1. Groups of Transformations

Maps and groups • *Permutations of a finite set* • *Morphisms of groups* • *Cosets and quotient groups.*

1.1. **Maps and groups.** Let M be a non-empty set. A **transformation** of M is a function (map or mapping) from M to M. The *identity mapping* on M is denoted by id_{M}. Let M^{M} denote the set of all transformations of M. (An element $\alpha \in \mathsf{M}^{\mathsf{M}}$ is written symbolically as $\alpha : \mathsf{M} \to \mathsf{M}$ or $\mathsf{M} \xrightarrow{\alpha} \mathsf{M}$.) M^{M} is a *monoid* with identity element $\mathbf{1}_{\mathsf{M}} = \mathrm{id}_{\mathsf{M}}$.

NOTE: A **semigroup** $(\mathsf{M}, *)$ consists of a (non-empty) set M on which an *associative* binary operation $*$ is defined; that is, $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$ for all elements $\alpha, \beta, \gamma \in \mathsf{M}$. If there exists an element ϵ satisfying $\alpha * \epsilon = \alpha = \epsilon * \alpha$ for all $\alpha \in \mathsf{M}$, then the semigroup is called a **monoid** having identity element ϵ. This element can easily be seen to be unique, and is usually denoted by $\mathbf{1}_{\mathsf{M}}$. An element α in a monoid $(\mathsf{M}, *)$ is called *invertible* if there exists an element $\beta \in \mathsf{M}$ such that $\alpha * \beta = \mathbf{1}_{\mathsf{M}} = \beta * \alpha$. (Clearly, in that case β is also invertible.)

The natural operation on M^{M} is the usual composition of mappings; the composite mapping $\alpha \circ \beta$ is called the *product* of α and β (in this order) and is denoted simply by $\alpha\beta$. (In general, the product of mappings is *not* commutative.)

A map (transformation) $\alpha : \mathsf{M} \to \mathsf{M}$ is said to be **injective** (or one-to-one) if $x_1 \neq x_2$ implies $\alpha(x_1) \neq \alpha(x_2)$ $(x_1, x_2 \in \mathsf{M})$; it is said to be **surjective** (or onto) if for every $y \in \mathsf{M}$ there exists (at least one) $x \in \mathsf{M}$ such that $\alpha(x) = y$.

◇ **Exercise 1.** Let $\alpha \in \mathsf{M}^{\mathsf{M}}$. Show that the following statements are logically equivalent.

(a) α is injective.
(b) $\alpha(x_1) = \alpha(x_2)$ implies $x_1 = x_2$ $(x_1, x_2 \in \mathsf{M})$.
(c) For every $y \in \mathsf{M}$ there exists *at most* one $x \in \mathsf{M}$ such that $\alpha(x) = y$.

◇ **Exercise 2.** Let $\alpha, \beta \in \mathsf{M}^{\mathsf{M}}$. Show that

(a) if α and β are injective, then so is the product $\alpha\beta$;
(b) if α and β are surjective, then so is the product $\alpha\beta$.

◇ **Exercise 3.** Let $\alpha, \beta \in \mathsf{M}^{\mathsf{M}}$ such that $\beta\alpha = \mathbf{1}_{\mathsf{M}}$. Show that α is injective and β is surjective.

As in any monoid, an element $\alpha \in \mathsf{M}^{\mathsf{M}}$ is said to be **invertible** if there exists an element $\beta \in \mathsf{M}^{\mathsf{M}}$ such that $\alpha\beta = \mathbf{1}_{\mathsf{M}} = \beta\alpha$. If that is the case, β is called an *inverse*

of α. If a mapping is invertible, then its inverse is unique (this is PROBLEM 2), and is denoted by α^{-1}.

PROPOSITION 1. *A transformation of* M *is invertible if and only if it is both injective and surjective (i.e., bijective).*

Proof. ($\Rightarrow$) Suppose that $\alpha \in \mathsf{M}$ has an inverse $\beta = \alpha^{-1}$. Then

$$\beta\alpha = \mathbf{1}_{\mathsf{M}} \quad \text{and} \quad \alpha\beta = \mathbf{1}_{\mathsf{M}}.$$

These two conditions and **Exercise 2** give both injectivity and surjectivity of α.

($\Leftarrow$) Conversely, if we suppose that α is bijective, for any $y \in \mathsf{M}$ we can find a *unique* element $x \in \mathsf{M}$ such that $\alpha(x) = y$. Setting $\beta(y) := x$, we define a map $\beta : \mathsf{M} \to \mathsf{M}$ such that $\alpha\beta = \mathbf{1}_{\mathsf{M}} = \beta\alpha$. Thus $\alpha^{-1} = \beta$. □

COROLLARY 2. *If* $\alpha \in \mathsf{M}^{\mathsf{M}}$ *is invertible, then* α^{-1} *is also invertible and* $(\alpha^{-1})^{-1} = \alpha$.

Proof. The equations

$$\alpha^{-1}\alpha = \mathbf{1}_{\mathsf{M}} \quad \text{and} \quad \alpha\alpha^{-1} = \mathbf{1}_{\mathsf{M}}$$

show that α is the inverse of α^{-1}. □

COROLLARY 3. *If* $\alpha, \beta \in \mathsf{M}^{\mathsf{M}}$ *are invertible, then the product (composition)* $\alpha\beta$ *is also invertible, and* $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

Proof. The equations

$$(\alpha\beta)(\beta^{-1}\alpha^{-1}) = \alpha(\beta\beta^{-1})\alpha^{-1} = \alpha\alpha^{-1} = \mathbf{1}_{\mathsf{M}}$$
$$(\beta^{-1}\alpha^{-1})(\alpha\beta) = \beta^{-1}(\alpha^{-1}\alpha)\beta = \beta^{-1}\beta = \mathbf{1}_{\mathsf{M}}$$

imply that $\beta^{-1}\alpha^{-1}$ is the inverse of $\alpha\beta$. □

Let M be a non-empty set. An invertible transformation of M is called a **permutation** (or **symmetry**) of M. The collection of all permutations of M form a *group*, denoted by $\mathfrak{S}_{\mathsf{M}}$ and called the **symmetric group** on M. So

$$\mathfrak{S}_{\mathsf{M}} := \left\{\alpha \in \mathsf{M}^{\mathsf{M}} \,:\, \alpha \text{ invertible}\right\}. \tag{1}$$

NOTE: A monoid G all of whose elements are invertible is called a **group**. In other words, the following axioms must hold:

(G1) a binary operation $(g_1, g_2) \mapsto g_1 g_2$ is defined on the set G;
(G2) this operation is associative: $(g_1 g_2)g_3 = g_1(g_2 g_3)$ for all $g_1, g_2, g_3 \in \mathsf{G}$;
(G3) G has a neutral (identity) element $\mathbf{1}_{\mathsf{G}} = \mathbf{1}$: $g\mathbf{1} = \mathbf{1}g = g$ for all $g \in \mathsf{G}$;
(G4) every element $g \in \mathsf{G}$ has an inverse g^{-1}: $gg^{-1} = g^{-1}g = \mathbf{1}$.

