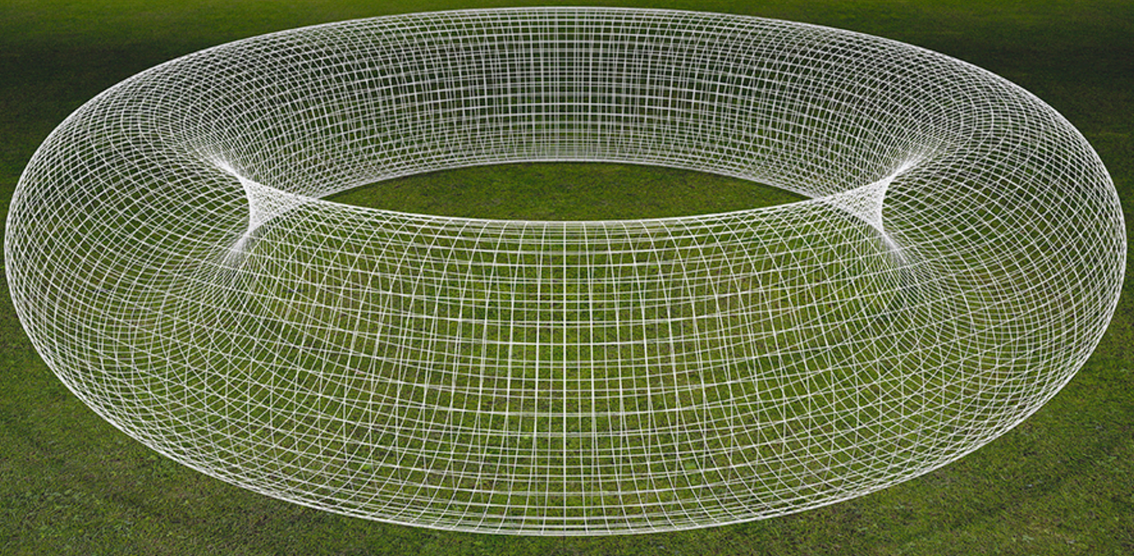
MATHEMATICAL METHODS FOR PHYSICS

An Introduction to Group Theory, Topology and Geometry



Esko Keski-Vakkuri, Claus Montonen and Marco Panero

Mathematical Methods for Physics

This detailed yet accessible text provides an essential introduction to the advanced mathematical methods at the core of theoretical physics. The book steadily develops the key concepts required for an understanding of symmetry principles and topological structures, such as group theory, differentiable manifolds, Riemannian geometry, and Lie algebras. Based on a course for senior undergraduate students of physics, it is written in a clear, pedagogical style and would also be valuable to students in other areas of science and engineering. The material has been subject to more than 20 years of feedback from students, ensuring that explanations and examples are lucid and considered, and numerous worked examples and exercises reinforce key concepts and further strengthen readers' understanding. This text unites a wide variety of important topics that are often scattered across different books, and provides a solid platform for more specialized study or research.

Esko Keski-Vakkuri received his Ph.D. in physics from Massachusetts Institute of Technology in 1995, and is currently a senior faculty member at the University of Helsinki. He has previously held positions at the California Institute of Technology and Uppsala University. His research is focused on string theory, black holes, holographic duality, and quantum information.

Claus K. Montonen received his Ph.D. from the University of Cambridge in 1974 and later held positions at the Université de Paris XI (CNRS), the Research Institute for Theoretical Physics, Helsinki, and CERN. He held various senior faculty positions in the Department of Physics at the University of Helsinki from 1978 until his retirement in 2011, where he was responsible for curriculum design in theoretical physics. His research interests are in S-matrix theory, string theory, and quantum field theory, having made major contributions to early string theory and duality in field and string theory.

Marco Panero received his Ph.D. in physics from the University of Turin in 2003, after which he held postdoctoral positions at the Dublin Institute for Advanced Studies, the University of Regensburg, ETH Zurich, the University of Helsinki, and the Autonomous University of Madrid. Since 2014 he has been an associate professor in physics at the University of Turin. His main research interests are in lattice field theory and in theoretical high-energy physics.

Mathematical Methods for Physics

An Introduction to Group Theory, Topology, and Geometry

ESKO KESKI-VAKKURI
University of Helsinki

CLAUS K. MONTONEN
University of Helsinki

MARCO PANERO
University of Turin

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University’s mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107191136

DOI: 10.1017/9781108120531

First published 2022

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication data
Names: Keski-Vakkuri, Esko, author. | Montonen, C. (Claus), author. |
Panero, Marco (Professor of physics), author.
Title: Mathematical methods for physics : an introduction to group theory,
topology and geometry / Esko Keski-Vakkuri, Claus Montonen, Marco Panero.
Description: Cambridge ; New York, NY : Cambridge University Press, 2022. |
Includes bibliographical references and index.
Identifiers: LCCN 2022016948 (print) | LCCN 2022016949 (ebook) |
ISBN 9781107191136 (hardback) | ISBN 9781108120531 (epub)
Subjects: LCSH: Mathematical physics. | BISAC: SCIENCE / Physics /
Mathematical & Computational
Classification: LCC QC20 .K437 2022 (print) | LCC QC20 (ebook) |
DDC 530.15–dc23/eng20220628
LC record available at https://lccn.loc.gov/2022016948
LC ebook record available at https://lccn.loc.gov/2022016949

ISBN 978-1-107-19113-6 Hardback

To Marika, Anne, and Juha

—Esko

To Leone

—Claus

To Saija, and to Mariangela and Giovanni

—Marco

Contents

1 Introduction

This textbook presents an introduction to a set of mathematical tools that are extensively used in modern physics, and is mainly aimed at advanced undergraduate, graduate, and doctoral students in physics, engineering, and mathematics. The reader is ideally accompanied on a journey through a number of different, albeit related, topics.

Chapter 2 introduces group theory and related notions, including, in particular, group homomorphisms and isomorphisms, before discussing in detail the group of permutations and some other particularly interesting finite groups. Then, the formalism of Young diagrams is introduced, and an alternative definition of groups in terms of their presentation is given. The rest of the chapter is devoted to continuous groups and to groups acting on a set.

The next chapter, Chapter 3, discusses the different representations that groups can have: After a brief reminder of linear-algebra concepts, the definition of group representations is formulated. Then, the discussion focuses on the concept of reducibility of group representations, which leads to a classification of irreducible representations. Group characters are introduced and their use in the classification of inequivalent irreducible representations is explained. The chapter also discusses the properties of the regular representation, which is induced by the action of the group on itself through a translation. The final part of the chapter introduces dual vectors and tensors, and an example of application of these notions for a spin-chain system of relevance in quantum physics and condensed-matter theory.

In Chapter 4 we first introduce the concepts that allow one to endow a generic set with a topology, then we define manifolds and, finally, differential manifolds. The chapter discusses in detail calculus on manifolds, differential forms and their integration, and finally presents a formulation of classical mechanics in terms of differential forms.

The following chapter, Chapter 5, is devoted to Riemannian geometry: Topics such as metric tensors, the induced metric, affine connections, connection coefficients, and their transformation properties under coordinate changes are discussed in detail. The chapter presents a thorough exposition of the concepts relevant for the general relativity theory of gravitation and for gauge theories, including parallel transport and holonomy, covariant derivatives, geodesics, curvature, and torsion. The final sections of the chapter are devoted to the discussion of isometries and Killing vector fields.

Chapter 6 presents a discussion of semisimple Lie algebras (highlighting their relevance for different physical applications, from quantum mechanics to the theory of elementary particles in and beyond the Standard Model) and their unitary representations. After defining the Lie algebras of the generators of Lie groups, we introduce the concepts of roots, weights, and Cartan generators, and present the systematic classification of the algebras associated with the classical and exceptional simple Lie groups with the corresponding Dynkin diagrams. The chapter also discusses in detail the explicit construction of irreducible representations for Lie algebras of special unitary groups, using tensor methods and Young diagrams. The last part of the chapter describes the representations of products of unitary groups (such as those that describe the gauge interactions between fundamental particles), and the Lorentz and Lorentz–Poincaré groups relevant for the theory of special relativity and for quantum field theory.

Finally, Appendix A presents detailed solutions for a subset of the problems included at the end of each of the previous chapters. Other solutions are made available to the course instructors through the website of Cambridge University Press.

The book is ideally suited for a university course on mathematical methods for physics; the main emphasis is on geometrical and topological concepts, which are essential for the understanding of the symmetry principles and topological structures in modern physics. The book is largely self-contained, but some important mathematical prerequisites are assumed: In particular, it is assumed that the reader is already familiar with the basics of real and complex analysis and linear algebra.

In writing this book, we put a very strong emphasis on the *pedagogical aspects*. The book is primarily targeted at physics and engineering students and, following M. David Merrill's *application principle* in instructional design (which states that learning is promoted when the learner applies the new knowledge), its goal is to enable them not only to learn a collection of fundamental notions in different branches of mathematical physics, but also to directly *apply* these tools to concrete problems. To this purpose, the final section of each chapter includes a large collection of original problems and exercises. As in actual scientific research, some of these problems stimulate the readers to combine tools which are relevant for the different subjects presented in the various chapters, and to keep a broad perspective – rather than adopting a narrow, hyperspecialized approach.

