by the previous theorem. To see that it is normal, let $a \in G$ and $h \in H$ and observe that since f is a homomorphism, the previous theorem tells us

$$f(a * h * a^{-1}) = f(a) \times f(h) \times f(a^{-1}) = f(a) \times \epsilon \times [f(a)]^{-1} = f(a) \times [f(a)]^{-1} = \epsilon$$

Hence, we know that $a * h * a^{-1} \in H$; and we may conclude that H is normal.

To prove Claim (2), we must construct an isomorphism from $\mathcal{G}/\mathcal{H}$ to $(f(G), \times)$. Suppose that $aH \in L_H$. If $x, y \in aH$, then Exercsie 4.14 tells us that $x * y^{-1} \in H$. Consequently, we know that

$$\epsilon = f(x * y^{-1}) = f(x) \times [f(y)]^{-1}$$

and this allows us to conclude that $f(x) = f(y)$ for all $x, y \in aH$. This suggests how we should go about defining the mapping from L_H to $f(G)$. Consider the function $\psi : L_H \longrightarrow f(G)$ defined by $\psi(aH) = f(a)$. Our previous argument shows that ψ is a function. It is clearly onto $f(G)$. To see that ψ is one-to-one, suppose $aH, bH \in L_H$ are such that $\psi(a) = \psi(b)$. Of couse, this means $f(a) = f(b)$ by the definition of the function ψ. Observe that

$$f(a) = f(b) \quad \Longrightarrow \quad f(a) \times [f(b)]^{-1} = \epsilon \quad \Longrightarrow \quad f(a) \times f(b^{-1}) = \epsilon \quad \Longrightarrow \quad f(a * b^{-1}) = \epsilon \quad \Longrightarrow \quad a * b^{-1} \in H$$

Now, Exercise 4.14 tells us that $a \in bH$. This is sufficient to prove that $aH = bH$; consequently, we may conclude that ψ is one-to-one. It is easy to see that ψ preserves the operation. Indeed, for all $aH, bH \in L_H$ we have

$$\psi(aH \circledast bH) = \psi((a * b)H) = f(a * b) = f(a) \times f(b) = \psi(aH) \times \psi(bH)$$

It follows that ψ is an isomorphism from $\mathcal{G}/\mathcal{H}$ to $(f(G), \times)$.

QED

Definition 98 *Let $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \times)$ be groups and suppose that $f : G \longrightarrow J$ is a homomorphism. The set $\mathtt{Pre}_f(\{\epsilon\}) = \{a \in G : f(a) = \epsilon\}$ is called the **kernel** of f and is denoted by $\mathtt{KER}(f)$.*

Example 99 *Consider the function $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f[(a, b)] = b - a$.*

1. *Show that f is a homomorphism from $\mathcal{Z} \times \mathcal{Z}$ to $\mathcal{Z}$.*
2. *Show that the kernel of f is isomorphic to $\mathcal{Z}$.*
3. *Show that the quotient $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$ is also isomorphic to $\mathcal{Z}$.*

Solution. In this case, the formula defining f is unambiguous, so it is clear that f is a function. To see that it is a homomorphism, observe that for $(x, y), (u, v) \in \mathbb{Z} \times \mathbb{Z}$, we have

$$\begin{aligned} f\left[(x, y) \oplus (u, v)\right] &= f[(x + u, y + v)] \\ &= (y + v) - (x + u) \\ &= (y - x) + (v - u) \\ &= f[(x, y)] \oplus f[(u, v)] \end{aligned}$$

Now, we know that $(a, b) \in \mathtt{KER}(f) \iff f[(a, b)] = 0 \iff b - a = 0 \iff b = a$. Hence, we know that $\mathtt{KER}(f) = \{(a, a) : a \in \mathbb{Z}\}$. It is easy to see that $(1, 1)$ serves as a generator for $\mathtt{KER}(f)$; thus we know $\mathtt{KER}(f)$ is a cyclic subgroup of $\mathcal{Z} \times \mathcal{Z}$. Because $\mathtt{KER}(f)$ is also clearly infinite, we must conclude that $\mathtt{KER}(f)$ is isomorphic to $\mathcal{Z}$. A left coset of $\mathtt{KER}(f)$ will have the form

$$(x, y)\mathtt{KER}(f) = \{(x, y) + (a, a) : a \in \mathbb{Z}\} = \{(x + a, y + a) : a \in \mathbb{Z}\}$$

Based on this description of its members, it is not obvious that $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$ is also isomorphic to $\mathcal{Z}$. However, $f([(0, b)] = b$ for any integer b; therefore, f is an epimorphism from $\mathcal{Z} \times \mathcal{Z}$ to $\mathcal{Z}$. The Fundamental Homomorphism Theorem forces us to conclude that $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$ is also isomorphic to $\mathcal{Z}$.