A group G is said to be **Abelian** if the group operation is *commutative* ($g_1g_2 = g_2g_1$ for all $g_1, g_2 \in \mathsf{G}$); the name "Abelian" is in honour of the Norwegian mathematician N.H. Abel (1802–1829). The term "group" itself was introduced by the French mathematician E. Galois (1811–1832) who considered finite groups of permutations.

A **subgroup** of a group G is a subset of G which itself forms a group under the group operation (multiplication). *A non-empty subset* H *of a group* G *is a subgroup if and only if* $g_1^{-1}g_2 \in \mathsf{H}$ *whenever* $g_1, g_2 \in \mathsf{H}$. If H is a subgroup of G we write $\mathsf{H} \leq \mathsf{G}$; H is said to be a *proper* subgroup if $\mathsf{H} \neq \mathsf{G}$. Any intersection of subgroups is a subgroup of G.

Here are some examples of groups.

(1) *Groups of numbers.* Let $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote respectively the set of all integers, rational numbers, real numbers, and complex numbers. Each set becomes a group if we specify ordinary addition as the group operation. The sets $\mathbb{Q}\setminus\{0\}, \mathbb{R}\setminus\{0\}$, and $\mathbb{C}\setminus\{0\}$ are groups with respect to ordinary multiplication. All these groups are Abelian.

(2) *Groups of matrices.* Let $\Bbbk$ be a *field* (think of $\mathbb{R}$ or $\mathbb{C}$) and let $\mathsf{GL}(n, \Bbbk)$ denote the set of all *nonsingular* $n \times n$ matrices over $\Bbbk$. Taking matrix multiplication as the group operation we see that $\mathsf{GL}(n, \Bbbk)$ is a group. This group is called the **general linear group** (of degree n over $\Bbbk$).

(3) *Groups of linear transformations.* If V is an n-dimensional *vector space* over the field $\Bbbk$, let $\mathsf{GL}(\mathsf{V})$ denote the set of all bijective linear transformations of V. Then $\mathsf{GL}(\mathsf{V})$ is a group if the usual functional composition is specified as the group operation: $\alpha\beta(v) := \alpha(\beta(v))$ for $v \in \mathsf{V}$ and $\alpha, \beta \in \mathsf{GL}(\mathsf{V})$.

There is a close connection between the groups $\mathsf{GL}(\mathsf{V})$ and $\mathsf{GL}(n, \Bbbk)$. For, if a fixed ordered basis for V is chosen, each bijective linear transformation of V is associated with a nonsingular $n \times n$ matrix over $\Bbbk$. This correspondence is an isomorphism from $\mathsf{GL}(\mathsf{V})$ to $\mathsf{GL}(n, \Bbbk)$ (the reason being that when two linear transformations are composed, the product of the corresponding matrices represents the composite).

(4) *Groups of isometries.* Let M be a *metric space* (with a distance function $d : \mathsf{M} \times \mathsf{M} \to \mathbb{R}$). An **isometry** of M is a bijective mapping $\alpha : \mathsf{M} \to \mathsf{M}$ (i.e., a permutation of M) which preserves distances: $d(\alpha(x), \alpha(y)) = d(x, y)$ for all $x, y \in \mathsf{M}$. It is easy to verify that the set of all isometries of M is a group (with respect to the operation of functional composition). We shall write this group $\mathsf{Isom}(\mathsf{M})$.

Suppose that S is a non-empty subset of (the metric space) M. If α is an isometry, define $\alpha \cdot \mathsf{S}$ to be the set $\{\alpha(x) : x \in \mathsf{S}\}$. The **symmetry group** of S (with respect to M) is the set

$$\mathsf{Sym}(\mathsf{S}) := \{\alpha \in \mathsf{Isom}(\mathsf{M}) : \alpha \cdot \mathsf{S} = \mathsf{S}\}$$

of all isometries that leave S fixed as a set (together with functional composition). Again, it is clear that this is a group. The more "symmetrical" the set S is, the larger is its symmetry group. Thus we arrive at the fundamental idea of a group as a measure of the symmetry of a structure.

(5) *Group-valued functions.* Let M be a non-empty set and let G be a group. The set G^{M} of all functions $\alpha : \mathsf{M} \to \mathsf{G}$ is a group with the group operation defined pointwise:

$\alpha\beta(x) := \alpha(x)\beta(x)$ for $x \in \mathsf{M}$ and $\alpha, \beta \in \mathsf{G}^{\mathsf{M}}$. In particular, the set $\mathbb{R}^{\mathsf{M}}$ of all real-valued functions defined on M is a group; clearly, this group is Abelian.

Notice that the set $\Bbbk^{[n]\times[n]}$ of all $\Bbbk$-valued functions defined on the set $\mathsf{M} = [n] \times [n]$ (where $[n] := \{1, 2, \dots, n\}$) is precisely the set of $n \times n$ matrices over (the ring) $\Bbbk$. We shall write this (Abelian) group $\Bbbk^{n\times n}$.

DEFINITION 1. Any subgroup of the symmetric group $\mathfrak{S}_{\mathsf{M}}$ is called a **transformation group** (or **permutation group**).

The *trivial group* $\{\mathbf{1}_{\mathsf{M}}\}$ and the symmetric group $\mathfrak{S}_{\mathsf{M}}$ itself are, of course, transformation groups. A collection $\mathsf{G} \subseteq \mathfrak{S}_{\mathsf{M}}$ of invertible transformations (permutations) of M is a transformation group if and only if $\alpha^{-1}\beta \in \mathsf{G}$ for all $\alpha, \beta \in \mathsf{G}$.

◇ **Exercise 4.**

(a) Let G be a group and $g \in \mathsf{G}$ is such that $\{g, g^2, g^3, \dots\}$ is *finite*. Show that there exists a positive integer k such that $g^k = \mathbf{1}$.

(b) Let G be a group and let S be a (non-empty) finite subset of G. Prove that S is a subgroup of G if and only if $g_1 g_2 \in \mathsf{S}$ for all $g_1, g_2 \in \mathsf{S}$.

EXAMPLE 2. Let $\Bbbk = \mathbb{R}$ or $\mathbb{C}$. In the general linear group $\mathsf{GL}(n, \Bbbk)$, consider the subset $\mathsf{SL}(n, \Bbbk)$ of matrices with determinant 1:

$$\mathsf{SL}(n, \Bbbk) := \{a \in \mathsf{GL}(n, \Bbbk) \,:\, \det a = 1\}.$$

Clearly, the **identity matrix** $\mathbf{1} = \mathrm{Id}_n \in \mathsf{SL}(n, \Bbbk)$. (The $n \times n$ matrix $\mathrm{Id}_n = [\delta_{ij}] \in \mathsf{SL}(n, \Bbbk)$ corresponds to the identity map $\mathrm{id}_{\Bbbk^n} : \Bbbk^n \to \Bbbk^n$.) The expression for the determinant of a product (i.e., $\det(ab) = \det a \cdot \det b$) implies that $\mathsf{SL}(n, \Bbbk)$ is a subgroup of $\mathsf{GL}(n, \Bbbk)$; it is called the **special linear group** (of degree n over $\Bbbk$).

The group $\mathsf{GL}(n, \Bbbk)$, which contains many other interesting groups (called **matrix groups**), has been for mathematicians of several generations a seemingly inexhaustible source of new ideas and unsolved problems.

