2 Groups

The cornerstone of modern algebra is the concept of a *group*. Groups are one of the simplest algebraic structures to possess a rich and interesting theory, and they are found embedded in almost all algebraic structures that occur in mathematics [1–3]. Furthermore, they are important for our understanding of some fundamental notions in mathematical physics, particularly those relating to *symmetries* [4].

The concept of a group has its origins in the work of Evariste Galois (1811–1832) and Niels Henrik Abel (1802–1829) on the solution of algebraic equations by radicals. The latter mathematician is honoured with the name of a special class of groups, known as *abelian*, which satisfy the commutative law. In more recent times, Emmy Noether (1888–1935) discovered that every group of symmetries of a set of equations arising from an action principle gives rise to conserved quantities. For example, energy, momentum and angular momentum arise from the symmetries of time translations, spatial translations and rotations, respectively. In elementary particle physics there are further conservation laws related to exotic groups such as $SU(3)$, and their understanding has led to the discovery of new particles. This chapter presents the fundamental ideas of group theory and some examples of how they arise in physical contexts.

2.1 Elements of group theory

A **group** is a set G together with a law of composition that assigns to any pair of elements $g, h \in G$ an element $gh \in G$, called their **product**, satisfying the following three conditions:

(Gp1) The **associative law** holds: $g(hk) = (gh)k$, for all $g,\ h,\ k\ \in G$.

(Gp2) There exists an **identity element** $e \in G$, such that

$$eg = ge = g \qquad \text{for all } g \in G.$$

(Gp3) Each element $g \in G$ has an **inverse** $g^{-1} \in G$ such that

$$g^{-1}g = gg^{-1} = e.$$

More concisely, a group is a semigroup with identity in which every element has an inverse.

Sometimes the fact that the product of two elements is another element of G is worth noting as a separate condition, called the **closure property**. This is particularly relevant when G is a subset of a larger set with a law of composition defined. In such cases it is always necessary to verify that G is **closed** with respect to this law of composition; that is, for every pair $g, h \in G$, their product $gh \in G$. Examples will soon clarify this point.

Condition (Gp1) means that *all* parentheses in products may be omitted. For example, $a((bc)d) = a(b(cd)) = (ab)(cd) = ((ab)c)d$. It is a tedious but straightforward matter to show that all possible ways of bracketing a product of any number of elements are equal. There is therefore no ambiguity in omitting all parentheses in expressions such as $abcd$. However, it is generally important to specify the *order* in which the elements appear in a product.

The identity element e is easily shown to be unique. For, if e' is a second identity such that $e'g = ge' = g$ for all $g \in G$ then, setting $g = e$, we have $e = e'e = e'$ by (Gp2).

Exercise: By a similar argument, show that every $g \in G$ has a *unique* inverse g^{-1}.

Exercise: Show that $(gh)^{-1} = h^{-1}g^{-1}$.

A group G is called **abelian** if the law of composition is commutative,

$$gh = hg \qquad \text{for all } g, h \in G.$$

The notation gh for the product of two elements is the default notation. Other possibilities are $a \cdot b$, $a \times b$, $a + b$, $a \circ b$, etc. When the law of composition is written as an *addition* $g + h$, we will always assume that the commutative law holds, $g + h = h + g$. In this case the identity element is usually written as 0, so that (Gp2) reads $g + 0 = 0 + g = g$. The inverse is then written $-g$, with (Gp3) reading $g + (-g) = 0$ or, more simply, $g - g = 0$. Again, the associative law means we never have to worry about parentheses in expressions such as $a + b + c + \cdots + f$.

A **subgroup** H of a group G is a subset that is a group in its own right. A subset $H \subseteq G$ is thus a subgroup if it contains the identity element of G and is closed under the operations of taking products and inverses:

(a) $h, k \in H \Rightarrow hk \in H$ (closure with respect to taking products);
(b) the identity $e \in H$;
(c) $h \in H \Rightarrow h^{-1} \in H$ (closure with respect to taking inverses).

It is not necessary to verify the associative law since H automatically inherits this property from the larger group G. Every group has two **trivial subgroups** $\{e\}$ and G, consisting of the identity alone and the whole group respectively.

Example 2.1 The integers $\mathbb{Z}$ with addition as the law of composition form a group, called the *additive group of integers*. Strictly speaking one should write this group as $(\mathbb{Z}, +)$, but the law of composition is implied by the word ‘additive’. The identity element is the integer 0, and the inverse of any integer n is $-n$. The *even integers* $\{0, \pm 2, \pm 4, \dots\}$ form a subgroup of the additive group of integers.

Example 2.2 The real numbers $\mathbb{R}$ form a group with addition $x + y$ as the law of composition, called the *additive group of reals*. Again the identity is 0 and the inverse of x is $-x$. The additive group of integers is clearly a subgroup of $\mathbb{R}$. The rational numbers $\mathbb{Q}$ are closed with respect to addition and also form a subgroup of the additive reals $\mathbb{R}$, since the number 0 is rational and if p/q is a rational number then so is $-p/q$.

Example 2.3 The non-zero real numbers $\dot{\mathbb{R}} = \mathbb{R} - \{0\}$ form a group called the *multiplicative group of reals*. In this case the product is taken to be ordinary multiplication xy, the identity is the number 1 and the inverse of x is $x^{-1} = 1/x$. The number 0 must be excluded since it has no inverse.

Exercise: Show that the non-zero rational numbers $\dot{\mathbb{Q}}$ form a multiplicative subgroup of $\dot{\mathbb{R}}$.

Exercise: Show that the complex numbers $\mathbb{C}$ form a group with respect to addition, and $\dot{\mathbb{C}} = \mathbb{C} - \{0\}$ is a group with respect to multiplication of complex numbers.

Exercise: Which of the following sets form a group with respect to addition: (i) the rational numbers, (ii) the irrational numbers, (iii) the complex numbers of modulus 1? Which of them is a group with respect to multiplication?

A group G consisting of only a finite number of elements is known as a **finite group**. The number of elements in G is called its **order**, denoted $|G|$.

Example 2.4 Let k be any natural number and $\mathbb{Z}_k = \{[0], [1], \dots, [k-1]\}$ the integers modulo k, defined in Example 1.3, with **addition modulo** k as the law of composition

$$[a] + [b] = [a + b].$$

$\mathbb{Z}_k$ is called the **additive group of integers modulo** k. It is a finite group of order k, written $|\mathbb{Z}_k| = k$. There is little ambiguity in writing the elements of $\mathbb{Z}_k$ as $0, 1, \dots, k-1$ and $[a + b]$ is often replaced by the notation $a + b \mod k$.

Exercise: Show that the definition of addition modulo k is independent of the choice of representatives from the residue classes $[a]$ and $[b]$.

Example 2.5 If a group G has an element a such that its powers $\{a, a^2, a^3, \dots\}$ run through all of its elements, then G is said to be a **cyclic group** and a is called a **generator** of the group. If G is a finite cyclic group and a is a generator, then there exists a positive integer m such that $a^m = e$. If m is the lowest such integer then every element $g \in G$ can be uniquely written $g = a^i$ where $1 \le i \le m$, for if $g = a^i = a^j$ and $1 \le i < j \le m$ then we have the contradiction $a^{j-i} = e$ with $1 \le (j - i) < m$. In this case the group is denoted C_m and its order is $|C_m| = m$. The additive group of integers modulo k is a cyclic group of order k, but in this case the notation a^n is replaced by

$$na = \underbrace{a + a + \cdots + a}_{n} \mod k.$$

Example 2.6 Let $p > 2$ be any prime number. The non-zero integers modulo p form a group of order $p - 1$ with respect to multiplication modulo p,

$$[a][b] = [ab] \equiv ab \mod p,$$

denoted G_p. The identity is obviously the residue class [1], but in order to prove the existence of inverses one needs the following result from number theory: if p and q are relatively prime numbers then there exist integers k and m such that $kp + mq = 1$. Since p is a prime number, if $[q] \neq [0]$ then q is relatively prime to p and for some k and m

$$[m][q] = [1] - [k][p] = [1].$$

Hence $[q]$ has an inverse $[q]^{-1} = [m]$.

For finite groups of small order the law of composition may be displayed in the form of a multiplication table, where the (i, j)th entry specifies the product of the ith element and the jth element. For example, here is the multiplication table of G_7:

G_7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

2.2 Transformation and permutation groups

All groups in the above examples are abelian. The most common examples of non-commutative groups are found in a class called *transformation groups*. We recall from Section 1.4 that a *transformation* of a set X is a map $g : X \to X$ that is one-to-one and onto. The map g then has an inverse $g^{-1} : X \to X$ such that $g^{-1} \circ g = g \circ g^{-1} = \mathrm{id}_X$. Let the product of two transformations g and h be defined as their functional composition $gh = g \circ h$,

$$(gh)(x) = g \circ h(x) = g(h(x)).$$

The set of all transformations of X forms a group, denoted Transf(X):

Closure: if g and h are transformations of X then so is gh;
Associative law: $f(gh) = (fg)h$;
Identity: $e = \mathrm{id}_X \in \mathrm{Transf}(X)$;
Inverse: if g is a transformation of X then so is g^{-1}.

Closure follows from the fact that the composition of two transformations (invertible maps) results in another invertible map, since $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. The associative law holds automatically for composition of maps, while the identity and inverse are trivial. By a **transformation group** of X is meant any subgroup of Transf(X).

If X is a finite set of cardinality n then the transformations of X are called **permutations** of the elements of X. The group of permutations of $X = \{1, 2, \dots, n\}$ is called the **symmetric group of order** n, denoted S_n. Any subgroup of S_n is called a **permutation group**. A permutation π on n elements can be represented by the permutation symbol

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

where $a_1 = \pi(1),\ a_2 = \pi(2)$, etc. The same permutation can also be written as

$$\pi = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

where $b_1,\ b_2, \dots, b_n$ are the numbers $1, 2, \dots, n$ in an arbitrary order and $c_1 = \pi(b_1),\ c_2 = \pi(b_2), \dots, c_n = \pi(b_n)$. For example, the permutation π that interchanges the elements 2 and 4 from a four-element set can be written in several ways,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \text{ etc.}$$

In terms of permutation symbols, if

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \quad \text{and} \quad \pi = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

then their product is the permutation $\pi\sigma = \pi \circ \sigma$,

$$\pi\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}.$$

Note that this product involves first performing the permutation σ followed by π, which is opposite to the order in which they are written; conventions can vary on this point. Since the product is a functional composition, the associative law is guaranteed. The identity permutation is

$$\mathrm{id}_n = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

while the inverse of any permutation is given by

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

The symmetric group S_n is a finite group of order $n!$, the total number of ways n objects may be permuted. It is not abelian in general. For example, in S_3

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

while

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

A more compact notation for permutations is the **cyclic notation**. Begin with any element to be permuted, say a_1. Let a_2 be the result of applying the permutation π to a_1, and let a_3 be the result of applying it to a_2, etc. Eventually the first element a_1 must reappear, say as $a_{m+1} = a_1$. This defines a **cycle**, written $(a_1\, a_2\, \dots a_m)$. If $m = n$, then π is said to be a **cyclic permutation**. If $m < n$ then take any element b_1 not appearing in the cycle generated by a_1 and create a new cycle $(b_1\, b_2\, \dots\, b_m)$ of successive images of b_1 under π. Continue until all the elements $1, 2, \ldots, n$ are exhausted. The permutation π may be written as the product of its cycles; for example,

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

Note that it does not matter which element of a cycle is chosen as the first member, so that $(1\,4\,7\,6) = (7\,6\,1\,4)$ and $(2\,5) = (5\,2)$.

