2

Relationships between Systems

We shift from individual systems to investigating relations between systems, motivated by several questions. When are two systems the same or similar? What are elements and "subsystems"? How can we build new systems from ones we know? Sections 2.1 and 2.4 address the first question, while Sections 2.2 and 2.3 provide important responses for the other two. Comparing different but related systems distinguishes modern mathematics, and abstract algebra has been at the forefront of investigating these connections. Before the nineteenth century, when there were essentially only one number system and one geometry, such comparisons would have seemed unimaginable. The nineteenth century brought about a profusion of each, as well as new kinds of systems. Over the last two hundred years, mathematical models of biological, physical, and economic systems have required a large variety of differing mathematical systems. Hence mathematicians need ways to compare systems to understand them.

2.1 Isomorphisms

What's in a name? that which we call a rose By any other name would smell as sweet… —Shakespeare (*Romeo and Juliet*)

In Section 1.3 addition in $\mathbb{Z}_3$ seemed exactly like composition in $\mathbf{C}_3$. Indeed, these systems differ only in the names of their elements and operations, not their algebraic structure. In contrast, as we will see, $\mathbb{Z}_3$ and $\mathbb{Z}_4$, although they have several elements with the same names, differ in their algebraic structure. The definition of an isomorphism will capture the idea of two systems with identical structure, illustrated in Example 1. Isomorphisms and their variants appear in many areas of mathematics. Section 2.4 considers a less exacting and so more broadly applicable concept, homomorphism, for related but not identical systems.

Example 1. Pair each element x of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with R^x in $\mathbf{C}_4 = \{I = R^0, R^1, R^2, R^3\}$. If we define $\alpha : \mathbb{Z}_4 \to \mathbf{C}_4$ by $\alpha(x) = R^x$, then composition matches addition: $R^x \circ R^y = R^z$ corresponds to $x +_4 y = z$ or more abstractly $\alpha(x) \circ \alpha(y) = \alpha(z) = \alpha(x +_4 y)$. The same pairing idea works for $\mathbb{Z}_n$ and $\mathbf{C}_n$, for any n. ♢

The concept of an isomorphism has two parts. First, a bijection matches elements, corresponding to the Greek prefix "iso," meaning "equal." As we will see, just matching elements with a bijection doesn't tell us much. The Greek root "morph" means "form" and refers to the second, structural requirement for an isomorphism. We want the bijection somehow to match the operations of the two systems, which define their algebraic properties and structure. In Example 1 the match between the equations illustrates this idea. That is, we get the same answer whether we map the elements to $\mathbf{C}_4$ and then compose them or we first add two elements in $\mathbb{Z}_4$ and then map the sum to $\mathbf{C}_4$. The equation $\alpha(x) \circ \alpha(y) = \alpha(x +_4 y)$ expresses this more formally and is the basis for our definition of isomorphism below. (If the mapping between systems has just this structural equality without the bijection, we will call it a homomorphism in Section 2.4.) We first consider systems with one operation.

Isomorphisms for One Operation.

Definition (Isomorphism). Two systems $(A, *)$ and $(B, \circledast)$ are *isomorphic* if and only if there is a bijection $\sigma : A \to B$ so that for all $x, y \in A$, $\sigma(x * y) = \sigma(x) \circledast \sigma(y)$. We call σ an *isomorphism* and write $(A, *) \approx (B, \circledast)$ or more simply $A \approx B$.

Example 2. Define $\psi : \mathbb{R} \to \mathbb{R}^+$ by $\psi(x) = e^x$, where $\mathbb{R}^+$ is the set of positive real numbers. Then, as we show, ψ is an isomorphism from $(\mathbb{R}, +)$ onto $(\mathbb{R}^+, \cdot)$. The familiar exponent rule $e^{x+y} = e^x e^y$ becomes $\psi(x + y) = \psi(x) \cdot \psi(y)$, proving operation preservation. Since $\ln : \mathbb{R}^+ \to \mathbb{R}$ given by $\ln(y) = x$ is the inverse function of ψ, ψ must be a bijection. Further, ln gives an isomorphism from $(\mathbb{R}^+, \cdot)$ onto $(\mathbb{R}, +)$. ♢

Example 3. The group S of solutions to the differential equation $y'' = -y$ from Example 4 of Section 1.2 is isomorphic to the complex numbers with addition. In a differential equations course, one can show that the solutions are of the form $a \sin(x) + b \cos(x)$. The reader can check that the mapping $\phi : \mathbb{C} \to S$ defined by $\phi(a + bi) = a \sin(x) + b \cos(x)$ fulfills all of the requirements of an isomorphism. The isomorphism helps us understand the group of solutions in terms of the complex numbers, which we understand better. You may understand the two-dimensional vector space $\mathbb{R}^2$ even better and there is an isomorphism from $\mathbb{R}^2$ with addition to $\mathbb{C}$ with addition, given by $\alpha(x, y) = x + yi$. We can combine these isomorphisms to connect the vector space with the solutions of the differential equation: define $\beta : \mathbb{R}^2 \to S$ by $\beta = \phi \circ \alpha$ or $\beta(a, b) = a \sin(x) + b \cos(x)$. ♢

Example 1 showed that $\mathbb{Z}_4$ is isomorphic to $\mathbf{C}_4$, but there are other groups with four elements also isomorphic to these two, for instance, the group $\{1, i, -1, -i\}$ from Example 3 of Section 1.2. Similarly there are other groups isomorphic to $\mathbb{Z}_n$. These types of groups, which we call *cyclic*, form building blocks for groups and rings. What unites them is that each one can be built from one element.

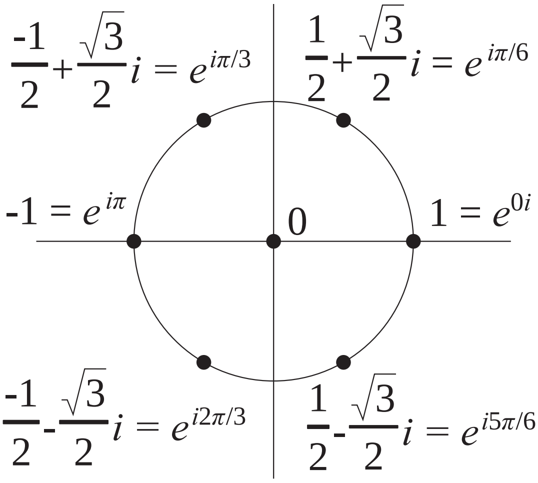
$\frac{-1}{2}+\frac{\sqrt{3}}{2}i = e^{i\pi/3}$
$\frac{1}{2}+\frac{\sqrt{3}}{2}i = e^{i\pi/6}$
$-1 = e^{i\pi}$
0
$1 = e^{0i}$
$\frac{-1}{2}-\frac{\sqrt{3}}{2}i = e^{i2\pi/3}$
$\frac{1}{2}-\frac{\sqrt{3}}{2}i = e^{i5\pi/6}$

Figure 2.1. The sixth roots of unity.

Definition (Cyclic group). A group $(G, *)$ is *cyclic* if and only if there is an element $g \in G$ so that for all $x \in G$ there is $k \in \mathbb{Z}$ such that $x = g^k$. We say g *generates* G and write $\langle g \rangle = G$.

The definition uses multiplicative notation, customary for general groups. It has the advantage of making clear the difference between g, an element of the group, and k, an integer written as an exponent indicating the number of times g is multiplied by itself. With additive notation, as in $\mathbb{Z}_5$, the repeated addition $2 + 2 + 2 = 1$ would become $3 \cdot 2 = 1$, and we could easily think that the 3 in this product came from $\mathbb{Z}_5$, which is not the intention.

Example 4. The nth *roots of unity* in $\mathbb{C}$ have the form $\cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n})$, where $0 \leq k < n$. They form a group under multiplication. The alternative notation $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ makes the multiplication easier to understand without the need for the addition formulas of trigonometry. We write the nth roots as $e^{2\pi ik/n} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n})$ and then $e^{2\pi ik/n} \cdot e^{2\pi iz/n} = e^{2\pi i(k+z)/n}$. Also, $e^{2\pi i} = 1$. This group is cyclic, generated by $e^{2\pi i/n}$. When n is greater than two, the group has other generators as well. In Figure 2.1 the two generators are $\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. ◊

The use of exponents in the definition of a cyclic group suggests that each cyclic group is isomorphic to one of the groups $\mathbb{Z}_n$ or, if the group is infinite, to $\mathbb{Z}$. Theorem 2.1.1 confirms this.

Theorem 2.1.1. *An infinite cyclic group is isomorphic to* $(\mathbb{Z}, +)$*. A cyclic group with* n *elements is isomorphic to* $(\mathbb{Z}_n, +_n)$*.*

Proof. Suppose that g generates an infinite cyclic group $(G, *)$ and define $\sigma : \mathbb{Z} \to G$ by $\sigma(x) = g^x$. To prove the "morphism" part let $y, z \in \mathbb{Z}$. Then $\sigma(y + z) = g^{y+z} = g^y * g^z = \sigma(y) * \sigma(z)$, by the definition of exponents. Because every element of G is of the form g^k, σ is an onto function.

For one-to-one, let $y, z \in \mathbb{Z}$, and suppose that $\sigma(y) = \sigma(z)$. That is, $g^y = g^z$. The inverse of g^y is g^{-y} so $e = g^0 = g^{y-y} = g^y * g^{-y} = g^z * g^{-y} = g^{z-y}$. We need to show that $y = z$. For a contradiction, suppose $y \neq z$, say $y > z$, and let $k = y - z > 0$. Then for all $i \in \mathbb{Z}$, $g^{ki} = g^k * g^k * \cdots * g^k$ (i times), which equals $e * e * \cdots * e = e$. Similarly, $g^{ki+r} = g^r$. If $x \equiv r \pmod{k}$, then $g^x = g^r$, giving only k different images, a contradiction. So σ is one-to-one, finishing the infinite case. See Exercise 2.1.15 for the finite case. □

To show that an isomorphism exists, we need a suitable bijection, but there can be lots of potential bijections. Theorem 2.1.2 provides some guidance as well as telling us some of the algebraic properties preserved under isomorphism.

Theorem 2.1.2. *Suppose $\sigma : (A, *) \to (B, \circledast)$ is an isomorphism.*

(i) *If e_A is the identity for A, then $\sigma(e_A)$ is the identity for B.*

(ii) *If $a \in A$ has an inverse, then $\sigma(a)$ has an inverse in B, which is $\sigma(a)^{-1} = \sigma(a^{-1})$.*

(iii) *If $*$ is associative, so is $\circledast$.*

(iv) *Suppose $*$ is associative. For all $a \in A$ and all $n \in \mathbb{N}$, $\sigma(a^n) = (\sigma(a))^n$.*

(v) *If $*$ is commutative, so is $\circledast$.*

(vi) *If $(A, *)$ is a group, so is $(B, \circledast)$.*

(vii) *If g generates the group $(A, *)$, then $\sigma(g)$ generates $(B, \circledast)$.*

Proof. We prove parts (i) and (iv). See Exercise 2.1.16 for the rest. Let e_A be the identity of A. We show that $\sigma(e_A)$ is the identity. Let b be any element of B. Since σ is a bijection, there is some $a \in A$ with $\sigma(a) = b$. Then $b = \sigma(a) = \sigma(a * e_A) = \sigma(a) \circledast \sigma(e_A) = b \circledast \sigma(e_A)$. Similarly, $\sigma(e_A) \circledast b = b$. From Lemma 1.2.1 $\sigma(e_A)$ is the identity of B.

We use induction to prove part (iv). When $n = 1$ we have $\sigma(a^1) = \sigma(a) = (\sigma(a))^1$. Suppose that $\sigma(a^n) = (\sigma(a))^n$. Then $\sigma(a^{n+1}) = \sigma(a^n \cdot a) = \sigma(a^n)\sigma(a) = (\sigma(a))^n\sigma(a) = (\sigma(a))^{n+1}$. □

Isomorphisms for Two Operations. The concept of an isomorphism extends readily from systems with one operation to systems with two, in which case Theorem 2.1.2 applies to both operations.

Definition (Isomorphism). Two systems $(A, +, \cdot)$ and $(B, \oplus, \odot)$ are *isomorphic* if and only if there is a bijection $\sigma : A \to B$ so that for all $x, y \in A$, $\sigma(x + y) = \sigma(x) \oplus \sigma(y)$ and $\sigma(x \cdot y) = \sigma(x) \odot \sigma(y)$.

Example 5. Let $B = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$, a subset of $M_2(\mathbb{R})$ with rational entries, and let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, a subset of the real numbers. We leave to Exercise 2.1.13 the verification that these systems are fields—the first with matrix addition and multiplication and the second with ordinary addition and multiplication. The use of a and b in the definitions of these sets suggests $\beta : B \to \mathbb{Q}(\sqrt{2})$ given by

$\beta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right) = a + b\sqrt{2}$ as a natural choice for an isomorphism. By Exercise 2.1.13 β is a bijection. For $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}, \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} \in B$,

$$\begin{aligned}\beta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right) &= \beta\left(\begin{bmatrix} a+c & 2(b+d) \\ b+d & a+c \end{bmatrix}\right) \\ &= (a+c) + (b+d)\sqrt{2}) = (a + b\sqrt{2}) + (c + d\sqrt{2}) \\ &= \beta\left(\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\right) + \beta\left(\begin{bmatrix} c & 2d \\ d & c \end{bmatrix}\right),\end{aligned}$$

so β preserves addition.

For multiplication, note that $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & 2ad+2bc \\ bc+ad & 2bd+ac \end{bmatrix}$. Similarly, $(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$. Thus the forms of the products in $\mathbb{Q}(\sqrt{2})$ and B match, so β preserves multiplication as well. Exercise 2.1.20 generalizes the curious ability of the factor of 2 in the matrix to mimic the $\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. ◊

Theorem 2.1.3. *Suppose $\sigma : (A, +, \cdot) \to (B, \oplus, \odot)$ is an isomorphism.*

(i) *If 1_A is a unity of A, then $\sigma(1_A)$ is a unity of B.*

(ii) *If $\cdot$ distributes over $+$, then $\odot$ distributes over $\oplus$. That is,*

$$\sigma(a\cdot(b+c)) = \sigma(a)\odot(\sigma(b)\oplus\sigma(c)) \quad \textit{and similarly for} \quad (b+c)\cdot a.$$

(iii) *If $(A, +, \cdot)$ is a ring, so is $(B, \oplus, \odot)$.*

(iv) *If $(A, +, \cdot)$ is a field, so is $(B, \oplus, \odot)$.*

Proof. See Exercise 2.1.17. □

Example 6. Let $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$. Define $\gamma : \mathbb{Z} \to 2\mathbb{Z}$ by $\gamma(x) = 2x$, which satisfies the definition of a function. Further, every even number is twice an integer, so γ is onto. For one-to-one, let $x, y \in \mathbb{Z}$, and suppose $\gamma(x) = \gamma(y)$. Then $2x = 2y$ and by cancellation $x = y$. Finally $\gamma(x+y) = 2(x+y) = 2x+2y = \gamma(x)+\gamma(y)$. Thus γ is an isomorphism for addition in both systems. This last string of equalities points out the important connection between isomorphism and distributivity of multiplication over addition. However, $\gamma(xy) = 2xy \neq 4xy = (2x)(2y) = \gamma(x)\gamma(y)$. So this mapping isn't a ring isomorphism. While this choice failed, perhaps another bijection among the infinitely many possibilities could succeed. However, no bijection can work, as we'll see in the next subsection. ◊

Nonisomorphic Systems. How can we determine when two systems fail to be isomorphic? If they have different numbers of elements, no bijection exists between them, let alone one preserving the structure. But for systems with the same number of elements (or for infinite sets, the same cardinality), we don't want to look at every possible bijection. Instead, as in the continuation of Examples 6 and 7, we find some structural difference making an isomorphism impossible. Theorems 2.1.2 and 2.1.3 provide several structural properties we can use.

Example 6 (Continued). While $\mathbb{Z}$ has 1 as the unity, $2\mathbb{Z}$ has no unity: A purported unity $2x$ in $2\mathbb{Z}$ would, for all $2y$, satisfy $(2x)(2y) = 2y$. But $(2x)(2y) = 4xy$. For $2y = 4xy$ to hold, either $2y = 0$ (instead of $2y$ being any element of $2\mathbb{Z}$) or we can cancel to get $2x = 1$ or $x = \frac{1}{2}$ (which is not in $2\mathbb{Z}$). By Theorem 2.1.3(i) these systems can't be isomorphic. ◊

Example 7. $(\mathbb{Z}_6, +_6)$ and $\mathbf{D}_3$ both have six elements, but they differ on at least two algebraic properties and so are not isomorphic. First $\mathbb{Z}_6$ is commutative, whereas from Table 1.5 $M_1 \circ R \neq R \circ M_1$, violating Theorem 2.1.2(v). Thus, no bijection can preserve the operation. In addition, we know that the identity and the three mirror reflections of $\mathbf{D}_3$ are their own inverses by Exercise 1.3.5(d). So by Theorem 2.1.2(ii) they must all map to elements in $\mathbb{Z}_6$ that are their own inverses. However, in $\mathbb{Z}_6$ only 0 and 3 are their own inverses, and a bijection can't map four elements to two. Again, this prohibits any isomorphism. ◊

Different operations can make it difficult to see connections even among familiar systems. The invention of logarithms four hundred years ago required great insight because addition and multiplication of specific numbers look so different. However, the modern notation of exponents and a structural orientation make the formal relationship of Example 2 clear and easy to prove. In the same way, Theorem 2.1.1 allows us to reduce the variety of cyclic groups, such as the nth roots of unity in Example 4, to $\mathbb{Z}$ and $\mathbb{Z}_n$, the easiest ones to understand. The focus on structure makes connections more transparent.

Exercises

2.1.1. (a) ⋆ Define $\mu : \mathbb{Z} \to \mathbb{Z}$ by $\mu(x) = -x$. Prove that μ is an isomorphism for addition.

(b) ⋆ Give an example to show that μ in part (a) is not an isomorphism for multiplication.

(c) Is $\delta : \mathbb{Z} \to \mathbb{Z}$ given by $\delta(x) = 3x$ an isomorphism for addition? If so, prove it; if not, show why not.

(d) Repeat part (c) for $\delta : \mathbb{Q} \to \mathbb{Q}$ given by $\delta(x) = 3x$.

(e) For parts (c) and (d), if δ is an isomorphism for addition, is it an isomorphism for multiplication? Prove your answer.

2.1.2. (a) Show that $\beta : \mathbb{R} \to \mathbb{R}^+$ given by $\beta(x) = 2^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \cdot)$.

(b) For all $k > 0$, show that $\gamma : \mathbb{R} \to \mathbb{R}^+$ given by $\gamma(x) = k^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \cdot)$.

(c) What is the inverse function of γ?

