# Algebra I: Chapter 3. Group Theory

## 3.1 Groups.

A **group** is a set $G$ equipped with a binary operation mapping $G \times G \to G$. Such a "product operation" carries each ordered pair $(x, y)$ in the Cartesian product set $G \times G$ to a group element which we write as $x \cdot y$, or simply $xy$. The product operation is required to have the following properties.

G.1 Associativity: $(xy)z = x(yz)$ for all $x, y, z \in G$.

This insures that we can make sense of a product $x_1 \cdot \cdots \cdot x_n$ involving several group elements without inserting parentheses to indicate how elements are to be combined two at a time. However, *the order in which elements appear in a product is crucial!* While it is true that $x(yz) = xyz = (xy)z$, the product $xyz$ can differ from $xzy$.

G.2 Unit element: There exists an element $e \in G$ such that $ex = x = xe$ for all $x \in G$.

G.3 Inverses exist: For each $x \in G$ there exists an element $y \in G$ such that $xy = e = yx$.

The inverse element $y = y(x)$ in G.3 is called the **multiplicative inverse** of $x$, and is generally denoted by $x^{-1}$. The group $G$ is said to be **commutative** or **abelian** if the additional axiom

G.4 :wq Commutativity: $xy = yx$ for all $x, y \in G$

is satisfied

Our first task is to show that the identity element and multiplicative inverses are uniquely defined, as our notation suggests.

**3.1.1 Lemma.** *In a group $(G, \cdot\,)$ the unit $e$ is unique, and so is $x^{-1}$ for each $x$.*

Proof: Suppose there is another element $e' \in G$ such that $e'x = x = xe'$ for all $x \in G$. Taking $x = e$ we get $e' = e'e = e$ as claimed. Next, let $x \in G$ and suppose $y, y'$ are elements such that $xy' = e = y'x$, $xy = e = yx$. Then look at the product $y'xy$ and apply G.1+G.2 to get

$$y' = y'e = y'(xy) = (y'x)y = ey = y$$

Thus $y' = y$ and every $x$ has a *unique* inverse which we hereafter label $x^{-1}$. □

**3.1.2 Some Examples of Groups.** We write $|G|$ for the number of elements in $G$, which could be $\infty$.

1. $G = \{e\}$. This is the **trivial group** with just one element $e$ such that $e \cdot e = e$. Here $e^{-1} = e$ and $|G| = 1$. Not very interesting. □
2. $G = (\mathbb{Z}, +)$. This is an infinite abelian group; integer addition $(+)$ is the group operation. The unit is $e = 0$, and the inverse of any element $x \in \mathbb{Z}$ is its negative $-x$. □
3. $G = (\mathbb{Z}_n, +)$, the integers (mod $n$) for some $n \in \mathbb{N}$, with addition of congruence classes
$$[x] + [y] = [x + y] \qquad \text{for all } x, y \in \mathbb{Z}$$
as the group operation. This is a finite abelian group with $|G| = n$. The identity element is $[0]$; the inverse of $[k] \in \mathbb{Z}_n$ is the congruence class $[-k] = [n - k]$. □

4. $G = (\mathrm{U}_n, \cdot\,)$, the set of multiplicative units in $\mathbb{Z}_n$. Here we take *multiplication* $[k] \cdot [\ell] = [k\ell]$ as the group operation. Recall that $\mathrm{U}_n$ can also be described as
$$\mathrm{U}_n = \{\, [k] : 0 < k < n \text{ and } \gcd(k, n) = 1 \,\}$$

as explained in 2.5.15. You should also recall the discussion of Section 2.5, where $(\mathbb{Z}_n, +, \cdot\,)$ was defined, to see why the group axioms are satisfied. The proofs are pretty obvious once you observe that the product of two units in $\mathbb{Z}_n$ is again a unit. The identity element in $\mathrm{U}_n$ is $e = [1]$; finding multiplicative inverses $[k]^{-1}$ requires some computation: using the GCD Algorithm we can find $r, s \in \mathbb{Z}$ such that $rk + sn = 1$ in $\mathbb{Z}$. Modulo $n$ we get $[r] \cdot [k] = [1]$ so that $[k]^{-1} = [r]$.

The group $\mathrm{U}_n$ is abelian and finite, but its size $\phi(n) = |\mathrm{U}_n|$ varies erratically as $n$ increases. This cardinality can be computed by hand in each case, but there is a general formula for $\phi(n)$ that depends on the prime factorization of $n$. The function $\phi(n)$ is so important in number theory it has a special name: the **Euler phi function**. □

We will resume our catalog of groups in a moment, but first some exercises you should think about right now.

**3.1.3 Exercise.** In any group, verify directly from the axioms that

(a) $(x^{-1})^{-1} = x$ for all $x$

(b) $(xy)^{-1} = y^{-1}x^{-1}$ for all $x, y \in G$. (Note the reversal here.) □

**3.1.4 Exercise.** Determine the units in $\mathbb{Z}_{14}$ and compute their inverses.
*Hint:* First check that in $\mathbb{Z}_n$ the multiplicative inverse of $[-1] = [n-1]$ is itself; then observe that $[-k] = [-1] \cdot [k]$. This cuts in half the number of inverses you must compute. For numbers this small you can find $r, s$ such that $rk + sn = 1$ by hand. □

**3.1.5 Exercise.** If $p > 1$ is a prime, explain why $|\mathrm{U}_p| = p - 1$.
*Note:* This is one of the few cases in which $\phi(n) = |\mathrm{U}_n|$ is easy to calculate. □

**3.1.6 Exercise.** Decide which of the following systems are groups.

(a) $G = (\mathbb{Z}, \cdot\,)$, the integers with *multiplication* as the binary operation.

(b) $G = (\mathbb{N}, \cdot\,)$, the natural numbers in $\mathbb{Z}$ with *multiplication* as the binary operation.

(c) $G = (\mathbb{N}, +)$, the natural numbers in $\mathbb{Z}$ with *addition* as the binary operation.

(d) $G = (\mathbb{R}, \cdot\,)$, the real numbers with *multiplication* as the binary operation.

(e) $G = (\mathbb{R}^\times_+, \cdot\,)$, the positive real numbers $x > 0$ with *multiplication* as the binary operation.

(f) $G = (\mathbb{C}^\times, \cdot\,)$, the nonzero complex numbers $z \neq 0$ with *multiplication* as the binary operation.

(g) $\mathbb{Z}_n$ with multiplication $[k] \cdot [\ell] = [k \cdot \ell]$ as the binary operation.

(h) $G = (\mathbb{Z}_9^\times, \cdot\,)$, the nonzero integers (mod 9) with *multiplication* $[k] \cdot [\ell] = [k\ell]$ as the binary operation.

(i) The group of units in $\mathbb{Z}_n$
$$\mathrm{U_n} = \{[k] \in \mathbb{Z}_n : 1 \leq j \leq n \text{ and } \gcd(k, n) = 1\}$$
with addition $[k] + [\ell] = [k + \ell]$ as the binary operation.

In each case, if $G$ is not a group which group axiom(s) fail to hold? □

**3.1.7 Examples of groups (continued).**

5. Let $G$ be any vector space $V$, equipped with vector addition as the binary operation. The identity element for this group is the zero vector $\mathbf{0}$, and the inverse of any element $\mathbf{x} \in V$ is its negative $-\mathbf{x} = (-1) \cdot \mathbf{x}$
6. $G = (\mathbb{R}^n, +)$ is a group, being a vector space, but so is the subset $G' = (\mathbb{Z}^n, +)$ of vectors in $\mathbb{R}^n$ with integer coordinates: $\mathbf{x} = (x_1, \ldots, x_n)$ such that $x_i \in \mathbb{Z}$ for $1 \leq i \leq n$.
7. The set $G = (\mathbb{C}, +)$ of *all* complex numbers, equipped with complex addition as the product operation, is a completely different abelian group.
8. The set $G = (\mathbb{C}^\times, \cdot\,)$ of *nonzero* complex numbers $\mathbb{C}^\times = \{z \in \mathbb{C} : z \neq 0 + i0\}$, equipped with multiplication as the product operation, is an abelian group.
9. The **circle group** $G = (S^1, \cdot\,)$ is the set of complex numbers that lie on the unit circle, so $|z| = 1$. This is an abelian group when $S^1$ is equipped with complex multiplication as the product operation because $|zw| = |z|\,|w|$. □

The next few examples are so important they deserve extensive discussion, so we consider them separately.

**Matrix Groups.** $\mathrm{M}(n, \mathbb{F})$ is the set of all $n \times n$ matrices with entries in some field of scalars $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_p$ where $p > 1$ is a prime. This is a vector space, and hence a group under the usual $(+)$ operation for matrices. The additive identity element is the zero matrix, all of whose entries are 0. However, $\mathrm{M}(n, \mathbb{F})$ is *not* a group under the usual matrix product operation $A \cdot B$

$$(A \cdot B)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj} \qquad \text{for all } 1 \leq i, j \leq n$$

Matrix multiply is associative, with $A(BC) = (AB)C$, and there is an identity element such that $IA = A = AI$, namely the $n \times n$ identity matrix, with 1's on the diagonal and zeros elsewhere. But some matrices (those with $\det(A) = 0$) have no multiplicative inverse such that $AA^{-1} = A^{-1}A = I$. Nevertheless, certain subsets of $\mathrm{M}(n, \mathbb{F})$ are groups of great importance in geometry and physics. To define them we must recall two facts.

> **Theorem.** *An $n \times n$ matrix $A$ has an inverse if and only if its determinant is nonzero:* $\det A \neq 0$. *Moreover, there is an explicit algorithm for computing $A^{-1}$ once we know* $\det A$.
>
> **Theorem.** *Determinants are multiplicative:* $\det(AB) = \det(A) \cdot \det(B)$ *and in particular* $\det A^{-1} = 1/\det(A)$ *if* $\det(A) \neq 0$.

**3.1.8 Example (Matrix Groups).** The set $\mathrm{GL}(n, \mathbb{F})$ of $n \times n$ matrices with nonzero determinant, usually referred to as the $n$-dimensional **general linear group** over $\mathbb{F}$, is a group when equipped with matrix multiplication. The identity element is the $n \times n$ identity matrix $I$, and the group inverse of any $A$ is its matrix inverse $A^{-1}$. If the field of scalars $\mathbb{F}$ is infinite the group $\mathrm{GL}(n, \mathbb{F})$ is infinite; it is not commutative unless $n = 1$.

Other classical matrix groups are subgroups of $\mathrm{GL}(n, \mathbb{F})$. To mention just a few:

1. $G = \mathrm{SL}(n, \mathbb{F})$ is the **special linear group** consisting of all $n \times n$ matrices $A$ such that $\det(A) = 1$.
2. $G = \mathrm{O}(n, \mathbb{F})$ is the **orthogonal group** consisting of all $n \times n$ matrices $A$ such that $A^{\mathrm{t}}A = I$, where $A^{\mathrm{t}}$ is the transpose matrix defined by $(A^{\mathrm{t}})_{ij} = A_{ji}$. Then we automatically have $AA^{\mathrm{t}} = I$ and $A^{\mathrm{t}} = A^{-1}$.

$G = \mathrm{SO}(n, \mathbb{F})$ is the **special orthogonal group** consisting of all $n \times n$ matrices $A \in \mathrm{O}(n, \mathbb{F})$ such that det $A = 1$, so that

$$(1) \qquad A \in \mathrm{SO}(n, \mathbb{F}) \;\Leftrightarrow\; A^{-1} = A^{\mathrm{t}} \text{ and } \det(A) = 1$$

An orthogonal matrix $A \in \mathrm{O}(n, \mathbb{F})$ always has determinant $\det(A) = 1$ or $\det(A) = -1$ because

$$1 = \det(I) = \det(A^{\mathrm{t}}A) = \det(A^{\mathrm{t}}) \cdot \det(A) = \big(\det(A)\big)^2$$

and in any field $\mathbb{F}$ the only solutions of the equation $z^2 - 1 = 0$ are $z = \pm 1$.

3. $G = \mathrm{O}(n)$ and $\mathrm{SO}(n)$. Important special cases arise when $\mathbb{F} = \mathbb{R}$. Then the orthogonal group is generally written as $\mathrm{O}(n)$, with the "$\mathbb{R}$" understood. It is not hard to show that the action of $A \in \mathrm{O}(n)$ on vectors in $\mathbb{R}^n$ preserves inner products and Euclidean distances between points

$$(A\mathbf{x}, A\mathbf{y}) = (\mathbf{x}, \mathbf{y}) \qquad \text{and} \qquad \|A\mathbf{x} - A\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|$$

when $\mathbb{R}^n$ is equipped with the usual inner product $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i$ and Euclidean distance function $\|\mathbf{x} - \mathbf{y}\| = \big(\sum_{i=1}^n |x_i - y_i|^2\big)^{1/2}$. Lengths of vectors are also preserved, with $\|A\mathbf{x}\| = \|\mathbf{x}\|$.

The (real) **special orthogonal group** $\mathrm{SO}(n)$ consists of all $n \times n$ real matrices $A \in \mathrm{O}(n)$ with determinant $= 1$.

$$(2) \qquad A \in \mathrm{SO}(n) \;\Leftrightarrow\; AA^{\mathrm{t}} = I \text{ (so } A^{-1} = A^{\mathrm{t}}) \text{ and } \det(A) = 1$$

As above, an orthogonal matrix $A \in \mathrm{O}(n)$ can only have determinant $\det(A) = 1$ or $\det(A) = -1$.

In 3 dimensions the real orthogonal group splits into two pieces $\mathrm{O}(3) = \mathrm{O}^+(3) \cup \mathrm{O}^-(3)$ according to whether det $A = \pm 1$. The negative piece $\mathrm{O}^-(3)$ consists of orientation-reversing transformations and includes reflections across planes theough the origin; it is *not* a subgroup of $\mathrm{O}(3)$ because, for one thing, it does not contain the identity $I$, which has determinant $+1$. We will see below that $\mathrm{O}^+(3) = \mathrm{SO}(3)$ is a subgroup whose elements correspond to the rotations $R_{\ell,\theta}$, by any angle $\theta$ about any oriented axis $\ell$ through the origin (Euler's Theorem 3.1.16). Transformations in $\mathrm{O}^+(3)$ are all orientation-preserving.

4. The **upper triangular group** consists of all $n \times n$ matrices of the form

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{nn} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ 0 & \dots & 0 & a_{nn} \end{bmatrix} \qquad \text{such that} \qquad \begin{cases} \det A = a_{11} \cdots a_{nn} \neq 0 \\ a_{ij} = 0 \text{ for below-diagonal entries} \end{cases}$$

If all the diagonal entries are equal to 1 we get the group of **strictly upper triangular** matrices.

5. The three-dimensional **Heisenberg group** of quantum mechanics consists of all real $3 \times 3$ matrices of the form

$$(3) \qquad A = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \qquad \text{with} \qquad x, y, z \in \mathbb{R}.$$

It plays a cenrtral role in Quantum Mechanics.

Other matrix groups will be mentioned later. □

**3.1.9 Exercise.** In the last two examples above, verify that each set of matrices is actually a group by checking that:

(a) The product of two such matrices has the same form.

(b) The inverse $A^{-1}$ of any such matrix has the proper form.

*Hint:* Start with the Heisenberg group, which is easier. Recall Cramer's formula for computing $A^{-1}$ in terms of subdeterminants. □

**3.1.10 Exercise.** Show that $\mathrm{SL}(2,\mathbb{R})$ is not commutative by producing two matrices such that $AB \neq BA$. □

**3.1.11 Exercise.** Suppose $H$ is a nonempty subset of $\mathrm{GL}(n,\mathbb{F})$ such that

(a) $I \in H$ (b) $A, B \in H \Rightarrow AB \in H$ (c) $A \in H \Rightarrow A^{-1} \in H$

Prove $H$ is a group when equipped with matrix multiply as its product operation. □

**Transformation Groups.** Many important groups are made up of bijective maps (transformations) $T : X \rightarrow X$ of some point set $X$. For example the $n$-dimensional group of **rigid motions** $\mathrm{M}(n)$ on Euclidean space $\mathbb{R}^n$ consists of all bijections $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ that preserve the usual Euclidean distance between points

$$\|\mathbf{x} - \mathbf{y}\| = \Big[\sum_{i=1}^{n} |x_i - y_i|^2\Big]^{1/2}$$

The natural "product" in such a group is composition of mappings $(S \circ T)(x) = S(T(x))$. This operation has the virtue that *composition of mappings is automatically an associative process* because

$$(R \circ (S \circ T))(x) = R(S(T(x))) = (R \circ S)(Tx) = ((R \circ S) \circ T)(x) \quad \text{for all } x \in X$$

This is important. For an abstract group – say one presented as an $n \times n$ "multiplication table" – verifying associativity is by far the most tedious computational task, requiring a check of $n^3$ identities. Associativity of the group operation is automatic in a transformation group. Not all bijections $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ in $\mathrm{M}(n)$ are *linear* mappings, for instance translations $T_{\mathbf{a}}(v) = v + a$ are rigid motions because

$$\|T_{\mathbf{a}}(v) - T_{\mathbf{a}}(v')\| = \|(v + \mathbf{a}) - (v' + \mathbf{a})\| = \|v - v'\|$$

but since $T_{\mathbf{a}}(\mathbf{0}) = \mathbf{a} \neq \mathbf{0}$ they aren't linear maps unless $\mathbf{a} = \mathbf{0}$.

A **transformation group** $G$ is a set of bijective mappings on some space $X$ such that $G$ satisfies the Axioms (G.1) - (G.3) when equipped with composition product ($\circ$). Associativity is automatic, the identity map $e = \mathrm{id}_X$ acts as a group identity, and every bijective map $T : X \rightarrow X$ has a set-theoretic inverse $T^{-1} : X \rightarrow X$ such that $T \circ T^{-1} = T^{-1} \circ T = e$ as required in (G.3).

We will examine transformation groups in more detail in Chapter 4, but for the moment offer some comments on an important special case closely related to the matrix groups mentioned above: transformations groups whose elements are *linear operators* on some vector space.

**Matrix Groups vs Linear Transformation Groups.** There is a natural correspondence between matrix space $M(n,\mathbb{F})$ (equipped with matrix multiplication) and the space

$\mathrm{Hom}(\mathbb{F}^n)$ of all linear operators $T : \mathbb{F}^n \rightarrow \mathbb{F}^n$ on coordinate space (equipped with composition product). It is given by

$$L : M(n, \mathbb{F}) \rightarrow \mathrm{Hom}(\mathbb{F}^n) \qquad L_A(\mathbf{x}) = A \cdot \mathbf{x} \text{ for all } \mathbf{x} \in \mathbb{F}^n \tag{4}$$

Here we regard a vector $\mathbf{x}$ as an $n \times 1$ matrix and $A \cdot \mathbf{x}$ is the $(n \times n) \cdot (n \times 1) = (n \times 1)$ matrix product. Its basic properties, worked out in any linear algebra course, are

- $L$ is a bijection: distinct matrices $A$ go to distinct linear operators $L_A$ and for every linear operator $T : \mathbb{F}^n \rightarrow \mathbb{F}^n$ there is a unique matrix $A$ such that $T = L_A$.
- $L$ respects all algebraic operations

$$L_{A+B} = L_A + L_B \qquad L_{\lambda A} = \lambda \cdot L_A \quad (\forall \lambda \in \mathbb{F}) \qquad L_{A \cdot B} = L_A \circ L_B \tag{5}$$

Within $M(n, \mathbb{F})$ we have the matrix group $\mathrm{GL}(n, \mathbb{F})$ and various subgroups, equipped with matrix multiply $(\cdot)$; each of these subgroups corresponds to a group of transformations in $\mathrm{Hom}(\mathbb{F}^n)$, for instance the group $\mathrm{GL}(\mathbb{F}^n)$ of invertible linear operators on $\mathbb{F}^n$ equipped with composition product $(\circ)$. This is a transformation group. The group law is automatically associative, and $\mathrm{GL}(\mathbb{F}^n)$ contains an identity element $e = \mathrm{id}_{\mathbb{F}^n}$; it is also closed under formation of inverses in view of the following exercise.

**3.1.12 Exercise.** Let $T : V \rightarrow W$ be a *bijective* linear map between vector spaces. Prove that the set-theoretic inverse map

$$T^{-1}(w) = (\text{the unique } v \in V \text{ such that } Tv = w) \qquad (w \in W)$$

is a *linear* map from $W$ to $V$.
*Hint*: $T \circ T^{-1} = \mathrm{id}_W$ and $T^{-1} \circ T = \mathrm{id}_V$. □

It is a fundamental result in linear algebra that the correspondence $L$ in (4) induces a bijection between these two groups

$$L : (\mathrm{GL}(n, \mathbb{F}), \cdot\,) \rightarrow (\mathrm{GL}(\mathbb{F}^n), \circ) \quad ,$$

which by (5) intertwines the group operations.

**3.1.12A Definition** *Two groups $(G, \cdot\,)$ and $(G', *)$ are* **isomorphic** *if there exists a bijection $\phi : G \rightarrow G'$ that intertwines the group operations*

$$\phi(x \cdot y) = \phi(x) * \phi(y) \qquad \textit{for all } x, y \in G$$

*We write $G \cong G'$ if such a map can be found. The inverse map $\phi^{-1} : G' \rightarrow G$ is also an isomorphism.*

Isomorphic groups have indistinguishable algebraic properties, and may be regarded as different concrete models of the same underlying algebraic structure; the structures are said to be "*the same up to isomorphism.*" The relation $G \cong G'$ on the family of all groups is easily seen to be an RST equivalence relation, and the possible groups really correspond to the equivalence classes under $(\cong)$.

Finding a suitable map $\phi : G \rightarrow G'$ is the tricky part in proving two groups are isomorphic. If you want to prove that they are *not* isomorphic the best way to procede is to show that one group has an algebraic property that the other does not. The preceding discussion shows that $(\mathrm{GL}(n, \mathbb{F}), \cdot\,) \cong (\mathrm{GL}(\mathbb{F}^n), \circ)$ despite the very different nature of their elements.

**3.1.13 Example (The 2-Dimensional Rotation Group).** The **two-dimensional rotation group** $\mathrm{Rot}(2)$ consists of all rotations $R_\theta$ about the origin: $R_\theta$ rotates every vector in $\mathbb{R}^2$ counterclockwise about $\mathbf{0} = (0, 0)$ by $\theta$ radians. In particular

- The identity map of the plane $I = R_{\theta=0}$ is the identity element in the group.
- $R_{-\theta} =$ (rotation *clockwise* by $\theta$ radians) is the inverse of $R_\theta$.