There are numerous sources that we have used in the preparation of this textbook. Our main inspiration and influence comes from this short list of classic works that we highly recommend for further reading on the subjects covered herein. We list them here, mentioning the chapters for which they are most relevant and highly recommended for further reading on the subjects:

- Important references for Chapters 2 and 3 are the books by Hugh F. Jones [6], by Michael Tinkham [13], and by Morton Hamermesh [4].
- For further reading about the topics of Chapters 4 and 5, we recommend the books by Mikio Nakahara [10], by Charles Nash and Siddhartha Sen [11], by John M. Lee [8], and by Jeffrey M. Lee [7], as well as the books on the theory of general relativity by Charles W. Misner, Kip S. Thorne, and John A. Wheeler [9], by Robert M. Wald [14], and by Sean M. Carroll [1].
- Useful references for further reading on the topics discussed in Chapter 6 are the books by Howard Georgi [2] and by Francesco Iachello [5]. The applications for elementary particle theory can be found in many excellent textbooks; our discussion of the symmetry representations of the Standard Model is closest to that in the book by Mark Srednicki [12].

We conclude this Introduction by thanking all of the students who have taken the course, on which this textbook is based, for helping us to present the topics of this book as clearly as we could. We also thank our former teaching assistants and our colleagues Antti Kupiainen and Jouko Mickelsson, who also taught these subjects, for additional inspiration, as well as Klaus Larjo and Niko Jokela for assistance in converting our original handwritten notes into electronic format. We also thank Jarkko Järvelä and Saga Säppi, who generously shared their solutions to some of the problems. In addition, we are indebted to many colleagues with whom we have discussed about and from whom we have learned the topics presented herein. Finally, we acknowledge with gratitude the careful work and patience of the editorial staff at Cambridge University Press, especially Sarah Armstrong, Elliot Beck, Henry Cockburn, Sapphire Duveau, Kuttappan Suresh Kumar, Sarah Lambert, Beverley Lawrence, Róisín Munnelly, Aparna Nair, Mathew Rohit, and in particular Nicholas Gibbons, who followed this book project from its beginning to its completion.

2 Group Theory

The first part of this chapter introduces the basic notions of group theory. Then we present a detailed discussion of some interesting finite groups. Next, we introduce Young diagrams and an alternative definition of a generic group in terms of its presentation. Finally, we discuss continuous groups and groups acting on a set.

2.1 Groups

2.1.1 Definitions: Groups, Abelian Groups, and Related Concepts

Consider an arbitrary set $G = \{a, b, \ldots\}$, and a composition law that, for every $a \in G$ and for every $b \in G$, assigns to the ordered pair (a, b) an element $a \cdot b$, which is also an element of G. Then, we define $(G, \cdot)$ to be a *group* if the following conditions simultaneously hold:

G1 (associativity): for all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
G2 (existence of the unit element): there is an element $e \in G$ such that for all $a \in G$: $a \cdot e = e \cdot a = a$;
G3 (existence of the inverse): for all $a \in G$ there is an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

In that case, the composition law is usually called the group *law of multiplication* (or *product*). We could have added an item **G0**: the composition law must be well defined. An attempt to define a product may not be consistent or well defined for all elements of the set. We will see examples of this later.

Moreover, we define an *Abelian group* as a group for which an additional condition holds:

AG4 (commutativity): for all $a, b \in G$: $a \cdot b = b \cdot a$.

Abelian groups are named after the Norwegian mathematician Niels Henrik Abel.

It is interesting to note that some different mathematical structures that share some properties with but are more general than groups can also be defined: For example, when the composition law is such that $\forall a \in G$ and $\forall b \in G$, one has $a \cdot b \in G$, but the properties **G1**–**G3** are not necessarily satisfied, then $(G, \cdot)$ is called a *magma*. A magma for which the associativity condition **G1** holds is called a *semigroup*. In addition, a semigroup for which also the condition **G2** is satisfied (i.e., a semigroup in which a unit element exists) is called a *monoid*. It turns out that groups have a much richer mathematical structure than magmas, semigroups, and monoids. In addition, groups have many more physics applications than magmas, semigroups, and monoids; hence, we will not discuss these more general structures in detail in this book, and we will primarily focus on groups.

Example Consider the set $G = \{e, a\}$ and the multiplication $\cdot$ defined as follows: $e \cdot e = e$, $a \cdot e = e \cdot a = a$, and $a \cdot a = e$. This is compatible with the group structure, e is the unit element, and a is the inverse of itself. The $(G, \cdot)$ group is called the *cyclic group of order* 2. It is an Abelian group, and is usually denoted as $\mathbb{Z}_2$. We will present a more general definition of cyclic groups in Section 2.4.

In the following, we will also use the simpler notation G rather than $(G, \cdot)$ to denote the group.

The number of elements in a set X is denoted by $|X|$. The number of elements $|G|$ in a group G is called the *order of the group*. If $|G|$ is finite, then G is said to be a *finite group*. We adopt some notations. We often drop the product symbol and write gh instead of $g \cdot h$ if there is no confusion. We also use the notation $g^n = g \cdots g$ for the product where g appears n times. For example, $g^2 = gg = g \cdot g, g^3 = ggg = g \cdot g^2$, etc. We then define the *order of the element* g to be the smallest positive number n such that $g^n = e$. For example, in $\mathbb{Z}_2$ the order of the element e is 1 and the order of a is 2.

The smallest finite group is called the *trivial group*: it contains only the unit element e, and thus has order 1. We denote the trivial group by $\mathbb{Z}_1$. The only multiplication that can be done among elements of this group is $e \cdot e = e$. There cannot be a group of order 0, because, in order to satisfy the property **G2**, a group must necessarily contain at least the unit element. A possible way to characterize a generic finite group is by means of its *Cayley table* (or *multiplication table*), named after the British mathematician Arthur Cayley. It is a square table, of size equal to the order of the group, listing all the products of the group elements. In particular, the entries of the Cayley table of a finite group are the products $p \cdot q$, where p is one of the group elements listed in the column on the left of the table, and q is one of the group elements listed in the row at the top of the table. Table 2.1 gives the Cayley table of $\mathbb{Z}_2$ as an example.

If $|G|$ is not finite, but G is a discrete set (i.e., a set whose elements can be put in one-to-one correspondence with the natural numbers), then $(G, \cdot)$ is called a *discrete group*. Conversely, when G is a continuous set, $(G, \cdot)$ is a called a *continuous group*.

Comments

1. The unit element of any group is unique. If both e and e' are unit elements, then $ee' = e'$ (because e is an unit element) and at the same time $ee' = e$ (because e' is an unit element). Therefore $e' = ee' = e$, so $e = e'$.

Table 2.1. The Cayley table of $\mathbb{Z}_2$

	e	a
e	e	a
a	a	e

2. For a given group, the inverse element of any element is unique. If both b and b' are inverse elements of a, then $ba = e$ and $ab' = e$. But then $bab' = eb'$, hence $b = b'$.
3. Note that, by definition, the unit element commutes with all elements of the group; however, the unit element is not necessarily the only element with this property. The subset of group elements that commute with all elements of the group is called the *center of the group*. The center of a group is always an Abelian group; if it contains only the unit element, then the group is said to have a *trivial center*.
4. The definition of a group, essentially, is the definition of the group multiplication among all possible ordered pairs of group elements, while the nature of the elements in the set G does not necessarily have to be specified.

The latter point means that the definition of a group is abstract. Specifying the nature of the set of group elements corresponds to defining a particular *realization* of the group. More precisely, a realization of an abstract group G is a map from G to a particular set, on which an internal binary operation exists, that satisfies the properties defining the group.

Example Consider the cyclic group of order 2 introduced above, $\mathbb{Z}_2$, with e as the unit element and a as the other element. Examples of realizations of $\mathbb{Z}_2$ include the following:

- Take $e = 0$, $a = 1$, and addition modulo 2 to be the group multiplication. It is trivial to show that $(\{0, 1\}, + \bmod 2)$ is an explicit realization of the abstract $\mathbb{Z}_2$ group structure defined above; it has the multiplication table as shown in Table 2.1.
- Take $e = 1$, $a = -1$, and the ordinary multiplication as the group multiplication. Also in this case, one can immediately show that $(\{1, -1\}, \cdot)$ is a realization of the $\mathbb{Z}_2$ group.
- Consider the set of truth variables of Boolean algebra, $\{\texttt{FALSE}, \texttt{TRUE}\}$, and the binary operator XOR ("exclusive or") as the group multiplication. Recalling that p XOR q is TRUE when p is TRUE and q is FALSE, or vice versa, while it is FALSE when p and q are both TRUE or both FALSE, one can explicitly check that the $\mathbb{Z}_2$ group structure is realized by identifying e = FALSE and a = TRUE.

A particularly important class of realizations of a group are those in which the group elements are associated with linear transformations among the elements of a vector space: Such realizations are called *representations*, and will be discussed thoroughly in Chapter 3.

It is also interesting to consider groups that are constructed by taking Cartesian pairs of elements from other groups. Given two groups G_1 and G_2, their *direct product* $G_1 \times G_2$ is defined as the set of all ordered pairs (g_1, g_2), with $g_1 \in G_1$ and $g_2 \in G_2$, with the multiplication $(g_1, g_2) \cdot (g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$, where $g_1 g'_1$ is computed using the group multiplication of G_1, while $g_2 g'_2$ is computed using the group multiplication of G_2.

It is straightforward to prove that $G_1 \times G_2$ is a group itself; in particular, its unit element is (e_1, e_2), where e_1 is the unit element of G_1 and e_2 is the unit element of G_2, and the inverse element of a generic element (g_1, g_2) is (g_1^{-1}, g_2^{-1}). It is also trivial to see that, if both G_1 and G_2 are finite, so is $G_1 \times G_2$, and its order is $|G_1 \times G_2| = |G_1||G_2|$.

