Chapter 1

GENERAL STRUCTURE AND PROPERTIES

1.1 Introduction

In this Chapter we would like to introduce the main definitions and describe the main properties of groups, providing examples to illustrate them. The detailed discussion of representations is however demanded to later Chapters, and so is the treatment of Lie groups based on their relation with Lie algebras.

We would also like to introduce several explicit groups, or classes of groups, which are often encountered in Physics (and not only). On the one hand, these "applications" should motivate the more abstract study of the general properties of groups; on the other hand, the knowledge of the more important and common explicit instances of groups is essential for developing an effective understanding of the subject beyond the purely formal level.

1.2 Some basic definitions

In this Section we give some essential definitions, illustrating them with simple examples.

1.2.1 Definition of a group

A group G is a set equipped with a binary operation $\cdot$, the *group product*, such that[1]

(i) the group product is *associative*, namely

$$\forall\, a, b, c \in G\ , \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c\ ; \tag{1.2.1}$$

(ii) there is in G an *identity* element e:

$$\exists\, e \in G \ \text{ such that } \ a \cdot e = e \cdot a = a\ \forall\, a \in G\ ; \tag{1.2.2}$$

(iii) each element a admits an *inverse*, which is usually denoted as a^{-1}:

$$\forall\, a \in G\ \exists\, a^{-1} \in G \ \text{ such that } \ a \cdot a^{-1} = a^{-1} \cdot a = e\ . \tag{1.2.3}$$

[1] Notice that the axioms (ii) and (iii) above are in fact redundant. Show as an exercise that it would be sufficient to require

(ii') $\exists\, e \in G$ such that $e \cdot a = a\ \forall\, a \in G$, i.e., there is a *left identity*;

(iii') $\forall\, a \in G\ \exists\, b \in G$ such that $b \cdot a = e$, i.e., each element a admits a *left inverse* b (here e is the left identity introduced in (ii')).

That e is also a right identity follows, and one retrieves (ii) and (iii).

In the following, we will often indicate the group product simply as ab. We may indicate it with different symbols when the particular group operation is usually denoted differently, e.g. as $a+b$, when the product law is in fact the usual addition. In such a case, to stress the specific choice of the product law, we may also indicate the group as, for instance, $(G, +)$.

Some examples

- Consider the set $\{0, 1\}$ with the group product being the usual addition defined mod 2; this is a group (show it), usually denoted as $\mathbb{Z}_2$.
- The set $\{1, -1\}$ with the usual multiplication as group product is a group (show it). We will see that this group is isomorphic, i.e. it has the same abstract structure, to the previous example.
- The set of real numbers $\mathbb{R}$, with the group law being the addition, is a group (show it).
- The set $U(1) \equiv \{e^{i\theta}; \theta \in [0, 2\pi]\}$ with the usual multiplication is a group.
- The groups $\{e, a, a^2 \equiv a \cdot a, \ldots, a^{k-1}\}$ containing all the "powers" of a single "generator" a with respect to the group product, with the single extra relation $a^k = e$, are named *cyclic groups*, and denoted as $\mathbb{Z}_k$. Do you see a concrete "realization" of these groups that justifies their name?
- The set of complex numbers of the form $a + b\sqrt{-5}$, with $a, b \in \mathbb{Q}$ and not simultaneously zero, forms a group under the usual multiplication of complex numbers (show it).
- The set of permutations of three numbered objects 1,2,3 form a group called S_3, the product law being the composition of the permutations. This group has order 6, containing: the identical permutation, three exchanges: $p_{12} = (1 \leftrightarrow 2)$, $p_{13} = (1 \leftrightarrow 3)$, $p_{23} = (2 \leftrightarrow 3)$ and two cyclic permutations $p_{123} = (1 \to 2 \to 3 \to 1)$ and $p_{132} = (1 \to 3 \to 2 \to 1)$.

1.2.2 Abelian groups

The group product is *not* required to be commutative. When the product *is* commutative, the group is called an *Abelian group*:

$$G \text{ Abelian}: \quad ab = ba \ \ \forall a, b \ \in G \ . \tag{1.2.4}$$

Abelian groups are of course the simplest types of groups. All the groups of the previous examples are in fact Abelian, except the permutation group S_3 (check both assertions).

1.2.3 The group commutator

Two elements g, h of a group commute if, with the group product, $gh = hg$, i.e., $ghg^{-1}h^{-1} = e$. (e being the identity). Then the *group commutator* of g and h, defined as

$$ghg^{-1}h^{-1} \tag{1.2.5}$$

indicates if (and how) the two elements fail to commute.

1.2.4 Conjugated elements

Two group elements h and h' are said to be *conjugated* (in which case we write $h \sim h'$) if

$$\exists g \in G \text{ such that } h' = g^{-1}\, h\, g \ . \tag{1.2.6}$$

If the group is Abelian, each element is conjugate only to itself. Notice that the relation "being conjugate to" is an *equivalence* relation, namely it is symmetric, reflexive and transitive:

(i) $(h \sim h') \Leftrightarrow (h' \sim h)$;
(ii) $h \sim h$;
(iii) $(h \sim h')$ and $(h' \sim h'') \Rightarrow (h \sim h'')$,

as it is elementary to check.

1.2.5 Order and dimension of a group

The "number" of elements of a group G can be (1) finite, (2) infinite but denumerable or (3) continuously infinite.

In the first two cases, the number of elements of G is named the *order* of the group, and denoted as $|G|$ (in the second case, $|G| = \infty$). A group of finite order is called a *finite group*.

Examples

- The cyclic group $\mathbb{Z}_k$ is a finite group of order k.
- The relative integers $\mathbb{Z}$ with the group product being the addition form a group of infinite order.
- The set of real numbers (with the zero excluded) $\mathbb{R} \setminus \{0\}$, with the ordinary product, is a continuous group.

1.2.6 Topological groups

A group G containing a continuous infinity of elements is called a *topological group* if G as a set is a topological space. The group product law and the topological structure are tied by the requirement that the map $\phi : G \times G \mapsto G$ defined by $\phi(x, y) = xy^{-1}$, $\forall\, x, y \in G$, be *continuous* in x and y. Notice that the continuity of xy^{-1} in x, y implies the continuity in x, y of the map xy and x^{-1}.

Example The set of real numbers $\mathbb{R}$, with the addition as product law, is an Abelian topological group. Indeed $\mathbb{R}$ is a topological space (topology of open intervals) and the map $\phi(x, y) = x - y$ is continuous.

In the cases relevant in Physics, usually the map $\phi(x, y)$ enjoys, beyond continuity, *differentiability* properties related to a finer structure of G, that of a *differentiable manifold*.

1.2.7 Lie groups

The group g is called a *Lie group* when G is a differentiable manifold and the group product is related to the differentiable structure of G by the condition that the map $\phi(x, y) = xy^{-1}$ is *differentiable* in x and y.

The concept of order of the group gets replaced by that of *dimension* of the group G, denoted as $\dim G$, which is the dimension of G as a manifold.

See Chapter ? for the treatment of Lie groups.

Examples

- The set of real numbers $\mathbb{R}$, with the addition as product law, is also a Lie group, as $\mathbb{R}$ is (the prototype of) a manifold and the map $\phi(x, y) = x - y$ is differentiable.
- Consider the group SU(2), i.e. the group of 2×2 unitary matrices with unit determinant, the group product being the matrix multiplication. A generic element g of this group satisfies $g^\dagger g = \mathbf{1}$ and $\det g = 1$, and can be thus written (show it) as

$$g = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} , \qquad a, b \in \mathbb{C} , \;\; |a|^2 + |b|^2 = 1 \tag{1.2.7}$$

or, introducing four real parameters x^a, defined by $a = x^0 + \mathrm{i}x^3$ and $b = x^2 + \mathrm{i}x^1$, as

$$g = \begin{pmatrix} x^0 + \mathrm{i}x^3 & x^2 + \mathrm{i}x^1 \\ -x^2 + \mathrm{i}x^1 & x^0 - \mathrm{i}x^3 \end{pmatrix} = x^0 \mathbf{1} + \mathrm{i}x^i \sigma^i \tag{1.2.8}$$

(where σ^i, $i = 1, 2, 3$ are the Pauli matrices), with

$$\sum_{a=0}^{3} (x^a)^2 = 1 \; . \tag{1.2.9}$$

We see that the elements of SU(2) are parameterized by the points of a three-sphere S_3 defined by Eq. (1.2.9). Thus $\dim \mathrm{SU}(2) = 3$. It is possible to show that it is a Lie group, as the product corresponds to a differentiable mapping.

1.2.8 Order of an element

If $a \in G$, then $a^2, a^3, \ldots \in G$. If all the powers of a are distinct, then a is an element of *infinite order* (then, of course, G cannot be a group of finite order). If some of the powers of a coincide, this means (show it) that there exist some integer m such that $a^m = e$. Let n be the smallest of such integers m. Then a is said to be an element *of order* n.

Observations

- In a finite group G all elements have order $\leq |G|$.
- If G is a cyclic group of order n, then the order of any element is a divisor of n. Indeed, any element can be written as a^k, with a being the single generator, for which $a^n = e$. Then, the order m of this element must be such that $(a^k)^m = e = a^n$. If in particular $n = p$, with p a prime, then all elements have order n, and the group is called a 'p-cyclic group.
- In a finite group, the inverse of any element a is a power of a: indeed, $a^{-1} = a^{n-1}$, where n is the order of a.

1.2.9 The multiplication table of a finite group

A group is abstractly defined by describing completely (i.e., $\forall g_1, g_2 \in G$) the product law $(g_1, g_2) \mapsto g_1 g_2$ namely, by identifying the result of each possible product. For finite groups this can be encoded explicitely in a *multiplication table* whose entry in the i-th row and j-th column describes which element is the result of the product $g_i g_j$ (so we use the convention that $g_1 = e$):

e	g_2	g_3	$\dots$
g_2	$(g_2)^2$	$(g_2 g_3)$	$\dots$
g_3	$(g_3 g_2)$	$(g_3)^2$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

Notice that all the elements appearing in a line of the multiplication table are different (and therefore all elements appear in each line). Indeed, if we had $g_i g_j = g_i g_k$ we could conclude that $g_j = g_k$. The same applies to each column. These properties constrain a lot the possible multiplication tables, expecially at low orders.

A finite group is abstractly defined by its multiplication table, up to relabeling of the elements (i.e., up to rearrangings of the rows and columns). A given table, i.e., a given group, may have different concrete realizations. We will shortly make more precise what we mean by this observation.

Examples

- The only possible multiplication table for a group of order 2 is the following:

e	a
a	e

  This is the multiplication table of the cyclic group $\mathbb{Z}_2$: indeed we have $a^2 = e$. This unique group of order 2 admits hosts of realizations, e.g.:
  - the set $\{0, 1\}$ with addition mod 2 as product law;
  - the set $\{1, 1\}$ under ordinary product;
  - the group of spatial inversions in three-space (reflections w.r.t. to the y, z plane), e being the identity transformation, a the inversion $x \mapsto -x$.
  - the group S_2 of permutations of two objects, e being the identical permutation, a the exchange.
- There is only one possible group of order 3, with multiplication table

e	a	b
a	b	e
b	e	a

  (show it). This is the multiplication table of $\mathbb{Z}_3$. Some realizations:
  - the set $\{0, 1, 2\}$ (with addition mod 3 as product law);
  - the set $\{\mathrm{e}^{2\pi n \mathrm{i}/3}; n = 0, 1, 2\}$ of cubic roots of unity, with the ordinary product.
- Show that there are two possible groups of order 4. One corresponds obviously to $\mathbb{Z}_4$, the other, as we will see, to the dihedral group D_2, that is the direct product $\mathbb{Z}_2 \otimes \mathbb{Z}_2$.
- Write down the multiplication table of the group S_3.

1.2.10 Homomorphisms, isomorphisms, automorphisms

We have seen that we can have different "realizations" of a given abstract group. We are interested in concrete realizations of the group, where the elements of the group aquire an explicit meaning as numbers, matrices, symmetry operations or other quantities with which we can perform explicit computations.

In precise terms, finding a different realization G' of a given group G means to find an *isomorphic mapping* (or *isomorphism*) between G and G'. Let us explain this terminology.

Homomorphisms A map ϕ from a group G to a group G' is called an *homomorphism* iff it preserves the group structure, namely iff

$$\forall\, g_1, g_2 \in G\,, \quad \phi(g_1 g_2) = \phi(g_1)\phi(g_2)\ , \tag{1.2.10}$$

where the products $g_1 g_2$ and $\phi(g_1)\phi(g_2)$ are taken with the group product law of G and G' respectively. The map is not required to be invertible, i.e. one-to-one.

Representations An homomorphism $D : G \to G'$, where G' is a *matrix group*, namely a group whose elements are square matrices and whose product is the usual matrix product, is called a *linear representation* (representation, for shortness) of the group G. The properties and classification of group representations are probably the most important aspect of Group Theory, for physicists.

Isomorphisms An homomorphism $\phi : G \to G'$ which is also *invertible* is called an *isomorphism*. Two groups G and G' such that there exists an isomorphism $\phi : G \to G'$ are said to be *isomorphic*. They correspond to different realizations of the same abstract group structure.

An isomorphism $DG \to G'$, with G' a*matrix group* defines a *faithful* representation.

Examples

- Find an homomorphic mapping of $\mathbb{Z}_4$ onto $\mathbb{Z}_2$.
- Describe the isomorphism between the group of cubic roots of unity and the integers mod 3.
- The group $(\mathbb{R}, +)$ and the group $(\mathbb{R}^+, \cdot)$ (strictly positive real numbers with the ordinary product) are isomorphic. An isomorphism between the two is given by the exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$. Indeed the map is invertible and it respects the group product: $\exp(x + y) = \exp(x)\exp(y)$.

Automorphisms An isomorphic mapping σ from a group G to itself is called an *automorphism* of G. The set of all automorphisms of a given group G forms a group called $\mathrm{Aut}(G)$, the product law being the composition of mappings. Indeed, the composition [2] $\sigma_1 \circ \sigma_2$ of two automorphisms σ_1 and σ_2 is still an automorphism:

$$\begin{aligned}(\sigma_1 \circ \sigma_2)(h_1 h_2) &= \sigma_1\left(\sigma_2(h_1 h_2)\right) = \sigma_1\left(\sigma_2(h_1)\sigma_2(h_2)\right) = \sigma_1\left(\sigma_2(h_1)\right)\sigma_1\left(\sigma_2(h_2)\right) \\ &= (\sigma_1 \circ \sigma_2)(h_1)(\sigma_1 \circ \sigma_2)(h_2)\end{aligned} \tag{1.2.11}$$

and of course the composition of mappings is associative, there's an identical automorphism and any automorphism is assumed to be invertible by definition so that the group axioms are satisfied.

For finite groups, the automorphisms of G are particular permutations of the elements of G, namely $\mathrm{Aut}(G)$ is a subgroup of $S_{|G|}$. They correspond to symmetries of the multiplication table of G, in the following sense. As we remarked, the ordering of the rows and columns of the multiplication table is irrelevant. If we apply a given map $\sigma : g \mapsto \sigma(g)$ to labels and entries of the multiplication table it may happen that the resulting table corresponds just to a rearrangement of rows and columns of the original table. In this case the permutation σ is an automorphism.

[2] By this notation we intend acting *first* with σ_2 and *then* with σ_1

Example For instance, consider the map σ exchanging a and a^2 in the group $\mathbb{Z}_3$ and in the group $\mathbb{Z}_4$, the other elements remaining invariant. Show that in the first case σ is an automorphism, in the second it is not. Drawing in the complex plane the third and fourth roots of unity, it results evident why this exchange is a symmetry in the first case but not in the second.

An important class of automorphic mappings is the one corresponding to conjugation by a fixed element of a group:

$$\sigma_g : h \in G \mapsto \sigma_g(h) = g^{-1}\, h\, g \in G \ . \tag{1.2.12}$$

Show that such a mapping is indeed an automorphism. Automorphisms that correspond to conjugations are called *inner automorphisms*, automorphisms which do not, *outer automorphisms*. Notice that for Abelian groups the only non-trivial automorphisms are outer ones.

1.2.11 Rank, generators, relations (cursory look)

Let the elements of a finite group G be $g_1 = e, g_2, g_3, \ldots$. All elements can be written in the form

$$g_k = g_{i_1} g_{i_2} \ldots g_{i_s} \ , \tag{1.2.13}$$

for suitable g_{i_j} elements (at worst the only possibility is $g_k = g_k$). A set of group elements (different from the identity e) which, multiplied in all possible ways, give *all* the elements of G (a part, at most, from the identity) is said to *generate* the group G. The minimal such set is a set of *generators* of G. The minimal number of generators is the *rank* of G.

If a group G is denumerable rather than finite, then we say that it is generated by a finite subset B of elements iff every element $g \in G$ can be written as

$$g = g_{i_1}^{\pm 1} g_{i_2}^{\pm 1} \ldots g_{i_s}^{\pm 1} \ , \tag{1.2.14}$$

with all the g_{i_l} belonging to B (they may be repeated, of course). So, with respect to the case of finite groups, now not only positive but also negative powers of generators may appear. In the case of finite groups, all generators have finite order, so their negative powers can be re-expressed in terms of the positive ones; this is not true in general.

Examples

- The cyclic groups $\mathbb{Z}_k$ have rank one, as all elements are powers of a single generator a: $\mathbb{Z}_k = \{e = a^0, a, a^2, \ldots a^{k-1}\}$.
- The permutation group S_3 is generated by the two exchanges p_{12} and p_{23}. Indeed one has then $p_{132} = p_{12}\, p_{23}$, $p_{123} = p_{23}\, p_{12}$ and $p_{13} = p_{12}\, p_{23}\, p_{12} = p_{23}\, p_{12}\, p_{23}$. S_3 has thus rank 2.

Presentation of a group. Relations A group can be described by giving its *generators* and (if present) the *relations* that they satisfy. Such a description of a group is called a *presentation* of the group.