2.1.3. Let $\mathbb{Z}[i] = \{ a + bi : a, b \in \mathbb{Z} \}$ (the *Gaussian integers*), and let $W = \{ a + bx : a, b \in \mathbb{Z} \}$, the first-degree polynomials with integer coefficients. Prove that $\alpha : \mathbb{Z}[i] \to W$ given by $\alpha(a + bi) = a + bx$ is an isomorphism for addition but not for multiplication.

2.1.4. ⋆ Show that $\mathbb{C} = \{ x + yi : x, y \in \mathbb{R} \}$, the field of complex numbers, is isomorphic to $J = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ with matrix addition and multiplication.

2.1.5. (a) Is $\kappa : \mathbb{C} \to \mathbb{C}$ given by $\kappa(x + yi) = x - yi$ an isomorphism for addition? If so, prove it; if not, give a counterexample.

(b) Repeat part (a) for multiplication.

(c) Repeat part (a) for $\theta : \mathbb{C} \to \mathbb{C}$ given by $\theta(x + yi) = y + xi$.

(d) Repeat part (c) for multiplication.

(e) Repeat part (a) for $\nu : \mathbb{C} \to \mathbb{C}$ given by $\nu(x + yi) = -x + yi$.

(f) Repeat part (e) for multiplication.

2.1.6. On $\mathbb{R}[x]$, the ring of polynomials with real coefficients, define $\delta(g) = g'$, the derivative of g. Determine whether δ is an isomorphism for addition or multiplication.

2.1.7. Is the mapping $\tau : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ given by $\tau(M) = M^T$, its transpose, an isomorphism for matrix addition? If so, prove it; if not provide a counterexample. Repeat for matrix multiplication.

2.1.8. (a) Let q be any nonzero rational number. Prove that $\xi(x) = qx$ is an isomorphism from $(\mathbb{Q}, +)$ to itself, but is an isomorphism for $(\mathbb{Q}, +, \cdot)$ if and only if $q = 1$. *Hint.* What is special about 1?

(b) Repeat part (a) for any field $(F, +, \cdot)$. *Hint.* See Exercise 1.2.29.

2.1.9. (a) Find a subset B of the rationals and a function $\gamma : \mathbb{Z} \to B$ so that $(\mathbb{Z}, +)$ is isomorphic to $(B, \cdot)$.

(b) Explain why, unlike Example 2, there can be no isomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{Q}^+, \cdot)$.

2.1.10. (a) ⋆ Let $3\mathbb{Z}_{12} = \{0, 3, 6, 9\}$. Find an isomorphism from $(\mathbb{Z}_4, +_4, \cdot_4)$ to $(3\mathbb{Z}_{12}, +_{12}, \cdot_{12})$. Prove your answer.

(b) Define $2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$. Repeat part (a) for $(\mathbb{Z}_5, +_5, \cdot_5)$ and $(2\mathbb{Z}_{10}, +_{10}, \cdot_{10})$.

(c) Find and prove an isomorphism from $(\mathbb{Z}_2, +_2)$ to $(\{I, M_k\}, \circ)$, where M_k is any mirror reflection in $\mathbf{D}_n$.

2.1.11. From Exercise 1.3.4 $\mathbf{D}_2$ is a group with four elements. Is it isomorphic to $(\mathbb{Z}_4, +_4)$? Prove your answer.

2.1.12. (a) Let $\gamma : \mathbb{R}^3 \to \mathbb{R}^3$ be given by $\gamma\big((a, b, c)\big) = (a + b, b, a - c)$. Prove that γ is an isomorphism of the vector space $\mathbb{R}^3$ to itself considered as the group $(\mathbb{R}^3, +)$.

(b) Find a 3×3 matrix M so that multiplication of M times the column vector (a, b, c) gives $\gamma\big((a, b, c)\big)$. What linear algebra property or properties of M corresponds to γ being an isomorphism?

(c) Let $\delta : \mathbb{R}^3 \to \mathbb{R}^3$ be given by $\delta\big((a, b, c)\big) = (a + b, b + c, -a + c)$. Prove that δ is not an isomorphism of the group $(\mathbb{R}^3, +)$.

(d) ⋆ Express δ as a 3×3 matrix. Relate your answer in part (c) to linear algebra properties.

(e) Can we use linear algebra to define an isomorphism from the group $(\mathbb{R}^3, +)$ to the group $(\mathbb{R}^2, +)$? If so, give a linear transformation (matrix) and prove that it is an isomorphism. If not, use linear algebra properties to prove that no such linear transformation can exist. *Remark.* There are isomorphisms between $(\mathbb{R}^3, +)$ and $(\mathbb{R}^2, +)$ involving advanced set theory.

2.1.13. (a) Show that β in Example 5 is a bijection. Assume that $\sqrt{2} \notin \mathbb{Q}$, a fact proven in Exercise 3.1.23.

(b) Show that the systems in Example 5 are, indeed, fields.

2.1.14. On $(X, \oplus)$, define z to be the *average* of x and y if and only if $x \oplus y = z \oplus z$.

(a) Suppose every two elements in X have an average. If $\sigma : X \to Y$ is an isomorphism from $(X, \oplus)$ to $(Y, *)$, prove that every two elements of Y have an average.

(b) Every two elements x and y of $(\mathbb{R}, +)$ has an average $\frac{x+y}{2}$, called their *arithmetic mean.* Using the isomorphism of Example 2, find a formula for the corresponding average of two elements in $(\mathbb{R}^+, \cdot)$, called their *geometric mean.*

(c) In $\mathbf{C}_3$ verify that every two rotations have an average.

(d) In $\mathbf{C}_4$ find two rotations that don't have an average.

(e) Determine for which n every pair of elements of $(\mathbb{Z}_n, +)$ have an average. Prove your answer.

(f) In $\mathbf{D}_3$ does every pair of symmetries have an average?

2.1.15. Finish the proof of Theorem 2.1.1 by showing that a cyclic group with n elements is isomorphic to $\mathbb{Z}_n$.

2.1.16. Finish the proof of Theorem 2.1.2.

2.1.17. Prove Theorem 2.1.3.

2.1.18. Prove that isomorphism has the three properties of an equivalence relation:

(a) (Reflexive) For any system, $(A, *) \approx (A, *)$.

(b) (Symmetric) For any two systems, if $(A, *) \approx (B, \circledast)$, then $(B, \circledast) \approx (A, *)$.

(c) (Transitive) For any three systems, if $(A, *) \approx (B, \circledast)$ and $(B, \circledast) \approx (C, \odot)$, then $(A, *) \approx (C, \odot)$.

2.1.19. (a) $\star$ Show that $([0,1], M)$ is isomorphic to $([0,1], m)$, where aMb is the maximum of a and b and amb is their minimum. *Hint.* Separate the cases $a < b$ and $a \geq b$.

(b) Let ${}_{12}D = \{1, 2, 3, 4, 6, 12\}$ be the divisors of 12, let $\gcd(a, b)$ be the greatest common divisor of a and b, and let $\operatorname{lcm}(a, b)$ be the least common multiple of a and b. Verify that gcd and lcm are operations on ${}_{12}D$ and find an isomorphism between $({}_{12}D, \gcd)$ and $({}_{12}D, \operatorname{lcm})$.

(c) Let $\mathcal{P}(X)$ be the set of all subsets of a set X, let $\bigcap$ be the operation of intersection, and let $\bigcup$ be the operation of union. Show that $(\mathcal{P}(X), \bigcap)$ and $(\mathcal{P}(X), \bigcup)$ are isomorphic. *Hint.* What is the identity of $\bigcap$? Of $\bigcup$? How can we relate these identities?

Remark. The algebraic systems in this exercise are examples of lattices, studied in Section 7.1.

2.1.20. (a) Let $k \in \mathbb{N}$ be a prime and define $\mathbb{Q}(\sqrt{k}) = \{a + b\sqrt{k} : a, b \in \mathbb{Q}\}$ and $B_k = \left\{ \begin{bmatrix} a & kb \\ b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$. For $\beta : B_k \to \mathbb{Q}(\sqrt{k})$ given by $\beta\left(\begin{bmatrix} a & kb \\ b & a \end{bmatrix}\right) = a + b\sqrt{k}$, determine whether β preserves addition and multiplication, similarly to Example 5. Prove your answers.

(b) What happens to the mapping in part (a) when $k = 1$? What other values of k cause β to fail to be an isomorphism? What is $\mathbb{Q}(\sqrt{k})$ for these k?

(c) For what values of k is $\mathbb{Q}(\sqrt{k})$ a field? Explain your answer.

(d) Verify for all $k \in \mathbb{Q}$ that B_k is a ring. When is B_k a field?

(e) For $k = 4$ explain why we can't define $\rho : \mathbb{Q}(\sqrt{4}) \to B_4$ by $\rho(a + b\sqrt{4}) = \begin{bmatrix} a & 4b \\ b & a \end{bmatrix}$.

2.1.21. An isomorphism from a group (or ring or field) to itself is called an *automorphism*. (For instance, μ in Exercise 2.1.1, $\varkappa$ in Exercise 2.1.5, and ξ in Exercise 2.1.8 are automorphisms.)

(a) Show that $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ given by $\sigma(x, y) = (x + 2y, y)$ is an automorphism of the vector space $\mathbb{R}^2$ as a group with addition.

(b) Is the function ρ mapping the 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to $\begin{bmatrix} d & c \\ b & a \end{bmatrix}$ an isomorphism for addition? Multiplication? Prove your answers.

(c) For all $n \in \mathbb{N}$ prove that $\lambda : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\lambda(x) = \begin{cases} n - x & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$ is a group automorphism, but when $n > 2$, it is not a ring automorphism.

(d) For which $k \in \mathbb{Z}_5$ is $\rho_k : \mathbb{Z}_5 \to \mathbb{Z}_5$ given by $\rho_k(x) = k \cdot_5 x$ a group automorphism?

(e) Repeat part (d) for $\mathbb{Z}_n$, for other values of n besides 5. Make a conjecture about which values of k give group automorphisms related to n.

2.1.22. Define an unusual addition $\oplus$ and multiplication $\odot$ on $\mathbb{Z}$ by $x \oplus y = x + y - 2$ and $x \odot y = xy - 2x - 2y + 6$.

(a) Verify that 2 is the additive identity for $\oplus$.

(b) ⋆ Find the additive inverse of x for $\oplus$.

(c) ⋆ Find the multiplicative unity for $\odot$.

(d) Prove that $(\mathbb{Z}, +, \cdot)$ with the usual operations is isomorphic to $(\mathbb{Z}, \oplus, \odot)$.

(e) Verify that $\mathbb{Z}$ is a ring with $\oplus$ and $\odot$.

2.1.23. Use the fact that $\alpha : \mathbb{Z} \to \mathbb{Z}$ given by $\alpha(x) = x + s$ is a bijection, where s is an integer, to define operations $\oplus$ and $\odot$ so that α is an isomorphism from $(\mathbb{Z}, +, \cdot)$ to $(\mathbb{Z}, \oplus, \odot)$. *Hint.* This exercise generalizes Exercise 2.1.22.

2.1.24. In the field of real numbers we can define "order" algebraically as follows: For $a \in \mathbb{R}$, $0 \leq a$ if and only if there is some $b \in \mathbb{R}$ such that $b^2 = a$ and $x \leq y$ if and only if $0 \leq y - x$.

(a) ⋆ Prove that if $\phi : \mathbb{R} \to \mathbb{R}$ is an isomorphism for addition and multiplication and $x \leq y$, then $\phi(x) \leq \phi(y)$.

(b) ⋆ Prove for any $x, y, z \in \mathbb{R}$ that if $x \leq y$, then $x + z \leq y + z$.

(c) Prove for any $x, y, z \in \mathbb{R}$ that if $x \leq y$ and $0 \leq z$, then $xz \leq yz$.

(d) Prove for any $x, y, z \in \mathbb{R}$ that if $x \leq y$ and $z \leq 0$, then $yz \leq xz$.

(e) Explain why the definition of order above won't completely order all of the rationals.

(f) Explain what goes wrong with the definition of order above for the complexes.

Remark. Exercises 3.2.28–3.2.30 investigate partial orders on groups and rings.

2.2 Elements and Subsets

Elements of algebraic systems often differ structurally from one another. We have already studied the special elements of identities and unities in groups and rings. Other elements can differ structurally from one another. Also some subsets of these elements form algebraically important sets, again based on their structure. With our understanding of isomorphism, structural differences and similarities matter in algebra, not the notation. To simplify notation from now on for general groups we will write the product $a * b$ more simply as the juxtaposition ab. We will similarly use juxtaposition for multiplication in a general ring, but we'll continue to write $a + b$ for addition. Also, for the rings $\mathbb{Z}_n$ we will generally no longer write the subscripts for the operations, writing $a + bc$ rather than the more cumbersome $a +_n b \cdot_n c$.

Order.

Definition (Order of an element)**.** The *order* of an element g of a group G is the smallest positive integer n so that $g^n = e$, the identity. We write $|g| = n$. If no such n exists, we say g has infinite order. If G is a ring, the *order* n of an element g refers to the additive operation, in which case $ng = 0$.

Definition (Cyclic subgroup)**.** We write $\langle g \rangle = \{ g^z : z \in \mathbb{Z} \}$, the subset (*subgroup*) *generated* by g. If the operation of G is addition, $g^n = e$ becomes $ng = 0$.

Definition (Order of a set)**.** Denote the number of elements of a finite set X by $|X|$, which we call the *order* of X.

Example 1. Table 2.1 gives the order of each element in the group $(\mathbb{Z}_{12}, +)$. The four elements with order 12, namely 1, 5, 7, and 11, generate all twelve elements of this cyclic group. Repeated addition of other elements generate subsets. Thus multiples of 2 and 10, which is the additive inverse of 2, give the even numbers: $\langle 2 \rangle = \langle 10 \rangle = \{2, 4, 6, 8, 10, 0\}$. The order of both 2 and 10 is 6 in $\mathbb{Z}_{12}$. Similarly, $\langle 3 \rangle = \langle 9 \rangle = \{3, 6, 9, 0\}$, $\langle 4 \rangle = \langle 8 \rangle = \{4, 8, 0\}$, $\langle 6 \rangle = \{6, 0\}$, and $\langle 0 \rangle = \{0\}$. Again, the order of each element matches the size of the subset of elements it generates. These subsets inherit the structure of the entire group and are examples of what we will shortly call subgroups. (The same analysis applies if we think of $\mathbb{Z}_{12}$ as a ring.) ◊

The orders of elements don't tell us everything about a group, but they give us valuable information and give us a feel for the group. We summarize this information

Table 2.1. The orders of elements in $\mathbb{Z}_{12}$.

Element	0	1	2	3	4	5	6	7	8	9	10	11
Order	1	12	6	4	3	12	2	12	3	4	6	12

Table 2.2. Table of orders for $\mathbb{Z}_{12}$.

order	1	2	3	4	6	12
number	1	1	2	2	2	4

Table 2.3. Table of orders for $\mathbf{D}_6$.

order	1	2	3	6
number	1	7	2	2

in a *table of orders*, illustrated in Table 2.2 for $\mathbb{Z}_{12}$ and in Table 2.3 for $\mathbf{D}_6$. Table 2.2 is derived from Table 2.1. The differences in Tables 2.2 and 2.3 indicate the groups are not isomorphic. Of course we could easily distinguish these groups without knowing the orders of elements, but the orders give us deeper understanding. The orders of elements of isomorphic groups match, as Theorem 2.2.1 states. (There are nonisomorphic groups with the same table of orders. See Exercise 3.3.14.)

Theorem 2.2.1. *Suppose $\sigma : G \to H$ is an isomorphism and $g \in G$. Then g and $\sigma(g)$ have the same order. That is, $|g| = |\sigma(g)|$.*

Proof. See Exercise 2.2.10. □

Example 2. In the familiar infinite groups under addition, such as $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, only the identity 0 has a finite order of 1. All the other elements have infinite order. The nonzero complex numbers under multiplication form a group with elements of every finite order. From Example 3 of Section 2.1, the nth roots of unity form a group isomorphic to $\mathbb{Z}_n$ and so all have finite order. For instance $e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ has order n. These complex roots of unity are the only elements of finite order in the nonzero complex numbers under multiplication. ◊

Subgroups, Subrings, and Subfields. Some subsets of algebraic systems are closed under the operations and so can form algebraic systems with properties inherited from the bigger set. In general, a subset is any collection without structure, and algebra focuses on structure. Thus subgroups (or subrings or subfields) need to be groups (or rings or fields) as well as subsets.

Definitions (Subgroup. Subring. Subfield)**.** A nonempty subset H of a group G is a *subgroup* of G if and only if H is a group using the same operation as G. If both G and H are rings with the same operations, H is a *subring* of G, and if both are fields, H is a *subfield* of G.