Similarly, one can also define the direct product of three or more groups.

Partly for historical reasons, several groups are defined from (and, sometimes, named after) their explicit realization in sets of numbers or of transformations of a vector space, by a process of *abstraction*, i.e., by focusing on the way the group multiplication acts on ordered pairs of elements, leaving the nature of the group elements (or, in fact, of the group multiplication itself) unspecified.

2.1.2 Examples of Groups

The definitions introduced above can be easily elucidated by some examples of groups:

- $\mathbb{Z}$, the set of integers, with $+$ (addition) as the multiplication law, is a discrete Abelian group. The "unit" element is 0, and, for any element $a \in \mathbb{Z}$, the inverse is $-a$.
- Similarly, $\mathbb{R}$, the set of real numbers, with the addition as the multiplication law, is a continuous Abelian group. Again, the "unit" element e is 0.
- $\mathbb{R}_0 = \mathbb{R} \setminus \{0\}$, the set of real, nonzero numbers, with $\cdot$ (multiplication) as the multiplication law, is a continuous Abelian group. The unit element is $e = 1$, and the inverse of a generic element g is $1/g$. In this case, the set of group elements was defined by removing 0, in order to ensure that all elements have an inverse.
- For any positive integers n and m, the set of $n \times m$ matrices with real entries, with the matrix addition as the group multiplication, forms a continuous Abelian group. The unit element of this group is the $n \times m$ matrix whose entries are all equal to 0, while, for a generic matrix M of elements M_{ij}, the inverse element has entries $-M_{ij}$. Note that, in practice, this group consists of nm independent copies of $(\mathbb{R}, +)$.
- For any positive integer n, the set of real square matrices of size n and nonvanishing determinant, with the matrix product as the group multiplication, forms a continuous group denoted by $\mathrm{GL}(n, \mathbb{R})$. The unit element is the identity matrix $\mathbb{1}$ (of elements $\mathbb{1}_{b,c} = \delta_{b,c}$), and the fact that the set includes only matrices M with $\det M \neq 0$ implies that the inverse matrix M^{-1} exists for any M in the set. In contrast to the previous example, this group is not Abelian (except for $n = 1$).
- Given a regular polygon of n sides, the set of geometric transformations that leave the polygon invariant forms the dihedral group D_n. This group includes n rotations and n reflections. For n odd, the reflections leaving the polygon invariant are about axes going through each of the polygon vertices, the center, and the midpoint of the opposite side, whereas for n even, there are $\frac{n}{2}$ reflections about axes going through opposite vertices and $\frac{n}{2}$ reflections about axes going through the midpoints of opposite sides. The dihedral groups D_n are finite groups of order $|D_n| = 2n$, and they are non-Abelian for all $n > 2$.
- Consider linear transformations of an orthonormal reference frame in the two-dimensional real vector space $\mathbb{R}^2$. They can be represented by real matrices of size 2×2, having (the components of) the vectors of the transformed reference frame as columns. If the transformations are required to preserve the orthonormality of the reference frame, then the columns of the matrix have to be orthogonal to each other, and normalized to 1. The most general form of the matrix is then

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \mp\sin\alpha & \pm\cos\alpha \end{pmatrix}, \qquad \alpha \in \mathbb{R}. \tag{2.1}$$

In the set of these transformations one can define an internal composition law, as the operation of applying two such transformations one after the other; it corresponds to the matrix product and satisfies the requirements of a group multiplication. The unit element of the group is the 2×2 identity matrix, and the inverse of a generic element of the group is obtained by taking the transpose of the original matrix. This is the orthogonal group of dimension 2, denoted as $\mathrm{O}(2, \mathbb{R})$ (or, more concisely, as $\mathrm{O}(2)$); it is the group of transformations of the two-dimensional Euclidean space, that preserve a fixed point and the length of vectors.

2.1.3 Examples of Sets That Are Not Groups

It is also instructive to list some examples of structures $(G, \cdot)$ that are *not* groups:

1. $\mathbb{N}$, the set of natural numbers, with addition as the "multiplication" is not a group, because no element (except for 0) admits an inverse in the group. $(\mathbb{N}, +)$ is, however, a monoid, because the addition is internal in $\mathbb{N}$ (the sum of any two natural numbers is a natural number) and is an associative operation, which admits the number 0 as the "unit element."
2. Consider the three-dimensional real vector space $\mathbb{R}^3$, and the multiplication law defined as the cross-product of vectors, namely $a \cdot b = a \times b$, that is, $(a \cdot b)_i = \sum_{j,k=1}^{3} \epsilon_{ijk} a_j b_k$, where $\epsilon_{ijk} = 1$ for $i = 1, j = 2$, and $k = 3$, and it is totally antisymmetric under the interchange of any pair of the indices (which, in particular, implies that $\epsilon_{ijk} = 0$ when at least two indices are equal). Since this multiplication law is internal in $\mathbb{R}^3$, it endows $\mathbb{R}^3$ with the structure of a magma. Given that this multiplication law is not associative, this magma is not a semigroup.
3. $\mathbb{R}^3$ with the multiplication law defined by the scalar product of vectors, namely $(a \cdot b) = \sum_{i=1}^{3} a_i b_i$, is not even a magma (because the multiplication law is not an internal operation in $\mathbb{R}^3$; the result of $a \cdot b$ is a real number, not a three-dimensional real vector).
4. For any positive integer n, the set of real square matrices of size n and nonvanishing determinant, with matrix addition as the group multiplication, is not a magma. For a generic element M (with entries $M_{b,c}$) in this set, the matrix N of entries $N_{b,c} = -M_{b,c}$ has determinant $(-1)^n \cdot \det M$, which is nonvanishing because $\det M \neq 0$, hence N also belongs to the set. But $(M + N)$ is the zero matrix, which is not in the set, because its determinant vanishes.

2.2 Subgroups

The concept of subgroup is a particularly important one in the theory of groups (and in its mathematical and physical applications). In short, a subgroup is a subset H of a group G, that is itself a group, with the same composition law as G.

More formally, a subset H of the group G is called a *subgroup* of G if it is closed under the group multiplication, i.e., $\forall h_1, h_2 \in H$ one has $h_1 \cdot h_2 \in H$, and if the inverse of each of its elements is also in H, i.e., $\forall\ h \in H$ also $h^{-1} \in H$.

Note that every subgroup of G must contain at least the unit element e of G.

A subgroup H of a group G is said to be a *trivial subgroup* if it contains only the unit element ($H = \{e\}$) or if it coincides with G itself ($H = G$). Every group admits at least these two trivial subgroups as subgroups. (For the trivial group $\mathbb{Z}_1$ the two coincide.)

Conversely, a subgroup H of a group G is said to be a *proper subgroup* if it is not trivial, i.e., if $H \neq \{e\}$ and $H \neq G$. If H is a proper subgroup of a finite-order group G, then $1 < |H| < |G|$.

A subgroup H of a group G is said to be a *normal subgroup* when, for all $h \in H$ and for all $g \in G$, the product $g \cdot h \cdot g^{-1}$ is also an element of H.

A group G that does not have proper normal Abelian subgroups is said to be a *semisimple group*; if it does not have proper normal subgroups, then it is said to be a *simple group*. Clearly, every simple group is also semisimple (but the converse is not true, as there exist semisimple groups which are not simple).

2.3 Group Homomorphisms and Isomorphisms

Two finite groups are “the same” (up to a relabeling of the elements of the groups) if they have the same Cayley table. We will introduce another technical notion to decide when two groups can be identified. For the comparison, we define maps from one group to another that preserve the group structure, mapping products to products of image elements. These maps are called group homomorphisms and group isomorphisms. Before defining them and discussing their properties, we introduce some further notions.

Given an arbitrary non-empty set X, a binary relation (denoted by $\diamond$) among elements of X is said to be an *equivalence relation* when it is simultaneously reflexive ($\forall x \in X$: $x \diamond x$), symmetric ($\forall x$, $y \in X$: $x \diamond y$ implies $y \diamond x$), and transitive ($\forall x$, y, $z \in X$: if $x \diamond y$ and $y \diamond z$, then $x \diamond z$).

Given a set X and an equivalence relation $\diamond$ among its elements, the *equivalence class* of a generic element $a \in X$ is the subset of X containing all elements x such that $x \diamond a$ holds, and is denoted as $[a]$. Then, any element belonging to $[a]$ is called a *representative* of that equivalence class. Note that, given any element $a \in X$, the equivalence class $[a]$ is non-empty, because the reflexivity of the equivalence relation $\diamond$ implies that $[a]$ contains at least a itself. Moreover, the following fact holds:

Theorem 2.1 *Any equivalence relation $\diamond$ defined in a set X partitions it into mutually disjoint equivalence classes.*

Proof Consider two distinct equivalence classes $[a]$ and $[b]$. Then, unless $[a]$ is a strict subset of $[b]$, there exists at least one element, say c, which belongs to $[a]$ (so that $c \diamond a$) but not to $[b]$. If $[a]$ and $[b]$ are non-disjoint, then $[a] \cap [b] \neq \emptyset$. Then, let d be an element of $[a] \cap [b]$: Since $d \in [a]$, it follows that $d \diamond a$. Then, the symmetry and transitivity of $\diamond$ imply that $c \diamond d$. On the other hand, since $d \in [b]$, it also follows that $d \diamond b$. Then, the transitivity of $\diamond$ implies that $c \diamond b$, i.e., $c \in [b]$, in contradiction with the assumption that c is not in b. Finally, if $[a]$ is a strict subset of $[b]$, the same argument can be applied by interchanging $[a]$ and $[b]$. □

Given a set X and an equivalence relation $\diamond$ among the elements of X, the *quotient space* induced by $\diamond$ is defined as the set of all equivalence classes into which $\diamond$ partitions X, and is denoted as $X/\diamond$.