It should be geometrically obvious that

$$R_{\theta_1+\theta_2} = R_{\theta_1} \circ R_{\theta_2} \text{ for all } \theta_1, \theta_2 \in \mathbb{R} \qquad \text{and} \qquad R_{-\theta} = R_\theta^{-1} \tag{6}$$

according to our interpretation of $R_{-\theta}$. Thus $(\mathrm{Rot}(2), \circ)$ is a transformation group. It is also commutative (a property not shared by the rotation groups in higher dimensions $n \geq 3$.

Notice that $R_\theta = R_{\theta+2\pi} = R_{\theta+2\pi k}$ for any integer $k$, so the symbols $R_\theta$ and $R_{\theta+2\pi k}$ all represent the same group operation. Only the value of $\theta$ (mod $2\pi$) matters in determining the geometric operation.

It is well known that every rotation $R_\theta$ is a linear operator on $\mathbb{R}^2$ and is represented by a $2 \times 2$ matrix with real entries: if vectors $\mathbf{x} = (x_1, x_2)$ are regarded as $2 \times 1$ column matrices we have

$$R_\theta \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \qquad \text{for all } \mathbf{x} \in \mathbb{R}^2 \tag{7}$$

The *rotation matrix* $A(\theta)$ appearing here is easily seen to lie in SO(2). In Exercises 3.1.14 and 3.1.14A we outline the steps needed to show that the matrices in (7) are are precisely those in

$$\mathrm{SO}(2) = \{A : A^{\mathrm{t}}A = I \;\text{ and }\; \det, A = 1\}$$

Thus when we identify operators $R_\theta$ with matrices $A(\theta)$ there is just one matrix $A \in \mathrm{SO}(2)$ for each distinct rotation operator, and composition of operators corresponds to the usual multiplication of matrices. Therefore the geometric group of rotations Rot(2) is in every respect equivalent to the group of real $2 \times 2$ matrices SO(2) – the groups are *isomorphic* $(\mathrm{SO}(2), \cdot\,) \cong (\mathrm{Rot}(2), \circ)$ under the bijective correspondence $\phi : A \rightarrow L_A$. It will be quite useful to have at our disposal both ways of looking at the same group. We will have a lot more to say about isomorphisms in Section 3.2. □

***3.1.13A Exercise.** Explain why the linear operator

$$L_A : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \qquad \text{for} \qquad A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

has the geometric effect of rotating every vector $\mathbf{x}$ counterclockwise by $\theta$ radians, as claimed in (7) □

***3.1.14 Exercise.** For a real $n \times n$ matrix $A$ show that the following conditions are equivalent

(a) $A \in \mathrm{O}(n)$, so that $A^{\mathrm{t}}A = I$ and $AA^{\mathrm{t}} = I$.

(b) The rows $R_1, \ldots, R_n$ of $A$ form an *orthonormal basis* with respect to the usual Euclidean inner product $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i$, on $\mathbb{R}^n$, so that

$$(R_i, R_j) = 0 \text{ for } i \neq j \qquad \text{and} \qquad \|R_i\|^2 = (R_i, R_i) = \sum_{i=1}^n x_i^2 = 1$$

(c) Likewise the columns in $A$ are orthonormal.

(d) $A$ preserves the standard inner product on $\mathbb{R}^n$, so that $(A\mathbf{x}, A\mathbf{y}) = (\mathbf{x}, \mathbf{y})$, and in particular distances between vectors

$$\|\mathbf{x} - \mathbf{y}\| = \Big[\sum_{i=1}^n (x_i - y_i)^2\Big]^{1/2} = \sqrt{(\mathbf{x} - \mathbf{y}\,,\, \mathbf{x} - \mathbf{y}\,)}$$

are preserved, making $L_A$ a *rigid motion* on $\mathbb{R}^n$.

*Hint*: How are entries in the matrix products $A^{\rm t}A$ and $AA^{\rm t}$ related to inner products of rows or columns? You might want to try it first for $n = 2, 3$. □

***3.1.14A Exercise.** For a real $2 \times 2$ matrix $A$ show that the following conditions are equivalent.

(a) $A \in \mathrm{SO}(2)$ so that $A^{\rm t}A = I$, $AA^{\rm t} = I$, and $\det A = 1$.

(b) There exist $a, b \in \mathbb{R}$ such that

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \qquad \text{with } a^2 + b^2 = 1$$

(c) There exists a real $\theta \in \mathbb{R}$ (not necessarily unique) such that

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

(d) The operator $L_A : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ such that $L_A(x) = Ax$ (product of $2 \times 2$ by $2 \times 1$ matrix) is a rotation $R_\theta$ about the origin by some angle of $\theta$ radians.

*Hint*: Exercise 3.1.14 applies taking $n = 2$. □

The situation in three dimensions is similar but more subtle.

***3.1.15 Example (The 3-Dimensional Rotation Group).** The set Rot(3) of rotations $R_{\ell,\theta}$, by any angle $\theta$ about any oriented axis $\ell$ through the origin, is a linear transformation group under composition ($\circ$). This is not completely obvious at the outset. For instance we may ask

> Question: Given rotations $R_{\ell_1,\theta_1}$ and $R_{\ell_2,\theta_2}$ how do you find $\ell_3$ and $\theta_3$ (if any) such that $R_{\ell_1,\theta_1} \circ R_{\ell_2,\theta_2} = R_{\ell_3,\theta_3}$?

The following theorem of Euler (too much of a digression to prove here) shows that SO(3) maps to the rotation group Rot(3) under the correspondence $A \mapsto L_A$ so there is an isomorphism $(\mathrm{SO}(3), \cdot\,) \cong (\mathrm{Rot}(3), \circ)$ between these groups.

**3.1.16 Theorem (Euler's Theorem).** *If $A \neq I$ in* SO(3)*, $\lambda = 1$ is the only real eigenvalue and its eigenspace is one-dimensional. The linear operator $L_A : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by $L_A(\mathbf{x}) = A\mathbf{x}$ is a rotation $R_{\ell,\theta}$ by some angle $\theta$ about the axis $\ell =$ (the one-dimensional $\lambda = 1$ eigenspace). The correspondence* (4) *is a bijection from* SO(3) *to the group of rotations* Rot(3)*, and is an isomorphism of groups.*

That concludes our excursion into linear algebra for the time being.

Here are a few more important groups, some of which happen to be groups of transformations.

**3.1.17 Example ($\mathbf{\Omega_n} = \mathbf{n^{th}}$ Roots of Unity).** Recall that every complex number $z \neq 0$ can be written in polar form $z = re^{i\theta} = (r\cos\theta) + i(r\sin\theta)$ as shown in Figure 3.1. Here $r = |z|$ and $\theta$ is the angle variable (angle from positive $x$-axis to the ray from the origin to $z$), in radians. An $n^{\rm th}$ root of unity is any $z$ such that $z^n = 1$ (so $z^n - 1 = 0$). The identity $|zw| = |z| \cdot |w|$ forces $z$ to lie on the unit circle $|z| = 1$ if $z^n = 1$, and hence have the form $z = e^{i\theta}$ for some $\theta \in \mathbb{R}$. Then $z^n = e^{in\theta}$ equals $1 \Leftrightarrow n\theta$ is a whole multiple of $2\pi$ radians, so the distinct $n^{\rm th}$ roots of unity are $\{e^{2\pi ik/n} : 0 \leq k \leq n-1\}$ . These are precisely the powers $1, \omega, \omega^2, \ldots, \omega^{n-1}$ of the *primitive $n^{\rm th}$ root* $\omega = e^{2\pi i/n}$, which makes a counterclockwise angle of $\theta = 2\pi/n$ radians with the $+x$-axis.

The set of $n^{\rm th}$ roots $\Omega_n$ is a group under complex multiplication. In fact, $1 \in \Omega_n$ and $z, w \in \Omega_n \Rightarrow z^n = 1, w^n = 1 \Rightarrow (zw)^n = z^n w^n = 1$, so $\Omega_n$ contains the multiplicative

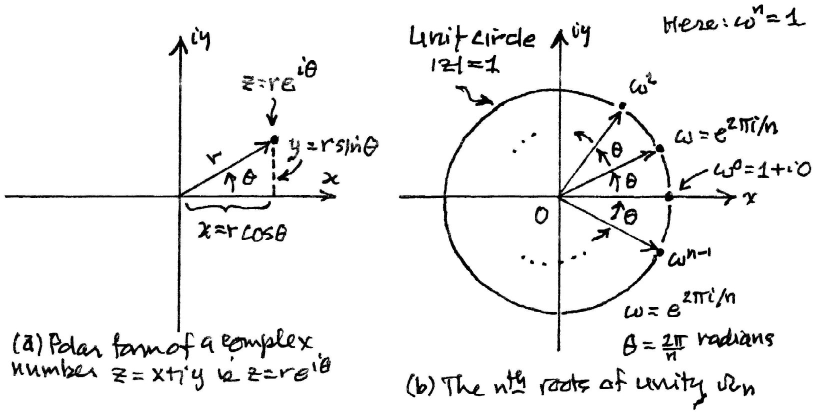

**Figure 3.1.** Geometric meaning of the polar form $z = re^{i\theta}$ of a complex number. In (b) we show the locations of the complex $n^{\text{th}}$ roots of unity, which are the powers $1, \omega, \omega^2, \ldots, \omega^{n-1}$ of the *primitive* $n^{\text{th}}$ *root* $\omega = e^{2\pi i/n}$.

identity 1 and is closed under formation of products. As for inverses, we have

$$z^n = 1 \;\Rightarrow\; \left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$$

so $\Omega_n$ is closed under inversion and $(\Omega_n, \cdot\,)$ is a group, a subgroup of the multiplicative group $(\mathbb{C}^\times, \cdot\,)$ of nonzero complex numbers. Later on we will see that the multiplicative group $(\Omega_n, \cdot\,)$ is isomorphic to the familiar additive group $(\mathbb{Z}_n, +)$. □

**Permutation Groups $\mathbf{S_n}$.** Next we introduce the permutation groups $S_n$, fundamental to all discussions of group theory. Here we provide a brief introduction; all of Chapter 5 will be devoted to further discussion of these groups.

**3.1.18 Example (Permutation Groups I).** The **permutation group** $S_n$ is the collection of all bijective maps $\sigma : X \rightarrow X$ of the set $X = \{1, 2, \ldots, n\}$, with composition of maps $(\circ)$ as the group operation. Our previous comments about composition show that $(S_n, \circ)$ is a group. The identity element is the identity map on $X$, $e = \mathrm{id}_X$, and the inverse of any $\sigma$ is the set-theoretic inverse map $\sigma^{-1}$ that undoes the action of $\sigma$. It is easily seen that $S_n$ is finite, with $|S_n| = n! = (n)(n-1)\cdots(3)(2)(1)$. It is non-commutative except when $n = 2$.

One (cumbersome) way to describe elements $\sigma \in S_n$ employs a data array to show where each $k \in X$ ends up:

$$\sigma = \left(\begin{array}{cccccc} 1 & 2 & \ldots & k & \ldots & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_n \end{array}\right)$$

where $(i_1, i_2, \ldots, i_n)$ is some ordered listing of the integers $1 \leq k \leq n$. In this notation the identity element is

$$e = \left(\begin{array}{cccccc} 1 & 2 & \ldots & k & \ldots & n \\ 1 & 2 & \ldots & k & \ldots & n \end{array}\right)$$

More efficient notation is afforded by the fact that every $\sigma$ can be uniquely written as a product of "elementary permutations" called **cycles**. We describe the notation for cycles here, so you will be able to handle meaningful examples; later on in Chapter 5 we will deal with the cycle decomposition of arbitrary permutations.

**3.1.19 Definition.** *For $k > 1$, a* $k$**-cycle** *is a permutation $\sigma = (i_1, \ldots, i_k)$ that acts on $X$ in the following way*

$$(8) \qquad \sigma \text{ maps } \begin{cases} i_1 \rightarrow i_2 \rightarrow \ldots \rightarrow i_k \rightarrow i_1 & (\text{a cyclic shift of list entries}) \\ j \rightarrow j \quad \text{for all } j \text{ not in the list } \{i_1, \ldots, i_k\} \end{cases}$$

*The action of $\sigma$ depends on the particular order of the list entries $i_1, \ldots, i_k$.*

For example,

The cycle $\sigma = (123)$ in $S_5$ maps $1 \rightarrow 2 \rightarrow 3 \rightarrow 1 \;\; ; \;\; 4 \rightarrow 4 \;\; ; \;\; 5 \rightarrow 5$

The cycle $\sigma = (12)$ in $S_5$ maps $1 \rightarrow 2 \rightarrow 1 \;\; ; \;\; 3 \rightarrow 3 \;\; ; \;\; 4 \rightarrow 4 \;\; ; \;\; 5 \rightarrow 5$

One-cycles $(k)$ are redundant; every one-cycle corresponds to the identity map $\text{id}_X$. We seldom write one-cycles explicitly, though it is permissible and sometimes useful. For instance the cycle $(123)$ in $S_5$ could also be written as the product of cycles $(123)(4)(5)$ because $(4) = (5) = \text{id}_X$.

The symbol $\sigma = (i_1, \ldots, i_k)$ denoting a cycle is ambiguous. If we make a cyclic shift of list entries we get $k$ different symbols that describe the same mapping of $X$.

$$(i_1, \ldots, i_k) = (i_2, \ldots, i_k, i_1) = (i_3, \ldots, i_k, i_1, i_2) = \ldots = (i_k, i_1, \ldots, i_{k-1})$$

For instance $(123) = (231) = (312)$ all specify the same operation $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$ in $X$. If we mess up the "cyclic order" of the entries we *do not* get the same element in $S_n$. Thus

$(123) \neq (132)$ because no *cyclic* shift of entries can make these symbols match

Indeed $(123) \neq (132)$ as operators on $X$ because the first operator sends $1 \rightarrow 2$ while the second sends $1 \rightarrow 3$. The notational ambiguity regarding cycles can be somewhat confusing, but the cycle concept is so useful that you will simply have to live with it.

Next you must understand how to evaluate the product $\sigma\tau = \sigma \circ \tau$ of two cycles. Since the product is composition of maps, the action of the product on an element $k \in X$ can be evaluated by feeding $k$ into the product *from the right*, as shown below taking $\sigma = (12)$ and $\tau = (123)$ in $S_5$.

$$\sigma\tau : k \xrightarrow{(123)} (123) \cdot k \xrightarrow{(12)} (12)((123) \cdot k) = (12)(123) \cdot k$$

(Warning: Not all authors adhere to this standard convention!) To determine the net effect of $\sigma\tau$, start by examining the fate of $k = 1$, then look at what happens to the image of 1, etc.

| **Action** | **Net Effect** |
|---|---|
| $1 \xrightarrow{(123)} 2 \xrightarrow{(12)} 1$ | $1 \rightarrow 1$ |
| $2 \xrightarrow{(123)} 3 \xrightarrow{(12)} 3$ | $2 \rightarrow 3$ |
| $3 \xrightarrow{(123)} 1 \xrightarrow{(12)} 2$ | $3 \rightarrow 2$ |
| $4 \xrightarrow{(123)} 4 \xrightarrow{(12)} 4$ | $4 \rightarrow 4$ |
| $5 \xrightarrow{(123)} 5 \xrightarrow{(12)} 5$ | $5 \rightarrow 5$ |

Examining the right hand column we see that the net effect of $\sigma\tau$ is to switch $2 \leftrightarrow 3$, leaving all other $k$ where they were. Thus

$$(12)(123) = (1)(23)(4)(5) = (23) \qquad \text{in } S_5$$

By a similar tracing of outcomes you can verify that

$$(123)(14) = (1423)(5) = (1423) \qquad \text{in } S_5$$

and so on. We exit our discussion of $S_n$ with some exercises along these lines. □

**3.1.20 Exercise.** Evaluate the net action of the following products of cycles

(a) $(12)(13)$ in $S_3$ (c) $(12)(12345)$ in $S_5$ (e) $(12)^2$ in $S_5$

(b) $(12)(13)$ in $S_5$ (d) $(12345)(12)$ in $S_5$ (f) $(123)^2$ in $S_5$

(g) $(15)(14)(13)(12)$ in $S_5$ □

***3.1.21 Exercise.** Given two cycles $\sigma = (i_1, \ldots, i_k),\ \tau = (j_1, \ldots, j_s)$ in $S_n$, explain why

(a) $\sigma^k = \mathrm{id}_X$ and $\tau^s = \mathrm{id}_X$

(b) $\sigma\tau = \tau\sigma$ (the operators commute) if their entries are disjoint in the sense that $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_s\} = \emptyset$.

*Note: Disjoint cycles always commute!* However, if entries overlap the cycles may fail to commute, as in the previous examples. □

**3.1.22 Exercise.** Determine the *inverses* $\sigma^{-1}$ of the following elements in $S_5$

(a) $(12)$ (c) Any 2-cycle $(i_1, i_2)$ with $i_1 \neq i_2$

(b) $(123)$ (d) Any $k$-cycle $(i_1, \ldots, i_k)$ with distinct $i_j$ □

**3.1.22A Exercise.** Prove that the product of 2-cycles $(1, k)(1, k-1) \cdots (1, 3)(1, 2)$ is equal to the $k$-cycle $(1, 2, \ldots, k)$.
*Note*: By relabeling $1 \rightarrow i_1, \ldots, k \rightarrow i_k$ where $i_1, \ldots, i_k$ are distinct elements in $\{1, 2, \ldots, n\}$ we see that a suitable product of 2-cycles yields an *arbitrary* $k$-cycle.

$$(i_1, i_k)(i_1, i_{k-1}) \cdot \ldots \cdot (i_1, i_2) = (i_1, \ldots, i_k)$$

This will be important later on. □

**A Notational Interlude:** Usually the operation in a group is written in multiplicative form as $x \cdot y$, but when $G$ is commutative it is often preferrable to use *additive notation*, writing the group operation as $x + y$. It is permissible, and often desirable, to use multiplicative notation with commutative groups, but that would be really awkward in some cases. You would encounter a lot of cognitive dissonance in discussing the group of integers $(\mathbb{Z}, +)$ if we insisted on using some sort of multiplicative notation $m * n$ for the group operation instead of $m + n$. On the other hand the group of units $(\mathrm{U}_n, \cdot\,)$ in $\mathbb{Z}_n$, or the $n^{\text{th}}$ roots of unity $(\Omega_n, \cdot\,)$, should obviously be handled using multiplicative notation. (The set of units isn't even closed under the $(+)$ operation in $\mathbb{Z}_n$, recall Exercise 3.1.6.)

When we do employ additive notation, various combinations of group elements must be rewritten accordingly. For instance in additive notation the identity element is always written as "0" rather than "$e$" and the additive inverse of an element is written $-x$ instead of $x^{-1}$, so the characteristic property defining the inverse of an element in $G$ takes the form

$$x + (-x) = 0 \qquad \text{instead of} \qquad x \cdot x^{-1} = e$$

The *additive* $k^{\text{th}}$ *power* of an element $x$ is then

$$\begin{aligned} k \cdot x &= x + \ldots + x \ \ (k \text{ times}) \qquad \text{instead of} \qquad x^k = x \cdot \ldots \cdot x \\ -k \cdot x &= (-x) + \ldots + (-x) \ \ (k \text{ times}) \qquad \text{instead of } x^{-k} = x^{-1} \cdot \ldots \cdot x^{-1} \end{aligned}$$

for $k > 0$ and $0 \cdot x = 0_G$ (the identity element in $G$) if $k = 0$. Here is a glossary for translating between multiplicative and additive notation

**Glossary**

| | Identity | Inverse | Product | Powers |
|---|---|---|---|---|
| Multiplicative Notation $(G, \cdot\,)$ | $e$ | $x^{-1}$ | $x \cdot y$ | $x^k = x \cdot \ldots \cdot x$ |
| Additive Notation $(G, +)$ | $0$ | $-x$ | $x + y$ | $k \cdot x = x + \ldots + x$ |

This dual notation may seem confusing at first, but it is so convenient and widely used that you simply must get a handle on it. Notice that in the particular additive group $(\mathbb{Z}_n, +)$ all of the following expressions

$$k \cdot [\ell] = [\ell] + \ldots + [\ell] \ (k \text{ times}) = [\ell + \ldots + \ell] = [k\ell]$$

stand for the additive $k^{\text{th}}$ power of a typical element $[\ell] \in \mathbb{Z}_n$.

**Subgroups of a group** $G$. We now examine some structural features of an abstract group. A nonempty subset $H$ in a group $G$ is a **subgroup** if it has the properties

(9)
(i) $H$ is closed under formation of products: $H \cdot H \subseteq H$, or equivalently $x, y \in H \Rightarrow xy \in H$.
(ii) The identity element $e$ lies in $H$.
(iii) $H$ is closed under inverses: $h \in H \Rightarrow h^{-1} \in H$.

Then the product operation $G \times G \to G$ restricts to give a product operation $H \times H \to H$ and one easily verifies that $(H, \cdot\,)$ satisfies the group axioms G.1 − G.3. For instance, associativity of the induced operation in $H$ follows immediately from associativity in the larger set $G$. The trivial groups $H = (e)$ and $H = G$ are subgroups; all other subgroups, if any, are referred to as **proper subgroups**. The suggestive notation $H \leq G$ is sometimes used to indicate that a subset $H \subseteq G$ is actually a subgroup.

The pattern of subgroups is an important structural feature of any group, so it is useful to understand how subgroups get "generated" by various nonempty subsets $S$ of elements in $G$. This idea, that every subset $S$ generates a *subgroup* $H = \langle S \rangle$, is based on the following easy theorem.

**3.1.23 Exercise.** Given any family $\{H_\alpha : \alpha \in I\}$ of subgroups in a group $G$, prove that their intersection

$$H = \bigcap_{\alpha \in I} H_\alpha = \{x \in G : x \in H_\alpha \text{ for all } \alpha \in I\}$$

is also a subgroup, even if there are infinitely many $H_\alpha$. □.

Given a nonempty subset $S \subseteq G$ there is always *some* subgroup that contains $S$ − for example $H = G$ itself. The intersection of *all* subgroups that contain $S$ is again a subgroup, by 3.1.23, and is evidently the *smallest possible* subgroup that contains $S$.

**3.1.24 Definition.** *Let $S$ be a nonempty subset of a group $G$. The intersection*

$$\langle S \rangle = \bigcap \{H : H \textit{ is a subgroup and } H \supseteq S\} \qquad (10)$$

*is a subgroup. It is called the* **subgroup generated by** *$S$, and the elements of $S$ are referred to as "generators" of this group.*

Different subsets might generate the same subgroup.