Example 1 (Continued)**.** The subsets $\langle k\rangle$ in the first part of Example 1 are not only subgroups, they are subrings of $\mathbb{Z}_{12}$. The additions in Tables 2.4, 2.5, and 2.6 should look familiar—these tables give groups isomorphic to cyclic groups. However, the multiplications can bring surprises. As Table 2.4 illustrates $(\langle 4\rangle, +, \cdot)$ is a field with unity 4,

Table 2.4. Cayley tables for $(\{0,4,8\},+,\cdot)$

$+_{12}$	0	4	8
0	0	4	8
4	4	8	0
8	8	0	4

$\cdot_{12}$	0	4	8
0	0	0	0
4	0	4	8
8	0	8	4

Table 2.5. Cayley tables for $(\{0,3,6,9\},+,\cdot)$

$+_{12}$	0	3	6	9
0	0	3	6	9
3	3	6	9	0
6	6	9	0	3
9	9	0	3	6

$\cdot_{12}$	0	3	6	9
0	0	0	0	0
3	0	9	6	3
6	0	6	0	6
9	0	3	6	9

Table 2.6. Cayley tables for $(\{0,2,4,6,8,10\},+,\cdot)$

$+_{12}$	0	2	4	6	8	10
0	0	2	4	6	8	10
2	2	4	6	8	10	0
4	4	6	8	10	0	2
6	6	8	10	0	2	4
8	8	10	0	2	4	6
10	10	0	2	4	6	8

$\cdot_{12}$	0	2	4	6	8	10
0	0	0	0	0	0	0
2	0	4	8	0	4	8
4	0	8	4	0	8	4
6	0	0	0	0	0	0
8	0	4	8	0	4	8
10	0	8	4	0	8	4

even though $\mathbb{Z}_{12}$, which is not a field, has 1 as its unity. So $\langle 4\rangle$ is a subring, but not a subfield of $\mathbb{Z}_{12}$. Also, $\langle 3\rangle$ is a subring of $\mathbb{Z}_{12}$ and, from Table 2.5, it has 9 as its unity. From Table 2.6 the subring $\langle 2\rangle$ of $\mathbb{Z}_{12}$ has no unity at all. Perhaps curiously only half of the elements of $\langle 2\rangle$ appear as products. ◊

Example 3. The field $(\mathbb{R},+,\cdot)$ of reals has a range of types of subsets. The subset of natural numbers $\mathbb{N}$ is closed under addition and multiplication, but doesn't form a subgroup, a subring, or a subfield of $\mathbb{R}$. The subset $\frac{1}{2}\mathbb{Z} = \{\, \frac{z}{2} : z \in \mathbb{Z}\,\}$ is a subgroup of $\mathbb{R}$ under addition. Since, for instance, $\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$, it is not closed under multiplication, so it is not a subring, let alone a subfield of $\mathbb{R}$. The integers $(\mathbb{Z},+,\cdot)$ form a subring and so a subgroup (under just addition), but not a subfield of $\mathbb{R}$. The rationals $(\mathbb{Q},+,\cdot)$ are a subfield and thus a subring and a subgroup of $\mathbb{R}$. The subset of positive rationals $\mathbb{Q}^+$ is a subgroup of $\mathbb{R}^+$ under multiplication, but is not a subgroup of $\mathbb{R}$ since their operations differ. ◊

Theorem 2.2.2. *Let g be an element of a group G. Then $\langle g\rangle$ is a subgroup of G and if g has order $|g| = n$, then $\langle g\rangle$ is isomorphic to $\mathbb{Z}_n$. If g has infinite order, $\langle g\rangle$ is isomorphic to $\mathbb{Z}$.*

Proof. Since $g \in \langle g\rangle$ and all g^z are in G, $\langle g\rangle$ is a nonempty subset of G. Further, for $g^x, g^y \in \langle g\rangle$, $g^x g^y = g^{x+y} \in \langle g\rangle$, showing that $\langle g\rangle$ is closed. Similarly, $g^0 = e$ and $g^{-z} = (g^z)^{-1}$ are in $\langle g\rangle$, showing that it has an identity and inverses. Since the operation is associative for all of G, it also is for any subset. Thus $\langle g\rangle$ is a subgroup of G. Suppose

$|g| = n$. Then $g^n = e$, so for all $q, r \in \mathbb{Z}$ with $0 \le r < n$, $g^{qn+r} = (g^n)^q g^r = eg^r = g^r$. So $\langle g \rangle$ has at most n different elements g^r with $0 \le r < n$. The additional condition of n being the smallest positive integer giving us the identity will force all of the g^r to be different, for suppose $0 \le p \le r < n$ and $g^p = g^r$. Then $e = g^{p-p} = g^{r-p}$. The only exponent $r - p$ with $0 \le r - p < n$ giving the identity is $r - p = 0$. Since $\langle g \rangle$ has n elements and is, by definition, cyclic, $\langle g \rangle \approx \mathbb{Z}_n$ by Theorem 2.1.1. Similarly if g has infinite order, different powers $z \ne x$ give $g^z \ne g^x$. Thus $\langle g \rangle$ is infinite and cyclic, and so isomorphic to $\mathbb{Z}$. □

In Example 1, $\frac{1}{2}\mathbb{Z}$ is the subgroup of $\mathbb{R}$ generated by $\frac{1}{2}$, but isn't a subring. So we can't extend Theorem 2.2.2 to rings and subrings.

Example 4. Not every subgroup is cyclic. That is, some subgroups are not generated by a single element. Consider in $\mathbf{D}_4$ the subgroup $\{I, R^2, M_1, M_3\}$. (See Table 1.6.) Here any element generates only itself and the identity. (This example deserves a caution: The seemingly similar subset $\{I, R^2, M_1, M_4\}$ is not a subgroup because $M_1 \circ M_4 = R$, which is not in the subset.) ◊

Exercise 2.2.1. ⋆ In $\mathbb{Z}_{10}$, write out the Cayley table for $\{2, 4, 6, 8\}$ with $\cdot_{10}$. Verify this forms a group with identity 6. Explain why it is not a subgroup of $\mathbb{Z}_{10}$.

Example 3 and Exercise 2.2.1 suggest the need for explicit criteria to prove a subset is a subgroup. As in Theorem 2.2.2, we never need to worry about associativity. Here is a complete list of things to verify: subset, same operation, nonempty, identity, inverses, and closure. The first two are usually immediate from the given information and you may simply note them. The identity element is generally the easiest element to verify is in the subset and immediately guarantees nonempty, so we can ignore nonempty. It might seem that we could dispense with both nonempty and identity by showing closure and inverses since $gg^{-1} = e$. However, the empty set satisfies closure and inverses "vacuously" since both of these properties start out "for all…" and so are true for the empty set.

Subgroup Test. To show H is a subgroup of a group G, verify

(i) H is a subset of G,

(ii) H has the same operation as G,

(iii) H has the identity of G,

(iv) H is closed under the operation of G, and

(v) all elements of H have inverses in H.

If G is a finite group, we can eliminate the last step: Consider the powers g, g^2, g^3, …. With only finitely many elements in G, the list repeats at some point, say $g^z = g^x$. Then $g^{z-x} = e$ and so g^{z-x-1} is the inverse of g.

When a group is nonabelian, it is noticeably harder to understand how its elements relate to each other. It helps to start with the part of the group where we do have commutativity, called the *center* of the group. (The German word for center starts with a "z," so we call the center $Z(G)$.)

Definition (Center of a group). The *center* of a group $(G, *)$ is $Z(G) = \{a \in G : \text{for all } g \in G, a * g = g * a\}$.

Example 5. If G is abelian, $Z(G) = G$. From Tables 1.5 and 1.6 the center of $\mathbf{D}_3$ is $Z(\mathbf{D}_3) = \{I\}$ and the center of $\mathbf{D}_4$ is $Z(\mathbf{D}_4) = \{I, R^2\}$. ◊

Example 6. The center of $\mathrm{GL}_n(\mathbb{R})$, the group of $n \times n$ invertible matrices contains only scalar multiples of the identity matrix, rI. (See Exercise 2.S.7.) ◊

The center of a group contains the elements most easily understood. It will reappear several times in later chapters.

Theorem 2.2.3. *The center of a group is a subgroup.*

Proof. See Exercise 2.2.17. □

Subring Test. To show T is a subring of a ring $(S, +, \cdot)$, verify

(i) $(T, +)$ is a subgroup of S and

(ii) T is closed under $\cdot$.

Exercise 2.2.2. ⋆ Explain why the two conditions of the subring test suffice to show that T is a subring. Determine what extra condition(s) is/are needed for a subfield test.

Relations of Subgroups and Subrings. The interrelations of the subgroups of groups and subrings of rings help us understand finite systems more deeply. We describe informally a figure, called a *Hasse diagram*, that enables us to see these relationships visually. The left Hasse diagram of Figure 2.2 illustrates how the six subrings (or subgroups) of $\mathbb{Z}_{12}$ from Example 1 relate. One of them, say A, is a subring of another, B, if and only if we can follow segments from A to B without ever going down. Similarly the Hasse diagram on the right relates the positive divisors of 12, where A is a divisor of B provided we can follow segments from A to B without ever going down. The collection of subrings of a ring (and similarly for groups or fields or divisors of a positive integer) forms an algebraic structure called a *lattice*, introduced in Exercises 2.2.26–2.2.28 and investigated in Section 7.1.

The lattices in Figure 2.2 suggest several questions: First, $\langle 4\rangle$ is a subring of $\langle 2\rangle$, which is a subring of $\langle 1\rangle$. Does this generalize to, “If A is a subring of B and B is a

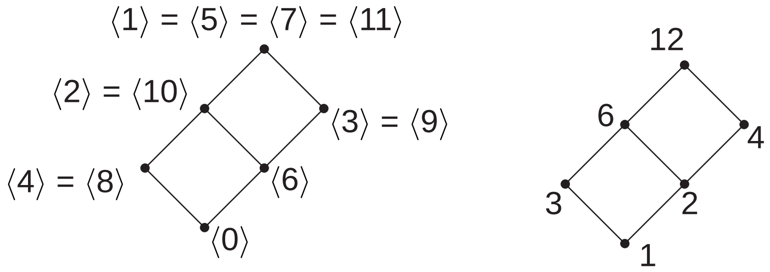

Figure 2.2. Subring (or subgroup) lattice of $\mathbb{Z}_{12}$ and lattice of divisors of 12.

subring of C, then is A a subring of C?" Next, the intersection of $\langle 2\rangle$ and $\langle 3\rangle$ is $\langle 6\rangle$. More generally, is the intersection of subrings always a subring? What about the union of two subrings or subgroups? Is there a relation between the numbers generating the same subring? Does the apparent isomorphism between the lattices in Figure 2.2 hold more generally? We answer some of these questions here and explore others in the exercises. To prove the isomorphism between the lattice of subrings of $\mathbb{Z}_n$ and the lattice of divisors of n requires a deeper investigation of number theory and cyclic groups; this is undertaken in Section 3.1.

Theorem 2.2.4. *The intersection of two subgroups is a subgroup.*

Proof. Let H and K be subgroups of a group G. By definition, they and $H \cap K$ use the same operation as G. Also $H \cap K$ is a subset of G and since e is in H and in K it is in $H \cap K$. Let $a, b \in H \cap K$. Then $a, b \in H$ and since H is a subgroup, ab and a^{-1} are in H. Similarly $ab, a^{-1} \in K$. So $ab, a^{-1} \in H \cap K$, showing $H \cap K$ has closure and inverses. By the subgroup test, $H \cap K$ is a subgroup of G. □

Theorem 2.2.5. *The intersection of two subrings is a subring.*

Proof. See Exercise 2.2.11. □

The lattice of subrings in Figure 2.2 depends on the algebraic structure. However, as Example 7 will illustrate, some concepts from number theory suffice to explain its connection with the lattice of divisors.

Definitions (Greatest common divisor. Least common multiple). For $a, b, d \in \mathbb{N}$, $\gcd(a, b) = d$, the *greatest common divisor* of a and b if and only if d divides a and d divides b and for all c dividing both a and b, $c \leq d$. For $a, b, m \in \mathbb{N}$, $\operatorname{lcm}(a, b) = m$, the *least common multiple* of a and b if and only if a divides m and b divides m and for all positive integers c for which both a and b divide c, $m \leq c$.

Example 7. The divisors of both 24 and 108 are 1, 2, 3, 4, 6, and 12. So $\gcd(24, 108) = 12$. Also, $24 = 2^3 \cdot 3$ and $108 = 2^2 \cdot 3^3$. When we factor 12 we get $12 = 2^2 \cdot 3$, which has both prime factors common to 24 and 108 and for each prime, its exponent is the lowest appearing in the factorizations of 24 and 108. There are infinitely many multiples common to both 24 and 108, all multiples of $\operatorname{lcm}(24, 108) = 216 = 2^3 \cdot 3^3$. For the least common multiple the exponent of each prime is the highest that appears in the factorization of 24 and 108. ◊

Both gcd and lcm are operations on $\mathbb{N}$. Even though the definition of a dividing b applies to negative integers, we can't extend lcm to negative integers since there is no least negative integer. For instance, all negative multiples of 216 are common multiples of 24 and 108. We can extend gcd to negative numbers, although the answer will always be positive by definition of greatest. However, gcd isn't an operation on all of $\mathbb{Z}$ because of one failure: $\gcd(0, 0)$ isn't defined since every number divides 0, and so there is no greatest common divisor of 0 with itself. For our work with cyclic groups we only need gcd and lcm on $\mathbb{N}$.

Example 8. Use gcd and lcm to relate lattices of the divisors of 12 and of the subgroups $\langle x\rangle$ of $\mathbb{Z}_{12}$ in Figure 2.2.

Solution. For the lattice of divisors, the smallest number in the lattice above or equal to a and b is $\operatorname{lcm}(a, b)$ and their gcd is the number below or equal to a and b. The subgroups are a bit trickier since many have more than one name. We see that $\gcd(1, 12) = 1 = \gcd(5, 12) = \gcd(7, 12) = \gcd(11, 12)$ and $\langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle$. Similarly, $\gcd(2, 12) = 2 = \gcd(10, 12)$ and $\langle 2\rangle = \langle 10\rangle$. Again, $\gcd(3, 12) = 3 = \gcd(9, 12)$ and $\langle 3\rangle = \langle 9\rangle$, while $\gcd(4, 12) = 4 = \gcd(8, 12)$ and $\langle 4\rangle = \langle 8\rangle$. If we consider 12 as another name for 0, we can rewrite $\langle 0\rangle$ as $\langle 12\rangle$. Then consider just the smallest representative from each subgroup: $\langle 1\rangle$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 4\rangle$, $\langle 6\rangle$, and $\langle 12\rangle$. This simplification confirms that the subgroup lattice basically flips the divisor lattice upside down. The intersection of two of the subgroups is related to the least common multiple. For instance, $\langle 2\rangle \cap \langle 3\rangle$ is $\langle \operatorname{lcm}(2, 3)\rangle = \langle 6\rangle$. $\diamondsuit$

Example 9. Compare the subgroup lattices of $\mathbb{Z}_6$ and $\mathbf{D}_3$.

Solution. Figure 2.3 gives the subgroup lattices of $\mathbb{Z}_6$ and $\mathbf{D}_3$. While $\mathbb{Z}_6$ has just one subgroup of each divisor of 6, the lattice for $\mathbf{D}_3$ is more complicated. When we investigate groups more deeply in Chapter 3 we will start with cyclic groups because of their simpler structure. However, already in Section 2.4 we'll see some ideas about subgroups and subrings that apply to all groups and rings. $\diamondsuit$

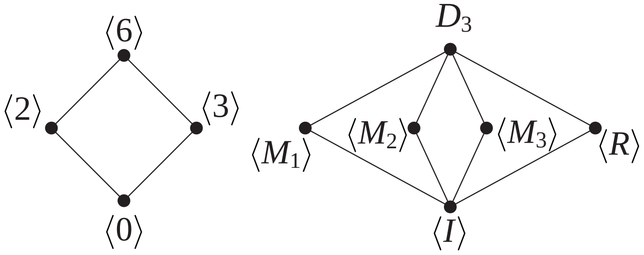

Figure 2.3. Subgroup lattice of $\mathbb{Z}_6$ and subgroup lattice of $\mathbf{D}_3$.

Exercises

2.2.3. Find the greatest common divisor and the least common multiple for these numbers.

(a) ⋆ 300 and 36.
(b) 33 and 35.
(c) 6, 10, and 15.
(d) 540, 600, and 2250.
(e) n and kn, for $1 \leq n$ and $1 \leq k$. Justify your answer.
(f) n and $n + 1$, for $1 < n$. Justify your answer.

2.2.4. (a) ⋆ Find the table of orders for $(\mathbb{Z}_5, +)$.
(b) ⋆ Repeat part (a) for $\mathbb{Z}_6$.
(c) Repeat part (a) for $\mathbb{Z}_7$.
(d) Repeat part (a) for $\mathbb{Z}_{12}$.

(e) Repeat part (a) for $\mathbb{Z}_{18}$.

(f) Make conjectures about the values in the table of orders for $\mathbb{Z}_n$. For instance, what are the possible orders, and how many elements of a given order are there?

2.2.5. (a) Find the table of orders for $\mathbf{D}_3$.

(b) ⋆ Repeat part (a) for $\mathbf{D}_4$.

(c) Repeat part (a) for $\mathbf{D}_5$.

(d) Repeat part (a) for $\mathbf{D}_6$.

(e) State how the table of orders for $\mathbf{D}_n$ relates to the table of orders for $\mathbb{Z}_n$, and prove your statement.

2.2.6. (a) Describe all subrings of $\mathbb{Z}_3$.

(b) Repeat part (a) for $\mathbb{Z}_4$.

(c) Repeat part (a) for $\mathbb{Z}_5$.

(d) Repeat part (a) for $\mathbb{Z}_6$.

(e) Make a conjecture about the subrings of $\mathbb{Z}_n$.

2.2.7. (a) Draw the Hasse diagram for the subring lattice for $\mathbb{Z}_4$.

(b) Repeat part (a) for $\mathbb{Z}_9$.

(c) Generalize parts (a) and (b) to $\mathbb{Z}_{p^2}$, where p is a prime.

(d) Repeat part (a) for $\mathbb{Z}_6$.

(e) Repeat part (a) for $\mathbb{Z}_{10}$.

(f) Generalize parts (d) and (e). *Hint.* How do 6 and 10 differ from p^2?

(g) Repeat part (a) for $\mathbb{Z}_8$.

(h) Repeat part (a) for $\mathbb{Z}_{27}$.

(i) Generalize parts (g) and (h).

(j) Generalize parts (c), (f), and (i).

2.2.8. (a) Draw the Hasse diagram for the subgroup lattice for $\mathbf{D}_2$.

(b) ⋆ Repeat part (a) for the ten subgroups $\mathbf{D}_4$. *Hint.* Two need two generators each.

(c) Repeat part (a) for the eight subgroups of $\mathbf{D}_5$.

(d) Make a conjecture about the subgroup lattice of $\mathbf{D}_p$ if p is a prime number. Justify your conjecture.

(e) Count the number of subgroups of $\mathbf{D}_6$, and classify them by what groups they are isomorphic to.

2.2.9. (a) Determine which of the subsets of $\mathbb{Z}[x]$ in Exercise 1.2.2 are subrings. For the others, show why they fail. Also, if they fail, determine whether they are subgroups.

(b) ⋆ For the set S of polynomials in $\mathbb{Z}[x]$ that are multiples of x^2, is S a subring? If not, is it a subgroup?

(c) Repeat part (b) for $\{\sum_{i=0}^{n} a_{2i}x^{2i} \,:\, a_{2i} \in \mathbb{Z}\}$ (just even powers of x).

(d) Polynomials of degree at most 3, together with 0.

(e) Polynomials of degree at least 3, together with 0.

2.2.10. (a) Prove Theorem 2.2.1.

(b) Prove that an element and its inverse in a group have the same order.

2.2.11. (a) Prove Theorem 2.2.5.

(b) Does part (a) extend to showing that the intersection of two subfields is a subfield? If so, prove it; if not, provide a counterexample.

(c) Suppose $\{H_i : i \in I\}$ is a finite or infinite collections of subgroups of a group G. Prove that $\bigcap_{i\in I} H_i$ is a subgroup of G.

(d) Extend part (c) to arbitrary collections of subrings and, if valid, to arbitrary collections of subfields.

(e) Suppose H is a subgroup of a group G and K is a subgroup of H. Prove K is a subgroup of G.

(f) Does part (e) extend to subrings and subfields? If so, prove it; if not, provide a counterexample.

2.2.12. Many designs, as in Figure 2.4, use two or more interchangeable colors to create more artistic interest. A *color preserving symmetry* of a design takes every region to a region of the same color. A *color switching symmetry* changes the colors of some regions and for every color A if some region of color A goes to color B, then every region of color A goes to color B. The *color group* of a design is the union of its color preserving and color switching symmetries.

(a) ⋆ Find the color preserving group for the first design in Figure 2.4.

(b) Repeat part (a) for the second and third designs in Figure 2.4.

(c) ⋆ Find the color group for the designs in Figure 2.4. (It is the same for all three designs.)

