Group Theory

23

The tale of mathematics and physics has been one of love and hate, of harmony and discord, and of friendship and animosity. From their simultaneous inception in the shape of calculus in the seventeenth century, through an intense and interactive development in the eighteenth and most of the nineteenth century, to an estrangement in the latter part of the nineteenth and the beginning of the twentieth century, mathematics and physics have experienced the best of times and the worst of times. Sometimes, as in the case of calculus, nature dictates a mathematical dialect in which the narrative of physics is to be spoken. Other times, man, building upon that dialect, develops a sophisticated language in which—as in the case of Lagrangian and Hamiltonian interpretation of dynamics—the narrative of physics is set in the most beautiful poetry. But the happiest courtship, and the most exhilarating relationship, takes place when a discovery in physics leads to a development in mathematics that in turn feeds back into a better understanding of physics, leading to new ideas or a new interpretation of existing ideas. Such a state of affairs began in the 1930s with the advent of quantum mechanics, and, after a lull of about 30 years, revived in the late 1960s. We are fortunate to be witnesses to one of the most productive collaborations between the physics and mathematics communities in the history of both.

It is not an exaggeration to say that the single most important catalyst that has facilitated this collaboration is the idea of **symmetry** the study of which is the main topic of the theory of groups, the subject of this chapter. Although group theory, in one form or another, was known to mathematicians as early as the beginning of the nineteenth century, it found its way into physics only after the invention of quantum theory, and in particular, Dirac's interpretation of it in the language of transformation theory. Eugene Wigner, in his seminal paper[1] of 1939 in which he applied group theoretical ideas to Lorentz transformations, paved the way for the marriage of group theory and quantum mechanics. Today, in every application of quantum theory, be it to atoms, molecules, solids, or elementary particles such as quarks and leptons, group-theoretical techniques are indispensable.

[1] E.P. Wigner, On the Unitary Representations of the Inhomogeneous Lorentz Group, *Ann. of Math.* **40** (1939) 149–204.

S. Hassani, *Mathematical Physics*, DOI 10.1007/978-3-319-01195-0_23,

23.1 Groups

The prototype of a group is a transformation group, the set of invertible mappings of a set onto itself. Let us elaborate on this. First, we take mappings because they are the most general operations performed between sets. From a physical standpoint, mappings are essential in understanding the symmetries and other basic properties of a theory. For instance, rotations and translations are mappings of space. Second, the mappings ought to be on a single set, because we want to be able to compose any given two mappings. We cannot compose $f : A \to B$ and $g : A \to B$, because, by necessity, the domain of the second must be a subset of the image of the first. With three sets, and $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, even if the composition $f \circ g$ is defined, $g \circ f$ will not be. Third, we want to be able to undo the mapping. Physically, this means that we should be able to retrace our path to our original position in the set. This can happen only if all mappings of interest have an inverse. Finally, we note that composing a mapping with its inverse yields identity. Therefore, the identity map must also be included in the set of mappings.

We shall come back to transformation groups frequently. In fact, almost all groups considered in this book are transformation groups. However, as in our study of vector spaces in Chap. 2, it is convenient to give a general description of (abstract) groups.

Group defined

Definition 23.1.1 A **group** is a set G together with an *associative* binary operation $G \times G \to G$ called **multiplication**—and denoted generically by $\star$—having the following properties:

1. There exists a unique element[2] $e \in G$ called the **identity** such that $e \star g = g \star e = g$.
2. For every element $g \in G$, there exists an element g^{-1}, called the **inverse** of g, such that $g \star g^{-1} = g^{-1} \star g = e$.

To emphasize the binary operation of a group, we designate it as $(G, \star)$.

Évariste Galois
1811–1832

Historical Notes

Évariste Galois (1811–1832) was definitely not the stereotypically dull mathematician, quietly creating theorems and teaching students. He was a political firebrand whose life ended in a mysterious duel when he was only 21 years old. An ardent republican, he was in the unfortunate position of having Cauchy, an ardent royalist, as the only French mathematician capable of understanding the significance of his work. His professional accomplishments (fewer than 100 pages, much of which was published posthumously) received the attention they deserved many years later. It is truly sad to realize that for decades, work from the man credited with the foundation of group theory were lost to the world of mathematics. Galois's early years were relatively happy. His father, a liberal thinker known for his wit, was director of a boarding school and later mayor of Bourg-la-Reine. Galois's mother took charge of his early education. A stubborn, eccentric woman, she mixed classical culture with a fairly stern religious upbringing.

The young Galois entered the College Louis-le-Grand in 1823, but found the harsh discipline imposed by church and political authorities difficult to bear. His interest in mathematics was sparked in class by Vernier, but Galois quickly tired of the elementary character of the material, preferring instead to read the more advanced original works on his

[2] To distinguish between identities of different groups, we sometimes write e_G for the identity of the group G.

own. After a flawed attempt to solve the general fifth-order equation, Galois submitted a paper to the *Académie des Sciences* in which he described the definitive solution with the aid of group theory, of which the young Galois can be considered the creator. However, this strong initial foray into the frontiers of mathematics was accompanied by tragedy and setback. A few weeks after the paper's submission, his father committed suicide, which Galois felt was largely to be blamed on those who politically persecuted his father. A month later the young mathematician failed the entrance examination to the Ecole Polytechnique, largely due to his refusal to answer in the form demanded by the examiner. Galois did gain entrance to a less prestigious school for the preparation of secondary-school teachers. While there he read some of Abel's results (published after Abel's death) and found that they contained some of the results he had submitted to the Academy including the proof of the impossibility of solving quintics. Cauchy, assigned as the judge for Galois's paper, suggested that he revise it in light of this new information. Galois instead wrote an entirely new manuscript and submitted it in competition for the grand prix in mathematics. Tragically, the manuscript was lost on the death of Fourier, who had been assigned to examine it, leaving Galois out of the competition. These events, fueled by a later, unfair dismissal of another of his papers by Poisson, seem to have driven Galois toward political radicalism and rebellion during the renewed turmoil then plaguing France. He was arrested several times for his agitations, although he continued work on mathematics while in custody. On May 30, 1832, he was wounded in a duel with an unknown adversary, the duel perhaps caused by an unhappy love affair. His funeral three days later sparked riots that raged through Paris in the days that followed.
The delay in recognition of the true scope of Galois's scant but amazing work stemmed partly from the originality of his ideas and the lack of competent local reviewers. Cauchy left France after seeing only the early parts of Galois's work, and much of the rest remained unnoticed until Liouville prepared the later manuscripts for publication a decade after Galois's death. Their true value wasn't appreciated for another two decades. The young mathematician himself added to the difficulty by deliberately making his writing so terse that the "established scientists" for whom he had so much disdain could not understand it. Those fortunate enough to appreciate Galois's work found fertile ground in mathematical research, in such fundamental fields as group theory and modern algebra, for decades to come.

order of a group

If the underlying set G has a finite number of elements, the group is called **finite**, and its number of elements, denoted by $|G|$, is called the **order** of G. We can also have an infinite group whose cardinality can be countable or continuous.

Given an element $a \in G$, we write

$$a^k \equiv \underbrace{a \star a \star \cdots \star a}_{k \text{ times}}, \qquad a^{-m} \equiv \underbrace{a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{m \text{ times}}$$

and note that

$$a^i \star a^j = a^{i+j} \quad \text{for all } i, j \in \mathbb{Z}.$$

Example 23.1.2 The following are examples of familiar sets that have group properties.