The foregoing "top-down" definition is rather transcendental and abstract, making it hard to wrap your mind around the concept of "generated subgroup." Fortunately, an alternative “bottom-up” description of $\langle S\rangle$ tells uusususuusss how to build it up from the elements in $S$. Starting from $S$, first form the set $S \cup S^{-1}$, which consists of elements of $S$ and their inverses. The sets $S, S^{-1}$ and $S \cup S^{-1}$ generate the same subgroup in $G$ since $G^{-1} = G$.

***3.1.25 Exercise.** Suppose $S$ and $S'$ are nonempty subsets in a group $G$. Prove that

(a) $S' \subseteq S \;\Rightarrow\; \langle S'\rangle \subseteq \langle S\rangle$ .

(b) If $S$ is already a subgroup, then $\langle S\rangle = S$. To put it another way, doing $\langle\,\cdot\,\rangle$ twice yields nothing new: $\langle\langle S\rangle\rangle = \langle S\rangle$.

(c) The sets $S$, $S^{-1} = \{s^{-1} : s \in S\}$, and $S \cup S^{-1}$ each generate the same subgroup in $G$. □

So, passing from $S$ to $S \cup S^{-1}$ we procede to form the set of all *words of finite length* whose entries are either an element of $S$ or the inverse of such an element:

(11) The set of “finite length words” $W_S$ is defined to be the set of all products $a_1 \cdots a_r$ such that $r < \infty$ and $a_i \in S \cup S^{-1}$

The set of symbols $S \cup S^{-1}$ is the “alphabet” from which words are constructed. It is crucial to realize that this set of “words” is precisely the subgroup generated by $S$, and this is the “bottom-up” interpretation of $\langle S\rangle$. We leave the verification to the reader.

***3.1.26 Exercise.** Verify that $W_S$ is indeed a subgroup of $G$, and that

$$\langle S\rangle = W_S = \{\, a_1 \cdots a_r : r < \infty \text{ and } a_i \in S \cup S^{-1} \,\} \tag{12}$$

for any nonempty set $S \subseteq G$.
*Hint:* Why is the identity $e$ in the set $W_S$? If $x \in W_S$ why is $x^{-1}$ in $W_S$? □

**3.1.27 Exercise.** Do we always get a subgroup if we form the set

$$E_S = \{\, a_1 \cdots a_r : r < \infty \text{ and } a_i \in S \,\} \quad \text{(no negative powers)?}$$

Prove or give a counterexample.
*Hint:* Try some subsets of $G = (\mathbb{Z}, +)$. □

**3.1.28 Exercise.** In $G = (\mathbb{Z}, +)$ consider the subsets

(i) $A = \mathbb{N}$ (ii) $B = \{2\}$ (iii) $C = \{2, 3\}$ (iv) $D = \{3, 21\}$ (v) $E = \{3, 23\}$

Determine the subgroups they generate. □

**3.1.29 Exercise.** In $G = (\mathbb{Z}_{12}, +)$, determine the subgroups generated by

(a) The additive identity element $[0]$

(b) The multiplicative identity element $[1]$

(c) The single element $x = [2]$

(d) The single element $y = [3]$

(e) The single element $z = [5]$

(f) The two elements $x = [5]$ and $y = [3]$ □

***3.1.30 Exercise.** Explain why every subgroup of $(\mathbb{Z}, +)$ has the form

$$H = m\mathbb{Z} = \{km : k \in \mathbb{Z}\}$$

for some $m \geq 0$
*Hint:* The trivial subgroup $0 \cdot \mathbb{Z} = \{0\}$ is obtained if we take $m = 0$; setting aside this special case we may assume $H \neq \{0\}$. Then $H \cap \mathbb{N}$ is nonempty (why?), and there is a smallest element $m = \min\{H \cap \mathbb{N}\}$ by the Minimum Principle. □

***3.1.30A Exercise.** Let $(G, +)$ be an abelian group described in additive notation, and let $a, b \in G$. Writing additive $k^{\text{th}}$ powers as $k \cdot x$, define the set of "integer linear combinations"

$$\mathbb{Z}\cdot a + \mathbb{Z}\cdot b = \{k\cdot a + \ell\cdot b : k, \ell \in \mathbb{Z}\}$$

Prove that

(a) $\mathbb{Z}\cdot a + \mathbb{Z}\cdot b$ is a subgroup in $(G, +)$.

(b) $\mathbb{Z}\cdot a + \mathbb{Z}\cdot b$ is precisely the group $H = \langle a, b\rangle$ generated by $a, b$.

*Note*: This helps in determining subgroups generated by elements of an abelian group. If $G$ is abelian and the group law is written in multiplicative form, the set $\mathbb{Z}\cdot a + \mathbb{Z}\cdot b$ becomes $\{a^k b^\ell : k, \ell \in \mathbb{Z}\}$. □

***3.1.30B Exercise.** In the additive group of integers $(\mathbb{Z}, +)$ determine the subgroups $H = \langle a, b\rangle$ generated by

(a) $a = 18$ and $b = 21$ (b) $a = 18$ and $b = 32$ (c) $a = 18, b = 32,$ and $c = 14$ □

*Hint*: Use the result of Exercise 3.1.30A and recall that $\gcd(a, b) =$ the smallest positive element in the lattice $\Lambda = \mathbb{Z}a + \mathbb{Z}b$.

Given a subset $S$ in $G$, determining the generated subgroup can be a vexing task. However, a complete analysis is possible in one very important case: when $S$ consists of a single point $a$ and the generated subgroup is $H = \langle a\rangle$. Subgroups generated by a single element are called **cyclic subgroups**. A cyclic subgroup can have various generators, so that $H = \langle a\rangle = \langle b\rangle$ with $a \neq b$. The case when $a = e$ is of no interest since $\langle e\rangle$ is the trivial subgroup.

Our analysis of cyclic subgroups requires some basic facts about powers $a^k$ of a group element. Proof from the axioms is quite straightforward, but involves an annoying number of cases, so we simply state the result and leave the proof to you.

**3.1.31 Theorem (The Exponent Laws).** *Let $(G, \cdot\,)$ be a group. For any element $a \in G$ and any $k \in \mathbb{N}$ define*

$$a^k = a \cdot \ldots \cdot a \qquad (k \textit{ times})$$
$$a^0 = e \qquad (\textit{the identity element})$$
$$a^{-k} = (a^{-1}) \cdot \ldots \cdot (a^{-1}) \qquad (k \textit{ times})$$

*Then the following* **exponent laws** *are valid for all $m, n \in \mathbb{Z}$.*

(a) $a^m \cdot a^n = a^{m+n}$

(b) $(a^m)^{-1} = (a^{-1})^m$

(c) $(a^m)^n = a^{mn}$

*If $G$ is abelian we also have*

(d) *If $G$ is abelian we also have $(ab)^n = a^n \cdot b^n$.*

The case $m, n > 0$ involves straightforward counting. For the rest use the fact that, by definition, $a^{-k} = (a^{-1})^k$ when $k > 0$ and $a^0 = e$.

***3.1.32.** Suppose $G$ is abelian and the group law is written in additive form $(G, +)$. Rewrite the Exponent Laws 3.1.31 in additive notation.
*Note:* You will find that the Exponent Laws written in this form recapitulate several of the rules in *Axiom Set I* in the definition of $\mathbb{Z}$. □

It follows immediately from the Exponent Laws that the subgroup generated by a single element $a \in G$ is precisely the set $H = \{a^k : k \in \mathbb{Z}\}$ of all positive and negative powers of $a$. But it is important to notice that the list $\ldots a^{-2}, a^{-1}, a^0 = e, a^1 = a, a^2, a^3, \ldots$ whose elements make up $H$ *may include repeats* – i.e. we might have $a^i = a^j$ with $i \neq j$ in $\mathbb{Z}$. Although there are infinitely many possible powers $a^k$, one for each integer, the set $H$ of *distinct* powers could be (and often is) *finite* if the list has repeats. You must distinguish between the infinite *list of powers* and the set of *distinct items* in that list.

**3.1.33 Exercise.** If $G$ is a group and $a \in G$, prove from the definition of "generated subgroup" that $\langle a \rangle$ coincides with the set of powers $H = \{a^k : k \in \mathbb{Z}\}$.
*Note:* This is true whether or not there are repeats among the powers $a^k$. □

To determine $H$ more precisely we examine the behavior of the sequence of non-negative powers $S' = \{e, a, a^2, a^3, \ldots\}$, where $e = a^0$ and $a = a^1$. There are two cases to consider.

Case 1: There are no repeats in $S'$. Then the larger sequence $\{a^k : k \in \mathbb{Z}\}$ consisting of *all* powers contains no repeats. In fact, if a repeat occurred there would be integers $\ell < k$ in $\mathbb{Z}$ such that $a^k = a^\ell$. By the exponent laws $a^k = a^{k-\ell} \cdot a^\ell = a^\ell$. Multiplying both sides on the right by $a^{-\ell}$ we get $a^{k-\ell} = e$; but $0 < k - \ell < k$ contrary to our hypothesis that the list of positive powers contains no repeats.

In Case 1 all the $a^k$ are distinct and the subgroup $H$ is an infinite group, which must be abelian since $a^k \cdot a^\ell = a^{k+\ell} = a^\ell \cdot a^k$ by the exponent laws. Furthermore there is a natural bijection $\phi : k \mapsto a^k$ between $(\mathbb{Z}, +)$ and $(H, \cdot\,)$ which has the interesting property that it *intertwines* the group operations

$$\phi(k + \ell) = \phi(k) \cdot \phi(\ell) \qquad \text{(because } a^{k+\ell} = a^k \cdot a^\ell\text{)}$$

Intuitively, that means $(H, \cdot\,) \cong (\mathbb{Z}, +)$ and $H$ is simply a copy of $(\mathbb{Z}, +)$ embedded within the abstract group $G$. (More on this later.)

Case 2: There is a repeat in the set $S'$. A trivial possibility is that $a^0 = a^1$; then $a = e$ and $H = \langle a \rangle$ reduces to the trivial subgroup $H = (e)$. Otherwise, a repeat will occur because there are integers $0 \leq \ell < k$ such that $a^\ell = a^k$.

We claim that

> *Let $k$ be the smallest index $k > 0$ for which a repeat occurs. Then $a^k = e$, so the first repeat* cannot *occur because $a^k$ is equal to some intermediate power $a^\ell$ with $0 < \ell < k$.*

If the repeat involved an intermediate power we would have $a^\ell = a^k$ for some $0 < \ell < k$. Then $a^\ell = a^k = a^{k-\ell} \cdot a^\ell$, and we may multiply on the right by $(a^\ell)^{-1} = a^{-\ell}$ to get $a^{k-\ell} = e$. That is impossible because $k - \ell > 0$ is smaller than the minimal exponent $k$.

In Case 2 the generated subgroup is $H = \{e, a, a^2, \ldots, a^{k-1}\}$, with $a^k = e$. [In fact $H$ is a subgroup because (i) $e \in H$; (ii) $a^i a^j = a^{i+j} \in H$ if $i + j < k$, and otherwise we have

$$a^{i+j} = a^{i+j-k} a^k = a^{i+j-k} \in H \quad \text{(because } i + j < 2k \Rightarrow i + j - k < k\text{)} \;\; ;$$

(iii) Finally we have $(a^i)^{-1} = a^{k-i} \in H$ because $0 \leq k - i < k$.] The elements $e, a, a^2, \ldots, a^{k-1}$ are distinct, the subgroup is finite with $|H| = k$, and $H$ is abelian (combine the Exponent Laws with the fact that $a^k = e$). Note that the set of positive powers $e, a, a^2, \ldots, a^{k-1}$ picks up all the negative powers automatically when $o(a) < \infty$, for instance. $a^{-1} = a^{k-1}, a^{-2} = a^{k-2}, \ldots$

In this situation we have a well-defined map $\phi : \mathbb{Z}_k \to H$ given by $\phi([j]) = a^j$ for each congruence class $[j]$ in $\mathbb{Z}_k$. This is a well defined map of congruence classes $[j]$ because

$$a^{j+nk} = a^j \big(a^k\big)^n k = a^j \cdot e = a^j \qquad \text{for all } n \in \mathbb{Z}$$

The value of $a^j$ depends only on the (mod $k$) congruence class of $j$ in $\mathbb{Z}$ and not on $j$ itself. In view of the following exercise, $H = \langle a \rangle$ is just an isomorphic copy of the finite group $(\mathbb{Z}_k, +)$ embedded in $G$. Note that $(\mathbb{Z}_k, +)$ is itself a cyclic group, generated by the element $[1]$. (There might be other cyclic generators of $\mathbb{Z}_k$, see 3.1.37 below.)

**3.1.34 Exercise.** Prove that the map $\phi : \mathbb{Z}_k \to H$ defined above is actually a bijection, and has the intertwining property

$$\phi([m] + [n]) = \phi([m]) \cdot \phi([n]) \qquad \text{for all } [m], [n] \in \mathbb{Z}_k.$$

Therefore $\phi$ is an isomorphism between the groups $(\mathbb{Z}_n, +)$ and $(H, \cdot)$.
*Hint:* Exponent laws. □

**3.1.35 Definition.** *Let $(G, \cdot\,)$ be a group. The* **order** *$o(a)$ of a group element $a \in G$ is the smallest positive exponent $k > 0$ such that $a^k = e$. If no such exponent exists the group element is said to have* **infinite order***, which we indicate by writing $o(a) = \infty$.*

For example, every element $a \neq 0$ in $(\mathbb{Z}, +)$ has infinite order; on the other hand, if $G$ is a *finite* group every element $a \in G$ has finite order since $o(a) \leq |G|$. By definition $o(a) \geq 1$, and we have $o(a) = 1 \Leftrightarrow a = e$.

The preceeding discussion is summarized in the following theorem.

**3.1.36 Theorem (Structure of Cyclic Subgroups).** *Let $(G, \cdot\,)$ be a group. A cyclic subgroup has the form $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ for some $a \in G$. There are two possibilities, which depend on the order $o(a)$ of the generator.*

(a) *$o(a) = \infty$. Then all powers $a^k$, $k \in \mathbb{Z}$, are distinct and $H$ is a copy of the infinite abelian group $(\mathbb{Z}, +)$ embedded in the abstract group $G$.*

(b) *$o(a) = k < \infty$. Then $H$ consists of the distinct elements $\{e, a, a^2, \ldots, a^{k-1}\}$, with $a^k = e$. In this case $H$ is a copy of the finite abelian group $(\mathbb{Z}_k, +)$ embedded in the abstract group $G$.*

**3.1.37 Exercise.** The element $[1]$ is a cyclic generator of the additive group $(\mathbb{Z}_{12}, +)$, but there are several other cyclic generators. Which other elements $a = [j]$ generate $(\mathbb{Z}_{12}, +)$?

(a) Determine the order of each element $[k]$ in $\mathbb{Z}_{12}$ by writing out all of its "additive powers" $m \cdot [k], m = 0, 1, 2 \ldots$ until you hit the first repeat $m \cdot [k] = [0]$. You have then determined the cyclic subgroup $H = \langle [k] \rangle$ and the additive order $o([k])$ of its generator. For which $k$, if any, is $o([k]) = 12$?

You might get away with less computation by noting the symmetries $[11] = -[1], [10] = -[2], \ldots, [6] = -[6]$.

(b) Verify that the elements $[k]$ and $-[k]$ always generate the same additive subgroup of $\mathbb{Z}_{12}$. □

**3.1.38 Exercise.** Repeat the previous exercise taking $G = (\mathbb{Z}_7, +)$ and $G = (\mathbb{Z}_6, +)$. □

No discussion of cyclic groups would be complete without mention of the following result, whose proof depends solely on properties of the system of integers (Euclidean Division Algorithm).

**3.1.39 Proposition.** *Every subgroup of a cyclic group is also cyclic.*

Proof: Let $G = \langle a \rangle$ be a cyclic group with generator $a$ and let $H$ be any subgroup. There is nothing to prove if $H = (e)$ or $H = G$, so we may assume $H$ is a *proper* subgroup of $G$. There are two cases to consider: (i) $o(a) = \infty$, and (ii) $o(a) = n < \infty$. The proof in

Case (i) is quite a bit simpler than that in Case (ii), though it employs the same general strategy; we leave the reader to work out the proof when $o(a) = \infty$ (Exercise 3.1.39A below) after reading the following discussion of the case $o(a) = n$.

When $a$ has finite order let $m$ be the smallest positive exponent such that $b = a^m$ lies in $H$. This obviously occurs for some exponent since $a$ generates $G$; furthermore $1 < m < n$ if $H$ is proper. (Why?)

We claim that $H = \langle b\rangle$. Obviously $\langle b\rangle \subseteq H$ since $b \in H$. For the reverse inclusion: if $y \in H$ then $y = a^\ell$ for some $\ell \in \mathbb{Z}$. Applying the Euclidean Division algorithm we may write $\ell = ms + r$ with $0 \leq r < m$, $s \in \mathbb{Z}$. Since $a^m = b$ by definition of $m$, we get

$$a^\ell = a^{ms+r} = \big(a^m\big)^s \cdot a^r = b^s \cdot a^r$$

and

$$a^r = b^{-s} \cdot a^\ell \qquad \text{(which is in } H \text{ since } a^\ell \text{ and } b \in H)$$

Thus $a^r \in H$, but $m$ is the smallest positive exponent such that $a^m \in H$; since $0 \leq r < m$ we arrive at a contradiction unless the remainder is zero. Hence $r = 0$, so

$$e = b^{-s} \cdot a^\ell \qquad \text{and} \qquad a^\ell = b^s$$

and $a^\ell \in \langle b\rangle$, proving the reverse inclusion $H \subseteq \langle b\rangle$. $\square$

***3.1.39A Exercise**. Suppose a cyclic group $G = \langle a\rangle$ is generated by an element of *infinite order*. Prove that any subgroup $H \subseteq G$ is also cyclic, $H = \langle b\rangle$ for some $b \in H$, and that $o(b) = \infty$ unless $H$ is the trivial subgroup $H = (e)$.
*Hint*: As mentioned earlier, $o(a) = \infty$ means that $G = \langle a\rangle$ is isomorphic to the additive group $(\mathbb{Z}, +)$. Thus we may as well assume $G = (\mathbb{Z}, +)$ and $H \subseteq \mathbb{Z}$. If $H \neq (0)$, look at the smallest additive power $b = m \cdot a$, $m \geq 1$, such that $m \cdot a$ lies in $H$. Use Euclidean Division by $m$ to prove $H \subseteq \langle b\rangle = b \cdot \mathbb{Z}$. $\square$

In particular all subgroups $H$ of $(\mathbb{Z}, +)$ are cyclic, and have the form $H_m = \mathbb{Z} \cdot m$ for some integer $m \geq 0$, with $H_0 = \{0\}$ and $H_1 = \mathbb{Z}, H_2 = 2 \cdot \mathbb{Z}$, etc.

The next result shows that the subgroups of the cyclic group $(\mathbb{Z}_n, +)$ correspond to the divisors of the modulus $n$.

***3.1.40 Exercise**. Let $n > 1$. For each divisor $d|n$, $1 \leq d \leq n$, construct an *explicit* cyclic subgroup $H_d \subseteq \mathbb{Z}_n$ such that $|H_d| = d$ by finding an element of order $d$ in $(\mathbb{Z}_n, +)$.
*Hints:* The cases $d = 1, d = n$ are trivial. You might try it first for, say, $n = 12$. $\square$

Later, at the end of Section 3.4, we will go further and prove that there is a *unique* subgroup $H_d \subseteq \mathbb{Z}_n$ for each divisor $d|n$, and that these are the *only* subgroups in $\mathbb{Z}_n$.

**3.1.41 Exercise**. Suppose a group element $x \in (G, \cdot\,)$ has the property $x^m = e$ for some integer $m \neq 0$. Then $x$ has finite order $o(x)$, but the exponent $m$ might not be the order $o(x)$ of the element $x$. Prove that any such exponent $m$ must be a multiple of $o(x)$.
*Hint:* Letting $s = o(x)$, write $m = qs + r$ with $0 \leq r < s$. $\square$

***3.1.41A Exercise**. If $G$ is a finite group, prove that there is an integer $N \in \mathbb{N}$ such that $x^N = e$ for all $x$ in $G$. $\square$

***3.1.41B Exercise**. Explain why the only group of order $|G| = 2$ is isomorphic to $(\mathbb{Z}_2, +)$. $\square$

**3.1.42 Example**. Let $(G, \cdot, )$ be a group of order $|G| = 3$. Prove that $G$ must be cyclic, hence commutative, and that $G$ is isomorphic to $(\mathbb{Z}_3, +)$.

Discussion: The maximum possible order $m$ of any element in $G$ can only be $m = 1, 2$, or 3, but if $m = 1$ that would mean $x^1 = e$ for all $x$, and then $G$ consists of the single element $e$, contrary to the the fact that $|G| = 3$. If $m = 3$ there is some element such that $e, a, a^2$ are distinct and $a^3 = e$ so $G = \{e, a, a^2\} = \langle a \rangle$ is a cyclic group generated by $a$ and is $\cong (\mathbb{Z}_3, +)$ as claimed.

In the one remaining case we have $m = 2$, which means

$$\begin{aligned} x^2 &= e \quad \text{and} \quad x^{-1} = x \quad \text{for all } x \in G \\ o(x) &= 2 \text{ for every } x \neq e. \end{aligned}$$

Therefore if $a \neq e$ we have $a^2 = e$ and $H = \{e, a\} = \langle a \rangle$ is a cyclic subgroup isomorphic to $\mathbb{Z}_2$. There must be one other element $b \notin H$, so that $G = \{e, a, b\}$ (three distinct elements). We see that this case cannot arise by observing that the product $ab$ must equal $e, a$, or $b$. But every possibility leads to a contradiction:

$$\begin{aligned} ab = e &\Rightarrow b = a^{-1} = a \text{ (contrary to } a \neq b) \\ ab = a &\Rightarrow b = e \text{ by cancellation. Contradiction.} \\ ab = a^2 &\Rightarrow b = a \text{ by cancellation. Contradiction.} \end{aligned}$$

The Case $m = 2$ cannot occur, so $m = 3$ is the only viable possibility and $G \cong (\mathbb{Z}_3, +)$. □

**3.1.43 Exercise**. If $G$ is a group of order $|G| = 4$, prove that $G$ is abelian.
*Hint:* Look at the largest order $o(x) = n$ for an element of $G$ and examine the cases $n = 1, 2, 3, 4$ (some of which cannot occur). If $n = 2$, *every* $x \neq e$ has $o(x) = 2$. □

Obviously [1] is a cyclic generator of $(\mathbb{Z}_n, +)$ since its additive $k^{\text{th}}$ power is

$$k \cdot [1] = [1] + \ldots + [1] = [k] \quad ,$$

but there may be other cyclic generators (for instance [3] in $\mathbb{Z}_4$ – try it!). So it is interesting to ask whether the elements $[k]$ that generate $\mathbb{Z}_n$ under the (+) operation can be identified explicitly. In fact they can, if you know a little about greatest common divisors (Chapter 2). The answer reveals an unexpected connection with the group of multiplicative units $(\mathrm{U}_n, \cdot\,)$ in $\mathbb{Z}_n$, which we introduced in Section 2.5. It begins to reveal the strong links that exist between group theory and number theory.