Cycles of length 1 such as (3) merely signify that the permutation π leaves the element 3 unchanged. Nothing is lost if we totally ignore such 1-cycles from the notation, writing

$$(1\,4\,7\,6)(2\,5)(3) = (1\,4\,7\,6)(2\,5).$$

The order in which cycles that have no common elements is written is also immaterial,

$$(1\,4\,7\,6)(2\,5) = (2\,5)(1\,4\,7\,6).$$

Products of permutations are easily carried out by following the effect of the cycles on each element in succession, taken in order from right to left. For example,

$$(1\,3\,7)(5\,4\,2)(1\,2)(3\,4\,6\,7)(1\,4\,6) = (1\,6\,5\,4)(2\,3)(7)$$

follows from $1 \to 4 \to 6$, $6 \to 1 \to 2 \to 5$, $5 \to 4$, $4 \to 6 \to 7 \to 1$, etc.

Exercise: Express each permutation on $\{1, 2, 3\}$ in cyclic notation and write out the 6×6 multiplication table for S_3.

Cycles of length 2 are called **interchanges**. Every cycle can be written as a product of interchanges,

$$(a_1\,a_2\,a_3\ \ldots\ a_n) = (a_2\,a_3)(a_3\,a_4)\ldots(a_{n-1}\,a_n)(a_n\,a_1),$$

and since every permutation π is a product of cycles, it is in turn a product of interchanges. The representation of a permutation as a product of interchanges is not in general unique, but the number of interchanges needed is either always odd or always even. To prove this, consider the homogeneous polynomial

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= \prod_{i<j}(x_i - x_j) \\ &= (x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_n)(x_2 - x_3)\ldots(x_{n-1} - x_n). \end{aligned}$$

If any pair of variables x_i and x_j are interchanged then the factor $(x_i - x_j)$ changes sign and the factor $(x_i - x_k)$ is interchanged with $(x_j - x_k)$ for all $k \neq i, j$. When $k < i < j$ or $i < j < k$ neither factor changes sign in the latter process, while if $i < k < j$ each factor suffers a sign change and again there is no overall sign change in the product of these two factors. The net result of the interchange of x_i and x_j is a change of sign in the polynomial $f(x_1, x_2, \ldots, x_n)$. Hence permutations may be called **even** or **odd** according to whether f is left unchanged, or changes its sign. In the first case they can be written as an even, and

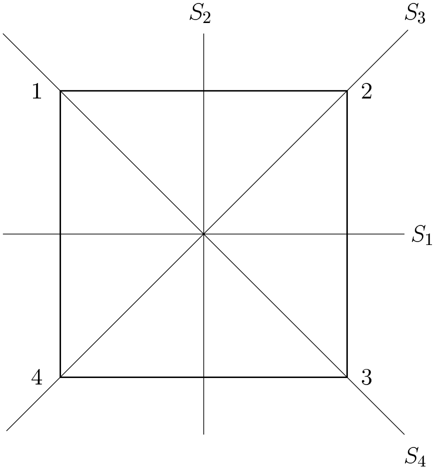


Figure 2.1 Symmetries of the square

only an even, number of interchanges, while in the second case they can only be written as an odd number. This quality is called the **parity** of the permutation and the quantity

$$(-1)^\pi = \begin{cases} +1 & \text{if } \pi \text{ is even,} \\ -1 & \text{if } \pi \text{ is odd,} \end{cases}$$

is called the **sign** of the permutation. Sometimes it is denoted sign π.

Exercise: Show that

$$(-1)^{\pi\sigma} = (-1)^{\sigma\pi} = (-1)^\pi(-1)^\sigma. \tag{2.1}$$

Example 2.7 In the Euclidean plane consider a square whose corners are labelled 1, 2, 3 and 4. The *group of symmetries of the square* consists of four rotations (clockwise by 0°, 90°, 180° and 270°), denoted R_0, R_1, R_2 and R_3 respectively, and four reflections S_1, S_2, S_3 and S_4 about the axes in Fig. 2.1.

This group is not commutative since, for example, $R_1 S_1 = S_4 \neq S_1 R_1 = S_3$ – remember, the rightmost operation is performed first in any such product! A good way to do these calculations is to treat each of the transformations as a permutation of the vertices; for example, in cyclic notation $R_1 = (1\,2\,3\,4)$, $R_2 = (1\,3)(2\,4)$, $S_1 = (1\,4)(2\,3)$, $S_3 = (1\,3)$, etc. Thus the symmetry group of the square is a subgroup of order 8 of the symmetric group S_4.

Exercise: Show that the whole group can be generated by repeated applications of R_1 and S_1.

Example 2.8 An important subgroup of S_n is the set of all even permutations, $(-1)^\pi = 1$, known as the **alternating group**, denoted A_n. The closure property, that the product of two even permutations is always even, follows immediately from Eq. (2.1). Furthermore, the identity permutation id_n is clearly even and the inverse of an even permutation π must be even since

$$1 = (-1)^{\mathrm{id}_n} = (-1)^{\pi\pi^{-1}} = (-1)^{\pi}(-1)^{\pi^{-1}} = (-1)^{\pi^{-1}}.$$

Hence A_n is a subgroup of S_n. Its order is $n!/2$.

Example 2.9 Let π be any permutation of $1, 2, \dots, n$. Since there are a total of $n!$ permutations of n objects, successive iterations $\pi^2, \pi^3, \dots$ must eventually arrive at repetitions, say $\pi^k = \pi^l$, whence $\pi^{l-k} = \mathrm{id}_n$. The smallest m with the property $\pi^m = \mathrm{id}_n$ is called the **order of the permutation** π. Any cycle of length k evidently has order k, and since every permutation can be written as a product of cycles, the order of a permutation is the lowest common multiple of its cycles. For example, the order of $(1\,2\,3)(4\,5)$ is the lowest common multiple of 3 and 2, which is 6. The set of elements $\{\mathrm{id}_n, \pi, \pi^2, \dots, \pi^{m-1} = \pi^{-1}\}$ form a subgroup of S_n, called the *subgroup generated by* π. It is clearly a cyclic group.

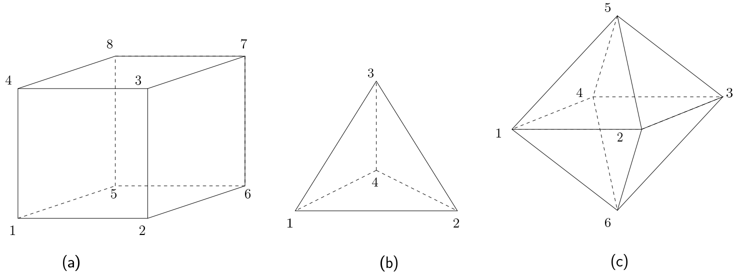
Problems

Problem 2.1 Show that the only finite subgroup of the additive reals is the singleton $\{0\}$, while the only finite subgroups of the multiplicative reals are the sets $\{1\}$ and $\{1, -1\}$.

Find all finite subgroups of the multiplicative complex numbers $\dot{\mathbb{C}}$.

Problem 2.2 Write out the complete 8×8 multiplication table for the group of symmetries of the square D_4 described in Example 2.7. Show that R_2 and S_1 generate an abelian subgroup and write out its multiplication table.

Problem 2.3 (a) Find the symmetries of the cube, Fig. 2.2(a), which keep the vertex 1 fixed. Write these symmetries as permutations of the vertices in cycle notation.
(b) Find the group of rotational symmetries of the regular tetrahedron depicted in Fig. 2.2(b).
(c) Do the same for the regular octahedron, Fig. 2.2(c).



(a)

(b)

(c)

Figure 2.2

Problem 2.4 Show that the multiplicative groups modulo a prime G_7, G_{11}, G_{17} and G_{23} are cyclic. In each case find a generator of the group.

Problem 2.5 Show that the order of any cyclic subgroup of S_n is a divisor of $n!$.

2.3 Matrix groups

Linear transformations

Let $\mathbb{R}^n$ be the space of $n \times 1$ real column vectors

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

A mapping $A : \mathbb{R}^n \to \mathbb{R}^n$ is said to be **linear** if

$$A(a\mathbf{x} + b\mathbf{y}) = aA(\mathbf{x}) + bA(\mathbf{y})$$

for all vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ and all real numbers $a, b \in \mathbb{R}$. Writing

$$\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{e}_i \quad \text{where} \quad \mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},\ \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

we have

$$A(\mathbf{x}) = \sum_{i=1}^{n} x_i A(\mathbf{e}_i).$$

If we set

$$A(\mathbf{e}_i) = \sum_{j=1}^{n} a_{ji} \mathbf{e}_j$$

the components x_i of the vector $\mathbf{x}$ transform according to the formula

$$\mathbf{x} \mapsto \mathbf{x}' = A(\mathbf{x}) \quad \text{where} \quad x'_i = \sum_{j=1}^{n} a_{ij} x_j (i = 1, \dots, n).$$

It is common to write this mapping in the form

$$\mathbf{x}' = \mathsf{A}\mathbf{x}$$

where $\mathsf{A} = [a_{ij}]$ is the $n \times n$ array

$$\mathsf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

A is called the **matrix of the linear mapping** A, and a_{ij} are its **components**. The matrix AB of the product transformation AB is then given by the matrix multiplication rule,

$$(\mathsf{AB})_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Exercise: Prove this formula.