(d) Prove for any design that, indeed, the color group is a group and the color preserving symmetries form a subgroup of it.

(e) Do the color switching symmetries form a subgroup? If so, prove it; if not, state which properties of a group fail.

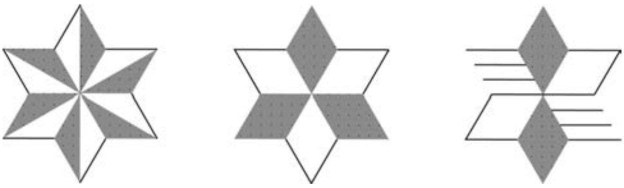

Figure 2.4. Designs with color symmetry.

2.2.13. Prove that the subsets of $\mathbb{Q}$ in parts (a) and (b) are subrings of $(\mathbb{Q}, +, \cdot)$.

(a) $\left\{\frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \text{ is odd}\right\}$.

(b) $\left\{\frac{p}{q} : p, q \in 2\mathbb{Z}, \text{ the even integers and } q \neq 0\right\}$.

(c) Describe the smallest subring of the rationals containing $\frac{1}{2}$.

(d) Repeat part (c), replacing $\frac{1}{2}$ with $\frac{1}{q}$. Justify your answer.

2.2.14. (a) Determine which of the subsets of $M_2(\mathbb{R})$ in Exercise 1.2.3 are subrings of it. For those that are not subrings, show why they fail. Also, if they fail, determine whether they are subgroups.

(b) Repeat part (a) for $\left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{R} \right\}$.

(c) Repeat part (a) for $\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{Z} \right\}$.

(d) Repeat part (a) for $\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{Z} \text{ and } b \in \mathbb{R} \right\}$.

(e) Repeat part (a) for $\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{R} \text{ and } b \in \mathbb{Z} \right\}$.

2.2.15. Prove these subsets of $\mathrm{GL}(2, \mathbb{R})$ are subgroups under multiplication.

(a) ★ $\left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R} \right\}$.

(b) $\left\{ \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} : c, d \in \mathbb{R} \text{ and } c \neq 0 \right\}$.

(c) $\{A \in \mathrm{GL}(2, \mathbb{R}) : \det(A) > 0\}$.

(d) $\{A \in \mathrm{GL}(2, \mathbb{R}) : A^T = A^{-1}\}$ (orthogonal matrices).

(e) Show that the group in part (a) is isomorphic to the real numbers under addition.

(f) Show that the group in part (b) is isomorphic to the set of linear functions $\alpha_{m,b}$ given by $\alpha_{m,b}(x) = mx + b$, where m, $b \in \mathbb{R}$ and $m \neq 0$ with the operation of composition.

(g) Generalize part (d) to $n \times n$ orthogonal matrices.

2.2.16. For each matrix below determine its order, if finite, in $\mathrm{GL}(2, \mathbb{R})$ or state that it has infinite order. Recall the operation is multiplication.

(a) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

(c) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

(d) ★ $\begin{bmatrix} \frac{-1}{2} & \frac{-\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2} \end{bmatrix}$

2.2.17. (a) Prove Theorem 2.2.3.

Define the *centralizer* of g in a group G to be $C(g) = \{x \in G : gx = xg\}$.

(b) ★ Find $C(M_1)$, the centralizer of M_1 in $\mathbf{D}_4$.

(c) Find $C(R)$ and $C(R^2)$ in $\mathbf{D}_4$.

(d) Find $C(M_1)$ and $C(R)$ in $\mathbf{D}_3$.

(e) Prove for each $g \in G$ that $C(g)$ is a subgroup of G.

(f) For a given $g \in G$, relate $C(g)$ to $Z(G)$. Prove your answer.

(g) Relate $Z(G)$ to the intersection of all of the $C(g)$. Prove your answer.

2.2.18. Define the *center* of a ring $(S, +, \cdot)$ as the set $\{\, s \in S \,:\, \text{for all } x \in S, s \cdot x = x \cdot s \,\}$.

(a) Is the center of a ring always a subring? If so, prove it; if not, give a counterexample.

(b) Find the center of $M_2(\mathbb{R})$, all 2×2 matrices.

2.2.19. For a, b in a group, if ab has order n, prove that ba has order n.

2.2.20. Suppose that T is a subring of S and both have unities. Must the unity of T be the unity of S? If so, prove it; if not, give a counterexample.

2.2.21. Suppose H is a subgroup of a finite group G. Consider examples to make a conjecture relating $|H|$ and $|G|$, the number of elements in each. Justify your conjecture.

2.2.22. (a) ⋆ In $\mathbf{D}_9$ find three subgroups isomorphic to $\mathbf{D}_3$. Explain why these subgroups must have the same rotations.

(b) In $\mathbf{D}_{12}$ how many subgroups are isomorphic to $\mathbf{D}_6$? to $\mathbf{D}_4$? to $\mathbf{D}_3$?

(c) Make and justify a conjecture generalizing parts (a) and (b).

2.2.23. (a) Give an example of a group and two subgroups whose union is not a subgroup.

(b) Generalize part (a) to n subgroups.

(c) Make and prove an if-and-only-if condition for when the union of two subgroups is a subgroup.

2.2.24. Find a necessary and sufficient condition on j and k so that $\langle j \rangle$ is a subgroup of $\langle k \rangle$ in $\mathbb{Z}_n$. Justify your answer.

2.2.25. Give an example of a ring S and a subring T that is a field, but for $t \in T$ with $t \neq 0$ the multiplicative inverse of t in T is not a multiplicative inverse of t in S.

Definition (Lattice). A *lattice* is a set L with two operations $\sqcap$ (called *meet*) and $\sqcup$ (called *join*) so that for all $x, y, z \in L$, the following hold.

$$\begin{array}{ccl}
x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z & x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z & \text{associative} \\
x \sqcap y = y \sqcap x & x \sqcup y = y \sqcup x & \text{commutative} \\
x \sqcap x = x & x \sqcup x = x & \text{idempotent} \\
x \sqcap (y \sqcup x) = x & x \sqcup (y \sqcap x) = y & \text{absorptive}
\end{array}$$

Examples:

(1) The positive divisors of a positive integer with $a \sqcap b = \gcd(a, b)$ and $a \sqcup b = \operatorname{lcm}(a, b)$.

(2) The subgroup lattice of a group with intersection for meet, and the smallest subgroup containing A and B for their join, $A \sqcup B$.

(3) The subring lattice of a ring, defined similarly.

(4) The set $\mathcal{P}(X)$ of all subsets of a nonempty set X with intersection for meet, and union for join.

2.2.26. (a) Draw the Hasse diagram for the lattice of the positive divisors of 18 and use it to draw the Hasse diagram for the subrings of $\mathbb{Z}_{18}$.

(b) Repeat part (a) replacing 18 with 20. Compare the diagrams for the divisors of 18 and of 20.

(c) Make a conjecture about when the Hasse diagrams of the divisors of n and k will be isomorphic.

2.2.27. (a) Draw the Hasse diagram for the lattice of all eight subsets of $\{a, b, c\}$.

(b) Draw the Hasse diagram for the lattice of subrings of $\mathbb{Z}_{30}$. Explain why this diagram looks isomorphic to the diagram in part (a).

(c) Make a conjecture about n and k so that the lattice of subrings of $\mathbb{Z}_n$ will be isomorphic to the lattice of all subsets of a set with k elements.

2.2.28. (a) Define a sublattice of a lattice.

(b) Explain why if $a \in L$, a lattice, then $\{a\}$ is a sublattice.

(c) In the lattice of divisors of 18, give sublattices of size 2, 3, and 4 and subsets of size 2, 3, and 4 that are not sublattices.

(d) Show that the lattice of positive divisors of $k \in \mathbb{N}$ is a sublattice of the lattice of positive divisors of $jk \in \mathbb{N}$.

2.3 Direct Products

Direct products help us define and investigate new systems from familiar ones. They generalize building multidimensional vector spaces from the one-dimensional system of real numbers in linear algebra. Vector spaces expand addition from numbers to vectors. The elements of a direct product, like vectors in $\mathbb{R}^n$, are ordered pairs or, more generally, ordered n-tuples forming a Cartesian product. To make them into an algebraic system we use one or more component-wise operations on ordered pairs, imitating vector addition. Direct products inherit many of the properties of their component systems, helping us understand these new systems. Further, some applications use direct products. For instance, UPC codes from Section 1.3 and more generally linear codes in Section 5.2 encode and decode messages as elements of direct products of $\mathbb{Z}_n$. We focus on structural properties of all direct products.

Example 1. The vector space $\mathbb{R}^2$ is $\{ (x, y) : x, y \in \mathbb{R} \}$, where we add the vectors (x, y) and (s, t) *component-wise*—that is, the coordinates (components) are added separately: $(x, y) + (s, t) = (x + s, y + t)$. Vector spaces also have scalar multiplication, a weaker extension of the multiplication of real numbers: $a(x, y) = (ax, ay)$. However, scalar multiplication is not an operation in $\mathbb{R}^2$ since the scalar a is not a vector. As such $\mathbb{R}^2$ is a group, but not a ring. ♢

Definition (Direct product). Given $(G, *)$ and $(H, \circ)$ define the operation $\diamond$ on the *Cartesian product* $G \times H = \{ (g, h) : g \in G, h \in H \}$ by $(a, b) \diamond (c, d) = (a * c, b \circ d)$. Then

Table 2.7. $\mathbb{Z}_2 \times \mathbb{Z}_2$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Table 2.8. $\mathbb{Z}_2 \times \mathbb{Z}_3$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,2)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$

$(G \times H, \diamond)$, or more simply $G \times H$ when there is no confusion, is the *direct product*. If G and H each have a second operation, we define a second operation on $G \times H$ similarly. We define the direct product of three or more systems analogously.

Example 2. The group $(\mathbb{Z}_2, +)$ combines with itself to give $\mathbb{Z}_2 \times \mathbb{Z}_2$ and with $(\mathbb{Z}_3, +)$ to give $\mathbb{Z}_2 \times \mathbb{Z}_3$. Use the Cayley tables in Tables 2.7 and 2.8 to compare $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ with the same sized groups $\mathbb{Z}_4$ and $\mathbb{Z}_6$, respectively. For simplicity we will use $+$ for all of the operations.

For both, $(0,0)$ is the identity and every element has an inverse. The main diagonal of Table 2.7 has only $(0,0)$, so in $\mathbb{Z}_2 \times \mathbb{Z}_2$ every element is its own inverse, unlike $\mathbb{Z}_4$. Thus $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$, but instead it is isomorphic to $\mathbf{D}_2$, introduced in Exercise 1.3.4. Let's show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$ are isomorphic by finding a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$, and so $\mathbb{Z}_2 \times \mathbb{Z}_3$ isn't really something new.

$$\begin{aligned}
(1,1)+(1,1) &= (0,2),\\
(1,1)+(1,1)+(1,1) &= (1,0),\\
(1,1)+(1,1)+(1,1)+(1,1) &= (0,1),\\
(1,1)+(1,1)+(1,1)+(1,1)+(1,1) &= (1,2), \quad \text{and}\\
(1,1)+(1,1)+(1,1)+(1,1)+(1,1)+(1,1) &= (0,0).
\end{aligned}$$

Since $(1,1)$ generates all of $\mathbb{Z}_2 \times \mathbb{Z}_3$, by Theorem 2.1.1 the group is isomorphic to $\mathbb{Z}_6$. ◊

Exercise 2.3.1. ⋆ Compare the multiplication tables for $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$ to verify that they are isomorphic as rings. Find an explicit isomorphism between them.

As Theorem 2.3.1 below illustrates, a direct product retains many of the properties of the individual systems from which it comes, just as vector spaces have many similarities to the real numbers. Because of the similarity of a direct product and its factors, after the proof of Theorem 2.3.1 we will not so carefully distinguish between the operations of the factors and the products. Verifying properties benefits greatly by an abstract approach since we can prove them for all suitable structures at once.

Theorem 2.3.1. *Suppose $(G \times H, \diamond)$ is the direct product of $(G, *)$ and $(H, \circ)$.*

(i) *If $*$ in G and $\circ$ in H are associative, so is $\diamond$ in $G \times H$.*

(ii) *If $*$ in G and $\circ$ in H are commutative, so is $\diamond$ in $G \times H$.*

(iii) *If e_G is the identity of G and e_H is the identity of H, then (e_G, e_H) is the identity of $G \times H$.*

(iv) *For (e_G, e_H) the identity of $G\times H$, if g^{-1} is the inverse of $g \in G$ and $h^{-1}$is the inverse of $h \in H$, then (g^{-1}, h^{-1}) is the inverse of $(g, h) \in G \times H$.*

(v) *If $*$ in G and $\circ$ in H are associative, then for all $(g, h) \in G \times H$ and all $n \in \mathbb{N}$ $(g, h)^n = (g^n, h^n)$.*

(vi) *If G and H are (abelian) groups, so is $G \times H$.*
Suppose $G \times H$ is the direct product of $(G, +, \cdot)$ and $(H, +, \cdot)$.

(vii) *If $\cdot$ distributes over $+$ in both G and H, distributivity also holds in $G \times H$.*

(viii) *If G and H are (commutative) rings (with unity), so is $G \times H$.*

Proof. (i) To prove associativity, let (p, q), (r, s), and (t, u) be elements of $G \times H$. Then $((p, q)\diamond(r, s))\diamond(t, u) = ((p*r, q\cdot s)\diamond(t, u)) = ((p*r)*t, (q\cdot s)\cdot u) = (p*(r*t), q\cdot(s\cdot u))$ by associativity in G and H. In turn this equals $(p, q) \diamond (r * t, s \cdot u) = (p, q) \diamond ((r, s) \diamond (t, u))$. See Exercise 2.3.17 for the rest. □

Since the direct product of groups is a group and of rings is a ring, you might naturally conjecture the same applies to fields. The following argument dashes this expectation.

Lemma 2.3.2. *If F and K are fields, $F \times K$ is not a field.*

Proof. Let 1_F be the unity of F, let 1_K be the unity of K, and let 0_K be the identity of K. Then $(1_F, 1_K)$ is the unity of $F \times K$. However, $(1_F, 0_K)$ is nonzero and no matter what (a, b) we pick in $F \times K$, $(1_F, 0_K) \cdot (a, b) = (a, 0_K) \neq (1_F, 1_K)$. □

While a direct product inherits many properties from its factors, it's a new system with new elements. However, we can expect that the orders of these new elements relate to the orders of their components. We investigate this relationship in Examples 3 and 4. Theorem 2.3.3 will completely describe the possibilities. Exercise 2.3.10 investigates direct products of cyclic groups where the product is cyclic, as in Example 2. Exercises 2.3.13 and 2.3.14 explore some of the more complicated possibilities for subgroups and subrings.

Example 3. Find the table of orders for $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Solution. The possible orders of elements in $\mathbb{Z}_2$ are 1 and 2, whereas in $\mathbb{Z}_4$ the possibilities are 1, 2, and 4. For any $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$, $(a, b) + (a, b) = (0, 2b)$ and so

Table 2.9. The group $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Order	1	2	4
Number	1	3	4

Table 2.10. The group $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Order	1	3
Number	1	8

$(a,b)+(a,b)+(a,b)+(a,b)=(0,0)$. Thus (a,b) has order 4 if and only if b has order 4 if and only if $b=1$ or $b=3$. So there are four elements of order 4. The other elements $(a,2b)$ have an even number for the second coordinate. Since $a+a=0$ and $2b+2b=0$, these elements have order at most 2. Only the identity has order 1, leaving three elements of order 2. The elements of $\mathbb{Z}_3$ have orders 1 and 3. Then in $\mathbb{Z}_3 \times \mathbb{Z}_3$ $(c,d)+(c,d)+(c,d)=(c+c+c,d+d+d)=(0,0)$. So except for the identity, elements are of order 3. Tables 2.9 and 2.10 summarize this reasoning. ◊

Theorem 2.3.3. *If x has order k in a group G and y has order n in a group H, then (x,y) has order* $\operatorname{lcm}(k,n)$ *in $G \times H$, where* $\operatorname{lcm}(k,n)$ *is the least common multiple of k and n.*

Proof. Since x has order k, the product $(x,y)^k=(x^k,y^k)=(e_G,y^k)$. In turn, for any multiple jk of k, $(x,y)^{jk}=(e_g,y^{jk})$ and if w is not a multiple of k, then $(x,y)^w \neq (e_G,y^w)$. Similarly, v is a multiple of n if and only if $(x,y)^v=(x^v,e_H)$. Hence for an integer z, $(x,y)^z=(e_G,e_H)$ if and only if z is a multiple of both k and n. Hence the order of (x,y) is the least positive such multiple, namely $\operatorname{lcm}(k,n)$. □

Corollary 2.3.4. *The group $\mathbb{Z}_k \times \mathbb{Z}_n$ is cyclic if and only if* $\operatorname{lcm}(k,n)=kn$.

Proof. The group $\mathbb{Z}_k \times \mathbb{Z}_n$, which has kn elements, is cyclic if and only if it has some element of order kn. We know that 1 has order k in $\mathbb{Z}_k$ and 1 has order n in $\mathbb{Z}_n$. So $(1,1)$ has order $\operatorname{lcm}(k,n)$ in $\mathbb{Z}_k \times \mathbb{Z}_n$. Thus this group is cyclic if and only if $\operatorname{lcm}(k,n)=kn$. □

Exercise 2.3.10 explores the generators of $\mathbb{Z}_k \times \mathbb{Z}_n$ when it is cyclic. While the characterization for cyclic groups in Corollary 2.3.4 is entirely correct, in most situations we think about the greatest common divisor of two or more numbers, rather than their least common multiple. Fact 2.3.5 allows us to restate Corollary 2.3.4 in terms of $\gcd(a,b)$ equaling 1. People often say a and b are *relatively prime* when $\gcd(a,b)=1$. Fortunately, there is a straightforward relationship between these two concepts. We delay its proof until Section 3.1 since it depends on the fundamental theorem of arithmetic (Theorem 3.1.7).

Fact 2.3.5. For all a, $b \in \mathbb{N}$, $\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab$. So $\operatorname{lcm}(a,b)=ab$ if and only if $\gcd(a,b)=1$.

Proof. See Corollary 3.1.8. □

We can use Theorem 2.3.3 to understand a direct product of groups more deeply through its table of orders, provided we know the orders of the elements of the groups.

However, it is more efficient to consider how many elements x have a given power x^k equal to the identity, as Example 4 illustrates. Since the operations in Example 4 are modular addition, instead of multiplicative notation, we use additive notation throughout, so, for instance $2(x, y) = (0, 0)$ indicates adding (x, y) to itself gives the identity, using the appropriate addition in each component.

Example 4. Determine the table of orders for $(\mathbb{Z}_4 \times \mathbb{Z}_6, +)$.