**3.1.44 Theorem**. *For $n > 1$, a nonzero element $x = [k]$ in $\mathbb{Z}_n$ is a cyclic generator under the (+) operation $\Leftrightarrow \gcd(k, n) = 1$ – i.e. if and only if $[k]$ lies in the set $\mathrm{U}_n$ of multiplicative units in $\mathbb{Z}_n$.*

NOTE: The element [0] can't generate $(\mathbb{Z}_n, +)$ if $n \geq 2$. Furthermore, in Theorem 2.5.16 we showed that if $[k] \neq [0]$ then we have $[k] \in \mathrm{U}_n \Leftrightarrow \gcd(k, n) = 1$. As we noted there, $\gcd(k', n) = \gcd(k, n)$ if $k' \equiv k \pmod{n}$, so the property $\gcd(k, n) = 1$ is an attribute of the entire congruence class $[k]$, independent of any choice of class representative $k$.

PROOF: An element $b$ in a cyclic group $H = \langle a \rangle$ generates $H \Leftrightarrow$ the known generator is a power of $b$, $a = b^m$ for some $m \in \mathbb{Z}$. [ Implication ($\Rightarrow$) is obvious, and ($\Leftarrow$) follows because every $x \in G$ has the form $x = a^i = (b^m)^i = b^{mi}$ for some exponent $i$.]

Since $a = [1]$ is an additive generator of $(\mathbb{Z}_n, +)$ we have

$$\mathbb{Z}_n = \langle [k] \rangle = \{m \cdot [k] : m \in \mathbb{Z}\} \;\Leftrightarrow\; [1] = m_0 \cdot [k] = [m_0]\,[k] \text{ in } \mathbb{Z}_n$$

for some exponent $m_0 \in \mathbb{Z}$. This happens $\Leftrightarrow$ $[k]$ is a unit in $\mathbb{Z}_n$ with $[k]^{-1} = [m_0]$; by 2.4.6 $[k]$ is a unit $\Leftrightarrow \gcd(k, n) = 1$. □

This reveals the connection between finding

(a) Cyclic generators $[k]$ of the additive group $(\mathbb{Z}_n, +)$

(b) Units $[k] \in \mathrm{U}_n$ and their multiplicative inverses in $\mathbb{Z}_n$

(c) The greatest common divisor $\gcd(k, n)$, the smallest positive element in the lattice $\Lambda = \mathbb{Z}k + \mathbb{Z}n = \{rk + sn : r, s \in \mathbb{Z}\}$.

Given two integers $0 < k < n$ the smallest element in $\Lambda \cap \mathbb{N}$ can often be determined by hand. For instance, to determine $\gcd(4, 27)$ this way, a little experimentation, calculator in hand, shows that $7 \cdot 4 + (-1) \cdot 27 = 1$ so that $\gcd(4, 27) = 1$. Even when $k, n$ are quite large, the GCD Algorithm is extremely efficient at finding the greatest common divisor $\gcd(k, n)$ *without any need to determine the prime factorizations of* $k$ *and* $n$, which could take a long time. As we saw in Chapter 2, variants of this algorithm allow us to quickly find coefficients $r, s \in \mathbb{Z}$ such that $ra + sb = \gcd(a, b)$.

Later on we will prove a remarkable fact about the group of units $\mathrm{U}_n$.

> *The multiplicative group of units* $(\mathrm{U}_p, \cdot\,)$ *is always* CYCLIC
> *when the modulus* $n$ *is a prime.*

Although this assures existence of a cyclic generator in $\mathrm{U}_p$ actually finding one can be quite difficult for large primes, a fact that can be exploited in cryptography. Since all nonzero elements in $\mathbb{Z}_p$ have multiplicative inverses when $p$ is a prime, we have $\mathrm{U}_p = \mathbb{Z}_p^\times = \mathbb{Z}_p \sim \{0\}$ and $|\mathrm{U}_p| = p - 1$. Once we know this group is cyclic, it follows that it is isomorphic to the *additive* group $\mathbb{Z}_{p-1}$ of the same cardinality, so that $(\mathrm{U}_p, \cdot\,) \cong (\mathbb{Z}_{p-1}, +)$ when $p$ is a prime.

We're not yet ready to do this proof, but to illustrate we invite you to examine the situation in $\mathrm{U}_{13}$.

**3.1.44A Exercise**. Show that the multiplicative group of units $(\mathrm{U}_8, \cdot\,)$ is not a cyclic group. Show that $(\mathrm{U}_7, \cdot\,)$ is cyclic and exhibit a cyclic generator. □

**3.1.45 Exercise**. The multiplicative group of units $\mathrm{U}_{13} = \mathbb{Z}_{13}^\times = \{[1], [2], \ldots, [12]\}$ can be shown to be cyclic by direct calculation.

(a) Find all cyclic generators of $(\mathrm{U}_{13}, \cdot\,)$ by calculating the multiplicative subgroup generated by each element $[k] \neq [0]$ in $\mathbb{Z}_{13}$.

(b) We know that $[1]$ and $-[1] = [12]$ are units in $\mathbb{Z}_{13}$. If $a$ is a cyclic generator for $(\mathrm{U}_{13}, \cdot\,)$ is $b = [-1]\,[a]$ also a cyclic generator? □

**Other Subgroups of G.** In addition to forming $H = \langle S \rangle$ there are other ways in which a nonempty subset can determine a subgroup in $G$. We mention here just two possibilities, which reveal important stuctural features of any group – i.e. group theorists really want to calculate these objects in order to understand the group. Other structural features will be introduced later on.

**3.1.46 Definition.** *The* **center** $Z(G)$ *of a group* $G$ *is the set of elements that commute with everyone in* $G$

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

*These elements form a subgroup that is one of the most important structural features of any group.*

*More generally, given a nonempty subset* $S \subseteq G$ *we may define*

(a) *The* **centralizer** *of* $S$ *is* $Z_G(S) = \{x \in G : xs = sx \text{ for all } s \in S\}$

*Notice that* $x$ *is in the centralizer if and only if* $xsx^{-1} = s$ *for each* $s \in S$. *That is a stronger requirement than the condition* $xSx^{-1} = S$ *mentioned next, which would allow points to be moved around within* $S$ *as long as the set* $S$ *remains invariant.*

(b) *The* **normalizer** *of* $S$ *is* $N_G(S) = \{x \in G : xSx^{-1} = S\}$

*Both* $Z_G(S)$ *and* $N_G(S)$ *are subgroups of* $G$, *with* $N_G(S) \supseteq Z_G(S) \supseteq Z(G)$.

An element $g \in G$ is in the center $Z(G)$ if and only $gxg^{-1} = x$ for all $x$, so we may write

$$Z(G) = \{g : gxg^{-1} = x \text{ for all } x \in G\}$$

Obviously $G$ is abelian $\Leftrightarrow Z(G) = G$.

**3.1.47 Exercise.** If $x, g \in G$ prove that $g$ commutes with $x \Leftrightarrow g^{-1}$ commutes with $x$. Use this to prove that the center $Z(G)$ is actually a subgroup in $G$ □

**3.1.48 Exercise.** Prove that

(a) The centralizer $Z_G(S)$ of a nonempty set $S$ actually is a subgroup. In particular the center $Z(G)$ is a subgroup, being the centralizer of $S = G$ .

(b) $S' \subseteq S \Rightarrow Z_G(S') \supseteq Z_G(S)$. Note the reversal here.

(c) If $S$ generates the subgroup $H$ then $S$ and $H$ have the same centralizer.

(d) $Z_G(S) \subseteq N_G(S)$ □

*Hint:* Recall our "bottom up" description 3.1.26 of the group generated by $S \subseteq G$. □

***3.1.49 Exercise.** Let $S$ be a nonempty subset that generates a group $G$. Prove that $x$ is in the center of $G \Leftrightarrow x$ commutes with each generator – i.e. $xs = sx$ for all $s \in S$. *Note:* This greatly simplifies the task of deciding whether a group element $g$ lies in the center, since it is easier to decide if it commutes with a small set of generators than to show it commutes with all elements in $G$. □

We close this section with a curious result regarding *finite* subgroups. In defining "subgroup" we required that a subset have several properties in addition to $H \cdot H \subseteq H$, which in general does not suffice to make $H$ a subgroup; just consider $H = \mathbb{N}$ in $G = (\mathbb{Z}, +)$. It is therefore surprising that this is all we need if the group is *finite*, or even if $|G| = \infty$ and the subset $H$ is finite.

**3.1.50 Theorem.** *Let $H$ be a nonempty* FINITE *subset of a group $G$, such that $H \cdot H = \{h_1h_2 : h_1, h_2 \in H\}$ is equal to $H$. Then the identity element $e$ automatically lies in $H$ and $H$ is a subgroup of $G$.*

Proof: Fix an element $a \in H$ and form the powers $a, a^2, a^3, \ldots$. These all lie in $H$. Since $|H| < \infty$ there must exist a first index $k \geq 2$ for which this list contains a repeat, say $a^k = a^\ell$, with $1 \leq \ell < k$. Multiply on the right by $a^{-\ell}$ to get $e = a^{k-\ell}$. Since $k - \ell > 0$, the identity element $e \in G$ appears in $H$.

To see why $a^{-1}$ (inverse in $G$) also lies in $H$, there are two possibilities to consider. Case 1: $k - \ell = 1$. Then $a^\ell = a^k \Rightarrow a^{k-\ell} = a^1 = e$. In this case, $a^{-1} = a = e$ is in $H$. Case 2: Again we have

$$e = a^{k-\ell} = a \cdot a^{k-\ell-1}$$

but now $a^{-1} = a^{k-\ell-1}$ lies in $H$ because $k-\ell-1 \geq 1$. Thus $H$ has all properties required of a subgroup. □

### Section 3.1: Additional Exercises

***3.1.51 Exercise.** Let $G$ be a group (finite or not).

(a) If $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$ show that $G$ must be commutative.

(b) If every element in $G$ is its own inverse (so $a^2 = e$ for all $a \in G$) show that $G$ must be commutative. □

**3.1.52 Exercise.** Let $G$ be a nonempty set closed under an associative product $(\cdot)$, which satisfies the *one-sided versions* of the other two group axioms:

(a) There is an element $e \in G$ such that $a \cdot e = a$ for all $a \in G$.

(b) For any $a \in G$ there exists a "right inverse" $y(a)$ such that $a \cdot y(a) = e$.

Prove that $(G, \cdot\,)$ must be a group. $\square$

**3.1.53 Exercise.** Let $G = \mathrm{GL}(2, \mathbb{Z}_3)$ be the group of all $2 \times 2$ matrices

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{such that } ad - bc \neq 0, \text{ and } a, b, c, d \in \mathbb{Z}_3 \text{ (integers mod 3)}$$

Such matrices can be multiplied in the usual way and matrix multiplication is associative because multiplication and addition are associative in $\mathbb{Z}_3$. Furthermore we may define $\det A$ in the usual way, $\det(A) = ad - bc \in \mathbb{F}$. Carry out the following:

(a) Verify that $G$, equipped with the usual matrix multiplication, actually *is* a group.

(b) Compute the order $|G|$ of this group.

(c) If we require that $ad-bc = 1$ instead of $ad-bc \neq 0$ in defining $G$, we get a subgroup $\mathrm{SL}(2, \mathbb{Z}_3) \subseteq \mathrm{GL}(2, \mathbb{Z}_3)$. What is the order of this subgroup?

*Hints:* In (a) use: (i) Every nonzero element in $\mathbb{Z}_3$ has a multiplicative inverse (likewise in $\mathbb{Z}_n$ provided $n$ is prime); (ii) $\det(AB) = \det(A) \cdot \det(B)$ even though matrix entries lie in $\mathbb{Z}_3$, and the usual formula for the inverse $A^{-1}$ of a $2 \times 2$ matrix still works whenever $\det A \neq 0$. $\square$

**3.1.54 Exercise.** If $G$ is a group that has no *proper* subgroups ($H \neq \{e\}$ or $G$), prove

(a) $G$ must be finite and cyclic.

(b) $G$ is either trivial or isomorphic to $(\mathbb{Z}_p, +)$ for some prime $p > 1$. $\square$

**3.1.55 Exercise (The "ax + b Group").** For each pair $a, b \in \mathbb{R}$ with $a \neq 0$ define the mapping

$$\tau_{a,b} : \mathbb{R} \to \mathbb{R} \qquad \text{such that} \qquad \tau_{a,b}(x) = ax + b \qquad \text{for all } x \in \mathbb{R}$$

Prove that

(a) Each map $\tau_{a,b}$ is a bijection from $\mathbb{R}$ to $\mathbb{R}$ and $G = \{\tau_{a,b} : a \neq 0, b \in \mathbb{R}\}$ is a group under composition ($\circ$) of operators.

(b) Find explicit formulas for the parameters $(a'', b'')$ in the composition product

$$\tau_{a,b} \circ \tau_{a',b'} = \tau_{a'',b''}$$

in terms of $a, b, a', b'$.

(c) Find the parameters $a', b'$ that describe the inverse $\tau_{a',b'} = (\tau_{a,b})^{-1}$ of an element in $G$. $\square$

**3.1.56 Exercise.** If $H$ is a subgroup of an arbitrary group $G$ prove that the normalizer

$$N_G(H) = \{x \in G : xHx^{-1} = H\}$$

is a subgroup, and that $N_G(H) \supseteq H$. $\square$

**3.1.57 Exercise.** If $H$ is a subgroup of $G$ the intersection $N = \bigcap_{x \in G} xHx^{-1}$ is a subgroup of $G$. Explain why $aNa^{-1} = N$ for all $a \in G$. $\square$

## 3.2. Subgroups, Cosets, and Homomorphisms of Groups.

A subgroup $H$ in a group $G$ determines a natural decomposition of the group into disjoint *cosets* of $H$.

**3.2.1 Definition.** *Given any subgroup $H \subseteq G$, its* **left cosets** *are the subsets of the* *form $xH = \{xh : h \in H\}$ with $x \in G$. These are of interest because the whole group splits into a disjoint union of its distinct cosets $xH$. One can also define* **right cosets** *as sets of the form $Hx$, right translates of $H$ by elements $x \in G$. There is no difference between left- and right cosets if the group $G$ is abelian, but we will encounter many non-commutative groups where the distinction must be recognized. The group element $x$ is a* **coset representative** *for $xH$. A coset can have various representatives, and in Lemma 3.3.1 below we will determine when $x, y \in G$ yield the same coset, $xH = yH$.*

For simplicity we will focus on left cosets $xH$, but everything said here applies equally well to right cosets. The union of all cosets $xH$ is all of $G$ because

$$x \in G \Rightarrow x = x{\cdot}e \in xH$$

but in fact these cosets partition $G$ into *disjoint* pieces. To see why, we observe that

(13) *Two cosets $xH$, $yH$ are either identical as subsets of $G$ or are disjoint, with $xH \cap yH = \emptyset$.*

To prove this claim, consider what would happen if $xH$ and $yH$ overlapped: there would exist $h_1, h_2 \in H$ such that $xh_1 = yh_2$. Multiplying on the right by $h_1^{-1}$ we get $y = xh'$ where $h' = h_1h_2^{-1} \in H$, which in turn implies that

$$yH = (xh')H = x(h'H) = xH$$

(We have $h'H = H$ if $h' \in H$ because $H$ is a subgroup, see the following Exercise). Thus cosets are *identical* if they overlap at all, and the distinct cosets partition $G$.

**3.2.2 Exercise.** If $G$ is a group and $A, B \subseteq G$ we define the **product set** to be

$$AB = \{ab : a \in A, b \in B\}.$$

If $H$ a subgroup and $h_0 \in H$, prove that the following product sets are all equal to $H$.

(a) $H \cdot H = \{xy : x \in H, y \in H\}$ (product of two sets in $G$)

(b) $h_0H = \{h_0y : y \in H\}$

(c) $Hh_0 = \{xh_0 : x \in H\}$ □

The following example provides a concrete illustration of what all this means.

**3.2.3 Example.** The coordinate plane $\mathbb{R}^2$ becomes an abelian group $G = (\mathbb{R}^2, +)$ when equipped with the usual vector addition operation $(+)$, and the $x$-axis $H = \{(x, 0) : x \in \mathbb{R}\}$ is easily seen to be a subgroup. If $\mathbf{x} = (x_0, y_0)$ the additive coset

$$\begin{aligned} \mathbf{x} + H &= \{(x_0, y_0) + (s, 0) : s \in \mathbb{R}\} = \{(x_0 + s, y_0) : s \in \mathbb{R}\} \\ &= \{(x, y) \in \mathbb{R}^2 : x \in \mathbb{R}, y = y_0\} \end{aligned}$$

is just the horizontal line passing through the point $\mathbf{x}$. In this group the cosets $\mathbf{x} + H$ are precisely the horizontal lines in the plane, which is the disjoint union of these lines. Two vectors $\mathbf{x}, \mathbf{y}$ determine the same coset, with $\mathbf{x} + H = \mathbf{y} + H$ if and only if the difference vector $\mathbf{y} - \mathbf{x}$ lies in $H$, see Figure 3.2 □

**Homomorphisms.** A **homomorphism** between two groups $(G, \cdot)$ and $(G', *)$ is any map $\phi : G \to G'$ that **intertwines** the group operations, in the sense that

$$\phi(x \cdot y) = \phi(x) * \phi(y) \qquad \text{for all } x, y \in G \tag{14}$$

The map is an **isomorphism** if it satisfies (14) and is also a bijection. Then the inverse map $\phi^{-1} : G' \to G$ exists and it too intertwines the group operations, in the reverse

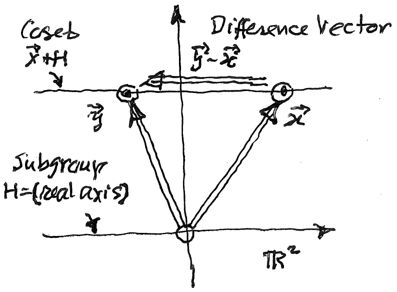

**Figure 3.2.** If $H = \{(x, 0) : x \in \mathbb{R}\}$ in $G = (\mathbb{R}^2, +)$, the coset $\mathbf{x} + H$ is the horizontal line passing through $\mathbf{x}$. Two vectors $\mathbf{x}$, $\mathbf{y}$ determine the same coset ⇔ their difference $\mathbf{y} - \mathbf{x}$ lies in $H$ (parallel to the $x$-axis).

direction. In fact, if $u, v \in G'$ there exist unique elements $x, y \in G$ such that $\phi(x) = u, \phi(y) = v$. Then by definition of $\phi^{-1}$ we have $\phi^{-1}(u) = x$, $\phi^{-1}(v) = y$, and we get

$$\begin{aligned}
\phi^{-1}(u * v) &= \phi^{-1}(\phi(x) * \phi(y)) \\
&= \phi^{-1}(\phi(x \cdot y)) \qquad \text{(since } \phi \text{ is a homomorphism)} \\
&= x \cdot y \qquad \text{(since } \phi^{-1} \circ \phi = \mathrm{id}_G) \\
&= \phi^{-1}(u) \cdot \phi^{-1}(v)
\end{aligned}$$

Both $\phi$ and $\phi^{-1}$ are isomorphisms.

Certain terminology is standard in discussing homomorphisms $\phi : G \to G'$ of groups.

(15)

1. The **kernel** of $\phi$ is the set of elements that get "killed" by $\phi$:

   $$\ker(\phi) = \{x \in G : \phi(x) = e'\} \ ,$$

   where $e'$ is the identity element in $G'$. The kernel is a subgroup of the initial group $G$.
2. The **range** range($\phi$) is the forward image of the initial group

   $$\mathrm{range}(\phi) = \phi(G) = \{\phi(x) : x \in G\}$$

   The range is always a subgroup of the target group $G'$, but it may be a proper subgroup.

Several basic properties of homomorphisms can be read out of equation (14).

(16) If $\phi : G \to G'$ is a homomorphism and $e \in G, e' \in G'$ are the respective identity elements, then $\phi(e) = e'$.

In fact, in any group the only solution of the "idempotent equation" $x^2 = x$ is the identity element; this follows if we multiply both sides by $x^{-1}$. In the present situation $\phi(e)^2 = \phi(e) * \phi(e) = \phi(e \cdot e) = \phi(e)$, so $\phi(e)$ satisfies this equation in $G'$ and $\phi(e) = e'$.

(17) If $\phi : G \to G'$ is a homomorphism and $x \in G$, the image $\phi(x^{-1})$ of an inverse is equal to the inverse $(\phi(x))^{-1}$ of the image in $G'$.

Since $x \cdot x^{-1} = e$ in $G$ we get $\phi(x) * \phi(x^{-1}) = \phi(e) = e'$ in $G'$, and (17) follows by definition of group inverse in $G'$.

(18) A homomorphism $\phi : G \to G'$ is one-to-one ⇔ $\ker(\phi) = (e)$

In fact, we have

$$\begin{aligned}\phi(x) = \phi(y) \quad &\Leftrightarrow \quad e = \phi(x)^{-1}\phi(y) = \phi(x^{-1}y)\\ &\Leftrightarrow \quad x^{-1}y \ \in K = \ker(\phi)\end{aligned}$$

so if $K$ is trivial we get $x^{-1}y = e$ and $x = y$. Conversely if $\phi$ is one-to-one the only element $x \in G$ such that $\phi(x) = e' = \phi(e)$ is $x = e$, so the kernel is trivial.

**3.2.4 Examples.** The *trivial homomorphism* $\phi_0 : G \to G'$ squashes all elements of the initial group to the identity element in $G'$, so that $\phi_0(x) = e'$ for all $x \in G$. The *identity map* $\mathrm{id} : G \to G$ of any group onto itself is another example of a homomorphism. More interesting examples include

(a) $G = G' = (\mathbb{Z}, +)$ with $\phi(x) = -x$, the *inversion* map. This map is clearly a bijection, and hence is a nontrivial isomorphism from $(\mathbb{Z}, +)$ to itself.