Linear maps on $\mathbb{R}^n$ and $n \times n$ matrices as essentially identical concepts, the latter being little more than a notational device for the former. Be warned, however, when we come to *general* vector spaces in Chapter 3 such an identification cannot be made in a natural way. In later chapters we will often adopt a different notation for matrix components in order to take account of this difficulty, but for the time being it is possible to use standard matrix notation as we are only concerned with the particular vector space $\mathbb{R}^n$ for the rest of this chapter.

A **linear transformation** A is a one-to-one linear mapping from $\mathbb{R}^n$ onto itself. Such a map is invertible, and its matrix A has non-zero determinant, $\det \mathsf{A} \neq 0$. Such a matrix is said to be **non-singular** and have an inverse matrix A^{-1} given by

$$(\mathsf{A}^{-1})_{ij} = \frac{A_{ji}}{\det \mathsf{A}},$$

where A_{ji} is the (j, i) cofactor of the matrix A, defined as the determinant of the submatrix of A formed by removing its jth row and ith column and multiplied by the factor $(-1)^{i+j}$. The inverse of a matrix acts as both right and left inverse:

$$\mathsf{AA}^{-1} = \mathsf{A}^{-1}\mathsf{A} = \mathsf{I}, \tag{2.2}$$

where I is the $n \times n$ **unit matrix**

$$\mathsf{I} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

The components of the unit matrix are frequently written as the **Kronecker delta**

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{2.3}$$

The inverse of AB is given by the matrix identity

$$(\mathsf{AB})^{-1} = \mathsf{B}^{-1}\mathsf{A}^{-1}. \tag{2.4}$$

Matrix groups

The set of all $n \times n$ non-singular real matrices is a group, denoted $GL(n, \mathbb{R})$. The key to this result is the product law of determinants

$$\det(\mathsf{AB}) = \det(\mathsf{A}) \det(\mathsf{B}). \tag{2.5}$$

Closure: this follows from the fact that $\det \mathsf{A} \neq 0$ and $\det \mathsf{B} \neq 0$ implies that $\det(\mathsf{AB}) = \det \mathsf{A} \det \mathsf{B} \neq 0$.
Associative law: $(\mathsf{AB})\mathsf{C} = \mathsf{A}(\mathsf{BC})$ is true of *all* matrices, singular or not.
Identity: the $n \times n$ unit matrix I is an identity element since $\mathsf{IA} = \mathsf{AI} = \mathsf{A}$ for all $n \times n$ matrices A.
Inverse: from Eq. (2.2) A^{-1} clearly acts as an inverse element to A. Equation (2.5) ensures that A^{-1} is non-singular and also belongs to $GL(n, \mathbb{R})$, since

$$\det \mathsf{A}^{-1} = \frac{1}{\det \mathsf{A}}.$$

A similar discussion shows that the set of $n \times n$ non-singular matrices with complex components, denoted $GL(n, \mathbb{C})$, also forms a group. Except for the case $n = 1$, these groups are non-abelian since matrices do not in general commute, $\mathsf{AB} \neq \mathsf{BA}$. The groups $GL(n, \mathbb{R})$ and $GL(n, \mathbb{C})$ are called the **general linear groups of order** n. Subgroups of these groups, whose elements are matrices with the law of composition being matrix multiplication, are generically called **matrix groups** [5].

In the following examples the associative law may be assumed, since the law of composition is matrix multiplication. Frequent use will be made of the concept of the **transpose** A^T of a matrix A, defined as the matrix formed by reflecting A about its diagonal,

$$(\mathsf{A}^T)_{ij} = a_{ji} \quad \text{where} \quad \mathsf{A} = [a_{ij}].$$

The following identities can be found in many standard references such as Hildebrand [6], and should be known to the reader:

$$(\mathsf{AB})^T = \mathsf{B}^T \mathsf{A}^T, \tag{2.6}$$

$$\det \mathsf{A}^T = \det \mathsf{A}, \tag{2.7}$$

and if A is non-singular then the inverse of its transpose is the transpose of its inverse,

$$(\mathsf{A}^{-1})^T = (\mathsf{A}^T)^{-1}. \tag{2.8}$$

Example 2.10 The **special linear group** or **unimodular group** of degree n, denoted $SL(n, \mathbb{R})$, is defined as the set of $n \times n$ **unimodular** matrices, real matrices having determinant 1. Closure with respect to matrix multiplication follows from Eq. (2.5),

$$\det \mathsf{A} = \det \mathsf{B} = 1 \Longrightarrow \det(\mathsf{AB}) = \det \mathsf{A} \det \mathsf{B} = 1.$$

The identity $\mathsf{I} \in SL(n, \mathbb{R})$ since $\det \mathsf{I} = 1$, and closure with respect to inverses follows from

$$\det \mathsf{A} = 1 \Longrightarrow \det \mathsf{A}^{-1} = \frac{1}{\det \mathsf{A}} = 1.$$

Example 2.11 A matrix A is called **orthogonal** if its inverse is equal to its transpose,

$$\mathsf{A}\mathsf{A}^T = \mathsf{A}^T\mathsf{A} = \mathsf{I}. \tag{2.9}$$

The set of real orthogonal $n \times n$ matrices, denoted $O(n)$, forms a group known as the **orthogonal group of order** n:
Closure: if A and B are orthogonal matrices, $\mathsf{A}\mathsf{A}^T = \mathsf{B}\mathsf{B}^T = \mathsf{I}$, then so is their product AB,

$$(\mathsf{AB})(\mathsf{AB})^T = \mathsf{ABB}^T\mathsf{A}^T = \mathsf{AIA}^T = \mathsf{AA}^T = \mathsf{I}.$$

Identity: the unit matrix I is clearly orthogonal since $\mathsf{I}^T\mathsf{I} = \mathsf{I}^2 = \mathsf{I}$.
Inverse: if A is an orthogonal matrix then A^{-1} is also orthogonal for, using (2.8) and (2.4),

$$\mathsf{A}^{-1}(\mathsf{A}^{-1})^T = \mathsf{A}^{-1}(\mathsf{A}^T)^{-1} = (\mathsf{A}^T\mathsf{A})^{-1} = \mathsf{I}^{-1} = \mathsf{I}.$$

The determinant of an orthogonal matrix is always ±1 since

$$\mathsf{AA}^T = \mathsf{I} \implies \det\mathsf{A}\det\mathsf{A}^T = \det(\mathsf{AA}^T) = \det\mathsf{I} = 1.$$

Hence $(\det\mathsf{A})^2 = 1$ by (2.7) and the result $\det\mathsf{A} = \pm 1$ follows at once. The orthogonal matrices with determinant 1 are called **proper orthogonal matrices**, while those with determinant -1 are called **improper**. The proper orthogonal matrices, denoted $SO(n)$, form a group themselves called the **proper orthogonal group of order** n. This group is often known as the **rotation group in** n **dimensions** – see Section 2.7. It is clearly a subgroup of the special linear group $SL(n, \mathbb{R})$.

Example 2.12 Let p and q be non-negative integers such that $p + q = n$, and define G_p to be the $n \times n$ matrix whose components $\mathsf{G}_p = [g_{ij}]$ are defined by

$$g_{ij} = \begin{cases} 1 & \text{if } i = j \le p, \\ -1 & \text{if } i = j > p, \\ 0 & \text{if } i \ne j. \end{cases}$$

We use $O(p, q)$ to denote the set of matrices A such that

$$\mathsf{A}^T\mathsf{G}_p\mathsf{A} = \mathsf{G}_p. \tag{2.10}$$

It follows from this equation that any matrix belonging to $O(p, q)$ is non-singular, for on taking determinants,

$$\det\mathsf{A}^T\det\mathsf{G}_p\det\mathsf{A} = \det\mathsf{G}_p.$$

Since $\det\mathsf{G}_p = \pm 1 \ne 0$ we have $\det\mathsf{A}^T\det\mathsf{A} = (\det\mathsf{A})^2 = 1$, and consequently

$$\det\mathsf{A} = \pm 1.$$

The group properties of $O(p, q)$ follow:

Closure: if A and B both satisfy Eq. (2.10), then so does their product AB, for

$$(\mathsf{AB})^T \mathsf{G}_p (\mathsf{AB}) = \mathsf{B}^T \mathsf{A}^T \mathsf{G}_p \mathsf{AB} = \mathsf{B}^T \mathsf{G}_p \mathsf{B} = \mathsf{G}_p.$$

Identity: the unit matrix $\mathsf{A} = \mathsf{I}$ clearly satisfies Eq. (2.10).
Inverse: if Eq. (2.10) is multiplied on the right by A^{-1} and on the left by $(\mathsf{A}^{-1})^T$, we have from (2.8)

$$\mathsf{G}_p = (\mathsf{A}^{-1})^T \mathsf{G}_p \mathsf{A}^{-1}.$$

Hence A^{-1} satisfies (2.10) and belongs to $O(p, q)$.

The group $O(p, q)$ is known as the **pseudo-orthogonal group of type** (p, q). The case $q = 0$, $p = n$ reduces to the orthogonal group $O(n)$. As for the orthogonal group, those elements of $O(p, q)$ having determinant 1 form a subgroup denoted $SO(p, q)$.

Example 2.13 Let J be the $2n \times 2n$ matrix

$$\mathsf{J} = \begin{pmatrix} \mathsf{O} & \mathsf{I} \\ -\mathsf{I} & \mathsf{O} \end{pmatrix},$$

where O is the $n \times n$ zero matrix and I is the $n \times n$ unit matrix. A $2n \times 2n$ matrix A is said to be **symplectic** if it satisfies the equation

$$\mathsf{A}^T \mathsf{J} \mathsf{A} = \mathsf{J}. \tag{2.11}$$

The argument needed to show that these matrices form a group is essentially identical to that just given for $O(p, q)$. Again, since $\det \mathsf{J} = 1$, it follows immediately from (2.11) that $\det \mathsf{A} = \pm 1$, and A is non-singular. The group is denoted $Sp(2n)$, called the **symplectic group of order** $2n$.

Exercise: Show that the symplectic matrices of order 2 are precisely the unimodular matrices of order 2. Hence for $n = 2$ all symplectic matrices have determinant 1. It turns out that symplectic matrices of *any* order have determinant 1, but the proof of this is more complicated.

Example 2.14 The **general complex linear group**, $GL(n, \mathbb{C})$, is defined exactly as for the reals. It is the set of non-singular complex $n \times n$ matrices, where the law of composition is matrix product using multiplication of complex numbers. We define special subgroups of this group the same way as for the reals:

$SL(n, \mathbb{C})$ is the **complex unimodular group of degree** n, consisting of complex $n \times n$ matrices having determinant 1;
$O(n, \mathbb{C})$ is the **complex orthogonal group of degree** n, whose elements are complex $n \times n$ matrices A satisfying $\mathsf{A}^T \mathsf{A} = \mathsf{I}$;
$SO(n, \mathbb{C})$ is the **complex proper orthogonal group**, which is the intersection of the above two groups.