Solution. We know the orders of elements of $\mathbb{Z}_4$ are 1, 2, or 4, while those of $\mathbb{Z}_6$ are 1, 2, 3, or 6. By Theorem 2.3.3 the possible orders of elements $\mathbb{Z}_4 \times \mathbb{Z}_6$ are 1, 2, 3, 4, 6, or 12. We work up from order 1, which only the identity has. Consider the elements (x, y) of $\mathbb{Z}_4 \times \mathbb{Z}_6$ which, when added to themselves, give the identity. For the first coordinate $x = 0$ or $x = 2$. Similarly, $y = 0$ or $y = 3$. Thus $2(x, y) = (0, 0)$ has four solutions, three elements of order 2 and $(0, 0)$.

For $3(x, y) = (0, 0)$, we need $x = 0$ and $y = 0$, $y = 2$, or $y = 4$. Of the three solutions, $(0, 0)$ has order 1 and the other two $(0, 2)$ and $(0, 4)$ have order 3.

For $4(x, y) = (0, 0)$, x can be any element and the order of y must divide 4. That is, $y = 0$ or $y = 3$, giving eight such elements. However, we already counted four elements of orders 1 and 2, leaving four elements of order 4.

Elements (x, y) satisfying $6(x, y) = (0, 0)$ must have $x = 0$ or $x = 2$, while y can be anything. Of the twelve such elements, six have orders 1, 2, or 3, giving six of order 6.

The eight remaining elements must have order 12. Table 2.11 gives the table of orders of $\mathbb{Z}_4 \times \mathbb{Z}_6$. ◊

The cyclic and dihedral groups give us many small groups. Combining them using direct products gives even more. While many more groups exist beyond these, we already can find most groups with at most twenty elements. The cyclic groups $\mathbb{Z}_n$ give us one for each size. Dihedral groups give another nine groups and direct products give twelve more. Thus we can now describe 41 of the 54 groups of order at most twenty indicated in Table 2.12. Example 5 and Exercises 2.3.15 and 2.3.16 explore this further. Later in Theorems 3.2.1 and 3.2.2 we will see how to describe all finite abelian groups. However, determining all groups of order n up to isomorphism is an unsolved problem in general. We will consider some aspects of this question in later sections.

Example 5. The top row of Table 2.13 gives the possible orders of the groups listed there. The rows below that one give the tables of orders for the groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$,

Table 2.11. The group $\mathbb{Z}_4 \times \mathbb{Z}_6$.

Order	1	2	3	4	6	12
$\mathbb{Z}_4 \times \mathbb{Z}_6$	1	3	2	4	6	8

Table 2.12. Number of abelian and nonabelian groups, up to isomorphism

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
abelian	1	1	1	2	1	1	1	3	2	1	1	2	1	1	1	5	1	2	1	2
nonabelian	0	0	0	0	0	1	0	2	0	1	0	3	0	1	0	9	0	3	0	3

Table 2.13. Some groups of order 8.

order	1	2	4	8
$\mathbb{Z}_8$	1	1	2	4
$\mathbb{Z}_4 \times \mathbb{Z}_2$	1	3	4	0
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	1	7	0	0
$\mathbf{D}_4$	1	5	2	0

Table 2.14. Some groups of order 12.

order	1	2	3	4	6	12
$\mathbb{Z}_{12}$	1	1	2	2	2	4
$\mathbb{Z}_4 \times \mathbb{Z}_3$	1	1	2	2	2	4
$\mathbb{Z}_6 \times \mathbb{Z}_2$	1	3	2	0	6	0
$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	1	3	2	0	6	0
$\mathbf{D}_6$	1	7	2	0	2	0
$\mathbf{D}_3 \times \mathbb{Z}_2$	1	7	2	0	2	0

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbf{D}_4$ and indicate that these groups are not isomorphic. So we know four of the five groups of order 8 from Table 2.12. Table 2.14, the table of orders for several groups of order 12 suggests a number of them may be isomorphic. In fact, we can only describe three of the five different groups of order 12 at this time. Thus Table 2.14 immediately suggests an important question: How can we determine when two representations of groups are isomorphic? For instance, if their tables of orders are identical, are the groups isomorphic? Further, the first four systems in this table can also be rings. If the groups are isomorphic, must the rings be? ◊

Example 6. The group $\mathbb{Z}_5 \times \mathbb{Z}_5$ has eight subgroups, starting with the entire group and the one with just $(0,0)$ in it. All other subgroups are cyclic. Figure 2.5 illustrates four of those subgroups, namely $\langle(1,0)\rangle, \langle(0,1)\rangle$, and $\langle(1,1)\rangle$, represented with dashed lines, and $\langle(1,2)\rangle$, represented by the two solid lines. Since $\mathbb{Z}_5 \times \mathbb{Z}_5$ is also a ring, we can ask which of its subgroups are also subrings. You can verify that $\langle(1,0)\rangle, \langle(0,1)\rangle$, and $\langle(1,1)\rangle$, with dashed lines in Figure 2.5, along with the entire ring and $\{(0.0)\}$ are subrings. However, $(1,2)\cdot(1,2) = (1,4)$ is not in the cyclic subgroup $\langle(1,2)\rangle$, which is therefore not a subring. Similarly, $\langle(1,3)\rangle$ and $\langle(1,4)\rangle$ are not subrings. Determining subgroups and subrings in general is challenging. See Exercises 2.3.13 and 2.3.14 and Project 2.P.2. ◊

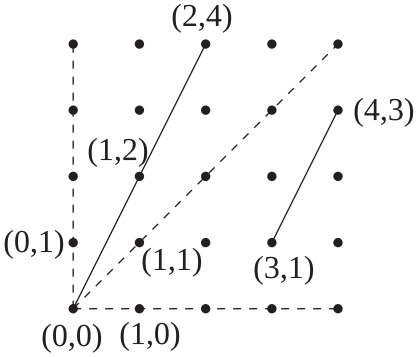

Figure 2.5. $\mathbb{Z}_5 \times \mathbb{Z}_5$.

Exercises

2.3.2. (a) Find the number of elements in $\mathbb{Z}_3 \times \mathbb{Z}_6$.

(b) What is the additive inverse of $(1,2)$ in $\mathbb{Z}_3 \times \mathbb{Z}_6$? Repeat for $(2,3)$ and $(1,5)$.

(c) What is the order of $(1,2)$ in $\mathbb{Z}_3 \times \mathbb{Z}_6$? Repeat for $(2,3)$ and $(1,5)$. List the possible orders of elements.

2.3.3. (a) ⋆ Find the number of elements in $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$.

(b) What is the inverse of $(0,0,1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$? Repeat for $(1,2,2)$ and $(1,3,3)$.

(c) What is the order of $(0,0,1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$? Repeat for $(1,2,2)$ and $(1,3,3)$. List the possible orders of elements.

2.3.4. (a) Find the number of elements in $\mathbf{D}_3 \times \mathbf{D}_3$.

(b) What is the inverse of (I,R) in $\mathbf{D}_3 \times \mathbf{D}_3$? Repeat for (R,R^2) and (M_1,R^2).

(c) What is the order of (I,R) in $\mathbf{D}_3 \times \mathbf{D}_3$? Repeat for (R,R^2) and (M_1,R^2). List the possible orders of elements. *Hint.* See Table 1.4.

2.3.5. (a) Prove that the ring $\mathbb{R} \times \mathbb{R}$ is not isomorphic to $\mathbb{C}$, the field of complex numbers.

(b) Prove that the group $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ with addition is isomorphic to the set of 2×2 matrices $M_2(\mathbb{R})$ with addition. Are they isomorphic as rings? Prove your answer.

2.3.6. (a) Give the table of orders for $(\mathbb{Z}_3 \times \mathbb{Z}_5, +)$.

(b) Repeat part (a) for $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$.

(c) Repeat part (a) for $\mathbb{Z}_3 \times \mathbb{Z}_6$.

(d) ⋆ Repeat part (a) for $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$.

(e) Repeat part (a) for $\mathbf{D}_3 \times \mathbf{D}_3$.

(f) Repeat part (a) for $\mathbf{D}_4 \times \mathbf{D}_4$.

2.3.7. (a) Find the table of orders for $(\mathbb{Z}_4 \times \mathbb{Z}_4, +)$.

(b) Repeat part (a) for $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

(c) Repeat part (a) for $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

(d) ⋆ Repeat part (a) for $\mathbb{Z}_{12} \times \mathbb{Z}_4$.

(e) Repeat part (a) for $\mathbb{Z}_{12} \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

(f) Make a conjecture about the number of elements of order 2 in the direct product of k cyclic groups, based on how many of the groups have an even number of elements.

2.3.8. (a) Find the table of orders for $\mathbb{Z}_3 \times \mathbb{Z}_3$.

(b) Repeat part (a) for $\mathbb{Z}_9 \times \mathbb{Z}_9$.

(c) Repeat part (a) for $\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9$.

(d) Make a conjecture about the number of elements of order 3 in the direct product of k cyclic groups, based on how many of the groups have order a multiple of 3.

2.3.9. We compare the table of orders of $\mathbf{D}_n \times \mathbb{Z}_2$ and $\mathbf{D}_{2n}$ beyond Example 5.

(a) ⋆ Find the table of orders for $\mathbf{D}_4 \times \mathbb{Z}_2$. Compare with the table of orders for $\mathbf{D}_8$.

(b) Repeat part (a) for $\mathbf{D}_5 \times \mathbb{Z}_2$. Compare with the table of orders for $\mathbf{D}_{10}$.

(c) Repeat part (a) for $\mathbf{D}_6 \times \mathbb{Z}_2$. Compare with the table of orders for $\mathbf{D}_{12}$.

(d) Make a conjecture about how the table of orders for $\mathbf{D}_n \times \mathbb{Z}_2$ compares with the table of orders for $\mathbf{D}_{2n}$.

2.3.10. (a) Find the four generators of $(\mathbb{Z}_3 \times \mathbb{Z}_4, +)$. How do they relate to the generators of $\mathbb{Z}_3$ and $\mathbb{Z}_4$?

(b) Find the generators of $(\mathbb{Z}_2 \times \mathbb{Z}_5, +)$. How do they relate to the generators of $\mathbb{Z}_2$ and $\mathbb{Z}_5$?

(c) Find several generators for $\mathbb{Z}_3 \times \mathbb{Z}_5$. How do they relate to generators of $\mathbb{Z}_3$ and $\mathbb{Z}_5$? Determine the number of generators of $\mathbb{Z}_3 \times \mathbb{Z}_5$.

(d) Make a conjecture describing the generators of $\mathbb{Z}_n \times \mathbb{Z}_k$, assuming it is cyclic.

(e) Suppose that $\mathbb{Z}_n \times \mathbb{Z}_k$ is isomorphic to $\mathbb{Z}_{nk}$ as groups. Are they isomorphic as rings? If so, explain why; if not, give a counterexample.

2.3.11. (a) Suppose S and T are rings. Prove that $S \times T$ and $T \times S$ are isomorphic.

(b) For a ring S, define $S^D = \{(s, s) : s \in S\}$, the diagonal elements in $S \times S$. Is S isomorphic to S^D? If so, prove it; if not, give a counterexample.

(c) For a ring S, define $S^{-D} = \{(s, -s) : s \in S\}$. Is S^{-D} a group? Is it a ring? Is S isomorphic to S^{-D} as a group or a ring? For each question, prove your answer.

2.3.12. Suppose G and H are groups. Let $\overline{G} = \{(g, e_H) : g \in G\}$ and $\overline{H} = \{(e_G, h) : h \in H\}$ be subsets of $G \times H$.

(a) Prove that $\overline{G}$ and $\overline{H}$ are subgroups of $G \times H$, called “projections” of $G \times H$.

(b) Prove that G and $\overline{G}$ are isomorphic. (Similarly, H and $\overline{H}$ are isomorphic.)

(c) For A a subgroup of G and B a subgroup of H, is $A \times B$ always a subgroup of $G \times H$? If so, prove it; if not, give a counterexample.

(d) Repeat parts (a), (b), and (c) for rings and subrings.

(e) Can every subgroup or subring of a direct product be written in the form of part (c)? If so, prove it; if not, give a counterexample.

2.3.13. The number in parentheses gives the number of subgroups for each part, including the entire set.

(a) Draw the subgroup lattice for $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. (5)

(b) ⋆ Repeat part (a) for $\mathbb{Z}_4 \times \mathbb{Z}_2$. (8)

(c) Repeat part (a) for $\mathbb{Z}_3 \times \mathbb{Z}_3$. (6)

(d) Repeat part (a) for $\mathbb{Z}_6 \times \mathbb{Z}_2$. (10)

(e) Repeat part (a) for $\mathbb{Z}_6 \times \mathbb{Z}_3$. (12)

2.3.14. The number in parentheses gives the number of subrings for each part, including the entire set. Compare with the lattices of subgroups in Exercise 2.3.13 parts (b), (c), and (e).

(a) Draw the subring lattice for $\mathbb{Z}_4 \times \mathbb{Z}_2$. (7)

(b) Repeat part (a) for $\mathbb{Z}_3 \times \mathbb{Z}_3$. (5)

(c) Repeat part (a) for $\mathbb{Z}_6 \times \mathbb{Z}_3$. (10)

2.3.15. (a) Use cyclic groups and direct products to describe the five nonisomorphic abelian groups of order 16 indicated by Table 2.12. Prove that they are nonisomorphic.

(b) ⋆ Describe as many nonisomorphic abelian groups of order 36 as you can and show them nonisomorphic.

(c) Repeat part (b) for abelian groups of order 32.

(d) Repeat part (b) for abelian groups of order 100.

(e) Make a conjecture based on parts (b) and (d).

2.3.16. (a) Describe ten nonabelian groups of order at most 20 using dihedral groups and direct products. Show that they are all nonisomorphic.

(b) ⋆ Describe as many nonisomorphic nonabelian groups of order 36 as you can and show them nonisomorphic.

(c) Repeat part (b) for nonabelian groups of order 32.

2.3.17. Finish the proof of Theorem 2.3.1.

2.3.18. (a) Describe two nonisomorphic abelian groups of order $9 = 3^2$. Describe three nonisomorphic abelian groups of order $27 = 3^3$.

(b) There are two nonisomorphic abelian groups of order p^2, where p is a prime. Use cyclic groups and direct products to describe them. Prove that they are nonisomorphic.

(c) There are three nonisomorphic abelian groups of order p^3, where p is a prime. Use cyclic groups and direct products to describe all three. Prove that they are nonisomorphic.

(d) Describe the five nonisomorphic abelian groups of order p^4, where p is a prime.

(e) Describe the seven nonisomorphic abelian groups of order p^5, where p is a prime.

2.3.19. (a) Show that if G is a nonabelian group and H is any group, then $G \times H$ is nonabelian.

(b) ⋆ Show that if S is a noncommutative ring and T is any ring, then $S \times T$ is noncommutative.

2.3.20. (a) ⋆ If the ring $S \times T$ has a unity, must S and T have unities? If so, prove it; if not, give a counterexample.

(b) If the rings S and T each have 1 as a unity, describe all $(s, t) \in S \times T$ with multiplicative inverses in terms of s and t. Justify your answer.

2.3.21. Let S and T be rings and suppose that $S \times T$ is a field and S has more than one element. Prove that $T = \{0\}$ and so S is a field isomorphic to $S \times T$.

2.3.22. Define the ring $\mathbf{B}_n$, a type of *Boolean ring*, to be the direct product of the ring $\mathbb{Z}_2$ with itself n times. (See Exercise 2.3.23, for Boolean rings in general, all named after the logician George Boole (1815–1864) who studied the algebraic structure of logic.) We show that the algebraic structure of $\mathbf{B}_n$ connects closely with set theory operations, which relate to logic.

(a) Explain why $\mathbf{B}_n$ has 2^n elements. Define $\beta : \mathbf{B}_n \to \mathcal{P}(n)$, the set of all subsets of $\{1, 2, \ldots, n\}$, by $\beta(b)$ is the set of nonzero coordinates of b. Prove that β is a bijection.

(b) $\star$ Prove that for all $b \in \mathbf{B}_n$, $b \cdot b = b$. We say b is *idempotent*. *Hint*. Consider the coordinates separately.

(c) Prove that β is an isomorphism between $(\mathbf{B}_n, \cdot)$ and $(\mathcal{P}(n), \cap)$.

(d) $\star$ Define $\sqcup$ on $\mathbf{B}_n$ by $b \sqcup c = b + c + (b \cdot c)$. Show that $\beta(b \sqcup c) = \beta(b) \cup \beta(c)$. *Hint*. Consider the coordinates separately.

(e) Describe the unity $\overline{1}$ of $\mathbf{B}_n$, and prove your choice correct.

(f) Define $b' = \overline{1} + b$. Show that $\beta(b')$ is the complement of $\beta(b)$ with respect to $\{1, 2, \ldots, n\}$. Thus $(\mathbf{B}_n, \cdot, \sqcup, ')$ is isomorphic to $(\mathcal{P}(n), \cap, \cup, ^c)$, where A^c is the set complement of A with respect to $\{1, 2, \ldots, n\}$. $(\mathbf{B}_n, \cdot, \sqcup, ')$ is an example of an algebraic system studied in Section 7.2 and called a *Boolean algebra*. A Boolean algebra is a special type of lattice, introduced in Section 7.1. Mathematical logic and computer circuitry use Boolean algebras and rings.

2.3.23. We generalize Exercise 2.3.22. A *Boolean ring* $\mathbf{B}$ is a ring with the property that $x \cdot x = x$ for all $x \in \mathbf{B}$.

(a) Prove for all $x \in \mathbf{B}$, $x + x = 0$. *Hint*. Consider $(x + x)(x + x)$.

(b) Prove $\mathbf{B}$ is a commutative ring.

(c) $\star$ Let S be a set with at least one element, and for T and W subsets of S, define $T \cdot W = T \cap W$ and $T + W = T \cup W - (T \cap W)$, where $A - B = \{a \in A : a \notin B\}$. Use Venn diagrams to verify that $(\mathcal{P}(S), +, \cdot)$ is a Boolean ring with unity S.

(d) Let $F(\mathbb{N})$ be the set of all finite subsets of $\mathbb{N}$. Verify that $F(\mathbb{N})$ is a Boolean ring using the operations of part (c). Show that it does not have a unity.

2.3.24. We investigate alternative multiplications on the group $(\mathbb{Z}_n \times \mathbb{Z}_n, +)$ besides component-wise multiplication.

(a) Define $(a, b) \odot (c, d) = (ac, ad + bc)$. Find the unity of $\odot$. Verify associativity and distributivity for $\odot$. Compare this multiplication with multiplying first-degree polynomials and ignoring the x^2 term.

(b) If we think of x as $\sqrt{k}$, we can define $(a + bx) \circledast (c + dx) = ac + bdk + (ad + bc)x$ for first-degree polynomials. Assume that this gives a ring. Explain why this is similar to defining $\circledast$ on $(\mathbb{Z}_n \times \mathbb{Z}_n, +)$ by $(a, b) \circledast (c, d) = (ac + kbd, ad + bc)$.