Given two arbitrary, non-empty sets X and Y, let $\mathrm{Map}(X, Y)$ denote the set of functions (or “mappings”) from X to Y:

$$\mathrm{Map}(X, Y) = \{f : X \to Y \,|\, \forall x \in X : \exists! f(x) \in Y\}. \tag{2.2}$$

Within $\mathrm{Map}(X, Y)$, there exist special types of functions.

- A function $f : X \to Y$ is called an *injection* (or a *one-to-one function*) if $f(x) \neq f(x')$ $\forall x \neq x'$.
- A function $f : X \to Y$ is called a *surjection* (or an *onto function*) if $\forall y \in Y$ there exists at least one $x \in X$, such that $f(x) = y$.
- A function $f : X \to Y$ is called a *bijection* if it is both an injection and a surjection.

If a function f is a bijection, then it is *invertible*, namely one can construct the *inverse function* $f^{-1} : Y \to X$, defined by the property that, for any $x \in X$, one has $f^{-1}(f(x)) = x$. In particular, the fact that f is a surjection implies that, for any $y \in Y$, $f^{-1}(y)$ can be defined, while the fact that f is an injection implies that $f^{-1}(y)$ is *uniquely* defined. Furthermore, f^{-1} is a bijection, too, and the inverse function of f^{-1} is f.

Example Consider a set of apples, $A = \{a_1, a_2, a_3\}$, and a set of oranges, $O = \{o_1, o_2, o_3\}$. A mapping $f(a_1) = f(a_2) = o_1$, $f(a_3) = o_2$ is not an injection, a mapping $g(a_1) = o_2$, $g(a_2) = o_3$, $g(a_3) = o_1$ is both an injection and a surjection, hence a bijection. The inverse map is $g^{-1}(o_1) = a_3$, $g^{-1}(o_2) = a_1$, $g^{-1}(o_3) = a_2$.

In general, a mapping $f : X \to Y$ is generally called a *homomorphism* when it preserves some structure. A homomorphism that is a bijection is called an *isomorphism*. In the following, we will be particularly interested in homomorphisms and isomorphisms between groups, which can be defined as follows.

Given two groups $(G, \cdot)$ and $(H, \bullet)$, a homomorphism $f : G \to H$ is called a *group homomorphism* if it preserves the group multiplication, i.e., if $\forall g_1, g_2 \in G$ one has $f(g_1 \cdot g_2) = f(g_1) \bullet f(g_2)$. When a group homomorphism f is bijective, it is called a *group isomorphism*. Two groups G and H are said to be *isomorphic* ($G \cong H$) if there exists at least a group isomorphism between them.

The relation of isomorphism among groups is an equivalence relation in the set of groups, because the relation of isomorphism among groups is reflexive (every group is isomorphic to itself; the identity mapping is the isomorphism that proves this), symmetric (if $f : G \to H$ is a isomorphism, then $\exists f^{-1} : H \to G$, which is also an isomorphism), and transitive (given two isomorphism $f : G \to H$ and $l : H \to K$, the composite map $l \circ f$ is an isomorphism from G to K).

Isomorphic groups have the same structure, so they can be identified. More precisely, each abstract group can be identified with an equivalence class defined by the equivalence relation of group isomorphism.

Example Take the two groups $G = (\mathbb{R}_+, \cdot)$ and $H = (\mathbb{R}, +)$. Define the mapping

$$f : G \to H, \quad f : x \to f(x) = \ln x. \tag{2.3}$$

Note that f is a group homomorphism, because $f(xy) = \ln(xy) = \ln x + \ln y = f(x) + f(y)$. In fact, f is also a group isomorphism, because it is a bijection, the inverse mapping being $f^{-1}(x) = e^x$.

2.4 The Smallest Finite Groups

Finite groups have several applications in physics. A classic example is in solid state physics, where they are used to classify general crystal structures (the so-called crystallographic point groups). In addition, they also have applications in classical mechanics, where they can be used to reduce the number of relevant degrees of freedom in systems with certain symmetries, as well as in many different areas of modern physics.

For certain (sufficiently small) finite sets, the requirements that a binary operation on the set elements has to satisfy, in order to be a group multiplication, are so constraining that they uniquely define the group. In this section, we present the list of all groups of finite order $N \leq 6$. Note that, since every group must contain at least the unit element, the order of the group is at least 1.

- **Order** $N = 1$**:** This is the trivial group $G = \{e\}$, containing only the unit element (which, by definition, is the inverse of itself).
- **Order** $N = 2$**:** In this case $G = \{e, a\}$, with $a \neq e$. The definition of the unit element implies that $e^2 = e$, $ea = ae = a$. The only remaining multiplication is a^2: To ensure that the multiplication is a closed operation in the group, the result must be either e or a. However, if $a^2 = a$, then $a = ae = a(aa^{-1}) = a^2a^{-1} = aa^{-1} = e$, in contradiction with the assumption that a and e are distinct. So the only possibility is $a^2 = e$. Accordingly, the Cayley table of the group of order 2 is uniquely fixed to be

$$\begin{array}{c|cc} & e & a \\ \hline e & e & a \\ a & a & e \end{array}\ . \tag{2.4}$$

  This is the $\mathbb{Z}_2$ group that we already introduced. One of its realizations, in addition to those already mentioned, is in terms of one the symmetric groups (that will be defined and discussed in detail in Section 2.5 and that contain permutations interchanging the group elements), the symmetric group of degree 2, $S_2 = \text{Perm}(\{1, 2\})$. Clearly, S_2 contains only two permutations: The identity permutation E, which leaves the order of the elements unchanged, and the permutation that interchanges them, which can be denoted as A, and which, in cycle notation, can be written as $(1, 2)$. It is easy to prove that S_2 is isomorphic to $\mathbb{Z}_2$: For example, considering the realization of $\mathbb{Z}_2$ in terms of $\{1, -1\}$ (with the ordinary product as the group multiplication), one can define the mapping $f : \mathbb{Z}_2 \to S_2$, such that $f(1) = E, f(-1) = A$. It is easy to see that f is a group isomorphism, so $\mathbb{Z}_2 \cong S_2$.

- **Order** $N = 3$**:** Consider the set $G = \{e, a, b\}$, assuming that both a and b are distinct from the unit element e, and that $a \neq b$. It turns out that, again, there is only one possible abstract group of order 3. This abstract group can be determined by working out its Cayley table:

$$\begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & ? & ? \\ b & b & ? & ? \end{array} . \tag{2.5}$$

Consider ab, and suppose it is equal to b. But then $a = a(bb^{-1}) = (ab)b^{-1} = bb^{-1} = e$, which contradicts the assumption that e, a, and b are all different. Similarly, if $ab = a$, then one would have $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}a = e$, again in contradiction with the assumption that e and b are different. So it must be $ab = e$. Analogously, one can prove that $ba = e$. These two equalities imply that a is the inverse of b (and vice versa). Then, consider a^2: If it were equal to a, then one would have $a = a(aa^{-1}) = a^2a^{-1} = aa^{-1} = e$, in contradiction to the assumption that $a \neq e$. Similarly, if $a^2 = e$, then one would have $b = eb = a^2b = a(ab) = ae = a$, contradicting the assumption that $a \neq b$. Thus, it must necessarily be $a^2 = b$. Similarly, one can show that $b^2 = a$. The complete Cayley table for the group of three elements reads as follows:

$$\begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array} . \tag{2.6}$$

This group is called $\mathbb{Z}_3$. Since $b = a^2$, one has $\mathbb{Z}_3 = \{e, a, a^2\}$. $\mathbb{Z}_3$ and $\mathbb{Z}_2$ (and, in fact, also the trivial group containing only the unit element) are examples of *cyclic groups*.

More in general, the *cyclic group* of order N, denoted as $\mathbb{Z}_N$, is defined as a finite group in which each element can be written as a power of a single *generating element* a.

Thus, the generic cyclic group of order N is

$$\mathbb{Z}_N = \{e, a, a^2, \ldots, a^{N-1}\}, \tag{2.7}$$

where the unit element is $e = a^0$, while the inverse of a generic element a^p is a^{N-p}. Note that a cyclic group can be defined for any order $N \geq 1$. Since $a^p \cdot a^q = a^{p+q (\text{mod } N)} = a^q \cdot a^p$ for any p and q, all cyclic groups are Abelian. One realization of cyclic groups is given by the complex Nth roots of 1: $\mathbb{Z}_N = \{\exp(2\pi ik/N), \text{ for } k = 0, 1, \ldots, N-1\}$, with the usual product as group multiplication. Thinking about the representation of the roots of 1 in the complex plane, this realization also reveals a geometric interpretation of $\mathbb{Z}_N$: It is the symmetry group of rotations of a regular directed polygon with n sides. It is trivial to prove that the set $\{0, 1, \ldots, N-1\}$, with the addition modulo N as the group multiplication, provides another realization of $\mathbb{Z}_N$.