There is no complex equivalent of the pseudo-orthogonal groups since these are all isomorphic to $O(n, \mathbb{C})$ – see Problem 2.7.

Example 2.15 The **adjoint** of a complex matrix A is defined as its complex conjugate transpose $\mathsf{A}^\dagger = \overline{\mathsf{A}^T}$, whose components are $a^\dagger_{ij} = \overline{a_{ji}}$ where a bar over a complex number refers to its complex conjugate. An $n \times n$ complex matrix U is called **unitary** if

$$\mathsf{U}\mathsf{U}^\dagger = \mathsf{I}. \tag{2.12}$$

It follows immediately that

$$\det \mathsf{U}\,\overline{\det \mathsf{U}} = |\det \mathsf{U}|^2 = 1,$$

and there exists a real number ϕ with $0 \le \phi < 2\pi$ such that $\det \mathsf{U} = \mathrm{e}^{i\phi}$. Hence all unitary matrices are non-singular and the group properties are straightforward to verify. The group of all $n \times n$ unitary matrices is called the **unitary group of order** n, denoted $U(n)$. The subgroup of unitary matrices having $\det U = 1$ is called the **special unitary group of order** n, denoted $SU(n)$.

Problems

Problem 2.6 Show that the following sets of matrices form groups with respect to addition of matrices, but that none of them is a group with respect to matrix multiplication: (i) real antisymmetric $n \times n$ matrices ($\mathsf{A}^T = -\mathsf{A}$), (ii) real $n \times n$ matrices having vanishing trace ($\operatorname{tr} \mathsf{A} = \sum_{i=1}^n a_{ii} = 0$), (iii) complex hermitian $n \times n$ matrices ($\mathsf{H}^\dagger = \mathsf{H}$).

Problem 2.7 Find a diagonal complex matrix S such that

$$\mathsf{I} = \mathsf{S}^T \mathsf{G}_p \mathsf{S}$$

where G_p is defined in Example 2.12. Show that:

(a) Every complex matrix A satisfying Eq. (2.10) can be written in the form

$$\mathsf{A} = \mathsf{S}\mathsf{B}\mathsf{S}^{-1}$$

where B is a complex orthogonal matrix (i.e. a member of $O(n, \mathbb{C})$).

(b) The complex versions of the pseudo-orthogonal groups, $O(p, q, \mathbb{C})$, are all isomorphic to each other if they have the same dimension,

$$O(p, q, \mathbb{C}) \cong O(n, \mathbb{C}) \quad \text{where} \quad n = p + q.$$

Problem 2.8 Show that every element of $SU(2)$ has the form

$$\mathsf{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{where} \quad a = \overline{d} \text{ and } b = -\overline{c}.$$

2.4 Homomorphisms and isomorphisms

Homomorphisms

Let G and G' be groups. A **homomorphism** $\varphi : G \to G'$ is a map from G to G' that preserves products,

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \text{for all } a, b \in G.$$

Theorem 2.1 *Under a homomorphism $\varphi : G \to G'$ the identity e of G is mapped to the identity e' of G', and the inverse of any element g of G to the inverse of its image $\varphi(g)$.*

Proof: For any $g \in G$

$$\varphi(g) = \varphi(ge) = \varphi(g)\varphi(e).$$

Multiplying both sides of this equation on the left by $(\varphi(g))^{-1}$ gives the desired result,

$$e' = e'\varphi(e) = \varphi(e).$$

If $g \in G$ then $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e) = e'$. Hence $\varphi(g^{-1}) = (\varphi(g))^{-1}$ as required. ■

Exercise: If $\varphi : G \to G'$ is a homomorphism, show that the image set

$$\mathrm{im}(\varphi) = \varphi(G) = \{g' \in G' \mid g' = \varphi(g),\ g \in G\} \tag{2.13}$$

is a subgroup of G'.

Example 2.16 For any real number $x \in \mathbb{R}$, define its *integral part* $[x]$ to be the largest integer that is less than or equal to x, and its *fractional part* to be $(x) = x - [x]$. Evidently $0 \le (x) < 1$. On the half-open interval $[0, 1)$ of the real line define *addition modulo 1* by

$$a + b \bmod 1 \;=\; (a + b) = \text{fractional part of } a + b.$$

This defines an abelian group, *the group of real numbers modulo 1*. To verify the group axioms we note that 0 is the identity element and the inverse of any $a > 0$ is $1 - a$. The inverse of $a = 0$ is 0.

The map $\varphi_1 : \mathbb{R} \to [0, 1)$ from the additive group of real numbers to the group of real numbers modulo 1 defined by $\varphi_1(x) = (x)$ is a homomorphism since $(x) + (y) = (x + y)$.

Exercise: Show that the *circle map* or *phase map* $C : \dot{\mathbb{C}} \to [0, 2\pi)$ defined by

$$C(z) = \theta \quad \text{where} \quad z = |z|\mathrm{e}^{i\theta}, 0 \le \theta < 2\pi$$

is a homomorphism from the multiplicative group of complex numbers to the additive group of reals modulo 2π, defined in a similar way to the reals modulo 1 in the previous example.

Example 2.17 Let sign : $S_n \to \{+1, -1\}$ be the map that assigns to every permutation π its parity,

$$\mathrm{sign}(\pi) = (-1)^{\pi} = \begin{cases} +1 & \text{if } \pi \text{ is even,} \\ -1 & \text{if } \pi \text{ is odd.} \end{cases}$$

From (2.1), sign is a homomorphism from S_n to the multiplicative group of reals

$$\mathrm{sign}(\pi\sigma) = \mathrm{sign}(\pi)\mathrm{sign}(\sigma).$$

Exercise: From Eq. (2.5) show that the determinant map $\det : GL(n, \mathbb{R}) \to \dot{\mathbb{R}}$ from the general linear group of order n to the multiplicative group of reals is a homomorphism.

Isomorphisms

An **isomorphism** is a homomorphism that is one-to-one and onto. If an isomorphism exists between two groups G and G' they are said to be **isomorphic**, written $G \cong G'$. The two groups are then essentially identical in all their group properties.

Exercise: Show that if $\varphi : G \to G'$ is an isomorphism, then so is the inverse map $\varphi^{-1} : G' \to G$.

Exercise: If $\varphi : G \to G'$ and $\psi : G' \to G''$ are isomorphisms then so is $\psi \circ \varphi : G \to G''$.

These two statements show that isomorphism is a symmetric and transitive relation on the class of all groups. Hence it is an equivalence relation on the class of groups, since the reflexive property follows from the fact that the identity map $\mathrm{id}_G : G \to G$ is trivially an isomorphism. Note that the word 'class' must be used in this context because the 'set of all groups' is too large to be acceptable. *Group theory* is the study of equivalence classes of isomorphic groups. Frequently it is good to single out a special representative of an equivalence class. Consider, for example, the following useful theorem for finite groups:

Theorem 2.2 (Cayley) *Every finite group G of order n is isomorphic to a permutation group.*

Proof: For every $g \in G$ define the map $L_g : G \to G$ to be left multiplication by g,

$$L_g(x) = gx \quad \text{where} \quad x \in G.$$

This map is one-to-one and onto since

$$gx = gx' \Longrightarrow x = x' \quad \text{and} \quad x = L_g(g^{-1}x) \qquad \text{for all } x \in G.$$

The map L_g therefore permutes the elements of $G = \{g_1 = e, g_2, \dots, g_n\}$ and may be identified with a member of S_n. It has the property $L_g \circ L_h = L_{gh}$, since

$$L_g \circ L_h(x) = g(hx) = (gh)x = L_{gh}(x), \quad \forall x \in G.$$

Hence the map $\varphi : G \to S_n$ defined by $\varphi(g) = L_g$ is a homomorphism,

$$\varphi(g)\varphi(h) = L_g \circ L_h = L_{gh} = \varphi(gh).$$

Furthermore, φ is one-to-one, for if $\varphi(g) = \varphi(h)$ then $g = L_g(e) = L_h(e) = h$. Thus G is isomorphic to the subgroup of $\varphi(G) \subseteq S_n$. ■

From the abstract point of view there is nothing to distinguish two isomorphic groups, but different 'concrete' versions of the same group may have different applications. The particular concretization as linear groups of transformations or matrix groups is known as *group representation theory* and plays a major part in mathematical physics.

Automorphisms and conjugacy classes

An **automorphism** is an isomorphism $\varphi : G \to G$ of a group onto itself. A trivial example is the identity map $\mathrm{id}_G : G \to G$. Since the composition of any pair of automorphisms is an automorphism and the inverse of any automorphism φ^{-1} is an automorphism, it follows that the set of all automorphisms of a group G is itself a group, denoted Aut(G).

If g is an arbitrary element of G, the map $C_g : G \to G$ defined by

$$C_g(a) = gag^{-1} \tag{2.14}$$

is called **conjugation** by the element g. This map is a homomorphism, for

$$C_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = C_g(a)C_g(b),$$

and $C_{g^{-1}}$ is its inverse since

$$C_{g^{-1}} \circ C_g(a) = g^{-1}(gag^{-1})g = a, \quad \forall a \in G.$$

Hence every conjugation C_g is an automorphism of G. Automorphisms that are a conjugation by some element g of G are called **inner automorphisms**. The identity $C_{gh} = C_g \circ C_h$ holds, since for any $a \in G$

$$C_gh(a) = gha(gh)^{-1} = ghah^{-1}g^{-1} = C_g(C_h(a)).$$

Hence the map $\psi : G \to \text{Aut}(G)$, defined by $\psi(g) = C_g$, is a homomorphism. The inner automorphisms, being the image of G under ψ, form a subgroup of Aut(G). Two subgroups H and H' of G that can be transformed to each other by an inner automorphism of G are called **conjugate subgroups**. In this case there exists an element $g \in G$ such that

$$H' = gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Exercise: Show that conjugacy is an equivalence relation on the set of all subgroups of a group G. What is the equivalence class containing the trivial subgroup $\{e\}$?