EXAMPLE 3. Transformations of the real line $\mathbb{R}$ of the form

$$\tau_{a,b} : x \mapsto ax + b \qquad (a, b \in \mathbb{R}, \;\; a \neq 0)$$

are called **affine transformations**. Clearly, the inverse of any such transformation is another of the same form: $\tau_{a,b}^{-1} : x \mapsto \frac{1}{a}x - \frac{b}{a}$. The set $\mathsf{Aff}(1, \mathbb{R})$ of all these transformations is a group, called the **affine group** (of the real line).

◇ **Exercise 5.** Show that the product of two affine transformations $\tau_{a,b}$ and $\tau_{c,d}$ is also an affine transformation.

The group $\mathsf{Aff}(1,\mathbb{R})$ can be viewed as a group of 2×2 matrices over $\mathbb{R}$: the transformation $\tau_{a,b}$ corresponds to the matrix $\begin{bmatrix}1 & 0\\ b & a\end{bmatrix} \in \mathsf{GL}(2,\mathbb{R})$ because

$$\begin{bmatrix}1 & 0\\ b & a\end{bmatrix}\begin{bmatrix}1\\ x\end{bmatrix} = \begin{bmatrix}1\\ ax+b\end{bmatrix}.$$

◇ **Exercise 6.** Use the fact that

$$\begin{bmatrix}1 & 0\\ b & a\end{bmatrix}^{-1} = \begin{bmatrix}1 & 0\\ -\frac{b}{a} & \frac{1}{a}\end{bmatrix}$$

to work out the inverse of (the affine transformation) $\tau_{a,b}$.

The group $\mathsf{Aff}(1,\mathbb{R})$ contains the subgroup $\mathsf{GL}(1,\mathbb{R})$ of linear transformations (affine transformations which leave the point $x=0$ fixed), and the subgroup of "translations" $x\mapsto x+b$.

EXAMPLE 4. A **Möbius transformation** (or a *fractional linear transformation*) is a function μ of a complex variable z that can be written in the form

$$\mu(z) = \frac{az+b}{cz+d} \tag{2}$$

for some complex numbers a,b,c,d with $ad-bc\neq 0$.

The deceptively simple form of (2) conceals two problems. First, a Möbius transformation can be written in the form (2) in many ways (just as a rational number can be written as $\frac{r}{s}$ in many ways). The second problem stems from the fact that, for example, $z\mapsto \frac{1}{z-z_0}$ is not defined at the point z_0; this means that there is no subset of $\mathbb{C}$ on which all Möbius maps are defined. Informally, the first difficulty is resolved by saying that the 4-tuple (a,b,c,d) is determined within a (complex) scalar multiple. The second difficulty is resolved by joining an extra point (which is called the *point at infinity*) to $\mathbb{C}$; this new point is denoted by ∞.

We make the following (standard) conventions: if $c\neq 0$, we define $\mu(\infty) := \frac{a}{c}$ and $\mu(-\frac{d}{c}) := \infty$; if $c=0$, we define $\mu(\infty):=\infty$. The set $\mathbb{C}\cup\{\infty\}$ is called the **extended complex plane** (sometimes called the *complex projective line*) and is denoted by $\mathbb{C}_\infty$.

It turns out that *each Möbius transformation is a bijection of* $\mathbb{C}_\infty$ *onto itself* (i.e., a permutation of the set $\mathbb{C}_\infty$). The set $\mathsf{Möb}$ of all Möbius transformations (on $\mathbb{C}_\infty$) is a group, called the **Möbius group**.

◇ **Exercise 7.** Show that

(a) the product of two Möbius transformations is another Möbius transformation;
(b) each Möbius transformation has an inverse which is also a Möbius transformation.

1.2. **Permutations of a finite set.** Let M be a finite set with m elements. We may assume that $\mathsf{M} = \{1, 2, \ldots, m\} =: [m]$. The group $\mathfrak{S}_{\mathsf{M}}$ is called the **symmetric group on m elements** and is denoted by $\mathfrak{S}_m$. The elements of $\mathfrak{S}_m$ are called permutations (of degree m).

◇ **Exercise 8.** Let M be a finite set with m elements. Show that

$$\left|\mathsf{M}^{\mathsf{M}}\right| = m^m \quad \text{and} \quad |\mathfrak{S}_m| = m!.$$

(The symbol $|\mathsf{S}|$ denotes the number of elements of the finite set S.)

It is customary, and convenient, to write a permutation $\pi \in \mathfrak{S}_m$ in the form

$$\pi = \begin{bmatrix} 1 & 2 & \ldots & m \\ \pi(1) & \pi(2) & \ldots & \pi(m) \end{bmatrix}$$

where the image $\pi(i)$ of i is placed in the second row underneath i in the first row; for example, the permutation (of degree four) such that $1 \mapsto 4, 2 \mapsto 2, 3 \mapsto 1$ and $4 \mapsto 3$ is denoted by

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}.$$

Two permutations $\pi, \sigma \in \mathfrak{S}_m$ are multiplied by the usual rule for composing maps: $(\pi\sigma)(i) = \pi(\sigma(i))$.

Example 5. The elements of $\mathfrak{S}_3$ are

$$\mathbf{1} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}.$$

Here are two representative computations:

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

Notice that

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

Therefore the symmetric group $\mathfrak{S}_3$ is not Abelian. We can immediately say that $\mathfrak{S}_m$ *is not Abelian when* $m \geq 3$. Why ? (In 1770, J.L. Lagrange (1736–1813) studied the groups $\mathfrak{S}_2, \mathfrak{S}_3$ and $\mathfrak{S}_4$ in relation to the solutions of equations of degree $2, 3$ and 4.)

Permutations in $\mathfrak{S}_m$ can be decomposed into products of simpler permutations. Let $a_1, a_2, \ldots, a_k \in [m]$. A permutation $\pi \in \mathfrak{S}_m$ such that

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_k \mapsto a_1$$

and leaving all other integers in $[m]$ fixed, is called a **cyclic permutation** and is denoted by $(a_1\ a_2\ \ldots\ a_k)$. The number k is its *length* and a cyclic permutation of length k is called a k-**cycle**. If $a \in [m]$, then the 1-cycle (a) is the identity permutation $\mathbf{1} \in \mathfrak{S}_m$.

EXAMPLE 6. The elements of $\mathfrak{S}_3$ are (in cycle notation)

$$\mathbf{1} = (1) = (2) = (3),\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2).$$

Notice that the calculation in EXAMPLE 5 becomes

$$(1\ 3\ 2)(1\ 3) = (1\ 2) \neq (2\ 3) = (1\ 3)(1\ 3\ 2).$$

Two cyclic permutations $\alpha = (a_1\ a_2\ \ldots\ a_r)$ and $\beta = (b_1\ b_2\ \ldots\ b_s)$ in $\mathfrak{S}_m$ are said to be **disjoint** if $a_i \neq b_j$ for all $i, j \in [m]$. For example, $(1\ 2\ 4)$ and $(3\ 5\ 6)$ are disjoint, but $(1\ 2\ 4)$ and $(3\ 4\ 6)$ are not. *Disjoint cycles commute*; that is, if α and β represent disjoint cycles, then $\alpha\beta = \beta\alpha$ (this is PROBLEM 3).