- **Order** $N = 4$**:** Since cyclic groups $\mathbb{Z}_N$ are defined for any positive integer N, we can immediately construct a finite group of order 4, namely $\mathbb{Z}_4 = \{e, a, a^2, a^3\}$. Its Cayley table is

$$\begin{array}{c|cccc} & e & a & a^2 & a^3 \\ \hline e & e & a & a^2 & a^3 \\ a & a & a^2 & a^3 & e \\ a^2 & a^2 & a^3 & e & a \\ a^3 & a^3 & e & a & a^2 \end{array} . \tag{2.8}$$

However, there exists also a different group of order 4: the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$. Denoting $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{f, b\} \times \{g, c\}$, with f and g the unit elements of the two groups, $b^2 = f$ and $c^2 = g$, the set of elements of this group can be written as $\{(f, g), (f, c), (b, g), (b, c)\}$. Note that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is an Abelian group, but it is different from $\mathbb{Z}_4$, because it is not a cyclic group. In particular, the elements (f, c) and (b, g) are not powers of the same element. Neither of the two is a power of the other, and they are not powers of the remaining two elements of the group either (by definition, any power of the unit element (f, g) is equal to itself, while all even powers of (b, c) are equal to the unit element, and all odd powers are equal to (b, c) itself). The Cayley table of $\mathbb{Z}_2 \times \mathbb{Z}_2$ can easily be worked out to be

$$\begin{array}{c|cccc} & (f,g) & (f,c) & (b,g) & (b,c) \\ \hline (f,g) & (f,g) & (f,c) & (b,g) & (b,c) \\ (f,c) & (f,c) & (f,g) & (b,c) & (b,g) \\ (b,g) & (b,g) & (b,c) & (f,g) & (f,c) \\ (b,c) & (b,c) & (b,g) & (f,c) & (f,g) \end{array} \tag{2.9}$$

and it is different from that of $\mathbb{Z}_4$. The $\mathbb{Z}_2 \times \mathbb{Z}_2$ group is also called *Vierergruppe* (and denoted by V_4) or *Klein four-group*, after the German mathematician Christian Felix Klein. Considering that the trivial group can be identified with $\mathbb{Z}_1$, the Klein four-group is the smallest noncyclic finite group. It is possible to show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are the only two groups of order 4.

- **Order** $N = 5$**:** The only finite group of order $N = 5$ is the cyclic group $\mathbb{Z}_5 = \{e, a, a^2, a^3, a^4\}$.
- **Order** $N = 6$**:** At order $N = 6$, there exist two non-isomorphic finite groups: One of them is the cyclic group $\mathbb{Z}_6 = \{e, a, a^2, a^3, a^4, a^5\}$, whose Cayley table is

$$\begin{array}{c|cccccc} & e & a & a^2 & a^3 & a^4 & a^5 \\ \hline e & e & a & a^2 & a^3 & a^4 & a^5 \\ a & a & a^2 & a^3 & a^4 & a^5 & e \\ a^2 & a^2 & a^3 & a^4 & a^5 & e & a \\ a^3 & a^3 & a^4 & a^5 & e & a & a^2 \\ a^4 & a^4 & a^5 & e & a & a^2 & a^3 \\ a^5 & a^5 & e & a & a^2 & a^3 & a^4 \end{array} . \tag{2.10}$$

Interestingly, the $\mathbb{Z}_6$ group turns out to be isomorphic to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. Denoting $\mathbb{Z}_2 = \{f, b\}$ (with f the unit element and $b^2 = f$) and $\mathbb{Z}_3 = \{g, c, c^2\}$ (with g the unit element and $c^3 = g$), the Cayley table of $\mathbb{Z}_2 \times \mathbb{Z}_3$ reads

$$\begin{array}{c|cccccc}
 & (f,g) & (f,c) & (f,c^2) & (b,g) & (b,c) & (b,c^2) \\
\hline
(f,g) & (f,g) & (f,c) & (f,c^2) & (b,g) & (b,c) & (b,c^2) \\
(f,c) & (f,c) & (f,c^2) & (f,g) & (b,c) & (b,c^2) & (b,g) \\
(f,c^2) & (f,c^2) & (f,g) & (f,c) & (b,c^2) & (b,g) & (b,c) \\
(b,g) & (b,g) & (b,c) & (b,c^2) & (f,g) & (f,c) & (f,c^2) \\
(b,c) & (b,c) & (b,c^2) & (b,g) & (f,c) & (f,c^2) & (f,g) \\
(b,c^2) & (b,c^2) & (b,g) & (b,c) & (f,c^2) & (f,g) & (f,c)
\end{array} \; . \tag{2.11}$$

An isomorphism relating this group to $\mathbb{Z}_6$ is the one mapping the generic element $(b^p, c^q) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ to the element $a^{(3p+4q) \bmod 6} \in \mathbb{Z}_6$: So, for example, $(f, c) = (b^0, c^1)$ corresponds to a^4, while $(b, c^2) = (b^1, c^2)$ is mapped to a^5. The product $(f, c) \cdot (b, c^2) = (b, g) = (b^1, c^0)$ is mapped to a^3, and this is consistent with the fact that the isomorphism preserves the group product, as $a^4 \cdot a^5 = a^3$ in $\mathbb{Z}_6$.

In addition to $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, there exists another, non-isomorphic, finite group of order 6: the symmetric group S_3, which is the smallest non-Abelian group (and which coincides with D_3, the group of symmetries of an equilateral triangle). Its elements can be written as: $\{e, a, b, aba, ab, ba\}$ and they satisfy $a^2 = b^2 = (ab)^3 = (ba)^3 = e$, with e the unit element. Note that these properties imply $aba = bab$. The Cayley table of S_3 is

$$\begin{array}{c|cccccc}
 & e & a & b & aba & ab & ba \\
\hline
e & e & a & b & aba & ab & ba \\
a & a & e & ab & ba & b & aba \\
b & b & ba & e & ab & aba & a \\
aba & aba & ab & ba & e & a & b \\
ab & ab & aba & a & b & ba & e \\
ba & ba & b & aba & a & e & ab
\end{array} \; . \tag{2.12}$$

Note that the non-Abelian nature of the group is reflected in the fact that the Cayley table is not symmetric under reflection about the diagonal.

- **Order** $N = 7$**:** The only finite group of order $N = 7$ is the cyclic group $\mathbb{Z}_7 = \{e, a, a^2, a^3, a^4, a^5, a^6\}$.
- **Order** $N = 8$**:** There exist five non-isomorphic finite groups of order 8; three of them are Abelian: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The remaining two groups of order 8 are non-Abelian. One of them is the dihedral group D_4, which can be interpreted as the symmetry group of a square: It consists of four rotations by angles which are integer multiples of $\pi/2$, two reflections about axes going through the midpoints of pairs of opposite sides, and two reflections about the diagonals of the square. The group elements can be written as $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where e is the unit element and $a^4 = b^2 = (ab)^2 = e$. In terms of transformations that leave a square invariant, a can be interpreted as a rotation by $\pi/2$ and b as a reflection about the axis going through the midpoints of two opposite sides. The Cayley table of D_4 is

$$\begin{array}{c|cccccccc}
 & e & a & a^2 & a^3 & b & ab & a^2b & a^3b \\
\hline
e & e & a & a^2 & a^3 & b & ab & a^2b & a^3b \\
a & a & a^2 & a^3 & e & ab & a^2b & a^3b & b \\
a^2 & a^2 & a^3 & e & a & a^2b & a^3b & b & ab \\
a^3 & a^3 & e & a & a^2 & a^3b & b & ab & a^2b \\
b & b & a^3b & a^2b & ab & e & a^3 & a^2 & a \\
ab & ab & b & a^3b & a^2b & a & e & a^3 & a^2 \\
a^2b & a^2b & ab & b & a^3b & a^2 & a & e & a^3 \\
a^3b & a^3b & a^2b & ab & b & a^3 & a^2 & a & e
\end{array} . \tag{2.13}$$

The last finite group of order 8 is the non-Abelian *quaternion group* $Q_8 = \{\pm e, \pm i, \pm j, \pm k\}$, where e is the unit element, and $i^2 = j^2 = k^2 = ijk = -e$. The Cayley table of Q_8 is

$$\begin{array}{c|cccccccc}
 & e & -e & i & -i & j & -j & k & -k \\
\hline
e & e & -e & i & -i & j & -j & k & -k \\
-e & -e & e & -i & i & -j & j & -k & k \\
i & i & -i & -e & e & k & -k & -j & j \\
-i & -i & i & e & -e & -k & k & j & -j \\
j & j & -j & -k & k & -e & e & i & -i \\
-j & -j & j & k & -k & e & -e & -i & i \\
k & k & -k & j & -j & -i & i & -e & e \\
-k & -k & k & -j & j & i & -i & e & -e
\end{array} . \tag{2.14}$$

If one identifies i, j, and k with the unit vectors defining a right-handed reference frame in the three-dimensional real vector space $\mathbb{R}^3$, then the group multiplication between these elements is consistent with the cross-product when they are distinct (and do not differ simply by a sign): $ij = k$, and cyclic permutations thereof. Note, however, that in $\mathbb{R}^3$ the cross-product of a vector with itself (or with its opposite) vanishes, whereas this is not the case for the group multiplication in Q_8. Q_8 has four proper subgroups

$$\{e, -e\} \cong \mathbb{Z}_2, \tag{2.15}$$

$$\{e, i, -e, -i\} \cong \mathbb{Z}_4, \tag{2.16}$$

$$\{e, j, -e, -j\} \cong \mathbb{Z}_4, \tag{2.17}$$

$$\{e, k, -e, -k\} \cong \mathbb{Z}_4, \tag{2.18}$$

all of which are normal subgroups.

2.5 Permutations, the Symmetric Group, and Cayley's Theorem

Consider again Map(X, Y), the set of mappings from a generic set X to another generic set Y. If the two sets coincide, then Map(X,X) can be endowed with a semigroup structure, by taking the composition of maps as the composition law:

$$fg = f \circ g, \qquad (f \circ g)(x) = f\big(g(x)\big) \quad \text{for } \forall x \in X. \tag{2.19}$$

Note that the composition is well defined only if $X = Y$, because g is a map from X to Y, but the domain of f is X.