Indeed, starting with the generators g_a ($a = 1, \ldots \operatorname{rank} G$) one can construct *words* of increasing length: g_a, then $g_a g_b$, etc. In this one obtains the further elements of G. In the process, however, me must take into account the *relations* to which the generators may be subject, which may be cast in the form $R_i(\{g_a\}) = e$, the R_i being a set of specific words. If G is a finite group, then each generator must be of finite order and therefore we have at least the relations $g_a^{n_a} = e$, where n_a is the order of g_a; there may then be others.

We will come back later in **??** to these concepts, to formalize them a bit more.

Examples

- The group S_3 is defined by its presentation consisting of two generators $s = p_{12}$ and $t = p_{13}$ subject to the relations that $s^2 = e$, $t^2 = e$ and $(st)^3 = e$. Show that indeed this presentation permits to retrieve S_3.

For continuous groups, as we will see, the analogue of generators and relations will be given by the existence of a set of "infinitesimal generators" closing a Lie algebra.

1.2.12 Subgroups

A subset $H \subset G$ is a *subgroup* of G if it is a group, with the same product law defined in G. To this effect it is sufficient that

i) $\forall h_1, h_2 \in H$, $h_1 h_2 \in H$;
ii) $\forall h_1 \in H$, $h_1^{-1} \in H$.

Show this. While for an infinite (or continuous) group both requirements are to be checked (find an example), if G is a finite group, then i) is enough; show it (hint: for a finite group all elements are of finite order).

Examples

- $\mathbb{Z} \subset \mathbb{R}$ (with the addition as product law) is a subgroup.
- A cyclic group $\mathbb{Z}_n$ admits a subgroup $\mathbb{Z}_m$ whenever $m|n$ (i.e., when "m divides n").

The relation "being subgroup of" is transitive:

$$\left\{ \begin{array}{l} H \subset G \ , \\ K \subset H \end{array} \right. \quad \Rightarrow K \subset G \ , \tag{1.2.15}$$

where, as we will do from now on unless there is risk of confusions, with $H \subset G$ we intend "H is a subgroup of G". In general, a given group G will admit chains of subgroups

$$G \supset H_1 \supset H_2 \ldots \supset e \ . \tag{1.2.16}$$

G itself and the group containing only the identity e are *trivial* subgroups of G, other subgroups are called *proper* subgroups. One of the most important problems in group theory is the determination of all proper subgroups of a given group.

Infinite groups may admit infinite sequences of subgroups. For instance, consider $(\mathbb{Z}, +)$:

$$\begin{array}{ccccc} \mathbb{Z} & = & G & = & \ldots, -2, -1, 0, 1, 2, \ldots \\ \cup & & \cup & & \\ 2\mathbb{Z} & = & H_1 & = & \ldots, -4, -2, 0, 2, 4, \ldots \\ \cup & & \cup & & \\ 4\mathbb{Z} & = & H_2 & = & \ldots, -8, -4, 0, 4, 8, \ldots \\ \vdots & & \vdots & & \vdots \end{array} \tag{1.2.17}$$

In this case, all the elements of the sequence are isomorphic.

1.3 Important examples

In this section we want to introduce many typical classes of groups which are encountered in Physics. This should "substantiate" the definitions given before and provide a set of important concrete examples which will be very useful (often essential) in the following.

1.3.1 Groups of matrices

Very often, physically interesting groups are *matrix groups*, i.e. groups whose elements are square matrices of a given dimension, and where the product law is the ordinary matrix multiplication. This product is in general non-commutative, but it is associative. The group must contain the identity matrix. All the matrices M in the group have to be invertible, i.e. $\det M \neq 0$, for axiom (iii) to be satisfied.

General linear groups The group of *all* $n \times n$ invertible matrices with complex entries is called the (complex) *general linear group* in n dimensions and is denoted as $\mathrm{GL}(n, \mathbb{C})$. If the entries are real, we have the real general linear group $\mathrm{GL}(n, \mathbb{R})$, which is a subgroup of the former. Could one also define a $\mathrm{GL}(n, \mathbb{Z})$ group?

An element of $\mathrm{GL}(n, \mathbb{C})$ is parameterized by n^2 complex numbers, the entries of the matrix (the n^2 parameters are real for $\mathrm{GL}(n, \mathbb{R})$, of course).

One can define further matrix groups by placing restrictions, typically in form of matrix equations or of conditions on the determinant, that are preserved by the matrix product.

Special linear groups The group of all $n \times n$ matrices with complex entries and *determinant equal to* 1 is named the *special linear group* and is indicated as $\mathrm{SL}(n, \mathbb{C})$. It is obviously a subgroup of $\mathrm{GL}(n, \mathbb{C})$: the condition of having unit determinant is preserved under the product. Similarly, one defines $\mathrm{SL}(n, \mathbb{R})$. One can also define the group $\mathrm{SL}(n, \mathbb{Z})$; the inverse matrices too have integer entries: the determinant, that would appear in the denominator, is 1.

An element of $\mathrm{SL}(n, \mathbb{C})$ depends on $n^2 - 1$ complex parameters, as the relation $\det M = 1$ has to be imposed on the n^2 entries of any matrix M. Such parameters are real (integers) for $\mathrm{SL}(n, \mathbb{R})$ or $\mathrm{SL}(n, \mathbb{Z})$.

Unitary groups The group of *unitary matrices* $\mathrm{U}(n, \mathbb{C}) \subset \mathrm{GL}(n, \mathbb{C})$ contains all the complex matrices U such that

$$U^\dagger U = \mathbf{1} \ . \tag{1.3.18}$$

Check that it is a group. Which values can the determinant of a unitary matrix assume?. Similarly one could define $\mathrm{U}(n, \mathbb{R}) \subset \mathrm{GL}(n, \mathbb{R})$, containing real unitary matrices: $U^\dagger U = U^T U = \mathbf{1}$, but these are nothing else than real orthogonal matrices, to be introduced shortly. So the group of complex unitary matrices is usually simply denoted as $\mathrm{U}(n)$. Complex unitary matrices are parameterized by $2n^2 - n^2 = n^2$ *real* parameters (we have to subtract the n^2 real conditions corresponding to the entries of the equation $U^\dagger U - \mathbf{1} = 0$ from the n^2 complex parameters of the matrix U). So the unitarity conditions halves the number of parameters, with respect to a generic complex matrix.

Special unitary groups The subgroup $\mathrm{SU}(n, \mathbb{C}) \subset \mathrm{U}(n, \mathbb{C})$ contains the unitary matrices with unit determinant. It is usually denoted simply as $\mathrm{SU}(n)$. It is determined by $n^2 - 1$ real parameters. We have to subtract the real condition of having determinant 1 from the parameters of a unitary

matrix; recall that the determinant of a unitary matrix can assume a continuous range of values $\exp(2\pi \mathrm{i}\theta)$, $\theta \in [0,1]$.

Orthogonal groups The group of *orthogonal matrices* $\mathrm{O}(n,\mathbb{C}) \subset \mathrm{GL}(n,\mathbb{C})$ contains all the complex matrices O such that

$$O^T O = \mathbf{1} \ . \tag{1.3.19}$$

Check that it is a group (which values can the determinant assume?). More frequently encountered are the *real* orthogonal matrices $\mathrm{O}(n,\mathbb{R}) \subset \mathrm{GL}(n,\mathbb{R})$. These groups are usually denoted simply as $\mathrm{O}(n)$. Real orthogonal matrices are parameterized by $n(n-1)/2$ real numbers. Indeed, from the n^2 parameters of a general real matrix, we have to subtract the $n(n+1)/2$ conditions given by the entries of the matrix condition $O^T O = \mathbf{1}$, which is *symmetric*.

Special orthogonal groups The group $\mathrm{SO}(n)$ contains the real orthogonal matrices with unit determinant. Analogously one could define its complex extension $\mathrm{SO}(n,\mathbb{C})$. They have the same number of parameters, $n(n-1)/2$, as the orthogonal matrices. Indeed, the determinant of an orthogonal matrix O can already have only a finite set of values: $\det O = \pm 1$; imposing $\det O = 1$ does not alter the dimensionality of the parameter space.

Symplectic groups The group of *symplectic matrices* $\mathrm{Sp}(n,\mathbb{C})$ contains the $2n \times 2n$ matrices A that preserve the "symplectic[3] form" Ω, namely the matrices such that

$$A^T \, \Omega \, A = \Omega \ , \qquad \Omega = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ -\mathbf{1} & \mathbf{0} \end{pmatrix} \ . \tag{1.3.20}$$

Similarly one defines $\mathrm{Sp}(n,\mathbb{R})$. Since the restriction Eq. (1.3.20) is an antisymmetric matrix expression, it poses $(2n)(2n-1)/2$ conditions, and the symplectic matrices depend thus on $(2n)^2 - (2n)(2n-1)/2 = n(2n+1)$ parameters (complex or real for $\mathrm{Sp}(n,\mathbb{C})$ or $\mathrm{Sp}(n,\mathbb{R})$).

The groups $\mathrm{U}(n)$, $\mathrm{O}(n)$ and $\mathrm{Sp}(n)$ form the three families of so-called "classical (matrix) groups".

1.3.2 Groups of transformations

Square matrices represent endomorphisms of some vector space. Thus the matrix groups are in fact groups of linear transformations of vector spaces. More in general, very often in physical applications the elements of G are transformations τ acting on some space V:

$$\tau \in G : \ v \in V \mapsto \tau(v) \in V \ , \tag{1.3.21}$$

and the group composition is the composition of transformations:

$$\tau_1 \tau_2 \in G : \ v \in V \mapsto \tau_1 \left(\tau_2 (v) \right) \in V \ . \tag{1.3.22}$$

In this case, the associativity is automatically satisfied. Notice our convention that in the product $\tau_1 \tau_2$ one acts first with τ_2 and then with τ_1: $v \overset{\tau_2}{\mapsto} \tau_2(v) \overset{\tau_1}{\mapsto} \tau_1(\tau_2(v)) \equiv \tau_1 \tau_2 (v)$. This is of course the same convention that arises in taking the matrix product as the group product law for groups of linear transformations on vector spaces.

Transformations groups are Abelian when the order in which two transformations are subsequently performed does not affect the final result.

Let us now consider some relevant examples.

[3] The symplectic form is the non-positive quadratic form often appearing in analytical mechanics, e.g., in the definition of the Poisson brackets: $\{F,G\} = \frac{\partial F}{\partial y^I} \Omega^{IJ} \frac{\partial F}{\partial y^J}$, where $y^I = (q^i, p^i)$ are the phase-space coordinates.

1.3.3 The permutation groups S_n

Consider a finite set A. The automorphisms of A, i.e., the *bijective mappings* $P : A \leftrightarrow A$, form a group $S(A)$, called the *symmetric group* of A. The nature of the objects in the set A does not matter, only their number $|A|$ does. So, if $|A| = n$, we can think the objects to be the numbers $1, 2, \ldots n$ and indicate the symmetric group, also called the *permutation group* on n objects, as S_n. An element of this group, a *permutation* P, i.e. a bijective map, is defined explicitely by its action on the elements $1, \ldots n$ of the set:

$$P = \begin{pmatrix} 1 & 2 & \ldots & n \\ P(1) & P(2) & \ldots & P(n) \end{pmatrix} . \tag{1.3.23}$$

The product law of the symmetric group is the composition of permutations, with the convention described above: PQ means effecting first the permutation Q and then the permutation P. While S_2 is Abelian, all S_n with $n > 2$ are not Abelian. (Show by picking some particular permutations that S_3 is not Abelian.) The symmetric group S_n has $n!$ elements (show it).

We may give an explicit expression of a permutation $P \in S_n$ as an $n \times n$ matrix defined by

$$(P)_{ij} = \delta_{i,P(j)} , \qquad i, j = 1, \ldots n . \tag{1.3.24}$$

In this way composition of permutations corresponds to the product of the defining matrix representatives Eq. (**??**):

$$(PQ)_{ij} = \sum_k \delta_{i,P(k)}\delta_{k,Q(j)} = \sum_k \delta_{i,P(k)}\delta_{P(k),P(Q(j))} = \delta_{i,P(Q(j))} . \tag{1.3.25}$$

Notice that the matrix representatives of permutations are unitary and real, that is, they are orthogonal matrices. So S_n can be seen as a subgroup of $U(n)$, and in particular of $O(n)$.

Cycle decomposition Let us illustrate the notion of "cycle" of a permutation by means of an example. Consider the permutation $P \in S_8$ given by

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 6 & 8 \end{pmatrix} . \tag{1.3.26}$$

Let us follow what happens to the various elements $1, \ldots 8$ if we repeatedly apply the permutation P. We have $1 \to 2 \to 3 \to 1$, after which everything repeats again. We say that $1, 2, 3$ form a cycle of order 3 in P, and we denote this cycle compactly as (123). We also have that $4 \to 5 \to 4$, so that we have a cycle (45). Also, $6 \to 7 \to 6$ and thus there's the cycle (67). Finally 8 is invariant, i.e., it is a trivial cycle (8). The permutation P has a the *cycle decomposition*

$$P = (123)(45)(67)(8) . \tag{1.3.27}$$

Often the cycles of length 1, such as (8) above, are omitted when writing the cycle decomposition. It is quite evident that the example we took is not limited in any way, and every permutation of any S_n group will admit a cycle decomposition. As we will see, the (type of) cycle decompositions of permutations is of fundamental importance in the analysis of permutation groups. Let us make some simple observations.

i) The sum of the lengths of the cycles in the cycle decomposition of $P \in S_n$ equals n: every element is in some cycle, and cycles do not have elements in common.

ii) Having no common elements, two cycles in the decomposition of a given permutation commute. For instance, in Eq. (1.3.27), $(123)(45) = (45)(123)$.
iii) Just by their definition, the cycles can be shifted freely without affecting them: $(123) = (231) = (312)$ (but $(123) \neq (213)$!)
iv) Every cycle can in turn be decomposed into a product of cycles of order 2, called also *transpositions* or *exchanges*. However the latter have now elements in common. For instance, $(123) = (13)(12)$. In general, $(12\dots n) = (1n)(1, n-1)\dots(13)(12)$; show this.

Odd and even permutations As discussed above, every permutation can be decomposed into a product of transpositions. A permutation is called *odd* or *even* depending if in such a decomposition an odd or even number of transpositions is needed.

The alternating groups The *even* permutations form a subgroup of S_n (the odd ones clearly do not form a subgroup) called the *alternating group* on n elements, denoted as A_n. Its order is $|A_n| = |S_n|/2 = n!/2$.

1.3.4 The Euclidean groups

The so-called Euclidean group in d dimension is the group of *isometry* transformations in an Euclidean space $\mathbb{R}^d$. It consists of translations, of rotations around some axis (proper rotations) and reflections with respect to hyperplanes. All such transformations leave unaltered the Euclidean distance between any two points of $\mathbb{R}^d$.

The Euclidean group in two dimensions Consider the transformations of a plane $\mathbb{R}^2$ into itself given by rigid rotations around a perpendicular axis through the origin. They clearly form a group. The elements R_θ of the group are identified by an angle θ (the angle of, e.g., anticlockwise, rotation) defined mod 2π; that it, the elements of the group correspond to the points of a circle S^1. The composition of two rotations results in $R_{\theta_1} R_{\theta_2} = R_{\theta_1+\theta_2}$; the group is Abelian. We can describe a transformation $R(\theta)$ via its effects on the Cartesian coordinates $\mathbf{x} \equiv (x, y)$ of a point: $\mathbf{x} \overset{R(\theta)}{\mapsto} \mathbf{x}'$, with

$$\begin{cases} x' = \cos\theta\, x + \sin\theta\, y \ , \\ y' = -\sin\theta\, x + \cos\theta\, y \ , \end{cases} \tag{1.3.28}$$

that is, $\mathbf{x}' = \mathcal{R}(\theta)\mathbf{x}$, with $\mathcal{R}(\theta)$ an orthogonal 2×2 matrix with unit determinant: $\mathcal{R}(\theta) \in \mathrm{SO}(2)$. In fact, this correspondence between rotations and matrices of SO(2) is an isomorphism. We can thus say, with a slight abuse of language, that SO(2) is the (proper) rotation group in two dimensions.

Also the translations $T(\mathbf{v})$ by a two-vector vector $\mathbf{v}$ acting on the Euclidean space $\mathbb{R}^2$, $T(\mathbf{v}) : \mathbf{x} \mapsto \mathbf{x} + \mathbf{v}$, $\forall \mathbf{x} \in \mathbb{R}^2$ form a group, with the composition of two translations resulting in $T(\mathbf{v}_1)T(\mathbf{v}_2) = T(\mathbf{v}_1 + \mathbf{v}_2)$; the group is Abelian.

Consider now the group of all transformations of $\mathbb{R}^2$ onto itself given by simultaneous rotations and/or translations with arbitrary parameters. Let us denote such transformations as $g(\theta, \mathbf{v}) \equiv (R(\theta), T(\mathbf{v}))$. They act on the coordinate vectors by

$$(R(\theta), T(\mathbf{v})) : \quad \mathbf{x} \mapsto \mathcal{R}(\theta)\mathbf{x} + \mathbf{v} \ . \tag{1.3.29}$$

Notice that the translation parameters $\mathbf{v}$, being vectors, are acted upon by the rotations. Check that the product law resulting from the composition of two such transformations is

$$(R(\theta_1), T(\mathbf{v}_1))(R(\theta_2), T(\mathbf{v}_2)) = (R(\theta_1)R(\theta_2), T(\mathbf{v}_1) + T(\mathcal{R}(\theta_1)\mathbf{v}_2)) \ , \tag{1.3.30}$$

i.e. also

$$g(\theta_1, \mathbf{v}_1)g(\theta_2, \mathbf{v}_2) = g(\theta_1 + \theta_2, \mathbf{v}_1 + \mathcal{R}(\theta_1)\mathbf{v}_2) \ . \tag{1.3.31}$$

Check that this is a group; in particular, find the expression of the inverse of a given transformation. This group is called "inhomogeneous rotation group" in two dimensions and indicated as ISO(2).

