Notes: F.P. Greenleaf, 2000-08

# Algebra I: Section 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 $x_1 \cdots x_n$ 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 *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

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

Therefore $y' = y$, and hence 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 $|G| = 1$. This is not a very interesting group. □
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 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. 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 no simple formula for it.

The function $\phi(n)$ is keyed to the distribution of primes in $\mathbb{N}$, and 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 $\mathbb{Z}_{12}$ and compute their inverses.
*Hint:* First check that in $\mathbb{Z}_n$ the multiplicative inverse of $[-1] = [n-1]$ is itself; then observe that $[-k] = [-1] \cdot [k]$. □

**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 there is an easy calculation for $\phi(n) = |\mathrm{U}_n|$. □

**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) $G = (\mathbb{R}^2, +)$, the Cartesian plane with *vector addition*

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

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) How about $G = (\mathbb{Z}_7^\times, \cdot)$? What might account for the difference between $\mathbb{Z}_9^\times$ and $\mathbb{Z}_7^\times$?

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

**3.1.2 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 $1 \leq i \leq n$. $\square$
7. The set $G = (\mathbb{C}, +)$ of *all* complex numbers, equipped with complex addition as the product operation, is a completely different abelian group. $\square$
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.

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

**Matrix groups.** We write $\mathrm{M}(n, \mathbb{F})$ for the set of all $n \times n$ matrices with entries in some field of scalars $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. This is a vector space, and hence a group, under the usual $(+)$ operation for matrices. The 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 product operation on matrices

$$(A \cdot B)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

As explained in linear algebra, this operation is associative, so that $A(BC) = (AB)C$. 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. The problem is that not every matrix $A$ has an inverse such that $A^{-1}A = I = AA^{-1}$. Nevertheless, certain subsets of $\mathrm{M}(n, \mathbb{F})$ are groups of great importance in geometry. To define them we must recall two facts from linear algebra.

> **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: $\det(AB) = \det(A) \cdot \det(B)$.

**3.1.7 Example (Matrix groups).** The set $\mathrm{GL}(n, \mathbb{F})$ of $n \times n$ matrices with nonzero determinant 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 just its matrix inverse $A^{-1}$. This group is infinite, and is not commutative except in the special case when $n = 1$. $\mathrm{GL}(n, \mathbb{F})$ is usually referred to as the $n$-dimensional **general linear group**.

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

   $$A^{-1} = A^{\mathrm{t}} \qquad \text{and} \qquad \det A = 1 \quad ,$$

   where $A^{\mathrm{t}}$ is the transpose matrix, defined by $(A^{\mathrm{t}})_{ij} = A_{ji}$. Clearly a matrix $A$ with determinant 1 is in $\mathrm{SO}(n, \mathbb{F}) \Leftrightarrow A^{\mathrm{t}}A = I = AA^{\mathrm{t}}$.
3. The **upper triangular group** consists of all $n \times n$ matrices of the form

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

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

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

There are many other matrix groups, which will be mentioned later. □

**3.1.8 Exercise.** In the last two examples above, verify that the 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. □

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

**3.1.10 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 that $H$ is a group when equipped with matrix multiply as its product operation.
*Note:* Condition (a) is superfluous, being a consequence of (b) + (c). □

The next example is geometric, and is the first of a whole series of examples extending to higher dimensions. It exploits a useful general fact about mappings $f : X \to X$ of a space into itself, namely

*Associativity of composition of maps:* The operation $(\circ)$ of composition of maps $f, g : X \to X$, given by

$$f \circ g(x) = f(g(x)) \qquad \text{for all } x \in X,$$

is automatically associative, so that $f \circ (g \circ h) = (f \circ g) \circ h$.

In fact, for any $x$ we have

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x))) = \ldots = (f \circ g) \circ h(x)$$

Thus if the elements of some proposed group $G$ are mappings of a space $X$, with composition $(\circ)$ as the group operation, associativity of the operation is guaranteed and need not be checked. This is important. For an abstract group – say one presented as a "multiplication table" – checking associativity is by far the most tedious computational task. Furthermore, if each mapping $f \in G$ is a *bijection*, then there is a "set-theoretic inverse map" $f^{-1}$ such that

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X \qquad \text{(the identity map of } X \text{ to itself)}$$

That means the identity map $\mathrm{id}_X$ is the identity element for $G$, and the group-theoretic inverse of any $f \in G$ is precisely the inverse map $f^{-1}$.

**3.1.11 Example (The 2-dimensional Rotation Group).** A *rotation* $R_\theta$ in the plane is the mapping $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ that rotates every vector counterclockwise about the origin $\mathbf{O} = (0, 0)$ by $\theta$ radians. We interpret

$R_0 = I$, the identity map of the plane

$R_{-\theta}$ = rotation *clockwise* by $\theta$ radians, the inverse of the map $R_\theta$.

It should be geometrically obvious that

$$R_{-\theta} = R_\theta^{-1} \qquad \text{and} \qquad R_{\theta_1+\theta_2} = R_{\theta_1} \circ R_{\theta_2} \text{ for all } \theta_1, \theta_2 \in \mathbb{R} \tag{2}$$

according to our interpretation of $R_{-\theta}$. It follows that the set $G$ of all rotations is a group, and that this infinite group is abelian (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.* In other words, the symbol $R_\theta$ is somewhat ambiguous; only the value of $\theta \pmod{2\pi}$ matters in determining the geometric operation.

Every rotation is a linear operator $R_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ and hence 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, then we have

$$R_\theta \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \qquad \text{for all } \mathbf{x} \in \mathbb{R}^2 \tag{3}$$

It can be shown that the matrices in (3) are precisely the special orthogonal matrices with entries in $\mathbb{R}$

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

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. Thus the geometric group of rotations $G$ is in every respect equivalent to the group of real $2 \times 2$ matrices $\mathrm{SO}(2)$ – i.e. the groups are *isomorphic*, in a sense we will make precise in Section 3.2. It will be quite useful to have two different ways of looking at the same group. □

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

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

(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 $L_A : \mathbb{R}^2 \to \mathbb{R}^2$ such that $L_A(x) = Ax$ (product of $2 \times 2$ by $2 \times 1$ matrix) is a rotation $R_\theta$ for some angle $\theta$. □

**3.1.13 Exercise (Euler's Theorem).** If $A \neq I$ in $\mathrm{SO}(3)$, prove that $\lambda = 1$ is an eigenvalue with multiplicity 1. Then prove that the linear operator $L_A : \mathbb{R}^3 \to \mathbb{R}^3$ given by $L_A(\mathbf{x}) = A\mathbf{x}$ (matrix multiply) is a rotation by some angle $\theta$ about the axis $\ell = \mathbb{R}\mathbf{e}$ where $\mathbf{e}$ is a nonzero eigenvector for the eigenvalue $\lambda = 1$. □

**3.1.14 Example ($\boldsymbol{\Omega_n = n^{\text{th}}}$ 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 $n^{\text{th}}$ root of unity is any $z$ such that $z^n = 1$. Since $|zw| = |z| \cdot |w|$ that forces $z$ to lie on the unit circle $|z| = 1$, and hence have the form $z = e^{i\theta}$. Then $z^n = e^{in\theta}$ equals $1 \Leftrightarrow n\theta$ is a whole multiple of $2\pi$ radians. Thus the distinct $n^{\text{th}}$ roots of unity are $\{e^{2\pi ik/n} : 0 \leq k < n-1\}$, which are precisely the powers $1, \omega, \omega^2, \ldots, \omega^{n-1}$ of the *primitive* $n^{\text{th}}$ *root* $\omega = e^{2\pi i/n}$.