(a) The set $\mathbb{Z}$ of integers under the binary operation of addition forms a group whose identity element is 0 and the inverse of n is $-n$. This group is countably infinite.
(b) The set $\{-1, +1\}$, under the binary operation of multiplication, forms a group whose identity element is 1 and the inverse of each element is itself. This group is finite.
(c) The set $\{-1, +1, -i, +i\}$, under the binary operation of multiplication, forms a finite group whose identity element is 1.

(d) The set $\mathbb{R}$, under the binary operation of addition, forms a group whose identity element is 0 and the inverse of r is $-r$. This group is uncountably infinite.
(e) The set $\mathbb{R}^+$ ($\mathbb{Q}^+$) of positive real (rational) numbers, under the binary operation of multiplication, forms a group whose identity element is 1 and the inverse of r is $1/r$. This group is uncountably (countably) infinite.
(f) The set $\mathbb{C}$, under the binary operation of addition, forms a group whose identity element is 0 and the inverse of z is $-z$. This group is uncountably infinite.
(g) The uncountably infinite set $\mathbb{C} - \{0\}$ of all complex numbers except 0, under the binary operation of multiplication, forms a group whose identity element is 1 and the inverse of z is $1/z$.
(h) The uncountably infinite set $\mathcal{V}$ of vectors in a vector space, under the binary operation of addition, forms a group whose identity element is the zero vector and the inverse of $|a\rangle$ is $-|a\rangle$.
(i) The set of invertible $n \times n$ matrices, under the binary operation of multiplication, forms a group whose identity element is the $n \times n$ unit matrix and the inverse of A is A^{-1}. This group is uncountably infinite.

The reader is urged to verify that each set given above is indeed a group.

In general, the elements of a group do not commute. Those groups whose elements do commute are so important that we give them a special name:

abelian groups defined

Definition 23.1.3 A group $(G, \star)$ is called **abelian** or **commutative** if $a \star b = b \star a$ for all $a, b \in G$. It is common to denote the binary operation of an abelian group by $+$.

All groups of Example 23.1.2 are abelian except the last.

Example 23.1.4 Let **A** be a vector potential that gives rise to a magnetic field **B**. The set of transformations of **A** that give rise to the same **B** is an abelian group. In fact, such transformations simply add the gradient of a function to **A**. The reader can check the details.

The reader may also verify that the set of invertible mappings $f : S \to S$, i.e., the **set of transformations** of S, is indeed a (nonabelian) group. If S has n elements, this group is denoted by S_n and is called the **symmetric group** of S. S_n is a nonabelian (unless $n \leq 2$) finite group that has $n!$ elements. An element g of S_n is usually denoted by two rows, the top row being S itself—usually taken to be $1, 2, \ldots, n$—and the bottom row its image under g. For example, $g \equiv \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)$ is an element of S_4 such that $g(1) = 2$, $g(2) = 3$, $g(3) = 4$, and $g(4) = 1$.

symmetric or permutation group

Consider two groups, the set of vectors in a plane $((x, y), +)$ and the set of complex numbers $(\mathbb{C}, +)$, both under addition. Although these are two different groups, the difference is superficial. We have seen similar differences in disguise in the context of vector spaces and the notion of isomorphism. The same notion applies to group theory:

Definition 23.1.5 Let $(G, \star)$ and $(H, \bullet)$ be groups. A map $f : G \to H$ is called a **homomorphism** if

homomorphism, isomorphism, and automorphism

$$f(a \star b) = f(a) \bullet f(b) \quad \forall a, b \in G.$$

An **isomorphism** is a homomorphism that is also a bijection. Two groups are **isomorphic**, denoted by $G \cong H$, if there is an isomorphism $f : G \to H$. An isomorphism of a group onto itself is called an **automorphism**.

An immediate consequence of this definition is that $f(e_G) = e_H$ and $f(g^{-1}) = [f(g)]^{-1}$ (see Problem 23.9).

Example 23.1.6 Let G be any group and $\{1\}$ the multiplicative group consisting of the single number 1. It is straightforward to show that $f : G \to \{1\}$, given by (the only function available!) $f(g) = 1$ for all $g \in G$ is a homomorphism. This homomorphism is called the **trivial** (or sometimes, **symmetric**) homomorphism.

trivial homomorphism

The establishment of isomorphism $f : \mathbb{R}^2 \to \mathbb{C}$ between $((x, y), +)$, and $(\mathbb{C}, +)$ is trivial: Just write $f(x, y) = x + iy$. A less trivial isomorphism is the exponential map, $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$. The reader may verify that this is a homomorphism (in particular, it maps addition to multiplication) and that it is one-to-one.

We have noted that the set of invertible maps of a set forms a group. A very important special case of this is when the set is a vector space $\mathcal{V}$ and the maps are all *linear*.

general linear group

Box 23.1.7 *The **general linear group** of a vector space $\mathcal{V}$, denoted by $GL(\mathcal{V})$, is the set of all invertible endomorphisms of $\mathcal{V}$. In particular, when $\mathcal{V} = \mathbb{C}^n$, we usually write $GL(n, \mathbb{C})$ instead of $GL(\mathbb{C}^n)$ with similar notation for $\mathbb{R}$.*

It is sometimes convenient to display a finite group $G = \{g_i\}_{i=1}^{|G|}$ as a $|G| \times |G|$ table, called the **group multiplication table**, in which the intersection of the ith row and jth column is occupied by $g_i \star g_j$. Because of its trivial multiplication, the identity is usually omitted from the table.

group multiplication table

23.2 Subgroups

It is customary to write ab instead of $a \star b$. We shall adhere to this convention, but restore the $\star$ as necessary to avoid any possible confusion.

Definition 23.2.1 A subset S of a group G is a **subgroup** of G if it is a group in its own right under the binary operation of G, i.e., if it contains the inverse of all its elements as well as the product of any pair of its elements.

subgroup defined

It follows from this definition that $e \in S$. It is also easy to show that the intersection of two subgroups is a subgroup (Problem 23.2).

Example 23.2.2 (Examples of subgroups)

trivial subgroup

1. For any G, the subset $\{e\}$, consisting of the identity alone, is a subgroup of G called the **trivial subgroup** of G.
2. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
3. The set of even integers (but not odd integers) is a subgroup of $(\mathbb{Z}, +)$. In fact, the set of all multiples of a positive integer m, denoted by $\mathbb{Z}m$, is a subgroup of $\mathbb{Z}$. It turns out that *all* subgroups of $\mathbb{Z}$ are of this form.
4. The subset of $GL(n, \mathbb{C})$ consisting of transformations that have unit determinant is a subgroup of $GL(n, \mathbb{C})$ because the identity transformation has unit determinant, the inverse of a transformation with unit determinant also has unit determinant, and the product of two transformations with unit determinants has unit determinant.

special linear group

Box 23.2.3 *The subgroup of $GL(n, \mathbb{C})$ consisting of elements having unit determinant is denoted by $SL(n, \mathbb{C})$ and is called the* ***special linear group****.*

unitary, orthogonal, special unitary, and special orthogonal groups

5. The set of unitary transformations of $\mathbb{C}^n$, denoted by $U(n)$, is a subgroup of $GL(n, \mathbb{C})$ because the identity transformation is unitary, the inverse of a unitary transformation is also unitary, and the product of two unitary transformations is unitary.

Box 23.2.4 *The set of unitary transformations $U(n)$ is a subgroup of $GL(n, \mathbb{C})$ and is called the* ***unitary group****. Similarly, the set of orthogonal transformations of $\mathbb{R}^n$ is a subgroup of $GL(n, \mathbb{R})$. It is denoted by $O(n)$ and called the* ***orthogonal group****.*

Each of these groups has a special subgroup whose elements have unit determinants. These are denoted by $SU(n)$ and $SO(n)$, and called **special unitary group** and **special orthogonal group**, respectively. The latter is also called the group of **rigid rotations** of $\mathbb{R}^n$.

6. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, and define an inner product on $\mathbb{R}^n$ by

$$\mathbf{x} \cdot \mathbf{y} = -x_1 y_1 - \cdots - x_p y_p + x_{p+1} y_{p+1} + \cdots + x_n y_n.$$

Denote the subset of $GL(n, \mathbb{R})$ that leaves this inner product invariant by[3] $O(p, n-p)$. Then $O(p, n-p)$ is a subgroup of $GL(n, \mathbb{R})$. The set of linear transformations among $O(p, n-p)$ that have determinant

[3] The reader is warned that what we have denoted by $O(p, n-p)$ is sometimes denoted by other authors by $O(n-p, p)$ or $O(n, p)$ or $O(p, n)$.

1 is denoted by $SO(p, n-p)$. The special case of $p = 0$ gives us the orthogonal and special orthogonal groups.[4] When $n = 4$ and $p = 3$, we get the inner product of the special theory of relativity, and $O(3, 1)$, the set of Lorentz transformations, is called the **Lorentz group**. If one adds translations of $\mathbb{R}^4$ to $O(3, 1)$, one obtains the **Poincaré group**, $P(3, 1)$.

Lorentz and Poincaré groups

7. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^{2n}$, and J the $2n \times 2n$ matrix $\left(\begin{smallmatrix} 0 & \mathsf{1} \\ -\mathsf{1} & 0 \end{smallmatrix}\right)$, where $\mathsf{1}$ is the $n \times n$ unit matrix. The subset of $GL(2n, \mathbb{R})$ that leaves $\mathsf{x}^t \mathsf{J} \mathsf{x}$, called an **anti-symmetric bilinear form**, invariant is a subgroup of $GL(2n, \mathbb{R})$ called the **symplectic group** and denoted by $Sp(2n, \mathbb{R})$. As we shall see in Chap. 28, the symplectic group is fundamental in the formal treatment of Hamiltonian mechanics.

symplectic group

8. Let S be a subgroup of G and $g \in G$. Then it is readily shown that the set

conjugate subgroup

$$g^{-1} S g \equiv \left\{ g^{-1} s g \mid s \in S \right\}$$

is also a subgroup of G, called the **subgroup conjugate to** S under g, or the **subgroup** g**-conjugate** to S.

When discussing vector spaces, we noted that given any sub*set* of a vector space, one could construct a sub*space* out of it by taking all possible linear combinations (natural operations of the vector space) of the vectors in the subset. We called the subspace thus obtained the *span of the subset*. The same procedure is applicable in group theory as well. If S is a subset of a group G, we can generate a subgroup out of S by collecting all possible products and inverses (natural operations of the group) of the elements of S. The reader may verify that the result is indeed a subgroup of G.

Definition 23.2.5 Let S be a subset of a group G. The **subgroup generated by** S, denoted by $\langle S \rangle$, is the union of S and all inverses and products of the elements of S.

subgroup generated by a subset

In the special case for which $S = \{a\}$, a single element, we use $\langle a \rangle$ instead of $\langle \{a\} \rangle$ and call it the **cyclic subgroup** generated by a. It is simply the collection of all integer powers of a.

cyclic subgroup

Definition 23.2.6 Let G be a group and $a, b \in G$. The **commutator** of a and b, denoted by $[a, b]$, is

commutator of group elements

$$[a, b] \equiv aba^{-1}b^{-1}.$$

The subgroup $\langle \bigcup_{a,b \in G} [a, b] \rangle$ generated by all commutators of G is called the **commutator subgroup** of G. The reader may verify that a group is abelian if and only if its commutator subgroup is the trivial subgroup, i.e., consists of only the identity element.

commutator subgroup of a group

[4] It is customary to write $O(n)$ and $SO(n)$ for $O(0, n)$ and $SO(0, n)$.

centralizer of an element in G and the center of G

Definition 23.2.7 Let $x \in G$. The set of elements of g that commute with x, denoted by $C_G(x)$, is called the **centralizer of** x **in** G. The set $Z(G)$ of elements of a group G that commute with all elements of G is called the **center** of G.

Theorem 23.2.8 *$C_G(x)$ is a subgroup of G and $Z(G)$ is an abelian subgroup of G. Furthermore, G is abelian if and only if $Z(G) = G$.*

Proof Proof is immediate from the definitions. □

kernel of a homomorphism

Definition 23.2.9 Let G and H be groups and let $f : G \to H$ be a homomorphism. The **kernel** of f is

$$\ker f \equiv \{x \in G \mid f(x) = e \in H\}.$$

The reader may check that $\ker f$ is a subgroup of G, and $f(G)$ is a subgroup of H. These are the analogues of the same concepts encountered in vector spaces. In fact, if we treat a vector space as an additive group, with the zero vector as identity, then the above definition coincides with that of linear mappings and vector spaces.

Carrying the analogy further, we recall that given two subspaces $\mathcal{U}$ and $\mathcal{W}$ of a vector space $\mathcal{V}$, we denote by $\mathcal{U} + \mathcal{W}$ all vectors of $\mathcal{V}$ that can be written as the sum of a vector in $\mathcal{U}$ and a vector in $\mathcal{W}$. There is a similar concept in group theory that is sometimes very useful.

Definition 23.2.10 Let S and T be subsets of a group $(G, \star)$. Then one defines the product of these subsets as

$$S \star T \equiv \{s \star t \mid s \in S \text{ and } t \in T\}.$$

In particular, if T consists of a single element t, then

$$S \star t = \{s \star t \mid s \in S\}.$$

left and right cosets

As usual, we shall drop the $\star$ and write ST and St. If S is a subgroup, then St is called a **right coset**[5] of S in G. Similarly, tS is called a **left coset** of S in G. In either case, t is said to **represent** the coset.

Example 23.2.11 Let $G = \mathbb{R}^3$ treated as an additive abelian group, and let S be a plane through the origin. Then $t + S$ is S if $t \in S$ (see Problem 23.5); otherwise, it is a plane parallel to S. In fact, $t + S$ is simply the translation of all points of S by t.

Theorem 23.2.12 *Any two right (left) cosets of a subgroup are either disjoint or identical.*

[5] Some authors switch our right and left in their definition.

Proof Let S be a subgroup of G and suppose that $x \in Sa \cap Sb$. Then $x = s_1 a = s_2 b$ with $s_1, s_2 \in S$. Hence, $ab^{-1} = s_1^{-1} s_2 \in S$. By Problem 23.6, $Sa = Sb$. The left cosets can be treated in the same way. □

A more "elegant" proof starts by showing that an equivalence relation can be defined on G by

$$a \bowtie b \iff ab^{-1} \in S$$

and then proving that the equivalence classes of this relation are cosets of S.

One interpretation of Theorem 23.2.12 is that a and b belong to the same right coset of S if and only if $ab^{-1} \in S$. A second interpretation is that a coset can be represented by *any* one of its elements (why?).

All cosets (right or left) of a subgroup S have the same cardinality as S itself. This can readily be established by considering the map $\phi : S \to Sa$ ($\phi : S \to aS$) with $\phi(s) = sa$ ($\phi(s) = as$) and showing that ϕ is bijective.