Given a non-empty set X, a bijective function $f : X \to X$ is called a *permutation* of X.

Example Let X be the set of 52 cards of a deck. Shuffling the deck executes a permutation of X.

The set of permutations of X is denoted as Perm(X). In this set one can introduce the composition of permutations (i.e., the operation consisting in applying one permutation after the other) as the group multiplication. Composition of maps is associative. Then, the identity map $E : X \to X$, $E : x \to E(x) = x$ for all $x \in X$ is the unit element of Perm(X). Finally, since permutations are bijections, every $f \in$ Perm(X) has an inverse, so Perm(X) is a group.

Note that the group multiplication in the set of permutations is defined according to the convention that the order in which they are applied is “from right to left,” meaning that first one performs the rightmost permutation in a given expression, then continues with the next one to its left, and so on. This convention is inherited from that of composite mappings, for which, for example, $(fg)(x)$ means $f\big(g(x)\big)$. In general, the result obtained by applying first one permutation, then another, is not the same that one obtains by multiplying the same permutations in the opposite order. Therefore, in general, Perm(X) is not an Abelian group.

Example Let X be a set of three elements, say $X = \{a, b, c\}$. Let f be the permutation that interchanges the second and the third element of X, leaving the first unchanged, i.e., $f(a) = a$, $f(b) = c$, $f(c) = b$, and let g be the permutation that interchanges the first and the second element, leaving the third unchanged, i.e., $g(a) = b$, $g(b) = a$, $g(c) = c$. Then, for instance, $(f \cdot g)(a) = f(g(a)) = c$, while $(g \cdot f)(a) = g(f(a)) = b$. Hence $f \cdot g \neq g \cdot f$, so Perm(X) is not an Abelian group.

When X has a finite number N of elements, its group of permutations is called the *symmetric group* (or *permutation group*) *of degree* N and is denoted by S_N. We leave it as an exercise (see Problem 2.6) to prove that S_N contains $N!$ elements.

The smallest symmetric groups are isomorphic to groups that we already mentioned. In particular, $S_1 = \{e\}$ is the trivial group $\mathbb{Z}_1$, containing only the unit element, while S_2 is isomorphic to $\mathbb{Z}_2$. Both of them are Abelian groups. On the contrary, S_3 is a non-Abelian group. It is isomorphic to D_3, the dihedral group of order 6, which describes the symmetries of an equilateral triangle.

A possible way to denote the elements of $S_N = \text{Perm}(\{1, 2, \ldots, N\})$ is in terms of matrices of size $2 \times N$, in which each row contains all the numbers from 1 to N, and the permutation acts by mapping each number in the first row to the one in the second row and in the same column. So, for example, the permutations in S_2 are

$$E = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \tag{2.20}$$

so that E leaves the order of the two elements unvaried, while A interchanges them.

A more compact and more convenient way to denote permutations, however, is the one in terms of cycles. Given a permutation $P \in S_N$, a *cycle* is defined as an ordered sequence of labels, which are subsequently mapped one to another by P, with the last element of the cycle being mapped to the first.

A cycle can be considered as a permutation acting only on its labels (leaving the others unchanged). They are often written by listing the sequence of labels in parentheses, e.g., (132). In a given permutation P, any label that is mapped to itself (i.e., left invariant) by P can be considered as a cycle of unit length, e.g., (4). This means that N cycles of unit length, which act on only one label, leaving it unchanged, correspond to the unit element of S_N.

Clearly, the order of the labels within a cycle of length larger than one is relevant: Cycles containing the same labels but in a different order describe different permutations. So, for instance, (132) and (123) are different. However, cycles which differ only by a cyclic permutation of their labels are equivalent: Thus, (132) and (321) describe the same permutation. By virtue of this latter property, one can for example define the convention that, in each cycle, the smallest label appears in the leftmost position.

A generic permutation (different from the unit element of S_N) can be written as the product of its disjoint cycles of length larger than 1. Note that, when a permutation is written as the product of cycles acting on disjoint sets of labels, the order in which such cycles are multiplied is irrelevant. Thus, for example,

$$(132)(45) \qquad \text{and} \qquad (45)(132) \tag{2.21}$$

describe the same permutation in S_5. (Thus, one can uniquely fix the expression of a permutation as a product of cycles, for example by imposing the convention that the cycles are ordered so that the smallest label in each cycle is always increasing, when going from the leftmost to the rightmost cycle factor.)

Given two permutations in cycle notation, the cycle notation of their product can be expressed as follows.

1. Write the first label (say, x) appearing in the first cycle of the permutation that is applied first.
2. Starting from x, read the label that follows it (say, y) in the permutation that is applied first.
3. Read the label (say, z) that follows y in the permutation that is applied as second, and write it in the cycle notation of the permutation product.
4. Iterate the procedure, starting from z in the permutation that is applied first, until a cycle is completed.
5. Repeat the procedure for the other labels in the cycles of the permutation that is applied first.

If a generic permutation P is written as the product of nonoverlapping cycles, the inverse permutation P^{-1} can be expressed by reversing the order of the labels within each cycle of P (up to cyclic permutations of the labels within each cycle).

The cycle notation for permutations is best illustrated by examples. For instance, the permutation of six labels

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix} \tag{2.22}$$

decomposes into the product of three disjoint cycles $1 \to 2 \to 5 \to 1$, $3 \to 6 \to 3$ and $4 \to 4$. Thus it can be written as $(125)(36)(4)$, or, omitting cycles of unit length, as

$$P = (125)(36). \tag{2.23}$$

As an example of product of permutations, the algorithm described leads to

$$(146)(253) \cdot (13)(26)(45) = (12)(34)(56). \tag{2.24}$$

Note that, in the product appearing on the left-hand side of this equation, the permutation that is applied first is the rightmost one, i.e., $(13)(26)(45)$.

Finally,

$$(142)(35) \qquad \text{and} \qquad (124)(35) \tag{2.25}$$

are an example of permutations that are the inverse of each other. (Note that the labels in the cycles of the permutation on the right-hand side have been written in the opposite order with respect to those of the permutation on the left-hand side, then – for notational convenience – they have been reordered by a cyclic label permutation within each cycle, in order to have each cycle start with the smallest label it contains.)

The cycle notation provides a convenient way to list the elements of S_N, according to their cycle structure, i.e., by the number and length of cycles they contain (and denoting the trivial permutation, i.e., the unit element, of S_N as E). For illustration, we list the first permutation groups S_N, for $1 \leq N \leq 4$:

$$S_2 = \{E, (12)\} \tag{2.26}$$

$$S_3 = \{E, (12), (13), (23), (123), (132)\} \tag{2.27}$$

$$\begin{aligned} S_4 = \{&E, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23),\\ &(123), (132), (124), (142), (134), (143), (234), (243),\\ &(1234), (1243), (1324), (1342), (1423), (1432)\}. \end{aligned} \tag{2.28}$$

The cycle notation makes it easy to write down all the permutations in a concise and systematic way (one which, if necessary, can be readily automated in numerical implementations).

The simplest nontrivial permutations are the 2-cycles, which interchange two labels. In fact, it is possible to show that *any* permutation can be built from products of overlapping 2-cycles; a generic cycle of length r can be written as the product of $r - 1$ overlapping 2-cycles:

$$(n_1 n_2 \ldots n_r) = (n_1 n_2)(n_2 n_3) \ldots (n_{r-1} n_r). \tag{2.29}$$

Then, since any permutation is a product of cycles, it can always be written as a product of 2-cycles. According to the number of 2-cycles they can be decomposed into, a generic permutation can be classified as “even” or “odd”: More precisely, a permutation is said to be an *even* permutation if it can be factored into a product of an even number of 2-cycles. Conversely, an *odd* permutation is one that factorizes into the product of an odd number of 2-cycles. The *signature* of a permutation P, denoted as $\text{sgn}(P)$, is defined as

$$\text{sgn}(P) = \begin{cases} 1 & \text{if } P \text{ is an even permutation} \\ -1 & \text{if } P \text{ is an odd permutation} \end{cases}. \tag{2.30}$$

Note that a generic r-cycle is even if r is odd (and vice versa), because it can be decomposed into the product of $r-1$ overlapping 2-cycles.

Also, note that the unit element of S_N, i.e., the identity permutation E, is even (it contains no 2-cycles).

The *alternating group* A_N is defined as the subgroup of even permutations of S_N. Its order is $|A_N| = |S_N|/2 = (N!)/2$, thus for any $N > 2$ the alternating group is a proper subgroup of S_N.

Note that the set of *odd* permutations is not a subgroup of S_N: In fact, the multiplication of two odd permutations is an even permutation, so the multiplication is not a closed operation in the set of odd permutations. This implies that the set of odd permutations is not even a magma.

The reason why groups of permutations have a special status among finite groups is because of the following theorem, named after Arthur Cayley and first proven by the French mathematician Marie Ennemond Camille Jordan.