(c) Find the unity of $(\mathbb{Z}_n \times \mathbb{Z}_n, +, \circledast)$ in part (b).

(d) For $n = 3$ and $k = 2$ in part (c), find the multiplicative inverse of each nonidentity element, verifying that this is a field with nine elements.

(e) ⋆ For $n = 3$ and $k = 1$ in part (c), does each nonidentity element have an inverse? If so, provide it; if not, give a counterexample.

(f) Compare part (d) with complex multiplication.

(g) Look for values of n and k in part (c) that give fields.

Bartel van der Waerden. Bartel van der Waerden (1903–1996) profoundly influenced the teaching of mathematics. All abstract algebra textbooks since 1930 have been patterned on his text. He organized the pioneering synthesis of Emmy Noether, under whom he had studied. Emmy Noether brought together the Chapter 2 concepts of isomorphism, subgroups, subrings, direct product, and homomorphism along with the structural ideas developed in Section 3.6 and 4.2 and more. Van der Waerden fully developed all of these ideas in his text.

After finishing his undergraduate degree in mathematics in his native Netherlands, Van der Waerden started his graduate studies in Germany, including his first time studying and working with Noether. When he returned to the Netherlands to finish his PhD at age 22 he was already a noted algebraist. In his mid-20s he wrote his ground-breaking algebra text. Van der Waerden made extensive contributions to mathematics outside of algebra, including algebraic geometry, topology, number theory, probability theory, and especially the history of mathematics.

Van der Waerden taught at Groningen University for two years and then Leipzig University in Germany from 1931 until 1943. In 1943 his house was bombed during World War II. His years under the Nazis were complicated. Although he was not Jewish, he tried to mitigate the Nazi suppression of Jewish mathematicians and their work. The Nazis pressured him to drop his Dutch citizenship, but he refused. He lived in various towns after his house was destroyed until after World War II, when he returned to the Netherlands. While he was offered a university position there, because he had worked in Germany during the war, the Dutch government wouldn't allow him to take it until 1948. In 1951 he moved to Zurich, Switzerland, where he remained for the rest of his life. His considerable influence continued there as everywhere else.

2.4 Homomorphisms

The rings $\mathbb{Z}_n$ come from and mimic important features of the integers $\mathbb{Z}$, even though they are finite. While isomorphisms match systems that are exactly alike, homomorphisms relate systems that are structurally similar, even if not the same size. Historically the connection between the integers and modular arithmetic came noticeably before the idea of a homomorphisms, but their relationship exemplifies this concept. In general a homomorphism can map a system to a less complicated system, and the simpler system can give us important insight about the original one. In a sense, homomorphisms provide a formal analogue to the idea of mathematical modeling—the model provides a simpler, artificial representation of certain aspects of a complicated real system. The formal definition of homomorphism gives structural benefits, not just analogies. It will lead us near the end of this section to one of the most important theorems of group theory, Lagrange's theorem, Theorem 2.4.4.

Example 1. We show for any $k \in \mathbb{N}$ that the function $\alpha : \mathbb{Z} \to \mathbb{Z}_k$ given by $\alpha(x) = r$, where $x \equiv r \pmod{k}$ and $0 \leq r < k$ preserves the structure—the "morphism" part of an isomorphism: $\alpha(x + y) = \alpha(x) + \alpha(y)$ and $\alpha(x \cdot y) = \alpha(x)\alpha(y)$.

Table 2.15. Cayley tables of $\mathbf{D}_n$ and $\mathbf{D}_1$.

$\circ$	R^j	M_k
R^i	R^{i+j}	M_{i+k}
M_p	M_{p-j}	R^{p-k}

$\circ$	I	M_1
I	I	M_1
M_1	M_1	I

Solution. Let $x, y \in \mathbb{Z}$ and suppose from the division algorithm (Theorem 1.3.6) that $x = qk + r$ and $y = pk + s$, where $0 \leq r, s < k$. Then $x + y = (q + p)k + r + s$ and so $\alpha(x)+\alpha(y) = r+s = t$, where $r+s \equiv t \pmod{k}$ and $0 \leq t < k$. Also, $\alpha(x+y) = \alpha(r+s) = t$. Multiplication is similar since $xy = (qk + r)(pk + s) = (qpk + qs + rp)k + rs$. ♢

Over 250 years ago mathematicians starting with Euler realized the value of this preservation of operations for investigating number theory. While the mapping α loses some information since it is not one-to-one, it often clarifies arguments. For instance, Lagrange proved in 1770 the long noted pattern that every natural number can be written as the sum of at most four squares. (For instance, $11 = 3^2 + 1^2 + 1^2$ and $23 = 3^2 + 3^2 + 2^2 + 1^2$.) A number needs four squares if and only if it is congruent to $7 \pmod 8$, shown by Legendre in 1797. Modular arithmetic shows one direction of Legendre's result and even suggests how to look for the squares: Note that 1^2, 3^2, 5^2, and 7^2 all equal $1 \pmod 8$, 2^2 and 6^2 equal $4 \pmod 8$, and 0^2 and 4^2 are $0 \pmod 8$. So to get a number congruent to $7 \pmod 8$ requires three squares congruent to 1 and another congruent to $4 \pmod 8$. ♢

Definition (Homomorphism). A function $\sigma : A \to B$ is a *homomorphism* from a system $(A, *)$ to a system $(B, \cdot)$ if and only if for all $x, y \in A$, $\sigma(x * y) = \sigma(x) \cdot \sigma(y)$. The set $\sigma[A]$, whether or not it is all of B, is the *homomorphic image* of A. If A and B have more than one operation, we require σ to preserve all of the corresponding operations.

Example 2. The symmetries of a dihedral group $\mathbf{D}_n$ split naturally into two subsets, the rotations and the mirror reflections. Define $\delta : \mathbf{D}_n \to \mathbf{D}_1$ by $\delta(R^i) = I = R^0$ and $\delta(M_k) = M_1$. The generic entries with exponents and subscripts $(\operatorname{mod} n)$ in the first Cayley table of Table 2.15 match the entries in the Cayley table of $\mathbf{D}_1$, enabling a proof of a homomorphism by cases. For instance, $\delta(R^i \circ M_k) = \delta(M_{i+k}) = M_1 = I \circ M_1 = \delta(R^i) \circ \delta(M_k)$. The other cases are similar. ♢

Example 3. By definition a linear transformation τ from a vector space V to another vector space W is a group homomorphism for vector addition: $\tau(\vec{x} + \vec{y}) = \tau(\vec{x}) + \tau(\vec{y})$. It also preserves scalar multiplication since $\tau(a\vec{v}) = a\tau(\vec{v})$. If V has dimension n and W has dimension m, then τ can be represented by an $m \times n$ matrix. ♢

Example 4. For $k \in \mathbb{Z}$, the function $\beta(x) = kx$ is a homomorphism from $(\mathbb{Z}, +)$ to itself. The distributivity of multiplication over addition corresponds exactly with operation preserving: $k(x+y) = kx+ky$ if and only if $\beta(x+y) = \beta(x)+\beta(y)$. This example extends to the additive group $(S, +)$ of any ring S and any element k of S. However, these functions are not likely to be ring homomorphisms since multiplication doesn't generally distribute over itself. (See Exercise 2.4.15.) ♢

As we saw in Section 2.1, isomorphisms completely preserve the structure of operations and so algebraic properties. Homomorphisms are not as strong as isomorphisms, preserving some properties and modifying others, as Theorem 2.4.1 will codify. The theorem requires the homomorphism to be onto because the definition only applies to images of elements from the domain. Example 5 illustrates why we need to restrict our attention to the homomorphic image.

Example 5. Let $\alpha : \mathbb{Z} \to \mathrm{GL}(2, \mathbb{R})$ be given by $\alpha(z) = \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}$. Then α is a homomorphism turning addition of integers into multiplication of matrices. While $\mathbb{Z}$ is abelian, the entire group $\mathrm{GL}(2, \mathbb{R})$ is not. However, the homomorphic image of $\mathbb{Z}$ is abelian, something the homomorphism can guarantee. ♢

Theorem 2.4.1. *For σ a homomorphism from a system A onto a system B:*

(i) *if A has associativity, commutativity, or distributivity, then so does B;*

(ii) *if A has an identity e_A, then $\sigma(e_A)$ is the identity e_B of B;*

(iii) *if a has an inverse a^{-1} in A, then $\sigma(a)$ has $\sigma(a^{-1})$ as an inverse in B;*

(iv) *if A is a group, so is B;*

(v) *if A is a ring, so is B;*

(vi) *for $n \in \mathbb{N}$, $(\sigma(a))^n = \sigma(a^n)$;*

(vii) *if $a \in A$ has order n, then $\sigma(a)$ has an order dividing n;*

(viii) *if H is a subgroup (subring) of A, then $\sigma[H]$ is a subgroup (subring) of B; and*

(ix) *if K is a subgroup (subring) of B and A is a group (ring), then the preimage $\sigma^{-1}[K]$ is a subgroup (subring) of A.*

If $\sigma : A \to B$ is not onto, then the preceding statements hold with B replaced by $\sigma[A]$.

Proof. See Exercise 2.4.20 for parts (i) to (vi) and (viii). To prove part (vii) suppose that $a \in A$ has order n. Then $a^n = e_A$ and so $\sigma(a)^n = (\sigma(a^n)) = \sigma(e_A) = e_B$ by parts (vi) and (ii). Thus the order of $\sigma(a)$, say k, is at most n. If $|\sigma(a)| = k$ divides n, we have $(\sigma(a))^n = e_B$. But we need more. Suppose k doesn't divide n, giving $n = kq + r$, where $0 < r < k$. Then $\sigma(a^n) = \sigma(a^{kq})\sigma(a^r) = e_B\sigma(a^r) \neq e_B$ by the assumption that k is the smallest positive exponent giving $(\sigma(a))^k = e_B$. So k must divide n.

To prove part (ix) let K be a subgroup of B. By definition $\sigma^{-1}[K]$ is a subset of A and uses the same operation as A. Also $e_B \in K$. By part (ii), $\sigma(e_A) = e_B \in K$, so $e_A \in \sigma^{-1}[K]$. For closure and inverses, let a, $a' \in \sigma^{-1}[K]$. Then there are k, $k' \in B$ with $\sigma(a) = k$ and $\sigma(a') = k'$. Further, $\sigma(aa') = \sigma(a)\sigma(a') = kk' \in K$ and by part (iii) $\sigma(a^{-1}) = (\sigma(a))^{-1} = k^{-1} \in K$. Thus $aa', a^{-1} \in \sigma^{-1}[K]$. □

Example 6. We can repurpose the homomorphism of Example 1 as a homomorphism from one ring $\mathbb{Z}_n$ onto another $\mathbb{Z}_k$, for carefully chosen values n and k. For instance, we will see that $\alpha : \mathbb{Z}_{12} \to \mathbb{Z}_4$ given by $\alpha(x) = r$, where $x \equiv r \pmod 4$ and $0 \leq r < 4$ is a homomorphism. It takes 0, 4, and 8 to 0; similarly 1, 5, and 9 go to 1; and 2, 6, and 10 go to 2; and 3, 7, and 11 go to 3. However, a seemingly similar mapping from $\mathbb{Z}_9$ to $\mathbb{Z}_4$ using (mod 4) fails to be a homomorphism for either addition or multiplication. For instance, $3 + 8 = 2$, but $\alpha(3) = 3$, $\alpha(8) = 0$, and $\alpha(2) = 2$. Then $\alpha(3 + 8) = 2$, whereas $\alpha(3) + \alpha(8) = 3 + 0 = 3$. Similarly, $\alpha(3 \cdot 8) = \alpha(6) = 2$, whereas $\alpha(3)\alpha(8) = 3 \cdot 0 = 0$. In $\mathbb{Z}_9$ the orders of elements are 1, 3, and 9. The only order in $\mathbb{Z}_4$ dividing these values is 1.

The previous discussion illustrates part (vii) of Theorem 2.4.1 relating the order of an image to the order of the original element. Indeed the only possible homomorphism from $\mathbb{Z}_9$ to $\mathbb{Z}_4$ takes every element to the identity 0. What about the function α from $\mathbb{Z}_{12}$ to $\mathbb{Z}_4$ discussed earlier? The reader can check that α satisfies part (vii) on the divisibility of orders. But that property doesn't immediately guarantee a homomorphism from $\mathbb{Z}_{12}$ onto $\mathbb{Z}_4$. The key is a compatibility of (mod 12) and (mod 4). More generally, for any $j, k \in \mathbb{N}$ and $x, y \in \mathbb{Z}$ with $x \equiv y \pmod{jk}$, we also have $x \equiv y \pmod{k}$: From $x \equiv y \pmod{jk}$ there is some $i \in \mathbb{N}$ so that $x - y = i(jk) = (ij)k$. Thus $x \equiv y \pmod{k}$. From this compatibility the proof of Example 1 shows that $\alpha : \mathbb{Z} \to \mathbb{Z}_k$ is also a homomorphism from $\mathbb{Z}_{jk}$ to $\mathbb{Z}_k$. ♢

Example 7. Evaluation of polynomials at a particular value is a homomorphism from the ring of polynomials $F[x]$ to the field F. That is, for $f \in F[x]$ with $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $c \in F$, we define $\phi_c : F[x] \to F$ by $\phi_c(f) = f(c) = a_n c^n + \cdots + a_1 c + a_0$. Exercises 2.4.3 and 2.4.12 consider aspects of this homomorphism. The evaluation homomorphism tells us that polynomials as formal symbols or as functions and their values have similar structure. ♢

Earlier examples may not seem very surprising, but homomorphisms can provide deeper insights, indicated by Examples 8 and 9. Example 10 relates homomorphisms to homomorphic encryption, a modern application of homomorphisms. Section 5.2 will discuss aspects of encryption, an area that uses abstract algebra extensively.

Example 8. The *modulus* of a complex number $x+yi$ is $|x + yi| = \sqrt{x^2 + y^2}$ and measures the size of a complex number, generalizing absolute value. It gives a function μ from $\mathbb{C}$ to the nonnegative reals $\mathbb{R}_{\geq 0}$, $\mu(x + yi) = \sqrt{x^2 + y^2}$. If we plot complex numbers on the plane, from the Pythagorean theorem the modulus is the distance $x + yi$ is from the origin $0 + 0i$. Even more, as Exercise 2.4.2 shows, μ is a homomorphism from the multiplicative group of nonzero complexes $(\mathbb{C}^*, \cdot)$ onto the positive reals $(\mathbb{R}^+, \cdot)$. That is, the modulus of a product is the product of the moduli of the factors. For instance, $|3 + 4i| = 5$, $|5 + 12i| = 13$, and so $|(3 + 4i)(5 + 12i)| = 5 \cdot 13 = 65$, without further computations. The usual complex multiplication $(3+4i)(5+12i) = (15-48)+(36+20)i = -33+56i$ obscures this insight. We can represent a complex number $x+yi$ as $re^{i\theta} = r(\cos(\theta) + i\sin(\theta))$, where $r = |x + yi|$, illustrated in Figure 2.6. This representation can confirm that μ is a homomorphism more easily and leads to a second one. The rules of exponents give us $(re^{i\theta})(se^{i\varphi}) = rse^{i(\theta+\varphi)}$, illustrated in Figure 2.7. The homomorphism μ fits with this: $\mu((re^{i\theta})(se^{i\varphi})) = rs = \mu(re^{i\theta})\mu(se^{i\varphi})$. Also, for the nonzero complex numbers, $\mathbb{C}^*$, the function $\alpha : \mathbb{C}^* \to \mathbb{R}$ defined by $\alpha(re^{i\theta}) = \theta$ gives another homomorphism from the complex numbers under multiplication to the real numbers under addition $\pmod{2\pi}$: $\alpha((re^{i\theta})(se^{i\varphi})) = \alpha(rse^{i(\theta+\varphi)}) = \theta + \varphi = \alpha(re^{i\theta}) + \alpha(se^{i\varphi})$. (Complex addition is not preserved under μ or α. For instance, $|1 + 2i| = \sqrt{5}$, $|2 + 2i| = 2\sqrt{2}$, but their sum, $3 + 4i$ has modulus 5, which is neither the product nor sum of these moduli. Similarly, their angles are approximately 1.107, 0.785, and 0.927, respectively.) ♢

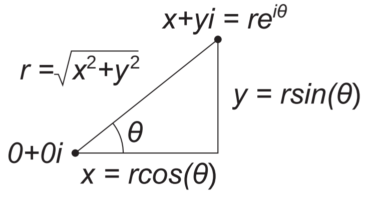

Figure 2.6. $x+yi=r(\cos(\theta)+i\sin(\theta)) = re^{i\theta}$

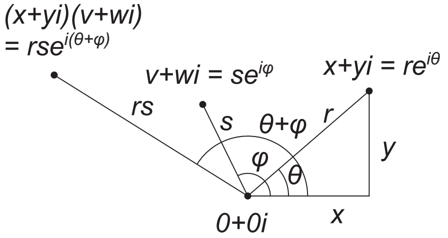

Figure 2.7. Complex multiplication.

Example 9. In 1891 Fedorov and Schönflies classified the 230 possible three-dimensional infinite groups corresponding to possible chemical crystals. Previously, mathematicians had classified the possible finite groups of three-dimensional transformations fixing a point. Homomorphisms sending all translations to the identity reduced the unwieldy problem of finding these infinite groups by mapping them to corresponding finite groups. Chemical properties restricted these finite groups to a manageable set of groups that can be described as subgroups of the symmetries of a cube or a hexagonal prism. From this list of possible finite groups one can determine the infinite groups that can map to them. While there are 230 of these infinite groups, Fedorov showed that this corresponded to the 33 types of chemical crystal types. Starting in 1914, x-ray crystallography confirmed the match between the atomic structure of crystals and the already developed theory. ♢

Example 10. In 2009 Craig Gentry introduced the first fully homomorphic encryption scheme. In 2014 Gentry received a MacArthur "genius" award for his pioneering work in cryptography. Encryption in general transforms messages to make it difficult, if not impossible, for anyone other than those given the decoding system to discover the content of the message. However, previous encryption methods focused on just transmitting a fixed message, rather than enabling people to modify the encoded message. The storage of data in the internet cloud makes it important for different people to be able to work on the same encrypted data. A fully homomorphic encryption scheme based on the ring $F[x]$ of polynomials over a finite field enables this because the encryption is a homomorphism and so preserves the structure of the changes. Also addition and multiplication in $F[x]$ have enough descriptive power to represent any transformation of the data, shown for some finite fields in Theorem 4.6.2.