There are many instances both in physics and mathematics in which a collection of points of a given set represent a single quantity. For example, it is not simply the set of ratios of integers that comprise the set of rational numbers, but the set of certain collections of such ratios: The rational number $\frac{1}{2}$ represents $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}$, etc. Similarly, a given magnetic field represents an infinitude of vector potentials each differing by a gradient from the others, and a physical state in quantum mechanics is an infinite number of wave functions differing from one another by a phase.

With the set of cosets constructed above, it is natural to ask whether they could be given an algebraic structure.[6] The most natural such structure would clearly be that of a group: Given aS and bS define their product as abS. Would this operation turn the set of (left) cosets into a group? The following argument shows that it will, under an important restriction.

It is clear that the identity of such a group would be S itself. It is equally clear that we should have $(b^{-1}S)(bS) = S$, so that $(b^{-1}Sb)S = S$. It follows from Problem 23.5 that we must have $b^{-1}Sb \subset S$ for all $b \in G$. Now replace b with b^{-1} and note that $bSb^{-1} \subset S$ as well. Let s be an arbitrary element of S. Then $bsb^{-1} = s'$ for some $s' \in S$, and $s = b^{-1}s'b \in b^{-1}Sb$. It follows that $S \subset b^{-1}Sb$ for all $b \in G$, and, with the reverse inclusion derived above, that $S = b^{-1}Sb$. This motivates the following definition.

Definition 23.2.13 A subgroup N of a group G is called **normal** if $N = g^{-1}Ng$ (equivalently if $Ng = gN$) for all $g \in G$. normal subgroup defined

The preceding argument shows that the set of cosets (no specification is necessary since the right and left cosets coincide) of a normal subgroup forms a group:

[6] The set of cosets of a subgroup is the analog of factor space of a subspace of a vector space (Sect. 2.1.2) and factor algebra of a subalgebra of an algebra (Sect. 3.2.1). We have seen that, while a factor space of *any* subspace can be turned into a vector space, that is not the case with an algebra: the subalgebra must be an ideal of the algebra. There is a corresponding restriction for the subgroup.

quotient or factor group

Theorem 23.2.14 *If N is a normal subgroup of G, then the collection of all cosets of N, denoted by G/N, is a group, called the* ***quotient group*** *or* ***factor group*** *of G by N.*

We note that the only subgroup conjugate to a normal subgroup N is N itself (see Example 23.2.2), and that all subgroups of an abelian group are automatically normal.

Example 23.2.15 Let $G = \mathbb{R}^3$ and let S be a plane through the origin as in Example 23.2.11. Since G is abelian, S is automatically normal, and G/S is the set of planes parallel to S. Let $\hat{\mathbf{e}}_n$ be a normal to S. Then it is readily seen that

$$G/S = \{r\hat{\mathbf{e}}_n + S \mid r \in \mathbb{R}\}.$$

We have picked the perpendicular distance between a plane and S (with sign included) to represent that plane. The reader may check that the quotient group G/S is isomorphic to $\mathbb{R}$. Identifying S with $\mathbb{R}^2$, we can write $\mathbb{R}^3/\mathbb{R}^2 \cong \mathbb{R}$. The cancellation of exponents is quite accidental here!

Let $G = \mathbb{Z}$ and $S = \mathbb{Z}m$, the set of multiples of the positive integer m. Since $\mathbb{Z}$ is abelian, $\mathbb{Z}m$ is normal, and $\mathbb{Z}/\mathbb{Z}m$ is indeed a group, a typical element of which looks like $k + m\mathbb{Z}$. By adding (or subtracting) multiples of m to k, and using $mj + m\mathbb{Z} = m\mathbb{Z}$ (see Problem 23.5), we can assume that $0 \leq k \leq m - 1$. It follows that $\mathbb{Z}/\mathbb{Z}m$ is a finite group. Furthermore,

$$(k_1 + m\mathbb{Z}) + (k_2 + m\mathbb{Z}) = k_1 + k_2 + m\mathbb{Z} = k + m\mathbb{Z},$$

where k is the remainder after enough multiples of m have been subtracted from $k_1 + k_2$. One writes $k_1 + k_2 \equiv k \pmod{m}$. The coset $k + m\mathbb{Z}$ is sometimes denoted by $\overline{k}$ and the quotient group $\mathbb{Z}/\mathbb{Z}m$ by $\mathbb{Z}_m$:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

$\mathbb{Z}_m$ is a prototype of the finite cyclic groups. It can be shown that every cyclic group of order m is isomorphic to $\mathbb{Z}_m$ a generator of which is $\overline{1}$ (recall that the binary operation is *addition* for $\mathbb{Z}_m$).

first isomorphism theorem

Theorem 23.2.16 (First isomorphism theorem) *Let G and H be groups and $f : G \to H$ a homomorphism. Then* $\ker f$ *is a normal subgroup of G, and $G/\ker f$ is isomorphic to $f(G)$.*

Proof We have already seen that $\ker f$ is a subgroup of G. To show that it is normal, let $g \in G$ and $x \in \ker f$. Then

$$\begin{aligned} f\left(gxg^{-1}\right) &= f(g)f(x)f\left(g^{-1}\right) = f(g)e_H f\left(g^{-1}\right) = f(g)f\left(g^{-1}\right) \\ &= f\left(gg^{-1}\right) = f(e_G) = e_H. \end{aligned}$$

It follows that $gxg^{-1} \in \ker f$. Therefore, $\ker f$ is normal. We leave it to the reader to show that $\phi : G/\ker f \to f(G)$ given by $\phi(g[\ker f]) \equiv \phi([\ker f]g) = f(g)$ is an isomorphism.[7] □

Example 23.2.17 The special linear group of $\mathcal{V}$ is a normal subgroup of the general linear group of $\mathcal{V}$. To see this, note that $\det : GL(\mathcal{V}) \to \mathbb{R}^+$ is a homomorphism whose kernel is $SL(\mathcal{V})$.

conjugate and conjugacy class defined

Definition 23.2.18 Let $x \in G$. A **conjugate** of x is an element y of G that can be written as $y = gxg^{-1}$ with $g \in G$. The set of all elements of G conjugate to one another is called a **conjugacy class**. The ith conjugacy class is denoted by K_i.

One can check that "x is conjugate to y" is an equivalence relation whose classes are the conjugacy classes. In particular, two different conjugacy classes are disjoint. One can also show that each element of the center of a group constitutes a class by itself. In particular, the identity in any group is in a class by itself, and each element of an abelian group forms a (different) class.

Although a normal subgroup N contains the conjugate of each of its elements, N is not a class. The class containing any given element of N will be only a proper subset of N (unless N is trivial). The characteristic feature of a normal subgroup is that it contains the conjugacy classes of all its elements. This is not shared by other subgroups, which, in general, contain only the trivial class of the identity element.