Actually, in any *abelian* group $(G, \cdot\,)$ the inversion map $J(x) = x^{-1}$ is an isomorphism $J : G \to G$. This is not true if $G$ is noncommutative because $J(xy) = (xy)^{-1} = y^{-1}x^{-1}$ need not equal $J(x)J(y) = x^{-1}y^{-1}$.

(b) In $G = (\mathbb{Z}_n, +)$ the inversion map takes the form

$$\phi([j]) = -[j] = [-1]\cdot[j] = [n-j] \qquad \text{for } 0 \leq j < n$$

It is clearly a bijection, and hence a nontrivial isomorphism from $(\mathbb{Z}_n, +)$ to itself (an "internal symmetry" of $\mathbb{Z}_n$).

(c) $G = (\mathbb{Z}, +)$ and $G' = (\mathbb{Z}_n, +)$ with $\phi(j) = [j]$. The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is well defined, with $\phi(0) = [0]$ and

$$\phi(k + \ell) = [k + \ell] = [k] + [\ell] = \phi(k) + \phi(\ell) \ \ ,$$

because of the way $(+)$ was defined in $\mathbb{Z}_n$ (cf. equation (15) of Chapter 2). The map is obviously surjective from $\mathbb{Z}$ to $\mathbb{Z}_n$ but its kernel

$$\ker(\phi) = \{k \in \mathbb{Z} : k \equiv 0 \pmod{n}\} = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

is not trivial. Thus $\phi$ fails to be one-to-one and is not an isomorphism. *Note:* The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is just the quotient map for the relation $x \underset{R}{\sim} y \Leftrightarrow x \equiv y \pmod{n}$ on $\mathbb{Z}$, as explained at the end of Chapter 2.

(d) $G = (\mathbb{R}, +)$ and $G' = (\mathbb{R}^\times, \cdot\,)$, the nonzero real numbers $\mathbb{R}^\times$ equipped with *multiplication* as its group operation. The usual *exponential map* $\phi(x) = e^x$ of Calculus is a group homomorphism from $\mathbb{R}$ to $\mathbb{R}^\times$. Its kernel is trivial because $e^x = 1 \Leftrightarrow x = 0$, so $\phi$ is one-to-one. But the map is not surjective, because $\phi(x) > 0$ for all $x$ while $\mathbb{R}^\times$ includes all negative numbers $y < 0$.

(e) If $(G, \cdot\,)$ is any *abelian* group and $k \in \mathbb{Z}$, the "$k^{\text{th}}$ *power map*" $\phi_k : G \to G$ given by $\phi_k(x) = x^k$ is always a homomorphism because $(xy)^k = x^k{\cdot}y^k$. In additive notation, writing $G = (G, +)$ we have $\phi_0(x) = 0_{_G}$ for all $x$ and for $k > 0$ the map $\phi_k$ becomes the *additive* $k^{\text{th}}$ *power map*

$$\phi_k(x) = k{\cdot}x = x + \ldots + x \quad (k \text{ times})$$

Similarly if $k < 0$. $\square$

**Notation:** The last example (e) will be particularly important in working with the additive groups $(\mathbb{Z}_n, +)$. In this situation $\phi_k$ takes the form

$$\phi_k([\ell]) = k \cdot [\ell] = [\ell] + \ldots + [\ell] = [k\ell] = [k]\cdot[\ell]$$

for all $[\ell] \in \mathbb{Z}_n$ and $k \in \mathbb{Z}$. Since the right-hand expression involves only the (mod $n$) congruence class of the "exponent" $k$, we see immediately that $\phi_{k'} = \phi_k$ as maps from $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ *if and only if* $k'$ is congruent to $k$ (mod $n$). It follows that there are only finitely many distinct homomorphisms $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ among the $\phi_k$, namely

$$\begin{aligned}
\phi_0 &= \text{ the ``zero homomorphism'' that maps every } [\ell] \text{ to } 0\cdot[\ell] = [0] \\
\phi_1 &= \text{ the identity map } \mathrm{id}_{\mathbb{Z}_n} \text{ because } \phi_1([\ell]) = 1\cdot[\ell] = [\ell] \\
\phi_2([\ell]) &= 2 \cdot [\ell] = [2\cdot\ell] = [2] \cdot [\ell] \\
&\vdots \\
\phi_{n-1}([\ell]) &= (n-1) \cdot [\ell] = [n-1] \cdot [\ell] = [-1] \cdot [\ell] = [-\ell] \quad \text{(inversion map)}
\end{aligned}$$

An arbitrary homomorphism $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ appears in this list because a homomorphism is determined by where it sends the additive generator [1] and we must have $\phi([1]) = [k]$ for some $0 \leq k \leq n-1$. If $\phi([1]) = [k]$ we get

$$\phi([2]) = \phi([1] + [1]) = \phi([1]) + \phi([1]) = [k] + [k] = 2 \cdot [k] = k \cdot [2] = [2k]$$

and similarly $\phi([\ell]) = k\cdot[\ell] = [k\cdot\ell] = \phi_k([\ell])$ for all $[\ell] \in \mathbb{Z}_n$. Thus $\phi = \phi_k$.

**3.2.5 Exercise.** In $(\mathbb{Z}_n, +)$ let $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be the homomorphism $\phi_3([\ell]) = 3\cdot[\ell] = [3\ell]$. Compute $\ker(\phi_3)$ and $\mathrm{range}(\phi_3)$ in the particular cases: (i) $n = 5$ and (ii) $n = 6$. □

The pattern of left cosets $xK$ of the kernel $K = \ker(\phi)$ of a homomorphism $\phi : G \rightarrow G'$ yields a geometric picture of the way $\phi$ acts, very much as the behavior of a linear operator $T : V \rightarrow V'$ between vector spaces is determined by the nature of its kernel $\ker(T) = \{\mathbf{v} \in V : T\mathbf{v} = \mathbf{0}\}$. Applying our previous discussion of cosets to the particular subgroup $H = \ker\,\phi$ we can read out the basic geometric facts about homomorphisms.

**3.2.6 Proposition.** *If $\phi : G \rightarrow G'$ is a homomorphism of groups and $K = \ker(\phi)$ is its kernel, then*

(a) *All points in a coset $xK$ map to a single point in $G'$ under $\phi$. Thus a homomorphism is constant on each coset of its kernel.*

(b) *Distinct cosets $xK \neq yK$ in $G$ are disjoint, with $xK \cap yK = \emptyset$, and they map to* DISTINCT *points in $G'$.*

*as shown in Figure 3.3. Furthermore $\phi$ is one-to-one, and hence an* ISOMORPHISM *from $G$ to the subgroup* $\mathrm{range}(\phi) \subseteq G'$, *if and only if its kernel is trivial:* $\ker(\phi) = (e)$.

Proof: Part (a) follows because

$$\phi(xk) = \phi(x) \cdot \phi(k) = \phi(x)\cdot e' = \phi(x)$$

for all $k \in K$. In (b),we have already seen that left cosets of any subgroup are disjoint. Furthermore

$$\phi(x) = \phi(y) \Leftrightarrow \phi(x^{-1}y) = \phi(x)^{-1}\phi(y) = e'$$

so $x^{-1}y \in K = \ker\,\phi$. Hence $\phi(yK) = \phi(xK)$ and $yK = xK$ by 3.2.2. □

We will have more to say about homomorphisms of groups, but for now we comment on the meaning of *isomorphism.* If two groups are isomorphic, which we indicate by writing $G \cong G'$, there is a bijection $\phi : G \rightarrow G'$ that intertwines the group operations, so that $\phi(x \cdot y) = \phi(x) * \phi(y)$. That means the groups have exactly the same properties as algebraic structures, and differ only superficially in the way we label objects in the group or in the symbols we use to indicate the group operations. *To an algebraist they are*

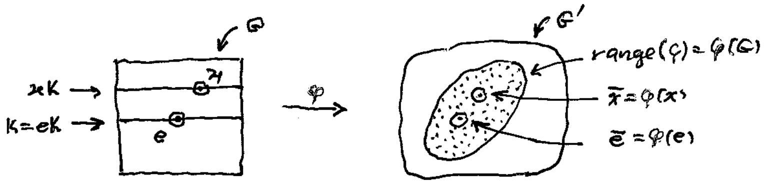

**Figure 3.3.** Mapping properties of a homomorphism $\phi : G \rightarrow G'$ are largely determined by its kernel $K = \ker(\phi) = \{x \in G : \phi(x) = e'\}$. Cosets $xK$ collapse to single points in $\text{range}(\phi) \subseteq G'$, and distinct cosets $xK \neq yK$ map to different points in the range.

*different models of the same group.* In contrast, existence of a *homomorphism* $\phi : G \rightarrow G'$ means that some, but not all, properties of the groups are closely related. The concepts of isomorphism and homomorphism play the same roles in algebra that congruence and similarity play in geometry.

The following concrete examples show how various familiar groups arise as homomorphic images of the particular groups $(\mathbb{R}, +)$ and $(\mathbb{Z}, +)$.

**3.2.7 Example.** Let $(S^1, \cdot\,)$ be the circle group, the set of complex numbers such that $|z| = 1$, equipped with complex multiplication as the group operation. The exponential map

$$\phi : (\mathbb{R}, +) \rightarrow (S^1, \cdot\,) \quad \text{given by} \quad \phi(\theta) = e^{2\pi i\theta} = \cos(2\pi\theta) + i\sin(2\pi\theta)$$

is a group homomorphism since $\phi(0) = 1 + i0$ and $e^{z+w} = e^z \cdot e^w$, which implies

$$\phi(\theta_1 + \theta_2) = e^{2\pi i(\theta_1+\theta_2)} = e^{2\pi i\theta_1} \cdot e^{2\pi i\theta_2} = \phi(\theta_1) \cdot \phi(\theta_2)$$

It is easily verified that $\text{range}(\phi)$ is all of $S^1$ because $e^{2\pi it} = \cos(2\pi t) + i\sin(2\pi t)$ sweeps out the unit circle as $t$ goes from $t = 0$ to $t = 1$. A real number $\theta$ is in the kernel $K = \ker(\phi)$ if and only if

$$1 = \phi(\theta) = e^{2\pi i\theta} \;\Leftrightarrow\; \begin{cases} \cos(2\pi\theta) = 1 \\ \sin(2\pi\theta) = 0 \end{cases} \quad \text{which happens} \Leftrightarrow\; \theta \in \mathbb{Z}$$

so $\ker(\phi) = \mathbb{Z}$ in $\mathbb{R}$. By 3.2.6 it follows that $\theta_1$ and $\theta_2$ have the same image under $\phi \Leftrightarrow e^{2\pi i(\theta_2-\theta_1)} = 1 \Leftrightarrow \theta_1$ and $\theta_2$ differ by an integer (i.e. they are "congruent mod 1"). □

**3.2.8 Example.** Similarly, there is a natural surjective homomorphism $\rho$ from $(\mathbb{R}, +)$ to the group $G = \{R_\theta : \theta \in \mathbb{R}\}$ of rotations about the origin in the Cartesian plane $\mathbb{R}^2$. As we showed in 3.1.11, $R_\theta = \text{id}_{\mathbb{R}^2}$ when $\theta = 0$ and $R_{\theta_1+\theta_2} = R_{\theta_1} \circ R_{\theta_2}$, so $G$ is a group under composition ($\circ$) of operators, and $\rho(\theta) = R_\theta$ is a surjective homomorphism $\rho : \mathbb{R} \rightarrow G$. Obviously $R_{\theta+2\pi k} = R_\theta$ for any integer $k$, and in fact

$$\theta \in \ker(\phi) \;\Leftrightarrow\; R_\theta = I \;\Leftrightarrow\; \theta \text{ is a whole multiple of } 2\pi \text{ radians}$$

Thus $\ker(\phi) = 2\pi\mathbb{Z} = \{2\pi k : k \in \mathbb{Z}\}$ and $\phi(\theta_1) = \phi(\theta_2) \Leftrightarrow \theta_1$ and $\theta_2$ differ by an integer multiple of $2\pi$. □

The strong similarity between Examples 3.2.7-3.2.8 will be explained when we take up the "First Isomorphism Theorem" later in this section.

**3.2.9 Example.** There is a natural surjective homomorphism $\psi_n$ from $(\mathbb{Z}, +)$ to the multiplicative group $(\Omega_n, \cdot\,)$ of $n^{\text{th}}$ roots of unity defined in 3.1.14. The appropriate map is

$$\psi_n(k) = \omega^k = e^{2\pi i k/n} \qquad \text{for all } k \in \mathbb{Z}$$

where $\omega$ is the primitive $n^{\text{th}}$ root of unity $\omega = e^{2\pi i/n}$. It is immediate from the exponent law $e^{z+w} = e^z \cdot e^w$ that $\psi_n : \mathbb{Z} \to \Omega_n$ is a homomorphism, and it is obviously surjective. To determine the kernel observe that

$$\begin{aligned} k \in \ker(\psi_n) \quad &\Leftrightarrow \quad 1 = \omega^k = e^{2\pi i k/n} \ \Leftrightarrow \ 2\pi \cdot \frac{k}{n} \text{ is a multiple of } 2\pi \\ &\Leftrightarrow \quad \frac{k}{n} \in \mathbb{Z} \ \Leftrightarrow \ k \text{ is divisible by } n \ \Leftrightarrow \ k \in n{\cdot}\mathbb{Z} \end{aligned}$$

Thus $\ker(\psi_n) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. By 3.2.6 we have $\psi_n(k) = \psi_n(\ell) \Leftrightarrow k$ and $\ell$ differ by a multiple of $n$. That is the same as saying $k \equiv \ell \pmod n$, so $\psi$ sends each $(\text{mod } n)$ congruence class in $\mathbb{Z}$ to a single point in $\Omega_n$, and different classes go to different roots of unity. Thus $\psi : \mathbb{Z}_n \to \Omega_n$ is bijective and $(\mathbb{Z}_n, +) \cong (\Omega_n, \cdot\,)$. $\square$

**3.2.10 Exercise.** Verify that the bijection $\psi : \mathbb{Z}_n \to \Omega_n$ in 3.2.9 intertwines the group operations $(+)$ and $(\cdot)$, making $\psi$ a group isomorphism as claimed. $\square$

**3.2.11 Exercise.** Below we give the multiplication tables for two groups $(G, \cdot\,)$ and $(G', *)$ of order 4.

(a) In each case, which is the identity element?

(b) Are both groups abelian?

(c) Are there any elements $a \neq e$ such that $a^2 = e$ – i.e with $o(a) = 2$?

(d) Is $G \cong G'$? (Prove or disprove.) $\square$

| | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $a$ | $d$ | $c$ |
| $c$ | $c$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $c$ | $b$ | $a$ |

**Product $x \cdot y$ in $G$**

| | $a'$ | $b'$ | $c'$ | $d'$ |
|---|---|---|---|---|
| $a'$ | $d'$ | $c'$ | $b'$ | $a'$ |
| $b'$ | $c'$ | $d'$ | $a'$ | $b'$ |
| $c'$ | $b'$ | $a'$ | $d'$ | $c'$ |
| $d'$ | $a'$ | $b'$ | $c'$ | $d'$ |

**Product $x * y$ in $G'$**

**3.2.12 Exercise.** Prove that the permutation group on three elements $S_3$ is *not* isomorphic to $(\mathbb{Z}_6, +)$, even though $|G| = 6$ in each case. $\square$

**3.2.13 Exercise.** If $G$ is any group and $a \in G$ any element of infinite order, explain why the subgroup it generates $H = \langle a \rangle$ is isomorphic to $(\mathbb{Z}, +)$. $\square$

**3.2.14 Exercise.** If $G$ is any group and $a \in G$ any element of finite order $o(a) = n$, explain why $H = \langle a \rangle$ is isomorphic to $(\mathbb{Z}_n, +)$. $\square$

**3.2.15 Exercise.** If $G$ is a finite *cyclic* group, say with $G = \langle x \rangle$ and $|G| = o(x) = n$, explain why $G$ is isomorphic to the additive group $(\mathbb{Z}_n, +)$. Thus all cyclic groups of the same size are isomorphic. $\square$

**3.2.16 Exercise.** Prove that the exponential map $\phi(t) = e^t$ is an isomorphism from $G = (\mathbb{R}, +)$ to the group $G' = \{x \in \mathbb{R} : x > 0\}$ of strictly positive real numbers, equipped with *multiplication* as the group operation. $\square$

***3.2.17 Exercise.** If a group $G$ is generated by a subset $S$, prove that any homomorphism $\phi : G \to G'$ *is determined by what it does to the generators*, in the following sense:

> *If $\phi_1, \phi_2 : G \to G'$ are homomorphisms such that $\phi_1(s) = \phi_2(s)$ for all $s \in S$, then $\phi_1 = \phi_2$ everywhere on $G$.*

This can be quite useful in constructing homomorphisms of $G$, especially when the group has a single generator. $\square$

Similarly a linear operator $T : V \rightarrow V'$ between vector spaces is determined by what it does to a set of basis vectors in the initial space $V$.

**3.2.18 Exercise.** For each integer $k \in \mathbb{Z}$ let $\phi_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be the homomorphism

$$\phi_k([\ell]) = k \cdot [\ell] = [k\ell] \qquad \text{for all } [\ell] \in \mathbb{Z}_n$$

as in the discussion of 3.2.1(e), where we remarked that

$$\phi_{k'} = \phi_k \text{ as maps on } \mathbb{Z}_n \;\Leftrightarrow\; k' \equiv k \pmod{n}$$

For each of the following moduli $n > 1$

$$\text{(a) } n = 7 \qquad \text{(b) } n = 8 \qquad \text{(c) } n = 12$$

determine all values of $0 \leq k < n$ such that $\phi_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is a *bijection.*
*Hint:* Since $\mathbb{Z}_n$ is finite, a homomorphism $\phi_k$ will be a bijection $\Leftrightarrow$ $\phi$ is one-to-one $\Leftrightarrow$ $\ker(\phi_k)$ is trivial (see 3.2.5). $\square$

For these $k$ the map $\phi_k$ is an *isomorphism* of $G$ with itself. These "self-isomorphisms," or "internal symmetries," of a group are referred to as **automorphisms** and will be of considerable interest as we go along. In each case in Exercise 3.2.18 you will discover that $\phi_k$ is a bijection $\Leftrightarrow$ $\gcd(k, n) = 1$.

**3.2.19 Exercise.** In each of the following decide whether the mapping $\phi : G \rightarrow G'$ is a *homomorphism.* For those that are, determine $\ker \phi$.

(a) $G =$ the nonzero real numbers $\mathbb{R} \sim \{0\}$ equipped with multiplication as the group operation, $G' = G$, $\phi(x) = x^2$ for all $x$.

(b) $G$ and $G'$ as in (a), with $\phi(x) = e^x$.

(c) $G = (\mathbb{R}, +)$, $G' = G$, $\phi(x) = x + 1$ for all $x$

(d) $G$ and $G'$ as in (c) with $\phi(x) = 13x$ for all $x$.

(e) $G$ is any abelian group, $G' = G$, and $\phi(x) = x^5$ for all $x$.

**3.2.20 Exercise.** Let $G$ be a finite abelian group with $|G| = n$. Let $k > 0$ be an integer such that $\gcd(k, n) = 1$. Prove that every $g \in G$ can be written in the form $g = x^k$ for some $x \in G$. $\square$

## 3.3 Coset spaces and quotient groups.

Let $H$ be a subgroup in a group $(G, \cdot\,)$. As in Section 3.2, the **left cosets** are the subsets having the form $xH = \{xh : h \in H\}$ for some $x \in G$, and the collection of all such cosets is denoted by $G/H$. Similarly we could define the space $H \backslash G$ of **right cosets**, which have the form $Hx$. We will mostly deal with $G/H$. We no longer assume $H$ is the kernel of a homomorphism $\phi : G \rightarrow G'$.

We are now going to regard $G/H$ as a "quotient space" of the group $G$, so you might want to review the discussion of "RST equivalence relations" at the end of Chapter 1, especially the definition of the quotient space $X/R$ associated with an equivalence relation $x \underset{R}{\sim} y$ on a set $X$. Let's start by asking when two group elements $x, y$ determine the same coset: $xH = yH$.

**3.3.1 Lemma.** *Let $H$ be a subgroup in $G$ and let $x, y$ be points in $G$. Then*

(a) *We have $xH = yH \Leftrightarrow$ there is some $h \in H$ such that $y = xh$. In particular, $xH = H \Leftrightarrow x \in H$.*

(b) *Two cosets $xH$ and $yH$ are either identical sets in $G$ or are disjoint.*

(c) *The relation $x \underset{R}{\sim} y \Leftrightarrow xH = yH$ is reflexive, symmetric, and transitive, and the equivalence classes for this relation are precisely the cosets in $G/H$: for any $x$ the class $[x] = \{g \in G : g \underset{R}{\sim} x\}$ is equal to $xH$.*

Proof: The first statement is a simple calculation: since $y \in yH$ the identity $xH = yH$ implies that $xh = y$ for some $h \in H$, and conversely if such an $h$ exists we get $yH = xhH = xH$ because $hH = H$ (recall 3.2.2). We proved (b) earlier, see (13), and we leave the reader to check that $x \underset{R}{\sim} y$ is in fact an RST equivalence relation. The equivalence class $[x] = \{y \in G : y \underset{R}{\sim} x\} = \{xh : h \in H\}$ is precisely the coset $xH$. □

The **space of cosets** $G/H$ is just the quotient space of equivalence classes under the RST relation $x \underset{R}{\sim} y$. Note carefully:

*Points* in the quotient space $G/H$ are *subsets* in the original group $G$.

The **quotient map** $\pi : G \rightarrow G/H$ for this relation is given by

$$\pi(x) = xH \qquad \text{(since } xH \text{ is the equivalence class for } x\text{)}$$

General properties of this surjective map follow directly from this definition.

- Under $\pi$, each coset $xH \subseteq G$ collapses to a single point in the quotient space $G/H$.
- Distinct (disjoint) cosets $xH \neq yH$ in $G$ are mapped by $\pi$ to distinct points in the quotient space $G/H$.

In Example 3.2.3 we described a quotient space $G/H$, in which $G = (\mathbb{R}^2, +)$, $H$ is the $x$-axis, and $G/H$ consisted of all horizontal lines in the plane; in that example the quotient map sends a vector $\mathbf{x} \in \mathbb{R}^2$ to the horizontal line $\mathbf{x} + H$, a point in $G/H$.