Conjugation also induces an equivalence relation on the original group G by $a \equiv b$ if and only if there exists $g \in G$ such that $b = C_g(a)$. The three requirements for an equivalence relation are easily verified: (i) reflexivity, $a = C_e(a)$ for all $a \in G$; (ii) symmetry, if $b = C_g(a)$ then $a = C_{g^{-1}}(b)$; (iii) transitivity, if $b = C_g(a)$ and $c = C_h(b)$ then $c = C_{hg}(a)$. The equivalence classes with respect to this relation are called **conjugacy classes**. The conjugacy class of an element $a \in G$ is denoted G_a. For example, the conjugacy class of the identity is always the singleton $G_e = \{e\}$, since $C_ge = geg^{-1} = e$ for all $g \in G$.

Exercise: What are the conjugacy classes of an abelian group?

Example 2.18 For a matrix group, matrices A and B in the same conjugacy class are related by a **similarity transformation**

$$\mathsf{B} = \mathsf{S}\mathsf{A}\mathsf{S}^{-1}.$$

Matrices related by a similarity transformation have identical invariants such as determinant, trace (sum of the diagonal elements) and eigenvalues. To show determinant is an invariant use Eq. (2.5),

$$\det \mathsf{B} = \det \mathsf{S} \det \mathsf{A} (\det \mathsf{S})^{-1} = \det \mathsf{A}.$$

For the invariance of trace we need the identity

$$\operatorname{tr}(\mathsf{AB}) = \operatorname{tr}(\mathsf{BA}), \tag{2.15}$$

which is proved by setting $\mathsf{A} = [a_{ij}]$ and $\mathsf{B} = [b_{ij}]$ and using the multiplication law of matrices,

$$\operatorname{tr}(\mathsf{AB}) = \sum_{i=1}^{n}\Big(\sum_{j=1}^{n} a_{ij}b_{ji}\Big) = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} b_{ji}a_{ij}\Big) = \operatorname{tr}(\mathsf{BA}).$$

Hence

$$\operatorname{tr}\mathsf{B} = \operatorname{tr}(\mathsf{SAS}^{-1}) = \operatorname{tr}(\mathsf{S}^{-1}\mathsf{SA}) = \operatorname{tr}(\mathsf{IA}) = \operatorname{tr}\mathsf{A},$$

as required. Finally, if λ is an eigenvalue of A corresponding to eigenvector $\mathbf{v}$, then $\mathsf{S}\mathbf{v}$ is an eigenvector of B with the same eigenvalue,

$$\mathsf{A}\mathbf{v} = \lambda\mathbf{v} \implies \mathsf{B}(\mathsf{S}\mathbf{v}) = \mathsf{SAS}^{-1}\mathsf{S}\mathbf{v} = \mathsf{SA}\mathbf{v} = \lambda\mathsf{S}\mathbf{v}.$$

Example 2.19 The conjugacy classes of the permutation group S_3 are, in cyclic notation,

$$\{e\}; \quad \{(1\,2),\ (1\,3),\ (2\,3)\}; \quad \text{and} \quad \{(1\,2\,3),\ (1\,3\,2)\}.$$

These are easily checked by noting that $(1\,2)^{-1}(1\,2\,3)(1\,2) = (1\,3\,2)$ and

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3), \text{ etc.}$$

It is a general feature of permutation groups that conjugacy classes consist of permutations having identical cycle structure (see Problem 2.11).

Problems

Problem 2.9 Show that Theorem 2.2 may be extended to infinite groups as well. That is, any group G is isomorphic to a subgroup of Transf(G), the transformation group of the set G.

Problem 2.10 Find the group multiplication tables for all possible groups on four symbols e, a, b and c, and show that any group of order 4 is either isomorphic to the cyclic group $\mathbb{Z}_4$ or the product group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Problem 2.11 Show that every cyclic permutation $(a_1\, a_2 \ldots a_n)$ has the property that for any permutation π,

$$\pi(a_1\, a_2 \ldots a_n)\pi^{-1}$$

is also a cycle of length n. [*Hint*: It is only necessary to show this for interchanges $\pi = (b_1\, b_2)$ as every permutation is a product of such interchanges.]

(a) Show that the conjugacy classes of S_n consist of those permutations having the same cycle structure, e.g. $(1\,2\,3)(4\,5)$ and $(1\,4\,6)(2\,3)$ belong to the same conjugacy class.
(b) Write out all conjugacy classes of S_4 and calculate the number of elements in each class.

Problem 2.12 Show that the class of groups as objects with homomorphisms between groups as morphisms forms a category – the *category of groups* (see Section 1.7). What are the monomorphisms, epimorphisms and isomorphisms of this category?

2.5 Normal subgroups and factor groups

Cosets

For any pair of subsets A and B of a group G, define AB to be the set

$$AB = \{ab \mid a \in A \text{ and } b \in B\}.$$

If H is a subgroup of G then $HH = H$.

When A is a singleton set, say $A = \{a\}$, we usually write aB instead of $\{a\}B$. If H is a subgroup of G, then each subset aH where $a \in G$ is called a **(left) coset of** H. Two cosets of a given subgroup H are either identical or non-intersecting. For, suppose there exists an element $g \in aH \cap bH$. Setting

$$g = ah_1 = bh_2 \quad (h_1, h_2 \in H)$$

we have for any $h \in H$

$$ah = bh_2 h_1^{-1} h \in bH,$$

so that $aH \subseteq bH$. Equally, it can be argued that $bH \subseteq aH$, whence either $aH \cap bH = \emptyset$ or $aH = bH$. Since $g = ge$ and $e \in H$, any element $g \in G$ always belongs to the coset gH. Thus the cosets of H form a family of disjoint subsets covering all of G. There is an alternative way of demonstrating this partitioning property. The relation $a \equiv b$ on G, defined by

$$a \equiv b \quad \text{iff} \quad b^{-1}a \in H,$$

is an equivalence relation since it is (i) reflexive, $a^{-1}a = e \in H$; (ii) symmetric, $a^{-1}b = (b^{-1}a)^{-1} \in H$ if $b^{-1}a \in H$; and (iii) transitive, $a^{-1}b \in H$, $b^{-1}c \in H$ implies $a^{-1}c = a^{-1}bb^{-1}c \in H$. The equivalence classes defined by this relation are precisely the left cosets of the subgroup H, for $b \equiv a$ if and only if $b \in aH$.

Theorem 2.3 (Lagrange) *If G is a finite group of order n, then the order of every subgroup H is a divisor of n.*

Proof: Every coset gH is in one-to-one correspondence with H, for if $gh_1 = gh_2$ then $h_1 = g^{-1}gh_2 = h_2$. Hence every coset gH must have exactly $|H|$ elements, and since the cosets partition the group G it follows that n is a multiple of $|H|$. ■

Corollary 2.4 *The order of any element is a divisor of $|G|$.*

Proof: Let g be any element of G and let m be its order. As shown in Example 2.5 the elements $\{g, g^2, \dots, g^m = e\}$ are then all unequal to each other and form a cyclic subgroup of order m. By Lagrange's theorem m divides the order of the group, $|G|$. ■

Exercise: If G has prime order p all subgroups are trivial – they are either the identity subgroup $\{e\}$ or G itself. Show that G is a cyclic group.

Normal subgroups

The **right cosets** Hg of a subgroup H are defined in a completely analogous way to the left cosets. While in general there is no obvious relationship between right and left cosets, there is an important class of subgroups for which they coincide. A subgroup N of a group G is called **normal** if

$$gNg^{-1} = N, \quad \forall g \in G.$$

Such subgroups are invariant under inner automorphisms; they are sometimes referred to as **invariant** or **self-conjugate** subgroups. The key feature of normal subgroups is that the systems of left and right cosets are identical, for

$$gN = gNg^{-1}g = Ng, \quad \forall g \in G.$$

This argument may give the misleading impression that every element of N commutes with every element of G, but what it actually demonstrates is that for every $n \in N$ and every $g \in G$ there exists an element $n' \in N$ such that $gn = n'g$. There is no reason, in general, to expect that $n' = n$.

For any group G the trivial subgroups $\{e\}$ and G are always normal. A group is called **simple** if it has no normal subgroups other than these trivial subgroups.

Example 2.20 The **centre** Z of a group G is defined as the set of elements that commute with all elements of G,

$$Z = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

This set forms a subgroup of G since the three essential requirements hold:

Closure: if $z, z' \in Z$ then $zz' \in Z$ since

$$(zz')g = z(z'g) = z(gz') = (zg)z' = (gz)z' = g(zz').$$

Identity: $e \in Z$, as $eg = ge = g$ for all $g \in G$.

Inverse: if $z \in Z$ then $z^{-1} \in Z$ since

$$z^{-1}g = z^{-1}ge = z^{-1}gzz^{-1} = z^{-1}zgz^{-1} = gz^{-1}.$$

This subgroup is clearly normal since $gZ = Zg$ for all $g \in G$.

Factor groups

When we multiply left cosets of a subgroup H together, for example

$$gHg'H = \{ghg'h' \mid h, h' \in H\},$$

the result is not in general another coset. On the other hand, the product of cosets of a *normal* subgroup N is always another coset,

$$gNg'N = gg'NN = (gg')N,$$

and satisfies the associative law,

$$(gNg'N)g''N = (gg'g'')N = gN(g'Ng''N).$$

Furthermore, the coset $eN = N$ plays the role of an identity element, while every coset has an inverse $(gN)^{-1} = g^{-1}N$. Hence the cosets of a *normal* subgroup N form a group called the **factor group** of G by N, denoted G/N.

Example 2.21 The even integers $2\mathbb{Z}$ form a normal subgroup of the additive group of integers $\mathbb{Z}$, since this is an abelian group. The factor group $\mathbb{Z}/2\mathbb{Z}$ has just two cosets $[0] = 0 + 2\mathbb{Z}$ and $[1] = 1 + 2\mathbb{Z}$, and is isomorphic to the additive group of integers modulo 2, denoted by $\mathbb{Z}_2$ (see Example 2.4).

Kernel of a homomorphism

Let $\varphi : G \to G'$ be a homomorphism between two groups G and G'. The **kernel** of φ, denoted $\ker(\varphi)$, is the subset of G consisting of those elements that map onto the identity e' of G',

$$\ker(\varphi) = \varphi^{-1}(e') = \{k \in G \mid \varphi(k) = e'\}.$$

The kernel $K = \ker(\varphi)$ of any homomorphism φ is a subgroup of G:

Closure: if k_1 and k_2 belong to K then so does k_1k_2, since

$$\varphi(k_1k_2) = \varphi(k_1)\varphi(k_2) = e'e' = e'.$$

Identity: $e \in K$ as $\varphi(e) = e'$.
Inverse: if $k \in K$ then $k^{-1} \in K$, for

$$\varphi(k^{-1}) = (\varphi(k))^{-1} = (e')^{-1} = e'.$$

Furthermore, K is a normal subgroup since, for all $k \in K$ and $g \in G$,

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e'(\varphi(g))^{-1} = e'.$$

The following theorem will show that the converse of this result also holds, namely that *every* normal subgroup is the kernel of a homomorphism.