A proper rotation sends an oriented orthogonal frame into a new orthogonal frame with the same orientation. Inversions (or reflections) of the plane with respect to a line through the origin also map it to an orthogonal frame, but with the opposite orientation. For instance, reflection with respect to the x-axis maps (x, y) to $(x, -y)$. The set of all transformations obtained as compositions of proper rotations and inversions is a group (show it). The inversion w.r.t. to a direction forming an angle θ with the x axis is effected by the matrix (show it)

$$\mathcal{I}(\theta) = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} = \mathcal{I}(0)\mathcal{R}(2\theta) \tag{1.3.32}$$

where $\mathcal{I}(0) = \mathrm{diag}(1, -1)$ is orthogonal but with determinant -1. Thus rotations plus inversions of the plane are represented by orthogonal 2×2 matrices, i.e., by elements of O(2).

Translations, rotations and inversions form a group, Eucl_2, which is called the Euclidean group (in two dimensions).

The Euclidean group in three dimensions The translations acting on $\mathbb{R}^3$ form an Abelian group (there's no difference from the $\mathbb{R}^2$ case).

Consider then the rotations around any axis through the origin. Such transformations form the group or *proper orthogonal rotations* in three dimensions; the effect of doing two subsequent rotations around two axis is again a rotations around some other axis. The proper rotations map an orthonormal frame into a new orthonormal frame with the same orientation, and are represented on the vectors by orthogonal 3×3 matrices with unit determinant. In fact, the group of proper rotations is isomorphic to SO(3). For instance, write the matrices representing rotations around the coordinate axis. (Other exercise: given a SO(3) matrix, individuate the axis and the angle of rotation by "diagonalizing" the matrix). The group of three–dimensional rotations SO(3) is *non Abelian* (for instance, consider products of rotations around the coordinate axes).

How is the rotation group parameterized? Take the rotation angle $\phi \in [-\pi, \pi]$. A given rotation is thus represented by a vector in three-space whose versor is that of the rotation axis, and whose algebraic length is ϕ. This describes a ball of radius π. However, rotations of π or of $-\pi$ around an axis are to be identified. Thus the point of the surface S^2 of the ball have to be identified pairwise (antipodal identification). The elements of the group corresponds thus to points of this space, which we will identify better later.

Again, the group $ISO(3)$ of roto-translations in three dimensions can be defined with no formal modifications with respect to the bi-dimensional case.

Reflections with respect to a plane and total spatial reflection $\mathbf{x} \mapsto -\mathbf{x}$ map orthogonal frames to orthogonal frames of opposite orientation. They are represented by orthogonal 3×3 matrices with determinant -1. Rotations and reflections form a thus group, which is isomorphic to the group O(3) of orthogonal matrices acting on the vectors.

Translations, rotations and reflections form the Euclidean group in three dimensions Eucl_3.

1.3.5 The Möbius group (complex projective transformations)

Consider the *conformal transformations* of the compactified complex plane (or Riemann sphere) $\tilde{\mathbb{C}} \equiv \mathbb{C} \cup \{\infty\}$. Conformal mappings $z \mapsto w$ are represented by *analytic* functions $w(z)$. We ask that the transformations be invertible, i.e. one-to-one, so the function $w(z)$ can have at most a pole (otherwise the point at infinity would have many counter-images) and therefore (logarithmic indicator...) at most a zero; moreover the Jacobian $\partial w/\partial z$ must not vanish. We have thus that a transformation M is given by

$$z \overset{M}{\mapsto} w(z) = \frac{az+b}{cz+d} \ , \quad a,b,c,d \in \mathbb{C}, \ \ ad-bc \neq 0 \ , \tag{1.3.33}$$

where the last condition follows from the invertibility condition $\partial w/\partial z \neq 0$ (check it). Notice that all transformation of parameters (ka, kb, kc, kd), $k \in \mathbb{C} \setminus \{0\}$ are equivalent: there is a scale invariance that we can use to fix $ad - bc = 1$. The transformations Eq. (1.3.33) are known as *fractal linear transformations*, *projective transformations* or *Möbius transformations*.

The composition of two Möbius transformations $M, M'$is again a Möbius transformation M'':

$$z \overset{M}{\mapsto} w = \frac{az+b}{cz+d} \overset{M'}{\mapsto} x = \frac{a'w+b'}{c'w=d'} = \frac{(a'a+b'c)z+a'b+b'd}{(c'a+d'c)z+c'b+d'd} = \frac{a''z+b''}{c''z+d''} \ . \tag{1.3.34}$$

Check that the product transformation $z \overset{M''}{\mapsto} x$ satisfies $a''d'' - b''c'' = 1$.

Thus, it is natural to associate to a Möbius transformation M a 2×2 matrix $\mathcal{M}$ with unit determinant

$$\mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ , \quad \det \mathcal{M} = ad - bc = 1 \ , \tag{1.3.35}$$

that is an element of $\mathrm{SL}(2,\mathbb{C})$. Then to a product of transformations $M'' = M'M$ corresponds a matrix which is the matrix product of the two factors: $\mathcal{M}'' = \mathcal{M}'\mathcal{M}$. However, the mapping from the group of Möbius transformations to $\mathrm{SL}(2,\mathbb{C})$ is one-to-two, as the matrices $\pm\mathcal{M}$ correspond to the same Möbius transformation M.

1.3.6 Groups of invariance (symmetry groups)

Very often one is interested in groups which can be defined as group of transformations such that they preserve some property or some operation defined in the space on which the transformations act. Such groups are then called *symmetry groups* or *groups of invariance*. This is the context in which group theory was originally developed, and also the framework of many of its physical applications, for instance, in quantum mechanics. Let us now discuss some important (classes of) examples.

1.3.7 Matrix groups and vector spaces

...

Special linear groups as volume-preserving transformations ...

In the particular case of $V^{\otimes n}$ (with V of dimension n), the fully antisymmetric subspace has dimension $\binom{n}{n} = 1$, and its basis element is $\vec{e}_1 \wedge \vec{e}_2 \ldots \wedge \vec{e}_n$. It is called[4] the *volume element*.

[4] Though this name is in fact appropriate for the *dual* basis element of $\Lambda_n(V)$, the space of *n-forms* or n-linear antisymmetric functionals on V.

A change of basis A on V induces a transformation of the volume element by a multiplicative factor:

$$(\vec{e}_1 \wedge \vec{e}_2 \ldots \wedge \vec{e}_n)' = \det A \, \vec{e}_1 \wedge \vec{e}_2 \ldots \wedge \vec{e}_n \ , \tag{1.3.36}$$

where the determinant arises from the application of Eq. (**??**):

$$\det A = \sum_{P \in S_n} (-1)^{\sigma(P)} \, A_1^{j_1} A_2^{j_2} \ldots A_n^{j_n} \ . \tag{1.3.37}$$

The permutations P act by exchanging the indices j_i.

We have defined the *special linear group* $\mathrm{SL}(n)$ (real or complex) to be the subgroup of the general linear group $\mathrm{GL}(n)$ (real or complex) containing the matrices A such that $\det A = 1$. We see now by Eq. (1.3.36) that the special linear group is the subset of basis changes on V that *preserve the volume* element of $V^{\otimes n}$.

Metrics (bilinear or sesquilinear forms) Let V be a vector space based on a field $\mathbb{F}$ (which can be either $\mathbb{R}$ or $\mathbb{C}$ for us). A *metric* on a vector space is a functional from $V \otimes V$ into the $\mathbb{F}$. That is, a metric is the assignment of a value in $\mathbb{F}$ to every pair of vectors:

$$g : \ \vec{v}_1, \vec{v}_2 \in V \mapsto (\vec{v}_1, \vec{v}_2) \in \mathbb{F} \ , \quad \forall \, \vec{v}_{1,2} \in V \ . \tag{1.3.38}$$

We have utilized above the notation $(,)$ for the metric action, which is natural since metrics are indeed utilized to define scalar products; however for this purpose some further properties are usually assumed. The metric can be required to be *bilinear*, in which case

$$\begin{aligned} (\vec{v}_1, \alpha\vec{v}_2 + \beta\vec{v}_3) &= \alpha(\vec{v}_1, \vec{v}_2) + \beta(\vec{v}_1, \vec{v}_3) \ , \\ (\alpha\vec{v}_1 + \beta\vec{v}_2, \vec{v}_3) &= \alpha(\vec{v}_1, \vec{v}_3) + \beta(\vec{v}_2, \vec{v}_3) \ , \end{aligned} \tag{1.3.39}$$

for any $\alpha, \beta \in \mathbb{F}$, or *sesquilinear*, in which case

$$\begin{aligned} (\vec{v}_1, \alpha\vec{v}_2 + \beta\vec{v}_3) &= \alpha(\vec{v}_1, \vec{v}_2) + \beta(\vec{v}_1, \vec{v}_3) \ , \\ (\alpha\vec{v}_1 + \beta\vec{v}_2, \vec{v}_3) &= \alpha^*(\vec{v}_1, \vec{v}_3) + \beta^*(\vec{v}_2, \vec{v}_3) \ . \end{aligned} \tag{1.3.40}$$

Of course, bi-linearity and sesquilinearity are different only if the field $\mathbb{F} = \mathbb{C}$. Let $\{\vec{e}_i\}$ be a basis for the vector space V. A metric is specified by its action on the pairs of basis vectors. Let us denote

$$(\vec{e}_i, \vec{e}_j) = g_{ij} \ . \tag{1.3.41}$$

Then we have, for instance with a sesquilinear metric, $(\vec{v}, \vec{u}) = v^{i^*} g_{ij} u^j$. We assume that the metric is *non-degenerate*, that is that $\det g \neq 0$ (where g is the matrix of elements g_{ij}). Under a change of basis A, a sesquilinear metric transforms as follows:

$$g'_{ij} = (A_i{}^k)^* \, g_{kl} \, A_j{}^l \ . \tag{1.3.42}$$

Notice that g_{ij} transforms covariantly. In matrix form, Eq. (1.3.42) reads $g' = A * g \, A^T = (A^T)^\dagger \, g \, A^T$.

Diagonalization of the metric. Signature. If a (sesquilinear) metric is *hermitean*: $g_{ij} = g^*_{ji}$ (as it should be the case if we want to use it to define a scalar product and a notion of distance on our complex vector space), then it is always possible to find a basis change that puts it into a canonical form

$$g_{ij} \to \mathrm{diag}(\underbrace{1, \dots, 1}^{p}, \underbrace{-1, \dots, -1}^{q}) \ . \tag{1.3.43}$$

Indeed, we can first diagonalize g_{ij} to $\lambda_i \, \delta_{ij}$ changing basis with its eigenvector matrix $\vec{e}_i{}' = S_i{}^j \vec{e}_j$. Since g_{ij} in our hypothesis is hermitean, the eigenvalues λ_i are real. We can then further change basis rescaling the basis vectors to $\vec{f}_i = |\lambda_i|^{-1/2} \vec{e}_i{}'$ to obtain Eq. (1.3.43). A metric of canonical form Eq. (1.3.43) is said to have *signature* (p, q).

Metric-preserving changes of basis Having endowed a vector space with a metric, we can consider those automorphisms that *preserve the metric*. It is not difficult to see that such changes of basis form a subgroup of the general linear group. Indeed, if A and B are two changes of bases that preserve the metric, then the product change of basis BA also preserves it (check it), so closure is verified. Also the inverse of a metric-preserving automorphism preserves it, and the identity certainly does.

We now can identify the classical matrix groups as those subgroups of the general linear group that preserve certain types of metrics.

- The *pseudo-unitary group*[5] $\mathrm{U}(p, q; \mathbb{C})$ is the subgroup of $\mathrm{GL}(p + q, \mathbb{C})$ that preserves an *hermitean* sesquilinear metric of signature (p, q). The prefix pseudo- is dropped when the metric s definite positive, i.e. when $q = o$. In this case the metric in canonical form $g = \mathbf{1}$ is preserved by a basis change U iff $U^\dagger U = \mathbf{1}$.
- The *pseudo-orthogonal group*[6] $\mathrm{O}(p, q; \mathbb{R})$ is the subgroup of $\mathrm{GL}(p + q, \mathbb{R})$ that preserves a *symmetric* bilinear metric of signature (p, q). Similarly one can define $\mathrm{O}(p, q; \mathbb{C})$. For a positive definite metric, the condition to be preserved by a basis change O is just $O^T O = \mathbf{1}$.

It is interesting to consider from a similar perspective also *antisymmetric* bilinear forms on vector spaces; they, for instance, appear naturally in Hamiltonian mechanics.

- The *symplectic group* $\mathrm{Sp}(m, \mathbb{R})$ is the subgroup of $\mathrm{GL}(2m, \mathbb{R})$ that preserves an *antisymmetric* bilinear form ω (also called symplectic form). One can similarly define $\mathrm{Sp}(m, \mathbb{C})$.
  Notice that also a bilinear *antisymmetric* form $\omega_{ij} = -\omega_{ij}$ can be put into a canonical form. Such a form is non-degenerate only if the dimension n of the space is even, $n = 2m$. Indeed, $\det \omega = \det \omega^T = \det(-\omega) = (-)^n \det \omega$. If $n = 2m$, $\omega_i j$ can be first "skew-diagonalized" by a change of basis:

$$\omega_{ij} \to \begin{pmatrix} 0 & \lambda_1 & & \mathbf{0} & \dots \\ -\lambda_1 & 0 & & & \\ & & 0 & \lambda_2 & \dots \\ \mathbf{0} & & -\lambda_2 & 0 & \\ \vdots & & \vdots & & \ddots \end{pmatrix} \tag{1.3.44}$$

  and then brought to a canonical form by rescaling suitably the basis vector. The canonical form can be that of Eq. (1.3.44), with all λ_i reduced to 1, or the so-called symplectic form Ω already introduced in Eq. (1.3.20), obtained by a further reordering of the basis vectors.

[5] One usually writes simply $\mathrm{U}(p, q)$, as the real unitary groups coincide with orthogonal real groups (on real vector spaces there's no difference between sesquilinear and bilinear).
[6] One usually writes simply $\mathrm{O}(p, q)$, as the complex orthogonal groups are not so frequently used.

We may further restrict the automorphisms to preserve the volume element, i.e. to have unit determinant. In this case the various group acquire the denomination "special" and an S is prepended to their notation. For instance, $\mathrm{SL}(n,\mathbb{C}) \cap \mathrm{U}(n) = \mathrm{SU}(n)$, the special unitary group.

Example Let us compare the groups $\mathrm{SO}(2)$ and $\mathrm{SO}(1,1)$. A generic matrix $R \in \mathrm{SO}(2)$, namely a matrix satisfying $A^T A = \mathbf{1}$ and $\det A = 1$, can be parameterized by an angle θ as

$$R = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} . \tag{1.3.45}$$

A matrix $\Lambda \in \mathrm{SO}(1,1)$ must satisfy the following equations: $\Lambda^T \eta \Lambda = \eta$, where $\eta = \mathrm{diag}\,(-1,1)$, anddet $\Lambda = 1$. Writing Λ as a generic real 2×2 matrix $\Lambda = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, these equation read:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a^2 + c^2 & -ab + cd \\ -ab + cd & -b^2 + d^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.3.46}$$

and $ad - bc = 1$. Work out directly the solution to these requirements, that turns out to be the following:

$$\Lambda = \begin{pmatrix} \cosh\nu & \sinh\nu \\ -\sinh\nu & \cosh\nu \end{pmatrix} , \tag{1.3.47}$$

with ν a real parameter, called the "rapidity". A possible alternative is to introduce a parameter β related to the rapidity by $\cosh\nu = 1/\sqrt{1-\beta^2}$, $\sinh\nu = v/\sqrt{1-\beta^2}$. Does the resulting expression of Λ remind you of something (expecially if you write β as v/c)?

1.3.8 Isometries

The Euclidean group Eucl_d in d dimensions is in fact the group of invertible transformations of the Euclidean space $\mathbb{R}^d$ into itself that preserve the Euclidean distance: for any transformation $\mathcal{E} \in \mathrm{Eucl}_d$, if $\mathbf{x}'_1, \mathbf{x}'_2$ are the images under $\mathcal{E}$ of $\mathbf{x}_1, \mathbf{x}_2$, we have $|\mathbf{x}'_2 - \mathbf{x}'_1| = |\mathbf{x}_2 - \mathbf{x}_1|$, for any couple $\mathbf{x}_1, \mathbf{x}_1$. Check that this agrees with the explicit description of $\mathrm{Eucl}_{2,3}$ given before. Notice that the Euclidean distance is the one arising from having endowed the vector space $\mathbb{R}^d$ with a symmetric bilinear metric positive definite $g_{ij} = \delta_{ij}$. This defines the scalar product $(\mathbf{x}, \mathbf{y}) = x^i g_{ij} y^j = \mathbf{x} \cdot \mathbf{y}$, and hence the distance $|\mathbf{x} - \mathbf{y}| = \sqrt{(\mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y})}$.

More in general, a notion of distance can be introduced not only on vector spaces, but on manifolds. Then one talks of Riemannian manifolds, i.e., differentiable manifolds of dimension d equipped with a positive definite quadratic form, that is a metric locally expressible as

$$ds^2 = g_{\alpha\beta}\, dx^\alpha \vee dx^\beta , \quad g_{\alpha\beta} = g_{\beta\alpha} \quad (\alpha, \beta = 1, \dots d) \tag{1.3.48}$$

with $g_{\alpha\beta}(x)$ a differentiable function of the coordinates (that transform as a two-tensor under coordinate changes). ds^2 defines the square length of the minimal arc connecting two points whose coordinates differ by dx^α.