**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* $\omega = e^{2\pi i/n}$.

The set $\Omega_n$ of $n^{\text{th}}$ roots forms 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 identity 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 $(\mathbb{C}^\times, \cdot\,)$. Later on we will see that $(\Omega_n, \cdot\,)$ is isomorphic to the familiar group $(\mathbb{Z}_n, +)$. $\square$

Next we introduce the permutation groups $S_n$, fundamental to all discussions of group theory. For the moment we provide a brief introduction; all of Chapter 5 will be devoted to further discussion of these groups.

**3.1.15 Example (Permutation groups: Part I).** The **permutation group** $S_n$ is the collection of all bijective maps $\sigma : X \to X$ of the interval $X = \{1, 2, \ldots, n\}$, 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:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_n \end{pmatrix}$$

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

$$e = \begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n \\ 1 & 2 & \ldots & k & \ldots & n \end{pmatrix}$$

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.

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

$$\sigma \text{ maps } \begin{cases} i_1 \to i_2 \to \ldots \to i_n \to i_1 & \text{(a cyclic shift of list entries)} \\ j \to j & \text{for all } j \text{ not in the list } \{i_1, \ldots, i_k\} \end{cases} \tag{4}$$

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

For example,

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

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

One-cycles $(k)$ are redundant; every one-cycle corresponds to the identity map $\mathrm{id}_X$. 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 $(4) = (5) = \mathrm{id}_X$.

The symbol $\sigma = (i_1, \ldots, i_k)$ denoting a cycle is ambiguous. If we make a cyclic shift of list entries we get other symbols

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

that describe the same mapping of $X$. For instance $(123) = (231) = (312)$ all specify the same operation $1 \to 2 \to 3 \to 1$ in $X$. If we mess up this order 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, as operators on $X$ we have $(123) \neq (132)$ because the first operator sends $1 \to 2$ while the second sends $1 \to 3$. 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** |
|---|---|
| $1 \xrightarrow{(123)} 2 \xrightarrow{(12)} 1$ | $1 \to 1$ |
| $2 \xrightarrow{(123)} 3 \xrightarrow{(12)} 3$ | $2 \to 3$ |
| $3 \xrightarrow{(123)} 1 \xrightarrow{(12)} 2$ | $3 \to 2$ |
| $4 \xrightarrow{(123)} 4 \xrightarrow{(12)} 4$ | $4 \to 4$ |
| $5 \xrightarrow{(123)} 5 \xrightarrow{(12)} 5$ | $5 \to 5$ |

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

$(12)(123) = (1)(23)(4)(5) = (23)$ in $S_5$

By a similar tracing of outcomes you can verify that

$(123)(14) = (1423)(5) = (1423)$ in $S_5$

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

**3.1.17 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 $S_5$ □

**3.1.18 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. □

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

(a) (12)
(b) (123)
(c) Any 2-cycle $(i_1, i_2)$ with $i_1 \neq i_2$
(d) Any $k$-cycle $(i_1, \ldots, i_k)$ with distinct $i_j$ □

**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 to use multiplicative notation with commutative groups, but that would be really awkward in some cases. How would you like to discuss the group of integers $(\mathbb{Z}, +)$ if we insisted on using some sort of multiplicative notation $m * n$ for the group operation instead of $m + n$? 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 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 notation for the $k^{\text{th}}$ power of an element $x$ becomes

$$k \cdot x = x + \ldots + x \ \ (k \text{ times}) \qquad \text{instead of} \qquad x^k = x \cdot \ldots \cdot x \ \ (k \text{ times})$$

and so on. Below we give a handy 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 widely used that you simply must get used to it. It is worth noting that in the particular additive group $(\mathbb{Z}_n, +)$ all of the following expressions

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

stand for the "$k^{\text{th}}$*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

(5)
(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 $H \times H \to H$. One easily verifies that $(H, \cdot\,)$ satisfies all the group axioms G.1 – G.3. For instance, associativity of the induced operation in $H$ follows immediately from associativity in the larger set $G$.

Subgroups always exist. For instance there are the trivial subgroups $H = (e)$ and $H = G$; all other subgroups, if any, are referred to as **proper subgroups**. The suggestive notation $H \leq G$ is often 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 $S \subseteq G$. This idea, that every subset $S$ generates a *subgroup* $H = \langle S \rangle$, is based on the following easy theorem.

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

$$H = \bigcap_{\alpha \in I} H_\alpha$$

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

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 3.1.17, and is evidently the *smallest possible* subgroup that contains $S$.

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

$$\langle S \rangle = \bigcap \{H : H \text{ is a subgroup and } H \supseteq S\} \tag{6}$$

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

Notice that 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, there is an alternative "bottom-up" description of $\langle S \rangle$ which tells you 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. It is not hard to see that both sets generates the same subgroup in $G$.

**3.1.22 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 $S \cup S^{-1}$ all generate the same subgroup in $G$. $\square$

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:

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

It is crucial to realize that this set of "words" is precisely the subgroup generated by $S$. We leave the verification to the reader.

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

$$\langle S \rangle = W_S = \{\, a_1 \cdots a_r : r < \infty \text{ and } a_i \in S \cup S^{-1} \,\} \tag{8}$$

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 $W_S$? $\square$

**3.1.24 Exercise.** Do we 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 $G = (\mathbb{Z}, +)$. □

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

(i) $S_1 = \mathbb{N}$ (ii) $S_2 = \{2\}$ (iii) $S_3 = \{2, 3\}$ (iv) $S_4 = \{3, 21\}$ (v) $S_5 = \{3, 23\}$

Determine the subgroups they generate. □

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

(a) The single element $x = [2]$
(b) The single element $y = [3]$
(c) The two elements $x = [2]$ and $y = [3]$ □

**3.1.27 Exercise.** Show that 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 $m_0 = \min\{H \cap \mathbb{N}\}$ by the Minimum Principle. □

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 different 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.

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

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

*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) $(a^m)^n = a^{mn}$
(d) *If $G$ is abelian then* $(ab)^n = a^n \cdot b^n$.

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

**3.1.29.** Suppose the group law is written in additive form $(G, +)$. Rewrite the Exponent Laws 3.1.28 in additive notation.
*Note:* You will find that the Exponent Laws written in this form recapitulate several of the axioms in *AxiomSetI* in the definition of $\mathbb{Z}$. □

It is a simple matter to verify 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 $a$. 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 the set $H$ *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.