Theorem 2.5 *Let G be a group. Then the following two properties hold:*

1. *If N is a normal subgroup of G then there is a homomorphism $\mu : G \to G/N$.*
2. *If $\varphi : G \to G'$ is a homomorphism then the factor group $G/\ker(\varphi)$ is isomorphic with the image subgroup $\mathrm{im}(\varphi) \subseteq G'$ defined in Eq. (2.13),*

$$\mathrm{im}(\varphi) \cong G/\ker(\varphi).$$

Proof: 1. The map $\mu : G \to G/N$ defined by $\mu(g) = gN$ is a homomorphism, since

$$\mu(g)\mu(h) = gNhN = ghNN = ghN = \mu(gh).$$

2. Let $K = \ker(\varphi)$ and $H' = \mathrm{im}(\varphi)$. The map φ is constant on each coset gK, for

$$k \in K \quad \Longrightarrow \quad \varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)e' = \varphi(g).$$

Hence the map φ defines a map $\psi : G/K \to H'$ by setting

$$\psi(gK) = \varphi(g),$$

and this map is a homomorphism since

$$\psi(gKhK) = \psi(ghK) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(gK)\psi(hK).$$

Furthermore ψ is one-to-one, for

$$\begin{aligned} \psi(gK) = \psi(hK) &\Longrightarrow \varphi(g) = \varphi(h) \\ &\Longrightarrow \varphi(gh^{-1}) = \varphi(g)(\varphi(h))^{-1} = e' \\ &\Longrightarrow gh^{-1} \in K \\ &\Longrightarrow g \in hK. \end{aligned}$$

Since every element h' of the image set H' is of the form $h' = \varphi(g) = \psi(gK)$, the map ψ is an isomorphism between the groups G/K and H'. ■

Example 2.22 Let G and H be two groups with respective identity elements e_G and e_H. A law of composition can be defined on the cartesian product $G \times H$ by

$$(g, h)(g', h') = (gg', hh').$$

This product clearly satisfies the associative law and has identity element (e_G, e_H). Furthermore, every element has a unique inverse $(g, h)^{-1} = (g^{-1}, h^{-1})$. Hence, with this law of composition, $G \times H$ is a group called the **direct product** of G and H. The group G is clearly isomorphic to the subgroup $(G, e_H) = \{(g, e_H) \mid g \in G\}$. The latter is a normal subgroup, since

$$(a, b)(G, e_H)(a^{-1}, b^{-1}) = (aGa^{-1}, be_Hb^{-1}) = (G, e_H).$$

It is common to *identify* the subgroup of elements (G, e_H) with the group G. In a similar way H is identified with the normal subgroup (e_G, H).

Problems

Problem 2.13 (a) Show that if H and K are subgroups of G then their intersection $H \cap K$ is always a subgroup of G.
(b) Show that the product $HK = \{hk \mid h \in H,\ k \in K\}$ is a subgroup if and only if $HK = KH$.

Problem 2.14 Find all the normal subgroups of the group of symmetries of the square D_4 described in Example 2.7.

Problem 2.15 The *quaternion group* G consists of eight elements denoted

$$\{1,\ -1,\ i,\ -i,\ j,\ -j,\ k,\ -k\},$$

subject to the following law of composition:

$$\begin{gathered}1g = g1 = g, \text{ for all } g \in Q,\\ -1g = -g, \text{ for } g = i,\ j,\ k,\\ i^2 = j^2 = k^2 = -1,\\ ij = k,\ jk = i,\ ki = j.\end{gathered}$$

(a) Write down the full multiplication table for Q, justifying all products not included in the above list.
(b) Find all subgroups of Q and show that all subgroups of Q are normal.
(c) Show that the subgroup consisting of $\{1,\ -1,\ i,\ -i\}$ is the kernel of a homomorphism $Q \to \{1,\ -1\}$.
(d) Find a subgroup H of S_4, the symmetric group of order 4, such that there is a homomorphism $Q \to H$ whose kernel is the subgroup $\{1,\ -1\}$.

Problem 2.16 A *Möbius transformation* is a complex map,

$$z \mapsto z' = \frac{az+b}{cz+d} \quad \text{where} \quad a, b, c, d \in \mathbb{C}, ad - bc = 1.$$

(a) Show that these are one-to-one and onto transformations of the extended complex plane, which includes the point $z = \infty$, and write out the composition of an arbitrary pair of transformations given by constants (a, b, c, d) and (a', b', c', d').
(b) Show that they form a group, called the *Möbius group*.
(c) Show that the map μ from $SL(2, \mathbb{C})$ to the Möbius group, which takes the unimodular matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the above Möbius transformation, is a homomorphism, and that the kernel of this homomorphism is $\{\mathsf{I}, -\mathsf{I}\}$; i.e. the Möbius group is isomorphic to $SL(2, \mathbb{C})/\mathbb{Z}_2$.

Problem 2.17 Assuming the identification of G with (G, e_H) and H with (e_G, H), show that $G \cong (G \times H)/H$ and $H \cong (G \times H)/G$.

Problem 2.18 Show that the conjugacy classes of the direct product $G \times H$ of two groups G and H consist precisely of products of conjugacy classes from the groups

$$(C_i, D_j) = \{(g_i, h_j) \mid g_i \in C_i,\ h_j \in D_j\}$$

where C_i is a conjugacy class of G and D_j a conjugacy class of H.

2.6 Group actions

A **left action** of a group G on a set X is a homomorphism φ of G into the group of transformations of X,

$$\varphi : G \to \text{Transf}(X).$$

It is common to write $\varphi(g)(x)$ simply as gx, a notation that makes it possible to write ghx in place of $(gh)x$, since

$$(gh)x = \varphi(gh)(x) = \varphi(g)\varphi(h)(x) = \varphi(g)(hx) = g(hx).$$

A left action ϕ of G on $\mathbb{R}^n$ all of whose images are linear transformations is a homomorphism

$$\phi : G \to GL(n, \mathbb{R}),$$

and is called an **n-dimensional representation** of G. Similarly, a homomorphism $\phi : G \to GL(n, \mathbb{C})$ is called a **complex n-dimensional representation** of G.

An **anti-homomorphism** is defined as a map $\rho : G \to \text{Transf}(X)$ with the property

$$\rho(gh) = \rho(h)\rho(g).$$

It can give rise to a **right action** $xg = \rho(g)(x)$, a notation that is consistent with writing xgh in place of $x(gh) = (xg)h$.

Exercise: If $\varphi : G \to H$ is a homomorphism show that the map $\rho : G \to H$ defined by $\rho(g) = \varphi(g^{-1})$ is an anti-homomorphism.

Let G be a group having a left action on X. The **orbit** Gx of a point $x \in X$ is the set of all points that can be reached from x by this action,

$$Gx = \{gx \mid g \in G\}.$$

We say the action of G on X is **transitive** if the whole of X is the orbit of some point in X,

$$\exists x \in X \quad \text{such that} \quad X = Gx.$$

In this case any pair of elements $y, z \in X$ can be connected by the action of a group element, for if $y = gx$ and $z = hx$ then $z = g'y$ where $g' = hg^{-1}$. Hence $X = Gy$ for all $y \in X$.

If x is any point of X, define the **isotropy group** of x to be

$$G_x = \{g \mid gx = x\}.$$

If $gx = x \Longrightarrow g = \text{id}_X$ the action of G on X is said to be **free**. In this case the isotropy group is trivial, $G_x = \{\text{id}_X\}$, for every point $x \in X$.

Exercise: Show that G_x forms a subgroup of G.

If $x \in X$ and $h, h' \in G$ then

$$hx = h'x \Longrightarrow h^{-1}h' \in G_x \Longrightarrow h' \in hG_x.$$

If G is a finite group, we denote the number of points in any subset S by $|S|$. Since hG_x is a left coset of the subgroup G_x and from the proof of Lagrange's theorem 2.3 all cosets have the same number of elements, there must be precisely $|G_x|$ group elements that map x to any point y of its orbit Gx. Hence

$$|G| = |Gx|\,|G_x|. \tag{2.16}$$

Example 2.23 The cyclic group of order 2, $\mathbb{Z}_2 = \{e, a\}$ where $a^2 = e$, acts on the real numbers $\mathbb{R}$ by

$$ex = x, \qquad ax = -x.$$

The orbit of any point $x \neq 0$ is $\mathbb{Z}_2 x = \{x, -x\}$, while $\mathbb{Z}_2 0 = \{0\}$. This action is not transitive. The isotropy group of the origin is the whole of $\mathbb{Z}_2$, while for any other point it is $\{e\}$. It is a simple matter to check (2.16) separately for $x = 0$ and $x \neq 0$.

Example 2.24 The additive group of reals $\mathbb{R}$ acts on the complex plane $\mathbb{C}$ by

$$\theta : z \mapsto z e^{i\theta}.$$

The orbit of any $z \neq 0$ is the circle centred 0, radius $r = |z|$. The action is not transitive since circles of different radius are disjoint. The isotropy group of any $z \neq 0$ is the set of real numbers of the form $\theta = 2\pi n$ where $n \in \mathbb{Z}$. Hence the isotropy group $\mathbb{R}_z$ for $z \neq 0$ is isomorphic to $\mathbb{Z}$, the additive group of integers. On the other hand the isotropy group of $z = 0$ is all of $\mathbb{R}$.

Example 2.25 A group G acts on itself by **left translation**

$$g : h \mapsto L_g h = gh.$$

This action is clearly transitive since any element g' can be reached from any other g by a left translation,

$$g' = L_{g'g^{-1}} g.$$

Any subgroup $H \subseteq G$ also acts on G by left translation. The orbit of any group element g under this action is the *right coset* Hg containing g. Similarly, under the right action of H on G defined by **right translation** $R_h : g \mapsto gh$, the orbits are the *left cosets* gH. These actions are not transitive in general.

Example 2.26 The process of conjugation by an element g, defined in Eq. (2.14), is a left action of the group G on itself since the map $g \mapsto C_g$ is a homomorphism,

$$C_{gh} a = (gh)a(gh)^{-1} = gha h^{-1} g^{-1} = C_g C_h a,$$

where we have written $C_g a$ for $C_g(a)$. The orbits under the action of conjugation are precisely the *conjugacy classes*. By Eq. (2.16) it follows that if G is a finite group then the number of elements in any conjugacy class, being an orbit under an action of G, is a divisor of the order of the group $|G|$.