Looking at the previous example, you would be justified in asking "If $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$ is cyclic, then what is a generator?" Again, the answer to this question is not obvious looking directly at the cosets of $\mathtt{KER}(f)$. However, the Fundamental Homomorphism Theorem comes to our aid here as well. According to the proof of the Fundamental Theorem, the isomorphism $\psi : L_{\mathtt{KER}(f)} \longrightarrow \mathbb{Z}$ is defined by $\psi[(x,y)\mathtt{KER}(f)] = f(x,y) = y - x$. Since we know that 1 serves as a generator for $\mathcal{Z}$, the fact that $\psi^{-1} : \mathbb{Z} \longrightarrow L_{\mathtt{KER}(f)}$ is also an isomorphism tells us that $\psi^{-1}(1)$ serves as a generator for $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$. Now, since $f[(2,1)] = 1$, we may conclude that $\psi^{-1}(1) = (2,1)\mathtt{KER}(f)$ is a generator for $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$.

The previous discussion leads us to a surprising conclusion — *Every* coset $(x,y)\mathtt{KER}(f)$ is a "power" of the coset $(2,1)\mathtt{KER}(f)$. Although the Fundamental Homomorphism Theorem forces us to conclude this, it is certainly not directly apparent why this should be the case. Observe that for each integer n, we have

$$[(2,1)\mathtt{KER}(f)]^n = (2n,n)\mathtt{KER}(f) = \{(2n+a, n+a) : a \in \mathbb{Z}\}$$

Therefore, if it is true that $(x,y)\mathtt{KER}(f) = [(2,1)\mathtt{KER}(f)]^n$ for some integer n, then there must exist an integer a such that $(x,y) = (2n+a, n+a)$. This gives rise to a system of two equations and two unknowns, namely

$$\left\{ \begin{array}{ccccc} 2n & + & a & = & x \\ n & + & a & = & y \end{array} \right.$$

This system is consistent; in fact, it has a unique solution, namely $n = x - y$ and $a = 2y - x$. This tells us that $(x,y) \in [(2,1)\mathtt{KER}(f)]^{x-y}$. Since the cosets of $\mathtt{KER}(f)$ are pairwise disjoint, this proves that $(x,y)\mathtt{KER}(f) = [(2,1)\mathtt{KER}(f)]^{x-y}$. Consequently, $(2,1)\mathtt{KER}(f)$ really is a generator for $(\mathcal{Z} \times \mathcal{Z})/\mathtt{KER}(f)$, just as the Fundamental Theorem predicts.

Corollary 100 *If $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \bullet)$ are groups, then $G \times \{\epsilon\}$ (where ϵ is the identity for $\mathcal{J}$) is a normal subgroup of $\mathcal{G} \times \mathcal{J}$, and $(\mathcal{G} \times \mathcal{J})/(G \times \{\epsilon\})$ is isomorphic to $\mathcal{J}$.*

Proof. Consider the function $\pi_J : G \times J \longrightarrow J$ defined by $\pi_J[(a,b)] = b$. (This function is called a *projection map.*) The map is clearly onto J; and, for all $(a,b), (c,d) \in G \times J$, we have

$$\pi_J[(a,b) \otimes (c,d)] = \pi_J[(a * c, b \bullet d) = b \bullet d = \pi_J[(a,b)] \bullet \pi_J[(c,d)]$$

Thus, π_J is a epimorphism from $\mathcal{G} \times \mathcal{J}$ to $\mathcal{J}$. Furthermore, observe that

$$(a,b) \in \mathtt{KER}(\pi_J) \iff \pi_J[(a,b)] = \epsilon \iff (a,b) \in G \times \{\epsilon\}$$

We see that $\mathtt{KER}(\pi_J) = G \times \{\epsilon\}$, so the Fundamental Homomorphism Theorem tells us that $G \times \{\epsilon\}$ is normal. This theorem also tells us that $(\mathcal{G} \times \mathcal{J})/(G \times \{\epsilon\})$ is isomorphic to $\mathcal{J}$, as desired.

QED

If $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \bullet)$ are groups, then it should be easy to see that $\mathcal{G}$ is isomorphic to $(G \times \{\epsilon\}, \otimes)$. Although it is a bit sloppy, we oftern summarize the previous corollary by the statement "$(\mathcal{G} \times \mathcal{J})/\mathcal{G}$ is isomorphic to $\mathcal{J}$." Of course, it is also true that "$(\mathcal{G} \times \mathcal{J})/\mathcal{J}$ is isomorphic to $\mathcal{G}$." We leave proof of this as an exercise.