**3.1.30 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 we would have $a^k = a^{k-\ell} \cdot a^\ell = a^\ell$. Multiplying both sides by $a^{-\ell}$ we get $a^{k-\ell} = e$, which is impossible since $k - \ell > 0$, contrary to our definition of $k$ and $\ell$.

Thus 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 $H$ 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

(9) *Let $k$ be the smallest index $k > 0$ for which a repeat occurs. Then $a^k = e$ – i.e. the first repeat* CANNOT *occur because $a^k$ is equal to some intermediate power $a^\ell$.*

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 cancel $a^\ell$ 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 $a^k = e$. The entries in this list are distinct, the subgroup is finite with $|H| = k$, and $H$ is abelian (combine the exponent laws with the fact that $a^k = e$). 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 $\mathbb{Z}_n$; this makes sense because $a^k = e$, which implies that $a^{j+nk} = a^j$ for all $n$. Thus the value of $a^j$ depends only on the (mod $k$) congruence class of $k$ in $\mathbb{Z}$ and not on $k$ itself. In view of the following exercise, $H = \langle a \rangle$ is just a copy of the finite group $(\mathbb{Z}_k, +)$ embedded in $G$.

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

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

*Hint:* Exponent laws. □

These observations can be summarized as follows.

**3.1.32 Definition.** *Let $G$ be a group and let $a \in G$. The* **order** *$o(a)$ of a group element 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 it is clear that 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.

**3.1.33 Theorem (Structure of Cyclic Subgroups).** *Let $G$ 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 $G$.*

**3.1.34 Exercise.** Let $G = (\mathbb{Z}_{12}, +)$. The element $[1]$ is a cyclic generator of the whole group.

(a) Which other elements $a = [j]$ are cyclic generators of $G$?

(b) Determine the order of each element $a \in G$ and describe the corresponding cyclic subgroups $H = \langle a \rangle$. □

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

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

**3.1.36 Proposition.** *Any subgroup of a cyclic group is also cyclic.*

Proof: Let $G = \langle a \rangle$ be a cyclic group whose generator has order $o(a) = n$, 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 $G$. Let $m$ be the smallest positive exponent such that $b = a^m$ lies in $H$; obviously $1 < m < n$ if $H$ is proper. (Why?)

We claim that $H$ is equal to $H_0 = \langle b \rangle$. Obviously $b \in H$, so $b^i \in H$ for all $i \in \mathbb{Z}$, and $H_0 = \langle b \rangle \subseteq H$. On the other hand if $y \in H$ then $y = a^\ell$ for some $\ell \in \mathbb{Z}$. Adding a suitable multiple of $m$ to $\ell$ we get $\ell' = \ell + km$ such that $0 \leq \ell' < m$ (Euclidean Division Algorithm). But $a^{\ell'} = a^\ell \cdot (a^m)^k = y \cdot (b)^k$ lies in $H$ because $y \in H$, and the exponent $\ell'$ is smaller than the minimal nonzero exponent $m$. Therefore $\ell' = 0$ and $y = b^{-k} \in H_0$, proving that $H \subseteq H_0$. □

**3.1.37 Exercise**. Let $n > 1$. For each divisor $d|n$, $1 \leq d \leq n$, construct an example of a (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 want to try it first for, say, $n = 12$. □

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 $\mathbb{Z}_n$.

**3.1.38 Exercise**. Suppose a group element $x \in G$ satisfies $x^m = e$ for some integer $m \neq 0$, so in particular $x$ has finite order $o(x)$. Prove that any such exponent $m$ must be a multiple of $o(x)$.
*Hint:* Letting $s = o(x)$, write $m = qs + r$ with $0 \leq r < s$. □

**3.1.39 Exercise**. Let $G$ be a group of order $|G| = 3$.

(a) Show that we cannot have $o(x) = 2$ for any element in $G$.

(b) Prove that $G$ is abelian (so $xy = yx$ for all $x$ and $y$).

*Hint:* If $H = \langle a \rangle$ for some element $a \in G$ of order 2, then $H = \{e, a\}$ and we may write $G = \{e, a, b\}$ with $b \neq e, a$. Where does $ab$ lie in $G$? $\square$

**3.1.40 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). $\square$

Obviously [1] is a cyclic generator of the additive group $(\mathbb{Z}_n, +)$ since $k \cdot [1] = [1] + \ldots + [1] = [k]$, 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 a curious 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.

**3.1.41 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 $[k]$ is a multiplicative unit in $\mathrm{U}_n$.*

NOTE: The element [0] can never generate $(\mathbb{Z}_n, +)$ if $n > 1$. (What if $n = 1$?) 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: For $(\Rightarrow)$ suppose $\mathbb{Z}_n = \langle [k] \rangle = \{m \cdot [k] : m \in \mathbb{Z}\}$ Since $[1] \in \mathbb{Z}_n$ there must exist some $m$ such that $m \cdot [k] = [k] + \ldots + [k]$ ($m$ times) $= [mk]$ is equal to [1], which means that $mk \equiv 1 \pmod{n}$. Hence there is some $\ell \in \mathbb{Z}$ such that $mk = 1 + \ell n$, or $1 = mk - \ell n$. But in 2.2.12 we saw that the greatest common divisor $c = \gcd(k, n)$ is the smallest positive element in the lattice $\Lambda = \mathbb{Z}k + \mathbb{Z}n$. The preceeding remarks show that $1 \in \Lambda$, and you can't get smaller than that; therefore $\gcd(k, n)$ must equal 1 and $k$ is relatively prime to the base $n$.

For $(\Leftarrow)$ suppose $\gcd(k, n) = 1$. Since $\gcd \in \Lambda$ there must exist integers $r, s$ such that $1 = \gcd(k, n) = rk + sn$. Modul $n$ that means $rk \equiv 1 \pmod{n}$, or equivalently $r \cdot [k] = [rk] = [r][k] = [1]$ in $\mathbb{Z}_n$. Hence $[k]$ is a multiplicative unit (and $[r]$ is its multiplicative inverse, which is also in $\mathrm{U}_n$). $\square$

The last paragraph of the proof 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 $\Lambda = \mathbb{Z}k + \mathbb{Z}n = \{rk + sn : r, s \in \mathbb{Z}\}$.

of 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. Variants of this algorithm allow us to quickly find coefficients $r, s \in \mathbb{Z}$ such that $ra + sb = \gcd(a, b)$.

**3.1.42 Theorem**. The preceeding remarks show that [10] is a unit in $\mathbb{Z}_{63}$. Given a representation of the greatest common divisor $1 = \gcd(10, 63)$ in the form $r \cdot 10 + s \cdot 63$ explain how you could quickly determine $[10]^{-1}$. Then find an explicit representation for the *gcd* and for $[10]^{-1}$. $\square$

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.