Theorem 2.2 (Cayley's theorem) *Every finite group of order N is isomorphic to a subgroup of S_N.*

Proof Let $(G, \cdot)$ be a generic finite group, with $|G| = N$. For any element $g \in G$, consider the function $f_g \in \text{Map}(G, G)$ defined as "multiplication by g on the left":

$$f_g : x \to f_g(x) = g \cdot x. \tag{2.31}$$

Note that f_g is an injection, because $f_g(x_1) = f_g(x_2)$ means $g \cdot x_1 = g \cdot x_2$; multiplying both sides of this equation by g^{-1} on the left, this implies $x_1 = x_2$. Furthermore, f_g is also a surjection, because, for any $y \in G$, there exists an element $x \in G$ such that $f_g(x) = y$: such x is simply $g^{-1} \cdot y$. Thus, $f_g : G \to G$ is a bijection, so it is a permutation of G. Now, consider the set of functions

$$K = \left\{ f_g : g \in G \right\}. \tag{2.32}$$

Defining the composition of functions as the group multiplication, K is endowed with group structure. Indeed, K is closed under the composition of functions (for any g_1 and $g_2 \in G$, the action of the composite map $f_{g_2} f_{g_1}$ on a generic $x \in G$ is defined as $f_{g_2}(f_{g_1}(x)) = f_{g_2}(g_1 \cdot x) = g_2 \cdot g_1 \cdot x = f_{g_2 \cdot g_1}(x)$, hence $f_{g_2} f_{g_1} = f_{g_2 \cdot g_1} \in K$, because $g_2 \cdot g_1 \in G$), which is an associative operation, f_e (with e the unit element of G) is the unit element of K, and the inverse of a generic $f_g \in K$ is $f_{g^{-1}}$. Note that this definition of group multiplication in K is the same as the definition of group multiplication in $\text{Perm}(G)$, since the operation of multiplying two permutations has been defined as applying one after the other (in particular, applying the one on the right first – in agreement with the rule of composition of functions). Thus, K is a set containing permutations of G, i.e., a subset of $\text{Perm}(G)$, and a group with the same group multiplication as $\text{Perm}(G)$. This means that K is a subgroup of $\text{Perm}(G)$. Also, note that, since G is completely generic, apart from being a finite group of order N, $\text{Perm}(G)$ is simply the group of permutations of a set with N elements, i.e., S_N. Next, it is trivial to show that there exists a group homomorphism $\mathcal{H}$ between G and K: Such homomorphism is just the function

$$\mathcal{H} : G \to K, \qquad g \to \mathcal{H}(g) = f_g, \tag{2.33}$$

on which the definition of K is based. $\mathcal{H}$ is a group homomorphism because, as we showed previously, the product $\mathcal{H}(g_2)\mathcal{H}(g_1) = f_{g_2}f_{g_1}$ in K is equal to $f_{g_2 \cdot g_1} = \mathcal{H}(g_2 \cdot g_1)$, hence $\mathcal{H}$ preserves the group product. Furthermore, $\mathcal{H}$ is an injection: $\mathcal{H}(g_1) = \mathcal{H}(g_2)$ means that the two functions f_{g_1} and f_{g_2} are equal, i.e., that, for any $x \in G$, one has $f_{g_1}(x) = f_{g_2}(x)$, that is $g_1 \cdot x = g_2 \cdot x$. Multiplying both sides of this equality by x^{-1} on the right, one gets $g_1 = g_2$. Finally, $\mathcal{H}$ is also a surjection, because K is defined as the set of functions f_g, that is, $\mathcal{H}(g)$, for all $g \in G$. This implies that the group homomorphism $\mathcal{H}$ is a bijection, i.e., it is a group isomorphism. We conclude that any generic finite group G of order N is isomorphic to a subgroup K of S_N. □

2.6 Partitions, Young Diagrams, and Multisets

2.6.1 Partitions

We noticed that the elements of S_N fall into subsets where the permutations have a similar cycle structure (or they are of similar *cycle type*).[1] For example, in S_4 we had the following types:

(1234), etc.	one 4-cycle	4
$(123)(4)$, etc.	one 3-cycle, one 1-cycle	$3+1$
$(12)(34)$, etc.	two 2-cycles	$2+2$
$(12)(3)(4)$, etc.	one 2-cycle, two 1-cycles	$2+1+1$
$(1)(2)(3)(4)$, etc.	four 1-cycles	$1+1+1+1.$

The right-hand column above lists the lengths of all cycles, including 1-cycles, for permutations of four elements. We notice that adding up the lengths always gives 4. More in general, in permuting N elements, the sum of lengths of all cycles must be N for the permutation to map all of the N elements. In the above, the different sums are different *partitions* of 4.

A *partition* of N is defined as a sum

$$N = \sum_i n_i, \tag{2.34}$$

where all $n_i \in \mathbb{Z}_+$. The number of different partitions of N (different ways of breaking N into a sum of type (2.34)), denoted $p(N)$, is called the *partition function*.

For example, $p(4) = 5$. One way to compute $p(N)$ is to use a generating function. One can show that the following identity holds:

$$\sum_{N=0}^{\infty} p(N)x^N = \prod_{k=1}^{\infty} \left(\frac{1}{1-x^k} \right). \tag{2.35}$$

Now, expanding all factors on the right-hand side as Taylor series:

$$\begin{aligned} (1-x)^{-1} &= 1 + x + x^2 + x^3 + \cdots \\ (1-x^2)^{-1} &= 1 + x^2 + x^4 + x^6 + \cdots \end{aligned}$$

[1] We will learn later that the subsets are the so-called *conjugacy classes* of S_N.

$$\begin{aligned}(1-x^3)^{-1} &= 1 + x^3 + x^6 + x^9 + \cdots\,, \\ &\text{etc.,}\end{aligned} \tag{2.36}$$

then

$$\begin{aligned}\prod_{k=1}^{\infty}\left(\frac{1}{1-x^k}\right) &= (1+x+x^2+\cdots)(1+x^2+x^4+\cdots)(1+x^3+\cdots)\cdots \\ &= 1 + x + 2x^2 + 3x^3 + \cdots\,.\end{aligned} \tag{2.37}$$

Matching the coefficients of x^N on both sides of (2.35) gives the values of $p(N)$: $p(0) = 1$, $p(1) = 1$, $p(2) = 2$, $p(3) = 3, \ldots$. For large values of N, Godfrey Harold Hardy and Srinivasa Ramanujan derived the asymptotic formula

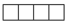
$$p(N) \sim \frac{1}{4N\sqrt{3}} \exp\left(\pi\sqrt{\frac{2N}{3}}\right), \quad N \to \infty. \tag{2.38}$$

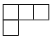
2.6.2 Young Diagrams

The different partitions can be represented graphically with *Young diagrams* (sometimes also called *Young tableaux*), which are named after the British mathematician Alfred Young. Recall the partition sum (2.34). Assume that the summands have been indexed in descending order: $n_1 \geq n_2 \geq n_3 \geq \cdots$. Then draw a figure with n_1 adjacent boxes on the first row, n_2 boxes in the second row, and so on.

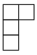
1	2	$\cdots$	$n_1 - 2$	$n_1 - 1$	n_1
1	2	$\cdots$	$n_2 - 1$	n_2	
1	2	$\cdots$	n_3		
$\vdots$	$\vdots$	$\ddots$			

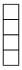
The resulting figure is the *Young diagram* corresponding to the partition (2.34). For example, for $N = 4$ we have the following partitions and Young diagrams.

4 

3 + 1 

2 + 2

2 + 1 + 1 

1 + 1 + 1 + 1 

The Young diagrams then also represent graphically the different types of permutations (different conjugacy classes) of S_N.

2.6.3 Multisets

Permutations reorder the elements of a set X with *distinct* elements. If we represent the elements by alphabetic letters and each ordering as a *word*, then each permutation generates an *anagram*. For instance, for a set of four elements T, E, A, and M we get $4! = 24$ different anagrams:

TEAM
MEAT
MATE
ATEM
...

What about words where the same letter appears more than once, such as

ABRACADABRA

How many different anagrams would we generate now? Let us first define a *multiset* as a set where an element x_i can appear multiple times, specified by its *multiplicity* m_i. For example, in

$$X = \{x_1, x_2, x_2, x_2, x_3, x_3\} \tag{2.39}$$

the element x_1 has multiplicity $m_1 = 1$, x_2 has $m_2 = 3$, x_3 has $m_3 = 2$. The total number of elements of X is $N = \sum_i m_i$ ($N = 6$ in the above example), when we do not require that all the elements are distinct. The letters of the word ABRACADABRA form the multiset

$$X = \{\mathrm{A, A, A, A, A, B, B, R, R, C, D}\} \tag{2.40}$$

with $m_\mathrm{A} = 5$, $m_\mathrm{B} = 2$, $m_\mathrm{R} = 2$, $m_\mathrm{C} = m_\mathrm{D} = 1$, and $N = 11$. Different words formed by the letters are the different permutations (reorderings) of the multiset. A priori, N elements can be reordered $N!$ times. But there are $m_1!$ ways to reorder the elements x_1 with no effect, $m_2!$ ways to reorder the elements x_2, and so on. Thus the total number of *distinct* reorderings of the elements of X is

$$\binom{N}{m_1, m_2, \ldots, m_k} \equiv \frac{N!}{m_1!\, m_2! \cdots m_k!}\,, \tag{2.41}$$

where k is the number of distinct elements of X, and $\sum_{i=1}^k m_i = N$ is a partition of N. Equation (2.41) defines a *multinomial coefficient*, which is a generalization of the binomial coefficient. The name comes from the generalization of the binomial theorem to k variables, the *multinomial theorem*

$$(x_1 + \cdots + x_k)^N = \sum_{\{m_i\}} \binom{N}{m_1, m_2, \ldots, m_k} x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}, \tag{2.42}$$

where the sum is over all partitions $\{m_i\}$ of N.