Notice that this indeed is the generalization of the concept of metric introduced for vector spaces, a part from the fact that here we require the metric to be symmetric, as we are interested in constructing a notion of distance. Indeed, the differentials dx^α are the generalization of the basis elements for the dual of a vector space, the space of linear functionals (as the partial derivatives $\vec{\partial}_\alpha$ are the generalizations of the basis vectors $\vec{e}_i$). The metric ds^2 of Eq. (1.3.48)

therefore is a functional assigning to any couple of tangent vectors $\vec{v} = v^\alpha \vec{\partial}_\alpha$, $\vec{w} = w^\beta \vec{\partial}_\beta$, a real number. The functional is specified by its value on any pair of basis vectors $\vec{\partial}_\alpha$, $\vec{\partial}_\beta$, namely $g_{\alpha\beta}$.

On Riemannian manifolds there is a notion of distance, defined through the metric:

$$d(x,y) = \min_\gamma \int_\gamma ds \ , \tag{1.3.49}$$

where γ is a path connecting the points x and y; the "minimal length" path (defined as in Eq. (1.3.49)) is called a *geodetic* curve. An *isometry of a Riemannian manifold* is an invertible coordinate[7] transformation $x \mapsto x'$that preserves the metric: $ds'^2 = g_{\alpha\beta}(x')dx^\alpha dx^\beta = ds^2$.

For Euclidean spaces $\mathbb{R}^d$, the metric can always be chosen to be constant. Thus the possible transformations are of the form $x'^\alpha = \mathcal{R}^\alpha{}_\beta \, x^\beta + v^\alpha$, that is, in matrix notation, $\mathbf{x}' = \mathcal{R}\mathbf{x} + \mathbf{v}$. It is easily seen that the metric, which in matrix notation is written as $ds^2 = d\mathbf{x}^T \, g \, d\mathbf{x}$, is invariant iff

$$\mathcal{R}^T \, g\mathcal{R} = g \ . \tag{1.3.50}$$

In a coordinate choice where $g_{\alpha\beta} = \delta_{\alpha\beta}$, the isometry condition becomes simply $\mathcal{R}^T\mathcal{R} = \mathbf{1}$, namely, $\mathcal{R} \in O(d)$. We retrieve thus the description of Euclidean isometries as products of translations ad orthogonal transformations (rotations plus inversions).

1.3.9 Geometric symmetry groups

The intuitive notion of "how much symmetry a geometric figure possesses" cen be made rigorous by turning it into the discussion of the symmetry group of the figure. The symmetry group of a given plane figure (or a body in three-space) is the subgroup of Eucl_2 (or of Eucl_3) containing all transformations (rotations, reflections, translations) that leave the figure invariant.

Only a figure which is infinitely extended or repeated in some direction can be invariant under a translation subgroup. We will concentrate here on finite figure, whose symmetry group is a subgroup of the (proper and improper) rotation group O(2) (or O(3) in the three-dimensional case).

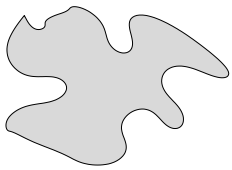

Figure 1.1. A generic plane figure has no symmetry.

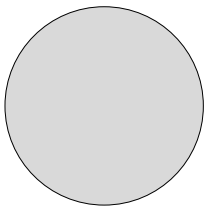

Figure 1.2. A circular disk is the most symmetric finite figure.

Consider for instance a *generic* "blot": it is not symmetric. In fact, only the identical transformation of the plane leaves it invariant, see Fig. 1.1: its symmetry group is the trivial subgroup of Eucl_2. Consider instead a round disk B_2, see Fig. 1.2. It is the most symmetric finite figure. Indeed it is left invariant by all rotations around its center, and by reflections w.r.t. to any axis through the center: its symmetry group is this the entire O(2) subgroup of Eucl_2.

[7] We are taking the so-called "passive" point of view instead of the "active" point of view used in previous examples, in which we regarded all transformations as mapping a point x to a different point x'. Both viewpoints are possible, but is more customary to take the passive one, expecially in the context of General Relativity.

Analogous rople is played by the three-ball B_3 (i.e., the filled three-sphere S_3) in $\mathbb{R}^3$ and, in general, by B_d in $\mathbb{R}^d$.

We will consider in the following regular polygons and regular polyhedra. It is intuitively clear that these figure possess symmetries forming discrete subgroups of the O(2) or O(3) symmetry of the disk or the three-sphere.

1.3.10 The dihedral groups $\mathbb{D}_n$

Let us start from the regular polygons in $\mathbb{R}^2$, and let us exhamine their symmetry groups. The the symmetry groups of regular n-gons are named dihedral groups and are denoted as $\mathbb{D}_n$.

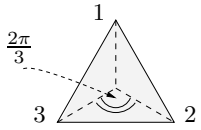

Figure 1.3. A regular triangle.

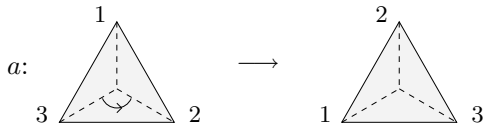

Figure 1.4. The generator of the $\mathbb{Z}_3$ rotation subgroup.

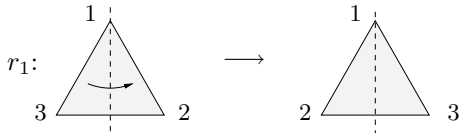

Figure 1.5. Reflection w.r.t the axis through the vertex 1.

Let us start grom an equilateral triangle, of which it is useful to label the vertices explicitely, see Fig. 1.3. The triangle is obviously invariant under the group of *rotations* around its center by angles which are multiple of $2\pi/3$. This is a $\mathbb{Z}_3$ group generated by (say) the counter-clock-wise rotation of $2\pi/3$, which we denote by a (see Fig. 1.4). It is also invariant under *reflections* r_i $(i = 1, 2, 3)$ with respect to an axis through the i-th vertex and the middle point of its opposite side, see Fig. 1.5.

Check that the 6 elements described above form a group (the product being the composition of the transformations) and write its multiplication table. Is the group, which is named $\mathbb{D}_3$, Abelian?

$\mathbb{D}_3$ has rank 2. Indeed it is generated by a and by one of the reflections which we may denote as b (for instance, $b = r_1$). Check that indeed one has $r_2 = ab$ and $r_3 = a^2 b$. Thus $\mathbb{D}_3$ can be abstractly seen as the group generated by a, b subject to the relations

$$a^3 = e \ , \quad b^2 = e \ , \quad (ab)^2 = e \ . \tag{1.3.51}$$

Above, $(ab)^2 = e$ because $ab = r_2$ is a reflection; check that the relation telling us that also $a^2 b$ is a reflection, namely $(a^2 b)^2 = e$, has not to be included separately in Eq. (1.3.51) as it follows from the others. The group $\mathbb{D}_3$ turns out to be isomorphic to to S_3 (check it).

Let us consider now the symmetries of a square, see Fig. 1.6. Of course, there is a $\mathbb{Z}_4$ cyclic subgroup generated by a, namely the counter-clock-wise rotation of $\pi/2$, see Fig. 1.7. Then there are the reflections w.r.t. the diagonals and the axes through the middle points of opposite sides. Let us name such reflections, using the labels of Fig. 1.8, as follows: r_1 is the reflection w.r.t to the axis $1 - 3$, r_1 is w.r.t. the axis $2 - 4$, r'_1 w.r.t. the axis $1' - 3'$ and r'_2 w.r.t. the axis $2' - 4'$.

Altogether, we have a group, $\mathbb{D}_4$, of order 8. It has rank 2, as it is generated by a and by b, where b is one of the reflections, e.g., $b = r_1$. Indeed, one can check easily that $ab = r'_1$, $a^2 b = r_2$

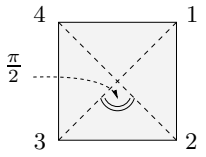

Figure 1.6. A square ($n = 4$).

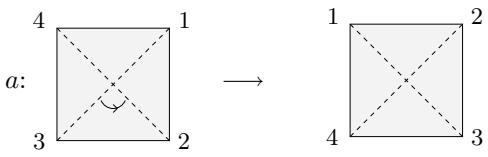

Figure 1.7. The generator of the $\mathbb{Z}_4$ rotation subgroup.

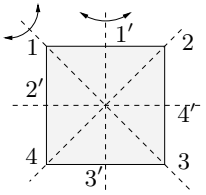

Figure 1.8. Axes defining the reflection symmetries.

and $a^3 b = r'_2$. The group is abstractely presented by means of two generators a, b subject to the relations

$$a^4 = e \ , \quad b^2 = e \ , \quad (ab)^2 = e \ . \tag{1.3.52}$$

Next comes the pentagon. It is easy to see that its symmetry group, $\mathbb{D}_5$, contains a cyclic subgroup $\mathbb{Z}_5$ and 5 reflections r_i w.r.t. the axes through the i-th vertex and the middle point of the opposite sid and that it is generated by a, b subject to the relations

$$a^5 = e \ , \quad b^2 = e \ , \quad (ab)^2 = e \ , \tag{1.3.53}$$

where b is any of the reflections.

The general outcome is that the group $\mathbb{D}_n$ contains

- the $\mathbb{Z}_n$ subgroup by a, where a is the counter-clock-wise rotation of angle $2\pi/n$ about the centre of the figure;
- n reflection operations with respect to n symmetry axes which are the following:
  - for n even, $n/2$ axes through opposite vertices, and $n/2$ axes through the middle points of opposite sides;
  - for n odd, n axes through a vertex and the middle point of its opposite side.

Such a group turns out to be abstractly described as the group generated by two generators a and b, subject to the relations

$$a^n = e \ , \quad b^2 = e \ , \quad (ab)^2 = e \ , \tag{1.3.54}$$

In the geometric interpretation, a is the rotation of angle $2\pi/n$ and b any of the reflections. It follows from the presentation Eq. (1.3.54) that the order of $\mathbb{D}_n$ is $|\mathbb{D}_n| = 2n$, the elements being

$$\{e, a, a^2, \ldots, a^{n-1}, b, ab, a^2 b, \ldots, a^{n-1} b\} \ . \tag{1.3.55}$$

1.3.11 Symmetry group of the tetrahedron

Analogously to the case of regular polygons in the plane, one can dissuss the symmetry groups of regular polyhedra in $\mathbb{R}^3$. Let us take the simplest example, the *tetrahedron*. In Fig. **??** are

described the proper rotations, i.e., the elements of SO(3), that leave invariant a tetrahedron. They form a group which is isomorphic to the alternating group A_4. Indeed, all these discrete operations correspond to an even permutation of the 4 vertices. If we adjoin to the above the reflections with respect to suitable planes, that is, if we consider symmetry operations that belong to $O(3)$, the symmetry group is enlarged to the full symmetric group S_4. Indeed, referring to the notations in Fig.**??**, consider for instance a reflection with respect to the plane containing the side 1-2 and the bisecant in 1 of the face individuated by $1, 3, 4$ (and the bisecant in 2 of the face individuated by $2, 3, 4$). This reflection corresponds to the single exchange (34). The single exchanges being obtained by reflections with respect to such symmetry planes, the entire S_4 is then generated by these.

1.3.12 Platonic solids and discrete subgroups of SO(3)

Regular polyhedra While there exist regular polygons in the plane with any given number of sides, it is well known since Plato that very few regular polyhedra can be constructed in $\mathbb{R}^3$. Indeed, consider a regular polyhedron made of plaquettes that are n-gons, such that in each vertex of the polyhedron we have the confluence of f plaquettes (with $f \geq 3$). The angle at each vertex of a regular n-gon is $\pi - 2\pi/n$, see Fig. **??**. In each vertex of the polyhedron, the sum of the vertex angles of the f plaquettes should be less than 2π, so that in the vertex a "positive curvature" is present, and the geometric figure can close itself: thus, the Diophantine inequality

$$f\left(\pi - \frac{2\pi}{n}\right) < 2\pi \quad \Rightarrow \quad f\left(1 - \frac{2}{n}\right) < 2 \tag{1.3.56}$$

must be satisfied. It is easy to check that this inequality admits anly 5 solutions.

	V	L	F	χ	dual to
Tetrahedron	4	6	4	2	self-dual
Octahedron	6	12	8	2	Cube
Icosahedron	12	30	20	2	Dodecahedron
Cube	8	12	6	2	Octahedron
Dodecahedron	20	30	12	2	Icosahedron

Table 1.1. Vertices, sides and faces of the possible regular polyhedra.

We may have $n = 3$ and $f = 3, 4, 5$, or $n = 4$ and $f = 3$, or $n = 5$ and $f = 3$. Thus a regular polyhedron can only have faces that are triangles ($n = 3$), squares ($n = 4$) or pentagons ($n = 5$). The polyhedron such that in each vertex enter $f = 3$ triangles is the *tetrahedron*, see Fig **??**. It has 4 vertices, 6 sides and 4 faces. If in any vertex enter $f = 4$ triangles, we have an *octahedron*, with 6 vertices, 12 sides and 8 faces, see Fig **??**. If in any vertex enter $f = 5$ triangles, we have an *icosahedron*, with 12 vertices, 30 sides and 20 faces, see Fig. **??**. The polyhedron with $f = 3$ squares meeting at ach vertex is the *cube*, see Fig. **??**; a cube has 8 vertices, 12 sides and 6 faces. Finally, $f = 3$ pentagons meeting in each vertex corresponds to the *dodecahedron*, with 20 vertices, 30 sides and 12 faces, see Fig. **??**.

Discrete subgroups of SO(3) A regular polygon with n sides in $\mathbb{R}^2$ could be regarder as the simplest geometric figures that is preserved by the discrete $\mathbb{Z}_n$ subgroup of the rotation group SO(2). In this perspective, the existence of infinite regular polygons is due to the existence of the infinite family $\mathbb{Z}_n$, with $n \in \mathbb{N} \geq 2$, of such discrete subgroups. The actual symmetry group of a

n-gon, as we saw, is enlarged from $\mathbb{Z}_n$ to $\mathbb{D}_n$ by reflections (elements of O(2) but not of SO(2); nevertheless the correct classification of polygons requires just the classification of SO(2) discrete subgroups.

In the three-dimensional case, one could take the same point of view and try to classify directly the possible discrete subgroups of SO(2). The result should be then compared to the geometrical classification of regular bodies.

....

1.3.13 The modular group

A torus $\mathcal{T}$ is a parallelogram with opposite sides identified, see Fig. 1.16. When embedded in $\mathbb{C}$,

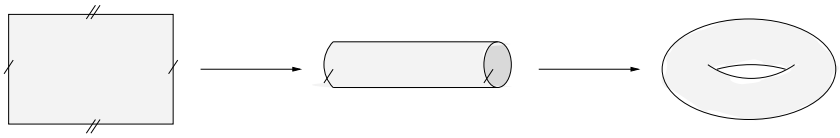

Figure 1.9. The torus seen as a parallelogram with sides identified.

the parallelogram is individuated by two vectors (i.e., two complex numbers) ω_1, ω_2. Indeed T can be defined (see Fig. 1.10) as the quotient space

$$\mathcal{T} = \mathbb{C}/\Lambda \ , \tag{1.3.57}$$

where Λ is the lattice generated by ω_1, ω_2:

$$\Lambda = \{m\omega_1 + n\omega_2 \ , \quad m, n \in \mathbb{Z}\} \ . \tag{1.3.58}$$

We require $\omega_1, 2 \neq 0$ and $\omega_1/\omega_2 \notin \mathbb{R}$ to avoid degeneracy (if $\omega_1/\omega_2 \in \mathbb{R}$, the two vectors are

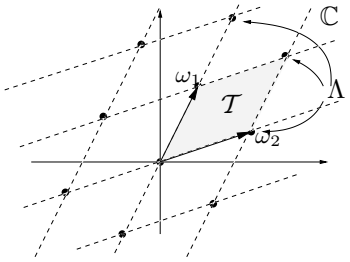

Figure 1.10. The torus seen as the quotient of the complex plane by a lattice Λ.

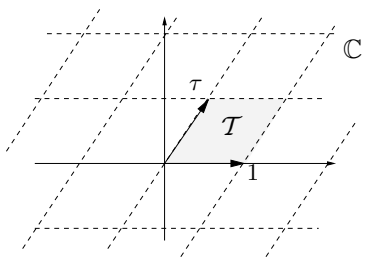

Figure 1.11. The canonical form of a torus in the complex plane.

linearly dependent), and in fact we impose further that $\mathrm{Im}(\omega_1/\omega_2) > 0$. This latter choice fixes n ordering (i.e., an orientation) so as to avoid redundant descriptions simply related by $\omega_1 \leftrightarrow \omega_2$.

By means of *conformal transformations*, i.e. analytic mappings well-defined on $\mathbb{C}$, of the form $z \to w = az + b$, we can rotate and rescale ω_2 to 1, putting the parallelogram in the canonical form of Fig. 1.11, where τ ($\equiv \omega_1/\omega_2$) is named the *modulus* of the torus $\mathcal{T}$. As we said, we take $\mathrm{Im}\tau > 0$. The modulus τ cannot be further changed by conformal transformations; it is a conformal invariant. Therefore there are infinitely many *conformally inequivalent* tori parametrized by $\tau \in \mathbb{H}$ (where $\mathbb{H}$ is the standard notation for the upper half-plane).

However, the torus being defined as $\mathcal{T} = \mathbb{C}/\Lambda$, it is invariant under *changes of basis* that *preserve the lattice* Λ: these are integer changes of bases with unit determinant:

$$\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \to \mathcal{M}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\ ,\quad a,b,c,d\in\mathbb{Z}\ ,\quad ad-bc=1\ . \tag{1.3.59}$$

Namely, the change of basis is by a matrix $\mathcal{M}\in \mathrm{SL}(2,\mathbb{Z})$. Under such a change of basis, the modulus τ undergoes the following transformation M:

$$M:\ \tau = \frac{\omega_1}{\omega_2} \mapsto \tau' = \frac{\omega_1'}{\omega_2'} = \frac{a\omega_1+b\omega_2}{c\omega_1+d\omega_2} = \frac{a\tau+b}{c\tau+d}\ . \tag{1.3.60}$$

The transformations described above form a group $\mathfrak{M}$ which is called the *modular group* of the torus $\mathcal{T}$. Notice that $\mathfrak{M}$ is *homomorphic* to $\mathrm{SL}(2,\mathbb{Z})$ through the two-to-one mapping

$$\sigma:\ \left(\pm\mathcal{M} = \pm\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z})\right) \mapsto \left(M:\ \tau\to\frac{a\tau+b}{c\tau+d}\in\mathfrak{M}\right)\ : \tag{1.3.61}$$

an overall change of sign does not matter in M as it cancels in the ratio.