**3.1.43 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.*

(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* $G$*.*

An element $x \in G$ is in the center $Z(G)$ if and only if it commutes with everybody in $G$, which is the same as saying $xgx^{-1} = g$ for all $g$. Obviously $G$ is abelian $\Leftrightarrow Z(G) = G$.

**3.1.44 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 $G$ $\square$

**3.1.45 Exercise.** Prove that

(a) The centralizer $Z_G(S)$ of a nonempty set $S$ actually is a subgroup.

(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) $Z_G(S) \subseteq N_G(S)$ $\square$

*Hint:* Recall our "bottom up" description 3.1.20 of the group generated by a set $S \subseteq G$. $\square$

**3.1.46 Exercise.** Let $S$ be a nonempty subset in a group $G$. Prove that $x$ is in the center of $G \Leftrightarrow x$ commutes with each generator – i.e. $xs = sx$ for all $s \in S$.
*Hint:* Recall the first step of 3.1.44.
*Note:* This greatly simplifies the task of deciding whether a group element lies in the center, since it is easier to decide if an element $g$ commutes with a small set of generators than to decide whether it commutes with all elements in $G$. $\square$

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.

**3.1.47 Theorem.** *Let* $H$ *be a nonempty finite subset of a group* $G$*, such that* $H \cdot H = \{h_1 h_2 : h_1, h_2 \in H\}$ *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. $\square$

## 3.2. Isomorphisms and Homomorphisms of Groups.

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

$$\phi(x \cdot y) = \phi(x) * \phi(y) \qquad \text{for all } x, y \in G \tag{10}$$

The map is an **isomorphism** if it satisfies (10) 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 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

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** $\mathrm{range}(\phi)$ is the forward image of the initial group $G$ (11)

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

The range is always a subgroup of the final group $G'$.

Some basic properties of homomorphisms can now be read out of equation (10).

(12) 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; to see this simply multiply both sides by $x^{-1}$. But $\phi(e)^2 = \phi(e) * \phi(e) = \phi(e \cdot e) = \phi(e)$ satisfies this equation in $G'$, so $\phi(e) = e'$.

(13) If $\phi : G \to G'$ is a homomorphism and $x \in G$ then $\phi(x^{-1})$ is equal to the inverse $(\phi(x))^{-1}$ in $G'$.

This follows from (12). Since $x \cdot x^{-1} = e$ in $G$, we get $\phi(x) * \phi(x^{-1}) = \phi(e) = e'$ in $G'$; then our claim follows by definition of group inverse in $G'$.

**3.2.1 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. Here are some more subtle examples.

(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* $G$ 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 $x^{-1}y^{-1}$.

(b) $G = G' = (\mathbb{Z}_n, +)$ with

$$\phi([j]) = -[j] = [-1] \cdot [j] = [n - j]$$

This is the inversion map on the group $\mathbb{Z}_n$. It is clearly a bijection, and hence is a nontrivial isomorphism from $(\mathbb{Z}_n, +)$ to itself.

(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 because $[j + k] = [j] + [k]$ according to our definition of the $(+)$ operation in $\mathbb{Z}_n$, cf equation (15) of Section 2. This map is surjective from $\mathbb{Z}$ to $\mathbb{Z}_n$ but its kernel is nontrivial, with $\ker(\phi) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, so $\phi$ is not one-to-one and is not an isomorphism.
*Note:* The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is the same as the quotient map for the relation $x \sim_R y \Leftrightarrow x \equiv y \pmod{n}$ on $\mathbb{Z}$.

(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* $\phi(x) = e^x$ 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) Let $G$ be any *abelian* group and $k \in \mathbb{Z}$ any integer. The map $\phi_k : G \to G$ given by $\phi_k(x) = x^k$ is always a homomorphism. Beware: This trick does not work for nonabelian groups! (Why?) $\square$

**Notation:** The last example (e) will be particularly important in our work with the additive group $(\mathbb{Z}_n, +)$. In this situation the definition of $\phi_k$ should be rewritten in additive notation

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

for all $[\ell] \in \mathbb{Z}_n$ and $k \in \mathbb{Z}$. Since the right-hand expression involves only the $(\mathrm{mod}\ n)$ congruence class of the "exponent" $k$, we see immediately that $\phi_{k'} = \phi_k$ as maps on $\mathbb{Z}_n$ if $k' \equiv k \pmod{n}$. In fact $\phi_{k'} = \phi_k$ *if and only if* $k'$ is congruent to $k$. To prove $(\Rightarrow)$, apply both maps to the element $[1]$; since the maps agree at every element in $\mathbb{Z}_n$, we get

$$[k'] = k' \cdot [1] = \phi_{k'}([1]) = \phi_k([1]) = k \cdot [1] = [k]$$

as required. It follows that there are only finitely many distinct maps among the $\phi_k$, namely

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

**3.2.2 Exercise.** In $(\mathbb{Z}_n, +)$ let $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ be the homomorphism $\phi([\ell]) = 3 \cdot [\ell] = [3\ell]$. (In multiplicative notation this is the map $\phi_3(a) = a^3$, as in 3.2.1(e) above.) Compute $\ker \phi$ and $\mathrm{range}(\phi)$ in the particular cases: (i) $n = 5$ and (ii) $n = 6$. $\square$

**3.2.3 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 $Hx,\ x \in G$.*

For simplicity we will focus on left cosets $xH$, but everything we say applies equally well to right cosets. To see that $G$ is a disjoint union of its left cosets, first note that the cosets fill $G$ because

$$x \in G \Rightarrow x \in xH \subseteq \bigcup_{g \in G} gH$$

To see that distinct cosets are disjoint, consider what happens if they are not. If $xH \cap yH \neq \emptyset$ then there exist $h_1, h_2 \in H$ such that $xh_1 = yh_2$. Multiplying on the right by $h_1^{-1}$, we see that $y = xh'$ where $h' = h_2 h_1^{-1} \in H$, which in turn implies that

$$yH = (xh')H = x(h'H) = xH \qquad (h'H = H \text{ because } H \text{ is a subgroup})$$

Thus cosets are *identical* if they overlap at all, and the distinct cosets partition $G$ as claimed in 3.2.3.

**3.2.4 Exercise.** If $G$ is a group, $H$ a subgroup, and $h_0 \in H$, prove that the following sets are all equal to $H$.

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

(b) $h_0 H = \{h_0 y : y \in H\}$

(c) $Hh_0 = \{xh_0 : x \in H\}$ □

Now consider cosets of the kernel

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

for some group homomorphism $\phi : G \to G'$. This kernel and its cosets $xK$ determine the overall behavior of the mapping $\phi$, very much as the behavior of a linear operator $T : V \to V'$ between vector spaces is determined by the nature of its kernel $\ker(T) = \{\mathbf{v} \in V : T\mathbf{v} = \mathbf{0}\}$.