THEOREM 4. *Any permutation of a finite set is either a cycle or can be written as a product of pairwise disjoint cycles; and, except for the order in which the cycles are written, and the inclusion or omission of* 1*-cycles, this can be done in only one way.*

We shall omit the proof of this theorem, but it is illustrated in the following example.

EXAMPLE 7. In each of the following equations the cycles on the right are pairwise disjoint.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{bmatrix} = (1\ 3)(2\ 4\ 5) = (2\ 4\ 5)(1\ 3)$$

$$(1\ 4\ 5)(2\ 3\ 5) = (1\ 4\ 5\ 2\ 3)$$

$$(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2) = (1\ 2\ 3\ 4\ 5\ 6)$$

$$(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1) = (1\ 4\ 3\ 2)$$

$$(1\ 5\ 4\ 6\ 3)(4\ 3\ 6)(2\ 5) = (1\ 5)(2\ 4).$$

NOTE: A 2-cycle is called a **transposition**. For example, the transpositions in $\mathfrak{S}_3$ are $(1,2), (1,3)$ and $(2,3)$. It can be verified that *every permutation in* $\mathfrak{S}_m$ *is a transposition or a product of transpositions.* The decomposition of permutations into transpositions is not unique.

For example, we can write

$$\begin{aligned}(1\ 2\ 3\ 4) &= (1\ 4)(1\ 3)(1\ 2)\\ &= (1\ 2)(2\ 3)(3\ 4)\\ &= (1\ 2)(1\ 4)(2\ 3)(1\ 4)(3\ 4).\end{aligned}$$

In general, it can be proved that the number of transpositions needed is necessarily either even or odd, depending *only* on the given permutation. So, a permutation (in $\mathfrak{S}_m$) which can be expressed as the product of an even number of transpositions is called an **even permutation**; the others are **odd permutations**. Since

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_3)(a_1\ a_2)$$

a cyclic permutation is even precisely when its length is odd.

◇ **Exercise 9.** Show that the set of all even permutations in $\mathfrak{S}_m$ forms a subgroup of $\mathfrak{S}_m$ for each $m \geq 2$. (This subgroup is called the **alternating group** on m elements and is denoted by $\mathfrak{A}_m$.)

◇ **Exercise 10.** If α, β are elements of $\mathfrak{S}_m$, check that $\alpha\beta\alpha^{-1}\beta^{-1}$ always lies in $\mathfrak{A}_m$, and that $\alpha\beta\alpha^{-1}$ belongs to $\mathfrak{A}_m$ whenever β is an even permutation. Work out these elements when $m = 4, \alpha = (2\ 1\ 4\ 3)$ and $\beta = (4\ 2\ 3)$.

◇ **Exercise 11.** Show that the symmetry group of a rectangle which is not a square has four elements. By labeling the vertices $1, 2, 3, 4$, represent the symmetry group as a group of permutations on four elements. (This is the so-called **Klein four-group** V_4.)

1.3. **Morphisms of groups.** The question of deciding when we should regard two groups as being "the same" group is an important one. What we need is a formal way of identifying groups that have identical structures; the identification of two groups is given by a special mapping called an *isomorphism*.

Definition 8. Let $\mathsf{G}, \overline{\mathsf{G}}$ be groups. A mapping $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ is an **isomorphism** if

(I1) Φ is a bijection;
(I2) $\Phi(gh) = \Phi(g)\Phi(h)$ for all $g, h \in \mathsf{G}$.

If such a Φ exists, we say that G and $\overline{\mathsf{G}}$ are *isomorphic* groups and we write $\mathsf{G} \cong \overline{\mathsf{G}}$.

Example 9. Consider the *exponential function* $\exp : \mathbb{R} \to \mathbb{R}^+, \quad x \mapsto e^x$ (here $\mathbb{R}^+ := \{x \in \mathbb{R} : x > 0\}$). It is known that this function is a bijection (from $\mathbb{R}$ onto $\mathbb{R}^+$). The crucial property $e^{x+y} = e^x e^y$ of exp is exactly the condition (I2) that is needed to show that exp is an isomorphism; thus the (additive) group $(\mathbb{R}, +)$ is isomorphic to the (multiplicative) group $(\mathbb{R}^+, \cdot)$.

◇ **Exercise 12.** Show that the (additive) group $\mathbb{R}$ is *not* isomorphic to the (multiplicative) group $\mathbb{R} \setminus \{0\}$.

◇ **Exercise 13.** Let $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ be an isomorphism. Show that

(a) if G is Abelian, then so is $\overline{\mathsf{G}}$;
(b) $\Phi(\mathbf{1}_{\mathsf{G}}) = \mathbf{1}_{\overline{\mathsf{G}}}$;
(c) $\Phi(g^{-1}) = \Phi(g)^{-1}$ for all $g \in \mathsf{G}$.

◇ **Exercise 14.** Show that if $\Phi_1 : \mathsf{G}_1 \to \mathsf{G}_2$ is an isomorphism, then so is $\Phi_1^{-1} : \mathsf{G}_2 \to \mathsf{G}_1$. If, in addition, $\Phi_2 : \mathsf{G}_2 \to \mathsf{G}_3$ is an isomorphism, then so is $\Phi_2 \circ \Phi_1 : \mathsf{G}_1 \to \mathsf{G}_3$.

The first *representation theorem* (for groups) was proved by A. Cayley (1821–1895) in 1878; it tells us that any group can be represented as (isomorphic to) something reasonably concrete: a group of permutations. In other words, the study of subgroups of symmetric groups is no less general than the study of all groups.

Theorem 5. *(Cayley's Theorem) Every group G is isomorphic to a permutation group on G (i.e., a subgroup of $\mathfrak{S}_{\mathsf{G}}$).*

Proof. Each element $a \in \mathsf{G}$ gives a permutation $L_a : \mathsf{G} \to \mathsf{G}$ defined by $L_a(g) := ag$. (L_a is *injective* because if $L_a(g_1) = L_a(g_2)$, then $ag_1 = ag_2$ giving $g_1 = a^{-1}ag_1 = a^{-1}ag_2 = g_2$. It is also *surjective* since if $h \in \mathsf{G}$, then $L_a(a^{-1}h) = aa^{-1}h = h$.) We call L_a the *left translation* by a. Let

$$\overline{\mathsf{G}} := \{L_a \,:\, a \in \mathsf{G}\} \subseteq \mathfrak{S}_{\mathsf{G}}.$$

We have

$$L_a(L_b(g)) = L_a(bg) = a(bg) = (ab)g = L_{ab}(g)$$

for all $g \in \mathsf{G}$. Therefore the product of two elements of $\overline{\mathsf{G}}$ lies in $\overline{\mathsf{G}}$. The identity element $\mathbf{1}_{\mathsf{G}}$ of $\mathfrak{S}_{\mathsf{G}}$ belongs to $\overline{\mathsf{G}}$, and the inverse of L_a in $\mathfrak{S}_{\mathsf{G}}$ is $L_{a^{-1}}$, which is also in $\overline{\mathsf{G}}$. This shows that $\overline{\mathsf{G}}$ is a *subgroup* of $\mathfrak{S}_{\mathsf{G}}$.