If G has a left action on a set X and if x and y are any pair of points in X in the same orbit, such that $y = hx$ for some $h \in G$, then their isotropy groups are conjugate to each other,

$$G_y = G_{hx} = h G_x h^{-1}. \tag{2.17}$$

For, let $g \in G_y$, so that $gy = y$. Since $y = hx$ it follows on applying h^{-1} that $h^{-1} g h x = x$. Hence $h^{-1} g h \in G_x$, or equivalently $g \in h G_x h^{-1}$. The converse, that $h G_x h^{-1} \subseteq G_y$, is straightforward: for any $g \in h G_x h^{-1}$, we have that

$$gy = ghx = hg' h^{-1} hx \quad \text{where} \quad g' \in G_x,$$

whence $gy = hx = y$ and $g \in G_y$. Thus the isotropy groups of x and y are isomorphic since they are conjugate to each other, and are related by an inner automorphism. If the action of G on X is transitive it follows that the isotropy groups of any pair of points x and y are isomorphic to each other.

Exercise: Under what circumstances is the action of conjugation by an element g on a group G transitive?

Problem

Problem 2.19 If H is any subgroup of a group G define the action of G on the set of left cosets G/H by $g : g'H \mapsto gg'H$.

(a) Show that this is always a transitive action of H on G.
(b) Let G have a transitive left action on a set X, and set $H = G_x$ to be the isotropy group of any point x. Show that the map $i : G/H \to X$ defined by $i(gH) = gx$ is well-defined, one-to-one and onto.
(c) Show that the left action of G on X can be identified with the action of G on G/H defined in (a).
(d) Show that the group of proper orthogonal transformations $SO(3)$ acts transitively on the 2-sphere S^2,

$$S^2 = \{(x, y, z) \,|\, r^2 = x^2 + y^2 + z^2 = 1\} = \{\mathbf{r} \,|\, r^2 = \mathbf{r}^T\mathbf{r} = 1\},$$

where $\mathbf{r}$ is a column vector having real components $x,\ y,\ z$. Show that the isotropy group of any point $\mathbf{r}$ is isomorphic to $SO(2)$, and find a bijective correspondence between the factor space $SO(3)/SO(2)$ and the 2-sphere S^2 such that $SO(3)$ has identical left action on these two spaces.

2.7 Symmetry groups

For physicists, the real interest in groups lies in their connection with the symmetries of a space of interest or some important function such as the Lagrangian. Here the concept of a *space* X will be taken in its broadest terms to mean a set X with a 'structure' imposed on it, as discussed in Section 1.6. The definitions of such spaces may involve combinations of algebraic and geometric structures, but the key thing is that their definitions invariably involve the specification of certain functions on the space. For example, algebraic structures such as groups require laws of composition, which are functions defined on cartesian products of the underlying sets. Geometric structures such as topology usually involve a selection of subsets of X – this can also be defined as a characteristic function on the power set of X. For the present purposes let us simply regard a *space* as being a set X together with one or more functions $F : X \to Y$ to another set Y defined on it. This concept will be general enough to encapsulate the basic idea of a 'space'.

If F is a Y-valued function on X, we say a transformation $g : X \to X$ leaves F **invariant** if

$$F(x) = F(gx) \qquad \text{for all } x \in X,$$

where, as in Section 2.6, we denote the left action by $gx \equiv g(x)$.

Theorem 2.6 *The set of all transformations of X leaving F invariant form a group.*

Proof: We show the usual three things:

Closure: if g and h leave F invariant then $F(x) = F(hx)$ for all $x \in X$ and $F(y) = F(gy)$ for all $y \in X$. Hence $gh \equiv g \circ h$ leaves F invariant since $F(ghx) = F(g(hx)) = F(hx) = F(x)$.
Identity: obviously $F(x) = F(\mathrm{id}_X(x))$; that is, id_X leaves F invariant.
Inverse: if g is a transformation then there exists an inverse map g^{-1} such that $gg^{-1} = \mathrm{id}_X$. The map g^{-1} leaves F invariant if g does, since

$$F(g^{-1}x) = F(g(g^{-1}x)) = F(x).$$

■

It is a straightforward matter to extend the above theorem to an arbitrary set $\mathcal{F}$ of functions on X. The group of transformations leaving all functions $F \in \mathcal{F}$ invariant will be called the **invariance group** or **symmetry group** of $\mathcal{F}$. The following are some important examples of symmetry groups in mathematical physics.

Example 2.27 The rotation group $SO(3)$. As in Example 2.11, let $\mathbb{R}^3$ be the set of all 3×1 column vectors

$$\mathbf{r} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad \text{such that} \quad x,\ y,\ z \in \mathbb{R}.$$

Consider the set of all linear transformations $\mathbf{r} \mapsto \mathbf{r}' = \mathsf{A}\mathbf{r}$ on $\mathbb{R}^3$, where A is a 3×3 matrix, which leave the distance of points from the origin $r = |\mathbf{r}| = \sqrt{x^2 + y^2 + z^2}$ invariant. Since $r^2 = \mathbf{r}^T\mathbf{r}$, we have

$$r'^2 = \mathbf{r}'^T\mathbf{r}' = \mathbf{r}^T\mathsf{A}^T\mathsf{A}\mathbf{r} = r^2 = \mathbf{r}^T\mathbf{r},$$

which holds for *arbitrary* vectors $\mathbf{r}$ if and only if A is an orthogonal matrix, $\mathsf{A}\mathsf{A}^T = \mathsf{I}$. As shown in Example 2.11, orthogonal transformations all have determinant ±1. Those with determinant $+1$ are called **rotations**, while transformations of determinant -1 must involve a reflection with respect to some plane; for example, the transformation $x' = x,\ y' = y,\ z' = -z$.

In a similar manner $O(n)$ is the group of symmetries of the distance function in n-dimensions,

$$r = \sqrt{x_1^2 + x_2^2 + \dots + x_n^2}$$

and those with positive determinant are denoted $SO(n)$, called the **group of rotations in n-dimensions**. There is no loss of generality in our assumption of *linear* transformations for this group since it can be shown that any transformation of $\mathbb{R}^n$ leaving r^2 invariant must be linear (see Chapter 18).

Example 2.28 The Euclidean group. The **Euclidean space** $\mathbb{E}^3$ is defined as the cartesian space $\mathbb{R}^3$ with a distance function between any pair of points given by

$$\Delta s^2 = (\mathbf{r}_2 - \mathbf{r}_1)^2 = \Delta\mathbf{r}^T\Delta\mathbf{r}.$$

A transformation of $\mathbb{E}^3$ that leaves the distance between any pair of points invariant will be called a **Euclidean transformation**. As for the rotation group, a Euclidean transformation $\mathbf{r} \to \mathbf{r}'$ has

$$\Delta\mathbf{r}' = \mathsf{A}\Delta\mathbf{r}, \qquad \mathsf{A}\mathsf{A}^T = \mathsf{I}.$$

For any pair of points $\mathbf{r}'_2 - \mathbf{r}'_1 = \mathsf{A}(\mathbf{r}_2 - \mathbf{r}_1)$, and if we set $\mathbf{r}_1 = \mathbf{0}$ to be the origin and $\mathbf{0}' = \mathbf{a}$, then $\mathbf{r}'_2 - \mathbf{a} = \mathsf{A}\mathbf{r}_2$. Since $\mathbf{r}_2$ is an arbitrary point in $\mathbb{E}^3$, the general Euclidean transformations have the form

$$\mathbf{r}' = \mathsf{A}\mathbf{r} + \mathbf{a} \quad \text{where} \quad \mathsf{A}^T\mathsf{A} = \mathsf{I}, \mathbf{a} = \text{const.} \tag{2.18}$$

Transformations of this form are frequently called **affine** or **inhomogeneous linear** transformations.

Exercise: Check directly that these transformations form a group – do not use Theorem 2.6.

The group of Euclidean transformations, called the **Euclidean group**, can also be written as a matrix group by replacing $\mathbf{r}$ with the 4×1 column matrix $(x, y, z, 1)^T$ and writing

$$\begin{pmatrix} \mathbf{r}' \\ 1 \end{pmatrix} = \begin{pmatrix} \mathsf{A} & \mathbf{a} \\ \mathbf{0}^T & 1 \end{pmatrix} \begin{pmatrix} \mathbf{r} \\ 1 \end{pmatrix} = \begin{pmatrix} A\mathbf{r} + \mathbf{a} \\ 1 \end{pmatrix}.$$

This may seem an odd trick, but its value lies in demonstrating that the Euclidean group is isomorphic to a matrix group – the Euclidean transformations are affine, not linear, on $\mathbb{R}^3$, and thus cannot be written as 3×3 matrices.

Example 2.29 The Galilean group. To find the set of transformations of space and time that preserve the laws of Newtonian mechanics we follow the lead of special relativity (see Chapter 9) and define an **event** to be a point of $\mathbb{R}^4$ characterized by four coordinates (x, y, z, t). Define **Galilean space** $\mathbb{G}^4$ to be the space of events with a structure consisting of three elements:

1. Time intervals $\Delta t = t_2 - t_1$.
2. The spatial distance $\Delta s = |\mathbf{r}_2 - \mathbf{r}_1|$ between any pair of **simultaneous events** (events having the same time coordinate, $t_1 = t_2$).
3. Motions of inertial (free) particles, otherwise known as **rectilinear motions**,

$$\mathbf{r}(t) = \mathbf{u}t + \mathbf{r}_0, \tag{2.19}$$

where $\mathbf{u}$ and $\mathbf{r}_0$ are arbitrary constant vectors.

Note that only the distance between *simultaneous* events is relevant. A simple example should make this clear. Consider a train travelling with uniform velocity v between two stations A and B. In the frame of an observer who stays at A the distance between the (non-simultaneous) events $E_1 =$ 'train leaving A' and $E_2 =$ 'train arriving at B' is clearly $d = vt$, where t is the time of the journey. However, in the rest frame of the train it hasn't moved at all and the distance between these two events is zero! Assuming no accelerations at the start and end of the journey, both frames are equally valid Galilean frames of reference.