Example 23.2.19 Consider the group $SO(3)$ of rotations in three dimensions. Let us denote a rotation by $R_{\hat{\mathbf{e}}}(\theta)$, where $\hat{\mathbf{e}}$ is the direction of the axis of rotation and θ is the angle of rotation. A typical member of the conjugacy class of $R_{\hat{\mathbf{e}}}(\theta)$ is $RR_{\hat{\mathbf{e}}}(\theta)R^{-1}$, where R is some rotation. Let $\hat{\mathbf{e}}' = R\hat{\mathbf{e}}$ be the vector obtained by applying the rotation R on $\hat{\mathbf{e}}$, and note that

$$RR_{\hat{\mathbf{e}}}(\theta)R^{-1}\hat{\mathbf{e}}' = RR_{\hat{\mathbf{e}}}(\theta)R^{-1}R\hat{\mathbf{e}} = RR_{\hat{\mathbf{e}}}\hat{\mathbf{e}} = R\hat{\mathbf{e}} = \hat{\mathbf{e}}',$$

where we used the fact that $R_{\hat{\mathbf{e}}}\hat{\mathbf{e}} = \hat{\mathbf{e}}$ because a rotation leaves its axis unchanged. This last statement, applied to the equation above, also shows that $RR_{\hat{\mathbf{e}}}(\theta)R^{-1}$ is a rotation about $\hat{\mathbf{e}}'$. Problem 23.18 establishes that the angle of rotation associated with $RR_{\hat{\mathbf{e}}}(\theta)R^{-1}$ is θ. We can summarize this as $RR_{\hat{\mathbf{e}}}(\theta)R^{-1} = R_{\hat{\mathbf{e}}'}(\theta)$.

all rotations having the same angle belong to the same conjugacy class

The result of this example is summarized as follows:

Box 23.2.20 *All rotations having the same angle belong to the same conjugacy class of the group of rotations in three dimensions.*

[7] Compare this theorem with the set-theoretic result obtained in Chap. 1 where the map $X/\bowtie \to f(X)$ was shown to be bijective if $\bowtie$ is the equivalence relation induced by f.

23.2.1 Direct Products

The resolution of a vector space into a direct sum of subspaces was a useful tool in revealing its structure. The same idea can also be helpful in studying groups. Recall that the only vector common to the subspaces of a direct sum is the zero vector. Moreover, any vector of the whole space can be written as the sum of vectors taken from the subspaces of the direct sum. Considering a vector space as a (abelian) group, with zero as the identity and summation as the group operation, leads to the notion of direct product.

internal direct product of groups

Definition 23.2.21 A group G is said to be the **direct product** of two of its subgroups H_1 and H_2, and we write $G = H_1 \times H_2$, if

1. all elements of H_1 commute with all elements of H_2;
2. the group identity is the only element common to both H_1 and H_2;
3. every $g \in G$ can be written as $g = h_1 h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$.

It follows from this definition that h_1 and h_2 are unique, and H_1 and H_2 are normal. This kind of direct product is sometimes called **internal**, because the "factors" H_1 and H_2 are chosen from inside the group G itself. The external direct product results when we take two unrelated groups and make a group out of them:

external direct product of groups

Proposition 23.2.22 *Let G and H be groups. The Cartesian product $G \times H$ can be given a group structure by*

$$(g, h) \star (g', h') \equiv (gg', hh').$$

*With this multiplication, $G \times H$ is called the **external direct product** of G and H. Furthermore, $G \cong G \times \{e_H\}$, $H \cong \{e_G\} \times H$, $G \times H \cong H \times G$, and to within these isomorphisms, $G \times H$ is the internal direct product of $G \times \{e_H\}$ and $\{e_G\} \times H$.*

The proof is left for the reader.

Niels Henrik Abel
1802–1829

Historical Notes

Niels Henrik Abel (1802–1829) was the second of seven children, son of a Lutheran minister with a small parish of Norwegian coastal islands. In school he received only average marks at first, but then his mathematics teacher was replaced by a man only seven years older than Abel. Abel's alcoholic father died in 1820, leaving almost no financial support for his young prodigy, who became responsible for supporting his mother and family. His teacher, Holmboe, recognizing his talent for mathematics, raised money from his colleagues to enable Abel to attend Christiania (modern Oslo) University. He entered the university in 1821, 10 years after the university was founded, and soon proved himself worthy of his teacher's accolades. His second paper, for example, contained the first example of a solution to an integral equation.

Abel then received a two-year government travel grant and journeyed to Berlin, where he met the prominent mathematician Crelle, who soon launched what was to become the leading German mathematical journal of the nineteenth century, commonly called *Crelle's Journal*. From the start, Abel contributed important papers to Crelle's Journal, including a classic paper on power series, the scope of which clearly reflects his desire for stringency. His most important work, also published in that journal, was a lengthy treatment of elliptic functions in which Abel incorporated their inverse functions to show

that they are a natural generalization of the trigonometric functions. In later research in this area, Abel found himself in stiff competition with another young mathematician, K.G.J. Jacobi. Abel published some papers on functional equations and integrals in 1823. In it he gives the first solution of an integral equation. In 1824 he proved the impossibility of solving algebraically the general equation of the fifth degree and published it at his own expense hoping to obtain recognition for his work.
Despite his proven intellectual success, Abel never achieved material success, not even a permanent academic position. In December of 1828, while traveling by sled to visit his fiancé for Christmas, Abel became seriously ill and died a couple of months later. Ironically, his death from tuberculosis occurred two days before Crelle wrote with the happy news of an appointment for Abel at a scientific institute in Berlin. In Abel's eulogy in his journal, Crelle wrote:
"He distinguished himself equally by the purity and nobility of his character and by a rare modesty which made his person cherished to the same degree as was his genius."

23.3 Group Action

The transformation groups introduced at the beginning of this chapter can be described in the language of abstract groups.

left action, right action, left invariance and right invariance

Definition 23.3.1 Let G be a group and M a set. The **left action** of G on M is a map $\Phi : G \times M \to M$ such that

1. $\Phi(e, m) = m$ for all $m \in M$;
2. $\Phi(g_1 g_2, m) = \Phi(g_1, \Phi(g_2, m))$.

One usually denotes $\Phi(g, m)$ by $g \cdot m$ or more simply by gm. The **right action** is defined similarly. A subset $N \subset M$ is called **left (right) invariant** if $g \cdot m \in N$ ($m \cdot g \in N$) for all $g \in G$, whenever $m \in N$.

any group is isomorphic to a subgroup of the group of transformations of an appropriate set

Example 23.3.2 If we define $f_g : M \to M$ by $f_g(m) \equiv \Phi(g, m) = g \cdot m$, then f_g is recognized as a transformation of M. The collection of such transformations is a *subgroup* of the set of all transformations of M. Indeed, the identity transformation is simply f_e, the inverse of f_g is $f_{g^{-1}}$, and the (associative) law of composition is $f_{g_1} \circ f_{g_2} = f_{g_1 g_2}$. There is a general theorem in group theory stating that any group is isomorphic to a subgroup of the group of transformations of an appropriate set.

orbit, stabilizer; transitive action and effective action

Definition 23.3.3 Let G act on M and let $m \in M$. The **orbit** of m, denoted by Gm, is

$$Gm = \{x \in M \mid x = gm \text{ for some } g \in G\}.$$

The action is called **transitive** if $Gm = M$. The **stabilizer** of m is $G_m = \{g \in G \mid gm = m\}$. The group action is called **free** if $G_m = \{e\}$ for all $m \in M$; it is called **effective** if $gm = m$ for all $m \in M$ implies that $g = e$.

Stabilizer is a subgroup.

The reader may verify that the orbit Gm is the smallest invariant subset of M containing m, and that

Box 23.3.4 *The stabilizer of m is a subgroup of G, which is sometimes called the* ***little group*** *of G at m.*

Remark 23.3.1 Think of the action of G on M as passing from one point of M to another. An element g of G "transits" a region of M to take $m \in M$ to $gm \in M$. The action is therefore, transitive, if G can transit (pass across) all of M, i.e., G can connect any two points of M.

Help with understanding the terminology of the definition above.

If you think of G_m as those elements of G that are confined to (stuck, or imprisoned at) m, then a "free" action of G does not allow any point of M to imprison any subset of G.

Any $g \in G$ such that $gm = m$ for all $m \in M$ has no "effect" on M. Therefore, this g is "ineffective" in its action on M. For G to act "effectively", it should not have any "ineffective" member.