The correspondence

$$\Phi : \mathsf{G} \to \overline{\mathsf{G}}, \quad a \mapsto L_a$$

is certainly surjective, and it sends the multiplication of G to that of $\overline{\mathsf{G}}$ because $ab \mapsto L_{ab} = L_aL_b$. It is injective since if $L_a = L_b$, then $a = L_a(\mathbf{1}) = L_b(\mathbf{1}) = b$. Therefore, we have constructed an isomorphism between G and the subgroup $\overline{\mathsf{G}}$ of $\mathfrak{S}_{\mathsf{G}}$. □

Corollary 6. *Every finite group of order m is isomorphic to a subgroup of $\mathfrak{S}_m$.*

Proof. If the elements of G are labeled $1, 2, \ldots, m$ in some way, then each permutation of G induces a permutation of $[m] = \{1, 2, \ldots, m\}$. This gives an isomorphism from $\mathfrak{S}_{\mathsf{G}}$ to $\mathfrak{S}_m$, and the subgroup $\overline{\mathsf{G}} \leq \mathfrak{S}_{\mathsf{G}}$ is therefore isomorphic to a subgroup G' of $\mathfrak{S}_m$. As G is isomorphic to $\overline{\mathsf{G}}$, and the composition of two isomorphisms is an isomorphism (this is **Exercise 14**), G is isomorphic to G'. □

NOTE: Despite its simplicity, CAYLEY'S THEOREM has an important meaning for group theory. It shows the existence of a sort of "universal object" – the family $(\mathfrak{S}_n)_{n\in\mathbb{N}}$ of symmetric groups – in which all finite groups (considered up to isomorphism) live. The phrase "up to isomorphism" is typical, not only of group theory, but of all mathematics, which tends to consider at once all objects having common properties.

If $\mathsf{G} = \overline{\mathsf{G}}$ in the definition of an isomorphism, we have the concept of an isomorphism $\Phi : \mathsf{G} \to \mathsf{G}$ of a group G to itself. Such an isomorphism is called an **automorphism** of G. For example, the identity mapping $\mathrm{id}_{\mathsf{G}} = \mathbf{1}_{\mathsf{G}} : \mathsf{G} \to \mathsf{G}$ (*not* to be confused with the identity element $\mathbf{1}_{\mathsf{G}} = \mathbf{1}$ of G) is an automorphism. In general, a group G also has non-trivial automorphisms. It is easy to see that *the set* $\mathsf{Aut}(\mathsf{G})$ *of all automorphisms of a group* G *forms a group*, in fact, a subgroup of the symmetric group $\mathfrak{S}_{\mathsf{G}}$.

The group of automorphisms $\mathsf{Aut}(\mathsf{G})$ of a group G contains a very special subgroup, which is denoted by $\mathsf{Inn}(\mathsf{G})$ and is called the **group of inner automorphisms**. Its elements are the mappings

$$\mathcal{I}_a : \mathsf{G} \to \mathsf{G}, \quad g \mapsto aga^{-1}.$$

(The inner automorphism $\mathcal{I}_a$ is also referred to as the *conjugation map*; note that $\mathcal{I}_a = L_a \circ R_{a^{-1}}$, where $R_{a^{-1}} : g \mapsto ga^{-1}$ is the *right translation* by a^{-1}.)

◇ **Exercise 15.** Verify that the set $\mathsf{Inn}(\mathsf{G}) := \{\mathcal{I}_a : a \in \mathsf{G}\}$ is a subgroup of $\mathsf{Aut}(\mathsf{G})$.

The mapping

$$\mathcal{I} : \mathsf{G} \to \mathsf{Inn}(\mathsf{G}), \quad a \mapsto \mathcal{I}_a$$

satisfies property (I2) in the definition of an isomorphism: $\mathcal{I}(ab) = \mathcal{I}(a) \circ \mathcal{I}(b)$. However, property (I1) is not necessarily satisfied. For example, if G is an Abelian group, then $aga^{-1} = g$ for all $a, g \in \mathsf{G}$; that is, $\mathcal{I}_a = \mathbf{1}_{\mathsf{G}}$ for all $a \in \mathsf{G}$ and so $\mathsf{Inn}(\mathsf{G})$ only consists of the identity element $\mathbf{1}_{\mathsf{G}}$.

NOTE: One way to study a relatively large and complicated group is to study its smaller and less complicated subgroups. But it would also be useful to be able to study the group as a whole. Homomorphisms, which are more general than isomorphisms, can help to do just that. A homomorphism is a mapping from one group to another that preserves the group operation but is not necessarily one-to-one. Thus the image of a homomorphism can be smaller than the domain, but it will generally reflect some essential features of the domain. Even more importantly, subgroups and images of homomorphisms can be used together to show that most groups are built up from smaller component groups. The concept of "homomorphism" also extends to other algebraic structures (for instance, to rings, fields, modules and algebras); it is unquestionably one of the most important concepts in algebra.

DEFINITION 10. A mapping $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ from the group G to the group $\overline{\mathsf{G}}$ is called a **homomorphism** if

$$\Phi(gh) = \Phi(g)\Phi(h) \qquad \text{for all } g, h \in \mathsf{G}.$$

Various properties of isomorphisms were checked (**Exercise 13**). Those arguments which do not use the fact that an isomorphism is a bijection are equally valid here. Therefore if $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ is a homomorphism, then

(H1) $\Phi(\mathbf{1}_{\mathsf{G}}) = \mathbf{1}_{\overline{\mathsf{G}}}$.
(H2) $\Phi(g^{-1}) = \Phi(g)^{-1}$ for all $g \in \mathsf{G}$.
(H3) The image $\mathsf{Im}\,\Phi := \{\Phi(g) : g \in \mathsf{G}\}$ of G is a subgroup of $\overline{\mathsf{G}}$.

DEFINITION 11. The **kernel** of the homomorphism $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ is the set

$$\mathsf{Ker}\,\Phi := \{g \in \mathsf{G} : \Phi(g) = \mathbf{1}_{\overline{\mathsf{G}}}\}.$$

THEOREM 7. *If $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ is a homomorphism, then its kernel $\mathsf{Ker}\,\Phi$ is a subgroup of G. Moreover, Φ is one-to-one if and only if $\mathsf{Ker}\,\Phi = \{\mathbf{1}_{\mathsf{G}}\}$.*

Proof. Let $a, b \in \mathsf{Ker}\,\Phi$. Then we have

$$\Phi(a^{-1}b) = \Phi(a^{-1})\Phi(b) = \Phi(a)^{-1}\Phi(b) = \mathbf{1}_{\overline{\mathsf{G}}}\,\mathbf{1}_{\overline{\mathsf{G}}} = \mathbf{1}_{\overline{\mathsf{G}}}$$

hence $a^{-1}b \in \mathsf{Ker}\,\Phi$. This shows that $\mathsf{Ker}\,\Phi$ is a subgroup of G.

Since $\mathbf{1}_{\mathsf{G}} \in \mathsf{Ker}\,\Phi$, it is clear that if Φ is one-to-one, then $\mathsf{Ker}\,\Phi = \{\mathbf{1}_{\mathsf{G}}\}$. Why ?