Note that Δt is a function on all of $\mathbb{G}^4 \times \mathbb{G}^4$, while Δs is a function on the subset of $\mathbb{G}^4 \times \mathbb{G}^4$ consisting of simultaneous pairs of events, $\{((\mathbf{r}, t), (\mathbf{r}', t')) \mid \Delta t = t' - t = 0\}$. We define a **Galilean transformation** as a transformation $\varphi : \mathbb{G}^4 \to \mathbb{G}^4$ that preserves the three given structural elements. All Galilean transformations have the form

$$t' = t + a \quad (a = \text{const}), \tag{2.20}$$

$$\mathbf{r}' = \mathsf{A}\mathbf{r} - \mathbf{v}t + \mathbf{b} \quad (\mathsf{A}^T\mathsf{A} = \mathsf{I}, \mathbf{v},\ \mathbf{b} = \text{consts}). \tag{2.21}$$

Proof: From the time difference equation $t' - 0' = t - 0$ we obtain (2.20) where $a = 0'$. Invariance of Property 2. gives, by a similar argument to that used to deduce Euclidean transformations,

$$\mathbf{r}' = \mathsf{A}(t)\mathbf{r} + \mathbf{a}(t), \qquad \mathsf{A}^T\mathsf{A} = \mathsf{I} \tag{2.22}$$

where $\mathsf{A}(t)$ is a time-dependent orthogonal matrix and $\mathbf{a}(t)$ is an arbitrary vector function of time. These transformations allow for rotating and accelerating frames of reference and are certainly too general to preserve Newton's laws.

Property 3. is essentially the invariance of Newton's first law of motion, or equivalently Galileo's principle of inertia. Consider a particle in uniform motion given by Eq. (2.19). This equation must be transformed into an equation of the form $\mathbf{r}'(t) = \mathbf{u}'t + \mathbf{r}'_0$ under a Galilean transformation. From the transformation law (2.22)

$$\mathbf{u}'t + \mathbf{r}'_0 = \mathsf{A}(t)(\mathbf{u}t + \mathbf{r}_0) + \mathbf{a}(t),$$

and taking twice time derivatives of both sides of this equation gives

$$0 = (\ddot{\mathsf{A}}t + 2\dot{\mathsf{A}})\mathbf{u} + \ddot{\mathsf{A}}\mathbf{r}_0 + \ddot{\mathbf{a}}.$$

Since $\mathbf{u}$ and $\mathbf{r}_0$ are arbitrary constant vectors it follows that

$$0 = \ddot{\mathsf{A}}, \quad 0 = \ddot{\mathsf{A}}t + 2\dot{\mathsf{A}} \quad \text{and} \quad 0 = \ddot{\mathbf{a}}.$$

Hence $\dot{\mathsf{A}} = 0$, so that A is a constant orthogonal matrix, and $\mathbf{a} = -\mathbf{v}t + \mathbf{b}$ for some constant vectors $\mathbf{v}$ and $\mathbf{b}$. ■

Exercise: Exhibit the Galilean group as a matrix group, as was done for the Euclidean group in (2.18).

Example 2.30 The Lorentz group. The Galilean transformations do not preserve the *light cone* at the origin

$$\Delta x^2 + \Delta y^2 + \Delta z^2 = c^2\Delta t^2 \quad (\Delta x = x_2 - x_1,\ \text{etc.}).$$

The correct transformations that achieve this important property preserve the metric of **Minkowski space**,

$$\begin{aligned}\Delta s^2 &= \Delta x^2 + \Delta y^2 + \Delta z^2 - c^2\Delta t^2 \\ &= \Delta\mathbf{x}^T\mathsf{G}\Delta\mathbf{x},\end{aligned}$$

where

$$\mathbf{x} = \begin{pmatrix} x \\ y \\ z \\ ct \end{pmatrix}, \quad \Delta\mathbf{x} = \begin{pmatrix} \Delta x \\ \Delta y \\ \Delta z \\ c\Delta t \end{pmatrix} \quad \text{and} \quad \mathsf{G} = [g_{\mu\nu}] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

The transformations in question must have the form

$$\mathbf{x}' = \mathsf{L}\mathbf{x} + \mathbf{a},$$

and the invariance law $\Delta s'^2 = \Delta s^2$ implies

$$\Delta\mathbf{x}'^T \mathsf{G} \Delta\mathbf{x}' = \Delta\mathbf{x}^T \mathsf{L}^T \mathsf{G} \mathsf{L} \Delta\mathbf{x} = \Delta\mathbf{x}^T \mathsf{G} \Delta\mathbf{x}.$$

Since this equation holds for arbitrary $\Delta\mathbf{x}$, the 4×4 matrix L must satisfy the equation

$$\mathsf{G} = \mathsf{L}^T \mathsf{G} \mathsf{L}\,. \tag{2.23}$$

The *linear* transformations, having $\mathbf{a} = 0$, are called **Lorentz transformations** while the general transformations with arbitrary **a** are called **Poincaré transformations**. The corresponding groups are called the **Lorentz group** and **Poincaré group**, respectively. The essence of the special theory of relativity is that all laws of physics are Poincaré invariant.

Problems

Problem 2.20 The *projective transformations* of the line are defined by

$$x' = \frac{ax + b}{cx + d} \quad \text{where} \quad ad - bc = 1.$$

Show that projective transformations preserve the cross-ratio

$$\frac{(x_1 - x_2)(x_3 - x_4)}{(x_3 - x_2)(x_1 - x_4)}$$

between any four points x_1, x_2, x_3 and x_4. Is every analytic transformation that preserves the cross-ratio between any four points on the line necessarily a projective transformation? Do the projective transformations form a group?

Problem 2.21 Show that a matrix U is unitary, satisfying Eq. (2.12), if and only if it preserves the 'norm'

$$\|\mathbf{z}\|^2 = \sum_{i=1}^{n} z_i \bar{z}_i$$

defined on column vectors $(z_1, z_2, \dots, z_n)^T$ in $\mathbb{C}^n$. Verify that the set of $n \times n$ complex unitary matrices $U(n)$ forms a group.

Problem 2.22 Show that two rotations belong to the same conjugacy classes of the rotation group $SO(3)$ if and only if they have the same magnitude; that is, they have the same angle of rotation but possibly a different axis of rotation.

Problem 2.23 The general Galilean transformation

$$t' = t + a, \quad \mathbf{r}' = \mathsf{A}\mathbf{r} - \mathbf{v}t + \mathbf{b} \quad \text{where} \quad \mathsf{A}^T\mathsf{A} = \mathsf{I}$$

may be denoted by the abstract symbol $(a, \mathbf{v}, \mathbf{b}, \mathsf{A})$. Show that the result of performing two Galilean transformations

$$G_1 = (a_1, \mathbf{v}_1, \mathbf{b}_1, \mathsf{A}_1) \quad \text{and} \quad G_2 = (a_2, \mathbf{v}_2, \mathbf{b}_2, \mathsf{A}_2)$$

in succession is

$$G = G_2 G_1 = (a, \mathbf{v}, \mathbf{b}, \mathsf{A})$$

where

$$a = a_1 + a_2, \quad \mathbf{v} = \mathsf{A}_2\mathbf{v}_1 + \mathbf{v}_2, \quad \mathbf{b} = \mathbf{b}_2 - a_1\mathbf{v}_2 + \mathsf{A}_2\mathbf{b}_1 \quad \text{and} \quad \mathsf{A} = \mathsf{A}_2\mathsf{A}_1.$$

Show from this rule of composition that the Galilean transformations form a group. In particular verify explicitly that the associative law holds.

Problem 2.24 (a) From the matrix relation defining a Lorentz transformation L,

$$\mathsf{G} = \mathsf{L}^T\mathsf{G}\mathsf{L},$$

where G is the 4×4 diagonal matrix whose diagonal components are $(1, 1, 1, -1)$; show that Lorentz transformations form a group.
(b) Denote the Poincaré transformation

$$\mathbf{x}' = \mathsf{L}\mathbf{x} + \mathbf{a}$$

by $(\mathsf{L}, \mathbf{a})$, and show that two Poincaré transformations $(\mathsf{L}_1, \mathbf{a})$ and $(\mathsf{L}_2, \mathbf{b})$ performed in succession is equivalent to the Poincaré transformation

$$(\mathsf{L}_2\mathsf{L}_1, \mathbf{b} + \mathsf{L}_2\mathbf{a}).$$

(c) From this law of composition show that the Poincaré transformations form a group. As in the previous problem the associative law should be shown explicitly.

Problem 2.25 Let V be an abelian group with law of composition $+$, and G any group with a left action on V, denoted as usual by $g : v \mapsto gv$. Assume further that this action is a homomorphism of V,

$$g(v + w) = gv + gw.$$

(a) Show that $G \times V$ is a group with respect to the law of composition

$$(g, v)(g', v') = (gg', v + gv').$$

This group is known as the **semi-direct** product of G and V, and is denoted $G \circledS V$.

(b) Show that the elements of type $(g, 0)$ form a subgroup of $G \circledS V$ that is isomorphic with G and that V is isomorphic with the subgroup (e, V). Show that the latter is a normal subgroup.

(c) Show that every element of $G \circledS V$ has a unique decomposition of the form vg, where $g \equiv (g, 0) \in G$ and $v \equiv (e, v) \in V$.

Problem 2.26 The following provide examples of the concept of semi-direct product defined in Problem 2.25:

(a) Show that the Euclidean group is the semi-direct product of the rotation group $SO(3, \mathbb{R})$ and $\mathbb{R}^3$, the space of column 3-vectors.

(b) Show that the Poincaré group is the semi-direct product of the Lorentz group $O(3, 1)$ and the abelian group of four-dimensional vectors $\mathbb{R}^4$ under vector addition (see Problem 2.24).

(c) Display the Galilean group as the semi-direct product of two groups.

Problem 2.27 The group A of **affine transformations** of the line consists of transformations of the form

$$x' = ax + b, \quad a \neq 0.$$

Show that these form a semi-direct product on $\dot{\mathbb{R}} \times \mathbb{R}$. Although the multiplicative group of reals $\dot{\mathbb{R}}$ and the additive group $\mathbb{R}$ are both abelian, demonstrate that their semi-direct product is not.

References

[1] G. Birkhoff and S. MacLane. *A Survey of Modern Algebra*. New York, MacMillan, 1953.

[2] R. Geroch. *Mathematical Physics*. Chicago, The University of Chicago Press, 1985.

[3] S. Lang. *Algebra*. Reading, Mass., Addison-Wesley, 1965.

[4] M. Hammermesh. *Group Theory and its Applications to Physical Problems*. Reading, Mass., Addison-Wesley, 1962.

[5] C. Chevalley. *Theory of Lie Groups*. Princeton, N.J., Princeton University Press, 1946.

[6] F. P. Hildebrand. *Methods of Applied Mathematics*. Englewood Cliffs, N. J., Prentice-Hall, 1965.