A transitive action is characterized by the fact that given any two points $m_1, m_2 \in M$, one can find a $g \in G$ such that $m_2 = gm_1$. In general, there may be several gs connecting m_1 to m_2. If there are $g, g' \in G$ such that $m_2 = gm_1 = g'm_1$, then

$$gm_1 = g'm_1 \quad \Rightarrow \quad m_1 = g^{-1}g'm_1.$$

If we want g to be unique for all m_1 and m_2, then the group action must be free.

By definition, the orbits of a group G in M are disjoint and their union is the entire M. Another way of stating the same thing is to say that G partitions M into orbits. It should be obvious that the action of G on any orbit is transitive.

From the remarks above, we conclude that

Box 23.3.5 *Two points of an orbit are connected by a unique element of G iff G acts freely on the orbit.*

Example 23.3.6 Let $M = \mathbb{R}^2$ and $G = SO(2)$, the planar rotation group. The action is rotation of a point in the plane about the origin by an angle θ. The orbits are circles centered at the origin. The action is effective but not transitive. The stabilizer of every point in the plane is $\{e\}$, except the origin, for which the whole group is the stabilizer. Since the stabilizer at the origin is not $\{e\}$, the group action is not free.

Let $M = S^1$, the unit circle, and $G = SO(2)$, the rotation group in two dimensions. The action is displacement of a point on the circle. There is only one orbit, the entire circle. The action is effective and transitive. The stabilizer of every point on the circle is $\{e\}$; therefore, the action is free as well.

Let $M = G$, a group, and let a (proper) subgroup H act on G by left multiplication. The orbits are right cosets Hg of the subgroup. The action is effective but not transitive. The stabilizer of every point in the group is $\{e\}$; hence the action is free.

Let $M = \mathbb{R} \cup \{\infty\}$, the set of real numbers including "the point at infinity". Define an action of $SL(2, \mathbb{R})$ on M by

$$g \cdot x \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = \frac{ax + c}{bx + d}.$$

This is a group action with a law of multiplication identical to the matrix multiplication. The action is transitive, but neither effective nor free. Indeed, the reader is urged to show that

$$g \cdot x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = x \ \forall x \quad \text{iff } g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad g = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

making the group action not effective. Furthermore, for every $x \in M$

$$G_x = \begin{pmatrix} a & b \\ bx^2 + (d-a)x & d \end{pmatrix}$$

making the group action not free.

realization of a group

Let M be a set and H the group of transformations of M. Suppose that there is a homomorphism $f : G \to H$ from a group G into H. Then there is a natural action of G on M given by $g \cdot m \equiv [f(g)](m)$. The homomorphism f is sometimes called a **realization** of G.

23.4 The Symmetric Group S_n

Because of its primary importance as the prototypical finite group, and because of its significance in quantum statistics, the symmetric (or permutation) group is briefly discussed in this section. It is also used extensively in the theory of representation of the general linear group and its subgroups.

A generic permutation π of n numbers is shown as

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(i) & \cdots & \pi(n) \end{pmatrix}. \tag{23.1}$$

Because the mapping is bijective, no two elements can have the same image, and $\pi(1), \pi(2), \ldots, \pi(n)$ exhaust all the elements in the set $\{i\}_{i=1}^n$.

We can display the product $\pi_2 \circ \pi_1$ of two permutations using $\pi_2 \circ \pi_1(i) \equiv \pi_2(\pi_1(i))$. For instance, if

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \text{and} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \tag{23.2}$$

Table 23.1 Group multiplication table for S_3

e	π_2	π_3	π_4	π_5	π_6
π_2	e	π_5	π_6	π_3	π_4
π_3	π_6	e	π_5	π_4	π_2
π_4	π_5	π_6	e	π_2	π_3
π_5	π_4	π_2	π_3	π_6	e
π_6	π_3	π_4	π_2	e	π_5

then the product $\pi_2 \circ \pi_1$ takes 1 to 3, etc., because $\pi_2 \circ \pi_1(1) \equiv \pi_2(\pi_1(1)) = \pi_2(3) = 3$, etc. We display $\pi_2 \circ \pi_1$ as

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Example 23.4.1 Let us construct the multiplication table for S_3. Denote the elements of S_3 as follows:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

We give only one sample evaluation of the entries and leave the straightforward—but instructive—calculation of the other entries to the reader. Consider $\pi_4 \circ \pi_5$, and note that $\pi_5(1) = 3$ and $\pi_4(3) = 2$; so $\pi_4 \circ \pi_5(1) = 2$. Similarly, $\pi_4 \circ \pi_5(2) = 1$ and $\pi_4 \circ \pi_5(3) = 3$. Thus

$$\pi_4 \circ \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \pi_2.$$

The entire multiplication table is given in Table 23.1.

Note that both the rows and columns of the group multiplication table include all elements of the group, and no element is repeated in a row or a column. This is because left-multiplication of elements of a group by a single fixed element of the group simply permutes the group elements. Stated differently, the left multiplication map $L_g : G \to G$, given by $L_g(x) = gx$, is bijective, as the reader may verify.

Because we are dealing with finite numbers, repeated application of a permutation to an integer in the set $\{i\}_{i=1}^n$ eventually produces the initial integer. This leads to the following definition.

cycles of symmetric group

Definition 23.4.2 Let $\pi \in S_n$, $i \in \{1, 2, \ldots, n\}$, and let r be the smallest positive integer such that $\pi^r(i) = i$. Then the set of r distinct elements $\{\pi^k(i)\}_{k=0}^{r-1}$ is called a **cycle** of π of length r or an **r-cycle** generated by i.

Start with 1 and apply π to it repeatedly until you obtain 1 again. The collection of elements so obtained forms a cycle in which 1 is contained. Then we select a second number that is not in this cycle and apply π to it repeat-

edly until the original number is obtained again. Continuing in this way, we produce a set of disjoint cycles that exhausts all elements of $\{1, 2, \ldots, n\}$.

Proposition 23.4.3 *Any permutation can be broken up into disjoint cycles.*

It is customary to write elements of each cycle in some specific order within parentheses starting with the first element, say i, on the left, then $\pi(i)$ immediately to its right, followed by $\pi^2(i)$, and so on. For example, the permutations π_1 and π_2 of Eq. (23.2) and their product have the cycle structures $\pi_1 = (13)(24)$, $\pi_2 = (124)(3)$, and $\pi_2 \circ \pi_1 = (132)(4)$, respectively.

Example 23.4.4 Let $\pi_1, \pi_2 \in S_8$ be given by

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 1 & 2 & 8 & 4 & 6 \end{pmatrix},$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 8 & 1 & 7 & 4 & 3 \end{pmatrix}.$$

The reader may verify that

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 4 & 2 & 5 & 3 & 8 & 7 \end{pmatrix}$$

and that

$$\pi_1 = (1374)(25)(68), \qquad \pi_2 = (125)(36748),$$
$$\pi_2 \circ \pi_1 = (16342)(5)(78).$$

In general, permutations do not commute. The product in reverse order is

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 8 & 6 & 3 & 4 & 1 & 7 \end{pmatrix} = (15387)(2)(46),$$

which differs from $\pi_2 \circ \pi_1$. However, note that it has the same cycle structure as $\pi_2 \circ \pi_1$, in that cycles of equal length appear in both. This is a general property of all permutations.

cyclic permutations defined

Definition 23.4.5 If $\pi \in S_n$ has a cycle of length r and all other cycles of π have only one element, then π is called a **cyclic permutation** of length r.