**3.3.2 Example.** If $G = (\mathbb{Z}, +)$ and $n \geq 2$ the set $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is a subgroup in $\mathbb{Z}$. Since $G$ is abelian there is no distinction between left and right cosets. Because the group operation is being written as $(+)$ the cosets take the form

$$\begin{aligned} x + H &= \{x + nk : k \in \mathbb{Z}\} \\ &= \{y \in \mathbb{Z} : y - x \text{ is a whole multiple of } n\} \\ &= \{y \in \mathbb{Z} : y - x \equiv 0 \pmod{n}\} \\ &= \{y \in \mathbb{Z} : y \equiv x \pmod{n}\} \end{aligned}$$

The cosets are precisely the (mod $n$) congruence classes in $\mathbb{Z}$, and the space of cosets $G/H$ is what we have been calling $\mathbb{Z}_n$. What's new is that we see $\mathbb{Z}_n$ as a quotient space associated with $G = \mathbb{Z}$. The quotient map $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ assigns to each $k \in \mathbb{Z}$ its (mod $n$) congruence class $[k] = k + n\mathbb{Z}$.

In this particular example the quotient space $G/H = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ inherits a natural group structure of its own, and the quotient map is easily seen to be a *homomorphism* from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +)$. (This is immediate from the definition of the group operation $[k] + [\ell] = [k + \ell]$ on congruence classes.) □

For more general groups $G$ and subgroups $H$ it is not always possible to impose a group structure on the quotient space $G/H$; it worked in the last example largely because the group was abelian.

Here is another example of this sort.

**3.3.3 Example.** Let $G = (\mathbb{R}, +)$ and $H = \mathbb{Z}$. The group is abelian, so left and right cosets coincide and have the form

$$\begin{aligned} x + H = x + \mathbb{Z} &= \{y \in \mathbb{R} : \exists\, k \in \mathbb{Z} \text{ such that } y = x + k\} \\ &= \{y \in \mathbb{R} : y \equiv x \pmod 1\} \end{aligned}$$

Obviously a coset $x+\mathbb{Z}$ is a periodic subset of $\mathbb{R}$ with spacing 1 between successive points. Note too that every coset can be written (uniquely) in the form $x+\mathbb{Z}$ with representative $0 \le x < 1$, so the cosets in $\mathbb{R}/\mathbb{Z}$ are labeled by the points in the interval $[0, 1)$ and the coset space $\mathbb{R}/\mathbb{Z}$ is uncountably infinite.

As in the last example, the quotient $G/H = \mathbb{R}/\mathbb{Z}$ inherits a group structure from $G$, obtained by imitating the definition of the $(+)$ operation in $\mathbb{Z}_n$. We define

$$(x + \mathbb{Z}) \oplus (y + \mathbb{Z}) = (x + y) + \mathbb{Z} \qquad \text{for } x, y \in \mathbb{R}, \tag{19}$$

and leave the reader to carry out the routine verification that

(i) The operation $(\oplus)$ is independent of the particular coset representatives $x$ and $y$ that appear in the definition (19).

(ii) Under the $(\oplus)$ operation $\mathbb{R}/\mathbb{Z}$ becomes an abelian group.

(iii) The identity element is the coset $[0] = 0 + \mathbb{Z}$ and additive inverses are given by $-(x + \mathbb{Z}) = (-x) + \mathbb{Z}$, so in terms of cosets we have $-[x] = [-x]$.

(iv) The quotient map $\pi : (\mathbb{R}, +) \to (\mathbb{R}/\mathbb{Z}, \oplus)$ is a surjective homomorphism of groups.

But what *is* the mysterious quotient group $(\mathbb{R}/\mathbb{Z}, \oplus)$? We now show it is isomorphic to something quite concrete and familiar, namely the "circle group"

$$S^1 = \{z \in \mathbb{C} : |z| = 1\} \quad \text{equipped with complex multiplication as the group law.}$$

The proof involves a construction that will be very important in what follows.

In Example 3.2.7 we saw that the exponential map $\phi(\theta) = e^{2\pi i\theta} = \cos(2\pi\theta) + i\sin(2\pi\theta)$ is a surjective homomorphism from $(\mathbb{R}, +)$ to the circle group $(S^1, \cdot\,)$. This map is, however, not one-to-one because its kernel $\ker(\phi) = \mathbb{Z}$, which we computed in 3.2.7, is nontrivial, recall (18). We now show how $\phi$ induces a *bijection* $\tilde{\phi}$ between the quotient space $\mathbb{R}/\mathbb{Z}$ and $S^1$ that turns out to be a group isomorphism. The idea is to define $\tilde{\phi}$ using coset representatives, letting

$$\tilde{\phi}(x + \mathbb{Z}) = \phi(x) = e^{2\pi i x} \qquad \text{for all } x \in \mathbb{R} \tag{20}$$

This makes sense because $\phi$ is constant on cosets $x + \mathbb{Z}$ since $\phi(x + m) = \phi(x)\cdot\phi(m) = \phi(x)\cdot e^{2\pi i m} = \phi(x)$ for all $x \in \mathbb{R}, m \in \mathbb{Z}$. Thus $\tilde{\phi}$ makes sense independent of the coset representative. Notice that our definition of $\tilde{\phi}$ makes the diagram in Figure 3.4 "commute," with $\tilde{\phi} \circ \pi = \phi$.

$$\begin{tikzcd} (\mathbb{R}, +) \arrow[r, "\phi"] \arrow[d, "\pi"'] & (S^1, \cdot\,) \\ (\mathbb{R}/\mathbb{Z}, \oplus) \arrow[ur, "\tilde{\phi}"'] & \end{tikzcd}$$

**Figure 3.4.** $\tilde{\phi}(x + \mathbb{Z}) = \phi(x)$.

Next, $\tilde{\phi}$ is one-to-one because, as noted earlier,

$$\tilde{\phi}(x + \mathbb{Z}) = \tilde{\phi}(y + \mathbb{Z}) \;\Leftrightarrow\; \phi(x) = \phi(y) \;\Leftrightarrow\; y = x + k \;\Leftrightarrow\; x + \mathbb{Z} = y + \mathbb{Z} \;\; .$$

The map is also onto, hence a bijection, because every point $p \in S^1$ can be expressed as $e^{2\pi i x} = \phi(x) = \tilde{\phi}(x + \mathbb{Z})$ for some real $x$. Finally, $\tilde{\phi}$ is a group homomorphism because

$$\begin{aligned} \tilde{\phi}\big((x + \mathbb{Z}) \oplus (y + \mathbb{Z})\big) &= \tilde{\phi}\big((x + y) + \mathbb{Z}\big) \;=\; \phi(x + y) \\ &= \phi(x) \cdot \phi(y) \;=\; \tilde{\phi}(x + \mathbb{Z}) \cdot \tilde{\phi}(y + \mathbb{Z}) \;\; . \end{aligned}$$

by definition of the $(\oplus)$ operation in $\mathbb{R}/\mathbb{Z}$. We conclude that $(\mathbb{R}/\mathbb{Z}, \oplus) \cong (S^1, \cdot\,)$ □

We will soon have more to say about the construction in 3.3.3, but first we consider a special class of subgroups $H$, the *normal subgroups.* For most groups and most choices of $H$ there is no way to define a group operation in the space of cosets $G/H$; we managed this miracle in Examples 3.3.2-3.3.3 only because the group $G$ was abelian. One might naively try to imitate what we did in defining the $(+)$ operations in $\mathbb{Z}_n$ or $\mathbb{R}/\mathbb{Z}$, by defining an operation $\otimes$ from $G/H \times G/H \rightarrow G/H$

$$(xH) \otimes (yH) = xyH \quad \text{for arbitrary cosets } xH, yH \in G/H$$

Unfortunately, the outcome $xyH$ is defined in terms of representatives $x, y$ of the initial cosets, and if no restrictions are placed on $H$ the coset $xyH$ might depend on the particular choice of representatives – i.e. there might exist $x', y'$ such that

$$x'H = xH \text{ and } y'H = yH, \text{ but } x'y'H \neq xyH$$

Indeed, $xyH$ might be a union of several cosets rather than a single coset in $G/H$. When this happens the outcome cannot be consistently determined from the cosets we started with and the "operation" $\otimes$ is not well-defined.

On the other hand a simple condition on $H$ insures that this construction does work, even if $G$ is nonabelian.

**3.3.4 Definition.** *A subgroup $N$ in $G$ is a* **normal subgroup** *if it has the property*

$$xN = Nx \qquad \textit{for all } x \in G\ , \tag{21}$$

*which means there is no difference between left- and right-cosets of $N$. All subgroups are normal if $G$ is abelian. Normality of a subgroup is indicated by writing $N \lhd G$.* □

It is easily seen that each of the following properties of a subgroup $N$ is equivalent to normality, which gives us some flexibility in determining whether a subgroup is normal.

**3.3.5 Lemma.** *If $N$ is a subgroup of $G$, each condition below implies the others.*

(a) The subgroup $N$ is normal: $xN = Nx$ for all $x \in G$.

(b) $xNx^{-1} = N$ for all $x \in G$.

(c) $xNx^{-1} \subseteq N$ for all $x \in G$.

(d) $xnx^{-1} \in N$ for all $x \in G, n \in N$.

Proof: Implications $(d) \Leftrightarrow (c) \Leftarrow (b) \Leftrightarrow (a)$ are obvious. To get $(c) \Rightarrow (b)$ we note that condition (c) says

$$\begin{array}{rcl} xNx^{-1} & \subseteq & N \quad \text{for all } x \in G, \text{ or} \\ N & \subseteq & x^{-1}Nx \quad \text{for all } x \in G \end{array}$$

But $x^{-1}$ runs through all of $G$ as $x$ runs through $G$, so in the last line we may replace $x^{-1}$ by $x$ (owing to the presence of the "for all" quantifier) to get

$$N \subseteq xNx^{-1} \quad \text{for all } x \in G$$

Since we already know that the reverse inclusion $xNx^{-1} \subseteq N$ holds, $N$ must be equal to $xNx^{-1}$ for all $x$, as required in (b). □

***3.3.6 Exercise.** If $H$ is a subgroup in $G$ and $N$ a normal subgroup, prove that the product set $HN$ is again a subgroup. If both $H$ and $N$ are normal subgroups, then $HN$

is also normal in $G$. $\square$

***3.3.6A Exercise.** Show that the center $Z(G) = \{x \in G : xg = gx, \forall g \in G\}$ is a *normal* subgroup of any group $G$. $\square$

Now we come to the definition of a product operation in the coset space $G/N$. When $N$ is a normal subgroup we can make sense of our earlier definition

$$(xN) \otimes (yN) = xyN \quad \text{for } x, y \in G \ . \tag{22}$$

We must first show that the outcome is independent of the coset representatives $x, y$ and then must show that the operation satisfies the group axioms. Neither is true in general; *normal* subgroups are what make it happen.

**Note:** If $N$ is a normal subgroup the product set $(xN) \cdot (yN)$ formed from two cosets can be rewritten as

$$(xN) \cdot (yN) = xyN$$

because $(xN)(yN) = x(Ny)N = x(yN)N = (xy)NN = xyN$ (recall 3.2.2). In this situation the outcome of the operation $(xN) \otimes (yN)$ introduced earlier is simply the product set $(xN) \cdot (yN)$, and we shall write it that way from now on.

**3.3.7 Theorem (Quotient Groups).** *Let $N$ be a* NORMAL *subgroup in a group $G$. Then the operation* (22) *is well defined: the outcome does not depend on the particular coset representatives $x$ and $y$. This product satisfies all the group axioms, making the coset space $G/N$ into a group in its own right. Finally, the quotient map $\pi : G \rightarrow G/N$ becomes a surjective homomorphism of groups with* $\ker(\pi) = N$.

Proof: The product is well defined: If we take other representatives such that $x'N = xN, y'N = yN$, then there exist elements $n_1, n_2 \in N$ such that $x' = xn_1, y' = yn_2$ and we get

$$x'y' = xn_1yn_2 = x(yy^{-1})n_1yn_2 = xy(y^{-1}n_1y)n_2$$

By Lemma 3.3.5(c) the element $y^{-1}n_1y$ is in $N$, hence the product to the right of $xy$ is an element of $N$ and we may write $x'y' = xyn''$ for some $n'' \in N$. Thus we get $x'y'N = xyn''N = xyN$ and the outcome in (22) does not depend on the choice of coset representatives.

Associativity of the operation in $G/N$ follows from associativity of the product operation in the original group because

$$(xN)\big((yN)\cdot(zN)\big) = (xN)(yzN) = x(Nyz)N = x(yzN)N = xyzN = \ldots = \big((xN)\cdot(yN)\big)zN$$

It is also clear that the *identity coset* $eN = N$ acts as an identity element in $G/N$, and that $x^{-1}N$ serves as the inverse to the coset $xN$. Thus $(G/N, \cdot)$ is a group and $\pi$ is a homomorphism of groups because $\pi(xy) = xyN = (xN) \cdot (yN) = \pi(x) \cdot \pi(y)$. $\square$

**3.3.8 Exercise.** If $G$ is an abelian group every subgroup $N$ is normal and the quotient group $G/N$ is always abelian. $\square$

The spaces $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ and $\mathbb{R}/\mathbb{Z}$ are examples of quotient groups. The latter example can be generalized considerably by taking $G = (\mathbb{R}^n, +)$ and $N$ the lattice subgroup of integer points $\mathbb{Z}^n$ in $n$-dimensional space. The group law is $(\mathbf{x} + \mathbb{Z}^n) + (\mathbf{y} + \mathbb{Z}^n) = (\mathbf{x} + \mathbf{y}) + \mathbb{Z}^n$, but in this algebraic picture the physical nature of the quotient group is elusive. It turns out that $\mathbb{R}^n/\mathbb{Z}^n$ can be viewed as an $n$-dimensional torus, which acquires a group law when we make this identification. For instance when $n = 2$, forming the quotient space $\mathbb{R}^2/\mathbb{Z}^2$ amounts to identifying points on opposite edges of the unit square $[0, 1] \times [0, 1]$ in $\mathbb{R}^2$, which in a certain sense is equivalent to making a donut-shaped torus. We omit these details.

It is not always easy to tell when two groups are isomorphic, especially when one of them is something as abstract as a quotient group. The next examples illustrates the sort of cunning that might be required to produce the necessary isomorphism map. We start with an easy one.

***3.3.9 Example.** In Example 3.2.8 we defined a surjective homomorphism $\psi : \mathbb{Z} \rightarrow \Omega_n$

$$\psi(k) = \omega^k = e^{2\pi ik/n} \qquad \text{where } \omega = e^{2\pi i/n} \text{ (the primitive } n^{\text{th}} \text{ root of unity)}$$

Its kernel was the subgroup $H = n\mathbb{Z} = \{nj : j \in \mathbb{Z}\}$ in $\mathbb{Z}$. Now consider the quotient group $\mathbb{Z}/H = \mathbb{Z}/(n\mathbb{Z})$. The group operation (22) in $\mathbb{Z}/H$ takes the form

$$(x + H) + (y + H) = (x + y) + H$$

The quotient homomorphism $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/(n\mathbb{Z})$ obviously has the same kernel $\ker(\pi) = H = n\mathbb{Z}$ as $\psi$; both $\pi$ and $\psi$ are constant on cosets $k+n\mathbb{Z}$. Following the ideas laid out in Example 3.3.3, this is all you need to construct an explicit isomorphism $\tilde{\psi} : \mathbb{Z}/H \rightarrow \Omega_n$ by taking $\tilde{\psi}(k + H) = \tilde{\psi}(k + n\mathbb{Z}) = \omega^k$. It follows that $\mathbb{Z}/H = \mathbb{Z}/(n\mathbb{Z}) = (\mathbb{Z}_n, +)$ is isomorphic to the group $(\Omega_n, \cdot\,)$ of $n^{\text{th}}$ roots of unity in $\mathbb{C}$. □

**3.3.10 Example.** Let $G$ be the set $\mathbb{C}^\times = \{z \in \mathbb{C} : z \neq 0\}$ of nonzero complex numbers, equipped with multiplication as the group operation. Within this abelian group we have the two-element normal subgroup $N = \{+1, -1\}$, which is obviously isomorphic to $(\mathbb{Z}_2, +)$. Since a coset has the form $zN = \{z, -z\}$, the quotient $G/N$ is obtained by lumping together each pair of points $+z, -z$ in $\mathbb{C}^\times$ to get a single element of the quotient group.

What is the nature of this quotient group? In particular,

> *Is $G/N$ isomorphic to the original group $\mathbb{C}^\times$, or have we created something new?*

It turns out that $G/N$ *is* isomorphic to $(\mathbb{C}^\times, \cdot\,)$; proving it is the challenge. The first step in mimicing the construction in 3.3.3 is to notice that there is a natural 2:1 homomorphism on $\mathbb{C}^\times$ whose kernel is also $N = \{\pm 1\}$, namely the "squaring map" $\phi : \mathbb{C}^\times \rightarrow \mathbb{C}^\times$ given by $\phi(z) = z^2$. As we saw in 3.2.1(e), this map is a homomorphism because $\mathbb{C}^\times$ is abelian; furthermore, it is surjective and is exactly two-to-one because every nonzero complex number $w$ has precisely two square roots, which lie in $\mathbb{C}^\times$. The kernel is $N = \ker\phi = \{\pm 1\}$. Notice what happens when we regard a coset $zN = \{\pm z\}$ as a subset of $\mathbb{C}^\times$ and take the forward image $\phi(zN)$: each coset collapses to a single point $z^2$.

This suggests the following ad-hoc construction of a natural surjective map $\Phi : G/N \rightarrow \mathbb{C}^\times$. Guided by 3.3.3 (taking the squaring map in place of the exponential map used there), we define

$$\Phi(zN) = \phi(z) = z^2$$

which makes sense because $\phi$ is constant on cosets $zN = \{z, -z\}$. Furthermore $\Phi$ is surjective because any complex number $z \neq 0$ has two square roots in $\mathbb{C}^\times$. $\Phi$ is also one-to-one, hence a bijection, because $\Phi(zN) = \Phi(wN) \Leftrightarrow z^2 = w^2 \Leftrightarrow w = \pm z \Leftrightarrow zN = wN$. To show $G/N \cong \mathbb{C}^\times$ it remains only to check whether $\Phi$ is a homomorphism. That is a routine calculation:

$$\Phi(zN \cdot wN) = \Phi(zwN) = (zw)^2 = z^2w^2 = \Phi(zN) \cdot \Phi(wN) \quad \square$$

In all these examples $G$ was abelian. We now prove a much more comprehensive result, valid whether or not $G$ is commutative.

**Isomorphism Theorems for Quotient Groups.** The isomorphisms in the last examples were all constructed "by hand." We now develop the basic machinery for deciding when quotient groups are isomorphic, so we won't have to re-invent the wheel every time we come to a new example. We start by clarifying the connection between homomorphisms $\phi : G \rightarrow G'$ and normal subgroups in $G$.

**3.3.11 Lemma.** *A subgroup $N$ in a group $G$ is normal if and only if $N$ is the kernel $\ker\phi = \{x \in G : \phi(x) = e'\}$ for some homomorphism $\phi : G \rightarrow G'$.*

Proof: Given $\phi$, its kernel $N$ is normal because

$$\phi(xnx^{-1}) = \phi(x)\phi(n)\phi(x^{-1}) = \phi(x)e'\phi(x)^{-1} = e'$$

for any $x \in G, n \in N$. Conversely, if $N$ is a normal subgroup the quotient map $\pi : G \rightarrow G/N$ is a homomorphism whose kernel is $N$. $\Box$

The mapping properties of any homomorphism are determined by the nature of its kernel. Our initial discussion of homomorphisms in 3.2.5 showed that

*If $\phi : G \rightarrow G'$ is a homomorphism, with kernel $K = \ker\phi = \{x \in G : \phi(x) = e'\}$, then*

(23)

(a) *Each coset $xK$ gets mapped to a single point in $G'$ under $\phi$.*

(b) *Distinct cosets $xK \neq x'K$ are disjoint in $G$ and get mapped to different points $\phi(x) \neq \phi(x')$ in $G'$*

*A homomorphism $\phi$ is one-to-one, and hence an isomorphism from $G$ to the subgroup $\phi(G) = \text{range}(\phi)$ in $G'$, if and only if its kernel is trivial: $\ker\phi = (e)$.*

(recall Figure 3.2). Furthermore any homomorphism $\phi : G \rightarrow G'$ is completely determined by its behavior on a set of generators of $G$, as explained in 3.2.17.

We now come to the *First Isomorphism Theorem* for quotient groups (there are two more). Let $\phi : G \rightarrow G'$ be a homomorphism and let $K = \ker\phi$. Obviously we could regard $\phi$ as a *surjective* homomorphism from $G$ to the subgroup $R = \text{range}(\phi) \subseteq G'$. Now consider the quotient map $\pi : G \rightarrow G/K$ (see Figure 3.5 at right). By definition of $\pi$ we have $\ker\phi = \ker\pi = K$. We claim that $\phi$ induces a natural *isomorphism* $\tilde{\phi}$ from $G/K$ to $R = \text{range}(\phi)$ that makes this diagram commute, in the sense that $\tilde{\phi} \circ \pi = \phi$. This is often expressed by saying that the original homomorphism $\phi$ "factors through" the quotient map $\pi$ to give the induced map $\tilde{\phi}$.

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\pi"'] & R \subseteq G' \\
G/K \arrow[ur, "\tilde{\phi}"'] &
\end{tikzcd}$$

**Figure 3.5.** Here we have $R = \text{range}(\phi)$, $K = \ker(\phi)$.

**3.3.12 Theorem (First Isomorphism Theorem).** *Let $\phi : G \rightarrow G'$ be a homomorphism, let $K = \ker(\phi)$, and let $\pi : G \rightarrow G/K$ be the quotient homomorphism. There is a unique map $\tilde{\phi} : G/K \rightarrow R = \text{range}(\phi)$ that makes the diagram in Figure 3.5 commute: $\tilde{\phi} \circ \pi = \phi$. This map is a group homomorphism and is bijective, so it is an isomorphism from the quotient group $G/K$ to $R = \text{range}(\phi)$. In particular, when $\phi$ is surjective we have $G' \cong G/K$.*

Proof: We know that $K$ is normal in $G$, so $G/K$ is a group, etc. Following the ideas laid down in Example 3.3.3, we try defining the missing map $\tilde{\phi}$ as

$$\tilde{\phi}(xK) = \phi(x) \qquad \text{for all } x \in G \ . \tag{24}$$

This map is well defined because $\phi : G \to G/K$ is constant on cosets $xK$. In fact, if $y \in xK$ there is some $k \in K$ such that $y = xk$, and then

$$\phi(y) = \phi(xk) = \phi(x)\phi(k) = \phi(x)e' = \phi(x)$$

Thus the outcome in (24) is independent of the coset representative.