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

(a) *Under $\phi$ all points in a coset $xK$ map to the single point $\phi(x)$ in $G'$.*

(b) *Distinct cosets $xK \neq yK$ in $G$ map to* DISTINCT *points in $G'$.*

*as shown in Figure 3.2. In particular $\phi$ is one-to-one (and hence an* ISOMORPHISM *from $G$ to the subgroup* $\text{range}(\phi)$ *in $G'$) if and only if the kernel is trivial:* $\ker(\phi) = (e)$.

PROOF: To prove (a) consider points $x \in G$, $k \in K$. Since $\phi(k) = e'$ by definition of $K$, we get $\phi(xk) = \phi(x)\phi(k) = \phi(x)$. Thus all points in the coset $xK$ map to the same point $\phi(x)$ in $G'$.

For (b), recall that $\phi$ maps $x^{-1}$ (inverse in $G$) to $\phi(x)^{-1}$ (inverse in $G'$), as shown in (13). Thus if $x, y \in G$ we have

$$\begin{aligned}
\phi(x) = \phi(y) \quad &\Leftrightarrow \quad e' = \phi(y)^{-1}\phi(x) = \phi(y^{-1}x) \\
&\Leftrightarrow \quad y^{-1}x \in K = \ker(\phi) \\
&\Leftrightarrow \quad x \in yK = \ker(\phi) \\
&\Leftrightarrow \quad \text{there exists some } k \in K \text{ such that } x = yk \\
&\Rightarrow \quad xK = ykK = y(kK) = yK \qquad \text{(by 3.2.4)}
\end{aligned}$$

so the cosets are identical, as required in (b).

Finally, suppose $\phi$ is one-to-one. Then $\ker(\phi) = (e)$ because all points in $K$ map to the same point $e'$ in $G'$. Conversely, if $K = (e)$ the cosets $xK$ reduce to single points in $G$, and then (b) says $\phi$ is one-to-one. □

We will have a lot more to say about homomorphisms of groups later on, 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 $\phi : G \to G'$ that intertwines the group operations, so we have $\phi(x \cdot y) = \phi(x) * \phi(y)$. 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 symbol we use to indicate the group operation. *To an algebraist they are the same group in different*

**Figure 3.2.** Mapping properties of a homomorphism $\phi : G \to G'$ are largely determined by its kernel $K = \ker(\phi) = \{x \in G : \phi(x) = e'\}$. Cosets $xK$ collapse to single points in range$(\phi) \subseteq G'$, and distinct cosets $xK \neq yK$ map to different points in the range.

*disguises.* In contrast, existence of a *homomorphism* $\phi : G \to G'$ 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 $(\mathbb{Z}, +)$.

**3.2.6 Example.** Let $(S^1, \cdot)$ be the circle group, the complex numbers of absolute value 1 equipped with complex multiplication as the group operation. The exponential map

$$\phi : \mathbb{R} \to S^1 \quad \text{given by} \quad \phi(\theta) = e^{2\pi i\theta}$$

is a group homomorphism since $\phi(0) = 1 + i0$ and

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

by the Exponent Laws. Obviously range$(\phi)$ is all of $S^1$. A real number $\theta$ is in the kernel $K = \ker(\phi)$ if and only if

$$1 = \phi(\theta) = e^{2\pi i\theta} \;\Leftrightarrow\; 2\pi i\theta \text{ is a whole multiple of } 2\pi \text{ radians} \Leftrightarrow \theta \in \mathbb{Z}$$

so that $\ker(\phi) = \mathbb{Z}$ in $\mathbb{R}$. By 3.2.5 it follows that $\theta_1$ and $\theta_2$ have the same image under $\phi \Leftrightarrow \theta_2$ and $\theta_1$ differ by an integer. $\square$

**3.2.7 Example.** Similarly, there is a natural surjective homomorphism 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, $R_{\theta_1+\theta_2} = R_{\theta_1} \circ R_{\theta_2}$ so $G$ is a group under composition $(\circ)$ of operators, and $\rho(\theta) = R_\theta$ is a surjective homomorphism $\rho : \mathbb{R} \to G$. Obviously $R_{\theta+2\pi k} = R_\theta$ for any integer $k$. Thus

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

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 3.2.6 - 7 will be explained when we take up the "First Isomorphism Theorem" later in this section. □

**3.2.8 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

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

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

$$\begin{aligned} k \in \ker(\psi_n) \quad &\Leftrightarrow \quad 1 = \omega^k = e^{2\pi ik/n} \;\Leftrightarrow\; 2\pi\frac{k}{n} \text{ is a multiple of } 2\pi \\ &\Leftrightarrow \quad \frac{k}{n} \in \mathbb{Z} \;\Leftrightarrow\; k \text{ is divisible by } n \;\Leftrightarrow\; k \equiv 0 \pmod{n} \end{aligned}$$

Thus $\ker(\psi_n) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, and by 3.2.5 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 the (mod $n$) congruence classes in $\mathbb{Z}$ collapse to single points in $\Omega_n$ under our homomorphism $\psi_n$ and different classes go to different roots of unity. □

Later we will show that $(\Omega_n, \cdot\,) \cong (\mathbb{Z}_n, +)$ as a consequence of the last result.

**3.2.9 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.) □

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

**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 $G'$**

**Figure 3.3.** Multiplication tables for two groups of order 4.

**3.2.10 Exercise.** Prove that the permutation group on two elements $S_2$ is isomorphic to $(\mathbb{Z}_2, +)$. Prove that *any* group with $|G| = 2$ is isomorphic to $(\mathbb{Z}_2, +)$. □

**3.2.11 Exercise.** Prove that any group such that $|G| = 3$ is isomorphic to $(\mathbb{Z}_3, +)$.
*Hint:* Look at an element with the largest possible order $o(a)$. Produce a contradiction if this order is equal to 1 or 2. □

**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. □

**3.2.13 Exercise.** If $G$ is any group and $a \in G$ any element of infinite order, prove that $H = \langle a \rangle$ is isomorphic to $(\mathbb{Z}, +)$. □

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

**3.2.15 Exercise.** If $G$ is a finite *cyclic* group, say with $G = \langle x \rangle$ and $|G| = o(x) = n$, prove

that $G$ 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 completely 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.
*Note:* There is a similar result for vector spaces. Any linear operator $T : V \to V'$ is completely determined by what it does to a set of basis vectors in the initial space $V$. $\square$

**3.2.18 Exercise.** For each integer $k \in \mathbb{Z}$ let $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ 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 $0 \le k < n$ such that $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ is a *bijection.*
*Hint:* Since $\mathbb{Z}_n$ is finite, a homomorphism $\phi_k$ will be a bijection $\Leftrightarrow \ker(\phi_k)$ is trivial.
*Note:* 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* of $G$ and will be of considerable interest as we go along. $\square$.

## 3.3 Coset spaces and quotient groups.

Let $H$ be a subgroup in $G$. 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 $G/H$.