A partial and simplified example would be to use the elements of $\mathbb{Z}_{26}$ to represent the letters of the alphabet, so $a = 0$, $b = 1$, etc. An easily cracked, partially homomorphic code might multiply each element by 3 (mod 26). Thus one person would encode $(m, a, t, h) = (13, 0, 20, 8)$ as $(39, 0, 60, 24) \equiv (13, 0, 8, 24) \pmod{26}$. Another person could have the program add 5 to each element, which when encoded would add 15, giving $(2, 15, 23, 13)$. To decode this change the original person could multiply each entry by 9 since $3 \cdot 9 = 27 \equiv 1 \pmod{26}$. This gives $(18, 135, 207, 117) \equiv (18, 5, 25, 13)$ (mod 26), which indeed adds 5 to each of the original entries. In principle the second person doesn't need to know the original message because the encryption scheme preserves addition. This is partially homomorphic since multiplication is not preserved. ♢

Kernels, Cosets, and Lagrange's Theorem. Besides their connection with modular arithmetic, homomorphisms generalize linear transformations and matrices from linear algebra, as Example 3 indicated. We consider related ideas, starting with the kernel or null space of a linear transformation. We state definitions and Theorems 2.4.2–2.4.7 for groups, but they apply equally to the additive operation of a ring since rings are groups. Theorem 2.4.8 will consider kernels for rings and fields. In addition to subspaces in linear algebra, other sets, effectively parallel to subspaces, play a useful role, clustering together solutions of systems. Cosets, the corresponding objects in groups, function in similar ways. They will lead to Lagrange's theorem, Theorem 2.4.4, a vital result counting things in groups. This theorem is the finite analogue to theorems about dimensions in linear algebra.

Definition (Kernel)**.** For groups A and B, the *kernel* of a homomorphism $\sigma : A \to B$ is the set $\ker(\sigma) = \{ a \in A : \sigma(a) = e_B \}$. If A and B are rings, $\ker(\sigma) = \{ a \in A : \sigma(a) = 0_B \}$.

By part (ix) of Theorem 2.4.1, the kernel of a group homomorphism is a subgroup since the identity of the image forms a subgroup. We use matrices to represent linear transformations and also systems of equations to solve. The solutions of the homogeneous system $M\vec{x} = \vec{0}$ form the kernel $\ker(M)$ when we think of M as a linear transformation. The solutions of a related nonhomogeneous system $M\vec{x} = \vec{b}$ come from translations of one such solution $\vec{a}$ by vectors from the kernel: if $M\vec{v} = \vec{0}$, then $M(\vec{a}+\vec{v}) = M\vec{a}+M\vec{v} = \vec{b}+\vec{0} = \vec{b}$. Theorem 2.4.2 and the definition of cosets generalize this idea. Nonabelian groups require the distinction in the definition between left and right cosets, illustrated in Example 13.

Theorem 2.4.2. *Let σ be a homomorphism from a group G to a group H. For all x, $y \in G$, $\sigma(x) = \sigma(y)$ if and only if there is some $k \in \ker(\sigma)$ so that $xk = y$. Also $\ker(\sigma)$ is a subgroup. A homomorphism σ is one-to-one if and only if $\ker(\sigma) = \{e_G\}$, the identity of G.*

Proof. Let $x, y \in G$.

($\Rightarrow$) Suppose that $\sigma(x) = \sigma(y)$. Pick $k = x^{-1}y$. Then $xk = y$ and $\sigma(k) = \sigma(x)^{-1}\sigma(y) = \sigma(x)^{-1}\sigma(x) = e_H$. Thus $k \in \ker(\sigma)$.

($\Leftarrow$) Suppose that $k \in \ker(\sigma)$ and $xk = y$. Then $\sigma(y) = \sigma(xk) = \sigma(x)\sigma(k) = \sigma(x)e_H = \sigma(x)$. For the rest see Exercise 2.4.21. □

Definition (Coset). For H a subgroup of a group G and $g \in G$, the *left coset* of g is $gH = \{ gh : h \in H \}$. The *right coset* is $Hg = \{ hg : h \in H \}$. If G is abelian and the operation is $+$, we write $g + H = \{ g + h : h \in H \}$ for the left coset and $H + g = \{ h + g : h \in H \}$ for the right coset, which for an abelian group equals the left coset $g + H$.

From Theorem 2.4.2, left cosets of kernels of homomorphisms act just like the solution sets of nonhomogeneous systems of equations. Linear algebra suggests another idea to generalize. Consider a linear transformation τ from a vector space V of dimension n onto W of dimension m with kernel $\ker(\tau)$, which is a subspace of V of dimension k. Then $n = m + k$: the dimension of V equals the sum of the dimension of

W plus the dimension of the kernel of τ. This important result of linear algebra corresponds to Corollary 2.4.6. This corollary comes directly from one of the key theorems of group theory and so much of abstract algebra: Lagrange's theorem, Theorem 2.4.4. It might seem surprising that a counting theorem gives crucial algebraic information, but in John Fraleigh's words, "never underestimate results that count something."

Example 11. Let $K = \{(0,0),(2,1),(0,2),(2,3)\}$, a subgroup of the group $(\mathbb{Z}_4 \times \mathbb{Z}_4, +)$. Its left cosets are $(0,0) + K = K$, $(1,0) + K = \{(1,0),(3,1),(1,2),(3,3)\}$, $(2,0) + K = \{(2,0),(0,1),(2,2),(0,3)\}$, and $(3,0) + K = \{(3,0),(1,1),(3,2),(1,3)\}$. The reader can verify that starting with a different element, say $(3,2)$, will give one of these four left cosets. Also, since $\mathbb{Z}_4 \times \mathbb{Z}_4$ is abelian, its left cosets equal its right cosets. As Theorem 2.4.3 proves in general, the cosets are all the same size as the kernel and any two different cosets are disjoint. Theorem 2.4.4 uses these properties one step further to show that the order of a subgroup must divide the order of the entire group.

We can think of K as the kernel of the homomorphism $\beta : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4$ given by $\beta(x,y) = x + 2y$. In this case we are mapping from a group of sixteen elements onto a group of four elements with each image having four preimages. ◊

Theorem 2.4.3. *For H a subgroup of a group G and $g, j \in G$,*

(i) *$\alpha : gH \to jH$ given by $\alpha(gh) = jh$ is a bijection.*

(ii) *$gH \cap jH = \emptyset$ or $gH = jH$.*

(iii) *$j \in gH$ if and only if $g^{-1}j \in H$.*

Proof. See Exercise 2.4.22 for parts (i) and (iii). To prove part (ii), if $gH \cap jH = \emptyset$, we are done. So suppose that $k \in gH \cap jH$. That is, there are $h_1, h_2 \in H$ so that $k = gh_1 = jh_2$. Then $g = jh_2h_1^{-1} \in jH$. For any $gh \in gH$, we have $gh = jh_2h_1^{-1}h$, showing $gH \subseteq jH$. The other inclusion is similar. □

Theorem 2.4.4 (Lagrange's theorem, 1770). *If H is a subgroup of a finite group G, then $|H|$, the order of H, divides $|G|$, the order of G.*

Proof. By part (i) of Theorem 2.4.3 the left cosets of H are all the same size: $|H| = |gH|$. Further, the left cosets do not overlap by part (ii) of Theorem 2.4.3. Since $g \in gH$, $G = \bigcup_{g \in G} gH$. If there are k left cosets, $|G| = k\,|H|$. □

Since the order of a subgroup divides the order of the group in Lagrange's theorem, we can ask what their quotient $|G| \,/\, |H|$ tells us. As Example 12 indicates, homomorphisms suggest a use for this number, which we call the *index*.

Example 12. The group $\mathbb{Z}_4 \times \mathbb{Z}_4$ with sixteen elements has the two element subgroup $H = \{(0,0),(0,2)\}$. Then H has eight disjoint cosets, each with two elements. For instance $(1,3) + H = \{(1,3),(1,1)\}$ and $(2,2) + H = \{(2,2),(2,0)\}$. The homomorphism $\gamma : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4 \times \mathbb{Z}_2$ given by $\gamma(x,y) = (x,\overline{y})$, where $\overline{y} \equiv y \pmod 2$ has H for its kernel. Further, the image has eight elements, which match with the eight cosets. The order of the original group is the product of the size of the kernel times the size of the image. This relationship corresponds to the property of linear transformations that the dimension of the original vector space equals the dimension of the kernel plus the dimension of the image. ◊

Definition (Index). The *index* of a subgroup H of a group G is the number of its left cosets, provided the number is finite. We write $[G : H]$ for the index.

Corollary 2.4.5. *In a finite group, the order of an element divides the order of the group.*

Proof. Apply Theorem 2.4.4 to the subgroup $\langle a \rangle$ for an element a. □

Corollary 2.4.6. *If $\sigma : G \to J$ is a group homomorphism onto J, for all $g, h \in G$, $\sigma(g) = \sigma(h)$ if and only if $h \in g\ker(\sigma)$. If G is finite, then $|G| = |J| \cdot |\ker(\sigma)|$.*

Proof. See Exercise 2.4.23. □

Example 13. In $\mathbf{D}_3$ the subgroup $H = \{I, M_1\}$ has left cosets $IH = H$, $RH = \{R, M_2\} = M_2H$, and $R^2H = \{R^2, M_3\} = M_3H$. These do not all match right cosets: $HI = H$, $HR = \{R, M_3\}$, and $HR^2 = (R^2, M_2\}$, requiring the distinction between right and left. However, the left and right cosets of $K = \{I, R, R^2\}$ do match: $IK = K = KI$ and $M_1K = \{M_1, M_2, M_3\} = KM_1$. In both cases 6, the order of $\mathbf{D}_3$, is the product of the order of the subgroup and its index, which is the number of right cosets as well as left cosets. ◊

Theorem 2.4.7. *For groups G and K, $g \in G$, and $\sigma : G \to K$ a homomorphism, $g\ker(\sigma) = \ker(\sigma)g$. That is, the left and right cosets of the kernel are equal.*

Proof. See Exercise 2.4.24. □

While kernels of group homomorphisms are subgroups, as a consequence of Theorem 2.4.7 and Example 13, not every subgroup can be a kernel of a homomorphism. We'll explore the distinction more carefully in Section 3.6. Similarly in Chapter 4 we'll explore the distinction between subrings and kernels of ring homomorphisms suggested by Theorem 2.4.8 and Example 14.

Theorem 2.4.8. *Suppose that $\phi : S \to T$ is a ring homomorphism.*

(i) $\ker(\phi)$ *is a subring of S.*

(ii) *If $s \in S$ and $a \in \ker(\phi)$, then sa and as are in* $\ker(\phi)$.

(iii) *If S is a ring with unity* 1, *and* $1 \in \ker(\phi)$, *then* $\ker(\phi) = S$.

(iv) *If S is a field, then* $\ker(\phi)$ *is either S or* $\{0\}$.

Proof. See Exercise 2.4.26. □

Example 14. The rationals have numerous subrings, including $\mathbb{Z}$, $3\mathbb{Z} = \{\, 3z : z \in \mathbb{Z} \,\}$, and $\{\, j2^k : j, k \in \mathbb{Z} \,\}$. However, by Theorem 2.4.8(iv), only $\{0\}$ and all of $\mathbb{Q}$ can be kernels. In contrast, every subring of the integers is of the form $k\mathbb{Z} = \{\, kz : z \in \mathbb{Z} \,\}$, where $k \in \mathbb{N}$, which is the kernel of the homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_k$ of Example 1. (As we will see in Section 3.1, the sets $k\mathbb{Z}$ are the only subgroups of $\mathbb{Z}$, so they are the only subrings.) ◊

Exercises

2.4.1. (a) For groups G and H define $\alpha : G \to H$ by $\alpha(g) = e_H$. Prove that α is a homomorphism.

(b) If G and H are rings, so that $e_H = 0$, is α from part (a) a ring homomorphism?

(c) What happens in part (b) if G and H are fields?

2.4.2. For complex numbers $a+bi$ and $c+di$ verify that $|a+bi| \cdot |c+di| = |ac - bd + (ad+bc)i|$. Explain why this shows that the modulus is a homomorphism from $\mathbb{C}$ to $\mathbb{R}_{\geq 0}$, using multiplication for both.

2.4.3. Let $\mathbb{R}[x]$ be the ring of all polynomials on $\mathbb{R}$, the real numbers.

(a) ⋆ Define $\beta : \mathbb{R}[x] \to \mathbb{R}$ by $\beta(f) = f(0)$, the value of the function f at 0. Prove that β is a ring homomorphism. What is the kernel of β? What is the left coset (under addition) of $f(x) = x^2 + 3$ for the subgroup $\ker(\beta)$?

(b) Repeat part (a) for $\gamma : \mathbb{R}[x] \to \mathbb{R}$ defined by $\gamma(f) = f(7)$.

2.4.4. (a) Prove that $\delta : \mathbb{R}[x] \to \mathbb{R}[x]$ given by $\delta(g) = g'$, the derivative of g, is a homomorphism for addition. What is the kernel of δ? What is the left coset of $g(x) = x^3 + 2x$ for $\ker(\delta)$?

(b) ⋆ Show with examples that δ from part (a) is not a homomorphism for function multiplication or function composition.

(c) Define $\lambda : \mathbb{R}[x] \to \mathbb{R}[x]$ by $\lambda(g) = \int g(x)dx = k(x)$, where k is the antiderivative of g so that $k(0) = 0$. Prove that λ is a homomorphism for addition. What is the kernel of λ? What is the left coset of $g(x) = 3x^2 - 2x + 1$ for $\ker(\lambda)$?

(d) Show with examples that λ from part (c) is not a homomorphism for function multiplication or function composition.

2.4.5. (a) In Example 1, what is the kernel of α? What is the left coset of 1 for $\ker(\alpha)$?

(b) Repeat part (a) for Example 4 with $k \neq 0$. What happens if $k = 0$?

(c) Repeat part (a) for Example 6 for $\alpha : \mathbb{Z}_{jk} \to \mathbb{Z}_k$.

(d) In Example 8 what is the kernel of μ? Describe geometrically the left cosets of $\ker(\mu)$. *Note.* The operation is multiplication.

(e) Repeat part (d) for α, where the operation is addition.

2.4.6. Let $M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$ and $J = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$, let M be linear transformation from V to W, and let J be a linear transformation from X to Y.

(a) Give the dimensions of V, W, X, and Y.

(b) ⋆ Find the kernels $\ker(M)$ and $\ker(J)$.

(c) ⋆ Find the left coset of $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ for M and of $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ for J.

(d) Determine whether M is one-to-one. Repeat for J.

(e) Determine whether M is onto. Repeat for J.

(f) For M^T and J^T, the transposes of M and J, respectively, determine their domains, codomains, kernels and whether they are one-to-one or onto.

2.4.7. (a) In $(\mathbb{Z}_9, +)$, find the left cosets of $H = \{0, 3, 6\}$.

(b) In $(\mathbb{Z}_{15}, +)$, find the left cosets of $H = \{0, 5, 10\}$.

(c) In $(\mathbb{Z}_{15}, +)$, find the left cosets of $H = \{0, 3, 6, 9, 12\}$.

(d) In $(\mathbb{Z}_{pq}, +)$, describe the left cosets of $H = \{0, p, 2p, \dots, (q-1)p\}$.

2.4.8. (a) In $(\mathbb{Z}_6 \times \mathbb{Z}_4, +)$, find the left cosets of $H = \{(0,0), (3,0), (0,2), (3,2)\}$.

(b) In $(\mathbb{Z}_6 \times \mathbb{Z}_4, +)$, find the left cosets of $K = \{(0,0), (2,0), (4,0), (0,2), (2,2), (4,2)\}$.

2.4.9. (a) In $\mathbf{D}_4$ find the left cosets of $K = \{I, R^2\}$. Verify that they equal the right cosets of K. (See Table 1.6.)

(b) ⋆ In $\mathbf{D}_4$ find the left cosets of $H = \{I, M_1\}$. Find the right cosets of H.

(c) In $\mathbf{D}_4$ find the left and right cosets of $J = \{I, M_1, M_3, R^2\}$.

2.4.10. (a) In $\mathbf{D}_3 \times \mathbb{Z}_2$ find the left cosets of $K = \{(I,0), (R,0), (R^2,0)\}$. Verify that they equal the right cosets of K. (See Table 1.5.)

(b) In $\mathbf{D}_3 \times \mathbb{Z}_2$ find the left cosets of $H = \{(I,0), (M_1,0)\}$. Find the right cosets of H.

(c) In $\mathbf{D}_3 \times \mathbb{Z}_2$ find the left cosets of $J = \{(I,0), (M_1,0), (I,1), (M_1,1)\}$. Find the right cosets of J.

2.4.11. (a) For $M \in M_2(\mathbb{R})$, the 2×2 matrices, $\mathrm{tr}(M)$, the *trace* of M is the sum of the elements on the main diagonal. Prove that $\mathrm{tr} : M_2(\mathbb{R}) \to \mathbb{R}$ is a homomorphism for addition.

(b) Give $\ker(\mathrm{tr})$ and describe its cosets.

(c) Is tr a homomorphism for multiplication? If so, prove it; if not, give a counterexample.

(d) For $M \in M_2(\mathbb{R})$, $\det(M)$ is the determinant of M, a real number. Is $\det : M_2(\mathbb{R}) \to \mathbb{R}$ a homomorphism for addition? If so, prove it; if not, give a counterexample.

(e) Repeat part (d) for matrix multiplication and multiplication in $\mathbb{R}$.

Remark. The answers for parts (a), (c), (d), and (e) generalize to $n \times n$ matrices.

2.4.12. Prove in Example 7 that $\phi_c : F[x] \to F$ is a homomorphism.

2.4.13. Make and justify a conjecture about a subgroup H of a general group G for when left cosets equal to right cosets.

2.4.14. (a) For rings S and T prove that $\rho : S \times T \to S$ given by $\sigma((s,t)) = s$ is a homomorphism.

(b) Give $\ker(\sigma)$ for σ in part (a) and describe its cosets.

(c) Repeat parts (a) and (b) for $\tau : S \times T \to T$ given by $\tau((s,t)) = t$.

(d) For a ring S define $\phi : S \times S \to S$ by $\phi(a,b) = a + b$. Is ϕ a homomorphism for addition? If so, prove it and give its kernel; if not, give a counterexample.

(e) Is ϕ in part (d) homomorphism for multiplication? If so, prove it; if not, give a counterexample.

2.4.15. Let S be a commutative ring with unity and define $\psi : S \to S$ by $\psi(x) = kx$. Prove that ψ is a ring homomorphism if and only if k is idempotent. That is, $k^2 = k$.

2.4.16. ⋆ If p is a prime and $k \neq 0$ for $k \in \mathbb{Z}_p$, prove that $\langle k \rangle = \mathbb{Z}_p$.

2.4.17. Prove that a group with a prime number of elements is cyclic.

2.4.18. Suppose G is a group with n elements. Prove for all $g \in G$ that $g^n = e$. Does this mean that the order of every element is n? Explain.

2.4.19. Let G be a group with subgroups H and J.

(a) How is the coset $a(H \cap J)$ related to the intersection of the cosets aJ and coset aH? Justify your answer.

Suppose for the rest of this problem that G is finite and $H \cap J = \{e\}$.

(b) ⋆ Give an example where the number of left cosets of H equals the size of J.