Corollary 101 *Let $\mathcal{G} = (G, *)$ be any group. A subset H of G is a normal subgroup of $\mathcal{G}$ if and only if it is the kernel of some homomorphism from $\mathcal{G}$ to another group.*

Proof. If H is the kernel of some homomorphism, then the Fundamental Homomorphism Theorem tells us that H is a normal subgroup. Conversely, suppose that H is a normal subgroup. This means we can form the quotient group $\mathcal{G}/\mathcal{H} = (L_H, \circledast)$. Consider the mapping $\nu : G \longrightarrow L_H$ defined by $\nu(a) = aH$. Since the members of L_H are pairwise disjoint, we know that ν is a function. Furthermore, since

$$\nu(a * b) = (a * b)H = aH \circledast bH = \nu(a) \circledast \nu(b)$$

we may conclude that ν is a homomorphism. (It is actually an epimorphism.) Now, observe that

$$a \in H \quad \Longleftrightarrow \quad aH = H \quad \Longleftrightarrow \quad \nu(a) = H$$

Since H is the identity element for $\mathcal{G}/\mathcal{H}$, it follows that $H = \texttt{KER}(\nu)$.

QED

The previous result tells us that all normal subgroups of a group can be created by first constructing homomorphisms to other groups and determining their kernels. It is not practical to use this method to determine all normal subgroups, since it is seldom obvious which groups to use or how to bild the homomorphisms. However, it is usually easier to construct a homomorphism than it is to build a normal subgroup.

EXERCISES FOR SECTION 6

.

1. Consider the group $\mathcal{Z}_4 \times \mathcal{U}_4$, where $\mathcal{U}_4$ is the group of units modulo 4. Let $H = \langle([2]_4, [3]_4)\rangle$ and $K = \langle([2]_4, [1]_4)\rangle$. (Remember that the product operation is addition modulo 4 in the first coordinate and multiplication modulo 4 in the second.)

   (a) Show that $\mathcal{H} = (H, \otimes)$ is isomorphic to $\mathcal{K} = (K, \otimes)$ (where $\otimes$ is the product operation restricted to H and K.)

   (b) Show that $(\mathcal{Z}_4 \times \mathcal{U}_4)/\mathcal{H}$ is *not* isomorphic to $(\mathcal{Z}_4 \times \mathcal{U}_4)/\mathcal{K}$. (Hence, isomorphic subgroups do not guarantee isomorphic quotient groups.)

2. In Exercise 4.25, you showed that the center of the group $\mathcal{M}_2$ is the set

$$Z(\mathcal{M}_2) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R}^* \right\}$$

   In Exercise 4.24, you showed that the center of any group is a normal subgroup of that group; hence, we may talk about the quotient group $\mathcal{M}_2/Z(\mathcal{M}_2)$.

   (a) If $N \in M_2$, show that the left coset $NZ(\mathcal{M}_2) = \{aN : a \in \mathbb{R}^*\}$.

   (b) Show by counterexample that the quotient group $\mathcal{M}_2/Z(\mathcal{M}_2)$ is not abelian.

3. Suppose that $\mathcal{G} = (G, *)$ is a cyclic group. If H is any subgroup of $\mathcal{G}$, prove that $\mathcal{G}/\mathcal{H}$ is cyclic.

4. Let $\mathcal{R}^* = (\mathbb{R}^*, \cdot)$ be the group of nonzero real numbers under multiplication. Show that the function $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = |x|$ is a homomorphism. What is the kernel of f?

5. Consider the function $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ defined by $f[(a, b)] = (b - a, 4a - 4b)$. Prove that f is a homomorphism. What is the kernel of f?

6. Let $\mathcal{R} = (\mathbb{R}, +)$ be the group of real numbers under addition. Show that the function $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ defined by $f(x) = \sqrt[3]{x}$ preserves the identity element and preserves additive inverses but is *not* a homomorphism from $\mathcal{R}$ to $\mathcal{R}$.

7. Let $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \bullet)$ be groups, and suppose $f : G \longrightarrow H$ is a homomorphism. Let $a \in G$.

   (a) Use mathematical induction to prove that $f(a^n) = [f(a)]^n$ for any positive integer n.

   (b) Use Part (a) and Theorem 95 to show that $f(a^n) = [f(a)]^n$ for any integer n.

8. Let $\mathcal{G} = (G, *)$ and $\mathcal{H} = (H, \bullet)$ be groups, and suppose $a \in G$ has finite order.

   (a) If $f : G \longrightarrow H$ is a homomorphism, show that the order of $f(a)$ in $\mathcal{H}$ is a divisor of the order of a in $\mathcal{G}$.