In the following discussion we are going to regard $G/H$ as a "quotient space" of the group $G$, so you might want to review Section 2.4, especially the definition of "equivalence relations." We start by determining when two group elements $x, y$ give 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 $x \sim_R y \Leftrightarrow xH = yH$ is reflexive, symmetric and transitive, and the equivalence classes for this relation are precisely the cosets in $G/H$: for any $x$ we have $\{g \in G : g \sim_R x\} = xH$.*

Proof: The first statement is a simple calculation: since $y = ye \in yH$ we have $xH = yH \Rightarrow$ there exists an $h \in H$ such that $xh = y$, and conversely if such an $h$ exists we get $yH = xhH = xH$ because $hH = H$ (recall 3.2.4).

If two cosets $xH, yH$ intersect nontrivially there is some $z \in xH \cap yH$. Then we can find $h', h'' \in H$ such that $z = xh' = yh''$, which $\Rightarrow y = xh'(h'')^{-1}$. Thus $y = xh$ for some $h \in H$, and as in (a) we get $xH = yH$. That proves (b).

We leave the reader to check that $\sim_R$ is in fact an RST relation. The equivalence class $[x] = \{xh : h \in H\}$ is precisely the coset $xH$. $\square$

Now consider the **space of cosets** $G/H$, which is just the quotient space of equivalence classes under the RST relation $\sim_R$ Note carefully:

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

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

$$\pi(x) = xH \qquad \text{(since } xH \text{ is the equivalence class for } x) \tag{14}$$

This map has the following general properties:

- 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 $G/H$.

Here are some important examples of coset spaces.

**3.3.2 Example.** If $G = (\mathbb{Z}, +)$ and $n \geq 2$ then 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; since the group operation is being written as $(+)$, the cosets are of the form

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

Obviously, 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 $\pi : \mathbb{Z} \to \mathbb{Z}_n$ assigns to each $k \in \mathbb{Z}$ its (mod $n$) congruence class $[k] = k + n\mathbb{Z}$. $\square$

Incidentally, in this particular example the quotient space $G/H$ has 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 put a natural group structure on the quotient space $G/H$; it worked in the last example largely because the group was abelian.

**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

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

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 $0 \leq x < 1$, so the cosets in $\mathbb{R}/\mathbb{Z}$ are labeled by the points in the interval $[0, 1)$.

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 addition in $\mathbb{Z}_n$. We define

$$(x + \mathbb{Z}) + (y + \mathbb{Z}) = (x + y) + \mathbb{Z} \qquad \text{for } x, y \in \mathbb{R}, \tag{15}$$

and leave the reader to carry out the routine verification that

(i) The operation $(+)$ is independent of the particular coset representatives $x$ and $y$ that appear in the definition (15).

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

(iii) The identity element is the class $[0] = 0 + \mathbb{Z}$, the additive inverse is given by $-(x + \mathbb{Z}) = (-x) + \mathbb{Z}$, so that in terms of equivalence classes we have $-[x] = [-x]$.

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

But what *is* the mysterious group $\mathbb{R}/\mathbb{Z}$? We now show it is isomorphic to something quite concrete and familiar, 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 become very important before long.

In Example 3.2.6 we showed 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 3.2.6, is nontrivial. (Recall 3.2.5.) We now show how $\phi$ can be used to create a *bijection* $\tilde{\phi}$ between the quotient space $\mathbb{R}/\mathbb{Z}$ and $S^1$; this turns out to be a group isomorphism. The idea is to define $\tilde{\phi}$ using coset representatives, letting

$$\tilde{\phi}(x + \mathbb{Z}) = \phi(x) = e^{2\pi ix} \qquad \text{for all } x \in \mathbb{R} \tag{16}$$

The first thing to do is check that $\tilde{\phi}$ makes sense independent of the coset representative, but that is clear since $x' + \mathbb{Z} = x + \mathbb{Z} \Rightarrow x' = x + k$ for some integer $k$, which means that $\phi(x') = \phi(x)$, as desired. Notice that our definition of $\tilde{\phi}$ makes the diagram in Figure 3.4 "commute," in the sense that $\tilde{\phi} \circ \pi = \phi$.

$$\begin{array}{ccc} R & \xrightarrow{\ \phi\ } & S^1 \\ \pi\downarrow & \nearrow & \\ \mathbb{R}/\mathbb{Z} & \tilde{\phi} & \end{array}$$

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

Next, $\tilde{\phi}$ is injective because, as noted earlier, we have

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

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

$$\tilde{\phi}((x + \mathbb{Z}) + (y + \mathbb{Z})) = \tilde{\phi}((x + y) + \mathbb{Z}) = \phi(x + y) = \phi(x) \cdot \phi(y) = \tilde{\phi}(x + \mathbb{Z}) \cdot \tilde{\phi}(y + \mathbb{Z}) \quad .$$

We conclude that $\mathbb{R}/\mathbb{Z} \cong (S^1, \cdot\,)$. $\square$

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 $G/H \times G/H \to G/H$ in the following way.

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

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

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

That means the outcome cannot be consistently determined from the cosets we start with, independent of representatives, and hence the "operation" $\otimes$ is not well-defined. It turns out that a simple condition on $H$ tells us when this construction works.

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

$$xN = Nx \qquad \text{for all } x \in G\ , \tag{17}$$

which means there is no difference between left- and right-cosets for this subgroup. Notice that *all* subgroups are normal if $G$ is abelian.
*Notation:* Normality of a subgroup is indicated by writing $N \lhd G$. $\square$

It is easily seen that each of the following properties of a subgroup $N$ is equivalent to normality, which gives us considerable flexibility in deciding when 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

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

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). Thus we 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). $\square$

**3.3.6 Lemma.** 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 $G$. $\square$

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

$$(xN) \cdot (yN) = xyN \quad \text{for } x, y \in G\ . \tag{18}$$

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 3.2.4). 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* (18) *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 $\pi : G \to G/N$ becomes a surjective homomorphism of groups.*

PROOF: To see the product is well defined, suppose 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 $x'y'N = xyn''N = xyN$; the product operation (18) is independent of coset representatives.

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

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

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. Then $\pi$ is a homomorphism of groups because $\pi(xy) = xyN = (xN)\cdot(yN) = \pi(x)\cdot\pi(y)$. That completes the proof. □

**3.3.8 Exercise.** If $G$ is an abelian group and $N$ is any normal subgroup, prove that the quotient group $G/N$ is abelian. □

We have already seen some examples of quotient groups, namely $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ and $\mathbb{R}/\mathbb{Z}$. The latter example can be generalized considerably by taking $G = (\mathbb{R}^n, +)$ and $N$ to be 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 Exercise.** In Example 3.2.8 we defined a surjective homomorphism $\psi : \mathbb{Z} \to \Omega_n$

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

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 (18) in $\mathbb{Z}/H$ takes the form $(x+H)+(y+H) = (x+y)+H$. The quotient homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/(n\mathbb{Z})$ obviously has the same kernel $\ker(\pi) = H = n\mathbb{Z}$ as $\psi$. Following the ideas laid out in Example 3.3.3, construct an explicit isomorphism $\tilde{\psi} : \mathbb{Z}/H \to \Omega_n$. 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 point in the quotient group.