Assume, on the other hand, that $\mathsf{Ker}\,\Phi = \{\mathbf{1}_{\mathsf{G}}\}$. If $a, b \in \mathsf{G}$ and $\Phi(a) = \Phi(b)$, then we have

$$\mathbf{1}_{\overline{\mathsf{G}}} = \Phi(b)^{-1}\Phi(b) = \Phi(a)^{-1}\Phi(b) = \Phi(a^{-1}b)$$

hence $a^{-1}b \in \mathsf{Ker}\,\Phi$ and so $a = b$. This proves that Φ is one-to-one. □

Let $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ be a homomorphism. In general, Φ is neither injective nor surjective. We can make Φ into a surjective mapping by replacing $\overline{\mathsf{G}}$ by $\mathsf{Im}\,\mathsf{G}$ (which is a subgroup of $\overline{\mathsf{G}}$). So the "main" difference between a homomorphism and a isomorphism is the presence of a non-trivial kernel $\mathsf{Ker}\,\Phi$ (which is, one might say, a measure of non-injectivity of Φ). If $\mathsf{Ker}\,\Phi = \{\mathbf{1}_{\mathsf{G}}\}$, then $\Phi : \mathsf{G} \to \mathsf{Im}\,\Phi$ is an isomorphism.

Let $\mathsf{H} = \mathsf{Ker}\,\Phi \leq \mathsf{G}$. We have (for $h \in \mathsf{H}$, $g \in \mathsf{G}$)

$$\Phi(ghg^{-1}) = \Phi(g)\,\Phi(h)\,\Phi(g)^{-1} = \Phi(g)\,\mathbf{1}_{\overline{\mathsf{G}}}\,\Phi(g)^{-1} = \mathbf{1}_{\overline{\mathsf{G}}}$$

i.e., $ghg^{-1} \in \mathsf{H}$; hence, $g\,\mathsf{H}\,g^{-1} \subseteq \mathsf{H}$. If we replace g by g^{-1} here, we obtain $g^{-1}\,\mathsf{H}\,g \subseteq \mathsf{H}$ so that $\mathsf{H} \subseteq g\,\mathsf{H}\,g^{-1}$. Thus

$$g\,\mathsf{H}\,g^{-1} = \mathsf{H} \quad \text{for all } g \in \mathsf{G}. \tag{3}$$

A subgroup which has this property is called a **normal subgroup** (or invariant subgroup); if H is a normal subgroup of G, we write $\mathsf{H} \trianglelefteq \mathsf{G}$. We have thereby proved

THEOREM 8. *The kernel of a homomorphism is always a normal subgroup.*

It is a remarkable fact that the converse of this theorem holds; that is, not only is the kernel of a homomorphism a normal subgroup, but *every normal subgroup is the kernel of a homomorphism* (this is **Exercise 18**).

◇ **Exercise 16.** Let H be a subgroup of G. Show that the following statements are logically equivalent.

(a) $g\,\mathsf{H}\,g^{-1} = \mathsf{H}$ for all $g \in \mathsf{G}$.
(b) $g\,\mathsf{H} = \mathsf{H}\,g$ for all $g \in \mathsf{G}$.
(c) $g\,\mathsf{H}\,g^{-1} \subseteq \mathsf{H}$ for all $g \in \mathsf{G}$.

NOTE: The terms "surjective map" (map onto), "injective map" (one-to-one map or imbedding) and "bijective map" (one-to-one correspondence) which can be used for maps between any sets (with or without any structure) are often replaced by other terms when used for groups (the same happens for other mathematical structures). We use the terms *epimorphism* (homomorphism onto), *monomorphism* (homomorphism whose kernel is the identity element) and *isomorphism* (homomorphism which is both an epimorphism and a monomorphism). There is a tendency to replace the term *homomorphism* with the word *morphism*.

We now give some further examples of group homomorphisms.

EXAMPLE 12. The function

$$\Phi : x \mapsto e^{2\pi i x}$$

is a homomorphism from the (additive) group $\mathbb{R}$ to the (additive) group $\mathbb{C}$. This homomorphism is neither injective nor surjective. It is very easy to see that the kernel is $\mathbb{Z}$ (the group of integers) and the image group is the *circle* $\mathbb{S}^1 := \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}$.

EXAMPLE 13. The *determinant* function

$$\Phi : \mathsf{GL}\,(n, \Bbbk) \to \Bbbk \setminus \{0\}, \quad a \mapsto \Phi(a) := \det a$$

is a homomorphism from the general linear group $\mathsf{GL}\,(n, \Bbbk)$ to the (multiplicative) group $\mathbb{R} \setminus \{0\}$. By definition, we have that $\mathsf{SL}\,(n, \Bbbk) = \mathsf{Ker}\,\Phi$.

EXAMPLE 14. Let π be a permutation in $\mathfrak{S}_n$, and let $\pi = \tau_1\tau_2\cdots\tau_k$ be any decomposition of π into a product of transpositions. Then the number $\epsilon(\pi) := (-1)^k$ is completely determined by π and does not depend on which decomposition is used. $\epsilon(\pi)$ is called the **signature** of π.

The function

$$\operatorname{sgn} : \mathfrak{S}_n \to \{-1, 1\}, \quad \pi \mapsto \epsilon(\pi)$$

is a (surjective) homomorphism from the symmetric group $\mathfrak{S}_n$ to the (multiplicative) group $\{-1,1\} \leq \mathbb{R} \setminus \{0\}$. Clearly, the kernel of (the signature epimorphism) sgn is the alternating group $\mathfrak{A}_n$.

EXAMPLE 15. Consider the function $\Phi : \mathfrak{S}_3 \to \mathsf{GL}(3,\mathbb{R})$ defined as follows:

$$\mathbf{1} \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (1\,2) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (1\,3) \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$(2\,3) \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad (1\,2\,3) \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad (1\,3\,2) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

It is easy to check that Φ is a monomorphism, and that for each $\pi \in \mathfrak{S}_3$ the determinant of $\Phi(\pi)$ is ± 1, depending on the *signature* of the permutation π.

In general, *there exists a monomorphism* $\Phi : \mathfrak{S}_n \to \mathsf{GL}(n,\mathbb{R})$ *such that the matrix* $\Phi(\pi)$, $\pi \in \mathfrak{S}_n$ *has determinant* $\epsilon(\pi)$. (Matrices of the form $\Phi(\pi)$, $\pi \in \mathfrak{S}_n$ are called **permutation matrices**.) The restriction of the monomorphism Φ to the (alternating) group $\mathfrak{A}_n$ is a monomorphism into $\mathsf{SL}(n,\mathbb{R})$. Given any finite group G, the composition $\Phi \circ L$ of the map $L : \mathsf{G} \to \mathfrak{S}_n$ (see CAYLEY'S THEOREM) and $\Phi : \mathfrak{S}_n \to \mathsf{GL}(n,\mathbb{R})$ gives a monomorphism $\mathsf{G} \to \mathsf{GL}(n,\mathbb{R})$.

EXAMPLE 16. Let denote by μ_{abcd} the Möbius transformation $z \mapsto \frac{az+b}{cz+d}$. The function

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \mu_{abcd}$$

is a (surjective) homomorphism from the general linear group $\mathsf{GL}(2,\mathbb{C})$ to the Möbius group $\mathsf{Möb}$. It is not hard to compute the kernel, which turns out to be the set (subgroup) of *scalar matrices*: $\{\lambda\mathbf{1} : \lambda \in \mathbb{C} \setminus \{0\}\} \leq \mathsf{GL}(2,\mathbb{C})$ (this group is isomorphic to $\mathbb{C} \setminus \{0\}$).