Now we can compute how many different anagrams of ABRACADABRA there are. The answer is

$$\frac{11!}{5!\,2!\,2!\,1!\,1!} = 83160. \tag{2.43}$$

2.7 Free Groups, Presentations of Groups, and Braid Groups

This section introduces a new way to construct groups.

2.7.1 Free Groups and Presentations

We begin by defining *free groups*.

Let G be a group and $X = \{g_1, g_2, \ldots, g_n\}$ a subset of elements of G. If *every* element $g \in G \setminus \{e\}$ (excluding the unit element e) can be *uniquely* written as a product

$$g = g_{j_1}^{i_1} g_{j_2}^{i_2} \cdots g_{j_m}^{i_m} \tag{2.44}$$

of elements g_{j_k} taken only from the set X with exponents $i_k \in \mathbb{Z} \setminus \{0\}$ such that no two adjacent elements are equal (i.e., $g_{j_i} \neq g_{j_{i+1}}$), we say that G is a *free group* and X is a *free set of generators* (of G).

The elements of X are called *letters*. An *arbitrary* product of letters

$$g = g_{j_1}^{i_1} g_{j_2}^{i_2} \cdots g_{j_m}^{i_m}, \tag{2.45}$$

where the exponents $i_k \in \mathbb{Z}$ (note: $i_k = 0$ is allowed) is called a *word*. If it satisfies the additional conditions of the previous definition, $i_k \neq 0$ and $g_{j_i} \neq g_{j_{i+1}}$, the word is called a *reduced word*.

Note that this is otherwise like the familiar construction of words with letters (with $a^3b^2 = aaabb$, etc.), except that group elements also have inverses. When all exponents are zero, the product is assumed to yield the unit element e. If a word is not a reduced word, one can perform a *reduction* to rewrite it in a reduced form (combining adjacent elements and removing unit elements). Note also that the product is in general not commutative: $ab \neq ba$.

Example Let $X = \{a, b, c\}$ be a collection of elements of a group G (excluding the unit element). For example, $g = a^3b^{-1}c^2b^4c$ is a reduced word, while $h = c^{-1}b^3b^{-2}a^0$ is a word, but not a reduced one. The reduction of h produces the reduced word $h' = c^{-1}b$.

Words can be joined together by forming a *product*. For example,

$$gh = a^3b^{-1}c^2b^4cc^{-1}b^3b^{-2}a^0. \tag{2.46}$$

The reduction of this gives the reduced word $(gh)' = a^3b^{-1}c^2b^5$. If we replace in the product the word h by its reduced form h' and then perform a reduction, we obtain the same reduced form: $(bh')' = (bh)'$. We can now define a free group G in an alternative way.

A *free group generated by X* is the set of of all reduced words formed from the letters of X and the empty word e, with products of words (joining of words) followed by reduction as the multiplication rule. To emphasize the generators X, we denote the free group generated by X by $F(X)$.

Example Let $X = \{a\}$. It generates the free group $F(X) = \{a^n | n \in \mathbb{Z}\}$, which is isomorphic to $(\mathbb{Z}, +)$. The isomorphism is $a^n \leftrightarrow n$, with $a^n a^m \leftrightarrow n + m$.

Example Let $X = \{a, b\}$. In this case the free group generated by X is

$$F(X) = \{e, a^n, b^n, a^n b^m, b^n a^m, a^n b^m a^k, b^n a^m b^k, \ldots\}, \tag{2.47}$$

where n, m, k, ... are integer numbers.

We can define a constraint by setting a reduced word to be equal to the unit element by an equation

$$r \equiv g_{j_2}^{i_1} g_{j_2}^{i_2} \cdots g_{j_m}^{i_m} = e. \tag{2.48}$$

Such a constraint is called a *relation*. There can be several independent relations r_1, $r_2, \ldots, r_n$.

Example Let $X = \{a\}$, set $r \equiv a^n = e$. With this relation, the set X generates the cyclic group $\{e, a, a^2, \ldots, a^n\} \cong \mathbb{Z}_n$.

A definition of a group now consists of the set of generators $X = \{g_1, g_2, \ldots, g_n\}$ and the complete list of independent relations $r_1, r_2, \ldots, r_m$. We use the notation $\langle g_1, g_2, \ldots, g_n | r_1, r_2, \ldots, r_m \rangle$ to denote this group, called the *presentation* of the group. For the previous example, the presentation of the group is

$$\langle a | a^n \rangle \cong \mathbb{Z}_n. \tag{2.49}$$

Additional Examples

1. Let $X = \{a, b\}$, $r = aba^{-1}b^{-1} = e$, and define the group $\langle a, b | aba^{-1}b^{-1} \rangle$. Note that the relation is equivalent to the equation $ab = ba$, meaning that the generators commute. Thus
$$\langle a, b, | aba^{-1}b^{-1} \rangle = \{a^n b^m | ab = ba;\ n, m \in \mathbb{Z}\} \cong (\mathbb{Z} \times \mathbb{Z}, +). \tag{2.50}$$
2. The *dihedral group* D_4 is the group of symmetries of a square. Consider the operations r = rotate the square by $\pi/2$ and f = reflect the square about the symmetry axis passing through the midpoints of opposite sides. The following relations are easy to see: $r^4 = e$ (rotation by 2π) and $f^2 = e$ (reflecting twice). A bit less obvious is $rfrf = e$, which is illustrated in Fig. 2.1. One can check that there are only these three independent relations. The dihedral group has then the presentation $D_4 = \langle r, f | r^4, f^2, rfrf \rangle$. More in general, dihedral groups D_n describe the symmetries of regular polygons with n sides, and can be defined via the presentation $D_n = \langle r, f | r^n, f^2, rfrf \rangle$.

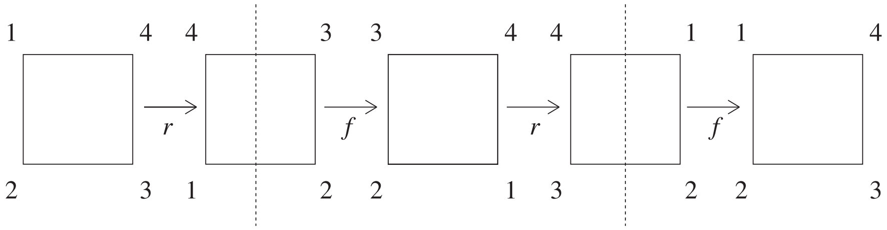


Fig. 2.1 Illustration of the relation $rfrf = e$, characterizing the dihedral group D_4.

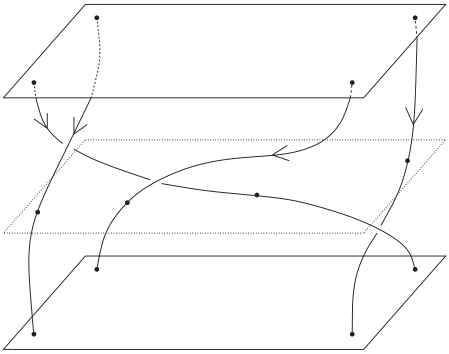


Fig. 2.2 Worldlines of four particles moving on a two-dimensional plane. Time runs from the top to the bottom, and the locations of the particles at the initial, at the final, as well as at a generic intermediate time (represented by the dotted plane) are shown by the black bullets.

3. The *Pauli group* G_1 is a finite group of order 16, consisting of the three Pauli matrices $\sigma_1, \sigma_2, \sigma_3$, and the identity matrix $\mathbb{1}_2$ multiplied by the factors $\pm 1, \pm i$:

$$G_1 = \{\pm\mathbb{1}_2, \pm i\mathbb{1}_2, \pm\sigma_1, \pm i\sigma_1, \pm\sigma_2, \pm i\sigma_2, \pm\sigma_3, \pm i\sigma_3\}. \tag{2.51}$$

Recalling the relations

$$\sigma_a^2 = \mathbb{1}_2 \ , \ \sigma_a\sigma_b = i\varepsilon_{abc}\sigma_c, \tag{2.52}$$

the Pauli group can be defined through the presentation

$$G_1 = \langle \sigma_1, \sigma_2, \sigma_3 | \sigma_a^2 = \mathbb{1}_2, \ \sigma_a\sigma_b = i\varepsilon_{abc}\sigma_c, \forall a \neq b, \ a, b \in \{1, 2, 3\}\rangle. \tag{2.53}$$

2.7.2 Braids

Next, we turn to consider something familiar from knitting. A *braid* consists of *strands* which run forward and can pass under or over each other. In a physics context, an important related situation is met when one considers worldlines of point particles moving in two space dimensions, as in Fig. 2.2. The particle worldlines then form strands that become entangled, just like knitting strands. This phenomenon gives rise to exotic quantum statistics for quantum particles in two dimensions,[2] in addition to the usual bosonic and fermionic statistics. Here we adopt a convention where the braid is drawn upright (another alternative would be to draw it sideways), with braiding of strands beginning from the top and proceeding downwards, as shown in Fig. 2.2. Braids are usually represented in a "flattened" form, as shown in Fig. 2.3.

One can imagine that the strands are like pieces of string or cord, and thus they can be moved and deformed continuously as shown in Fig. 2.4, or as in the example in Fig. 2.5.

In a braid of n strands, the strands can be labeled by an index i running from 1 to n, from left to right. A possible way to move strands in a braid, shown in Fig. 2.5, is known as the *Reidemeister move of the second type*.[3] To form braids, another

[2] The reason why this is not true in three or more space dimensions is that there the strands can then be disentangled. Likewise, all one-dimensional knots in higher dimensions become trivial.

[3] There exists also a move called the *Reidemeister move of the first type*, which is simply defined as untwisting a strand passing over itself.