It follows that $\pi_2 \in S_4$ as defined earlier is a cyclic permutation of length 3. Similarly,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 3 & 5 & 4 \end{pmatrix}$$

is a cyclic permutation of length 4 (verify this).

transpositions defined

Definition 23.4.6 A cyclic permutation of length 2 is called a **transposition**.

A transposition (ij) simply switches i and j.

Example 23.4.7 Products of (not necessarily disjoint) cycles may be associated with a permutation whose action on i is obtained by starting with the first cycle (at the extreme right), locating the first occurrence of i, and keeping track of what each cycle does to it or its image under the preceding cycle. For example, let $\pi_1 \in S_6$ be given as a product of cycles by $\pi_1 = (143)(24)(456)$. To find the permutation, we start with 1 and follow the action of the cycles on it, starting from the right. The first and second cycles leave 1 alone, and the last cycle takes it to 4. Thus, $\pi_1(1) = 4$. For 2 we note that the first cycle leaves it alone, the second cycle takes it to 4, and the last cycle takes 4 to 3. Thus, $\pi_1(2) = 3$. Similarly, $\pi_1(3) = 1$, $\pi_1(4) = 5$, $\pi_1(5) = 6$, and $\pi_1(6) = 2$. Therefore,

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 5 & 6 & 2 \end{pmatrix}.$$

We note that π_1 is a cyclic permutation of length 6.

It is left to the reader to show that the permutation $\pi_2 \in S_5$ given by the product $\pi_2 = (13)(15)(12)(14)$ is cyclic: $\pi_2 = (14253)$.

The square of any transposition is the identity. Therefore, we can include it in any product of permutations without changing anything.

Proposition 23.4.8 *An r-cycle $(i_1, i_2, \ldots, i_r)$ can be decomposed into the product of $r-1$ transpositions*:

$$(i_1, i_2, \ldots, i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2).$$

Proof The proof involves keeping track of what happens to each symbol when acted upon by the RHS and the LHS and showing that the two give the same result. This is left as an exercise for the reader. □

Although the decomposition of Proposition 23.4.8 is not unique, it can be shown that the **parity** of the decomposition (whether the number of factors is even or odd) is unique. For instance, it is easy to verify that

parity of a permutation defined

$$(1234) = (14)(13)(12) = (14)\underbrace{(34)(34)}_{\mathbf{1}}\overbrace{(23)\underbrace{(12)(12)}_{\mathbf{1}}(23)}^{\mathbf{1}}(13)(12).$$

That is, (1234) is written as a product of 3 or 9 transpositions, both of which are odd.

We have already seen that any permutation can be written as a product of cycles. In addition, Proposition 23.4.8 says that these cycles can be further broken down into products of transpositions. This implies the following (see [Rotm 84, p. 38]):

parity of a permutation is unique

Proposition 23.4.9 *Any permutation can be decomposed as a product of transpositions. The parity of the decomposition is unique.*

Definition 23.4.10 A permutation is **even** (**odd**) if it can be expressed as a product of an even (odd) number of transpositions.

even and odd permutations

The parity of a permutation can be determined from its cycle structure and Proposition 23.4.8.

The reader may verify that the mapping from S_n to the multiplicative group of $\{+1, -1\}$ that assigns $+1$ to even permutations and -1 to odd permutations is a group homomorphism. It follows from the first isomorphism theorem (Theorem 23.2.16) that

Box 23.4.11 *The set of even permutations, denoted by A_n, forms a* normal *subgroup of S_n.*

This homomorphism is usually denoted by ϵ. We therefore define

$$\epsilon(\pi) \equiv \epsilon_\pi = \begin{cases} +1 & \text{if } \pi \text{ is even,} \\ -1 & \text{if } \pi \text{ is odd.} \end{cases} \tag{23.3}$$

Sometimes $\delta(\pi)$ or δ_π as well as $\text{sgn}(\pi)$ is also used. The symbol, $\epsilon_{i_1 i_2 \ldots i_n}$ used in the definition of determinants, is closely related to $\epsilon(\pi)$. In fact,

$$\epsilon_{\pi(1)\pi(2)\ldots\pi(n)} \equiv \epsilon_\pi .$$

Suppose $\pi, \sigma \in S_n$, and note that[8] $\sigma(i) \overset{\sigma^{-1}}{\longmapsto} i \overset{\pi}{\longmapsto} \pi(i) \overset{\sigma}{\longmapsto} \sigma \circ \pi(i)$, i.e., the composite $\sigma \circ \pi \circ \sigma^{-1}$ of the three permutations takes $\sigma(i)$ to $\sigma \circ \pi(i)$. This composite can be thought of as the permutation obtained by applying σ to the two rows of $\pi = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{smallmatrix}\right)$:

$$\sigma \circ \pi \circ \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma \circ \pi(1) & \sigma \circ \pi(2) & \cdots & \sigma \circ \pi(n) \end{pmatrix}.$$

In particular, the cycles of $\sigma \circ \pi \circ \sigma^{-1}$ are obtained by applying σ to the symbols in the cycles of π. Since σ is bijective, the cycles so obtained will remain disjoint. It follows that $\sigma \circ \pi \circ \sigma^{-1}$, a conjugate of π, has the same cycle structure as π itself. In fact, we have the following:

Theorem 23.4.12 *Two permutations are conjugate if and only if they have the same cycle structure.*

To find the distinct conjugacy classes of S_n, one has to construct distinct cycle structures of S_n. This in turn is equivalent to partitioning the numbers from 1 to n into sets of various lengths. Let ν_k be the number of k-cycles in a permutation. The cycle structure of this permutation is denoted

[8] Recall from Chap. 1 that $x \overset{f}{\longmapsto} y$ means $y = f(x)$.

by $(1^{\nu_1}, 2^{\nu_2}, \ldots, n^{\nu_n})$. Since the total number of symbols is n, we must have $\sum_{k=1}^{n} k\nu_k = n$. Defining $\lambda_j \equiv \sum_{k=j}^{n} \nu_k$, we have

$$\lambda_1 + \lambda_2 + \cdots + \lambda_n = n, \quad \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0. \tag{23.4}$$

partition of n

The splitting of n into nonnegative integers $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ as in Eq. (23.4) is called a **partition of** n. There is a 1–1 correspondence between partitions of n and the cycle structure of S_n. We saw how ν_k's gave rise to λ's. Conversely, given a partition of n, we can construct a cycle structure by $\nu_k = \lambda_k - \lambda_{k+1}$. For example, the partition (32000) of S_5 corresponds to $\nu_1 = 3 - 2 = 1$, $\nu_2 = 2 - 0 = 2$, i.e., one 1-cycle and two 2-cycles. One usually omits the zeros and writes (32) instead of (32000). When some of the λ's are repeated, the number of occurrences is indicated by a power of the corresponding λ; the partition is then written as $(\mu_1^{n_1}, \mu_2^{n_2}, \ldots, \mu_r^{n_r})$, where it is understood that λ_1 through λ_{n_1} have the common value μ_1, etc. For example, $(3^2 1)$ corresponds to a partition of 7 with $\lambda_1 = 3$, $\lambda_2 = 3$, and $\lambda_3 = 1$. The corresponding cycle structure is $\nu_1 = 0$, $\nu_2 = 2$, and $\nu_3 = 1$, i.e., two 2-cycles and one 3-cycle. The partitions of length 0 are usually ignored. Since $\sum \lambda_i = n$, no confusion will arise as to which symmetric group the partition belongs to. Thus (32000) and (332000) are written as (32) and $(3^2 2)$, and it is clear that (32) belongs to S_5 and $(3^2 2)$ to S_8.