1.4. **Cosets and quotient groups.** Let H be a subgroup of G.

DEFINITION 17. A **left coset** of H in G is a set of the form $g\,\mathsf{H} := \{gh : h \in \mathsf{H}\}$. (The element g is called a **coset representative** for $g\,\mathsf{H}$.)

Similarly, we define a **right coset** $\mathsf{H}\,g$.

◇ **Exercise 17.** Let H be a subgroup of G and let $g \in \mathsf{G}$. Show that the following statements are logically equivalent.

(a) $g \in \mathsf{H}$.
(b) $g\,\mathsf{H} = \mathsf{H}$.
(c) $\mathsf{H}\,g = \mathsf{H}$.

If $\mathsf{H} = \mathsf{Ker}\,\Phi$ is the kernel of a homomorphism, then $g\,\mathsf{H} = \mathsf{H}\,g$ because H is normal in G (see THEOREM 7 and **Exercise 16**). Note that *the subgroup* H *itself is a coset*: $\mathsf{H} = \mathbf{1}_\mathsf{G}\,\mathsf{H} = \mathsf{H}\,\mathbf{1}_\mathsf{G}$. However, none of the other cosets can be a (proper) subgroup because, if $g\,\mathsf{H}$ were a subgroup, then we would have $\mathbf{1}_\mathsf{G} \in g\,\mathsf{H}$, so that $\mathbf{1}_\mathsf{G} = gh$, $g = h^{-1}$ and hence $g\,\mathsf{H} = h^{-1}\,\mathsf{H} = \mathsf{H}$.

THEOREM 9. *Let* H *be a subgroup of* G. *Then* G *is the union of its left cosets, and any two left cosets are either equal or disjoint. Further, the left cosets* $a\,\mathsf{H}$ *and* $b\,\mathsf{H}$ *are equal if and only if* $a^{-1}b \in \mathsf{H}$. *(Similar statements are true for right cosets.)*

Proof. Since each element $g \in \mathsf{G}$ is contained in the coset $g\,\mathsf{H}$, the set G is a union of left cosets of H: $\mathsf{G} = \bigcup g_i\,\mathsf{H}$. Suppose that two left cosets $a\,\mathsf{H}$ and $b\,\mathsf{H}$ have an element in common: $g = ah = bh'$. Then $b = ahh'^{-1}$, and any element bh'' of the coset $b\,\mathsf{H}$ has the form $a(hh'^{-1}h'')$. Thus $b\,\mathsf{H} \subseteq a\,\mathsf{H}$. We similarly prove that every element of $a\,\mathsf{H}$ is contained in $b\,\mathsf{H}$. Hence $a\,\mathsf{H} = b\,\mathsf{H}$.

Let $a, b \in \mathsf{G}$ such that $a^{-1}b \in \mathsf{H}$. Then $b \in a\,\mathsf{H}$ and thus $b\,\mathsf{H} \subseteq a\,\mathsf{H}$. We similarly show that $a\,\mathsf{H} \subseteq b\,\mathsf{H}$. Hence $a\,\mathsf{H} = b\,\mathsf{H}$. Conversely, assume that $a\,\mathsf{H} = b\,\mathsf{H}$. Then $ah = bh'$ implies $a^{-1}b = hh'^{-1} \in \mathsf{H}$. This concludes the argument. □

COROLLARY 10. *The partition of* G *into left cosets of* H *gives an equivalence relation on* G.

NOTE: Given a set M, a (binary) *relation* $\sim$ on M is called an **equivalence relation** if the following conditions hold for all $a, b, c \in \mathsf{M}$:

(ER1) $a \sim a$ (reflexivity);
(ER2) if $a \sim b$, then $b \sim a$ (symmetry);
(ER3) if $a \sim b$ and $b \sim c$, then $a \sim c$ (transitivity).

The subset $[a] := \{x \in \mathsf{M} : a \sim x\} \subseteq \mathsf{M}$ (of all elements equivalent to a given element a) is called the **equivalence class** containing a. Clearly, $a \in [a]$. The set of equivalence classes of $\sim$ form a partition of M. (A *partition* of a given set is a collection of non-empty, mutually disjoint subsets such that their union is the whole set.) Conversely, any partition $(C_i)_{i\in I}$ of M defines an equivalence relation $\sim$ on M by $a \sim b$ if and only if $a, b \in C_i$ (for some $i \in I$). If $a \in C_i$, then $[a] = C_i$ and so the sets C_i are precisely the equivalence classes for $\sim$. In particular, the partition of the group G into left cosets of its subgroup H induces an equivalence relation $\sim$ on G, defined by

$$a \sim b \quad \Longleftrightarrow \quad a^{-1}b \in \mathsf{H}.$$

(Condition $a^{-1}b \in \mathsf{H}$ is logically equivalent to condition $a\,\mathsf{H} = b\,\mathsf{H}$.)

Normal subgroups are important because their (left) cosets form a group in a natural way.

THEOREM 11. *If* H *is a normal subgroup of* G*, then the set of all left cosets of* H *in* G *forms a group.*

Proof. The product of two left cosets is again a left coset because

$$(a\,\mathsf{H})(b\,\mathsf{H}) = (ab)\,\mathsf{H} \tag{4}$$

for any two elements $a, b \in \mathsf{G}$. Accepting this for a moment, the coset $\mathbf{1}_{\mathsf{G}}\,\mathsf{H} = \mathsf{H}$ acts as an identity, and $(a^{-1})\,\mathsf{H}$ is the inverse of $a\,\mathsf{H}$ for each $a \in \mathsf{G}$. So we do indeed have a group.

Just why does (4) hold and what does it have to do with the hypothesis that H be a *normal* subgroup of G ? Each element of $(a\,\mathsf{H})(b\,\mathsf{H})$ has the form $ahbh'$ for some $h, h' \in \mathsf{H}$. Rewrite this as

$$ab\left(b^{-1}hb\right)h'$$

and notice that $b^{-1}hb \in \mathsf{H}$ precisely because H is a normal subgroup of G. Why ? Hence $b^{-1}hb = h''$ for some $h'' \in \mathsf{H}$, giving

$$ahbh' = ab\left(b^{-1}hb\right)h' = ab(h''h') \in (ab)\,\mathsf{H}.$$

Thus we have $(a\,\mathsf{H})(b\,\mathsf{H}) \subseteq (ab)\,\mathsf{H}$. The reverse inclusion is easier to check (and works for any subgroup H). Each element of $(ab)\,\mathsf{H}$ has the form abh for some $h \in \mathsf{H}$. Rewriting this as $(a\mathbf{1}_{\mathsf{G}})(bh)$ shows that it belongs to $(a\,\mathsf{H})(b\,\mathsf{H})$, and we deduce $(ab)\,\mathsf{H} \subseteq (a\,\mathsf{H})(b\,\mathsf{H})$. This completes the argument. □

The group of left cosets of H in G introduced above is called the **quotient group** (or factor group) of G by H and denoted by G/H. (Recall that the left cosets of H in G form a partition of G. Each of these cosets represents a *single element* in G/H and it is, in this sense, that we have "divided G by H".)