(c) Give an example where the number of left cosets of H is greater than the size of J. Must the number of left cosets of J be greater than the size of H in this case? Justify your answer.

(d) Can the number of left cosets of H ever be less than the size of J when $H \cap J = \{e\}$? Justify your answer.

2.4.20. Prove the remaining parts of Theorem 2.4.1.

2.4.21. Prove the rest of Theorem 2.4.2.

2.4.22. (a) Prove the remaining parts of Theorem 2.4.3.

(b) Modify Theorem 2.4.3. for right cosets, and prove this modification.

2.4.23. (a) Prove Corollary 2.4.6.

(b) In Corollary 2.4.6 show that $\sigma(g) = \sigma(h)$ if and only if $h \in \ker(\sigma)g$.

2.4.24. Prove Theorem 2.4.7.

2.4.25. Let $\sigma : S \to T$ be a ring homomorphism onto T. If $\ker(\sigma) = \{0\}$, prove that σ is an isomorphism.

2.4.26. Prove Theorem 2.4.8.

2.4.27. Suppose for a subgroup H of a group G that $aH = bH$. Must $Ha = Hb$? If so, prove it; if not, give a counterexample.

2.4.28. Suppose $\alpha : \mathbb{Z}_n \to \mathbb{Z}_k$ is a group homomorphism for addition.

(a) Explain why the value of $\alpha(1)$ determines all values $\alpha(j)$.

(b) Use part (a) to determine all homomorphisms from $\mathbb{Z}_4$ to $\mathbb{Z}_4$.

(c) Repeat part (b) for homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_4$.

(d) Repeat part (b) for homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{12}$.

(e) Use part (a) and Theorem 2.4.1 to determine all homomorphisms from $\mathbb{Z}_4$ to $\mathbb{Z}_{12}$.

(f) Which of the homomorphisms in part (d) are isomorphisms?

(g) Generalize your answers in parts (b) through (e), and justify your answers.

(h) When is a group homomorphism $\alpha : \mathbb{Z}_n \to \mathbb{Z}_k$ also a ring homomorphism?

2.4.29. (a) Prove that onto group homomorphisms satisfy the reflexive property: for any group X there is a homomorphism from X onto X.

(b) Prove that onto group homomorphisms satisfy a transitive-like property: for any groups X, Y, and Z, if there is a homomorphism from X onto Y and a homomorphism from Y onto Z, then there is a homomorphism from X onto Z.

(c) Show with a counterexample that onto group homomorphisms do not satisfy the symmetric property: for all groups X and Y, if $\alpha : X \to Y$ is a homomorphism onto Y, then there does not need to be a homomorphism from Y onto X.

(d) Show with a counterexample that onto group homomorphisms do not satisfy the antisymmetric property: for any groups X and Y, if $\alpha : X \to Y$ is a homomorphism onto Y and $\beta : Y \to X$ is a homomorphism from Y onto X, then $X = Y$.

(e) Show that onto group homomorphisms satisfy a modified antisymmetric property for finite groups: for any finite groups X and Y, if $\alpha : X \to Y$ is a homomorphism onto Y and $\beta : Y \to X$ is a homomorphism from Y onto X, then X and Y are isomorphic. *Remark.* The finite condition is necessary in part (e). See Project 2.P.4 for an example.

2.4.30. Suppose that G is a group whose only subgroups are G and $\{e\}$.

(a) First prove that G is cyclic, then prove that G is finite.

(b) What can you say about $|G|$ in this case? Prove your answer.

2.4.31. (a) For T a subring of a ring S and $a, b \in S$, define $a \sim_T b$ if and only if there is $t \in T$ so that $a + t = b$. Show that $\sim_T$ is an equivalence relation on S.

(b) Similar to part (a) define $a \bowtie_T b$ if and only if there is $t \in T$ so that $at = b$. Is $\bowtie_T$ always an equivalence relation? If so prove it; if not, for for each property that can fail, provide a counterexample. If not, also state conditions on S and T so that $\bowtie_T$ is an equivalence relation.

2.4.32. Let $\mathbb{H}(G)$ be the set of all group homomorphisms from an abelian group $(G, +)$ to itself. Define the operations $+$ and $\circ$ on $\mathbb{H}(G)$ by $(\alpha + \beta)(x) = \alpha(x) + \beta(x)$ and $(\alpha \circ \beta)(x) = \alpha(\beta(x))$, where $\alpha, \beta \in \mathbb{H}(G)$ and $x \in G$.

(a) Use Exercise 2.4.28(b) to describe $\mathbb{H}(\mathbb{Z}_4)$.

(b) Use Exercise 2.4.28(d) to describe $\mathbb{H}(\mathbb{Z}_{12})$.

(c) Prove that $+$ and $\circ$ are operations on $H(G)$. That is, for $\alpha, \beta \in \mathbb{H}(G)$, prove that $\alpha + \beta$ and $\alpha \circ \beta$ are homomorphisms in $\mathbb{H}(G)$.

(d) Is $(\mathbb{H}(G), +)$ a group? Is $(\mathbb{H}(G), +, \circ)$ a ring? Prove or provide a counterexample.

(e) If G is a ring, and α and β are ring homomorphisms, is $\alpha + \beta$ a ring homomorphism? Prove or provide a counterexample.

(f) Repeat part (e) for $\alpha \circ \beta$.

(g) If G is a ring and α and β are ring homomorphisms, try to define $\cdot$ on $\mathbb{H}(G)$ by $\alpha \cdot \beta(x) = \alpha(x) \cdot \beta(x)$. Show by an example that this is not always a ring homomorphism. *Remark.* Homomorphisms of an algebraic system to itself are called endomorphisms.

Joseph-Louis Lagrange. Both Italy and France lay claim to Joseph-Louis Lagrange (1736–1813), one of the great mathematicians of his day. Until age 30 Lagrange lived in Turin, Italy. In those years he impressed Euler and other leading mathematicians with his results in physics, calculus, and more advanced areas of analysis, such as differential equations and the calculus of variations. He was elected to the Berlin Academy at age 20 and mathematicians from there tried to entice him more than once to come to Berlin. At age 30 he finally agreed and spent twenty productive years there. He continued publishing in his earlier areas and added number theory and algebra.

In 1770 Lagrange published a seminal paper in algebra, including what we now call Lagrange's theorem (Theorem 2.4.4). This was decades before the concept of a group occurred to mathematicians, but the patterns Lagrange elucidated pushed mathematicians toward the modern approach to algebra. This paper gave a deep analysis of why the quadratic formula and those for the third- and fourth-degree equations worked. Lagrange focused on permutations of the roots of the equations. As we will see in Sections 3.5 and 3.7, permutations form groups, but their structure is much more complicated than the other examples of the time, such as $\mathbb{Z}_n$. However, as later mathematicians proved, permutation groups and Lagrange's approach were the key to proving the inability to find a general formula for fifth-degree equations.

In 1787 just prior to the French Revolution, Lagrange moved to Paris, where he spent the rest of his life as the leading mathematician of France and one of the greatest in all of Europe. His famous work *Mécanique analytique* gave a completely mathematical foundation for physics, based on algebra and calculus. He narrowly avoided the purges of the Reign of Terror of the French Revolution in 1793, even though he was a foreigner and other equally renowned scientists were sentenced to death. The next year the revolutionary government founded the École Polytechnique, which quickly became the pre-eminent education and research institution of France. Lagrange was its first mathematics professor while continuing his research. He had avoided teaching for decades, but had no choice under the new regime. His students apparently found him a poor teacher.

Historical Reflection. As often happens in mathematics, the pedagogical order of presentation doesn't reflect the historical order. We give credit to Lagrange for "Lagrange's theorem," even if he couldn't have recognized how we state it today. The general definitions of groups, subgroups, and cosets coalesce around 100 years after Lagrange's insights. Évariste Galois (1811–1832) proved deep results we discuss in Sections 5.3 to 5.7 connecting what we now call groups and fields. But the concept of a field comes into focus even more slowly than groups. In 1871 Richard Dedekind (1831–1916) defined fields in the context of subfields of the reals and complexes. A general abstract definition had to wait until 1893. The idea of a direct product also emerges slowly from coordinates in two and more dimensions around the same time. Similarly, the term "homomorphism" and the general concept of it seem to date from 1892 when Felix Klein (1849–1925) introduced it. But in 1870 Camille Jordan (1838–1922) proved a version of a theorem we now state using homomorphisms (Theorem 3.6.5). The modern version of it needed to wait over 50 years until the work of Emmy Noether (1882–1935). She fit the full range of ideas of abstract algebra into the modern coherent whole we see today, and she proved a number of results.

Supplemental Exercises

2.S.1. We define the operation $*$ on the set $\mathbb{R} \times \{1, -1\}$ by $(a, b) * (c, d) = (a + bc, bd)$.

(a) Show that $(0, 1)$ is an identity for $*$.

(b) Find the inverse of each element. *Hint.* Consider $(a, 1)$ separately from $(a, -1)$.

(c) Prove that this operation gives a group.

(d) Explain why this group could be considered the "dihedral group of a line."

2.S.2. (a) Give an example of three subgroups of a group G so that none is a subgroup of the others but their union is a subgroup.

(b) Repeat part (a) with four subgroups.

(c) Repeat part (a) with $p + 1$ subgroups, where p is a prime.

(d) Repeat part (a) with infinitely many subgroups.

(e) Show that there is no group with two subgroups satisfying the condition in part (a).

2.S.3. (a) A nonempty collection of subsets $\{A_i : i \in I\}$ is a "chain" of a set G if and only if for all $i, k \in I$, $A_i \subseteq A_k$ or $A_k \subseteq A_i$. If $\{A_i : i \in I\}$ is a chain of subgroups of a group G, prove that $\bigcup_{i \in I} A_i$ is a subgroup of G. (Do not assume that the union is one of the A_i.)

(b) Does your argument in part (a) extend to chains of subrings? Subfields? Justify your answers.

2.S.4. (a) Let G be an abelian group, and let $H_2 = \{g \in G : g^2 = e\}$. Show that H_2 is a subgroup of G.

(b) If we replace H_2 in part (a) by $H_n = \{g \in G : g^n = e\}$, for $n \in \mathbb{N}$, do we still get a subgroup? Prove or give a counterexample.

(c) Let H be the subset of all elements of G of finite order, where G is abelian. If we replace H_2 in part (a) by H, do we still get a subgroup? Prove or give a counterexample.

(d) If we drop the condition that G is abelian, is H_2 always a subgroup? Prove or give a counterexample.

(e) Repeat part (d) replacing H_2 with H from part (c).

2.S.5. We consider an alternative multiplication $*_b$ on $(\mathbb{Z}_n, +)$.

(a) For $b \in \mathbb{Z}_n$, define $1 *_b 1 = b$. Assume that $*_b$ distributes over $+$ and show that for all $j, k \in \mathbb{Z}_n$, $1 *_b k = bk$ and $j *_b k = bjk$.

(b) Explain why $(\mathbb{Z}_n, +, *_b)$ is a commutative ring.

(c) For which b in $\mathbb{Z}_3$, does $(\mathbb{Z}_3, +, *_b)$ have a unity? For this (or these) b, is $(\mathbb{Z}_3, +, *_b)$ a field?

(d) Repeat part (c), replacing 3 with 4.

(e) Repeat part (c), replacing 3 with 5.

(f) Repeat part (c), replacing 3 with 6.

(g) Make a conjecture about when $(\mathbb{Z}_n, +, *_b)$ is a ring with unity and when it is a field.

2.S.6. We consider trying to define a multiplication $*$ that distributes over composition in $\mathbf{D}_3$, the smallest nonabelian group.

(a) What does $M_i \circ M_i = I$ and distributivity tell us about $R * M_i$?

(b) Repeat part (a) using the equation $R \circ R \circ R = I$.

(c) What do parts (a) and (b) imply?

Remark. This illustrates why we require the addition in a ring to be abelian.

2.S.7. Do the following steps to show that the center of $\mathrm{GL}(2, \mathbb{R})$, the group of 2×2 invertible real matrices, is $\{ rI : r \in \mathbb{R} \}$, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, the identity under multiplication.

(a) If $b \neq 0$ in $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, find a 2×2 matrix W so that $MW \neq WM$.

(b) Repeat part (a), where $c \neq 0$.

(c) Repeat part (a), where $b = 0 = c$ and $a \neq d$.

2.S.8. Define the operation $\ominus$ on $\mathbb{Z}$ by $x \ominus y = |x - y|$. For which $n \in \mathbb{N}$ is the mapping $\alpha : \mathbb{Z} \to \mathbb{Z}_n$ given by $\alpha(z) = r$, where $z \equiv r \pmod{n}$ from Example 1 of Section 2.4 a homomorphism for some appropriate operation $\triangle$ in $\mathbb{Z}_n$? Explain.

Projects

2.P.1. **Cancellation.** Suppose for groups G, H and J that $G \times H \approx J \times H$. The cancellation property of ordinary multiplication suggests that $G \approx J$.

(a) Investigate cancellation for direct products with finite abelian groups. Give a proof or a counterexample.

(b) Extend the investigation of part (a) to other finite groups.

(c) Give a proof or a counterexample for the following conjecture.

Conjecture. *If G, H, and J are finite groups and $G \times H \approx J \times H$, then $G \approx J$.*

(d) Show that cancellation fails in general for direct products of groups. *Hint.* Use the set $\mathbb{R}^{\mathbb{N}}$ of all sequences of real numbers, which forms a group under component-wise addition. Calculus and analysis study the limits of sequences of real numbers $(a_n) = (a_1, a_2, a_3, \dots)$, but we don't consider limits here.

2.P.2. **Subgroups and subrings.**

(a) Determine the number of subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$, where p is a prime and describe them.

(b) Explain why in part (a) $\mathbb{Z}_p \times \mathbb{Z}_p$, considered as a ring, has exactly five subrings.

(c) Repeat part (a) for $\mathbb{Z}_n \times \mathbb{Z}_n$, where $n \in \mathbb{N}$. Determine its subrings.

(d) Generalize part (c) to $\mathbb{Z}_n \times \mathbb{Z}_k$, where $n, k \in \mathbb{N}$.

(e) Generalize parts (a), (c), and (d) for direct products of three or more cyclic groups.

2.P.3. **Multiplications on $\mathbb{R} \times \mathbb{R}$.** For $j, k \in \mathbb{R}$, define an alternative multiplication $*$ on $(\mathbb{R} \times \mathbb{R}, +)$ by $(a, b) * (c, d) = (ac + jbd, ad + bc + kbd)$. Assume that $*$ is always associative and distributes over $+$.

(a) Prove if $j = -1$ and $k = 0$, then $(\mathbb{R} \times \mathbb{R}, +, *)$ is isomorphic to the complex numbers.

(b) Prove for all $j, k \in \mathbb{R}$ that $(\mathbb{R} \times \mathbb{R}, +, *)$ is a commutative ring with unity.

(c) When $j = 1$ and $k = 0$, this ring is called the "split-complex numbers", which we'll denote $\mathbb{R} \times \mathbb{R}^S$. It has been used in studying the special theory of relativity. Show that $\mathbb{R} \times \mathbb{R}^S$ has zero divisors and characterize its zero divisors. (From Project 1.P.2 of Chapter 1, a nonzero element x is a *zero divisor* if and only if there is a nonzero element y so that $xy = 0$.)

(d) Some mathematicians have modelled rings with *infinitesimals*, elements infinitely close to 0 by choosing $j = 0 = k$. In this ring, denoted $\mathbb{R} \times \mathbb{R}^I$, the elements $(0, b)$ are the infinitesimals and (a, b) and (a, c) are infinitely close to one another. Show that $(a, b) + (c, d)$ is infinitely close to $(a, 0) + (c, 0)$ and $(a, b) * (c, d)$ is infinitely close to $(a, 0) * (c, 0)$. Describe all zero divisors in $\mathbb{R} \times \mathbb{R}^I$.

(e) Determine conditions on j and k so that $(\mathbb{R} \times \mathbb{R}, +, *)$ has zero divisors.

(f) Determine conditions on j and k so that $(\mathbb{R} \times \mathbb{R}, +, *)$ is isomorphic to $\mathbb{C}$.

(g) Are there values of j and k besides those covered in parts (e) and (f)?

(h) Investigate which values of j and k give rings $(\mathbb{R} \times \mathbb{R}, +, *)$ with zero divisors that are isomorphic to $\mathbb{R} \times \mathbb{R}^S$ or $\mathbb{R} \times \mathbb{R}^I$ (or both).

(i) Prove your answers.

2.P.4. **Homomorphisms as a "partial" partial order.** From Exercise 2.4.29(e) onto group homomorphisms satisfy a modified antisymmetric property for finite groups: for any finite groups X and Y, if $\alpha : X \to Y$ is a homomorphism onto Y and $\beta : Y \to X$ is a homomorphism from Y onto X, then X and Y are isomorphic. Use a direct product of infinitely many finite cyclic groups to show that the property in part (e) does not hold for infinite groups. *Hint.* Use groups of different orders in the product.

2.P.5. **Finite complex-like rings.** We define a multiplication on the group $(\mathbb{Z}_n \times \mathbb{Z}_n, +)$ as in the complex numbers: $(a, b) \odot (c, d) = (ac - bd, ad + bc)$. Assume that $(\mathbb{Z}_n \times \mathbb{Z}_n, +, \odot)$ is a commutative ring with unity $(1, 0)$.

(a) Verify that $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, \odot)$ is a field. Note that you only need to find inverses for all nonzero elements.

(b) If n is not a prime, show that $(\mathbb{Z}_n \times \mathbb{Z}_n, +, \odot)$ is not a field.

(c) Show that $(\mathbb{Z}_5 \times \mathbb{Z}_5, +, \odot)$ is not a field.

(d) Determine whether $(\mathbb{Z}_7 \times \mathbb{Z}_7, +, \odot)$ is a field. Prove your answer.

(e) Repeat part (d) for $(\mathbb{Z}_p \times \mathbb{Z}_p, +, \odot)$ for some other primes p and make a conjecture about what values of p give fields.

(f) For values of n for which $(\mathbb{Z}_n \times \mathbb{Z}_n, +, \odot)$ is not a field, investigate which subgroups $\langle (a, b) \rangle$ are subrings as well.

(g) On $\mathbb{Z}_n \times \mathbb{Z}_n$ define an alternative multiplication by $(a, b) \otimes (c, d) = (ac + 2bd, ad + bc)$. Is $(\mathbb{Z}_5 \times \mathbb{Z}_5, +, \otimes)$ a field? Prove your answer. Are there other primes p for which $(\mathbb{Z}_p \times \mathbb{Z}_p, +, \otimes)$ a field?

(h) On $\mathbb{Z}_n \times \mathbb{Z}_n$ define an alternative multiplication by $(a, b) \circledast (c, d) = (ac + kbd, ad + bc)$, for $k \in \mathbb{Z}_n$. Investigate for various primes p which values of k give a field. Make a conjecture.