   (b) If K is a normal subgroup of $\mathcal{G}$, explain why the order of aK in $\mathcal{G}/\mathcal{K}$ is a divisor of the order of a in $\mathcal{G}$. (Consider the mapping $\nu : G \longrightarrow L_K$ introduced in the proof of Corollary 101.)

9. Consider the function $f : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by

$$f([x]_6) = \begin{cases} ([0]_2, [0]_2) & \text{if } x \text{ is even} \\ ([0]_2, [1]_2) & \text{if } x \text{ is odd} \end{cases}$$

   (a) Show that f is a homomorphism.

   (b) Determine the kernel of f.

   (c) Construct the quotient group $\mathcal{Z}_6/\texttt{KER}(f)$.

10. Let $\mathcal{G} = (G, *)$ be an abelian group. If H is any subgroup of $\mathcal{G}$, prove that $\mathcal{G}/\mathcal{H}$ is abelian.

11. If $\mathcal{G} = (G, *)$ and $\mathcal{J} = (J, \bullet)$ are groups, prove that $\{e\} \times J$ (where e is the identity for $\mathcal{G}$) is a normal subgroup of $\mathcal{G} \times \mathcal{J}$, and $(\mathcal{G} \times \mathcal{J})/(\{e\} \times J)$ is isomorphic to $\mathcal{G}$.

12. Let $\mathcal{G} = (G, *)$ be any group and suppose H is a normal subgroup of $\mathcal{G}$. If $[G : H] = n$ for some positive integer n, use Exercise 4.15 to show that $a^n \in H$ for all $a \in G$.

13. Let $\mathcal{G} = (G, *)$ be any group and suppose H is a normal subgroup of $\mathcal{G}$. Use Exercise 4.14 to prove that the following statements are equivalent:

   (a) The quotient group $\mathcal{G}/\mathcal{H}$ is cyclic.

   (b) There exists an $a \in G$ such that, for all $x \in G$ we have $x * a^n \in H$ for some integer n.

14. Let $\mathcal{F} = (F, *)$ and $\mathcal{G} = (G, \bullet)$ be groups and suppose that H is a normal subgroup of $\mathcal{F}$ and J is a normal subgroup of $\mathcal{G}$.

   (a) Show that the mapping $\phi : F \times G \longrightarrow L_F \times L_G$ defined by $\phi[(a, b)] = (aH, bJ)$ is a epimorphism from $\mathcal{F} \times \mathcal{G}$ to $(\mathcal{F}/\mathcal{H}) \times (\mathcal{G}/\mathcal{J})$.

   (b) Show that $\texttt{KER}(\phi) = H \times J$.

   (c) Explain why $(\mathcal{F} \times \mathcal{G}) / (\mathcal{H} \times \mathcal{J})$ is isomorphic to $(\mathcal{F}/\mathcal{H}) \times (\mathcal{G}/\mathcal{J})$.

15. Let $\mathcal{G} = (G, *)$ be any group. In Exercise 4.24, you showed that the set $\texttt{INN}(\mathcal{G})$ of inner automorphisms of $\mathcal{G}$ is a subgroup of the automorphism group $\mathcal{A}_G = (A_G, \circ)$ for $\mathcal{G}$.

   (a) Show that the mapping $f : G \longrightarrow A_G$ defined by $f(a) = \varphi_a$ is a homomorphism with $f(G) = \texttt{INN}(\mathcal{G})$. (The function φ_a is defined in Exercise 4.24.)

   (b) Show that $\texttt{KER}(f) = Z(\mathcal{G})$.

   (c) Explain why $\mathcal{G}/\mathcal{Z}(\mathcal{G})$ is isomorphic to $(\texttt{INN}(\mathcal{G}), \circ)$.

16. Let $\mathcal{G} = (G, *)$ be any group. Suppose that H and K are subgroups of $\mathcal{G}$, and suppose that H is a normal subgroup of $\mathcal{G}$. In Exercise 4.27, you proved that $H \cap K$ is a normal subgroup of $\mathcal{K} = (K, *)$, that HK is a subgroup of $\mathcal{G}$, and that H is a normal subgroup of $\mathcal{HK} = (HK, *)$. This means we can discuss the quotient groups $\mathcal{HK}/\mathcal{H}$ and $\mathcal{K}/(H \cap K)$.

(a) Show that every left coset of H in HK can be written as Hk for some $k \in K$. (Use Exercise 4.12.)

(b) Show that the mapping $f : K \longrightarrow L_H$ defined by $f(k) = Hk$ is an epimorphism.

(c) Show that $\texttt{KER}(f) = H \cap K$.

(d) Explain why $\mathcal{K}/(H \cap K)$ is isomorphic to $\mathcal{HK}/\mathcal{H}$. (This result is called the *First Isomorphism Theorem*.)