The modular group $\mathfrak{M}$ has rank 2. It is generated by

$$S:\ \tau\to -\frac{1}{\tau}\ ,\qquad \left(\text{corresponding to }\ \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right)\ ; \tag{1.3.62}$$

and

$$T:\ \tau\to\tau+1\ ,\qquad \left(\text{corresponding to }\ \pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)\ . \tag{1.3.63}$$

These generators are subject to the following two relations:

$$S^2 = \mathbf{1}\ ,\qquad (ST)^3 = \mathbf{1}\ . \tag{1.3.64}$$

The first relation is obvious, the second arises as follows:

$$\tau \xrightarrow{ST} -\frac{1}{\tau+1} \xrightarrow{ST} -\frac{\tau+1}{\tau} \xrightarrow{ST} \tau\ . \tag{1.3.65}$$

Notice that ST corresponds in $\mathrm{SL}(2,\mathbb{Z})$ to $\pm\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$, whose cube is indeed $\pm\mathbf{1}$.

1.3.14 Symmetry operations in quantum mechanics

We all know that symmetry operations are implemented in quantum mechanics as unitary operators on the Hilbert space. For instance, geometrical transformations in the coordinate space $\mathbb{R}^3$, such as translations or rotations, are associated to linear operators acting on wave-functions $\psi(\mathbf{x})$ as follows. Consider a transformation $\mathcal{R}:\ \mathbf{x}\mapsto\mathbf{x}' = R\mathbf{x}$. The corresponding action R on the wave-functions is defined requiring that

$$(R\psi)(\mathcal{R}\mathbf{x}) = \psi(\mathbf{x})\ , \tag{1.3.66}$$

or equivalently that $R\psi(\mathbf{x}) = \psi(\mathcal{R}^{-1}\mathbf{x})$. That is, the value if the transformed wave-function $R\psi$ at a point $\mathbf{x}$ is the value of the original function ψ at the pre-image $\mathcal{R}^{-1}\mathbf{x}$ of the point. The

operator R so defined is generically *unitary* (certainly it is so if the operation is an isometry of $\mathbb{R}^3$, as the scalar product involves an integration:

$$(R\psi, R\phi) = (\psi, \phi) = \int d^3x\, \psi^*(\mathbf{x})\phi(\mathbf{x}) \ . \tag{1.3.67}$$

For instance, translations by a vector $\mathbf{a}$, $\mathcal{T} : \mathbf{x} \mapsto \mathbf{x} + \mathbf{a}$ is realized by the operator $T = \exp(-\mathrm{i}\mathbf{a} \cdot \mathbf{p}/\hbar)$, where $\mathbf{p} = -\mathrm{i}\,\hbar\nabla$ is the momentum operator. Rotations $\mathcal{R}$ of an angle θ around an axis individuated by a versor $\mathbf{n}$ are represented by the operator $R = \exp(-\mathrm{i}\mathbf{n} \cdot \mathbf{L}/\hbar)$, where $\mathbf{L} = -\mathrm{i}\,\hbar\mathbf{x} \wedge \nabla$ is the angular momentum operator[8].

If the transformations $\mathcal{R}$ form a group, the composition of such transformations maps homomorphically into products of linear operators. In fact, to the transformation $\mathbf{x} \mapsto \mathcal{R}(\mathcal{S}\mathbf{x})$ is associated the operator RS:

$$\psi(\mathcal{S}^{-1}(\mathcal{R}^{-1}\mathbf{x})) = S\psi(\mathcal{R}^{-1}\mathbf{x}) = RS\psi(\mathbf{x}) \ . \tag{1.3.68}$$

Thus, symmetry groups have a *representation* by means of unitary operators acting on the Hilbert space. It is then clear that unitary representations of groups are a subject of great importance in group theory, expecially for a physicist.

1.3.15 Groups of invariance of operators

Consider a group G acting as a transformation group on a given space, typically as a group of linear operators on a vector space V, finite or infinite-dimensional. In the case of quantum mechanics, for instance, think of a group of unitary operators on the Hilbert space associated to some symmetry group. Consider any other operator O acting on the same space V (for instance, a quantum mechanical hermitean operator on the Hilbert space corresponding to some observable). The group transformations R induce an action on O given by

$$O \mapsto O' = R\,O\,R^{-1} \ . \tag{1.3.69}$$

In the case of quantum mechanics, for instance, in fact we determine O' by requiring $(\psi, O\phi) = (R\psi, O'R\phi)$, whence $O' = ROR^{-1}$ indeed.

In particular, in quantum mechanics, consider the Hamiltonian operator H. A transformation R on the Hilbert space is a *symmetry* of the quantum mechanical system if it leaves the Hamiltonian invariant, that is if

$$R\,H\,R^{-1} = H \ , \tag{1.3.70}$$

or, equivalently, $RH = HR$, namely if R *commutes* with H. The set of transformations that leave H invariant form a group, the *group of invariance* of the Hamiltonian. Some typical examples:

- *Rotations* The group of invariance of a quantum mechanical system with spherically symmetric potential contains the rotation group SO(3), a continuous group.
- *Point groups* Consider a crystalline configuration. The Hamiltonian is invariant under symmetry operations that bring the arrangement of atoms into itself (these form discrete groups).
- *Translations* The electron wave-function in a perfect crystal feels a periodic potential. The Hamiltonian is invariant under lattice translations.

[8] Note that the unitary operators above are written as exponentials of *hermitean* operators, e.g the momentum and the angular momentum, which generate *infinitesimal* transformations. We will come back to this when discussing continuous groups

- *Identical particles* The Hamiltonian H for a system of n identical particles is invariant with respect to permutations of the particles' coordinates.

We will see that the structure of representations of the group of invariance of H leads to a group-theoretical explanation of the degenerations of the eigenvalues of H, i.e. of the energy levels.

1.3.16 The first homotopy group of a manifold

Certain groups, called *homotopy groups* of a manifold $\mathcal{M}$, and denoted as $\Pi_n(\mathcal{M})$, with $n \in \mathbb{N}$, play a very important role in the topological characterization of manifolds. We will discuss here the group $\Pi_1(\mathcal{M})$, which will also play some role later in our discussion of the topological properties of continuous groups. Our description will be at an extremely intuitive level. We refer to other text such as ... for a more precise and rigorous introduction to the subject.

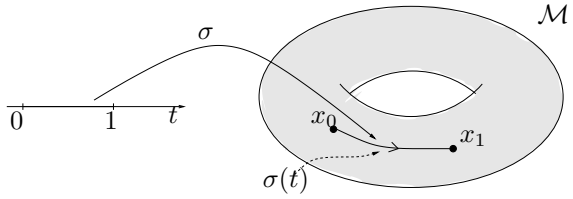

Figure 1.12. Curves $\sigma : I \subset \mathbb{R} \mapsto \mathcal{M}$ on a manifold $\mathcal{M}$

We consider *curves* on a manifold $\mathcal{M}$, namely maps σ from an interval $I \subset \mathbb{R}$ (which can be fixed, without loss of generality, to $I = [0, 1]$) to $\mathcal{M}$; see Fig. 1.12. The curves can be naturally "oriented" by considering that the curve evolves in the direction of t growing (we may think of the parameter t as a "time" during which we follow the path $\sigma(t)$ on $\mathcal{M}$. Thus a curve σ goes from $x_0 = \sigma(0)$ to $x_1 = \sigma(1)$.

It is possible and natural to define the *product* $\tau\sigma$ of two curves τ and σ as the curve obtained by doing "first" the path σ and then the path τ. That is, supposing that σ goes from x_0 to x_1, and τ from x_1 to x_2, we define

$$\tau\sigma(t) = \begin{cases} \sigma(2t) \ , & 0 \leq t \leq \frac{1}{2} \ ; \\ \tau(2t-1) \ , & \frac{1}{2} < t \leq 1 \ . \end{cases} \tag{1.3.71}$$

Two curves σ, τ having the same extrema x_0, x_1 are said to be *homotopic* (and we write then $\sigma \sim \tau$) iff they are continuously deformable into each other. In more precise terms, there must exist a *continuous* function $F : I \times I \mapsto \mathcal{M}$ such that

$$\begin{cases} F(t,0) = \sigma(t) \ , \\ F(t,1) = \tau(t) \ , \end{cases} \quad \forall t \in I \ ; \quad \begin{cases} F(0,s) = x_0 \ , \\ F(t,1) = x_1 \ , \end{cases} \quad \forall s \in I \ . \tag{1.3.72}$$

Namely, $F(t, s)$ represent a family of curves, parametrized by s, all with the same fixed extrema, and such that they are continuosly deformed from the curve $\sigma(t)$ (for $s = 0$) to the curve $\tau(t)$ (for $s = 1$), see Fig. 1.13.

The relation "being homotopic to" is an *equivalence relation*, as it is easy to see. Therefore, it makes sense to discuss *homotopy classes* of curves, denoted as $[\sigma]$. It is immediate to verify that the product of curves, defined as in Eq. (1.3.72), respects the homotopy relation. Namely,

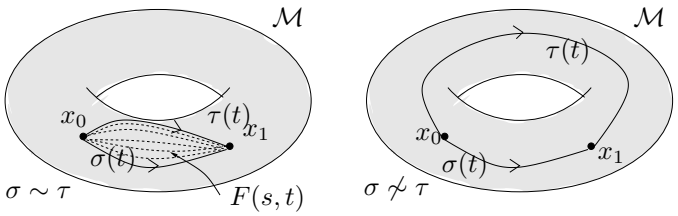

Figure 1.13. Homotopically versus non-homotopically equivalent curves.

if $\sigma \sim \sigma'$ and $\tau \sim \tau'$, then also $\tau\sigma \sim \tau'\sigma'$. Thus the product Eq. (1.3.72) gives rise to a *product of homotopy classes*: $[\sigma][\tau] \equiv [\sigma\tau]$.

Let us consider the *loops* based in a point $x_0 \in \mathcal{M}$, that is the curves σ such that $\sigma(0) = \sigma(1) = x_0$. These curves can be viewed as continuous maps $\sigma(t)$ from S_1 into $\mathcal{M}$, where the circle S_1 is the *compactification* of the interval $I = [0, 2\pi]$

Let $\Pi_1(\mathcal{M}; x_0)$ be the set of *homotopy classes of loops* based at x_0. Equipped with the product of homotopy classes defined as above, $\Pi_1(\mathcal{M}; x_0)$ is a group. The identity is the class of constant loops, i.e. the class of *homotopically trivial* loops. The inverse of a loop is the loop with the opposite orientation: $\sigma^{-1}(t) = \sigma(1-t)$. Indeed, with this definition $\sigma^{-1}\sigma$ is homotopic to x_0, i.e. the constant loop, see Fig. 1.14.

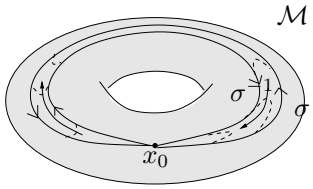

Figure 1.14. The product $\sigma^{-1}\sigma$ is homotopically trivial

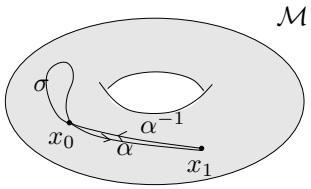

Figure 1.15. A curve α maps a loop based on x_0 into a loop based in x_1.

Any continuous path α from x_0 to x_1 establishes an *isomorphism* ϕ_α between the homotopy groups based at x_0 and x_1, see Fig. 1.15. Explicitely,

$$\begin{aligned} &\phi_\alpha \,:\, \Pi_1(x_0; \mathcal{M}) \longrightarrow \Pi_1(x_1; \mathcal{M}) \text{ , such that} \\ &\phi_\alpha \,: [\sigma] \mapsto [\alpha^{-1}\sigma\alpha] \text{ ,} \end{aligned} \tag{1.3.73}$$

where σ is a loop based in x_0. Check that the map ϕ_α is an homomorphism, and furthemore is invertible.

Thus, for an *arc-wise connected* manifold $\mathcal{M}$, that is, for a manifold such that any two points of $\mathcal{M}$ are joined by at least one *continuous* path, the abstract group $\Pi_1(x_0; \mathcal{M})$ is independent from the choice of the base point x_0. We can simply denote this group, which is known as the *first homotopy group* or *fundamental group* of $\mathcal{M}$, as $\Pi_1(\mathcal{M})$.

An arc-wise connected manifold is said to be *simply-connected* iff its homotopy group $\Pi_1(\mathcal{M})$ is trivial.

Examples

- On the two-sphere S_2, any two loops are deformable into each other, an in particular into

the constant loop, see Fig. **??**. Thus, there is an unique homotopy class: $\Pi_1(S_2)$ is trivial, and S_2 is simply connected.

- On the two-torus T_2, there are homotopically inequivalent loops, see Fig. **??**. Thus $\Pi_1(T_2)$ is non-trivial, and the torus T_2 is not simply-connected.

Homotopy groups are usually and naturally described in terms of *generators and relations*.

Examples

- Consider a circle S_1. The simplest homotopically non-trivial curve we can draw on it (see Fig. **??**): it is a map from S_1 to S_1 with *winding number* 1; let us call its homotopy class a. All further non-trivial classes are generated by taking products of this class. The generator a is of infinite order, since there is no way that making a map wind a certain number of times it becomes trivial. In this way we obtain classes a^n, for all $n \in \mathbb{Z}$. There is an evident isomorphism
$$\Pi_1(S_1) \leftrightarrow \mathbb{Z} \ , \tag{1.3.74}$$
given by associating $a^n \leftrightarrow n$. Indeed $a^n a^m = a^{n+m}$.
Notice that all higher-dimensional spheres S_d, $d > 1$, are instead simply-connected; we cannot draw any non-trivial loop on them.
- On the torus T_2 there are two evident instances of homotopically non-trivial loops. These loops are traditionally denoted as a, b, and are most easily described in when representing the torus as a parallelogram with opposite sides identified, see Fig. **??**. More complicated loops are obtained by taking products of a, b (and of their inverses). Thus, $\Pi_1(T_2)$ is a group of rank 2, generated by a, b. The generators satisfy a single relation, which is evident in the drawing of Fig. **??**:
$$aba^{-1}b{-}1 = e \ , \tag{1.3.75}$$
where of course e represent the trivial homotopy class. The relation Eq. (1.3.75) tells us that a and b commute. The group $\Pi_1(T_2)$ generated by a, b subject to this condition is Abelian, and a generic "word" constructed out of the generators, $a^{m_1}b^{n_1}a^{m_2}b^{n_2}\dots a^{m_k}b^{n_k}$, with $m_i, n_i \in \mathbb{Z}$, can be rearranged in the form $a^m b^n$. Thus, the products of loops of type a and of type b are completely independent, each corresponding to the homotopy group of an S_1, i.e. to $\mathbb{Z}$. The group $\Pi_1(T_2)$ is thus isomorphic to the*direct product*[9] of two $\mathbb{Z}$ groups:
$$\begin{aligned} \Pi_1(T_2) &\leftrightarrow \mathbb{Z} \oplus \mathbb{Z} \ , \\ a^m b^n &\leftrightarrow (m, n) \ . \end{aligned} \tag{1.3.76}$$
This decomposition of the fundamental group is related to the fact, easy to visualize, that topologically two-torus is the direct product of two circles: $T_2 = S_1 \times S_1$. In fact, it is possible to prove in general that for a direct product manifold one has
$$\Pi_1(\mathcal{M}_1 \times \mathcal{M}_2) = \Pi_1(\mathcal{M}_1) \otimes \Pi_1(\mathcal{M}_2) \ . \tag{1.3.77}$$
- For a multi-dimensional torus T_d, which can be defined as an hypercube with sides identified pairwise, the story is analogous to the case of T_2. Indeed, one finds d generators subjects to relations imposing that they commute with each other, so that in the end
$$\Pi_1(T_d) \leftrightarrow \underbrace{\mathbb{Z} \oplus \mathbb{Z} \dots \oplus \mathbb{Z}}_{d \,\text{times}} \ . \tag{1.3.78}$$

[9] We will discuss later the notion of *direct product* $G_1 \otimes G_2$ of two groups. Let us notice here that the additive notation $\oplus$ for the direct *product* $\mathbb{Z} \oplus \mathbb{Z}$ is traditional and due to the fact that the group operation in $\mathbb{Z}$, the addition, is denoted as $+$.

This agrees with the fact that topologically $T_d = S_1 \times S_1 \ldots \times S_1$ (d times).

- In the examples above, all generators of the fundamental group were of infinite order. This is not always true. As an example,consider the manifold[10] $S^2/\mathbb{Z}_2$. The $\mathbb{Z}_2$ by which we are taking the quotient acts by identification of anti-podal points. Thus $S^3/\mathbb{Z}_2$ can be described as an hemi-sphere, with the equator being further subject to the identification of opposite points. On this space there there is a non-trivial loop a, which is closed only because of the identifications on the equator, see Fig. **??**. This non-trivial loop can be continuosly deformed, as suggested in the figure, into its inverse a^{-1}. This means that $[a] = [a^{-1}] = [a]^{-1}$, namely, the homotopyclass of a is of order 2. There is no other non-trivial class, so all in all

$$\Pi_1(S^2/\mathbb{Z}_2) = \mathbb{Z}_2 \ . \tag{1.3.79}$$

  As another example, try to describe the fundamental group of the Moebious strip (assuming you know what it is).