What is the nature of the 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" $\phi : \mathbb{C}^\times \to \mathbb{C}^\times$ given by $\phi(z) = z^2$. This map is a homomorphism, as we saw in 3.2.1(e); 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 $\phi(zN)$: the coset collapses to a single point $z^2$.

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

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

This makes sense independent of the choice of coset representative $z$, because the only other representative is $-z$, and $(-z)^2 = z^2$; furthermore $\Phi$ is surjective, by our remark regarding square roots. And, $\Phi$ 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 for nonabelian $G$.

**Isomorphism theorems for quotient groups.** The isomorphisms in the last examples were all constructed "by hand." We now develop some 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 $\phi : G \to G'$ 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 $\phi : G \to G'$.*

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 $\pi : G \to G/N$ is a homomorphism whose kernel is $N$. $\square$

The mapping properties of any homomorphism are determined by the nature of its kernel, as mentioned in our initial discussion of homomorphisms. The basic properties are:

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

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

(b) Distinct cosets $xK \neq x'K$ 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). It is also important to note that any homomorphism $\phi : G \to G'$ is completely determined by its behavior on a set of generators of $G$, as explained in 3.2.17.

We now come to what is called the *First Isomorphism Theorem* for quotient groups (there are two more). Suppose $\phi : G \to G'$ is 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 $\pi : G \to G/K$ (see Figure 3.6 at right). By definition of $\pi$ we have $\ker\phi = \ker\pi = K$. We claim that there is a natural *isomorphism* $\tilde{\phi}$ from $G/K$ to $R = \text{range}(\phi)$ that makes this diagram commutative, in the sense that $\tilde{\phi} \circ \pi = \phi$. This is often expressed by saying that the original homomorphism $\phi$ "factors through" the quotient homomorphism $\pi$ to give an "induced map" $\tilde{\phi}$.

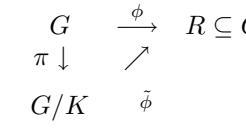


**Figure 3.5.** Here we have $R = \text{range}(\phi)$, $K = \ker(\phi)$.

**3.3.12 Theorem (First Isomorphism Theorem).** *Let $\phi : G \to G'$ be a homomorphism, let $K = \ker(\phi)$, and let $\pi : G \to G/K$ be the quotient homomorphism. Then there is a unique map $\tilde{\phi} : G/K \to R = \text{range}(\phi)$ that makes the diagram in Figure 3.5 commute: $\tilde{\phi} \circ \pi = \phi$. This map is a group homomorphism and is bijective, so that $R = \text{range}(\phi)$ is isomorphic to the quotient group $G/K$. 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 as

$$\tilde{\phi}(xK) = \phi(x) \qquad \text{for all } x \in G\ . \tag{20}$$

This map is well defined because $xK = yK \Rightarrow \exists\, k \in K$ such that $y = xk \Rightarrow \phi(y) = \phi(xk) = \phi(x)\phi(k) = \phi(x)e' = \phi(x)$; since $\phi(y) = \phi(x)$, the outcome in (21) is independent of the coset representative.

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

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

Commutativity of the diagram is automatic from our definition (21).

Now, $\tilde{\phi}$ is one-to-one because, by definition of $K = \ker\phi$,

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

Furthermore, $\tilde{\phi}$ maps $G/K$ *onto* the range $R$, which makes it an isomorphism between these groups as claimed. In fact, if $r \in R$ then $r = \phi(x)$ for some $x \in G$, and then $\pi(x) = xK$ gives $\tilde{\phi}(xK) = \phi(x) = r$, so $\tilde{\phi}$ is 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 $K$ : $\ker(\phi) = K$.*

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 $N = \{\pm 1\}$. For any integer $k = 1, 2, 3, \ldots$ the "$k^{\text{th}}$ power map" $\phi_k : x \mapsto x^k$ is a homomorphism $\phi_k : \mathbb{C}^\times \to \mathbb{C}^\times$ because $(\mathbb{C}^\times, \cdot\,)$ is abelian; $\phi_k$ even maps $\mathbb{C}^\times$ *onto* $\mathbb{C}^\times$ because every nonzero complex number $w$ has at least one $k^{\text{th}}$ root $z = w^{1/k}$, for which $\phi_k(z) = z^k = w$. Now ask yourself: do any of these homomorphisms have $\ker(\phi_k) = \{\pm 1\}$? If so, we can immediately conclude that $G/N \cong \mathbb{C}^\times$. The answer to our question is obviously affirmative: just take $k = 2$, which gives the "squaring map" employed in 3.3.10.

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

There is a natural homomorphism $\phi : \mathrm{GL}(n,\mathbb{C}) \to \mathbb{C}^\times$, namely the determinant map $\phi(A) = \det A$. This is obviously a group homomorphism since 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 $\lambda^{1/n} = r^{1/n}e^{i\theta/n}$ 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

(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:* Consider the map $\psi(a(A\cap N)) = aN$ for $a \in A$. Start be 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-theoretic 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 $n = 1, 2, \ldots$. □

**3.3.17 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 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. Prove that the quotient group $(\mathbb{Z}_n/H_d, +)$ is isomorphic to $(\mathbb{Z}_{n/d}, +)$.
*Hint:* By 3.3.17, the quotient is cyclic. What do you know about its cardinality?
*Note:* Since $H_d \cong \mathbb{Z}_d$, this result might be paraphrased as saying that $(\mathbb{Z}_n)/(\mathbb{Z}_d) \cong \mathbb{Z}_{n/d}$. □

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

$$\begin{aligned}\mathbb{C}^\times I &= \{\lambda I : \lambda \neq 0 \text{ in } \mathbb{C}\}\\ \Omega_n I &= \{\lambda I : \lambda \in \Omega_n\}\end{aligned}$$

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. Note that if $N = \mathbb{C}^\times I$ then $N \cdot \mathrm{SL}(n,\mathbb{C}) = \mathrm{GL}(n,\mathbb{C})$. □

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, hence 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.

## 3.4 Basic counting principles in group theory.

We now turn our attention to some basic counting principles in group theory. The following principle is fundamental. It 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*

$$|G| = |G/H| \cdot |H| \tag{21}$$

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

Proof: Any left translation $\tau_x : G \to G$, with $\tau_x(g) = xg$, is easily seen to be a bijection; for one thing, the operator $\tau_{x^{-1}}$ is its inverse. That means all $H$-cosets have the same cardinality because $|xH| = |\tau_x(H)| = |H|$. Since the $H$-cosets form a disjoint partition of $G$ 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* $p = 7$; consequently, *$G$ cannot contain any proper subgroups* – 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 abelian.*

**3.4.5 Corollary.** 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 actually occur in this group?

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

**3.4.7 Exercise.** If $(\mathbb{Z}_n, +, \cdot)$ 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 $(\mathrm{U}_{12}, \cdot)$?