Once we know $\tilde{\phi}$ is well defined, it is a homomorphism because $K$ is normal and

$$\tilde{\phi}(xK \cdot yK) = \tilde{\phi}(xyK) = \phi(xy) = \phi(x) \cdot \phi(y) = \tilde{\phi}(xK) \cdot \tilde{\phi}(yK)$$

Commutativity of the diagram is automatic from definition (24). Then $\tilde{\phi}$ is one-to-one because, by definition of $K = \ker \phi$,

$$\begin{aligned} \tilde{\phi}(xK) = \tilde{\phi}(yK) \quad &\Rightarrow \quad \phi(x) \ = \ \phi(y) \ \Rightarrow \ \phi(y^{-1}x) = \phi(y)^{-1}\phi(x) = e' \\ &\Rightarrow \quad y^{-1}x \in K \ \Rightarrow \ y^{-1}xK = K \ \Rightarrow \ xK = yK \end{aligned}$$

Furthermore, $\tilde{\phi}$ maps $G/K$ *onto* the range $R$ because $\phi = \tilde{\phi} \circ \pi$; this will make $\phi$ an isomorphism between the groups. In fact, if $r \in R$ then $r = \phi(x)$ for some $x \in G$, and then $\pi(x) = xK$ gives $\tilde{\phi}(xK) = \phi(x) = r$, making $\tilde{\phi}$ surjective. □

In 3.3.12 a homomorphism $\phi : G \to G'$ was given and $K$ was its kernel; if $\phi$ is surjective we proved that $G/K \cong G'$. In applying the First Isomorphism Theorem we often take a different point of view, in which some normal subgroup $K$ is *given* and we want to identify the abstract quotient group $G/K$ with some known group $G'$. Using 3.3.12 we can conclude that $G/K \cong G'$

> *provided we can find some surjective homomorphism $\phi : G \to G'$ whose kernel is the same as $K$, so* $\ker(\phi) = K$ *and $\phi$ is constant on cosets $xK$.*

The problem now is to find a suitable homorphism $\phi$ once $K$ has been specified. This is what we did in Example 3.3.10 where $G = \mathbb{C}^\times$ and the specified normal subgroup was $N = \{\pm 1\}$. There the "squaring map" $\phi(z) = z^2$ was a surjective homomorphism $\phi : \mathbb{C}^\times \to \mathbb{C}^\times$ such that $\ker(\phi) = N = \{\pm 1\}$, allowing us to conclude that $G/N \cong \mathbb{C}^\times$. □

**3.3.13 Example.** Let $G$ be the matrix group $\mathrm{GL}(n, \mathbb{C})$ of all $n \times n$ matrices $A$ with complex entries and $\det(A) \neq 0$. This *is* a group under matrix multiplication, and so is the subgroup $N = \mathrm{SL}(n, \mathbb{C})$ of matrices with determinant $+1$. We claim that $N$ is normal in $G$, and that the quotient group $G/N$ is isomorphic to the group $(\mathbb{C}^\times, \cdot\,)$ of nonzero complex numbers under multiplication.

Discussion: Normality of $N$ follows because the determinant has the properties

$$\det I = 1 \qquad \det(AB) = \det(A) \cdot \det(B) \qquad \det(A^{-1}) = \frac{1}{\det(A)}$$

If $A \in G$ and $B \in N$ we get $\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(B) = 1$, which shows that $ANA^{-1} \subseteq N$ for all $A \in G$. Thus $N$ is normal.

The determinant map $\phi(A) = \det A$ is a natural homomorphism $\phi : \mathrm{GL}(n, \mathbb{C}) \to \mathbb{C}^\times$. It is a group homomorphism because the determinant is multiplicative, and it is surjective because if $\lambda \neq 0$ in $\mathbb{C}$ the diagonal matrix $D = \mathrm{diag}(\lambda^{1/n}, \ldots, \lambda^{1/n})$ has $\det D = \lambda$. (Here $\lambda^{1/n}$ is any complex $n^{\text{th}}$ root of $\lambda$; for instance if $\lambda$ has polar form $\lambda = re^{i\theta}$ we can take the principal $n^{\text{th}}$ root $\lambda^{1/n} = r^{1/n}e^{i\theta/n}$ where $r^{1/n}$ is the usual $n^{\text{th}}$ root of a non-negative real number.)

The kernel of $\phi$ is precisely $N = \mathrm{SL}(n, \mathbb{C})$, by definition of $\mathrm{SL}(n, \mathbb{C})$. The conditions of the First Isomorphism Theorem are fulfilled. We conclude that $\mathrm{GL}(n, \mathbb{C})/\mathrm{SL}(n, \mathbb{C}) \cong (\mathbb{C}^\times, \cdot\,)$ as claimed. □

***3.3.14 Exercise (Second Isomorphism Theorem).** Let $A$ be any subgroup in $G$ and let $N$ be a normal subgroup. Show that

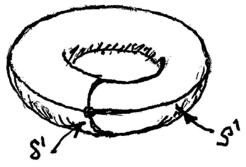

**Figure 3.6.** Points on a torus $X$ can be located by specifying two angle variables. Thus $X$ can be regarded as the Cartesian product $S^1 \times S^1$ of two circles.

(a) The product set $AN$ is a subgroup in $G$, with $N \lhd AN$.

(b) $A \cap N$ is a normal subgroup in $A$.

(c) $AN/N \cong A/(A \cap N)$

*Hint:* In (c) consider the map $\psi : A/(A \cap N) \to AN/N$ given by $\psi(a(A \cap N)) = aN$ for $a \in A$. Start by showing this map is well-defined: if $a(A \cap N) = a'(A \cap N)$ then $aN = a'N$ □

**3.3.15 Exercise (Third Isomorphism Theorem).** Let $G \supseteq A \supseteq B$ be groups such that $A$ and $B$ are both normal subgroups in $G$. Prove that $(G/B)/(A/B) \cong G/A$.
*Note:* This is the group-theory analog of the arithmetic relation $(a/c)/(b/c) = a/b$. □

**3.3.16 Exercise.** Let $N = \Omega_n$ be the group of $n^{\text{th}}$ roots of unity in $G = (\mathbb{C}^\times, +)$. Use 3.3.12 to prove that $G/N = \mathbb{C}^\times/\Omega_n$ is isomorphic to $(\mathbb{C}^\times, \cdot\,)$ for all $n = 1, 2, \ldots$. □

***3.3.16A Exercise.** The *torus group* $S^1 \times S^1$ is the Cartesian product of circles

$$S^1 \times S^1 = \{\mathbf{z} = (z_1, z_2) : z_1, z_2 \in \mathbb{C} \text{ and } |z_1| = |z_2| = 1\}$$

equipped with multiplication operation

$$\mathbf{z} \cdot \mathbf{w} = (z_1 w_1 \,,\, z_2 w_2)$$

(see Figure 3.6).

(a) Show that $(S^1 \times S^1, \cdot\,)$ is a commutative group. What is its identity element?

(b) Prove that the quotient group $(\mathbb{R}^2/\mathbb{Z}^2, +)$ is isomorphic to the torus group $(S^1 \times S^1, \cdot\,)$.

*Hints:* Recall the discussion for $\mathbb{R}/\mathbb{Z} \cong S^1$; use the First Isomorphism Theorem. □

**3.3.17 Exercise.** If $G$ is a cyclic group (finite or not) and $N$ is any normal subgroup, prove that the quotient group $G/N$ is cyclic.
*Note:* We have shown that any *subgroup* of a cyclic group is cyclic; the present result is the analogous result for quotients. □

**3.3.18 Exercise.** If $G = (\mathbb{Z}_n, +)$ and $d$ is a divisor of $n$, we have shown that there is a subgroup $H_d \subseteq \mathbb{Z}_n$ such that $|H_d| = d$, and we will soon prove that there is *exactly one* such subgroup for each divisor. Explain why the quotient group $(\mathbb{Z}_n/H_d, +)$ must be isomorphic to $(\mathbb{Z}_{n/d}, +)$.
*Hint:* By 3.3.17, the quotient is cyclic. What is its cardinality?
*Note:* Since $H_d \cong \mathbb{Z}_d$, this result says that $(\mathbb{Z}_n)/(\mathbb{Z}_d) \cong \mathbb{Z}_{n/d}$ for any divisor of $n$. □

***3.3.19 Exercise.** Use 3.3.12 to prove the following useful variant of the First Isomorphism Theorem.

**Proposition.** *If $G, G_1, G_2$ are groups and $\phi_i : G \to G_i$ are surjective homomorphisms* WITH THE SAME KERNEL $K = \ker(\phi_1) = \ker(\phi_2)$*, then* $G_1 \cong G_2$*.*

*Hint:* Prove $G_1 \cong G/K \cong G_2$. □

**3.3.20 Exercise.** In $\mathrm{GL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{C})$ define the subgroups of *scalar* matrices

$$\mathbb{C}^\times I = \{\lambda I : \lambda \neq 0 \text{ in } \mathbb{C}\} \qquad \Omega_n I = \{\lambda I : \lambda \in \Omega_n\}$$

where $\Omega_n$ are the complex $n^{\text{th}}$ roots of unity.

(a) Prove that $\mathbb{C}^\times I$ and $\Omega_n I$ are normal in $\mathrm{GL}(n, \mathbb{C})$ and $\mathrm{SL}(n, \mathbb{C})$ respectively.

(b) Prove that $\mathrm{GL}(n, \mathbb{C})/\mathbb{C}^\times I \cong \mathrm{SL}(n, \mathbb{C})/\Omega_n I$

*Hint:* Use the Second Isomorphism Theorem. If $N = \mathbb{C}^\times I$ show that $N \cdot \mathrm{SL}(n, \mathbb{C}) = \mathrm{GL}(n, \mathbb{C})$. □

The quotient group $\mathrm{PSL}(n, \mathbb{C}) = \mathrm{SL}(n, \mathbb{C})/\Omega_n I$ is the "projective special linear group" (hence the symbol "PSL"), a group that plays a crucial role in projective geometry. One can prove that this quotient is *not* isomorphic to $\mathrm{SL}(n, \mathbb{C})$ for $n \geq 2$. For one thing, we will eventually see that the center of $\mathrm{SL}(n, \mathbb{C})$ is precisely the set of scalar matrices $\Omega_n \cdot I$, and is nontrivial; $\mathrm{PSL}(n, \mathbb{C})$ has trivial center and cannot be isomorphic to any group with nontrivial center. A deeper result asserts that $\mathrm{PSL}(n, \mathbb{C})$ is not isomorphic to *any* group of matrices $G \subseteq \mathrm{GL}(m, \mathbb{C})$, $m \in \mathbb{N}$, even though it is a quotient of a matrix group.

### Section 3.3: Additional Exercises

In the next questions the **index** $[G : H]$ of a subgroup $H$ in $G$ is the number of $xH$-cosets $|G/H|$, which may be finite even if $G, H$ are infinite. It is convenient to label them as $H = eH, a_2H, \ldots, a_nH$ $(a_i \in G)$ when the index is finite.

**3.3.21 Exercise.** If $H$ is a subgroup of a group $G$, prove that the intersection

$$N = \bigcap_{x \in G} xHx^{-1}$$

is a subgroup and that $aNa^{-1} = N$ for all $a \in G$, so it is normal in $G$.
*Note*: $N$ is the largest normal subgroup in $G$ contained in $H$; it might be trivial. □

**3.3.22 Exercise.** If $H$ is a subgroup of finite index in a group $G$, prove that there are only finitely many distinct "conjugate" subgroups $aHa^{-1}$ for $a \in G$. □

**3.3.23 Exercise.** If $H$ is a subgroup of finite index in a group $G$, prove that there is a subgroup $M \subseteq H$ such that (i) $M$ has finite index in $G$, and (ii) $M$ is normal in $G$, so $aMa^{-1} = M$ for all $a \in G$.
*Note*: We do not assume $G$ and $H$ are finite. □

**3.3.24 Exercise.** Let $G = (\mathbb{R}^\times, \cdot\,)$ be the multiplicative group of nonzero real numbers, and let $N$ be the subgroup consisting of the numbers $\pm 1$. Let $G' = (0, +\infty)$ equipped with multiplication as its group operation. Prove that $N$ is normal in $G$ and that $G/N \cong G' \cong (\mathbb{R}, +)$. □

**3.3.25 Exercise.** If $G$ is a group and $H$ a subgroup such that $|G/H| = 2$, prove that $H$ must be a *normal* subgroup.
*Hint:* There are just two cosets, $H$ and $xH$. How are $H, xH$, and $Hx$ related? □

**3.3.26 Exercise.** If $H$ is a subgroup in $G$ and $N$ is a normal subgroup in $G$, prove that $N \cap H$ is *normal in* $H$. In particular an intersection $N_1 \cap N_2$ of normal subgroups is normal. □

**3.3.27 Exercise.** If $H$ is a subgroup of $G$, its *normalizer* is $N_G(H) = \{g : gHg^{-1} = H\}$. Prove that

(a) $N_G(H)$ is a subgroup.

(b) $H$ is a normal subgroup in $N_G(H)$.

(c) If $H \subseteq K \subseteq G$ are subgroups such that $H$ is a normal subgroup in $K$, prove that $K$ is contained in the normalizer $N_G(H)$.

(d) A subgroup $H$ is normal in $G \Leftrightarrow N_G(H) = G$.

*Note:* Part (c) shows that $N_G(H)$ is the largest subgroup of $G$ in which $H$ is normal. □

***3.3.28 Exercise.** If $x, y \in G$, products of the form $[x, y] = xyx^{-1}y^{-1}$ are called *commutators* and the subgroup they generate

$$[G, G] = \left\langle\, xyx^{-1}y^{-1} : x, y \in G \,\right\rangle$$

is the **commutator subgroup** of $G$. Prove that

(a) The subgroup $[G, G]$ is normal in $G$.

(b) The quotient $G/[G, G]$ is abelian.

(c) $H = [G, G]$ is the *smallest* normal subgroup such that $G/H$ is abelian.

*Hint:* In (a) recall that a subgroup $H$ is normal if $\alpha_g(H) = gHg^{-1} \subseteq H$ for all $g \in G$. What do conjugations $\alpha_g$ do to the generators $[x, y]$ of the commutator subgroup? □

**3.3.29 Exercise.** For $a, b$ real with $a \neq 0$ define the operators $\tau_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$ via $\tau_{a,b}(x) = ax+b$. Let $G$ be the group of operators $\{\tau_{a,b} : a, b \in \mathbb{R}, a \neq 0\}$ with composition $(\circ)$ as the group operation. Prove that

(a) The set of translations $N = \{\tau_{1,b} : b \in \mathbb{R}\}$ is a normal subgroup in $G$.

(b) The set of scaling operations $H = \{\tau_{a,0} : a \neq 0 \text{ in } \mathbb{R}\}$ is a subgroup but is not normal.

(c) Every element $g \in G$ has a unique factorization $g = nh$ with $n \in N, h \in H$

(d) The quotient $G/N$ is isomorphic to the group of nonzero real numbers $\mathbb{R}^\times$ under multiplication. □

**3.3.30 Exercise.** Let $G$ be the group $\mathbb{C}^\times$ of all nonzero complex numbers under multiplication. Let $G'$ be the group of real $2 \times 2$ matrices

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{with } a, b, \in \mathbb{R} \text{ and } a^2 + b^2 \neq 0 \ ,$$

with matrix multiply as the operation in $G'$. Verify that these matrices form a group and prove that $G \cong G'$ by exhibiting an explicit isomorphism $\phi : G \rightarrow G'$. □

**3.3.31 Exercise.** Let $G$ be the group of all real $2 \times 2$ matrices of the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \text{such that } ad \neq 0 \ .$$

Show that the commutator subgroup $[G, G]$ defined in Exercise 3.3.28 is precisely the subset of matrices in $G$ with 1's on the diagonal and an arbitrary entry in the upper right corner. □

## 3.4 Basic Counting Principles in Group Theory.

We now examine some basic counting principles in group theory. The following fundamental result places severe constraints on the possible pattern of subgroups in a group of finite order $|G| = n$, in terms of the divisors of $n$.

**3.4.1 Theorem (Lagrange).** *If $G$ is a group of finite order $|G| = n$ and $H$ is a subgroup, then $|H|$ must divide $|G|$. In fact, we have*

$$|G| = |G/H| \cdot |H| \tag{25}$$

*so the number of left cosets in $G/H$ also divides $|G|$.*

Proof: Any left translation $\tau_x : G \rightarrow G$, with $\tau_x(g) = xg$, is easily seen to be a bijection; for one thing, the operator $\tau_{x^{-1}}$ is its inverse because

$$\tau_x \circ \tau_{x^{-1}}(g) = x \cdot x^{-1} \cdot g = g \quad \text{for all } g \in G$$

That means all left $H$-cosets have the same cardinality: $|xH| = |\tau_x(H)| = |H|$. We proved earlier that $G$ is a disjoint union of its distinct left $H$-cosets so we get

$$|G| = \#(H\text{-cosets}) \cdot (\text{size of each coset}) = |G/H| \cdot |H|$$

as claimed. □

**3.4.2 Corollary.** *If $G$ is a finite group and $a \in G$ then the order $o(a)$ of this element must divide $|G|$.*

Proof: If $o(a) = k$ that means $\{e, a, a^2, \ldots, a^{k-1}\}$ are distinct and $a^k = e$. The cyclic group $H = \langle a \rangle$ has order $k$, which must divide $|G|$. □

**3.4.3 Corollary.** *If a group $G$ has finite order $|G| = n$ then $a^n = e$ for all elements $a \in G$.*

Proof: We know that the order $k = o(a)$ of a group element divides the order of the group. Thus $n = km$ and

$$a^n = (a^k)^m = e^m = e$$

as claimed. □

As an example of what can be done with this theorem, consider the cyclic group $G = \mathbb{Z}/(7\mathbb{Z}) = \mathbb{Z}_7$ of (mod 7) congruence classes, with $(+)$ as the group operation. The order of this group is a *prime* $p = 7$; by Lagrange, $G$ *cannot contain any subgroups* other than $H = \{e\}$ and $H = G$. By the same reasoning, applied to any prime $p > 1$, we obtain our first general structure theorem for finite groups

**3.4.4 Corollary.** *If $G$ is a finite group whose order is a prime $|G| = p > 1$, then $G = \langle a \rangle$ for every element $a \neq e$ and $G \cong (\mathbb{Z}_p, +)$. In particular, every finite group of prime order is cyclic, abelian.*

**3.4.5 Exercise.** If an element $x$ in a group satisfies $x^m = e$ for some integer $m \in \mathbb{N}$, prove that $m$ must be a multiple of the order $o(x)$ of that element. □

***3.4.6 Exercise.** By Lagrange, the cyclic abelian group $G = (\mathbb{Z}_{12}, +)$ could have subgroups of order $|H| = 1, 2, 3, 4, 6, 12$. By 3.1.30 we know that all subgroups of a cyclic group are themselves cyclic, so there is a subgroup with one of these orders if and only if there exist elements in $G$ of order $o(a) = 1, 2, 3, 4, 6, 12$.

(a) What is the size of the cyclic subgroup generated by $a = [2]$?

(b) Which of the possible orders of elements in this group actually occur?

(c) We know that $a = [1]$ is a cyclic generator of the whole group under the $(+)$ operation. Identify all other elements $a$ such that $G = \langle a \rangle$. □

Note the contrast: when $|G|$ is a prime, as with $\mathbb{Z}_7$, *every* element $a \neq e$ is a cyclic generator; this is no longer true in $\mathbb{Z}_n$ if $n$ has proper divisors.

***3.4.7 Exercise.** In $(\mathbb{Z}_n, +, \cdot\,)$ the *group of units* $\mathrm{U}_n$ is the set of elements $[k] \in \mathbb{Z}_n$ that have a multiplicative inverse: there exists an $[\ell]$ such that $[k][\ell] = [1]$.

(a) Explain why the set of units $(\mathrm{U}_n, \cdot\,)$, equipped with multiplication $[j] \cdot [k] = [jk]$ as its operation, is always a group.

Now consider the particular group $(\mathbb{Z}_{12}, +)$.

(b) Identify the set of units $\mathrm{U}_{12}$.

(c) What is the order of the multiplicative group $(\mathrm{U}_{12}, \cdot\,)$? Is this abelian group *cyclic*?

(d) Can you list *all* the subgroups of $(\mathrm{U}_{12}, \cdot\,)$?

*Hint*: What is the maximal order of any element $g \in \mathrm{U}_{12}$? □

***3.4.7A Exercise**. If $G$ is a group that has *no proper subgroups* ($H \neq (e)$ and $H \neq G$) prove that

(a) $G$ must be cyclic and finite.

(b) Either $G$ is trivial or $G \cong (\mathbb{Z}_p, +)$ for some prime $p > 1$.

*Note*: We do not assume $G$ is finite. Use Lagrange in (b). □

Earlier we showed that the additive group $(\mathbb{Z}_n, +)$, the exemplar of all cyclic groups of order $|G| = n$, must have subgroups $H_d$ of order $d$ for every divisor $d|n$, $1 \leq d \leq n$. By 3.1.36 all subgroups of $\mathbb{Z}_n$ are cyclic. Using Lagrange we now prove the definitive result regarding subgroups of $\mathbb{Z}_n$ (or any finite cyclic group).

**3.4.8 Theorem**. *In $(\mathbb{Z}_n, +)$, for every divisor $d$ of $n$, $(1 \leq d \leq n)$ there is a* UNIQUE *(cyclic) subgroup $H_d$ such that $|H_d| = d$*

PROOF: For existence we may take $H_d = \langle [n/d] \rangle$. This makes sense because $n/d$ is an integer, and the element $x = [n/d]$ has order $d$ because the elements

$$0 < \frac{n}{d} < 2 \cdot \frac{n}{d} < \ldots < (d-1) \cdot \frac{n}{d} < n$$

are distinct, with $d \cdot [n/d] = [0]$. Thus $|H_d| = d$.

For uniqueness, suppose there were two subgroups $A, B$ of order $d$. Since $\mathbb{Z}_n$ is abelian it is easy to see that the "product set" (written in additive notation)

$$A + B = \{x + y : x \in A, y \in B\}$$

is a *subgroup* in $\mathbb{Z}_n$. All subgroups of $\mathbb{Z}_n$ are cyclic, so there is a $y$ such that $A + B = \langle y \rangle$ and $o(y) = |A + B| \geq |A| = d$. On the other hand we must have $y = a + b$ and then $d \cdot y = (d \cdot a) + (d \cdot b) = 0 + 0 = 0$, which forces $o(y) \leq d$. Thus $o(y) = d$, $|A + B| = |A| = d$, and we must have $A = B = A + B$, as required to prove uniqueness. □

We now turn to a more sophisticated counting principle for groups. If $A, B$ are subsets of $(G, \cdot\,)$, the product set $AB$ is $\{ab : a \in A, b \in B\}$. Unless $G$ is abelian, we might not have $AB = BA$; in any case we have a crude estimate for the size of this set, namely $|AB| \leq |A| \cdot |B|$. (Why?) Unfortunately, that's not good enough – there could be many pairs for which $ab = a'b'$, so $|AB|$ could be a lot smaller than this upper bound.