1.4 Basic structure properties of groups

A basic aim of group theory is that of *classifying* the groups. If this was accomplished, given a specific realization of a group arising, e.g., in some physical situation, one could then just look for an isomorphic realization of the group sitting in the general classification and read from it (via the isomorphism) the relevant properties of the group. For finite groups, this would mean to classify all the possible distinct (non-isomorphic) groups of a given finite order n. This is too much, but there is a logical way to proceed.

One is able to single out certain types of groups (the so-called *simple* groups) which are the "hard core" of the possible different group structures. These have to be classified. This has been achieved (recently? What are the references) after a huge effort, and with much aid from computers. We will not discuss the classification, except for some series that are easily individuated or defined.

Then one has to study the possible *extensions* by which further groups can be built, having simple groups as building blocks, and so on. Again, we will not discuss much this problem, except for some simple instances of extensions such as the direct and semi-direct products.

Also for groups of infinite order there are some general results in the line of a classification, mainly regarding Abelian groups. we will touch briefly on this.

Finally, for Lie groups the quest for a classification follows a very similar pattern to the case of finite groups, involving the definition of *simple* Lie groups to be classified first. This we will discuss in later chapters.

To start the search for the classification of groups, though, one has first of all to introduce many concepts and entities related to the inner structure of a given group; for instance, essential is the concept of conjugacy classes and of *invariant* subgroups[11]. These concepts and entities which permits us to discuss in much finer detail the structure of groups (in particular of finite groups) are the subject of this section.

[10] This manifold is also called $\mathbb{R}P^2$, the *real projective plane*, namely the space of all lines through the origin in $\mathbb{R}^3$, which indeed are in correspondence with the points of an unit S_2 up to identification of antipodal points.

[11] Indeed the essential properties of a group should be independent from the labeling of elements; the term *invariant* used above means in fact invariant under (inner) automorphisms, as we will see.

1.4.1 Cayley's theorem

Let us start with a theorem that at first sight seems to bring under control the problem of the classification of finite groups.

Cayley's theorem states that any group G of *finite* order $|G|$ is *isomorphic to a subgroup of the permutation group* on $|G|$ objects, $S_{|G|}$.

An obvious consequence of Cayley's theorem is that the number of distinct groups of order G is finite, as the number of subgroups of $S_{|G|}$ certainly is. It can also be used to determine the possible group structures of low orders. However, though the permutation groups are easily defined, the structure of its subgroups is far from obvious, and the problem of classifying the finite groups is far from being solved by Cayley's theorem alone.

The proof of Cayley's theorem stays in the observation that the in fact each row of the multiplication table defines a distinct permutation of the elements of the group. We can thus associate to a given element $g \in G$ the permutation $\pi \in S_{|G|}$ that acts as $g_k \overset{\pi_i}{\longmapsto} (gg_k)$ ($k = 1, \dots |G|$). To distinct group elements are associated distinct permutations. The identity e is mapped into the identical permutation π_e. The product is preserved by the mapping: indeed we have, for any $c, b \in G$,

$$\pi_c \pi_c = \begin{pmatrix} bg_1 & \dots & bg_n \\ cbg_1 & \dots & cbg_n \end{pmatrix} \begin{pmatrix} g_1 & \dots & g_n \\ bg_1 & \dots & bg_n \end{pmatrix} = \begin{pmatrix} g_1 & \dots & g_n \\ cbg_1 & \dots & cbg_n \end{pmatrix} = \pi_{cb} \ , \tag{1.4.80}$$

were we have described, for convenience, π_c by its action on the elements bg_i; this amounts just to a relabeling of the elements g_i. All in all, the set $\{\pi_b \, : \, b \in G\}$ is a subgroup of $S_{|G|}$ isomorphic to G.

Regular permutations The permutations π_g associated to the elements $g \in G$ in the previous isomorphism can be read directly from the multiplication table of the group. Such permutations are called *regular* permutations, and the subgroups of S_n isomorphic to groups G of order n are subgroups of regular permutations. Let us summarize here some properties of such subgroups.

i) A part from the identical permutation, all other π_g do not leave any "symbol" (any of the objects on which the permutation acts) invariant; this corresponds to the property of the rows of the multiplication table of G.
ii) Any of the n permutations $\pi_g$maps a given symbol in a different symbol; this corresponds to the property of the columns of the multiplication table.
iii) All the cycles in the cycle decomposition of a regular permutation have the same length. Indeed, if a regular permutation π_g had two cycles of lengths $l_1 < l_2$, then $(\pi_g)^{l_1}$would leave invariant the elements of the first cycle, but not those of the second, which however cannot be the case for a regular permutation.

Cayley's theorem is useful in determining the possible group structures, for instance of low order. As an exercise, use it to determine the possible group structures of order 4, 5 and 6. Also, the following result can be obtained as corollary of Cayley's theorem.

Groups of prime order The only group structure of order p, where p is a prime, is the cyclic group $\mathbb{Z}_p$. Indeed, by Cayley's theorem, such a group is isomorphic to a subgroup of S_p made of regular permutations. Since all cycles of a regular permutation must have the same length, this latter must be a divisor of p. But then the possible regular permutations have p cycles of length 1 (in which case we have the identical permutation) or one cycle of length p, which is the case for cyclic permutations. The subgroup can only be the subgroup of cyclic permutations, which is isomorphic to $\mathbb{Z}_p$.

1.4.2 Left and right cosets

Let $H = \{e = h_1, h_2, \dots h_m\}$ be a subgroup of G of order $|H| = m$. Given an element a_1 not in H, $a_1 \in G \setminus H$, define its *right coset* (or "complex")

$$a_1 H = \{a_1, a_1 h_2, \dots a_1 h_m\} \ . \tag{1.4.81}$$

Since $h_i \neq h_j$, $\forall\, i, j = 1, \dots m$, we have also $a_1 h_i \neq a_1 h_j$ (otherwise $a_1 = e$, but then a_1 would belong to H). Moreover, $\forall\, i$, $a_1 h_i \notin H$, otherwise $a_1 h_i = h_j$ for some j, and therefore $a_1 = h_j (h_i)^{-1}$ would belong to H. We can now take another element a_2 of $G \setminus H$ not yet contained in $a_1 H$. The m elements of its left coset $a_2 H$ are again all distinct, for the same reasoning as above. Moreover, $\forall\, i$, $a_2 h_i \notin H$, as above, but also $a_2 h_i \notin a_1 H$, otherwise we would have $a_2 h_i = a_1 h_j$, for some j, so that $a_2 = a_1 h_j (h_i)^{-1}$ would belong to $a_1 H$. We can iterate the reasoning until we exhaust all the elements of G.

Thus G decomposes into a *disjoint union* (or *partition*) of right cosets with respect to a subgroup H:

$$G = H \cup a_1 H \cup a_2 H \cup \dots \cup a_l H \ . \tag{1.4.82}$$

Of course, in a perfectly analogous manner, given a subgroup H, we can introduce the *left cosets*

$$H a_1 = \{a_1, h_2 a_1, \dots h_m a_1\} \ , \tag{1.4.83}$$

and we can repeat the entire reasoning done above for the left cosets.

A consequence of the above construction is the following important theorem.

1.4.3 Lagrange's theorem

Lagrange's theorem states that the order of a subgroup H of a finite group G is a divisor of the order of G:

$$\exists\, l \in \mathbb{N} \text{ such that } \ |G| = l\, |H| \ . \tag{1.4.84}$$

The integer l is called the *index* of H in G. Lagrange's theorem is very important for the task of classifying possible subgroups of given groups. For instance, if $|G| = p$ is a prime, G does not admit any proper subgroup. This indeed is the case for $G = \mathbb{Z}_p$ (the only group of order p, as we saw before).

Corollary A corollary of Lagrange's theorem is that the *order* of any element of a finite group G is a *divisor* of the order of G. Indeed, if the order of an element $a \in G$ is h, then a generates a cyclic subgroup of order h $\{e, a, a^2, \dots, a^{h-1}\}$. This being a subgroup of G, its order h must be a divisor of $|G|$.

1.4.4 Conjugacy classes

We have already introduced (see sec. 1.2.4) the relation of conjugacy between elements of a group G, ($g' \sim g \Leftrightarrow \exists h \in G$ such that $g' = h^{-1} g h$). We remarked that it is an equivalence relation. We can therefore consider the quotient of G (as a set) by this equivalence relation. The elements of the quotient set are the *conjugacy classes*. Any group element g defines a conjugacy class $[g]$:

$$[g] \equiv \{g' \in G \text{ such that } g' \sim g\} = \{h^{-1} g h\,, \text{ for } h \in G\} \ . \tag{1.4.85}$$

Basically, conjugation is the implementation of an inner automorphism (see sec. 1.2.10) of the group; we may think of it as a "change of basis" in the group (it is indeed so for matrix groups).

Often, one is interested in properties and quantities which are independent of conjugation. Such properties pertain to the conjugacy classes rather than to single elements.

1.4.4.1 Conjugacy classes of the symmetric groups and Young tableaux

The key fact that allows an efficient description the conjugacy classes of the symmetric group S_n is that the *structure* of the *cycle decomposition* of a permutation $P \in S_n$ is *invariant* under conjugation.

Indeed, suppose that P contains a cycle of length k, $(p_1, p_2, \ldots, p_k)$. Then a conjugate permutation $Q^{-1}PQ$ contains a cycle of the same length, namely $\big(Q^{-1}(p_1), Q^{-1}(p_2), \ldots, Q^{-1}(p_k)\big)$:

$$\begin{aligned}&\big(Q^{-1}(p_1), Q^{-1}(p_2), \ldots, Q^{-1}(p_k)\big) \xrightarrow{Q} (p_1, p_2, \ldots, p_k) \xrightarrow{P} (p_2, p_3, \ldots, p_1)\\ &\xrightarrow{Q^{-1}} \big(Q^{-1}(p_2), Q^{-1}(p_3), \ldots, Q^{-1}(p_1)\big) \ .\end{aligned} \tag{1.4.86}$$

Thus, *conjugacy classes* of S_n are in one-to-one correspondence with possible *structures of cycle decompositions*. If a permutation P is decomposed into r_l cycles of length l ($l = 1, \ldots n$), there is an obvious request

$$\sum_{l=1}^{n} r_l \, l = n \tag{1.4.87}$$

stating that the cycle decomposition must contain once and only once all elements $1, \ldots, n$. The conjugacy class of P is determined by the set of integers $\{r_l\}$ describing how many cycles of each length l appear in its decomposition. The possible conjugacy classes are thus in correspondence with the set of solutions to equation Eq. (1.4.87). These solutions, in turn, correspond to the set of *partitions* of n. A partition[12] of n is a set of integers $\{\lambda_i\}$, with

$$\sum_i \lambda_i = n \ , \qquad \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq 0 \ . \tag{1.4.89}$$

Indeed, a set $\{r_l\}$ of integers satisfying Eq. (1.4.87) is obtained from a partition $\{\lambda_i\}$ by setting

$$r_1 = \lambda_1 - \lambda_2 \, , \quad r_2 = \lambda_2 - \lambda_3 \, , \quad \ldots \, , \quad r_{n-1} = \lambda_{n-1} - \lambda_n \, , \quad r_n = \lambda_n \ . \tag{1.4.90}$$

Thus, conjugacy classes of S_n are in one-to-one correspondence with partitions of n, which in turn can be graphically represented by means of *Young tableaux* with n boxes, see Fig. **??**. In a Young tableaux, the boxes are distributed in rows of non-increasing length. The length of the i-th row is λ_i; the label r_l (the number of cycles of length l) corresponds instead to the difference between the length of the l-th and the $(l+1)$-th row.

The number of elements in a given conjugacy class $\{r_l\}$, that we call the order of the class and denote as $|\{r_l\}|$, is obtained as follows. The n elements $1, \ldots, n$ must be distributed in the collection $\{r_l\}$ of cycles, ordered as follows:

$$\underbrace{(\cdot)\ldots(\cdot)}_{r_1} \ \underbrace{(\cdot\cdot)\ldots(\cdot\cdot)}_{r_2} \ \underbrace{(\cdot\cdot\cdot)\ldots(\cdot\cdot\cdot)}_{r_3} \ \ldots \ . \tag{1.4.91}$$

[12] The number of partitions of n, $p(n)$ is expressed through the generating function

$$P(q) \equiv \sum_{n=0}^{\infty} p(n) q^n = \prod_{k=1}^{\infty} \frac{1}{1-q^k} \ . \tag{1.4.88}$$

The coefficient of q^n in the expansion of the infinite product given indeed the number of partitions of n.

There are n possible positions, so $n!$ possibilities. However, distributions differing for a permutation between cycles of the same length correspond to the same element (of course, (12)(45) is the same as (45)(12)); thus we must divide by $r_1!r_2!\ldots$. Moreover, in each cycle of length l we can make l periodic shifts (by 1,, by 2, ... by $l-1$) that leave the cycle invariant. Thus we must divide by $1^{r_1}2^{r_2}3^{r_3}\ldots$. Altogether we have obtained

$$|\{r_l\}| = \frac{n!}{r_1!\,2^{r_2}r_2!\,3^{r_3}r_3!\ldots} \ . \tag{1.4.92}$$

1.4.5 Conjugate subgroups

Let H be a subgroup of a group G. Let us consider

$$H_g \equiv \left\{h_g \in G \,:\, h_g = g^{-1}hg\,,\ \text{for } h \in H\right\} \ , \tag{1.4.93}$$

which we will also write simply as $H_g = g^{-1}Hg$. It is esay to see (check it) that H_g is a subgroup. The subgroups H_g are called *conjugate subgroups* to H.

1.4.6 Invariant subgroups

A subgroup H of a group G is called an *invariant* (or *normal*) subgroup if it coincides with all its conjugate subgroups: $\forall g \in G,\ H_g = H$. A rather practical alternative definition is that an invariant subgroup H is such that for any $h \in H$, all elements conjugated to h belong to H: if H contains an element, then it contains all its conjugacy class.

Left and right cosets (again) Given any subgroup H of G, we can define two equivalence relations in G:

$$\begin{aligned} g_1 \sim_L g_2 &\Leftrightarrow \exists\, h \in H \,:\, g_1 = hg_2 \ \text{(left equivalence)}\ , \\ g_1 \sim_R g_2 &\Leftrightarrow \exists\, h \in H \,:\, g_1 = g_2h \ \text{(right equivalence)}\ . \end{aligned} \tag{1.4.94}$$

Show that these are indeed equivalence relations. We can therefore consider the set of equivalence classes with respect to this left (right) equivalence, the *left (right) cosets*. The right coset G/H contains the left classes already introduced in sec. 1.4.2, that we write simply as gH. The right coset $H\backslash G$ contains the left classes Hg.

If H is an invariant subgroup, then the two equivalence relations of Eq. (1.4.94) coincide (show it):

$$g_1 \sim_L g_2 \Leftrightarrow g_1 \sim_R g_2 \ . \tag{1.4.95}$$

In this case, the right and left cosets coincide: $H\backslash G =$ for H an invariant subgroup.Indeed, in thsi case $gH = gHg^{-1}g = Hg$.

Eq. 1.4.96 amounts to the same as saying that the two equivalence relations are *compatible* with the group structure:

$$\left\{ \begin{array}{l} g_1 \sim g_2 \\ g_3 \sim g_4 \end{array} \right. \Leftrightarrow g_1g_3 \sim g_2g_4 \ , \tag{1.4.96}$$

where $\sim$ stands for $\sim_L$ (or $\sim_R$). Show indeed that requiring Eq. (1.4.96) for $\sim_{L,R}$ implies that they should coincide.

There is a further important property of G/H.

1.4.7 Factor groups

If H is an invariant subgroup of G, then G/H $(= H\backslash G)$ is a group, with respect to the product of classes defined as follows:

$$(g_1H)(g_2H) = g_1g_2H. \tag{1.4.97}$$

This product is well-defined. Infact (since $g_2H = Hg_2$ for H invariant) we have $g1H\, g_2H = g_1g_2HH$ but in this formal writing $HH = H$, as it is a subgroup. H itself is the identity of G/H, and the inverse of an element gH is $g^{-1}H$. We have thus a natural *homomorphism* from G to the factor group G/H, in which all elements of G belonging to the same conjugacy class are mapped to a single element in G/H.

A sort of converse to the above statement is also true: if $\phi : G \to G'$ is an homomorphism, then there exists an invariant subgroup $H \subset G$ such that $G' = G/H$.

Example Consider the group $n\mathbb{Z}$, namely the set of multiples of n: $\{\ldots, -2n, -n, 0, n, 2n, \ldots\}$, with the addition as group law. Show that it is an invariant subgroup of $\mathbb{Z}$. Show that the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the cyclic group $\mathbb{Z}_n$.

1.4.8 Centre, centralizers, normalizers

The centre of a group The centre $Z(G)$ of a group G is the set of all those elements of G that commute (in the group sense) with all the elements of G:

$$Z(G) = \left\{ f \in G \,:\, g^{-1}fg = f \,,\ \forall\, g \in G \right\} \ . \tag{1.4.98}$$

Show that $Z(G)$ is an Abelian subgroup of G.

Example: the centres of $\mathrm{U}(N)$ *and* $\mathrm{SU}(N)$ The centres of $\mathrm{U}(N)$ or $\mathrm{SU}(N)$ must consist of matrices A commuting with all unitary or special unitary matrices; the only possibility is that they are *proportiona*l to the unit matrix : $A = a\mathbf{1}$, with $a \in \mathbb{C}$. For A to be unitary, a must be a phase: $A = \mathrm{e}^{\mathrm{i}\alpha}\mathbf{1}$. For A to be spacial unitary, $\det A = a^N = 1$ implies that a is an N-th root of unity, so $A = \exp(\frac{2\pi \mathrm{i} k}{N})\mathbf{1}$. Altogether, we have

$$C\left(\mathrm{U}(N)\right) \cong \mathrm{U}(1) \ ; \qquad C\left(\mathrm{SU}(N)\right) \cong \mathbb{Z}_N \ . \tag{1.4.99}$$

The centralizer of a subset The *centralizer* $C(A)$ of a subset $A \subset G$ is the subset of G containing all those elements that commute with all the elements of A:

$$C(A) = \left\{ g \in G \,:\, \forall\, a \in A \,,\ (g)^{-1}ag = a \right\} \ . \tag{1.4.100}$$

A is (loosely speaking) in the centre of $C(A)$, which explains the nomenclature. If A contains a single element a, then $C(A)$ is simply called the centralizer of a and indicated as $C(a)$.