◇ **Exercise 18.** Show that if $\mathsf{H} \trianglelefteq \mathsf{G}$, then the mapping

$$\mathsf{G} \to \mathsf{G}/\mathsf{H}, \quad g \mapsto g\,\mathsf{H}$$

is a surjective homomorphism, and its kernel is H. (This homomorphism is called the **natural homomorphism** of G onto G/H.)

The natural homomorphism $\mathsf{G} \to \mathsf{G}/\mathsf{H}$ shows that each quotient group of a group G is a homomorphic image of G. The next theorem shows that the converse is also true: each homomorphic image of G is (isomorphic to) a quotient group of G.

THEOREM 12. *(*FIRST ISOMORPHISM THEOREM*) Let* $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ *be a homomorphism with* $\operatorname{Ker}\Phi = \mathsf{H}$*. Then the mapping*

$$\widehat{\Phi} : \mathsf{G}/\mathsf{H} \to \operatorname{Im}\Phi, \quad g\,\mathsf{H} \mapsto \Phi(g)$$

is an isomorphism. (Therefore $\mathsf{G}/\mathsf{H} \cong \operatorname{Im}\Phi$*.)*

Proof. If two cosets $a\,\mathsf{H}, b\,\mathsf{H} \in \mathsf{G}/\mathsf{H}$ are equal, then $a^{-1}b \in \mathsf{H}$. Applying Φ gives

$$\Phi(a^{-1}b) = \Phi(a)^{-1}\Phi(b) = \mathbf{1}_{\overline{\mathsf{G}}}$$

and therefore $\Phi(a) = \Phi(b)$. This means that the function $\widehat{\Phi} : g\,\mathsf{H} \mapsto \Phi(g)$ is *well defined*. Reversing the above computation shows that if $\Phi(a) = \Phi(b)$, then $a\,\mathsf{H} = b\,\mathsf{H}$. So $\widehat{\Phi}$ is injective. The function $\widehat{\Phi}$ is a homomorphism because

$$\widehat{\Phi}\left((a\,\mathsf{H})(b\,\mathsf{H})\right) = \widehat{\Phi}\left((ab)\,\mathsf{H}\right) = \Phi(ab) = \Phi(a)\Phi(b) = \widehat{\Phi}(a\,\mathsf{H})\widehat{\Phi}(b\,\mathsf{H})$$

for any cosets $a\,\mathsf{H}, b\,\mathsf{H} \in \mathsf{G}/\mathsf{H}$. Finally, the image of $\widehat{\Phi}$ is the same as the image of Φ. We have proved that $\widehat{\Phi}$ is an isomorphism from G/H to the image of Φ. □

NOTE: Let π denote the natural projection/homomorphism of G onto $\mathsf{G}/\mathsf{Ker}\,\Phi$, and ι denote the natural inclusion of $\mathsf{Im}\,\Phi$ into $\overline{\mathsf{G}}$. Schematically, the two ways (Φ and $\iota \circ \widehat{\Phi} \circ \pi$) of getting from G to $\overline{\mathsf{G}}$ give the same result for every element of G. This is described by saying that the following diagram commutes:

$$\begin{array}{ccc} \mathsf{G} & \xrightarrow{\Phi} & \overline{\mathsf{G}} \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ \mathsf{G}/\mathsf{Ker}\,\Phi & \xrightarrow{\widehat{\Phi}} & \mathsf{Im}\,\Phi \end{array}$$

Two special cases are particularly useful.

COROLLARY 13. *If $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ is an epimorphism, then $\mathsf{G}/\mathsf{Ker}\,\Phi$ is isomorphic to $\overline{\mathsf{G}}$.*

COROLLARY 14. *Suppose $\Phi : \mathsf{G} \to \overline{\mathsf{G}}$ is an epimorphism. Then Φ is an isomorphism if and only if its kernel $\mathsf{Ker}\,\Phi$ consists just of the identity element of G.*

PROBLEMS (1–5)

(1) Let M be a *finite* set and let $\alpha : \mathsf{M} \to \mathsf{M}$. Prove that the following statements are logically equivalent.
   (a) α is injective.
   (b) α is surjective.
   (c) α is bijective (i.e., a permutation).

(2) Let $\alpha, \beta, \gamma \in \mathsf{M}^{\mathsf{M}}$ such that

$$\beta\alpha = \gamma\alpha = \mathbf{1}_{\mathsf{M}} \quad \text{and} \quad \alpha\beta = \alpha\gamma = \mathbf{1}_{\mathsf{M}}.$$

   Deduce that $\beta = \gamma$. (This proves that each invertible mapping has a unique inverse.)

(3) Assume that α and β are disjoint cycles representing elements of $\mathfrak{S}_m$, say $\alpha = (a_1\ \ldots\ a_r)$ and $\beta = (b_1\ \ldots\ b_s)$ with $a_i \neq b_j$ for all $i, j \in [m]$.

(a) Compute $(\alpha\beta)(a_i)$ and $(\beta\alpha)(a_i)$ for $i \in [r]$.
(b) Compute $(\alpha\beta)(b_j)$ and $(\beta\alpha)(b_j)$ for $j \in [s]$.
(c) Compute $(\alpha\beta)(k)$ and $(\beta\alpha)(k)$ for $k \in [m]$ with $k \neq a_i$ and $k \neq b_j$ for all $i, j \in [m]$.
(d) What do parts (a),(b) and (c), taken together, prove about the relationship between $\alpha\beta$ and $\beta\alpha$?

(4) (Second Isomorphism Theorem) Let H, K be subgroups of G with K normal in G. Then HK is a subgroup of G, $\mathsf{H} \cap \mathsf{K}$ is a normal subgroup of H, and the quotient groups HK/K and $\mathsf{H}/\mathsf{H} \cap \mathsf{K}$ are isomorphic.

(5) Let G be a group.
(a) Given $x \in \mathsf{G}$, the element gxg^{-1} $(= \mathcal{I}_g(x))$ is known as the **conjugate** of x by g. The set of all conjugates of x, that is $C(x) := \{gxg^{-1} : g \in \mathsf{G}\}$ is known as the **conjugacy class** of x (in G). Show that the collection of all conjugacy classes in G constitutes a partition of G.
(b) Given $x \in \mathsf{G}$, define the **centralizer** of x (in G) by

$$\mathsf{Z}(x) := \left\{g \in \mathsf{G} : gxg^{-1} = x\right\}.$$

(Thus the centralizer of x consists of all elements that commute with x.)
(i) Show that, for each $x \in \mathsf{G}$, the centralizer $\mathsf{Z}(x)$ is a subgroup of G.
(ii) Show that conjugates gxg^{-1} and hxh^{-1} of x are equal if and only if $g\,\mathsf{Z}(x) = h\,\mathsf{Z}(x)$. (This means that there is a a one-to-one correspondence between the conjugacy classes of x in G and the set of left cosets of the centralizer of x.)
(c) The **center** of G consists of all those elements which commute with every element of G. It is usually denoted by $\mathsf{Z}(\mathsf{G})$ so that

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

(i) Show that $\mathsf{Z}(\mathsf{G})$ is an Abelian subgroup of G, and is made up of the conjugacy classes which contain just one element.
(ii) Show that the group $\mathsf{Inn}(\mathsf{G})$ of inner automorphisms of G is isomorphic to the quotient group $\mathsf{G}/\mathsf{Z}(\mathsf{G})$.