Is there anything more to say about the stucture of $\mathrm{U}_{12}$ ? □

Earlier we showed that the additive group $(\mathbb{Z}_n, +)$, up to isomorphism 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 $d|n,\ 1 \leq d \leq n$ 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 are two subgroups $A, B$ of order $d$. 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 $G$, 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 $|AB|$.

**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*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|} \tag{22}$$

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 part ($\Rightarrow$) in (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 $ab \in AB$ then 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

$$a_2 = a_1x^{-1} \quad \text{and} \quad b_2 = xb_1 \qquad \text{for some element } x \in A \cap B\ . \tag{23}$$

This is a *necessary* condition in order that $a_1b_1 = a_2b_2$. It is also sufficient, because if (25) holds we then have

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

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.

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

$$\begin{aligned} |A \times B| &= \#(\text{equivalence classes}) \cdot \#(\text{points per class}) \\ &= \#(\text{image points in } AB) \cdot |A \cap B| \\ &= |AB| \cdot |A \cap B| \end{aligned}$$

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 become 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** of $G$ – which are obtained by letting $G$ act on itself by **conjugation**. Just as in linear algebra, we say that one element $y$ is conjugate to 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) $\alpha_e = \mathrm{id}_G$, the identity map on $G$.

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

(c) $\alpha_{x^{-1}} = (\alpha_x)^{-1}$ (set-theoretic inverse map)

It follows that $(\mathrm{Int}(G), \circ)$ is a group under composition of operators, and hence a subgroup of $\mathrm{Aut}(G)$.

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

We call $\mathrm{Int}(G)$ the group of **inner automorphisms** of $G$. Notice that $\mathrm{Int}(G)$ 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. Finding them 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 that 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. We have determined all possible homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$; they are just the "$k^{\text{th}}$ power maps $\phi_k(m) = k \cdot m$ for $k \in \mathbb{Z}$. Any automorphisms of $\mathbb{Z}$ must appear within this 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 automorphisms. If $k = 0$, $\phi_0$ is the zero map and is not one-to-one; we leave the reader to verify that $\phi_k$ fails to be surjective if $k \neq -1, 1$. Thus we have computed $\mathrm{Aut}(\mathbb{Z}, +) = \{\mathrm{id}_G, -\mathrm{id}_G\}$. Since there are only two elements, this group is abelian and is isomorphic to $(\mathbb{Z}_2, +)$. Obviously $\mathrm{Int}(\mathbb{Z}) = \{\mathrm{id}_G\}$. $\square$

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

$$\mathrm{Aut}(\mathbb{Z}_n, +) \cong (\mathrm{U}_n, \cdot) \tag{24}$$

*where* $\mathrm{U}_n = \{[k] \in \mathbb{Z}_n : 1 \le k \le n-1$ *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.*

PROOF: The group $G = \mathbb{Z}_n$ is cyclic, with [1] as a generator under the (+) operation. Following the lines of Example 3.5.2, we note that a *homomorphism* $\phi : G \to G$ is determined by what it does to this generator, and we can try all the possible assignments $\phi_k([1]) = [k], 0 \le k \le n-1$. If we assign $[1] \to [k]$ then $[2] \to [2k]$, etc and we find that $\phi_k([m]) = [km] = [k][m]$ for all $[m] \in \mathbb{Z}_n$. These maps are just the homomorphisms $\phi_0, \ldots, \phi_{n-1}$ discussed in 3.2.1(e); they are the *only* homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. As mentioned earlier, $\phi_k$ depends only on the (mod $n$) conjugacy class $[k]$ of $k$; furthermore, $\phi_k = \phi_m \Leftrightarrow k \equiv m \pmod n$ because $\phi_k([1]) = [k]$ and [1] generates $(\mathbb{Z}_n, +)$. (Recall 3.2.17.)

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, then there is some $[\ell]$ such that $[k][\ell] = [1]$, which means $[k] \in \mathrm{U}_n$ 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 $\Phi : \mathrm{U}_n \to \mathrm{Aut}(\mathbb{Z}_n, +)$ that maps $[k]$ to $\Phi([k]) = \phi_k$. The map $\Phi$ is a bijection. It is also a homomorphism, essentially as a consequence of the exponent laws for groups, which in an additive abelian group take the form:

$$\text{(i)}\ \ (\ell + m) \cdot a = \ell \cdot a + m \cdot a \text{ and (ii)}\ \ (\ell m) \cdot a = \ell \cdot (m \cdot a) \qquad \text{for all } \ell, m \in \mathbb{Z} \text{ and } a \in \mathbb{Z}_n$$

The second of these laws law says that

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

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

Since every cyclic group of finite order $|G| = n$ is isomorphic to $(\mathbb{Z}_n, +)$ we have determined the automorphisms of all cyclic groups. Writing the group law as multiplication rather than (+), the homomorphisms of $G$ take the form $\phi_k(a) = a^k$ for $0 \le k \le n-1$; 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 $G$:

$$Z(G) = \{a \in G : ga = ag, \forall\, g \in G\} = \{a \in G : gag^{-1} = a, \forall\, g \in G\} \quad \square \tag{25}$$

The center is a subgroup. It is also normal. In fact, if $a \in Z(G)$ and $b \in G$, then

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

and hence $bab^{-1}$ is again 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 $\Phi : G \to \mathrm{Int}(G) \subseteq \mathrm{Aut}(G)$ 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 the subgroup $\mathrm{Int}(G)$, 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 3.6. The induced diagonal map $\tilde{\Phi}$ is a bijective map to $\mathrm{range}(\Phi) = \mathrm{Int}(G)$, and is a homomorphism; hence we have an isomorphism of groups $\mathrm{Int}(G) \cong G/Z(G)$.

We summarize this as follows:

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \mathrm{Int}(G) \subseteq \mathrm{Aut}(G) \\ \pi \downarrow & \nearrow & \\ G/Z(G) & \tilde{\Phi} & \end{array}$$

**Figure 3.6.**

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

**3.5.6 Exercise.** Verify the properties (i) $\alpha_e = \mathrm{id}_{_G}$, (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 $N$. Since $N$ is invariant under inner automorphisms, we get an automorphism $\alpha_x|N \in \mathrm{Aut}(N)$ by taking $(\alpha_x|N)(n) = \alpha_x(n) = xnx^{-1}$ for all $n \in N$. Now consider the *restriction map* $R : (\mathrm{Int}(G), \circ) \to (\mathrm{Aut}(N), \circ)$ which takes an inner automorphism $\alpha_x$ of to its restriction $R(\alpha_x) = \alpha_x|N$. Prove that the restriction map is a homomorphism $R : \mathrm{Int}(G) \to \mathrm{Aut}(N)$.
*Note:* Arbitrary automorphisms $\beta \in \mathrm{Aut}(G)$ *need not* leave a normal subgroup invariant, so we cannot expect the restriction $\beta|N$ to be a well defined 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 $\mathrm{Int}(G)$ of inner automorphisms is a *normal* subgroup in $\mathrm{Aut}(G)$. □