For any fixed element g, the product of the order of the conjugacy class of g and of its centralizer equals the order of G:

$$|[g]|\ |C(g)| = |G| \ . \tag{1.4.101}$$

Indeed, let $g' = u^{-1}gu$ be an element of $[g]$ different from g. Also the conjugation of g by $w = ut$, where $t \in C(g)$, gives g': in fact, $w^{-1}gw = u^{-1}t^{-1}gtu = u^{-1}gu = g'$. Thus, constructing $[g]$ as the set $\left\{u^{-1}gu \,:\, u \in G\right\}$ we obtain $|C(g)|$ times each distinct element.

Example: centralizers of permutations Let a permutation $P \in S_n$ be decomposed into a set of $\{r_l\}$ cycles. It is easy to convince oneself that any permutation that i) permutes between themselves the cycles of equal length in P or ii) effects arbitrary periodic shifts within any cycle (there are l possibilities for each cycle of length l) *commutes* with P. Thus, the number of permutations commuting with P is given by

$$|C(P)| = \prod_{l=1}^{n} r_l!\, l^{r_l} \ . \tag{1.4.102}$$

We see that this expression, together with Eq. (1.4.92) giving the order of the conjugacy class of P, is consistent with Eq. (1.4.101).

The normalizer of a subset The *normalizer* $N(A)$ of a subset $A \subset G$ is the subset of elements of G with respect to which A is invariant:

$$N(A) = \left\{ g \in G \ : \ (g)^{-1} A g = A \right\} \ . \tag{1.4.103}$$

If A contains a single element a, then $N(A)$ is simply called the normalizer of a and indicated as $N(a)$, and it coincides with the centralizer $C(a)$.

1.4.9 The derived group

The group of commutators, or *derived group* $\mathcal{D}(G)$ of a group G (ofted also indicated as G') is the group *generated* by the set of all group commutators in G (namely, it contains all group commutators and products thereof).

The derived group $\mathcal{D}(G)$ is normal in G, i.e. it is an *invariant subgroup*. Indeed, take an element of $\mathcal{D}[G]$ which is a commutator, say $ghg^{-1}h^{-1}$. Then, any conjugate of it by an element $f \in G$, $f^{-1}ghg^{-1}h^{-1}f$ is still a commutator, that of $f^{-1}gf$ and $f^{-1}hf$. To an element of $\mathcal{D}[G]$ that is a product of commutators, the reasoning applies with little modification.

The factor group $G/\mathcal{D}(G)$ is *Abelian*: it is the group obtained from G by "pretending" it is abelian. Another property is that any subgroup $H \subset G$ that contains $\mathcal{D}(G)$ is *normal*.

Example: the alternating groups A_n On the one hand, we know that the alternating group A_n contains the derived group of the symmetric group S_n:

$$A_n \supseteq \mathcal{D}(S_n) \ , \tag{1.4.104}$$

because the factor group S_n/A_n contains only two elements, and thus it is isomorphic to $\mathbb{Z}_2$ and in particular it is *Abelian*. On the other hand, since $A_n \subset S_n$, also

$$\mathcal{D}(A_n) \subseteq \mathcal{D}(S_n) \tag{1.4.105}$$

For $n = 2, 3, 4$, it is easy to construct directly the commutator subgroups $\mathcal{D}(S_n)$ and verify explicitely (do it as an exercise!) that

$$A_n = \mathcal{D}(S_n) \ , \quad (n = 2, 3, 4) \ . \tag{1.4.106}$$

For $n \geq 5$ we can proceed in a systematic way, by showing that

$$\mathcal{D}(A_n) = A_n \ , \quad (n \geq 5) \ . \tag{1.4.107}$$

Indeed, for $n \geq 3$, A_n certainly contains 3-cycles (arising from products of two exchanges). For $n \geq 5$ there exist couples of 3-cycles whose commutator is again a 3-cycle; for instance, commutator of (124) and (135) gives (124)(135)(142)(153)= ... = (123). The point is that such 3-cycles must have only one elemet in common; this is possible only for $n \geq 5$. In this case, $\mathcal{D}(A_n)$ contains some 3-cycle; by normality, it contains the entire conjugacy class, namely it contains *all* 3-cycles. But it is possible to show that, for $n \geq 5$, all *even* permutations can be generated by 3-cycles. Indeed, even permutations are generated by pairs of transpositions, so it is sufficient to show that every pair of transpositions can be obtained as products of suitable 3-cycles. If the two transposition have an elemet in common, then they directly correspond to a 3-cycle. Consider instead two exchanges with no element in common : $(a_1, a_2)(b_1, b_2)$, with a_i, b_i all distinct. Then, for $n \geq 5$, $\exists c \neq a_i, b_i$, and we have (check it!)

$$(a_1, a_2)(b_1, b_2) = (c, a_1)(c, a_2)(c, a_1)(c, b_1) = (a_1 c a_2)(a_1 c b_1)(b_2 c b_1) \ . \tag{1.4.108}$$

From Eq.s (1.4.104,1.4.105.1.4.107) it follows immediately that, for $n \geq 5$, the alternating group A_n coincides with the derived group of the symmetric group S_n:

$$A_n = \mathcal{D}(S_n) \ , \quad (n \geq 5) \ . \tag{1.4.109}$$

1.4.10 Simple, semi-simple, solvable groups

A given group G will in general admit a chain of invariant subgroups, called a *subnormal series*:

$$G = G_r \supset G_{r-1} \supset G_{r-2} \supset \ldots \supset G_1 \supset \{e\} \ , \tag{1.4.110}$$

with every G_i a normal subgroup.

Simple groups G is a *simple* group if it has *no proper invariant subgroup*. For simple groups, the subnormal series is minimal:

$$G \supset \{e\} \ . \tag{1.4.111}$$

Simple groups are the "hard core" of the possible group structures. There is no factor group G/H smaller than G out of which the group G could be obtained by some "extension", because there's no normal subgroup H other than the trivial one or G itself.

Semisimple groups G is a *semi-simple* group if it has *no proper invariant subgroup* which is *abelian*.

Solvable groups G is *solvable* if it admits a subnormal series Eq. (1.4.110) such that all the factor groups G/G_1, G_1/G_2, ..., G_{k-1}/G_k, ... are *abelian*.

Example: the symmetric groups S_n for $n \leq 4$ Let us write down the subnormal series for the symmetric groups of low order.

- S_2, isomorphic to $\mathbb{Z}_2$ is obviously solvable, being Abelian.
- For S_3, the subnormal series is

  $$S_3 \supset \mathcal{D}(S_3) = A_3 \supset \{e\} \ . \tag{1.4.112}$$

  Since $S_3/A_3 = \mathbb{Z}_{\not 2}$ and $A_3 = \{e, (123), (132)\}$, isomorphic to $\mathbb{Z}_3$, is abelian, the group S_3 is solvable.

- For S_4, the subnormal series is

$$S_4 \supset \mathcal{D}(S_4) = A_4 \supset \mathbb{D}_2 = \mathbb{Z}_2 \otimes \mathbb{Z}_2 \supset \{e\} \ . \tag{1.4.113}$$

The alternating group

$$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\} \tag{1.4.114}$$

is no longer abelian, as A_3 was. It admits several subgroups, for instance a $\mathbb{Z}_3$ subgroup $\{e, (123)((132)\}$, which are not invariant, and a single *invariant* subgroup $\mathbb{D}_2 = \{e, (12)(34), (13)(24), (14)(23)\}$. We have denoted this agroup as $\mathbb{D}_2$ as it is indeed isomorphic to the symmetry group of a 2-gon (i.e., a segment) in the plane (show it), which is also isomorphic to the *direct product* $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ (the notion of direct product will be discussed shortly). Since $|A_4|/|\mathbb{D}_2| = 12/4 = 3$, the factor group $A_4/\mathbb{D}_2$ can only be isomorphic to $\mathbb{Z}_3$, hence Abelian. Therefore the factor groups in the subnormal series Eq. (1.4.114) are all Abelian, and S_4 is solvable.

1.4.11 Some important example of simple groups

Cyclic groups of prime order Cyclic groups $\mathbb{Z}_p$ with p a prime are simple. Indeed, they are abelian, so every subgroup would be a normal subgroup. However, by Lagrange's theorem, the order of any subgroup of $\mathbb{Z}_p$ should be a divisor of p, which leaves only the improper subgroups $\{e\}$ and $\mathbb{Z}_p$ itself. What is absolutely non trivial, and therefore we will just mention it `:-)`, is that in fact the cyclic groups of prime order are the *only simple groups of odd order*.

The alternating groups A_n It is possible to show that the alternating groups A_n with $n \geq 5$ are simple. This can be shown by directly looking at the various possible expressions in terms of cycle of a supposed normal subgroup H of A_n. The key point are

i) Any element of A_n, i.e., any even permutation, for $n \geq 5$, is a product of 3-cycles.
ii) If H contains a 3-cycle, being normal, it contains all its conjugacy class, namely all three-cycles; then $H = A_n$ by i).
iii) If H contains an element made of two disjoint permutations, then by its normality it contains all elements of its conjugacy class, namely all elements with two disjoint permutations; multiplying certain such elements one certainly can reconstruct a 3-cycle, and we go back to ii).
iv) Looking at the various possible cycle decompositions of an element of H, one sees that by the normality of H one is forced to have in H elements that fall in cases ii)= or iii).

Solvable groups and solvable equations The theory of groups originated from the work of E. Galois regarding the properties of algebric equations of degree n (and, in particular, the possibility of solving such equations by radicals). Galois understood that many properties of an equations are encoded in a certain group, called after him the *Galois group* of the equation. In particular, the algebric equation is *solvable by radicals* iff its Galois group is *solvable*. The Galois group of a *generic* equation of degree n is S_n. THe symmetric group S_n is not solvable for $n \geq 5$: its subnormal series is just

$$S_n \supset A_n \supset \{e\} \ , \quad (n \geq 5) \ , \tag{1.4.115}$$

because A_n is simple, and it is not a solvable series because A_n is not Abelian. It follows that the generic equation of degree $n \geq 5$ cannot be solved by radicals (Abel-Ruffini theorem).

1.4.12 Homomorphism theorems

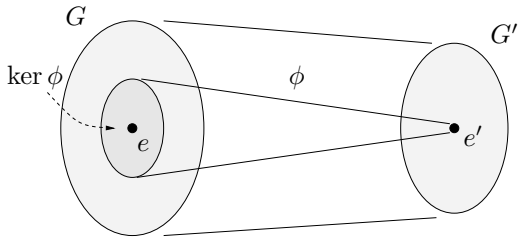

Figure 1.16. An homomorphism $\phi : G \mapsto G'$ and its kernel.

The important *homomorphism theorem*, also known as *first isomorphism theorem*, states that, given an homomorphism ϕ of G onto G':

i) the kernel of the homomorphism, $\ker\phi$, is an *invariant subgroup* of G;
ii) the restriction of the map ϕ to the factor group $G/\ker\phi$ gives rise to an *isomorphism* between $G/\ker\phi$ and G'.

The kernel of ϕ is the subset of G that is mapped onto the identity element e' of G':

$$\ker\phi = \{g \in G \,:\, \phi(g) = \mathrm{e}'\} \ . \tag{1.4.116}$$

It is immediate to see that $\ker\phi$ is a subgroup. It is also normal, because if $g \in \ker\phi$, then also its conjugates belongs to it: $\phi(u^{-1}gu) = \phi(u^{-1})\phi(g)\phi(u) = [\phi(u)]^{-1}e'\phi(u) = e'$; this proves i). In case of finite groups, if $\ker\phi$ has order m, then ϕ is an m-to-one mapping. Indeed, if k_i $(i = 1, \dots m)$ are the elements of $\ker\phi$, then the image $\phi(g)$ of a given element coincide with that of the elements $\phi(k_i g)$: The kernel being an invariant subgroup , we can define the factor group $G/\ker\phi$. Since the kernel of the map $\phi : G/\ker\phi \to G'$ contains now only the identity of the factor group, this map is an isomorphism. This proves ii).

There are other theorems regarding homomorphisms that we mention without proof.

The *correspondence* theorem states that, if $\phi : G \to G'$ is an homomorphism, then

i) the *preimage* $H = \phi^{-1}(H')$ of any subgroup H' of G' is a subgroup of G containing $\ker\phi$ (this generalizes the property of $\ker\phi = \phi^{-1}(e')$ of being a subgroup). If H' is normal in G', then so is H in G.
ii) If there is any other subgroup H_1 of G, containing $\ker\phi$, that is mapped onto H' by ϕ, then $H_1 = H$.

The above statements can be rephrased (via the first isomorphism theorem) in terms of factor groups:

i) Let L be a subgroup of a factor group G/N. Then $L = H/N$ for H a subgroup of G (containing N). If L is normal in G/N, then H is normal in G.
ii) If $H/N = H_1/N$, with H and H_1 subgroups of G containing N, then $H = H_1$.

The *factor of a factor* theorem states that if in the factor group G/N ther is a normal subgroup of the form M/N, with $M \supseteq N$, then M is a normal subgroup of G, and

$$G/M \sim (G/N)/(M/N) \ . \tag{1.4.117}$$

1.4.13 Direct products

The direct product $G \otimes F$ of two groups G and F is, as a set, the cartesian product of G and F:

$$G \times F = \{(g, f) \, : g \in G \, , \; f \in F\} \; . \tag{1.4.118}$$

Elements of $G \otimes F$ are couples, and $|G \otimes F| = |G| \, |F|$. The group operation is defined as follows. Elements of $G \otimes F$ have to multiplied "independently" in each entry, in the first entry with the product law of G, in the second with the product law of F:

$$(g, f)(g', f') = (gg', ff') \; . \tag{1.4.119}$$

Examples

- Construct the direct product group $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ and show it is isomorphic to the dihedral group D_2.
- Construct (and identify) the direct product $\mathbb{Z}_2 \otimes \mathbb{Z}_3$.

Conversely, given a group G, we say that it is the direct product of certain subgroups:

$$G = H_1 \otimes H_2 \otimes \ldots \otimes H_n \tag{1.4.120}$$

if and only if

i) elements belonging to different subgroups H_i commute;
ii) the only element common to the various subgroups H_i is the identity;
iii) any element $g \in G$ can be expressed as product

$$g = h_1 h_2 \ldots h_n \; , \qquad (h_1 \in H_1, \ldots h_n \in H_n) \; . \tag{1.4.121}$$

From ii), iii) it follows that the decomposition Eq. (1.4.121) is univoquely defined. Condition i) is equivalent to the fact that all the subgroups H_i are normal (show it).

Example The orthogonal group in three dimensions, O(3) is the direct product of the special orthogonal group SO(3) and of the matrix group (isomorphic to $\mathbb{Z}_2$) given by the two 3×3 matrices $\{\mathbf{1}, -\mathbf{1}\}$.

The direct product is the simplest way to build larger groups out of smaller building blocks. We can start from, say, two simple groups G and F to obtain a larger group $G \otimes F$ which is no longer simple as it admits G and F as normal subgroups. These normal subgroups are embedded into $G \times F$ in the simplest way; the homomorphism $\phi : \, (G \otimes F) \to G$ corresponds simply to neglect the F component: $\phi : \, (g, f) \mapsto g$.

1.4.14 Semi-direct products

A slightly more complicated construction, which is of great relevance in physics, to obtain a larger group from two building blocks is the semi-direct product. Let G and K be two groups, and assuume that G can be seen (that is, has an isomorphic image) as a *group of transformations* acting on K:

$$\forall \, g \in G \, , \quad g \, : \; k \in K \mapsto g(k) \in K \; . \tag{1.4.122}$$

Let us use the symbols $k_1 \circ k_2$ and $g_1 \cdot g_2$ for the group products in K and G respectively. The *semi-direct product* of G and K, denoted as $G\circledS K$, is the cartesian product of G and K as sets,

$$G\circledS K = \{(g,k) \,:\, g \in G\,,\ k \in K\}\ , \tag{1.4.123}$$

but the product in $G\circledS K$ is defined as follows:

$$(g_1,k_1)(g_2,k_2) = (g_1 \cdot g_2, k_1 \circ g_1(k_2))\ . \tag{1.4.124}$$

That is, "before" being multiplied by k_1, the element k_2 is acted upon by g_1. The inverse of an element of $G\circledS K$ is then given by (check it)

$$(g,k)^{-1} = \left(g^{-1}, [g^{-1}(k)]^{-1}\right)\ , \tag{1.4.125}$$

where the inverse g^{-1} is with respect to the product in G, while the "external" inverse in $[g^{-1}(k)]^{-1}$ is with respect to the product in K.

The semi-direct product $G\circledS K$ possesses an *invariant* subgroup $\tilde{K}$, isomorphic to K, given by the elements of the form (e,k), with e the identity of G and $k \in k$. Indeed, any conjugated of such an element is again in the subgroup $\tilde{K}$:

$$(g,h)^{-1}(e,h)(g,k) = \left(g^{-1}, [g^{-1}(h)]^{-1}\right)(g, h\circ k) = \left(e, [g^{-1}(h)]^{-1} \circ g^{-1}(h\circ k)\right)\ . \tag{1.4.126}$$

The subgroup, isomorphic to G, containing elements of the form (g,e), where e is the identity in K and $g \in G$, is instead *not* invariant.

Conversely, given a groups G, we say that is the semi-direct product $G = G_1\circledS G_2$ of two subgroups G_1 and G_2 iff:

i) G_2 is an invariant subgroup of G;
ii) G_1 and G_2 have only the identity in common;
iii) every element of G can be written as a product of an element of G_1 and one of G_2.