Conjugacy classes of S_n are related to the partition of n.

Example 23.4.13 Let us find the different cycle structures of S_4. This corresponds to different partitions of 4. We can take $\lambda_1 = 4$ and the rest of the λ's zero. This gives the partition (4). Next, we let $\lambda_1 = 3$; then λ_2 *must* be 1, giving the partition (31). With $\lambda_1 = 2$, λ_2 can be either 2 or 1. In the latter case, λ_3 must be 1 as well, and we obtain two partitions, (2^2) and (21^2). Finally, if $\lambda_1 = 1$, all other nonzero λ's must be 1 as well (remember that $\lambda_k \geq \lambda_{k+1}$). Therefore, the last partition is of the form (1^4). We see that there are 5 different partitions of 4. It follows that *there are 5 different conjugacy classes in* S_4.

23.5 Problems

23.1 Let S be a subset of a group G. Show that S is a subgroup if and only if $ab^{-1} \in S$ whenever $a, b \in S$.

23.2 Show that the intersection of two subgroups is a subgroup.

a **word** on a subset of a group

23.3 Let X be a *subset* of a group G. A **word** on X is an element w of G of the form

$$w = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n},$$

where $x_i \in X$ and $e_i = \pm 1$. Show that the set of all words on X is a subgroup of G.

23.4 Let $[a, b]$ denote the commutator of a and b. Show that

(a) $[a,b]^{-1} = [b,a]$,
(b) $[a,a] = e$ for all $a \in G$, and
(c) $ab = [a,b]ba$. It is interesting to compare these relations with the familiar commutators of operators.

23.5 Show that if S is a subgroup, then $S^2 \equiv SS = S$, and $tS = S$ if and only if $t \in S$. More generally, $TS = S$ if and only if $T \subset S$.

23.6 Show that if S is a subgroup, then $Sa = Sb$ if and only if $ba^{-1} \in S$ and $ab^{-1} \in S$ ($aS = bS$ if and only if $a^{-1}b \in S$ and $b^{-1}a \in S$).

23.7 Let S be a subgroup of G. Show that $a \triangleright b$ defined by $ab^{-1} \in S$ is an equivalence relation.

23.8 Show that $C_G(x)$ is a subgroup of G. Let H be a subgroup of G and suppose $x \in H$. Show that $C_H(x)$ is a subgroup of $C_G(x)$.

23.9 (a) Show that the only element a in a group with the property $a^2 = a$ is the identity. (b) Now use $e_G \star e_G = e_G$ to show that any homomorphism maps identity to identity. (c) Show that if $f : G \to H$ is a homomorphism, then $f(g^{-1}) = [f(g)]^{-1}$.

23.10 Establish a bijection between the set of right cosets and the set of left cosets of a subgroup. Hint: Define a map that takes St to $t^{-1}S$.

23.11 Let G be a finite group and S one of its subgroups. Convince yourself that the union of all right cosets of S is G. Now use the fact that distinct right cosets are disjoint and that they have the same cardinality to prove that the order of S divides the order of G. In fact, $|G| = |S||G/S|$, where $|G/S|$ is the number of cosets of S (also called the index of S in G). This is **Lagrange's theorem**. Lagrange's theorem

23.12 Let $f : G \to H$ be a homomorphism. Show that $\phi : G/\ker f \to f(G)$ given by $\phi(g[\ker f]) \equiv \phi([\ker f]g) = f(g)$ is an isomorphism.

23.13 Let G' denote the commutator subgroup of a group G. Show that G' is a *normal* subgroup of G and that G/G' is abelian.

23.14 Let $M = \mathbb{R} \cup \{\infty\}$, and define an action of $SL(2,\mathbb{R})$ on M by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = \frac{ax+c}{bx+d}.$$

(a) Show that this is indeed a group action with a law of multiplication identical to the matrix multiplication.
(b) Show that the action is transitive.
(c) Show that beside identity, there is precisely one other element g of the group such that $g \cdot x = x$ for all $x \in M$.

(d) Show that for every $x \in M$,

$$G_x = \begin{pmatrix} a & b \\ bx^2 + (d-a)x & d \end{pmatrix}$$

23.15 Show that two conjugacy classes are either disjoint or identical.

23.16 Show that if all conjugacy classes of a group have only one element, the group must be abelian.

23.17 Consider a map from the conjugacy class of G containing $x \in G$ to the set of (left) cosets $G/C_G(x)$ given by $\phi(axa^{-1}) = aC_G(x)$. Show that ϕ is a bijection. In particular, show that $|C_G(x)| = |G|/|K_x^G|$ where K_x^G is the class in G containing x and $|K_x^G|$ its order (see Problem 23.11). Use this result and Problems 23.8 and 23.11 to show that $|H|/|K_x^H|$ divides $|G|/|K_x^G|$.

23.18 Show that $RR_{\hat{\mathbf{e}}}(\theta)R^{-1}$ corresponds to a rotation of angle θ. Hint: Consider the effect of rotation on the vectors in the plane perpendicular to $\hat{\mathbf{e}}$, and note that the rotated plane is perpendicular to $\hat{\mathbf{e}}' \equiv R\hat{\mathbf{e}}$.

23.19 Let G act on M and let $m_0 \in M$. Show that Gm_0 is the smallest invariant subset of M containing m_0.

23.20 Suppose G is the direct product of H_1 and H_2 and $g = h_1h_2$. Show that the factors h_1 and h_2 are unique and that H_1 and H_2 are normal.

23.21 Show that $(g, h), (g', h') \in G \times H$ are conjugate if and only if g is conjugate to g' and h is conjugate to h'. Therefore, conjugacy classes of the direct product are obtained by pairing one conjugacy class from each factor.

23.22 Find the products $\pi_1 \circ \pi_2$ and $\pi_2 \circ \pi_1$ of the two permutations

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 1 & 2 \end{pmatrix} \quad \text{and} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 5 & 4 \end{pmatrix}.$$

23.23 Find the inverses of the permutations

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 1 & 2 & 8 & 4 & 6 \end{pmatrix},$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 8 & 1 & 7 & 4 & 3 \end{pmatrix}$$

and show directly that $(\pi_1 \circ \pi_2)^{-1} = \pi_2^{-1} \circ \pi_1^{-1}$.

23.24 Find the inverse of each of the following permutations: $\pi_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{smallmatrix}\right)$, $\pi_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{smallmatrix}\right)$, $\pi_3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{smallmatrix}\right)$, and $\pi_4 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{smallmatrix}\right)$.

23.25 Express each of the following products in terms of disjoint cycles. Assume that all permutations are in S_7.

(a) $(123)(347)(456)(145)$. (b) $(34)(562)(273)$.

(c) $(1345)(134)(13)$.

23.26 Express the following permutations as products of disjoint cycles, and determine which are cyclic.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 6 & 2 \end{pmatrix}$, (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix}$,

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$.

23.27 Express the permutation $\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 3 & 6 & 8 & 7 & 5 \end{smallmatrix}\right)$ as a product of transpositions. Is the permutation even or odd?

23.28 Express the following permutations as products of transpositions, and determine whether they are even or odd.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$, (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 7 & 8 & 3 & 6 & 5 & 2 \end{pmatrix}$,

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

23.29 Show that the product of two even or two odd permutations is always even, and the product of an even and an odd permutation is always odd.

23.30 Show that π and π^{-1} have the same parity (both even or both odd).

23.31 Find the number of distinct conjugacy classes of S_5 and S_6.