Suppose $A$ and $B$ are *subgroups.* The product set $AB$ need not be a subgroup, though it often is. The next result tells us when this happens, and also tells us how to calculate $|AB|$ whether or not $AB$ is a subgroup.

**3.4.9 Theorem (A Counting Principle).** *Let $G$ be a group and $A, B$ subgroups. Then*

(a) *The product set $AB$ is a subgroup $\Leftrightarrow AB = BA$.*

(b) *Whether or not $AB$ is a subgroup, we always have*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|} \tag{26}$$

Proof: Write $A^{-1} = \{a^{-1} : a \in A\}$ for any subset $A \subseteq G$; obviously $A^{-1} = A$ if $A$ is a subgroup. To prove ($\Rightarrow$) in part (a): if $AB$ is a subgroup we have

$$AB = (AB)^{-1} = \{(ab)^{-1} = b^{-1}a^{-1} : a \in A, b \in B\} = B^{-1}A^{-1} = BA$$

because $A$ and $B$ are subgroups. To prove ($\Leftarrow$) let $a, a_1 \in A$ and $b, b_1 \in B$, and assume $AB = BA$. Then we may rewrite $ba_1 = a'b'$, and hence may rewrite the product of two elements $ab$, $a_1b_1$ in the product set $AB$ as follows

$$(ab)(a_1b_1) = a(ba_1)b_1 = a(a'b')b_1 = (aa')(b'b_1) \in AB$$

Thus the set $AB$ is closed under formation of products. Obviously the identity element $e = ee$ is in $AB$, and if $ab \in AB$ its inverse is also in $AB$ because $(ab)^{-1} = b^{-1}a^{-1} \in BA = AB$. Thus $AB$ is a subgroup.

As for the counting formula, one might get an idea how to procede by starting with the special case $A \cap B = (e)$. In general, we look at the map $\rho : A \times B \to AB \subseteq G$ defined by setting $\rho(a, b) = ab$, and ask:

> Question: *For how many pairs $(a, b)$ in the Cartesian product set $A \times B$ do the group elements $\rho(a, b) = ab$ take on the same value?*

Consider $a_1, a_2 \in A$ and $b_1, b_2 \in B$; clearly $a_1b_1 = a_2b_2 \Leftrightarrow a_2^{-1}a_1 = b_2b_1^{-1}$. But then the common value $x = a_2^{-1}a_1 = b_2b_1^{-1}$ is an element of $A \cap B$, and we have

$$a_2 = a_1x^{-1} \quad \text{and} \quad b_2 = xb_1 \qquad \text{for some element } x \in A \cap B\ . \tag{27}$$

Existence of an $x \in A \cap B$ such that (27) holds is a *necessary* condition in order that $a_1b_1 = a_2b_2$. It is also sufficient, because if (27) holds we have

$$\begin{aligned} &a_2 = a_1x^{-1} \in A \quad \text{and} \quad b_2 = xb_1 \in B \qquad (\text{true for any } x \in A \cap B) \\ &a_2b_2 = a_1x^{-1}xb_1 = a_1b_1 \end{aligned}$$

Finally, $(ax^{-1}, xb) = (ay^{-1}, yb)$ in the Cartesian product for $x, y \in A \cap B \Leftrightarrow x = y$, so there is a one-to-one match between pairs $(a', b')$ such that $a'b' = ab$ and elements $x \in A \cap B$.

We conclude that for any point $g \in AB$ the number of pairs such that $\rho(a, b) = g$ is equal to the number of points $x \in A \cap B$; furthermore, this is true no matter which point $g$ in the set $AB$ we look at. Put another way, given one pair $(a_0, b_0)$ such that $\rho(a_0, b_0) = g$, the other pairs with the same image are $\{(a_0x^{-1}, xb_0) : x \in A \cap B\}$, and there are precisely $|A \cap B|$ such pairs, a distinct pair for each $x$.

Thus the Cartesian product set $A \times B$, which has size $|A| \cdot |B|$, gets partitioned into disjoint "clumps" which correspond one-to-one with the distinct image points in the product set $AB$ under $\rho$. Since

$$\begin{aligned} |A \times B| &= \#(\text{“clumps”}) \cdot \#(\text{points per “clump”}) \\ &= \#(\text{image points in } AB) \cdot |A \cap B| \\ &= |AB| \cdot |A \cap B| \end{aligned}$$

we arrive at $|A| \cdot |B| = |A \times B| = |AB| \cdot |A \cap B|$. $\square$

## 3.5. Automorphisms and Inner Automorphisms.

An **automorphism** of a group is an isomorphism from $G$ to itself. These maps may be regarded as the "self-symmetries" of the group, and are important in understanding the structure of $G$. The set $\mathrm{Aut}(G)$ of all automorphisms becomes a group if we take composition of operators ($\circ$) as the product operation; the verification is routine. $\mathrm{Aut}(G)$ always includes the trivial automorphism $\mathrm{id}_G$; it also includes a special set of automorphisms – the **inner automorphisms** $\mathrm{Int}(G)$ – which are obtained by letting $G$ act on itself by **conjugation**. Just as in linear algebra, we say that one element $y$ is a **conjugate** of another element $x$ if there is some $g \in G$ such that $y = gxg^{-1}$. Focusing on the conjugation operators $\alpha_g(x) = gxg^{-1}$ we note the following easily verified facts.

***3.5.1 Exercise.** Let $G$ be any group and let $\mathrm{Int}(G)$ be the set of conjugation operations $\alpha_g(x) = gxg^{-1}$ on $G$. Prove that

(a) Each map $\alpha_g$ is a homomorphism from $G \rightarrow G$.

(b) Each map $\alpha_g$ is a bijection, hence an automorphism in $\mathrm{Aut}(G)$.

(c) $\alpha_e = \mathrm{id}_G$, the identity map on $G$.

(d) $\alpha_{xy} = \alpha_x \circ \alpha_y$ for all $x, y \in G$.

(e) $\alpha_{x^{-1}} = (\alpha_x)^{-1}$ (set-theoretic inverse map for the bijection $\alpha_x$)

It follows that $(\mathrm{Int}(G), \circ)$ is a group under composition of operators, and the inner automorphisms $\mathrm{Int}(G) = \{\alpha_g : g \in G\}$ are a subgroup of $\mathrm{Aut}(G)$.

(f) Prove that $\mathrm{Int}(G)$ is normal in $\mathrm{Aut}(G)$. □.

The subgroup $\mathrm{Int}(G)$ is trivial if $G$ is abelian, and so is the conjugation process: in an abelian group $y$ is conjugate to $x$ if and only if $y = x$. But in such groups there might be plenty of "outer" automorphisms lying in $\mathrm{Aut}(G) \sim \mathrm{Int}(G)$. Finding these "outer" automorphisms is an interesting problem. Here are a few examples.

**3.5.2 Example.** Let $G = (\mathbb{Z}, +)$. To determine $\mathrm{Aut}(G)$ we note that automorphisms are homomorphisms, and are determined by what they do to a set of generators. But $\mathbb{Z}$ is cyclic, with generator $x = 1$ under the ($+$) operation, so suppose $\phi$ is a homomorphism that sends 1 to $k$. Writing ($+$) for the group operation we must then have $\phi(m) = \phi(1 + 1 + \ldots + 1) = \phi(1) + \phi(1) + \ldots + \phi(1) = km$, at least for $m \geq 0$; but this is easily seen to be true for all $m \in \mathbb{Z}$, and $\phi = \phi_k$ is completely determined: it is just the "additive $k^{\text{th}}$ power map" $\phi_k(m) = k \cdot m$ for $m \in \mathbb{Z}$. We have determined all possible homomorphisms $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$. The maps $\phi_k$ are distinct since $\phi_k(1) = k$, and every automorphisms of $\mathbb{Z}$ must appear within the list $\{\phi_k : k \in \mathbb{Z}\}$.

Which of the $\phi_k$ are bijections? Clearly $\phi_1 = \mathrm{id}_G$ and $\phi_{-1} = -\mathrm{id}_G$ (the *inversion map*) are bijections, hence automorphisms. If $k = 0$, $\phi_0$ is the zero map and is not one-to-one; we leave the reader to verify that $\phi_k$ cannot be surjective if $k \neq -1, 0, 1$. Thus we have determined $\mathrm{Aut}(\mathbb{Z}, +) = \{\mathrm{id}_G, -\mathrm{id}_G\}$. Since there are only two elements, this group is abelian and isomorphic to $(\mathbb{Z}_2, +)$. Obviously $\mathrm{Int}(\mathbb{Z})$ is trivial. □

**3.5.3 Theorem.** *Let $G = (\mathbb{Z}_n, +)$, the group of (mod $n$) congruence classes in $\mathbb{Z}$. Then*

$$\big(\mathrm{Aut}(\mathbb{Z}_n, +), \circ\big) \text{ is isomorphic to the group of units } (\mathrm{U}_n, \cdot\,) \tag{28}$$

*where $\mathrm{U}_n = \{[k] \in \mathbb{Z}_n : 1 \leq k \leq n - 1$ and $\gcd(k, n) = 1\}$ is the group of units in $(\mathbb{Z}_n, +, \cdot\,)$, the elements with multiplicative inverses. The group law in $\mathrm{U}_n$ is multiplication, not addition, and in $\mathrm{Aut}(\mathbb{Z}_n)$ it is composition of mappings of $G$.*

Proof: The group $G = \mathbb{Z}_n$ is cyclic, with [1] as a generator under the ($+$) operation. As in Example 3.5.2, a *homomorphism* $\phi : G \rightarrow G$ is determined by what it does to this generator, and we can try all the possible assignments $\phi_k([1]) = [k],\ 0 \leq k \leq n-1$. In 3.2.1(e) we found that the homomorphisms of $(\mathbb{Z}_n, +)$ are precisely the maps

$$\phi_k([m]) = k\cdot[m] = [km] = [k]\cdot[m] \qquad \text{for } 0 \leq k \leq n-1$$

This formula shows that the map $\phi_k$ depends only on the (mod $n$) conjugacy class $[k]$ of $k$. The $\phi_k, 0 \leq k < n$, are a complete list of the homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_n$.

To be an automorphism $\phi_k$ must be bijective, but since $\mathbb{Z}_n$ is a finite set that will happen $\Leftrightarrow$ $\phi_k$ is one-to-one $\Leftrightarrow$ $\phi_k$ is onto. We claim that $\phi_k$ is onto precisely when $\gcd(k, n) = 1$. In fact, if $\phi_k$ is surjective there is some $[\ell]$ such that $[k][\ell] = [1]$, which means $[k] \in \mathrm{U}_n$ with $[k]^{-1} = [\ell]$, and hence that $k$ is relatively prime to $n$. Conversely, if $[k] \in \mathrm{U}_n$ and if $[m]$ is any element in $\mathbb{Z}_n$, we may write $[m] = [k]\cdot[k]^{-1}[m] = \phi_k([k]^{-1}[m])$, and so $\phi_k$ is surjective. That proves our claim.

We have shown that the elements in $\mathrm{Aut}(\mathbb{Z}_n, +)$ correspond one-to-one with the classes in $\mathrm{U}_n$ under the correspondence $\Phi : \mathrm{U}_n \rightarrow \mathrm{Aut}(\mathbb{Z}_n, +)$ that sends $[k]$ to $\Phi([k]) = \phi_k$. The preceding remarks show that this makes sense independent of the representative of the congruence class $[k]$, and that $\Phi$ is a bijection. It is also a homomorphism from $(\mathrm{U}_m, \cdot\,)$ to $(\mathrm{Aut}(\mathbb{Z}_n, +), \circ)$. In fact, we have

$$\phi_{[\ell][m]}([k]) = [\ell]\cdot[m]\cdot[k] = \phi_{[\ell]} \circ \phi_{[m]}([k])$$

which means that $\Phi([\ell][m]) = \Phi([\ell]) \circ \Phi([m])$ for all $[\ell], [m] \in \mathbb{Z}_n$. Thus $\Phi$ is a homomorphism, and hence an isomorphism, from $\mathrm{U}_n$ equipped with the $(\cdot)$ operation to $\mathrm{Aut}(G)$ equipped with $(\circ)$. □

We noted earlier that every cyclic group of finite order $|G| = n$ is isomorphic to $(\mathbb{Z}_n, +)$, so we have actually determined the automorphisms of all cyclic groups. Writing the group law as multiplication rather than $(+)$, the homomorphisms of $G$ are the distinct multiplicative $k^{\text{th}}$ power maps $\phi_k(a) = a^k$ for $0 \leq k \leq n-1$; the automorphisms are obtained by requiring that $\gcd(k, n) = 1$.

We close this section with an example illustrating the interplay between automorphisms and quotient groups.

**3.5.4 Definition.** *The* **center** *of a group $G$ is the set of elements $a \in G$ that commute with everbody in $G$:*

$$Z(G) = \{a \in G : ga = ag, \forall\, g \in G\} = \{a \in G : gag^{-1} = a, \forall\, g \in G\} \tag{29}$$

The center is a subgroup. It is also normal because if $a \in Z(G)$ and $b \in G$ we get

$$g(bab^{-1})g^{-1} = (gb)a(gb)^{-1} = a \qquad \text{for all } b, g \in G \quad ,$$

and hence $bab^{-1}$ is again in $Z(G)$ if $a \in Z(G)$. Thus $bZ(G)b^{-1} \subseteq Z(G)$ for all $b \in G$ and $Z(G) \lhd G$. For abelian groups the center is all of $G$.

The center becomes relevant in understanding automorphisms because a conjugation operation $\alpha_a(x) = axa^{-1}$ is trivial (with $\alpha_a = \mathrm{id}_G$) if and only if $axa^{-1} = x$ for all $x$, which means precisely that $a \in Z(G)$.

Now consider $\Phi : G \rightarrow \mathrm{Int}(G) \subseteq \mathrm{Aut}(G)$ given by $\Phi(g) =$ the inner automorphism $\alpha_g$. This map is a homomorphism because

$$\Phi(e) = \mathrm{id}_G \qquad \text{and} \qquad \Phi(xy) = \alpha_{xy} = \alpha_x \circ \alpha_y = \Phi(x) \circ \Phi(y)$$

Its range is $\mathrm{Int}(G)$ by definition of inner automorphisms. The kernel is just the center $Z(G)$:

$$\ker\Phi = \{g : \alpha_g = \mathrm{id}_G\} = \{g : gxg^{-1} = x, \forall\, x \in G\} = Z(G)$$

Applying the First Isomorphism Theorem 3.3.12 we obtain the commutative diagram shown in Figure 3.7. The induced diagonal map $\tilde{\Phi}$ is a bijective map to range$(\Phi) = \text{Int}(G)$, and is a homomorphism; hence we have an isomorphism of groups $\text{Int}(G) \cong G/Z(G)$.

We summarize this as follows:

$$\begin{tikzcd} G \arrow[r, "\Phi"] \arrow[d, "\pi"'] & \text{Int}(G) \subseteq \text{Aut}(G) \\ G/Z(G) \arrow[ur, "\tilde{\Phi}"'] & \end{tikzcd}$$

**Figure 3.7.**

**3.5.5 Theorem.** *For any group $G$ we have* $\text{Int}(G) \cong G/Z(G)$ *where* $Z(G)$ *is the center of* $G$*.*

**3.5.6 Exercise.** Verify the properties (i) $\alpha_e = \text{id}_G$, (ii) $\alpha_{xy} = \alpha_x \circ \alpha_y$, and (iii) $\alpha_{x^{-1}} = (\alpha_x)^{-1}$ for all $x, y \in G$. □

**3.5.7 Exercise.** If $G$ is a group and $N$ a normal subgroup, we may restrict any inner automorphism $\alpha_x : G \to G$ to $N$. Normality means $N$ is invariant under inner automorphisms, so we get an automorphism $\alpha_x|N \in \text{Aut}(N)$

$$(\alpha_x|N)(n) = \alpha_x(n) = xnx^{-1} \text{ for all } n \in N$$

Now consider the *restriction map* $R : (\text{Int}(G), \circ) \to (\text{Aut}(N), \circ)$ which takes an inner automorphism $\alpha_x$ of $G$ to its restriction $R(\alpha_x) = \alpha_x|N$. Verify that the restriction map is a homomorphism $R : \text{Int}(G) \to \text{Aut}(N)$.

*Note:* Arbitrary automorphisms $\beta \in \text{Aut}(G)$ *need not* leave a normal subgroup invariant, so we cannot expect the restriction $\beta|N$ to be an automorphism of $N$. Furthermore, the restriction $\alpha_x|N$ of an inner automorphism $\alpha_x$ on $G$ need not be an *inner* automorphism of $N$ – i.e. there might not be any $y \in N$ such that $\alpha_x(n) = yny^{-1}$ for all $n \in N$. □

***3.5.8 Exercise.** Show that the group $\text{Int}(G)$ of inner automorphisms is a *normal* subgroup in $\text{Aut}(G)$.

*Note*: The quotient $\text{Aut}(G)/\text{Int}(G)$ is regarded as the group of *outer automorphisms* $\text{Out}(G)$. □

### Section 3.5: Additional Exercises

**3.5.9 Exercise.** Are the following maps $\phi : G \to G$ automorphisms of their respective groups? Explain.

(a) $G = (\mathbb{Z}, +)$; $\phi(x) = -x$ for all $x$.

(b) $G =$ the positive real numbers $(0, \infty)$ with multiplication; $\phi(x) = x^2$.

(c) $G =$ a cyclic group of order 12; $\phi(x) = x^3$.

(d) $G =$ the permutation group $S_3$; $\phi(x) = x^{-1}$ for all $x$. □

**3.5.10 Exercise.** The permutation group $G = S_3$ on three objects has $6 = 3!$ elements

$$S_3 = \{e, (12), (23), (13), (123), (132)\}$$

Prove by direct calculation that $G \cong \text{Int}(G)$ – i.e. prove the center of $S_3$ is trivial. □

***3.5.11 Exercise.** Let $G = \{e, a, b, c\}$ be the group of order 4 such that $a^2 = b^2 = e$ and $c = ab = ba$.

(a) Make a multiplication table and verify that: (i) $G$ is abelian, (ii) $x^2 = e$ for all $x \in G$.

(b) Prove that $\text{Aut}(G)$ is isomorphic to the permutation group $S_3$.

*Hints:* (i) To see why automorphisms $\alpha$ might correspond to permutations, ask yourself: *What 3 objects might be permuted by any* $\alpha \in \text{Aut}(G)$*?* (ii) To show that a map $\phi : G \to G$

is a *homomorphism* you must check that $\phi(xy) = \phi(x)\phi(y)$ for all pairs $(x, y)$. However, this property is trivial if $x = e$ or $y = e$, or if $x = y$ (because $x^2 = e$ for all $x$). That means we only have to check 6 out of the original 16 pairs, and we can eliminate half of those remaining because $G$ is abelian. So for this group the homomorphism property can be checked by looking at only *three* pairs. □

**3.5.12 Exercise.** A subgroup $H$ in $G$ is said to be a **characteristic subgroup** if $\alpha(H) = H$ for *all* automorphisms $\alpha \in \mathrm{Aut}(G)$, not just the conjugations $\alpha_g(x) = gxg^{-1}$ as in the definition of a normal subgroup.

(a) Prove that a characteristic subgroup must be normal in $G$.

(b) Prove that the converse of (a) is false.

*Hint:* In (b), think: $G = (\mathbb{R}^2, +)$; then

$$\mathrm{Aut}(G) = \text{all linear operators } \tau_A(v) = Av \quad \text{(a } (2\times 2)\cdot(2\times 1) \text{ matrix product)},$$

where $A$ is any $2 \times 2$ matrix with nonzero determinant. □

**3.5.13 Exercise.** For any group $G$ prove that the commutator subgroup $[G, G]$ defined in Exercise 3.3.28 is a *characteristic subgroup*, as defined in 3.5.12.
*Hint:* What does an automorphism do to the generators of $[G, G]$?
*Note*: This example shows that if $G$ is abelian its automorphism gorup may nevertheless be noncommuative (while $\mathrm{Int}(G)$ is trivial). □

**3.5.14 Exercise.** Let $G$ be a group and $Z(G)$ its center. If $\alpha$ is any automorphism of $G$ prove that $\alpha(Z(G)) = Z(G)$, so the center of any group is a *characteristic subgroup.* □

**3.5.15 Exercise.** Since $p = 7$ is a prime the group of units in the ring $(\mathbb{Z}_7, +, \cdot\,)$ is

$$\mathrm{U}_7 = \mathbb{Z}_7^\times = \{[k] \in \mathbb{Z}_7 : [k] \neq [0]\}$$

so $|\mathrm{U}_7| = 6$.

(a) Show that $(\mathrm{U}_7, \cdot\,)$ is cyclic by directly calculating the orders of each of its elements.

(b) If $n \in \mathbb{N}$ and $[k]$ is a cyclic generator for $(\mathrm{U}_n, \cdot\,)$ is $-[k] = [-1]\cdot[k] = [-k]$ always a cyclic generator? Explain. □

Later on we will prove that $(\mathrm{U}_p, \cdot\,)$ is always cyclic if $p > 1$ is a prime. Since $|\mathrm{U}_p| = |\mathbb{Z}_p^\times| = p - 1$ this will imply that $(\mathrm{U}_p, \cdot\,) \cong (\mathbb{Z}_{p-1}, +)$. Combining this with (28) we conclude that

$$\big(\mathrm{Aut}(\mathbb{Z}_p, +), \circ\big) \cong (\mathrm{U}_p, \cdot\,) \cong (\mathbb{Z}_{p-1}, +) \tag{30}$$

for primes $p > 1$.

**3.5.16 Exercise.** Suppose $G$ is an abelian group and $a, b \in G$ have orders $m = o(a), n = o(b)$

(a) Explain why the order $o(ab)$ is a divisor of the least common multiple $\mathrm{lcm}\big(o(a), o(b)\big)$.

(b) Produce a counterexample showing that $o(ab)$ is not always equal to $\mathrm{lcm}\big(o(a), o(b)\big)$.

*Hint*: Try some elements in $\mathbb{Z}_n$ for suitably chose $n$. □

**3.5.17 Exercise.** If $G$ is a group, $Z$ is its center, and the quotient group $G/Z$ is *cyclic*, prove that $G$ must be abelian. □