From ii) and iii) it follows that the decomposition iii) is unique.

The euclidean groups The euclidean groups Eucl_d are semi-direct products of the orthogonal group $\mathrm{O}(d)$ and of the abelian group T_d of d-dimensional translations. Their structure as semi-direct product has been discussed in in Eq.s (1.3.29,1.3.30) for the inhomogeneous rotation group ISO(2), the extension to Euclidean groups is immediate.

Consider in particular the group $\mathrm{ISO}(2) = \mathrm{SO}(2)\circledS T_2$. Every element $g(\theta,\mathbf{v}) = (R(\theta), T(\mathbf{v}))$ can be written as the product of rotation and a translation: indeed, according to the semi-direct product law Eq. (1.4.124), which in this specific case was described in Eq. (1.3.31), we have

$$g(\theta,\mathbf{b})g(-\theta,\mathbf{0}) = g(0,\mathbf{b})\ , \tag{1.4.127}$$

namely

$$g(\theta,\mathbf{b})R(\theta)^{-1} = T(\mathbf{b})\ , \tag{1.4.128}$$

whence

$$g(\theta,\mathbf{b}) = T(\mathbf{b})R(\theta)\ . \tag{1.4.129}$$

Writing the elements in this form, the semi-direct product law of the full group is determined from the products in T_2 and in S)(2) *plus* the "adjoint" action of SO(2) on the invariant translation subgroup T_2:

$$R(\theta)T(\mathbf{b})R^{-1}(\theta) = T(\mathcal{R}(\theta)\mathbf{b}) \tag{1.4.130}$$

Indeed,

$$\begin{aligned} T(\mathbf{b}_1)R(\theta_1)T(\mathbf{b}_2)R(\theta 2) &= T(\mathbf{b}_1)R(\theta_1)T(\mathbf{b}_2)R(\theta_1)^{-1}R(\theta_1)R(\theta 2) \\ &= T(\mathbf{b}_1)T(\mathcal{R}(\theta_1)\mathbf{b}_2)R(\theta_1)R(\theta 2) \\ &= T(\mathbf{b}_1 + \mathcal{R}(\theta_1)\mathbf{b}_2)R(\theta_1 + \theta_2) \ , \end{aligned} \tag{1.4.131}$$

in accordance with Eq. (1.3.30).

The Poincaré group Consider a Poincaré transformation of a quadri-vector x^μ:

$$x^\mu \to \Lambda^\mu{}_\nu x^\nu + c^\mu \ . \tag{1.4.132}$$

Here Λ is a pseudo-orthogonal matrix, $\Lambda \in \mathrm{O}(1,3)$, namely is a matrix such that $\Lambda^T \eta \Lambda = \eta$, where $\eta = \mathrm{diag}\,(-1,1,1,1)$ is the Minkowski metric, see sec. 1.3.7. These matrices implement rotaions corresponding to Lorenz transformations. The 4-vector c^μ is instead a translation parameter. Poincaré transformations are the *isometries* of the Minkowski space $\mathbb{R}^{1,3}$; they are the analogue of the transformations of the euclidean groups, but for the metric which they preserve, $\eta_{\mu\nu}$, being non-positive definite. Notice that the translation parameters, c^μ are 4-vectors and as such are acted upon by the Lorenz transformations: $c^\mu \to \Lambda^\mu{}_\nu c^\nu$. The composition of two Poincaré transformations gives

$$x^\mu \xrightarrow{(2)} \Lambda^\mu_{(2)\nu} x^\nu + c^\nu_{(2)} \xrightarrow{(1)} \Lambda^\mu_{(1)\nu}\left(\Lambda^\nu_{(2)\rho} x^\rho + c^\rho_{(2)}\right) + c^\mu_{(1)} = (\Lambda_{(1)}\Lambda_{(2)})^\mu{}_\rho x^\rho + (\Lambda_{(1)} c_{(2)})^\mu + c^\mu_{(1)} \ . \tag{1.4.133}$$

We see that the product law for the Poincaré group is

$$(\Lambda_{(1)}, c_{(1)})(\Lambda_{(2)}, c_{(2)}) = (\Lambda_{(1)}\Lambda_{(2)}, \Lambda_{(1)} c_{(2)} + c_{(1)}) \tag{1.4.134}$$

and the Poincaré group is the *semi-direct product* of the Lorenz group $\mathrm{O}(1,3)$ and the translation group.

1.4.15 Extensions of a group

We have said that we can regard simple groups as building blocks of general groups. In fact, the structure of a non-simple group G, with a nonrmal subgroup H, is substantially dependent on the structure of H and on that of the factor group G/H.

Extension of a group In fact we say that a group G is an *extension* of a group H by a group K iff there exists $\tilde{H}$, normal in G, such that $G/\tilde{H} = \tilde{K}$, with $\tilde{H}, \tilde{K}$ isomorphic to H, K: $\tilde{H} \simeq H$, $\tilde{K} \simeq K$.

The question is: how can be G be built out of $\tilde{H}$ and $\tilde{K}$? We will not exhamine the general case, but only a (quite important) subcase, that of so-called *splitting extensions*.

Splitting of a group Let H be a normal subgroup of G, and let X be a so-called (left) *transversal* of H, namely a set containing one and only one element from each coset of H in G. Suppose that X is in fact a subgroup of G. The situation is altogether that

$$H \text{ normal in } G \ , \ \ X \text{ subgroup of } G \ , \ \ XH = G \ , \ \ H \cap X = \{e\} \ . \tag{1.4.135}$$

In such a case, G is said to *slit over* H, and X is called a *complement* of H. Indeed, one can show that any element $g \in G$ can be written uniquely as a product $g = xh$, with $x \in X$ and $h \in H$, so $XH = G$, and every element of X lies in a distinct coset of H, so $H \cap X = \{e\}$. Conversely, if G splits over H, any complement X of H can be taken as a left transversal for H in G.

If G splits over H and X is a complement of H, then

$$G/H = HX/H = X/(H \cap X) = X \ , \tag{1.4.136}$$

that is, G is an extension of H by X. In other words, if G splits over H, G/H is isomorphic to any complement of H.

Splitting extension of a group One then introduces the following definition: G is a *splitting extension* of H by X if there exists $\tilde{H}$ normal in G and such that $\tilde{X} = G/H$ is isomorphic to X.

Reconstructing a group by splitting extension All the products in a group G obtained by the splitting extension of H by X are determined from:

a) the product law in H;
b) the product law in X;
c) an "adjoint" action of X on H, that is an homomorphism $\phi : X \to \mathrm{Aut}(H)$.

In simple words, take two elements $a, b \in G$. They will decompose as $a = A\alpha$ and $b = B\beta$, with $A, B \in X$ and $\alpha, \beta \in H$. Then we have

$$ab = A\alpha B\beta = ABB^{-1}\alpha B\beta \ , \tag{1.4.137}$$

where now AB is a product in X. Moreover, $B^{-1}\alpha B$ is again in H as H is normal, so $B \in X$ defines an automorphism of H. Assigning to each $B \in X$ an automorphism of H, namely point c) above, is thus a key point to determine the products in G. FInally, the product $B^{-1}\alpha B\beta$ is then within H.

Direct and semi-direct products It is not difficult to see that a direct product group $G = H \otimes K$ is in fact a particular splitting extension of H by K, in which the "adjoint" action of K on H is trivial (namely $B^{-1}\alpha B = \alpha$, $\forall\, B \in K$ and $\forall\, \alpha \in H$. Similarly, one can see that a semi-direct product group $G = K \circledS H$ is also a splitting extension of H by K.

1.4.16 Free groups

When a group G is generated by a set $X = \{x_i\}$ of elements, we say that $G = \mathrm{gp}\,(X)$, with

$$\mathrm{gp}\,(X) = \{x_1^{\pm 1} \dots x_n^{\pm 1} \ ,\ x_i \in X \ ,\ n \in \mathbb{N}\} \ . \tag{1.4.138}$$

Namely, $\mathrm{gp}\,(X)$ contains all the *words*, of any length n, formed with the generators x_i.

We name *reduced words* those words in which the obvious simplifications $x_i x_i^{-1}$ have been carried out. For instance, the non reduced word $xyy^{-1}xxy$ becomes has the reduced form $xxxy$.

Consider the infinite cyclic group $\mathrm{gp}\,(x)$ generated by a single generator x (mapping x into 1 and the product to be the addition, $\mathrm{gp}\,(x) \cong \mathbb{Z}$, hence the name). It has the obvious property that $(x^m = x^n) \Rightarrow m = n$, that is, different reduced expressions correspond to different elements.

The infinite cyclic group is the prototype of the so-called freely generated groups. We say that G is the *free group on* X (or that G is *freely generated by* X iff

i) $G = \mathrm{gp}\,(X)$, i.e., G is generated by X;
ii) distinct reduced products correspond to distinct elements.

I will use for brevity the notation $G = \mathrm{freegp}\,(X)$ for the gree group on X (this notation is not very diffuse). Intuitively, this means that there are no relations between the generators that could be used to write the same element in different ways. Note that if G is a free group, every element is written uniquely as $x_{i_1}^{\epsilon_1}....x_{i_n}^{\epsilon_n}$, so that we can associate to it the length n.

An important theorem (which we do not prove) states that every subgroup of a free group is free.

Another fundamental result (which again we mention without proof) is that every *finite* group G is the *homomorphic image* of some *free group*.

This last fact leads to the possibility of describing the group G by means of a *presentation*, consisting of *generators* and *relations*, as we already metioned in sec. 1.2.11.

To define precisely the notion of presentation of a group, we need the concept of *normal closure* $\mathcal{N}(S)$ of a subset $S \subset G$. It is the intersection of all the normal subgroups of G containing S. It is a normal subgroup of G (check it) containing S, adn can be written as

$$\mathcal{N}(S) = \mathrm{gp}\,\left(\{g^{-1}sg\,:\;s \in S\,, g \in G\}\right)\;. \tag{1.4.139}$$

A *presentation* is a couple $(X; R)$ with X a set of generators, R a set of words in $\mathrm{freegp}\,(X)$ A presentation $(X; R)$ defines a group denoted as $\mathrm{gp}\,(X; R)$ as follows:

$$\mathrm{gp}\,(X; R) = \mathrm{freegp}\,(X)/\mathcal{N}(R)\;, \tag{1.4.140}$$

namely as the quotient of the free group on X by the normal closure generated by the set of relations.

Example Let $X = \{a\}$ consist of a single generator, and let $R = \{a^2\}$ contain the single word a^2. The free group on X is then

$$\mathrm{freegp}\,(X) = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}\;,$$

so that $\mathrm{freegp}\,(X) \cong \mathbb{Z}$, and the normal closure of R is

$$\mathcal{N}(R) = \{\ldots, a^{-4}, a^{-2}, e, a^2, a^4, \ldots\}\;,$$

, so that $\mathcal{N}(R) \cong 2\mathbb{Z}$. The presentation $(X; R)$ defines the group

$$\mathrm{freegp}\,(X)/\mathcal{N}(R) \cong \mathbb{Z}/(2\mathbb{Z}) \cong \mathbb{Z}_2\;.$$

A group G *admits a finite presentation* iff it is isomorphic to some $\mathrm{gp}\,(X; R)$.

Example The homotopy group of a two-torus T_2, see sec. 1.3.16, arises naturally as $\mathrm{gp}\,(X; R)$, where $X = \{a, b\}$ are the two simplest non-trivial homotopy classes and $R = \{aba^{-1}b^{-1}$, namely the single relation is the commutator. As we discussed, it follows that $\Pi_1(T_2) = \mathrm{gp}\,(X; R)$ is abelian and is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$ (using the additive notation). More in general, if $X = \{a_i\}$, $i = 1, \ldots, n$ and R contains all the commutators: $R = \{a_i a_j a_i^{-1} a_j^{-1}\,, \forall i, j\}$, it follows that

$$\mathrm{gp}\,(X; R) = \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n \text{ times}}\;.$$

1.4.17 Finitely generated Abelian groups

Additive notation For Abelian groups, the *additive* notation is often used. The group product of two elements is indicated as $a + b$ and powers of an element become integer multiples of it: $a \to a + a = 2a \to a + a + a = 3a \ldots$; the inverse of a is denoted as $-a$, and the identity as 0. One speaks of direct sum $G \oplus G'$ instead of direct product of groups. If $G = \oplus_{i=1}^{n} G_i$, every g in G can be decomposed uniquely (up to irrelevat reordering) as $g = g_1 + g_2 + \ldots + g_n$. A coset of an element g with respect to a subgroup H is denoted as $g + H$.

Free Abelian groups G is a *free abelian group* (on $X = \{x_i\}$) iff

i) $G = \mathrm{gp}\,(X)$
ii) $G = \oplus_i G_i$, with every $G_i = \mathrm{gp}\,(x_i)$ an *infinite cyclic* group: $G_i \cong \mathbb{Z}$.

For instance, the free Abelian group on two generators x, contains all words formed with the two generators assuming that the product is Abelian; namely, we may seea the two generators joined by a *direct product*:

$$X = \{(x, 0), (0, y)\}\ , \ \Rightarrow \ \mathrm{gp}\,(X) = \{(nx, my)\,,\ n, m \in \mathbb{Z}\} \cong \mathbb{Z} \oplus \mathbb{Z}$$

(we are using the additive notation).

Every Abelian group is the homomorphic image of some free Abelian group. If g_i are the elements of G, the free Abelian group $F = \oplus_i \mathrm{freegp}\,(x_i)$ where the generators x_i can be put into 1-to-1 correspondence with the elements g_i. The map $x_i \to g_i$ extends naturally to an homomorphism from F to G.

Classification of Abelian groups Abelian groups can be distinguished in the following classes.

- *Torsion-free groups* The Abelian group G is a torsion-free group iff every element g in G (except the identity) is of infinite order.
  Examples of such groups are $\mathbb{Z}$ and $\mathbb{Q}$ (as additive groups).
- *Torsion groups* The Abelian group G is a torsion group iff every element g of G is of finite order.
  Examples:
  - In a cyclic group $\mathbb{Z}_n$, all elements are of finite order. In general, if G is finite, all its elements are of finite order.
  - The factor group $\mathbb{Q}/\mathbb{Z}$ is a torsion group. Indeed, an element $r \in \mathbb{Q}$ is of the form $r = m/n$, with $m, n \in \mathbb{Z}$. Elements of $\mathbb{Q}/\mathbb{Z}$ are coosets $[r] \equiv r + \mathbb{Z}$ (i.e., "up to integers"). But the n-th "power" of $[r]$, is given by $[nr] = nr + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$, i.e. the identity class. So every element $[r] = [m/n]$ of $\mathbb{Q}/\mathbb{Z}$ has order equal to the denominator n of r.
- *Mixed groups* The Abelian group G is a torsion group iff it contains elements both of finite and infinite order.
  An example is provided by $\mathbb{C} \setminus \{0\}$, the multiplicative group of complex numbers. Indeed, the elements $\exp(2\pi \mathrm{i}/n)$ have order n. Any element z with $|z| \neq 1$ has infinite order (only $z^0 = 1$).

The torsion subgroup Let G be an Abelian group. Let $T(G)$ be the subset of elements of G that are of finite order. $T(G)$ is a subgroup of G, called the *torsion subgroup*. Indeed (in additive notation), let $a, b \in G$ have finite orders $m = |a|, n = |b|$, so that $ma = 0$, $nb = 0$. Then $mn(a - b) = mna - mnb = 0$, so that also $a - b$ has finite order mn.

An Abelian group can be finitely generated without being freely generated; it may be given by a presentation $(X; R)$. The typical example are the cyclic groups $\mathbb{Z}_n$, with X containing a single generator: $X = \{a\}$, and R consisting of the single word a^n. The non-trivial fact is that in fact this type of relations are the only that really give rise to different Abelian group structures. Other relations, such as, for instance, those imposing that two generators commute, are in fact equivalent to assesrting that the group decomposes in a direct sum of smaller groups, see above.

One has in fact the important result that *every finitely generated Abelian group* G is isomorphic to a *direct sum of cyclic groups*, of infinite or finite order:

$$G = \mathbb{Z} \oplus \ldots \mathbb{Z} \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k} \ . \tag{1.4.141}$$

Moreover, sometimes the finite cyclic groups $\mathbb{Z}_n$ can in turn be decomposed into direct sums of smaller cyclic groups. More precisely:

- The groups $\mathbb{Z}_{p^q}$, with p a prime, and $q \in \mathbb{N}$, cannot be decomposed.
- The groups $\mathbb{Z}_n$ with a generic $n = p_1^{q_1} p_2^{q_2} \ldots$. with p_i primes, can be decomposed as

$$\mathbb{Z}_n = \oplus_i \mathbb{Z}_{p_i^{q_i}} \ . \tag{1.4.142}$$

For instance, $\mathbb{Z}_4$ cannot be further decomposed: $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$. Indeed, all elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are of order 2, while in $\mathbb{Z}_4$ we have elements of order 4. We have instead $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. In this case, the element $(a, b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_3$, with a the generator of $\mathbb{Z}_2$ and b the generator of $\mathbb{Z}_3$, is of order 6 (the m.c.m. of 2 and 3). It is along these line that one proves in general Eq. (1.4.142).

Altogether, using Eq. (1.4.142) in Eq. (1.4.141), we see that every finitely generated Abelian group G can be written "canonically" as

$$G = \mathbb{Z} \oplus \ldots \mathbb{Z} \oplus \mathbb{Z}_{p_1^{q_1}} \oplus \ldots \oplus \mathbb{Z}_{p_m^{q_m}} \ . \tag{1.4.143}$$

The type of decomposition individuated by the canonical decomposition Eq. (1.4.143) identifies G up to isomorphisms; i.e., all isomorphic finitely generated Abelian groups have the same decomposition type and an abstract group structure of this type is individuated by a decomposition as in Eq. (1.4.143).